Positive Technologies Next Generation Firewall версия 1.11

Руководство администратора

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 12.08.2026

Содержание

1. Об этом документе ... 8
   1.1. Условные обозначения ... 8
   1.2. Другие источники информации о PT NGFW ... 8
2. О PT NGFW ... 10
   2.1. Назначение PT NGFW ... 10
   2.2. Дополнительные возможности ... 11
   2.3. Использование PT NGFW ... 12
3. Обновление PT NGFW ... 17
   3.1. Обновление системы управления ... 18
   3.2. Обновление выделенных сборщиков журналов ... 20
   3.3. Обновление межсетевых экранов ... 21
      3.3.1. Подготовка к обновлению ... 21
      3.3.2. Обновление одиночного межсетевого экрана ... 21
      3.3.3. Обновление кластера межсетевого экрана ... 22
   3.4. Действия для обновления устройств с АМДЗ ... 24
      3.4.1. Действия с ПАК «Соболь» ... 24
      3.4.2. Действия с «Аккорд-АМДЗ» ... 25
   3.5. Загрузка с установочного носителя ... 28
   3.6. Обновление баз контента ... 30
4. Развертывание виртуального PT NGFW ... 36
   4.1. Программные и аппаратные требования ... 36
   4.2. Развертывание системы управления ... 38
      4.2.1. Развертывание виртуальной машины в среде ESXi ... 39
      4.2.2. Развертывание виртуальной машины в среде KVM ... 45
      4.2.3. Первоначальная настройка ... 47
   4.3. Развертывание виртуальной машины PT NGFW ... 47
      4.3.1. Развертывание виртуальной машины в среде ESXi ... 48
      4.3.2. Развертывание виртуальной машины в среде KVM ... 54
      4.3.3. Первоначальная настройка ... 59
   4.4. Развертывание системы мониторинга ... 59
      4.4.1. Развертывание виртуальной машины в среде ESXi ... 59
      4.4.2. Настройка интерфейса управления (MGMT) ... 64
      4.4.3. Настройка DNS-сервера в ОС ... 65
      4.4.4. Настройка синхронизации времени с NTP-сервером ... 65
      4.4.5. Первоначальная настройка ... 66
5. Подготовка к работе ... 67
   5.1. Настройка необходимых сетевых доступов ... 68
   5.2. Настройка системы управления ... 75
      5.2.1. Настройка интерфейса управления (MGMT) ... 75
      5.2.2. Настройка синхронизации времени с NTP-сервером ... 79
      5.2.3. Настройка IP-адреса сетевого интерфейса узла системы управления для возможности загрузки обновлений на межсетевые экраны ... 80
      5.2.4. Настройка сборщиков журналов ... 80

5.3. Настройка межсетевого экрана ... 80
5.3.1. Изменение имени хоста (hostname) ... 82
5.3.2. Настройка интерфейса управления (MGMT) ... 83
5.3.3. Подключение межсетевого экрана к DNS-серверу (серверам) для разрешения FQDN в политиках безопасности ... 84
5.3.4. Настройка синхронизации времени с NTP-сервером ... 85
5.3.5. Подключение межсетевого экрана к системе управления ... 85
5.3.6. Первичная настройка интерфейсов ... 87
5.4. Настройка системы мониторинга ... 88
5.4.1. Настройка сервера СУБД и визуализации ... 89
5.4.2. Установка и настройка клиента ... 97
5.5. Настройка выделенного сборщика журналов ... 106
5.5.1. Настройка интерфейса управления (MGMT) ... 107
5.5.2. Настройка синхронизации времени с NTP-сервером ... 111
6. Принцип работы ... 112
6.1. Режимы работы сетевых интерфейсов ... 113
6.2. Принципы обработки трафика ... 113
6.3. Инспекция SSL/TLS-трафика ... 121
6.4. Правила межсетевого экрана ... 123
6.5. Группы устройств ... 125
6.6. Виртуальные контексты ... 126
6.7. Виртуальные роутеры ... 127
6.8. Зоны безопасности ... 127
6.9. Ролевая модель ... 128
7. Вход в PT NGFW ... 130
8. Интерфейс PT NGFW ... 131
9. Начало работы ... 133
10. Управление учетными записями ... 134
11. Работа с сертификатами ... 136
11.1. Установка собственного сертификата для веб-интерфейса системы управления ... 136
11.2. Настройка mTLS для защиты взаимодействия PT NGFW с системой управления ... 137
11.3. Установка собственного сертификата для расшифрования TLS/SSL-трафика ... 139
11.4. Установка сертификата удостоверяющего центра на сетевых узлах пользователей ... 139
12. Добавление устройств ... 141
13. Настройка сетевых интерфейсов ... 144
14. Настройка маршрутизации ... 146
14.1. Статическая маршрутизация ... 146
14.2. Динамическая маршрутизация ... 147
14.2.1. Настройка OSPF ... 148
14.2.2. Настройка BGP ... 159
14.2.3. Перераспределение маршрутов ... 169
14.3. Маршрутизация по политикам (PBR) ... 171
14.4. Профили проверки доступности ... 174
14.5. BFD ... 179
15. Виртуальные соединения (vWire) ... 183
16. Работа с правилами межсетевого экрана ... 184

17. Объекты ... 191
18. Категории URL ... 195
18.1. Принцип категоризации трафика ... 195
18.2. Порядок указания URL и выражений ... 196
18.3. Примеры wildcard-выражений ... 198
18.4. Добавление категории URL ... 207
18.5. Предустановленные категории ... 208
19. Работа с группами устройств ... 209
20. Работа с виртуальными контекстами ... 210
21. Работа с виртуальными роутерами ... 211
22. IPS (система предотвращения вторжений) ... 212
23. Антивирусная проверка трафика ... 222
24. NAT ... 223
24.1. Пример настройки Source NAT ... 225
24.2. Примеры настройки Destination NAT ... 227
24.3. Пример двойной трансляции (Twice NAT) ... 231
24.4. Пример U-Turn NAT (Hairpin NAT, Loopback NAT, Reflection NAT) ... 233
24.5. Proxy ARP ... 236
25. Агрегирование каналов (LAG, LACP) ... 238
25.1. Создание LAG-интерфейса ... 239
25.2. Агрегирование каналов в кластере ... 240
25.3. Примеры настройки LACP со сторонним оборудованием ... 242
25.3.1. Диагностика LAG LACP на PT NGFW ... 256
25.3.2. Диагностика LAG LACP на Juniper MX ... 258
26. Тайм-ауты сетевых сессий ... 262
26.1. Настройка тайм-аутов для устройства ... 263
26.2. Настройка тайм-аутов для виртуального контекста ... 264
26.3. Настройка тайм-аутов для сервиса ... 266
26.4. Особенности настройки тайм-аутов для сервисов ... 267
27. Зеркалирование расшифрованного трафика ... 268
28. Подключение к Active Directory ... 269
28.1. Схема работы ... 269
28.2. Известные ограничения ... 271
28.3. Настройка сервера Microsoft Active Directory ... 271
28.3.1. Установка роли AD на Windows-сервер (опционально для тестов) ... 272
28.3.2. Создание учетной записи сервисного пользователя ... 276
28.3.3. Добавление учетной записи NETWORK SERVICE в группу безопасности ... 278
28.3.4. Настройка хостового межсетевого экрана на контроллере домена ... 287
28.3.5. Выпуск сертификатов на сервере системы управления ... 288
28.3.6. Запуск службы WinRM ... 291
28.3.7. Настройка журналирования событий безопасности ... 296
28.4. Настройка агента Identity Control (IDC) ... 304
28.4.1. Настройка PT NGFW для подключения к агенту ... 305
28.4.2. Настройка агента подключения (на сервере системы управления) ... 305
28.4.3. Настройка RADIUS-серверов в агенте Identity Control ... 310

28.5. Полезные команды, журналы, статистика ... 312
28.6. Настройка подключения к WEC ... 316
28.7. Пример настройки нескольких подключений LDAP и WinRM ... 332
29. Captive Portal ... 335
30. Кластер межсетевого экрана ... 340
30.1. Виртуальный MAC-адрес и GARP ... 343
30.2. Работа в виртуальной среде в режиме маршрутизации ... 353
30.3. Режим vWire ... 354
30.4. Приоритет устройств в кластере ... 357
30.5. Приоритетное замещение (Preemption) ... 357
30.6. Graceful restart (OSPF, BGP) ... 358
30.7. Состояния узлов кластера ... 361
30.8. Состояния кластера ... 363
30.9. Состояния конфигурации кластера ... 364
30.10. Требования для создания кластера active-standby ... 365
30.11. Создание кластера ... 371
30.12. Процесс объединения узлов в кластер ... 380
30.13. Изменение параметров кластера ... 384
30.14. Приостановка узла в кластере (Suspend) ... 385
30.15. Мониторинг устройств кластера ... 390
30.16. Split-brain (раскол кластера) ... 393
30.17. Мониторинг интерфейсов кластера ... 394
30.18. Удаление устройств из кластера ... 399
30.19. Добавление устройств в кластер ... 404
30.20. Удаление кластера ... 410
31. Кластер системы управления ... 414
32. Туннелирование GRE и GRE over IPsec ... 419
32.1. Настройка туннеля GRE ... 419
32.2. Настройка туннеля GRE over IPsec ... 421
33. IPsec site-to-site VPN ... 426
33.1. Преимущества Site-to-Site VPN ... 426
33.2. Принцип работы и условия использования ... 427
33.3. Создание Site-to-Site VPN-соединения ... 429
34. Remote Access VPN ... 435
34.1. Настройка RA VPN-шлюза ... 435
34.1.1. Генерация сертификатов шлюза ... 436
34.1.2. Создание туннеля RA VPN ... 439
34.2. PT VPN Agent ... 444
34.2.1. Аппаратные и программные требования ... 445
34.2.2. Установка PT VPN Agent ... 445
34.2.3. Обновление PT VPN Agent ... 446
34.2.4. Удаление PT VPN Agent ... 447
34.2.5. Интерфейс PT VPN Agent ... 447
34.2.6. Настройка PT VPN Agent ... 449
34.2.7. Просмотр журналов ... 451

35. DHCP relay ... 452
35.1. Обработка DHCP-сообщений при использовании DHCP relay в PT NGFW ... 452
35.2. Настройка DHCP relay ... 454
36. ICAP ... 457
36.1. Реализация отправки данных по ICAP в PT NGFW ... 458
36.2. Настройка отправки данных по ICAP ... 462
37. Аутентификация пользователей ... 470
38. SNMP-мониторинг ... 472
38.1. Настройка и запуск SNMP-агента ... 473
38.2. Поддерживаемые объекты из стандартных MIB ... 477
38.3. Перечень объектов из проприетарной MIB ... 481
39. Работа с журналами ... 482
39.1. Настройка сборщиков журналов ... 483
39.2. Просмотр журналов ... 484
39.3. Передача журналов по протоколу syslog ... 485
39.4. Работа с системным журналом ... 487
39.5. Параметры событий, регистрируемых в журналах ... 487
39.6. Параметры syslog-сообщений ... 502
39.7. Причины завершения сессий ... 518
40. Описание графиков дашборда PT NGFW Lite ... 521
41. Резервное копирование и восстановление ... 530
42. Предустановленные категории URL ... 533
43. Сетевые протоколы, обнаруживаемые PT NGFW ... 550
44. Промышленные протоколы, обнаруживаемые PT NGFW ... 555
45. Использование API ... 557
46. Интерфейс командной строки (CLI) ... 559
46.1. Вход и работа в CLI ... 559
46.2. Операционные команды ... 560
46.2.1. Синтаксис команд ... 560
46.2.2. Иерархическое представление команд ... 561
46.2.3. Команды на уровне устройства ... 562
46.2.4. Команды на уровне виртуального контекста ... 565
47. Получение телеметрии ... 578
48. Часто используемые команды ... 579
49. О технической поддержке PT NGFW ... 581

1. Об этом документе

Руководство администратора содержит пошаговые инструкции и справочную информацию об использовании Positive Technologies Next Generation Firewall (далее также — PT NGFW). В руководстве описаны ключевые и дополнительные функции PT NGFW, а также настройка функций для выполнения конкретных задач.

Руководство адресовано специалистам, администрирующим PT NGFW.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о PT NGFW (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT NGFW

Вы можете найти дополнительную информацию о PT NGFW на портале технической поддержки.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 49).

2. О PT NGFW

В этом разделе

Назначение PT NGFW (см. раздел 2.1)

Дополнительные возможности (см. раздел 2.2)

Использование PT NGFW (см. раздел 2.3)

2.1. Назначение PT NGFW

PT NGFW — многофункциональный межсетевой экран с функциями глубокого анализа и фильтрации трафика, сочетающий возможности традиционных межсетевых экранов с современными системами защиты на уровне приложений, пользователей и контента.

PT NGFW предназначен для комплексной защиты корпоративных сетей различного масштаба и высоконагруженных систем. Он защищает периметр и внутренние сегменты корпоративной сети за счет микро- и макросегментации, а также может защищать каналы передачи данных между датацентрами и облачную инфраструктуру.

PT NGFW в зависимости от исполнения выпускается на базе специализированных аппаратных платформ, либо в виде образов виртуальной машины для развертывания на платформах виртуализации.

Возможности PT NGFW:

— Анализ и фильтрация трафика на сетевом и транспортном уровнях с контролем состояния сессий.

— Расширенная инспекция трафика (Deep Packet Inspection) с целью анализа сетевой активности и фильтрации трафика приложений и прикладных протоколов.

— Расшифрование и анализ SSL/TLS – трафика.

— Обнаружение и нейтрализация сетевых вторжений.

— URL- и контент-фильтрация трафика.

— Зеркалирование расшифрованного трафика с целью его анализа внешними системами информационной безопасности.

— Поддержка виртуальных роутеров и виртуальных контекстов — логических сетевых устройств, обладающих независимыми таблицами маршрутизации и набором политик безопасности, соответственно.

— Задание политик безопасности для пользователей сети.

— Проверка данных, передаваемых по протоколам HTTP и HTTPS, потоковым антивирусом.

— Интеграция с другими решениями в области информационной безопасности и сетевых технологий.

2.2. Дополнительные возможности

Следующие функции дополняют возможности PT NGFW по обработке сетевого трафика и интеграции со сторонним оборудованием (коммутаторами, маршрутизаторами, источниками бесперебойного питания) и внешними информационными системами:

Поддержка сетевых функций

— Поддержка виртуальных локальных сетей VLAN IEEE 802.1Q.

— Трансляция сетевых адресов источника (SNAT) и назначения (DNAT).

— Агрегирование сетевых интерфейсов (LAG, LACP) и балансировка нагрузки в агрегированных каналах.

— Объединение удаленных сетей с помощью IPsec site-to-site VPN.

— Работа в режиме прозрачного моста с помощью технологии vWire.

Поддержка сетевых служб

— Статическая и динамическая маршрутизация IP-трафика.

— Встроенный агент DHCP-relay.

Централизованное управление и мониторинг

— Централизованная система управления для управления и настройки PT NGFW с помощью веб-интерфейса.

— Централизованная система мониторинга.

— Диагностика основных параметров PT NGFW по протоколу SNMP.

— Централизованный доступ к сборщикам журналов с целью анализа операций и событий информационной безопасности.

Интеграция с информационными системами

— REST API для интеграции с внешними информационными системами.

— Использование внешнего портала аутентификации для идентификации пользователей сети.

— Перенаправление трафика для обработки внешними серверами и сетевыми песочницами по протоколу ICAP.

— Экспорт журналируемых событий по протоколу syslog.

Резервирование и отказоустойчивость

— Работа в отказоустойчивом кластере Active – Standby.

— Резервирование системы управления и сборщиков журналов.

2.3. Использование PT NGFW

Общие рекомендации

Вы можете использовать PT NGFW для защиты корпоративной сети от внешних угроз, разграничения доступа сетевых узлов и пользователей, а также для управления доступом к внутренним и внешним сетевым ресурсам. Для этого PT NGFW устанавливается на границах защищаемых подсетей или на периметре корпоративной сети, чтобы трафик проходил через него. Таким образом локальная сеть разделяется на сегменты, обладающие индивидуальным набором политик безопасности. Для управления PT NGFW используется выделенная локальная сеть, обеспечивающая связь между компонентами PT NGFW и доступ администратора сети к системе управления.

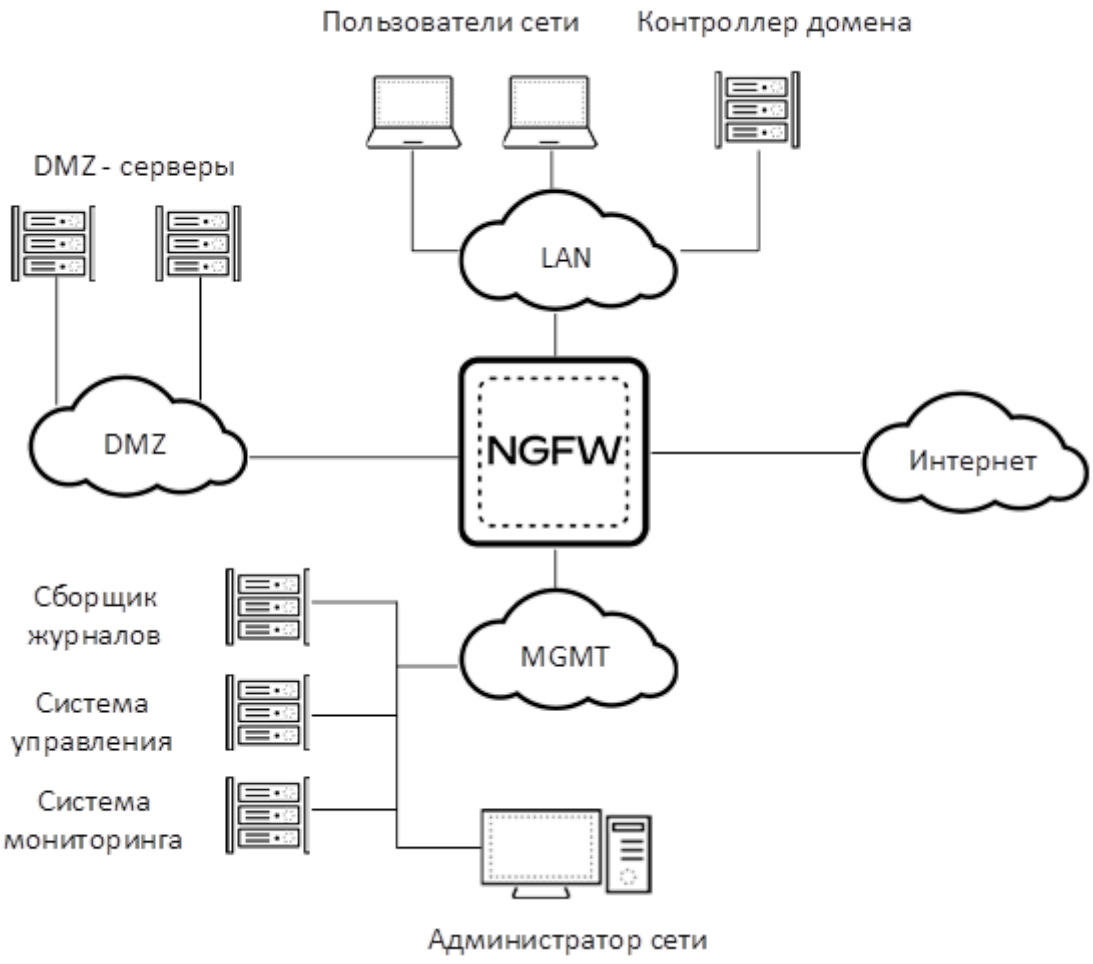


Рисунок 1. Схема развертывания PT NGFW в корпоративной сети

В корпоративной сети разворачиваются следующие компоненты PT NGFW:

— Система управления — обязательный компонент, предназначенный для централизованного конфигурирования и управления межсетевыми экранами с помощью веб-интерфейса. Система управления может быть развернута на базе выделенной аппаратной платформы, либо установлена в виртуальном исполнении на платформу виртуализации.

— Межсетевой экран PT NGFW — основной компонент (ядро) системы, осуществляющий анализ и фильтрацию трафика. Межсетевой экран не имеет собственного пользовательского интерфейса и его настройка и управление осуществляется с помощью системы управления. Узлы PT NGFW подключаются к сети одним из способов в зависимости от конфигурации сети и выполняемых функций, а также могут быть объединены в отказоустойчивый кластер.

— Система мониторинга — сетевой узел для централизованного сбора и хранения параметров работоспособности и данных телеметрии с узлов PT NGFW для их последующего просмотра и визуализации с помощью графического интерфейса. Необязательный компонент системы.

— Сборщик журналов — сетевой узел, используемой системой журналирования PT NGFW для централизованной регистрации и хранения событий. Один узел PT NGFW может быть подключен к нескольким сборщикам журналов, при этом для записи событий используется только основной сборщик, а остальные задействуются при недоступности основного. Сборщик журналов по умолчанию разворачивается на узле системы управления либо на базе выделенной аппаратной платформы (при повышенных требованиях к производительности системы журналирования).

Способы подключения PT NGFW к сети

Прозрачный режим (L2 transparent) — межсетевой экран устанавливается в разрыв канала связи либо перед, либо после пограничного маршрутизатора, при этом сетевые интерфейсы PT NGFW работают в режиме vWire и не имеют присвоенных IP-адресов.

Если при этом требуется трансляция адресов, то NAT настраивается на пограничном маршрутизаторе, а PT NGFW устанавливается перед ним.

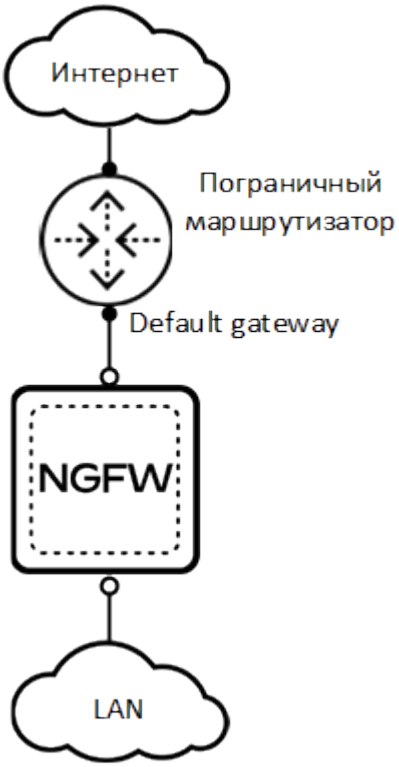


Рисунок 2. Прозрачный режим

Режим маршрутизации — PT NGFW устанавливается в разрыв канала связи и на нем настраиваются IP-адресация и правила маршрутизации. Такой режим может быть использован при необходимости маршрутизации трафика между несколькими подсетями, либо для реализации сложной маршрутизации на основе политик.

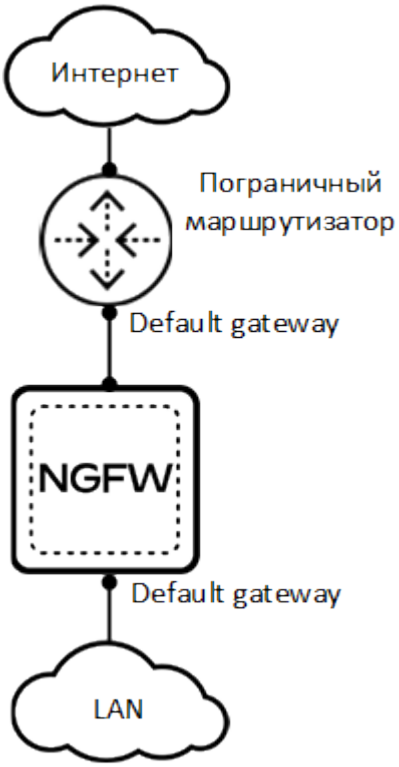


Рисунок 3. Режим маршрутизации

Прозрачный режим без разрыва канала связи — применяется, когда нет возможности установить PT NGFW в разрыв канала связи. Для этого пограничный маршрутизатор должен поддерживать функцию VRF (virtual routing and forwarding) и на нем выделяются два сетевых порта LAN и WAN, к которым подключается PT NGFW в прозрачном режиме.

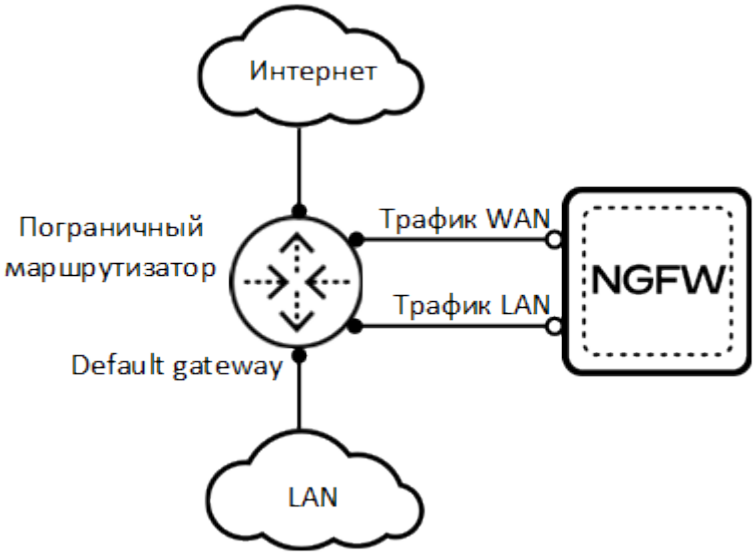


Рисунок 4. Прозрачный режим без разрыва канала

Прозрачный режим с преобразованием VLAN ID — в этом режиме и входящий, и исходящий трафик передаются между пограничным маршрутизатором и PT NGFW через один сетевой интерфейс (группу интерфейсов) и различаются VLAN-метками. При этом физическому сетевому порту PT NGFW сопоставляются два сабинтерфейса, различающиеся своими VLAN ID и работающие в режиме vWire. При передаче трафика между такими сабинтерфейсами происходит преобразование VLAN-меток, образуя прозрачный мост между двумя VLAN-подсетями.

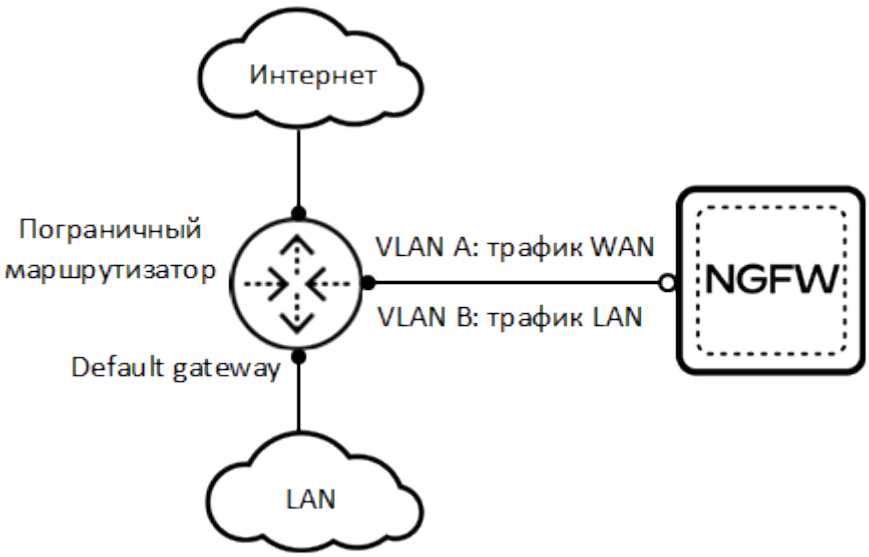


Рисунок 5. Прозрачный режим с преобразованием VLAN ID

Режим маршрутизации с преобразованием VLAN ID — этот режим аналогичен прозрачному режиму с преобразованием VLAN ID, но сабинтерфейсы PT NGFW работают в режиме маршрутизации и имеют IP-адреса.

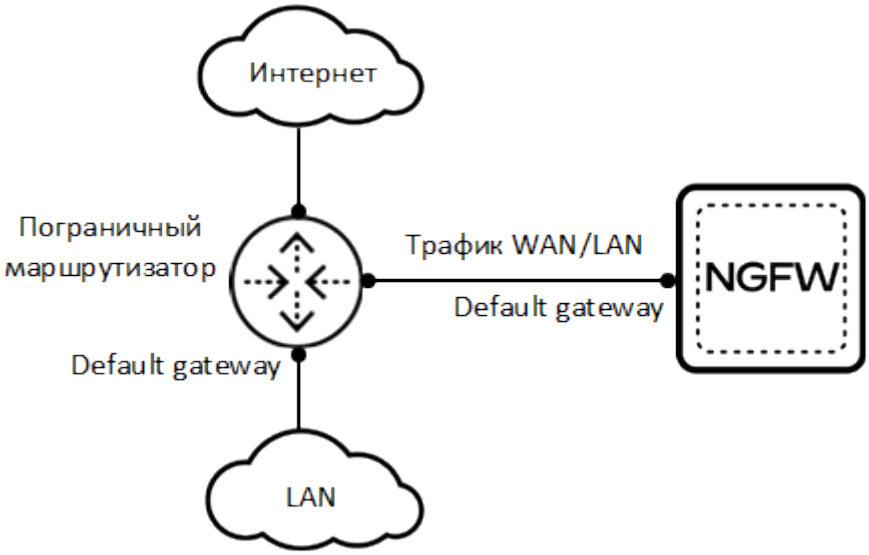


Рисунок 6. Режим маршрутизации с преобразованием VLAN ID

3. Обновление PT NGFW

Обновление до версии 1.11.0 выполняется в следующем порядке:

1. Подготовка к обновлению (см. ниже).
2. Обновление системы управления и встроенного сборщика журналов (см. раздел 3.1).
3. Обновление выделенных сборщиков журналов (см. раздел 3.2) (если используются).
4. Обновление межсетевых экранов (см. раздел 3.3).

Внимание! В процессе эксплуатации рекомендуется всегда использовать одинаковые версии всех компонентов PT NGFW (системы управления, межсетевого экрана, выделенного сборщика журналов). При этом допускается использование разных патч-версий в рамках одной минорной версии (например, 1.10.1 и 1.10.2). Использование разных минорных версий (например, 1.9.2 и 1.10.0) допускается только во время проведения планового обновления.

Примечание. Рекомендуется выполнять обновление в часы наименьшей нагрузки или во время технологического окна.

Подготовка к обновлению

- Чтобы подготовиться к обновлению,

  запишите ISO-образ с ПО PT NGFW на USB-накопитель емкостью не менее 16 ГБ.

  Примечание. Запись ISO-образа может осуществляться, например, с помощью Rufus или Etcher.

В этом разделе

Обновление системы управления (см. раздел 3.1)

Обновление выделенных сборщиков журналов (см. раздел 3.2)

Обновление межсетевых экранов (см. раздел 3.3)

Действия для обновления устройств с АМДЗ (см. раздел 3.4)

Загрузка с установочного носителя (см. раздел 3.5)

Обновление баз контента (см. раздел 3.6)

3.1. Обновление системы управления

Обновление системы управления происходит следующим образом:

— Одиночная (некластерная) система управления обновляется путем создания резервной копии, переустановки ПО с помощью установочного носителя, первичной настройки и восстановления из резервной копии.

— Кластер обновляется путем создания резервной копии, разбора кластера, переустановки ПО на устройствах кластера, первичной настройки, повторного создания кластера и восстановления из резервной копии.

Переустановка осуществляется одним из двух методов:

— **Update.** При переустановке этим методом сохраняются некоторые параметры системы управления, что упрощает первичную настройку, и данные журналов, хранящиеся во встроенном сборщике журналов.

— **Install.** Этот метод не предполагает сохранение каких-либо параметров и данных журналов и предусмотрен для использования, когда возникает ошибка при переустановке методом Update. Ошибка возникает, если текущая разметка диска не соответствует ожидаемой. Переустановка этим методом сопровождается переразметкой диска.

  Внимание! Переустановка методом Update недоступна при обновлении с версии ниже 1.9

  Примечание. Если вы используете систему управления в виртуальном исполнении, то вместо переустановки вы можете развернуть новую виртуальную машину (см. раздел 4.2). Развертывание виртуальной машины влечет за собой потерю данных журналов и потребует полной первичной настройки системы управления (см. раздел 5.2).

Ниже приведены пошаговые инструкции по обновлению системы управления с переустановкой.

Подготовка к обновлению

Перед тем как приступить к обновлению, подготовьте установочный носитель (см. раздел 3).

Обновление одиночной системы управления

► Чтобы обновить одиночную систему управления:

1. Создайте резервную копию системы управления (см. раздел 41).

   Примечание. После создания резервной копии скачайте ее на отдельное устройство.

2. Загрузите устройство с установочного носителя (см. раздел 3.5).

3. Выберите **Update** → **MGMT with built-in LOG**.

   Внимание! Если в процессе переустановки появилось сообщение об ошибке и произошел возврат в меню установочного носителя, выберите **Install** → **MGMT with built-in LOG**.

4. Выполните одно из следующих действий:
   - Если переустановка происходила методом Update, настройте систему управления (см. раздел 5.2), пропустив настройку интерфейса управления (MGMT).
   - Если переустановка происходила методом Install, настройте систему управления (см. раздел 5.2).
5. Войдите в систему управления, используя логин `admin` и пароль `admin`.
6. Восстановите конфигурацию из резервной копии (см. раздел 41).
7. Отправьте конфигурацию на межсетевые экраны, нажав **Отправить на устройства**.

Обновление кластера системы управления

- Чтобы обновить кластер системы управления:

1. Создайте резервную копию системы управления (см. раздел 41).

   Примечание. После создания резервной копии скачайте ее на отдельное устройство.
2. Подключитесь к командному интерпретатору активного устройства.
3. Переключите активное устройство в режим обслуживания:
   ```
   $ sudo msctl maintenance --enable
   ```
4. Подключитесь к командному интерпретатору резервного устройства.
5. Переключите резервное устройство в режим обслуживания:
   ```
   $ sudo msctl maintenance --enable
   ```
6. Переключите резервное устройство в активный режим:
   ```
   $ sudo msctl active
   ```
7. Переустановите ПО на устройствах кластера, начав с любого из них:
   - Загрузите устройство с установочного носителя (см. раздел 3.5).
   - Выберите **Update** → **MGMT with built-in LOG**.

     Внимание! Если в процессе переустановки появилось сообщение об ошибке и произошел возврат в меню установочного носителя, выберите **Install** → **MGMT with built-in LOG**.
8. Для каждого из устройств кластера выполните одно из следующих действий:
   - Если переустановка происходила методом Update, настройте систему управления (см. раздел 5.2), минуя настройку интерфейса управления (MGMT).
   - Если переустановка происходила методом Install, настройте систему управления (см. раздел 5.2).
9. Войдите в систему управления, используя логин `admin` и пароль `admin`.
10. Заново разверните кластер системы управления (см. раздел 31).

11. Восстановите конфигурацию из резервной копии (см. раздел 41).
12. Отправьте конфигурацию на межсетевые экраны, нажав **Отправить на устройства**.

3.2. Обновление выделенных сборщиков журналов

Обновление выделенного сборщика журналов выполняется путем переустановки ПО с использованием установочного носителя и первичной настройки.

> **Примечание.** Эта инструкция подходит только для конфигураций с выделенным сборщиком журналов, развернутым отдельно от системы управления. Встроенный сборщик журналов обновляется вместе с системой управления.

Переустановка осуществляется одним из двух методов:

- **Update.** При переустановке этим методом будут сохранены данные журналов и некоторые параметры сборщика журналов, что упрощает первичную настройку.
- **Install.** Этот метод не предполагает сохранение каких-либо параметров или данных и используется в случае возникновения ошибки при переустановке методом Update. Ошибка возникнет при обнаружении несоответствия текущей разметки диска ожидаемой. Переустановка этим методом сопровождается переразметкой диска.

Ниже приведены пошаговые инструкции по обновлению выделенного сборщика журналов.

Подготовка к обновлению

Перед тем как приступить к обновлению, подготовьте установочный носитель (см. раздел 3).

Обновление выделенного сборщика журналов

- Чтобы обновить выделенный сборщик журналов:

  1. Загрузите устройство с установочного носителя (см. раздел 3.5).
  2. Выберите **Update** → **LOG only**.

     Внимание! Если в процессе переустановки появилось сообщение об ошибке и произошел возврат в меню установочного носителя, выберите **Install** → **LOG only**.
  3. Выполните одно из следующих действий:

     - Если переустановка происходила методом Update, настройте синхронизацию времени с NTP-сервером (см. раздел 5.5.2).
     - Если переустановка происходила методом Install, настройте выделенный сборщик журналов (см. раздел 5.5).

3.3. Обновление межсетевых экранов

Обновление межсетевых экранов происходит следующим образом:

— Одиночный (некластерный) межсетевой экран обновляется путем переустановки ПО с использованием установочного носителя и первичной настройки.

— Кластер обновляется путем удаления резервного межсетевого экрана из кластера, переустановки на этом устройстве ПО с использованием установочного носителя, первичной настройки, возврата устройства в кластер и повторения этих действий над вторым устройством.

Примечание. Переустановка ПО сопровождается переразметкой диска.

Примечание. Если вы используете межсетевой экран в виртуальном исполнении, то вместо переустановки вы можете развернуть новую виртуальную машину (см. раздел 4.3).

При обновлении межсетевого экрана в виртуальном исполнении под ESXi необходимо сменить сетевой адаптер с e1000e на VMXNET3.

Ниже приведены пошаговые инструкции по обновлению межсетевого экрана с переустановкой.

В этом разделе

Подготовка к обновлению (см. раздел 3.3.1)

Обновление одиночного межсетевого экрана (см. раздел 3.3.2)

Обновление кластера межсетевого экрана (см. раздел 3.3.3)

3.3.1. Подготовка к обновлению

Перед тем как приступить к обновлению, подготовьте установочный носитель (см. раздел 3).

3.3.2. Обновление одиночного межсетевого экрана

► Чтобы обновить одиночный (некластерный) межсетевой экран:

1. Если вы используете ПАК 1005, 1010, 1020 или 1050, переведите устройство в технологический режим:
   - Отключите устройство от питания.
   - Нажмите кнопку включения и, удерживая ее нажатой, подключите питание.
   - Когда индикатор на задней панели начнет моргать, отпустите кнопку питания.
   - Включите устройство.
2. Если вы используете ПАК с АМДЗ, выполните действия, описанные в инструкции (см. раздел 3.4).

3. Загрузите устройство с установочного носителя:
   - Если вы используете ПАК с АМДЗ, выберите установочный носитель в качестве устройства для загрузки.

     Внимание! Соответствующее меню появится автоматически при загрузке устройства. До появления меню возникнет сообщение об ошибке. При возникновении сообщения следует нажать Enter.
   - Если вы используете ПАК без АМДЗ или виртуальную машину, загрузите устройство с установочного носителя по инструкции (см. раздел 3.5).
4. Выберите **Install** → **Firewall**.

   Примечание. Начнется переустановка ПО. По завершении отобразится поле для ввода логина от предустановленной учетной записи базовой ОС.
5. Если вы используете ПАК с «Аккорд-АМДЗ», активируйте АМДЗ, как описано в инструкции (см. раздел 3.4).
6. Настройте межсетевой экран (см. раздел 5.3).

См. также

Загрузка с установочного носителя (см. раздел 3.5)

Настройка межсетевого экрана (см. раздел 5.3)

Действия для обновления устройств с АМДЗ (см. раздел 3.4)

3.3.3. Обновление кластера межсетевого экрана

Перед обновлением кластера рекомендуется убедиться в его работоспособности. Для этого можно приостановить активное устройство (см. раздел 30.14), убедиться, что трафик начал обрабатываться вторым устройством, а затем вывести активное устройство из состояния **Приостановлен** с помощью команды **Возобновить** (**Unsuspend**).

Обновление текущего резервного устройства

- Чтобы обновить резервный межсетевой экран:
  1. Удалите резервное устройство из кластера (см. раздел 30.18).
  2. Если вы используете ПАК 1005, 1010, 1020 или 1050, переведите устройство в технологический режим:
     - Отключите устройство от питания.
     - Нажмите кнопку включения и, удерживая ее нажатой, подключите питание.
     - Когда индикатор на задней панели начнет моргать, отпустите кнопку питания.
     - Включите устройство.

3. Если вы используете ПАК с АМДЗ, выполните действия, описанные в инструкции (см. раздел 3.4).
4. Загрузите устройство с установочного носителя:
   - Если вы используете ПАК с АМДЗ, выберите установочный носитель в качестве устройства для загрузки.

     Внимание! Соответствующее меню появится автоматически при загрузке устройства. До появления меню возникнет сообщение об ошибке. При возникновении сообщения следует нажать Enter.
   - Если вы используете ПАК без АМДЗ или виртуальную машину, загрузите устройство с установочного носителя по инструкции (см. раздел 3.5).
5. Выберите **Install** → **Firewall**.

   Примечание. Начнется переустановка ПО. По завершении отобразится поле для ввода логина от предустановленной учетной записи базовой ОС.
6. Если вы используете ПАК с «Аккорд-АМДЗ», активируйте АМДЗ, как описано в инструкции (см. раздел 3.4).
7. Настройте межсетевой экран (см. раздел 5.3).
8. Добавьте устройство в кластер (см. раздел 30.19).

Обновление второго устройства

► Чтобы обновить второе устройство:

1. Удалите второе устройство из кластера (см. раздел 30.18).
2. Если вы используете ПАК 1005, 1010, 1020 или 1050, переведите устройство в технологический режим:
   - Отключите устройство от питания.
   - Нажмите кнопку включения и, удерживая ее нажатой, подключите питание.
   - Когда индикатор на задней панели начнет моргать, отпустите кнопку питания.
   - Включите устройство.
3. Если вы используете ПАК с АМДЗ, выполните действия, описанные в инструкции (см. раздел 3.4).
4. Загрузите устройство с установочного носителя:
   - Если вы используете ПАК с АМДЗ, выберите установочный носитель в качестве устройства для загрузки.

     Внимание! Соответствующее меню появится автоматически при загрузке устройства. До появления меню возникнет сообщение об ошибке. При возникновении сообщения следует нажать Enter.

- Если вы используете ПАК без АМДЗ или виртуальную машину, загрузите устройство с установочного носителя по инструкции (см. раздел 3.5).

5. Выберите **Install** → **Firewall**.

   Примечание. Начнется переустановка ПО. По завершении отобразится поле для ввода логина от предустановленной учетной записи базовой ОС.

6. Если вы используете ПАК с «Аккорд-АМДЗ», активируйте АМДЗ, как описано в инструкции (см. раздел 3.4).
7. Настройте межсетевой экран (см. раздел 5.3).
8. Добавьте устройство в кластер (см. раздел 30.19).

См. также

Удаление устройств из кластера (см. раздел 30.18)

Загрузка с установочного носителя (см. раздел 3.5)

Настройка межсетевого экрана (см. раздел 5.3)

Добавление устройств в кластер (см. раздел 30.19)

Действия для обновления устройств с АМДЗ (см. раздел 3.4)

3.4. Действия для обновления устройств с АМДЗ

В этом разделе

Действия с ПАК «Соболь» (см. раздел 3.4.1)

Действия с «Аккорд-АМДЗ» (см. раздел 3.4.2)

3.4.1. Действия с ПАК «Соболь»

На межсетевых экранах с ПАК «Соболь» в начале обновления необходимо подключить идентификатор администратора АМДЗ к устройству. Идентификатор должен быть подключен на время обновления.

Во время обновления потребуется многократно вводить пароль по запросу АМДЗ – следует указывать `p0sitive` (пароль при поставке). После каждого ввода будет необходимо выбрать **Настройки** и нажать **Сохранить** (если доступно) → **Загрузка**.

> **Примечание.** Вы можете использовать Tab или Shift+Tab для выбора элемента и Enter или клавишу пробела для активации элемента. Выбранный элемент выделяется рамкой.

3.4.2. Действия с «Аккорд-АМДЗ»

На межсетевых экранах с «Аккорд-АМДЗ» в начале обновления потребуется выполнить ряд действий в указанном порядке: переключить устройство в технологический режим (если это еще не было сделано), деактивировать АМДЗ, удалить загрузчик.

В конце обновления потребуется активировать АМДЗ.

Переключение в технологический режим

- Чтобы перевести устройство в технологический режим:

  1. Отключите устройство от питания.
  2. Нажмите кнопку включения и, удерживая ее нажатой, подключите питание.
  3. Когда индикатор на задней панели начнет моргать, отпустите кнопку питания.
  4. Включите устройство.

Деактивация АМДЗ

- Чтобы деактивировать АМДЗ:

  1. Подключите монитор, клавиатуру и опционально мышь.
  2. Подключите к устройству токен администратора.
  3. Перезагрузите устройство.
  4. Сразу после появлении надписи «Positive Technologies» при запросе пароля введите `p0sitive`.

     Примечание. Пароль для обоих токенов при поставке «Аккорд-АМДЗ» — `p0sitive`.
  5. Выберите **Администрирование**.

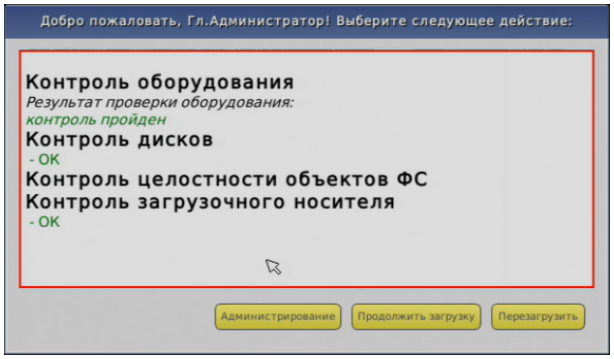


Рисунок 7. Меню «Аккорд-АМДЗ»

Примечание. При работе с помощью клавиатуры это можно сделать, используя Tab или Shift+Tab, что позволяет выбрать элемент, и Enter или клавиши пробела, что позволяет активировать элемент. Выбранный элемент выделяется рамкой.

6. Слева выберите **Настройки**.

   Примечание. Это можно сделать, нажав Alt+7.

7. Установите флажок **Деактивировать Аккорд-АМДЗ**.

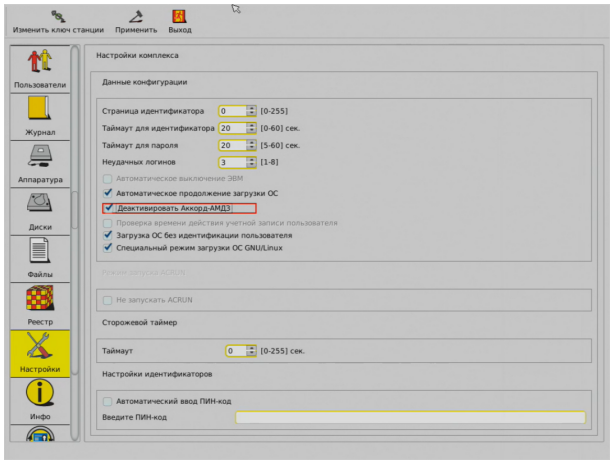


Рисунок 8. Меню «Аккорд-АМДЗ»

8. Вверху нажмите **Применить**.

   Примечание. Это можно сделать, нажав F2.

9. Вверху нажмите **Выход**.

   Примечание. Это можно сделать, нажав F3.

10. Нажмите **Перезагрузка**.

    Примечание. После перезагрузки отобразится поле для ввода логина от предустановленной учетной записи базовой ОС.

Удаление загрузчика

Удаление загрузчика сделает возможным переход в меню выбора устройства загрузки BIOS.

- Чтобы удалить загрузчик:

  1. Выполните следующие команды:

     ```
     sudo mount -a
     sudo rm -rfv /boot/efi/EFI/ /boot/eficopy/*/EFI/
     ```

  2. Перезагрузите устройство:

     ```
     sudo reboot
     ```

Активация АМДЗ

- Чтобы активировать АМДЗ:

1. Подключите монитор, клавиатуру и опционально мышь.
2. Подключите к устройству токен администратора.
3. Перезагрузите устройство.
4. При появлении надписи «Positive Technologies» нажмите и не отпускайте клавишу ESC.
5. Когда надпись исчезнет и появится текст «Starting AMDZ», отпустите клавишу.

   Примечание. Если текст не появился, перезагрузите устройство и повторите предыдущий шаг, зажав Ctrl+B вместо ESC.
6. При запросе пароля введите `p0sitive`.
7. Выберите **Администрирование**.
8. Слева выберите **Настройки**.

   Примечание. Это можно сделать, нажав Alt+7.
9. Снимите флажок **Деактивировать Аккорд-АМДЗ**.
10. Вверху нажмите **Применить**.

    Примечание. Это можно сделать, нажав F2.
11. Если у вас включен контроль оборудования и дисков, то подтвердите изменения:
    - Выберите **Аппаратура**.
    - Выберите **Пересчитать** → **Сохранить**.
    - Выберите **Диски**.
    - Выберите **Пересчитать** → **Сохранить**.
12. Вверху нажмите **Выход**.

    Примечание. Это можно сделать, нажав F3.
13. Нажмите **Перезагрузка**.

    Примечание. Теперь при каждой загрузке устройства будет происходить загрузка «Аккорд-АМДЗ».

3.5. Загрузка с установочного носителя

Чтобы загрузить обновляемый узел с установочного носителя:

1. Завершите работу обновляемого узла и выключите питание.
2. Обеспечьте загрузку обновляемого узла с USB-накопителя. Для этого выполните одно из действий в зависимости от исполнения и типа обновляемого компонента:
   - Для компонентов на базе аппаратных платформ — подключите USB-накопитель к USB-разъему аппаратной платформы.

     Примечание. Для компонентов PT NGFW на базе аппаратных платформ PT NGFW 2010, 2020, 2050, 3010, 3040, 3050, а также PT NGFW MNGT M1 и PT NGFW LOG M1 вы также можете удаленно подключить ISO-образ через KVM-консоль (см. раздел 3.5).
   - Для компонентов, развернутых на виртуальных узлах — подключите USB-накопитель и добавьте ISO-образ к виртуальному узлу средствами платформы виртуализации.
3. Включите обновляемый узел.
4. Во время начальной загрузки нажмите **F2** (либо другую клавишу, указанную на экране загрузки), чтобы войти в настройки BIOS/UEFI системы.

   Примечание. Для компонентов PT NGFW на базе аппаратных платформ PT NGFW 2010, 2020, 2050, 3010, 3040, 3050, а также PT NGFW MNGT M1 и PT NGFW LOG M1 вы можете пропустить этот этап и сразу выполнить загрузку. Для этого нажмите **F11** и выберите подключенный USB-накопитель в меню загрузки.
5. Выберите способ загрузки:
   - **CD-ROM** — при удаленном подключении через KVM;
   - **USB-накопитель** — в остальных случаях.
6. Сохраните изменения и перезагрузите обновляемый узел, после чего начнется его загрузка с подключенного ISO-образа.

Удаленное подключение через KVM-консоль

Аппаратные платформы, оборудованные консолью управления шасси AMI MegaRAC SP-X, позволяют удаленно подключиться и смонтировать ISO-образ через KVM-консоль.

Чтобы удаленно смонтировать образ через KVM-консоль:

1. Подключитесь к консоли управления шасси.

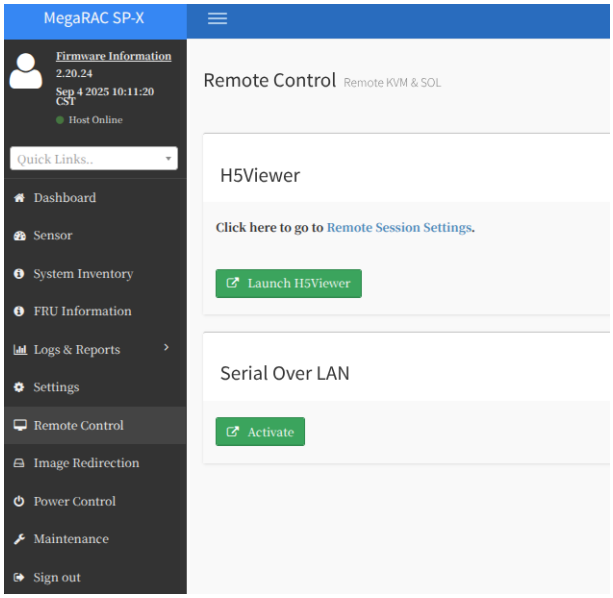


Рисунок 9. Консоль управления AMI MegaRAC SP-X

2. Выберите **Remote Control** → **Launch H5Viewer** для запуска KVM-консоли.

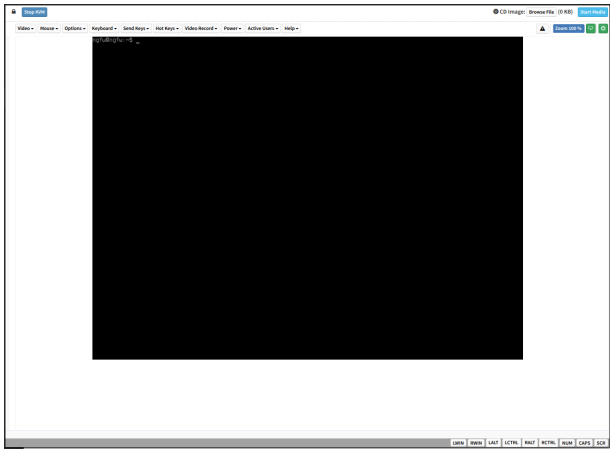


Рисунок 10. Окно KVM-консоли

3. В меню KVM-консоли нажмите **Browse File**.
4. Выберите ISO-образ с ПО PT NGFW.
5. Нажмите **Start Media**.

3.6. Обновление баз контента

Базы контента содержат справочные данные и данные различных подсистем PT NGFW, такие как перечень категорий URL и GeoIP, вирусные сигнатуры, базы правил IPS и пр. Чтобы поддерживать их в актуальном состоянии, их необходимо периодически обновлять. Для этого используется специальный архив `*.tar`, содержащий обновления следующих баз контента:

- **Антивирус** — база вирусных сигнатур;
- **Приложения** — данные классификатора DPI;
- **GeoIP** — данные географической привязки IP-адресов и подсетей;
- **IPS** — база сигнатур службы предотвращения вторжений IPS;
- **URL categories** — категории пользовательского контента и таблицы категоризированных URL.

PT NGFW позволяет загружать несколько обновлений в каждой из категорий контента. Количество загружаемых обновлений не ограничено и определяется объемом доступного дискового пространства. Во время загрузки и установки обновлений обработка трафика не прерывается.

- Чтобы узнать текущие версии баз контента,

  в главном меню выберите **Параметры** → **Обновления**.

  Будет выведен список загруженных и установленных баз контента и информация о них: текущий статус, дата выпуска, версия и размер обновления. Также выводится статистическая информация о количестве устройств, на которые загружены и установлены обновления.

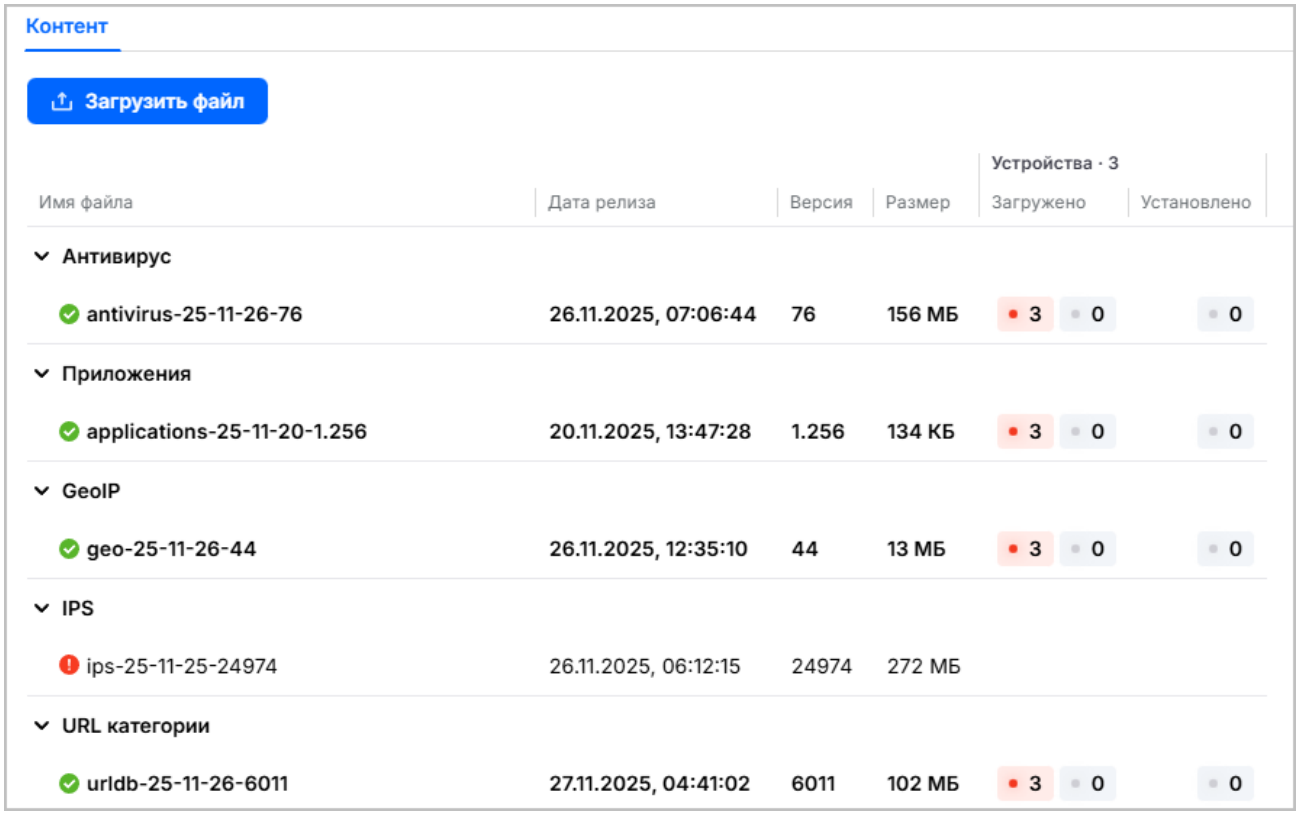


Рисунок 11. Просмотр установленных баз контента

Внимание! Перед тем, как начать процесс обновления баз контента, убедитесь, что в системе управления правильно настроен IP-адрес сетевого интерфейса для возможности загрузки обновлений на межсетевые экраны (см. раздел 5.2.3).

Внимание! Если PT NGFW работает в кластере, то версии баз контента на обоих узлах должны совпадать.

Загрузка и обновление баз контента

- Чтобы загрузить и обновить базы контента:

1. Получите у администратора файл обновления баз контента или скачайте его с сервера обновлений.
2. В главном меню выберите **Параметры** → **Обновления**.
3. Нажмите **Загрузить**.
4. Перетащите файл обновления в окно загрузки или **выберите** путь к файлу обновления.

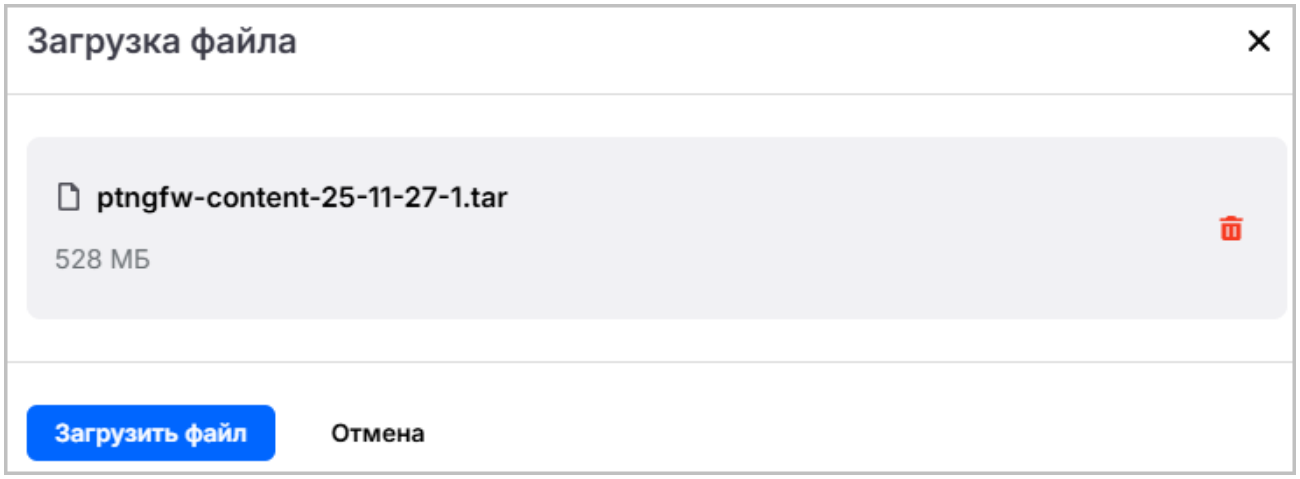


Рисунок 12. Загрузка файла

5. Нажмите **Загрузить**.

   В процессе загрузки будет проверена целостность файла обновления и состав устанавливаемых обновлений.

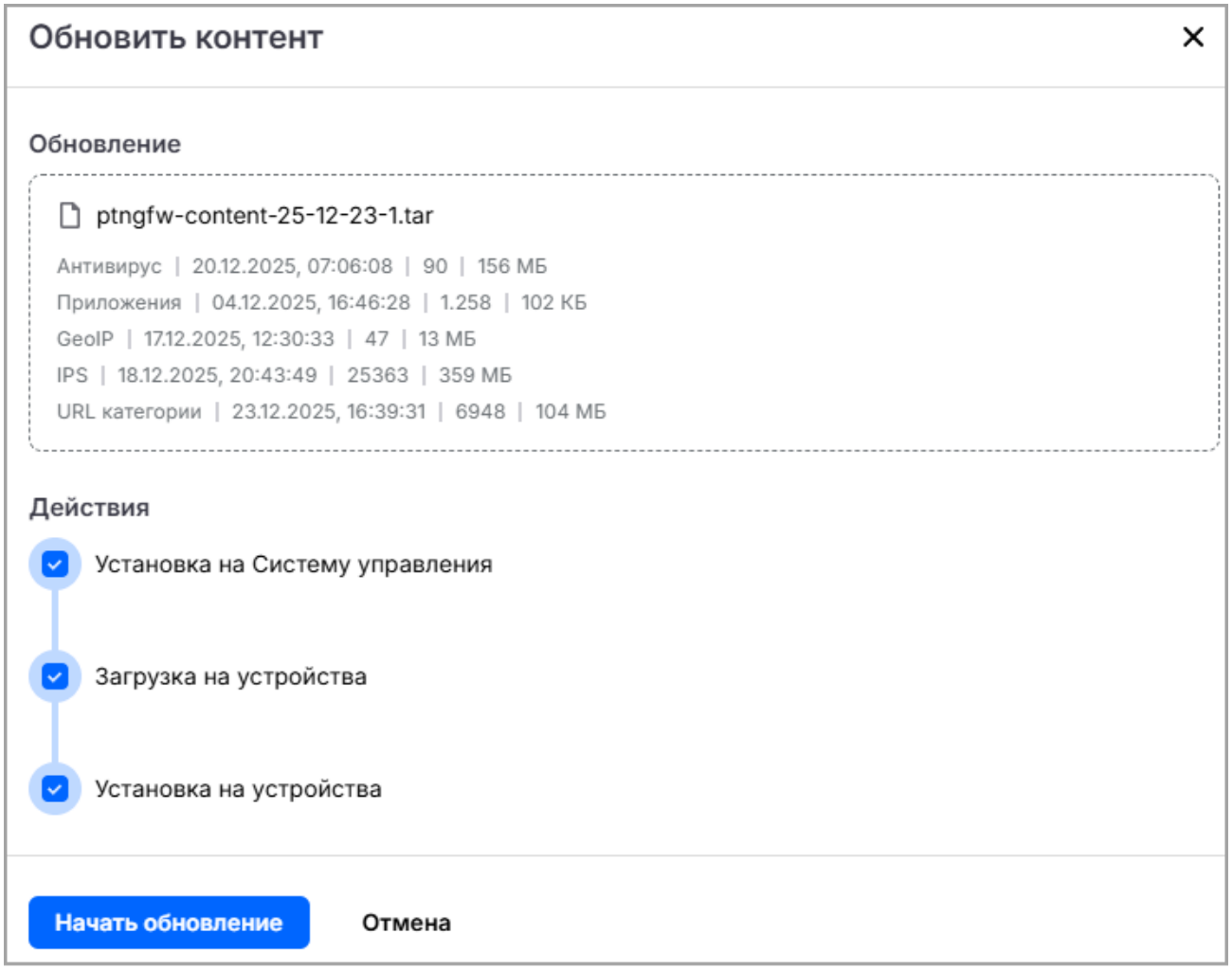


Рисунок 13. Окно установки обновления

6. В окне установки обновления выберите одно или несколько действий:
   - **Установка на систему управления** — обновление будет установлено только на систему управления. Вы сможете загрузить и установить его на устройства позднее.
   - **Загрузка на все устройства** — обновление будет загружено на все устройства, но не установлено.
   - **Установка на все устройства** — обновление будет загружено и установлено на все устройства.
7. Нажмите **Начать обновление**.

Установка ранее загруженных обновлений

- Чтобы установить ранее загруженные обновления:

  1. В главном меню выберите **Параметры** → **Обновления**.
  2. Выберите нужное обновление и в контекстном меню выберите **Обновить**.
  3. В окне обновления контента выберите требуемые действия.

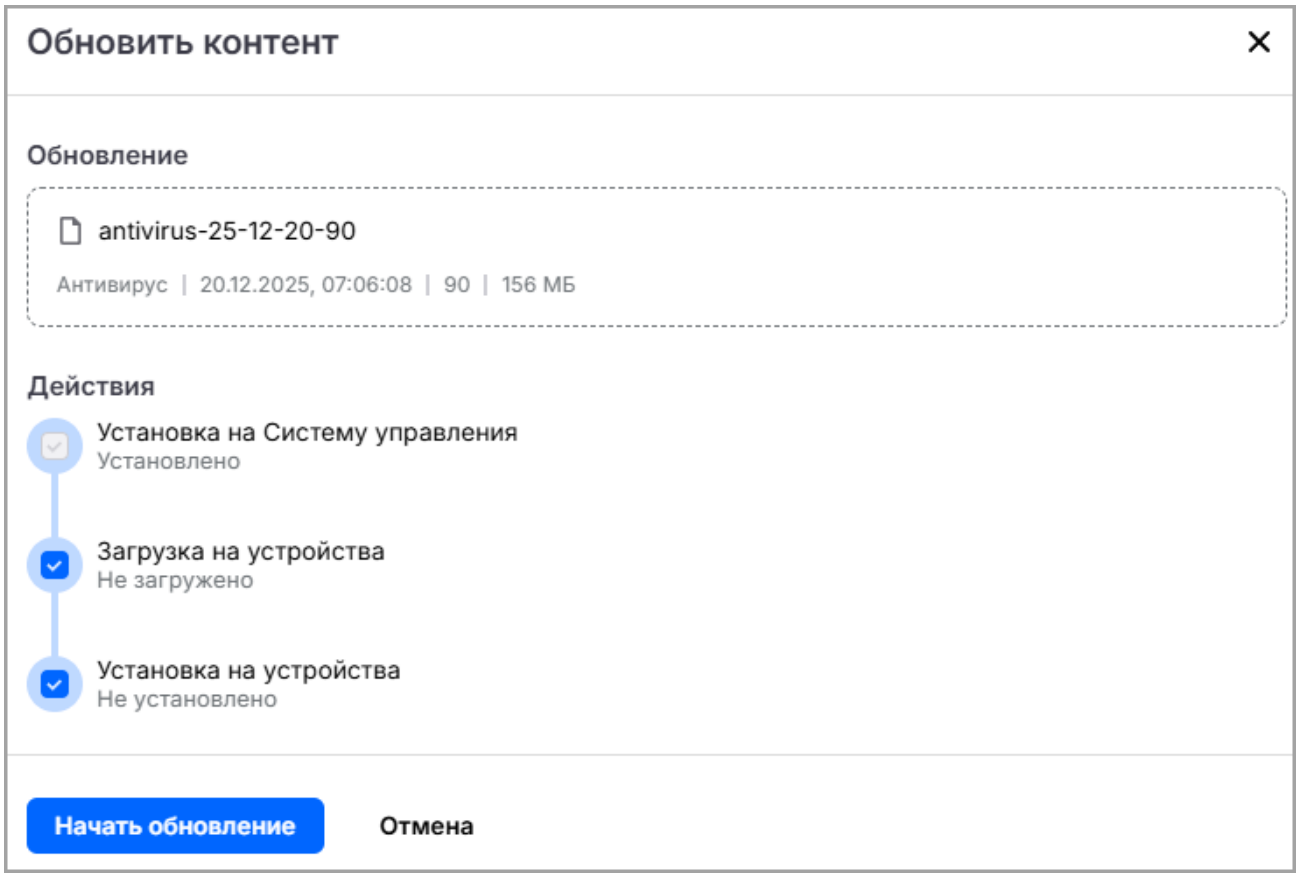


Рисунок 14. Окно обновления контента

  4. Нажмите **Начать обновление**.

     В результате базы контента будут загружены и установлены на устройствах.

Удаление загруженных обновлений

- Чтобы удалить загруженные обновления:

  1. В главном меню выберите **Параметры** → **Обновления**.
  2. Нажмите на название обновления и в контекстном меню выберите **Удалить**.

Внимание! Если загруженное обновление было отправлено на устройства, то его удаление недоступно.

4. Развертывание виртуального PT NGFW

В этом разделе приводятся инструкции по установке системы управления, межсетевого экрана и системы мониторинга. Установка каждого из этих компонентов производится через развертывание соответствующего виртуального образа в среде ESXi или KVM. Установка компонента требуется при поставке последнего в виде виртуального образа.

Программно-аппаратные комплексы поставляются с предустановленным ПО. Инструкции по первичной настройке ПАК и обновлению версии ядра PT NGFW приведены в соответствующих разделах документации на ПАК.

> **Внимание!** Не выполняйте самостоятельно обновление базовой операционной системы межсетевого экрана без получения рекомендации от производителя.

В этом разделе

Программные и аппаратные требования (см. раздел 4.1)

Развертывание системы управления (см. раздел 4.2)

Развертывание виртуальной машины PT NGFW (см. раздел 4.3)

Развертывание системы мониторинга (см. раздел 4.4)

4.1. Программные и аппаратные требования

Программные требования

Виртуальные образы могут быть развернуты в среде ESXi версии 7 (hardware version 19) и выше или KVM. Для работы с системой управления рекомендуется использовать последнюю версию браузера Chrome, Firefox или Edge.

После развертывания и первичной настройки PT NGFW необходимо настроить синхронизацию системного времени с NTP-серверами. Вы можете использовать NTP-клиент systemd-timesyncd, поставляемый с дистрибутивом Debian. Подробное описание настройки systemd-timesyncd приведено в документации к Debian.

> **Внимание!** При необходимости создания снапшота виртуальная машина должна быть переведена в выключенное состояние. В случае кластерной конфигурации необходимо с минимальным интервалом сначала остановить активный узел, затем резервный, после чего создать снапшоты обеих виртуальных машин. Включение следует выполнять в обратном порядке: сначала резервный узел, затем активный.

Аппаратные требования

Ниже представлены минимальные требования для развертывания виртуальных образов.

Таблица 2. Аппаратные требования для межсетевого экрана

	VM-1010	VM-1050	VM-2010	VM-2020	VM-2050
Модель процессоров	Intel Xeon Scalable, Intel Xeon версии 4 и выше				
Виртуальные CPU (частота не ниже 2,1 ГГц) **Внимание!** Все требуемые ядра должны быть зарезервированы (изолированы) для виртуальной машины. Не допускается расположение виртуальной машины на разных NUMA-узлах	4 vCPU	8 vCPU	10 vCPU	12 vCPU	14 vCPU
ОЗУ **Внимание!** Вся требуемая оперативная память должна быть выделена (изолирована) для виртуальной машины	16 ГБ	20 ГБ	24 ГБ	28 ГБ	32 ГБ
Дисковое пространство	250 ГБ				
Выделенный интерфейс для системы управления	1 шт.				
Выделенный интерфейс для кластерного sync-link	1 шт.				
Сетевые интерфейсы dataplane	6 шт.				

Внимание! Для работы межсетевого экрана требуется, чтобы процессор хостовой машины гипервизора поддерживал технологию 1GB huge pages (наличие флага pdpe1gb).

Внимание! При необходимости создания кластера на виртуальных машинах с использованием виртуального MAC-адреса в гипервизоре должны быть включены параметры Promiscuous Mode, MAC Address Changes и Forged Transmits.

> **Внимание!** Виртуальная машина поддерживает только интерфейс UEFI. При использовании режима эмуляции BIOS (Legacy) корректная загрузка операционной системы невозможна.

Межсетевой экран поддерживает следующие типы виртуальных адаптеров:

— VMXNET3 (ESXi);

— virtio (KVM).

Таблица 3. Аппаратные требования для системы управления

Модель	vCPU	ОЗУ, ГБ	Дисковое пространство, ГБ
PT-NGFW-MNGT-VM-ES	4	10	500
PT-NGFW-MNGT-VM-S	8	16	500
PT-NGFW-MNGT-VM-M	16	64	500
PT-NGFW-MNGT-VM-L	32	128	500

Примечание. Конфигурация виртуальной машины выбирается по целевому значению EPS — ожидаемому потоку генерации журналируемых событий всеми обслуживаемыми межсетевыми экранами. Выбирайте тип конфигурации, у которого номинальное значение EPS не ниже требуемого, с разумным запасом на пиковые периоды:
– **PT-NGFW-MNGT-VM-ES** — до 50 000 EPS. Предназначена для лабораторной среды и пилотных проектов. Не рекомендуется использовать в продуктивной среде.
– **PT-NGFW-MNGT-VM-S** — до 130 000 EPS.
– **PT-NGFW-MNGT-VM-M** — до 250 000 EPS.
– **PT-NGFW-MNGT-VM-L** — до 350 000 EPS.

Таблица 4. Аппаратные требования для системы мониторинга

Параметр	Требование
Виртуальные CPU	4 vCPU
ОЗУ	4 ГБ
Дисковое пространство	250 ГБ

Примечание. Указаны минимальные характеристики, которые подходят для ознакомления с системой мониторинга и не предназначены для работы в продуктивной среде. Обратитесь в службу технической поддержки, если в вашей системе используется более двух межсетевых экранов.

4.2. Развертывание системы управления

В этом разделе приводятся инструкции по развертыванию системы управления PT NGFW.

Внимание! При необходимости создания снапшота виртуальная машина должна быть переведена в выключенное состояние. В случае кластерной конфигурации необходимо с минимальным интервалом сначала остановить активный узел, затем резервный, после чего создать снапшоты обеих виртуальных машин. Включение следует выполнять в обратном порядке: сначала резервный узел, затем активный.

В этом разделе

Развертывание виртуальной машины в среде ESXi (см. раздел 4.2.1)

Развертывание виртуальной машины в среде KVM (см. раздел 4.2.2)

Первоначальная настройка (см. раздел 4.2.3)

4.2.1. Развертывание виртуальной машины в среде ESXi

- Чтобы развернуть виртуальную машину в среде ESXi:

1. Перейдите в раздел **Virtual Machines**.
2. Начните процесс создания новой виртуальной машины, нажав **Create / Register VM**.

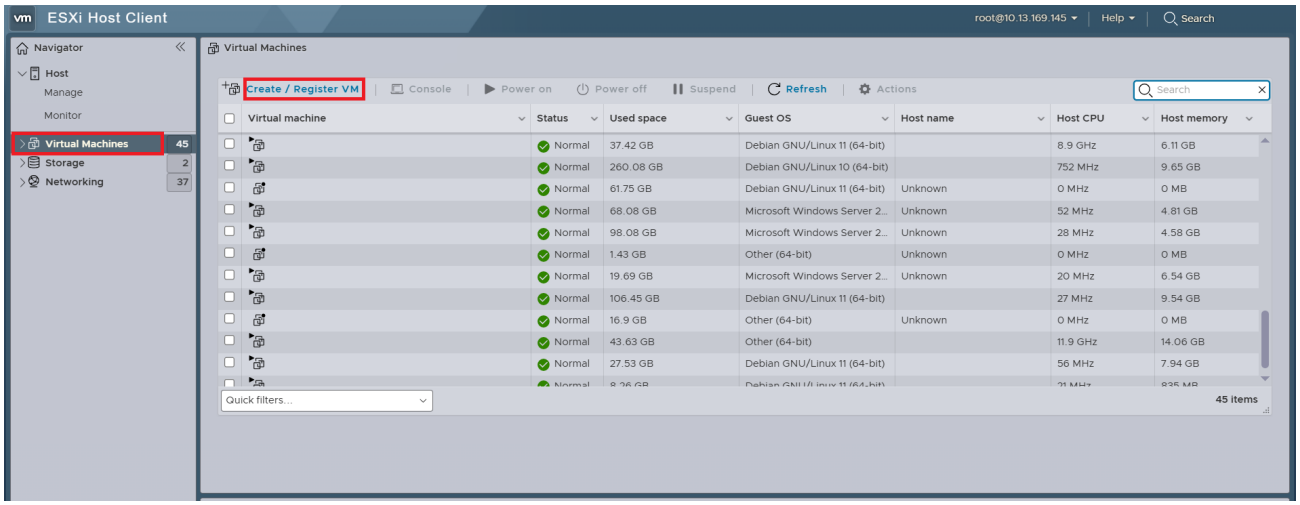


Рисунок 15. Создание виртуальной машины

3. Выберите тип развертывания из образа OVA — **Deploy a virtual machine from an OVF or OVA file** и нажмите **NEXT**.

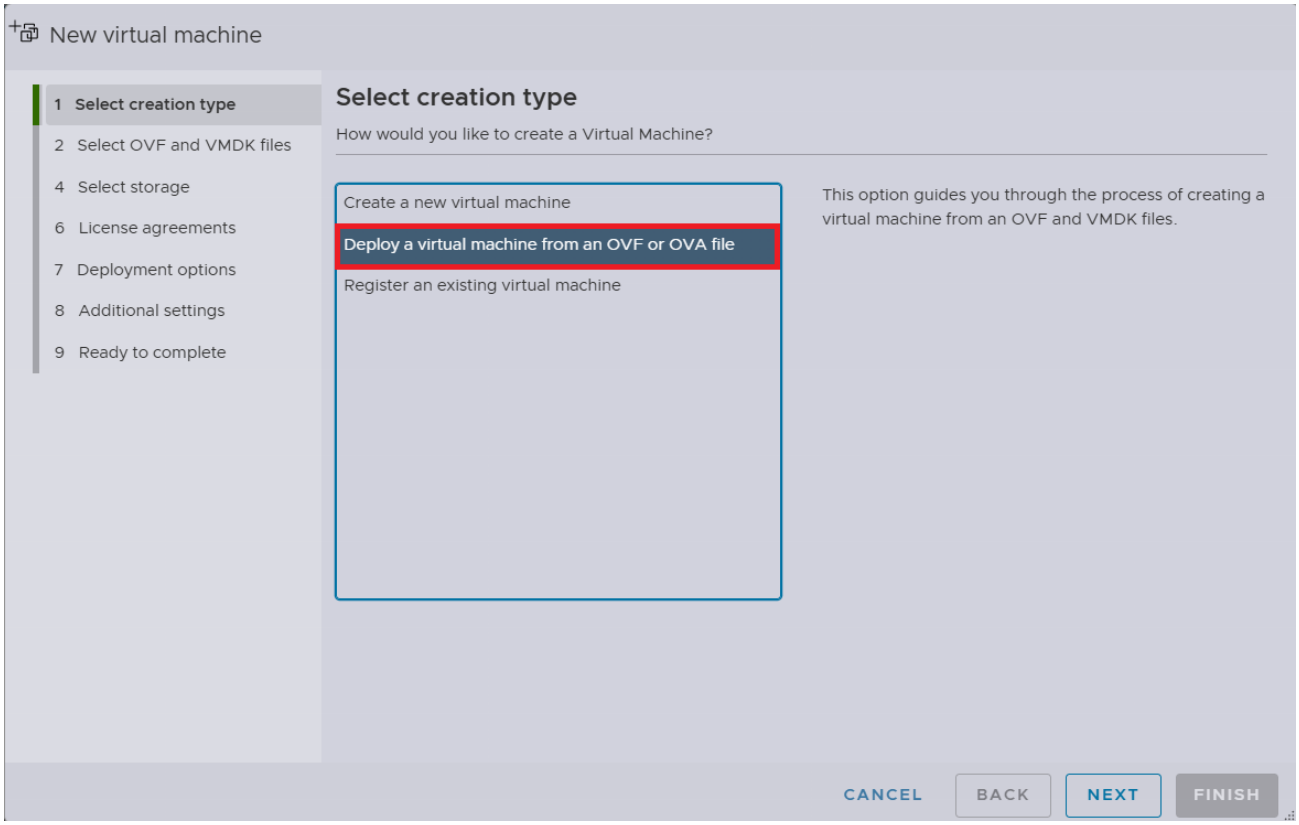


Рисунок 16. Развертывание из образа OVA

4. Введите имя будущей виртуальной машины.
5. Нажмите **Click to select files or drag/drop** и выберите файл с расширением OVA виртуальной машины системы управления PT NGFW.
6. Нажмите **NEXT**.

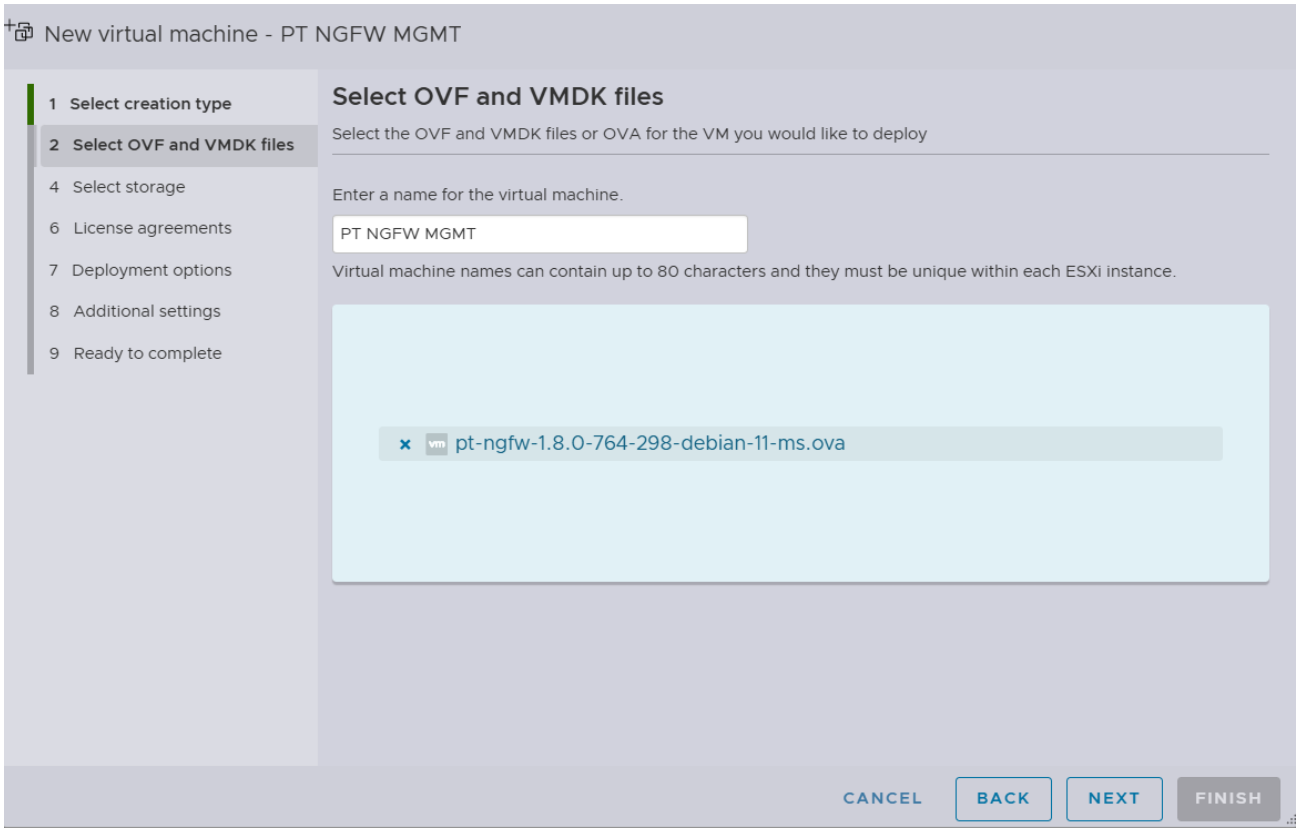


Рисунок 17. Ввод имени виртуальной машины и выбор файлов

7. Выберите хранилище, в котором будут находиться файлы виртуальной машины.

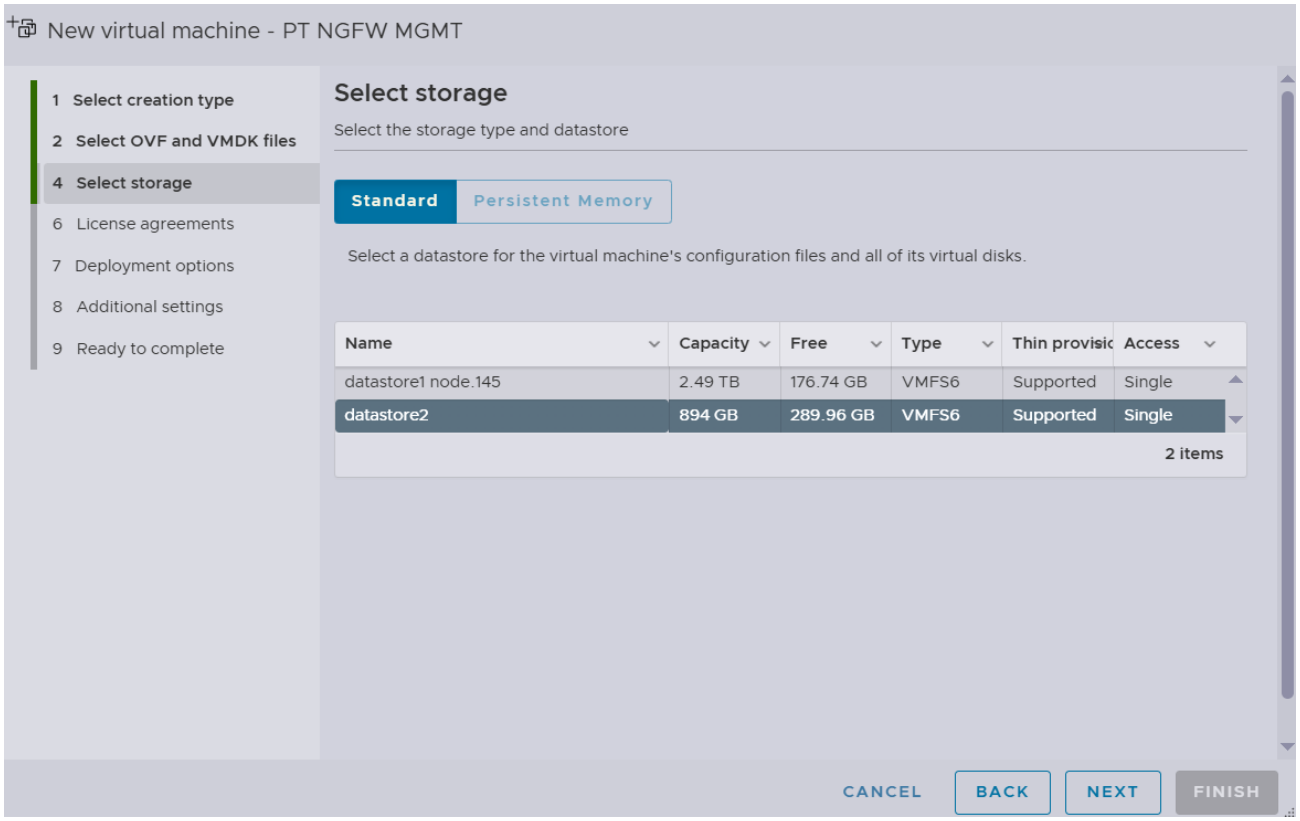


Рисунок 18. Выбор хранилища

8. Ознакомьтесь с условиями лицензионного соглашения и примите его, нажав **I AGREE**.
9. Нажмите **NEXT**.

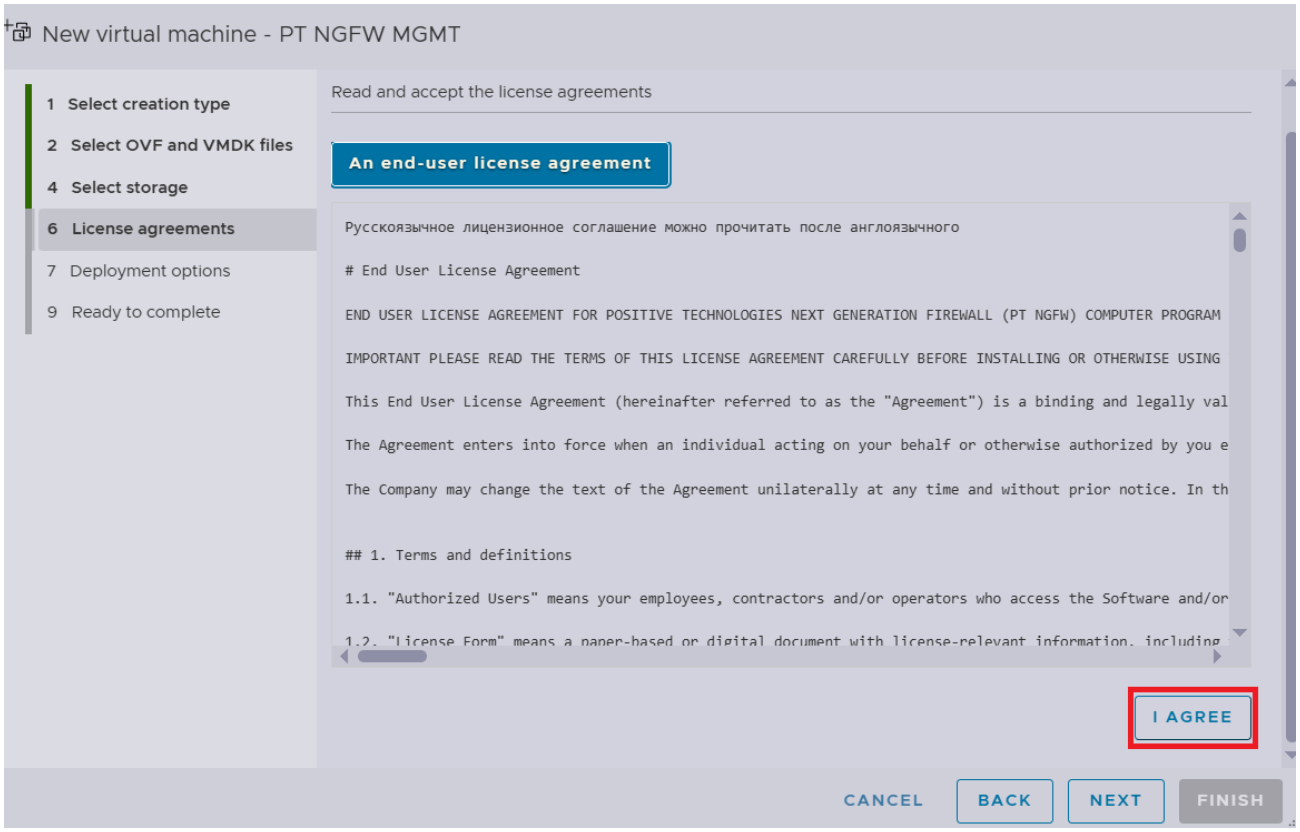


Рисунок 19. Лицензионное соглашение

10. В блоке параметров **Deployment options** настройте следующие параметры:

- **Network mappings** → **Management network** — выберите порт-группу виртуального коммутатора ESXi, к которому должен быть подключен сетевой интерфейс системы управления PT NGFW. Через этот сетевой интерфейс будет происходить подключение к GUI и оболочке Shell системы управления PT NGFW, а также система управления будет обращаться к узлам PT NGFW.
- **Disk provisioning** — если вы собираетесь использовать виртуальную машину в рабочей среде, выберите тип **Thick**. Для лабораторного или тестового использования допускается тип **Thin**.
- **Deployment type** — в раскрывающемся списке выберите конфигурацию разворачиваемой виртуальной машины.

  Примечание. Конфигурация виртуальной машины выбирается по целевому значению EPS — ожидаемому потоку генерации журналируемых событий всеми обслуживаемыми межсетевыми экранами. Выбирайте тип конфигурации, у которого номинальное значение EPS не ниже требуемого, с разумным запасом на пиковые периоды:
  – **PT-NGFW-MNGT-VM-ES** — до 50 000 EPS. Предназначена для лабораторной среды и пилотных проектов. Не рекомендуется использовать в продуктивной среде.
  – **PT-NGFW-MNGT-VM-S** — до 130 000 EPS.
  – **PT-NGFW-MNGT-VM-M** — до 250 000 EPS.
  – **PT-NGFW-MNGT-VM-L** — до 350 000 EPS.

- **Power on automatically** — если вы хотите, чтобы виртуальная машина была запущена сразу после развертывания, оставьте установленным флажок **Power on automatically**.

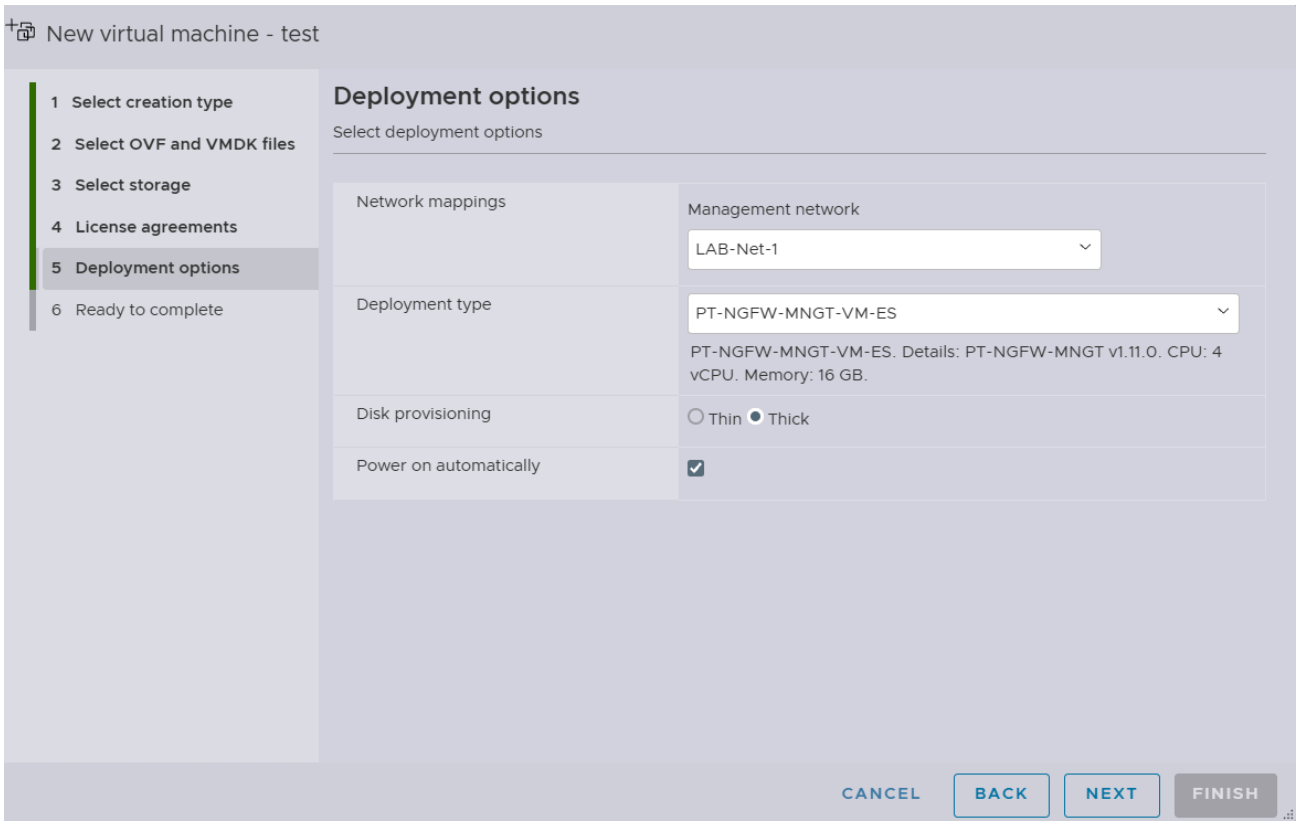


Рисунок 20. Блок параметров **Deployment options**

11. Проверьте параметры установки в окне со сводной информацией и, если все указано верно, нажмите **FINISH**.

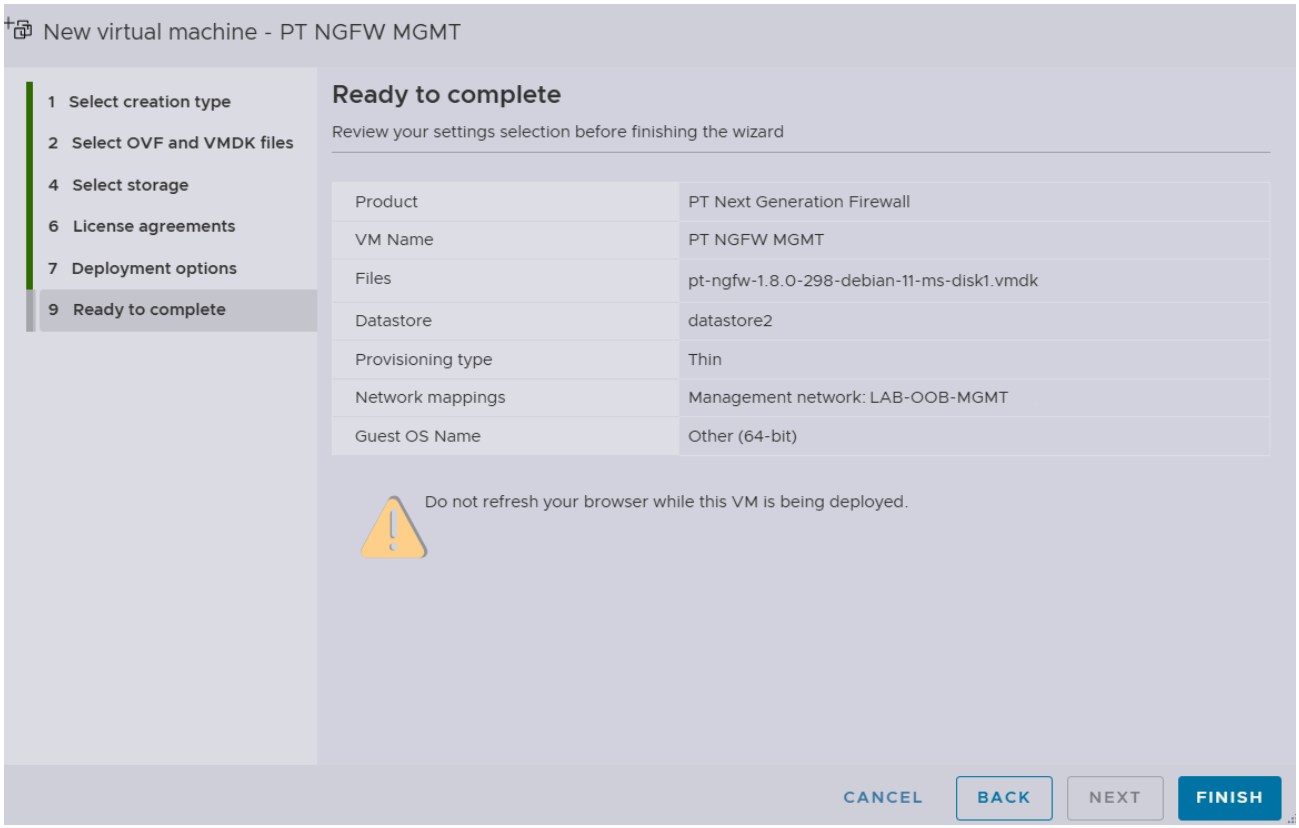


Рисунок 21. Завершение развертывания виртуальной машины в среде ESXi

4.2.2. Развертывание виртуальной машины в среде KVM

- Чтобы развернуть виртуальную машину в среде KVM:

1. Начните процесс импортирования виртуальной машины, нажав **Import VM**.

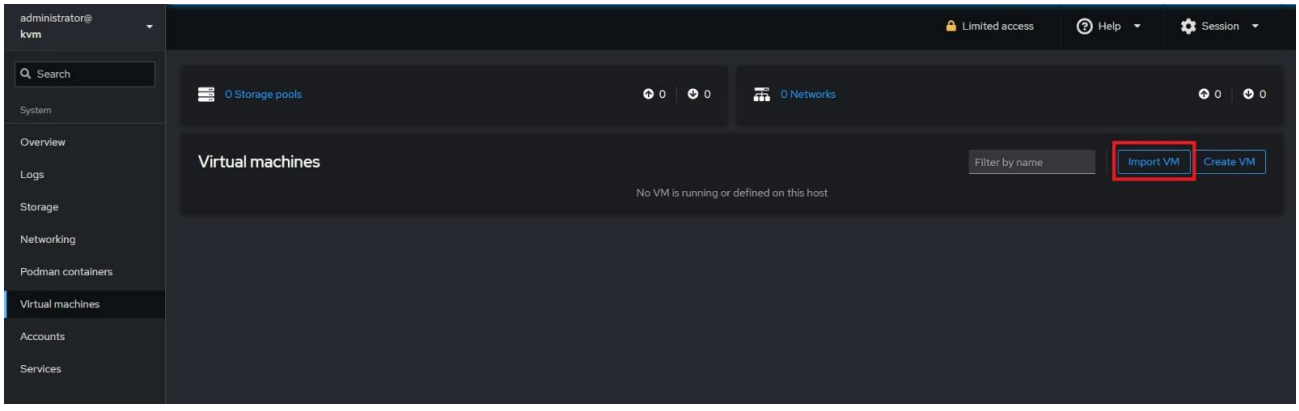


Рисунок 22. Импортирование виртуальной машины

2. Укажите параметры импортируемой машины и нажмите **Import and run**.

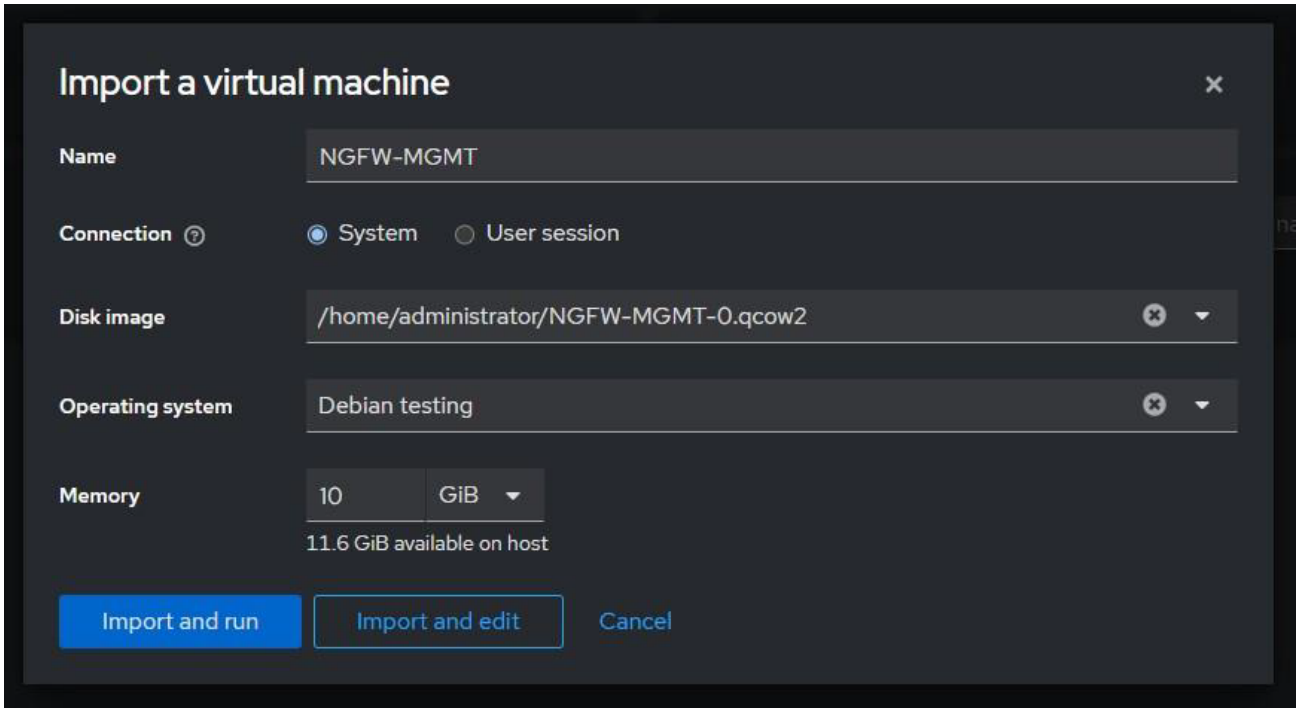


Рисунок 23. Параметры импортируемой машины

3. По завершении процесса импортирования измените параметры процессора:
   - Укажите количество ядер.

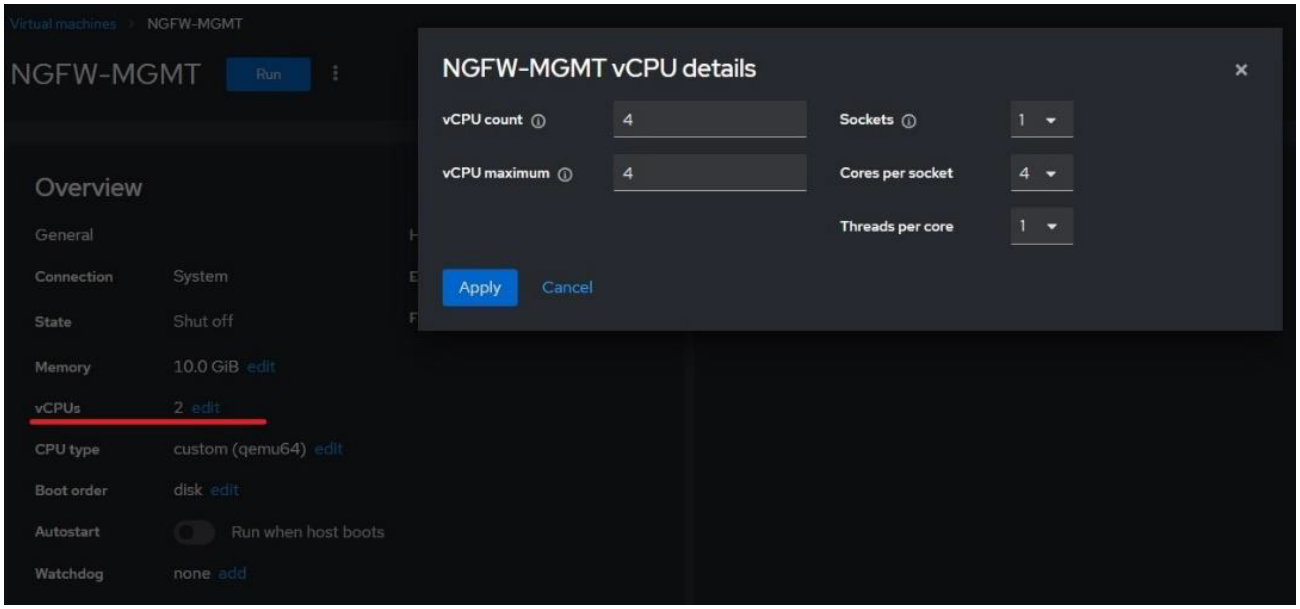


Рисунок 24. Параметры процессора (количество ядер)

   - Укажите тип процессора и тип прошивки.

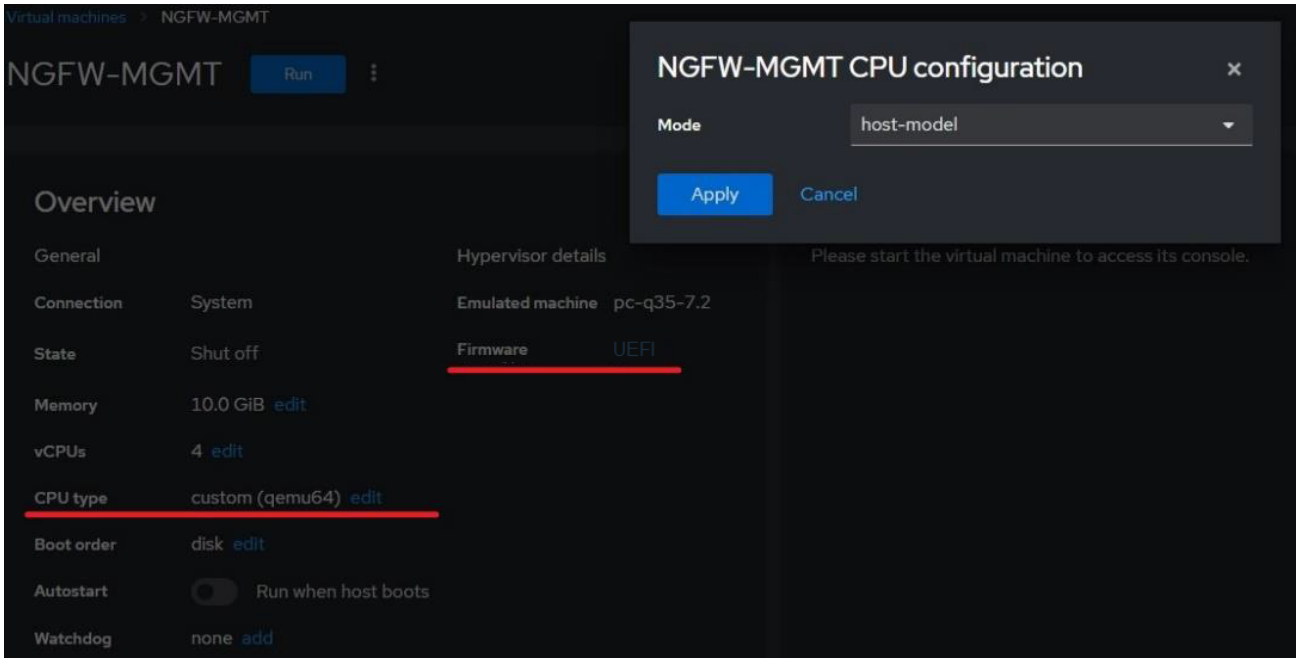


Рисунок 25. Параметры процессора (тип процессора и тип прошивки)

4.2.3. Первоначальная настройка

- После успешного развертывания:

  1. Запустите виртуальную машину с развернутой системой управления и дождитесь завершения загрузки.
  2. Выполните настройку системы управления (см. раздел 5.2).

4.3. Развертывание виртуальной машины PT NGFW

Внимание! При необходимости создания снапшота виртуальная машина должна быть переведена в выключенное состояние. В случае кластерной конфигурации необходимо с минимальным интервалом сначала остановить активный узел, затем резервный, после чего создать снапшоты обеих виртуальных машин. Включение следует выполнять в обратном порядке: сначала резервный узел, затем активный.

В этом разделе

Развертывание виртуальной машины в среде ESXi (см. раздел 4.3.1)

Развертывание виртуальной машины в среде KVM (см. раздел 4.3.2)

Первоначальная настройка (см. раздел 4.3.3)

4.3.1. Развертывание виртуальной машины в среде ESXi

- Чтобы развернуть виртуальную машину в среде ESXi:

  1. Перейдите в раздел **Virtual Machines**.
  2. Начните процесс создания новой виртуальной машины, нажав **Create / Register VM**.

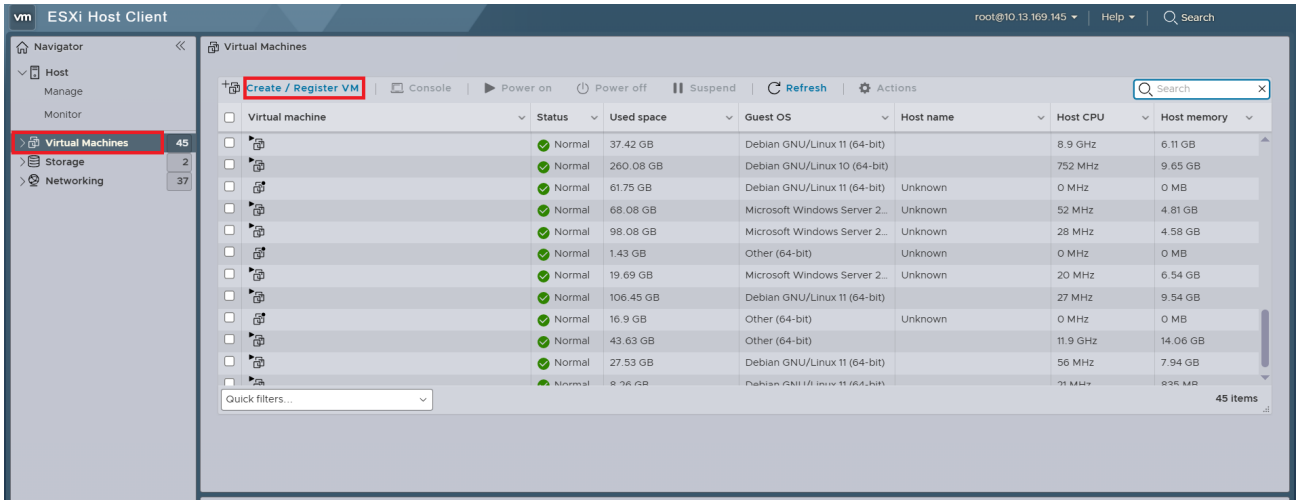


Рисунок 26. Создание виртуальной машины

  3. Выберите тип развертывания из образа OVA — **Deploy a virtual machine from an OVF or OVA file** и нажмите **NEXT**.

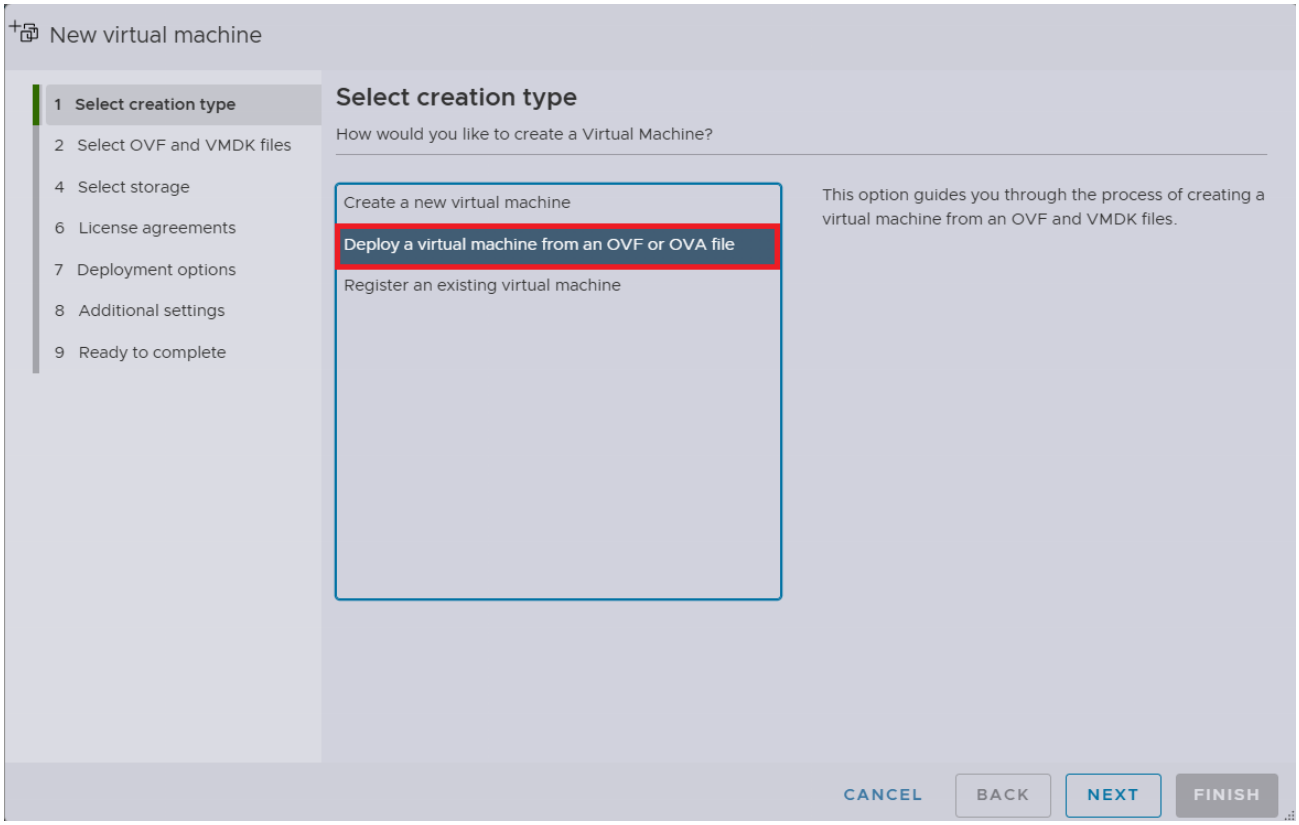


Рисунок 27. Развертывание из образа OVA

4. Введите имя будущей виртуальной машины.
5. Нажмите **Click to select files or drag/drop** и выберите файл с расширением OVA виртуальной машины системы управления PT NGFW.
6. Нажмите **NEXT**.

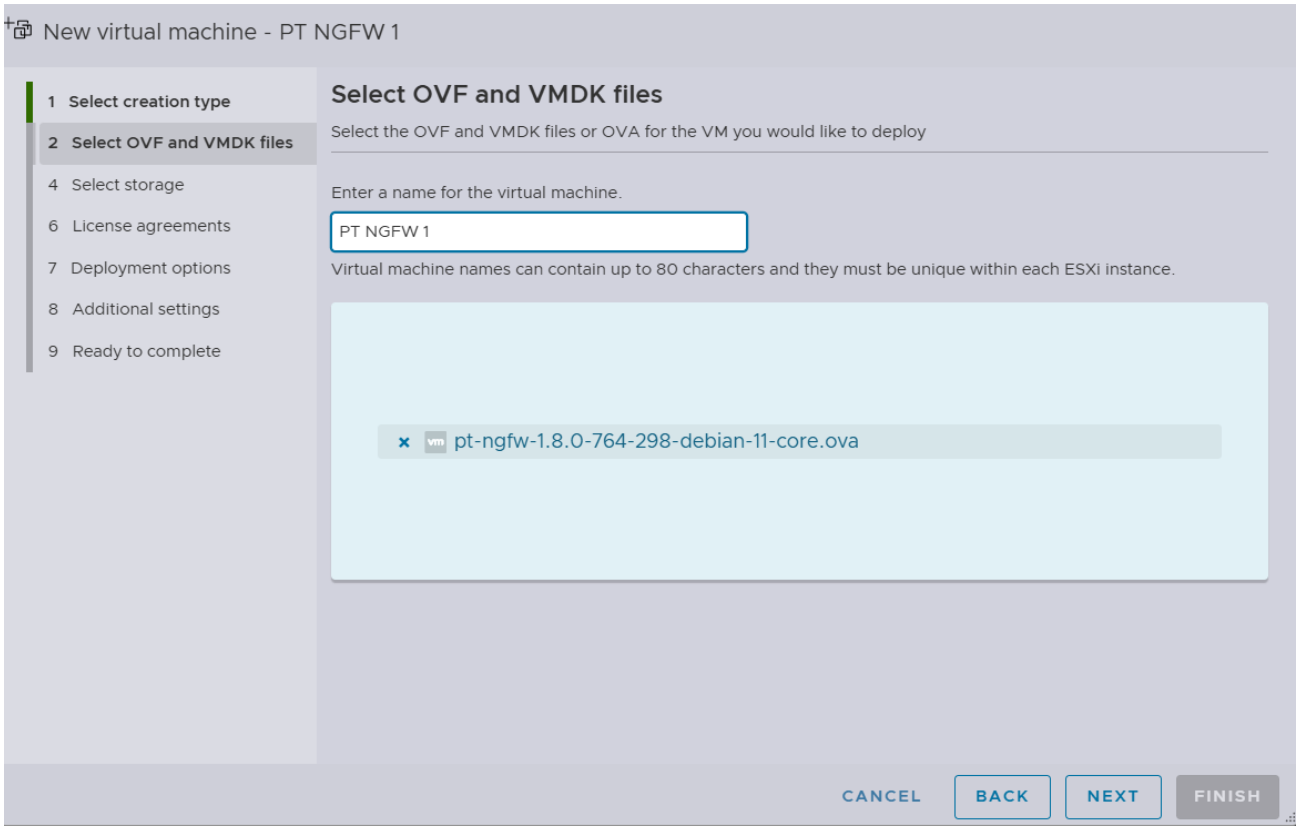


Рисунок 28. Ввод имени виртуальной машины и выбор файлов

7. Выберите хранилище, в котором будут находиться файлы виртуальной машины.

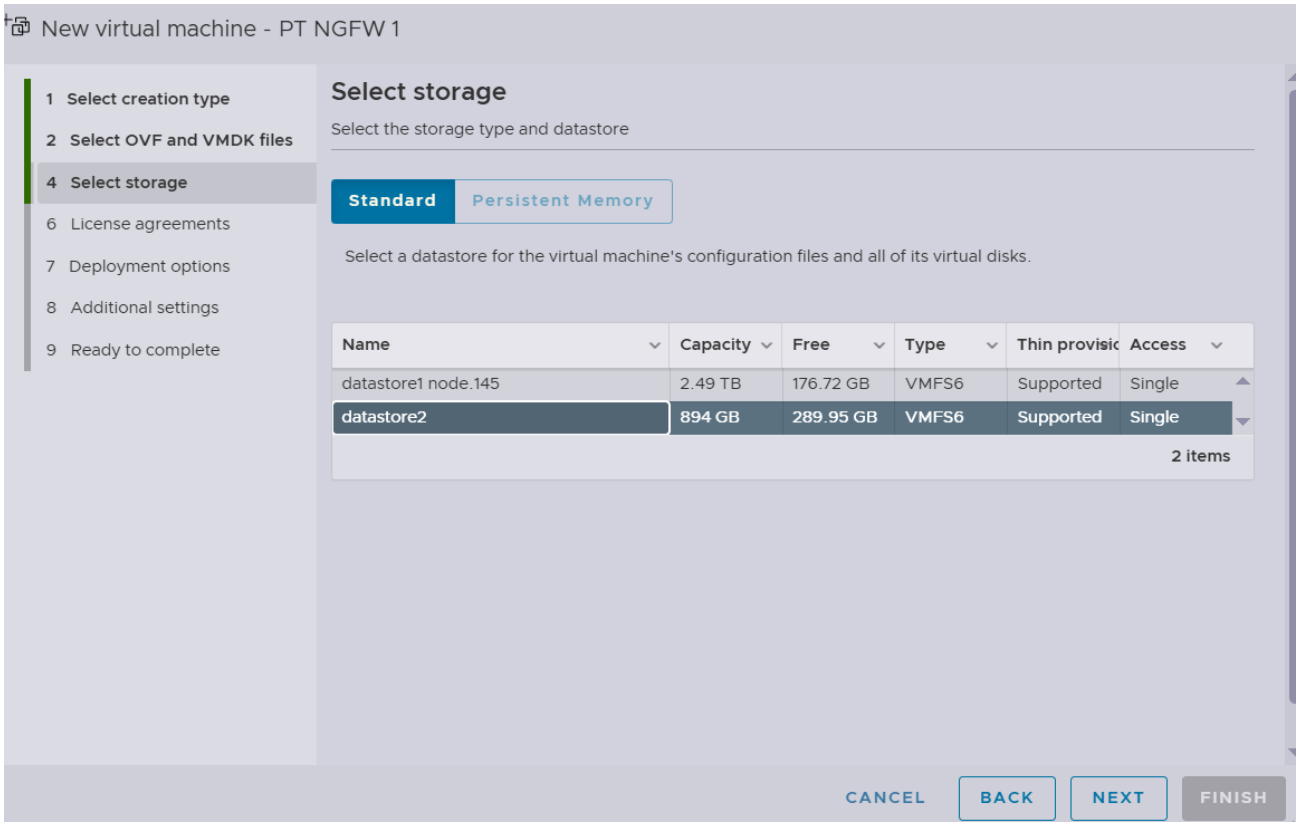


Рисунок 29. Выбор хранилища

8. Ознакомьтесь с условиями лицензионного соглашения и примите его, нажав **I AGREE**.
9. Нажмите **NEXT**.

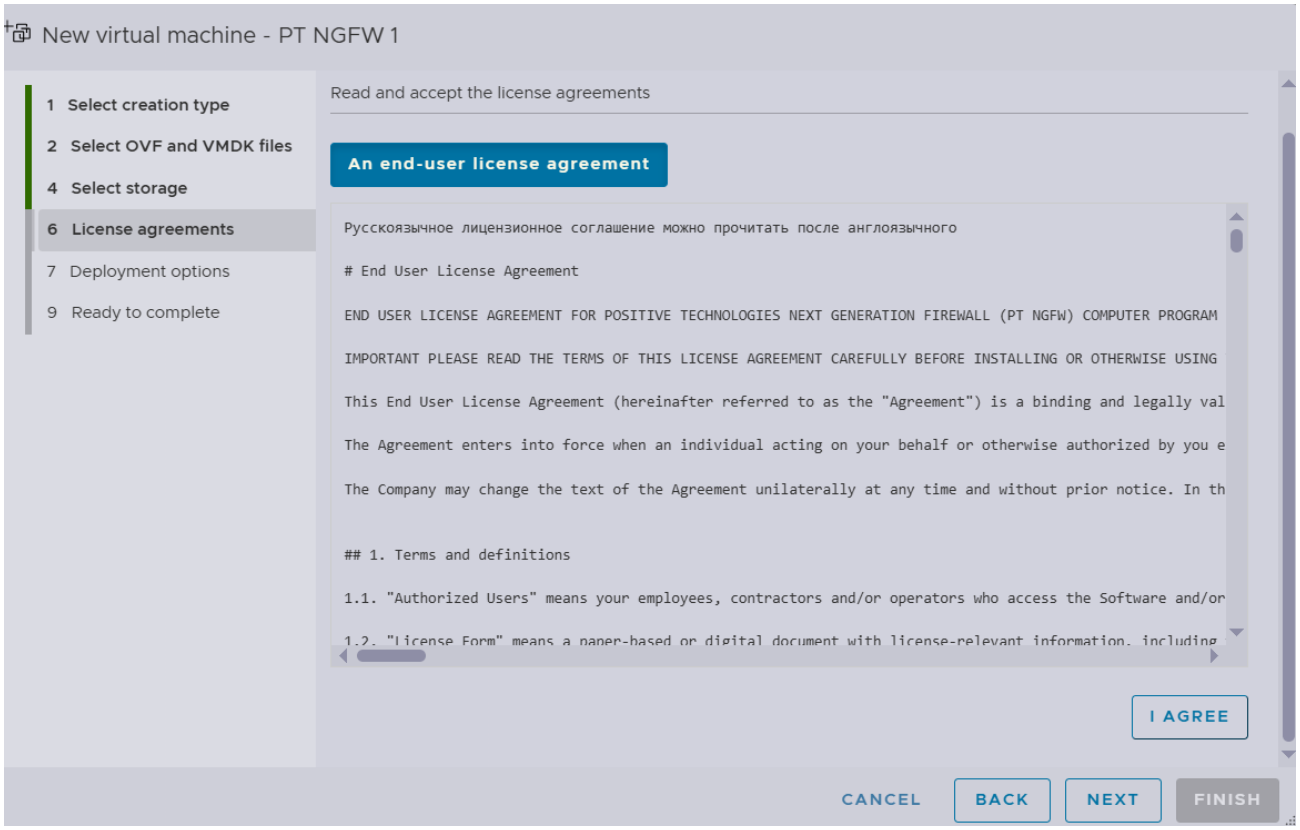


Рисунок 30. Лицензионное соглашение

10. В блоке параметров **Deployment options** настройте следующие параметры:

- **Network mappings** → **Management network** — выберите порт-группу виртуального коммутатора ESXi, к которому должен быть подключен сетевой интерфейс системы управления PT NGFW.
- **Cluster Sync-link** — если разворачиваемая виртуальная машина PT NGFW будет объединяться в кластер с другим виртуальным PT NGFW, выберите порт-группу виртуального коммутатора ESXi, которая будет использоваться для канала синхронизации кластера Sync-link.

  Примечание. Порт-группа для канала синхронизации кластера Sync-link должна быть отдельной порт-группой, которая не используется для подключений к ней каких-либо других сетевых интерфейсов.
- **Deployment type** — в раскрывающемся списке выберите модель разворачиваемой виртуальной машины.

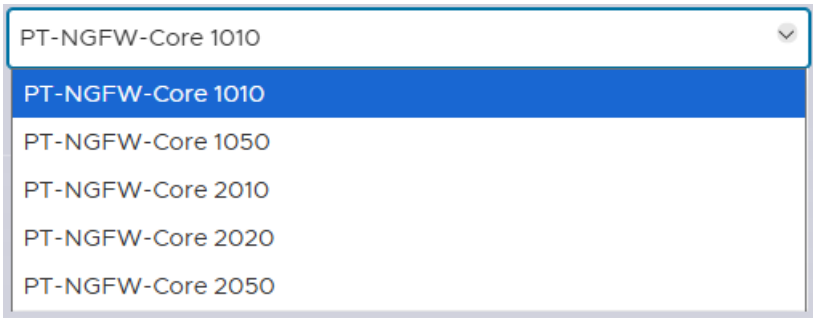


Рисунок 31. Выбор модели разворачиваемой виртуальной машины

Примечание. Модель виртуальной машины определяет объем выделяемых ресурсов: количество ядер виртуального процессора (vCPU), объем оперативной памяти (vRAM) и, следовательно, ее производительность. Перед выбором модели виртуальной машины убедитесь, что виртуальная среда имеет ресурсы, требуемые виртуальной машине PT NGFW. Объем необходимых ресурсов для каждой из моделей виртуального PT NGFW указан в разделе «Программные и аппаратные требования» Справки PT NGFW.

- **Disk provisioning** — если вы собираетесь использовать виртуальную машину в рабочей среде, выберите тип **Thick**. Для лабораторного или тестового использования допускается тип **Thin**.
- **Power on automatically** — если требуется, чтобы виртуальная машина была запущена сразу после развертывания, оставьте установленным флажок **Power on automatically**.

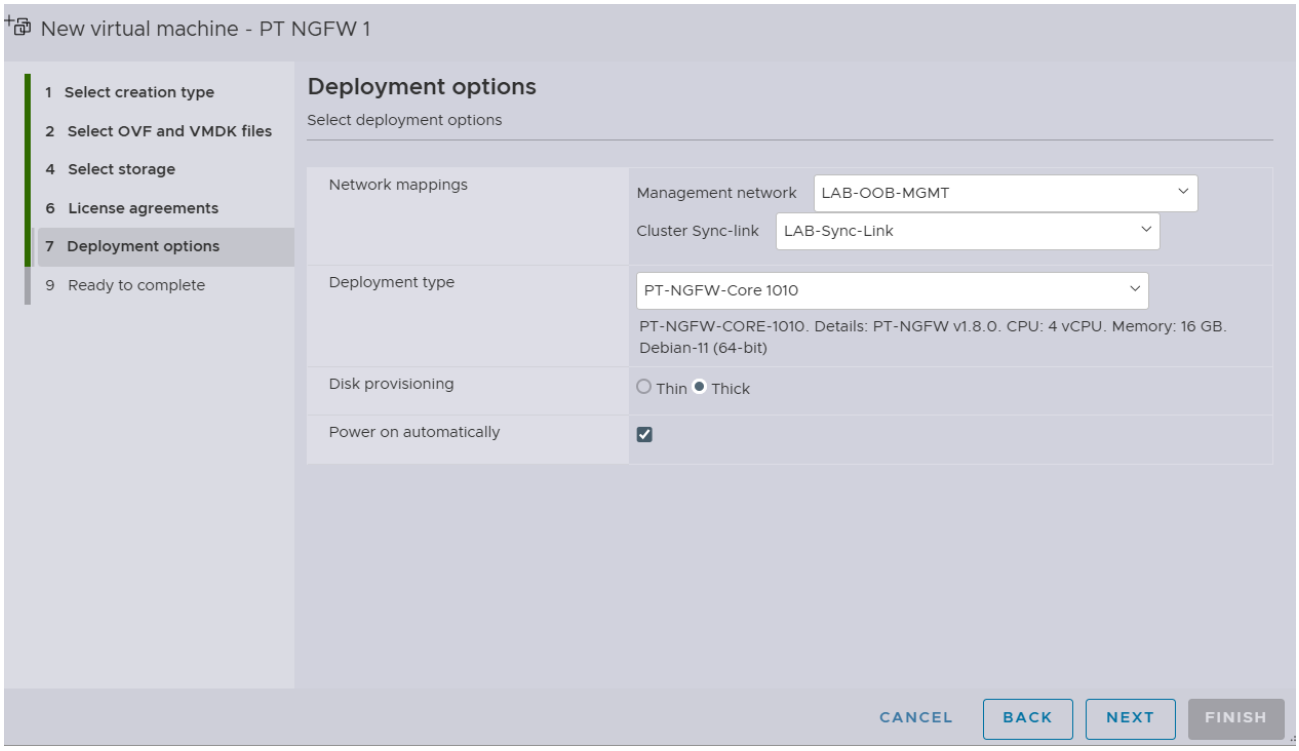


Рисунок 32. Блок параметров **Deployment options**

11. Проверьте параметры установки в окне со сводной информацией и, если все указано верно, нажмите **FINISH**.

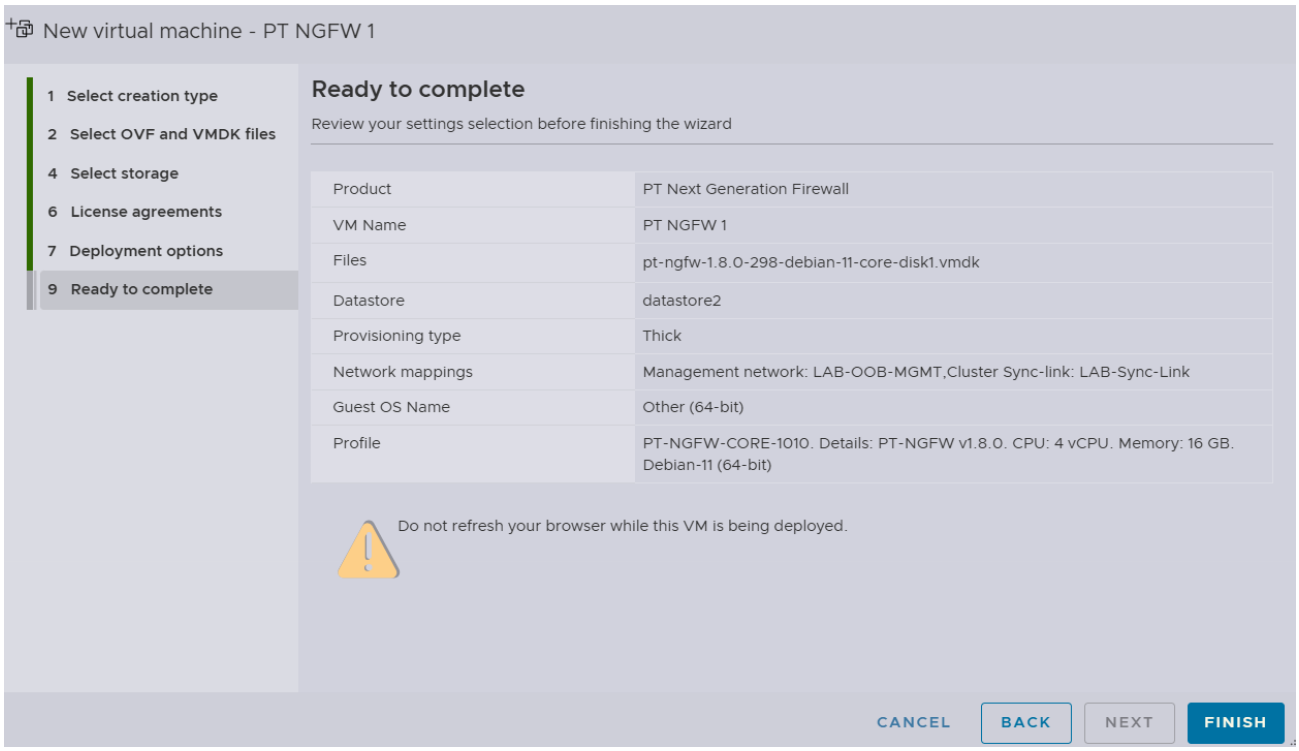


Рисунок 33. Завершение развертывания виртуальной машины в среде ESXi

4.3.2. Развертывание виртуальной машины в среде KVM

- Чтобы развернуть виртуальную машину в среде KVM:

1. Начните процесс импортирования виртуальной машины, нажав **Import VM**.

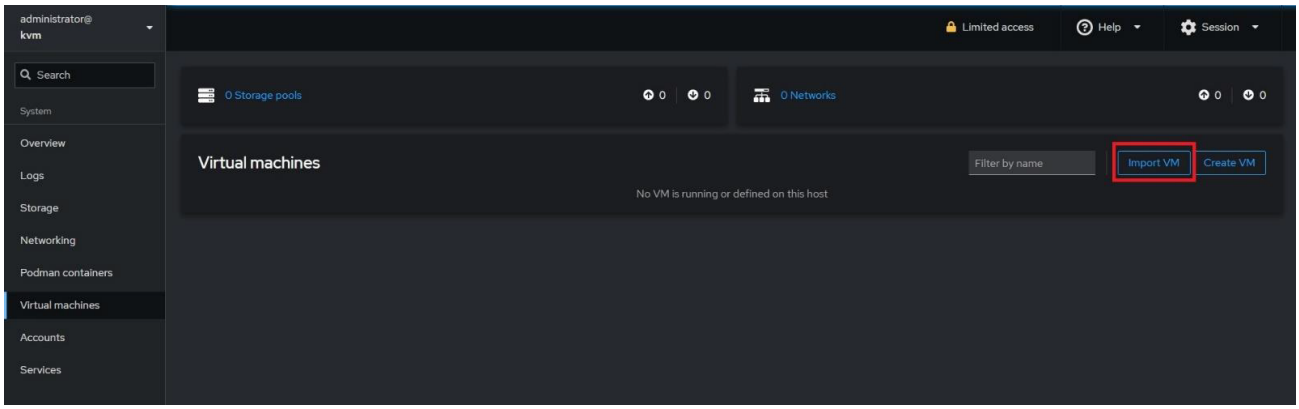


Рисунок 34. Импортирование виртуальной машины

2. Введите параметры импортируемой машины и нажмите **Import and run**.

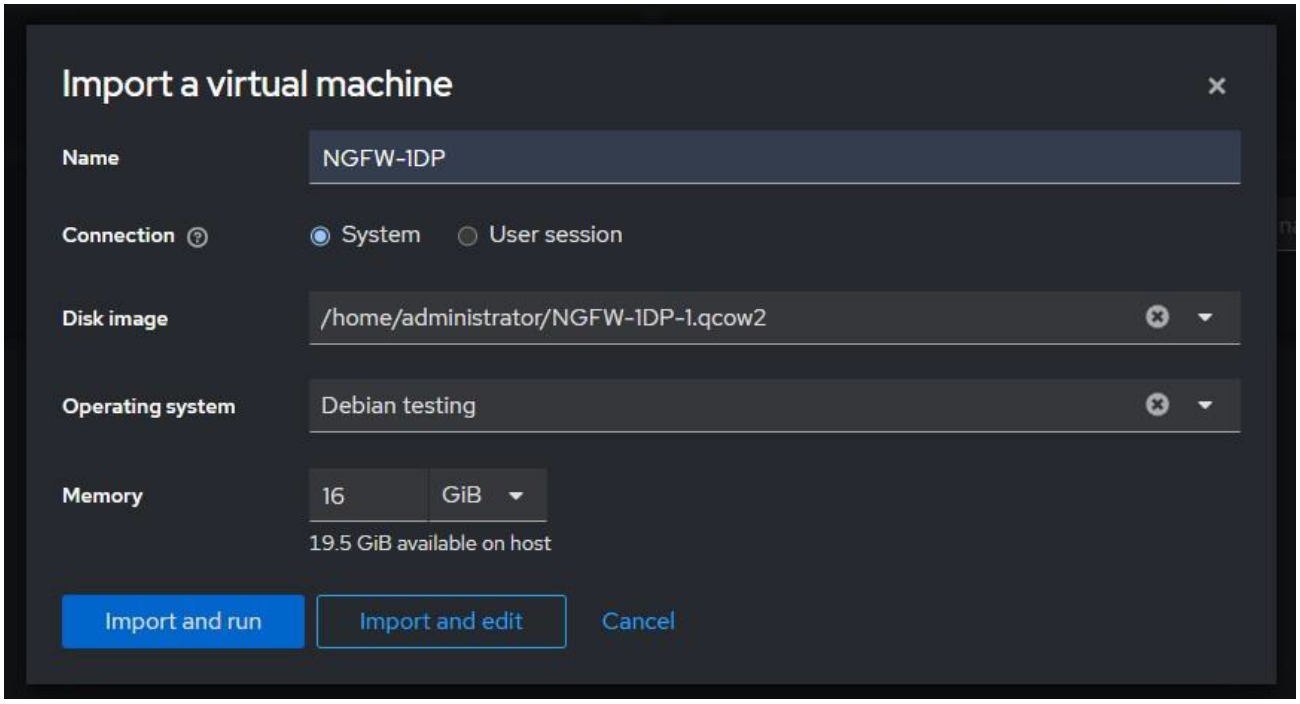


Рисунок 35. Ввод параметров импортируемой машины

3. По завершении импортирования измените параметры процессора:

   - Укажите количество ядер.

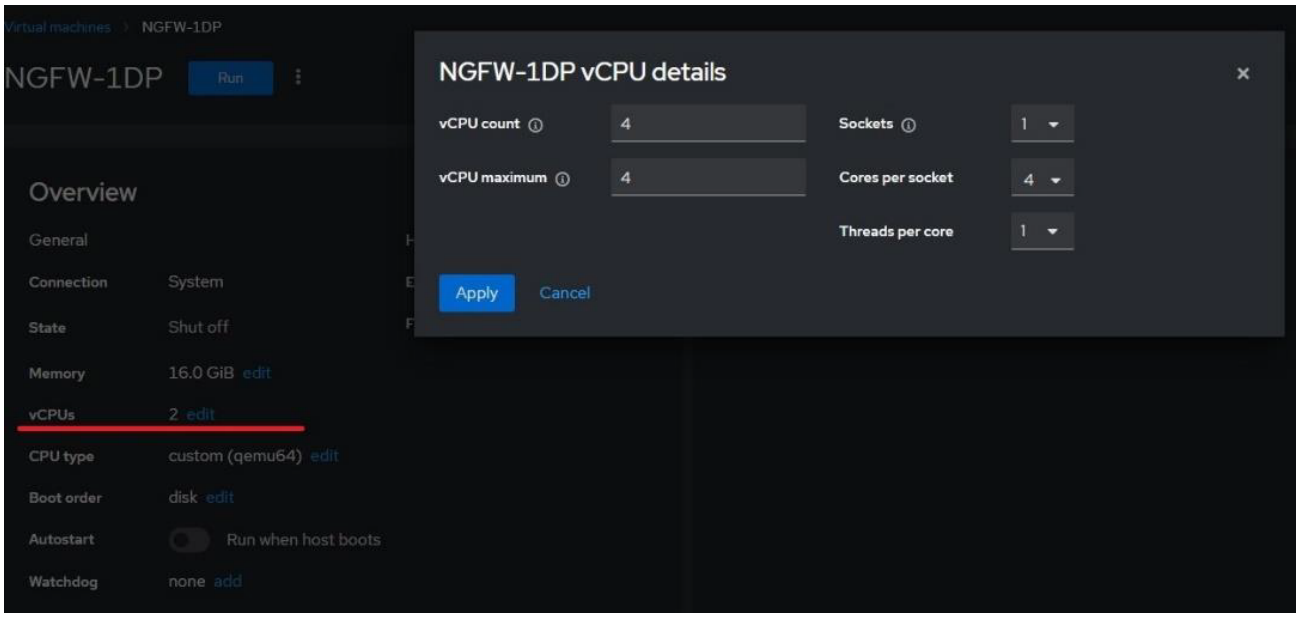


Рисунок 36. Параметры процессора (количество ядер)

   - Укажите тип процессора и тип прошивки.

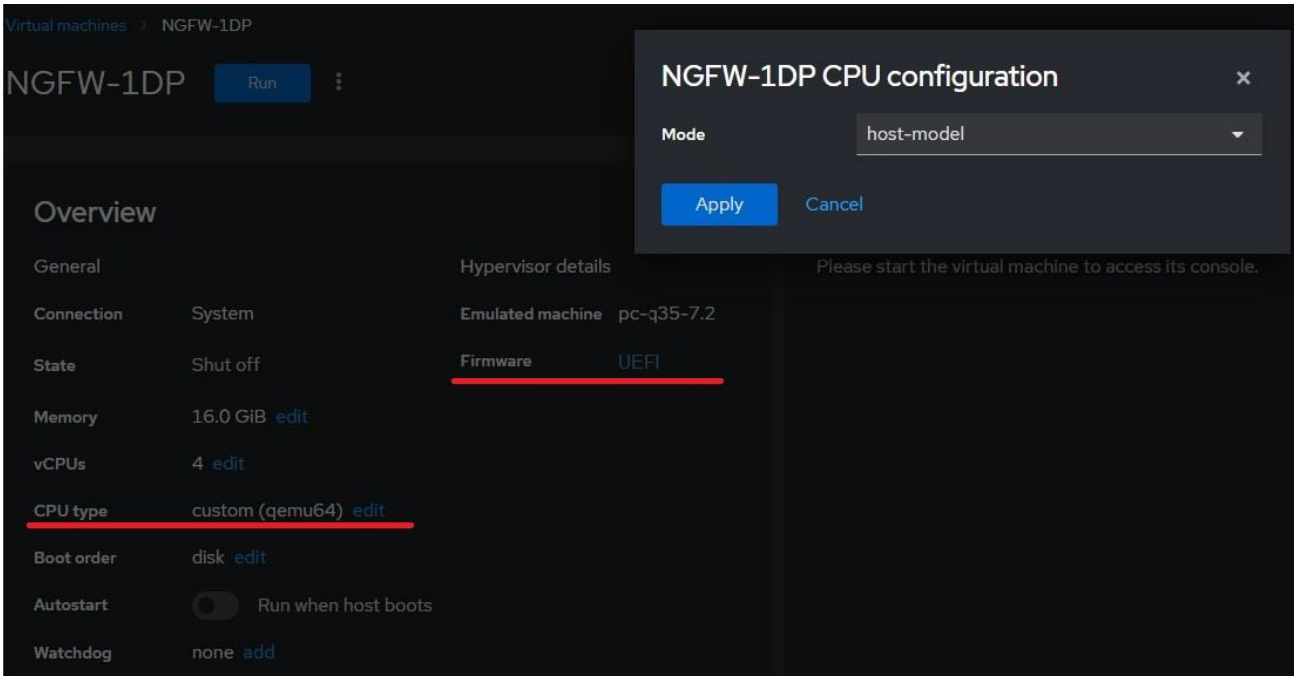


Рисунок 37. Параметры процессора (тип процессора и тип прошивки)

4. Добавьте сетевые интерфейсы.

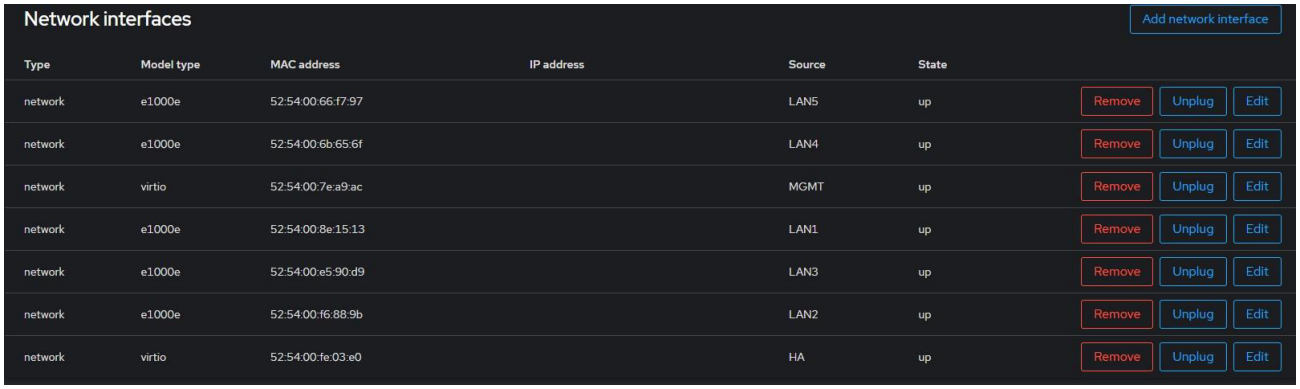


Рисунок 38. Сетевые интерфейсы

Примечание. Готовые образы рассчитаны на 8 сетевых интерфейсов.

5. Запустите виртуальную машину и подключитесь к консоли управления.
6. Войдите в учетную запись ОС, используя логин `ngfw` и пароль `p0sitive`.
7. Просмотрите список адаптеров и убедитесь в корректности их адресов:
   ```
   sudo lspci | grep -i eth
   ```

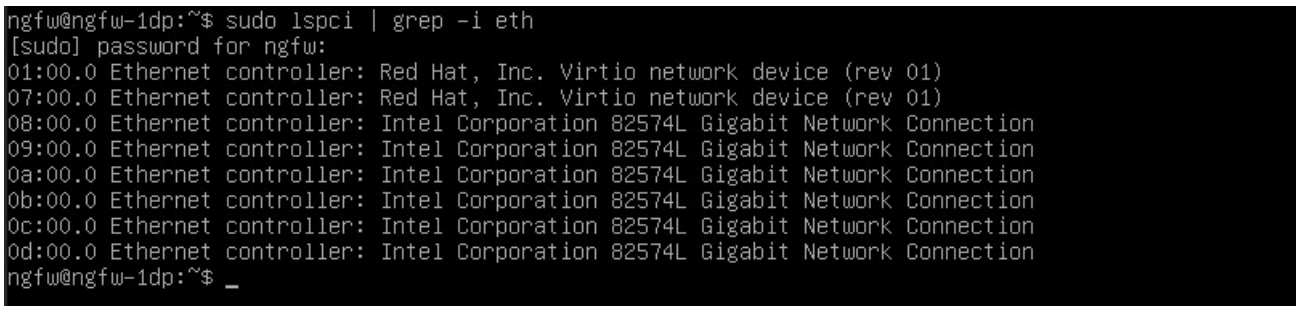


Рисунок 39. Просмотр списка адаптеров

В этом примере адаптер по адресу 08:00.0 это интерфейс eth1-1, адаптер по адресу 09:00.0 это интерфейс eth1-2 и т. д.

8. Если требуется, измените в файле `pt-ngfw.conf` в разделе `devices` адреса адаптеров `eth1-1`, `eth1-2`, `eth1-3`, `eth1-4`, `eth1-5` и `eth1-6` (значение `addr`):

   ```
   sudo nano /opt/pt-ngfw/ngfw-core/etc/config/pt-ngfw.conf
   ```

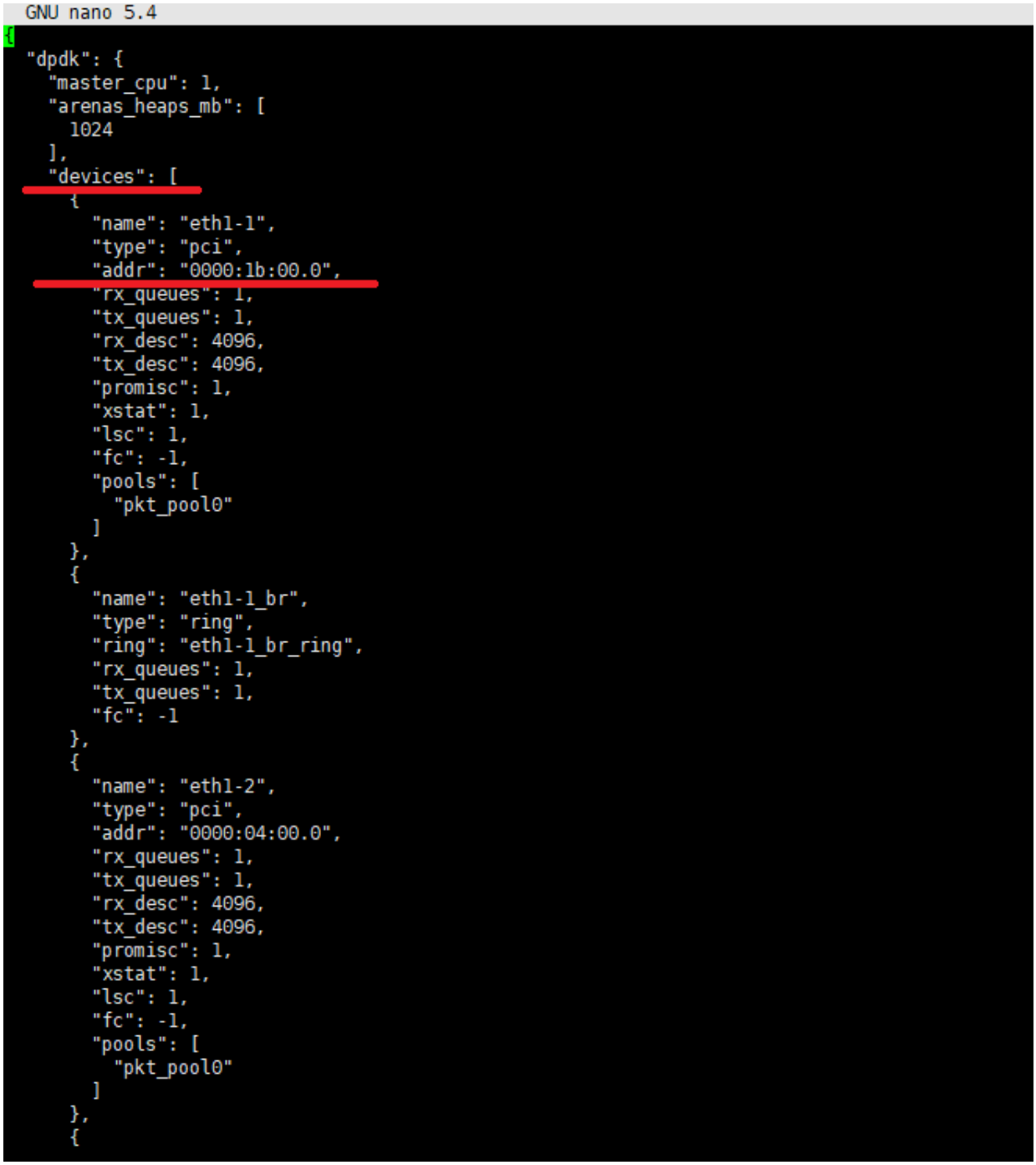


Рисунок 40. Содержимое файла `pt-ngfw.conf`

9. Перезапустите сервис, чтобы изменения вступили в силу:

   ```
   sudo systemctl restart pt-ngfw-core.service
   ```

4.3.3. Первоначальная настройка

- После успешного развертывания:

  1. Запустите виртуальную машину с развернутым межсетевым экраном и дождитесь завершения загрузки.
  2. Выполните настройку межсетевого экрана (см. раздел 5.3).

См. также

Настройка системы управления (см. раздел 5.2)

4.4. Развертывание системы мониторинга

В этом разделе приводятся инструкции по развертыванию системы мониторинга PT NGFW.

В этом разделе

Развертывание виртуальной машины в среде ESXi (см. раздел 4.4.1)

Настройка интерфейса управления (MGMT) (см. раздел 4.4.2)

Настройка DNS-сервера в ОС (см. раздел 4.4.3)

Настройка синхронизации времени с NTP-сервером (см. раздел 4.4.4)

Первоначальная настройка (см. раздел 4.4.5)

4.4.1. Развертывание виртуальной машины в среде ESXi

- Чтобы развернуть виртуальную машину в среде ESXi:

  1. Начните процесс создания новой виртуальной машины, нажав **Create / Register VM**.

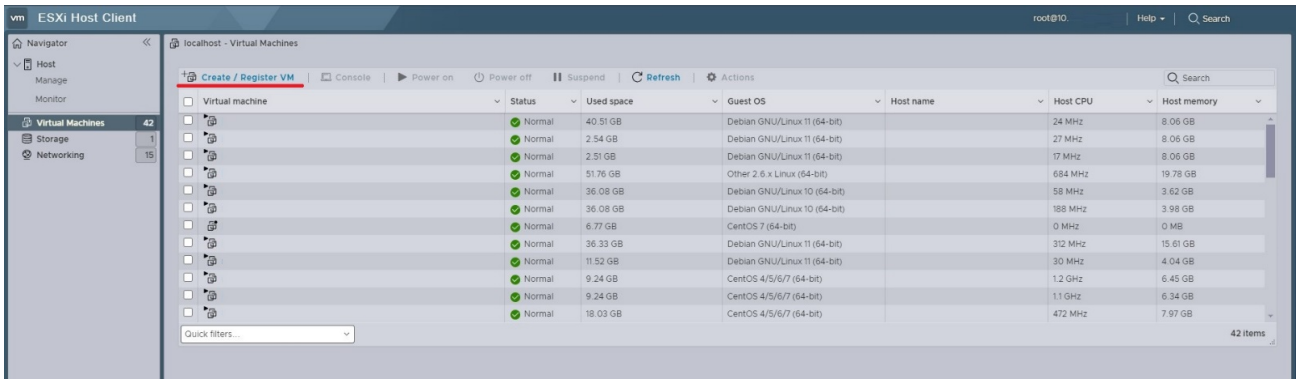


Рисунок 41. Создание новой виртуальной машины

  2. Выберите вариант развертывания из образа OVF.

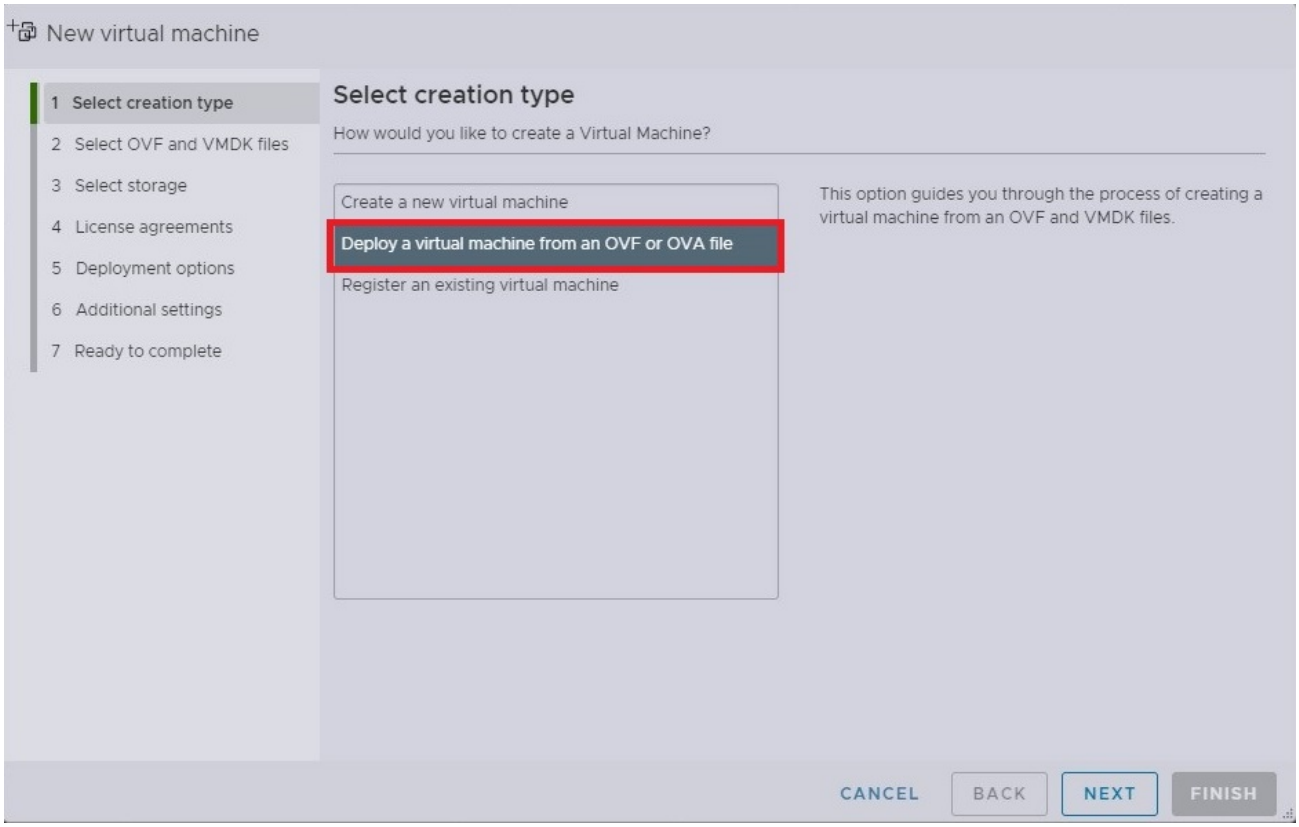


Рисунок 42. Развертывание из образа OVF

3. Выберите файлы OVF и VMDK.
4. Введите имя виртуальной машины.

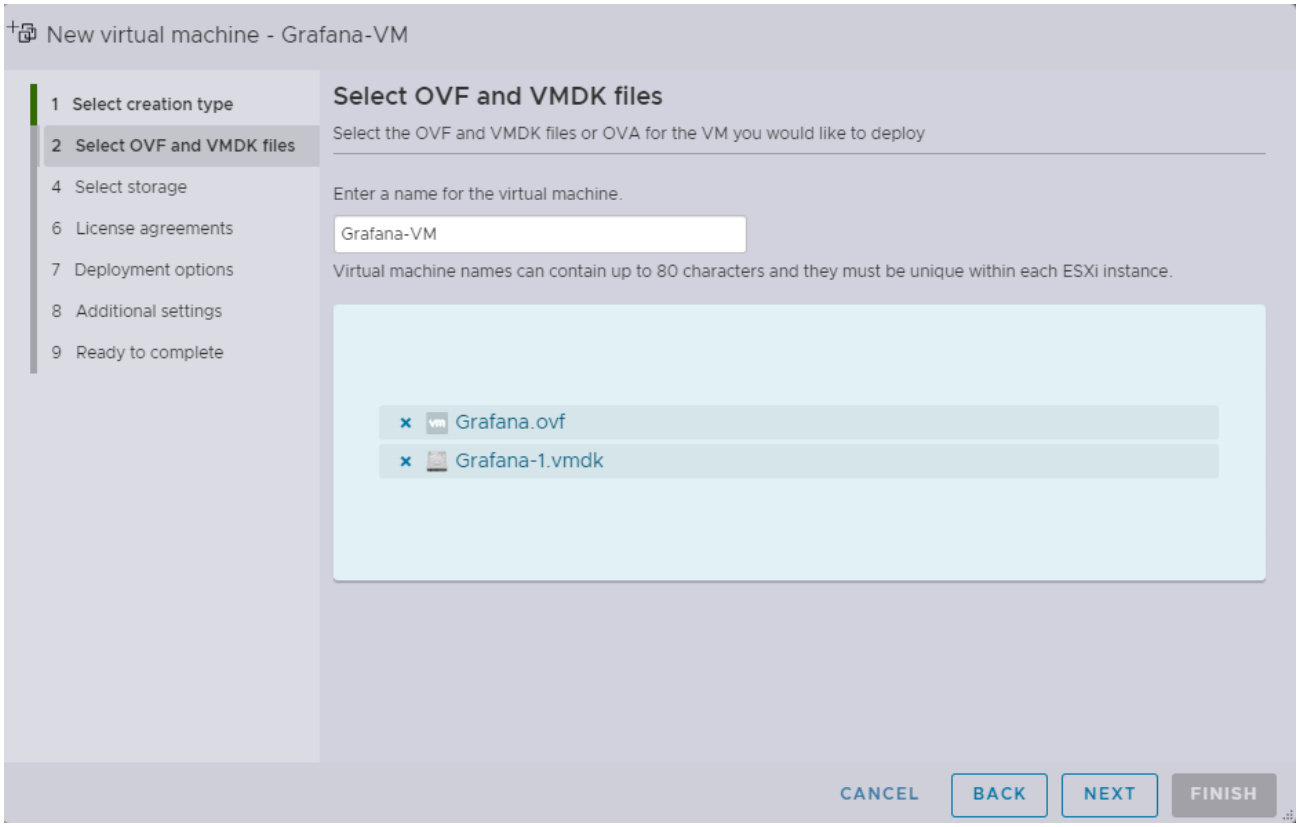


Рисунок 43. Ввод имени виртуальной машины и выбор файлов

5. Выберите хранилище.

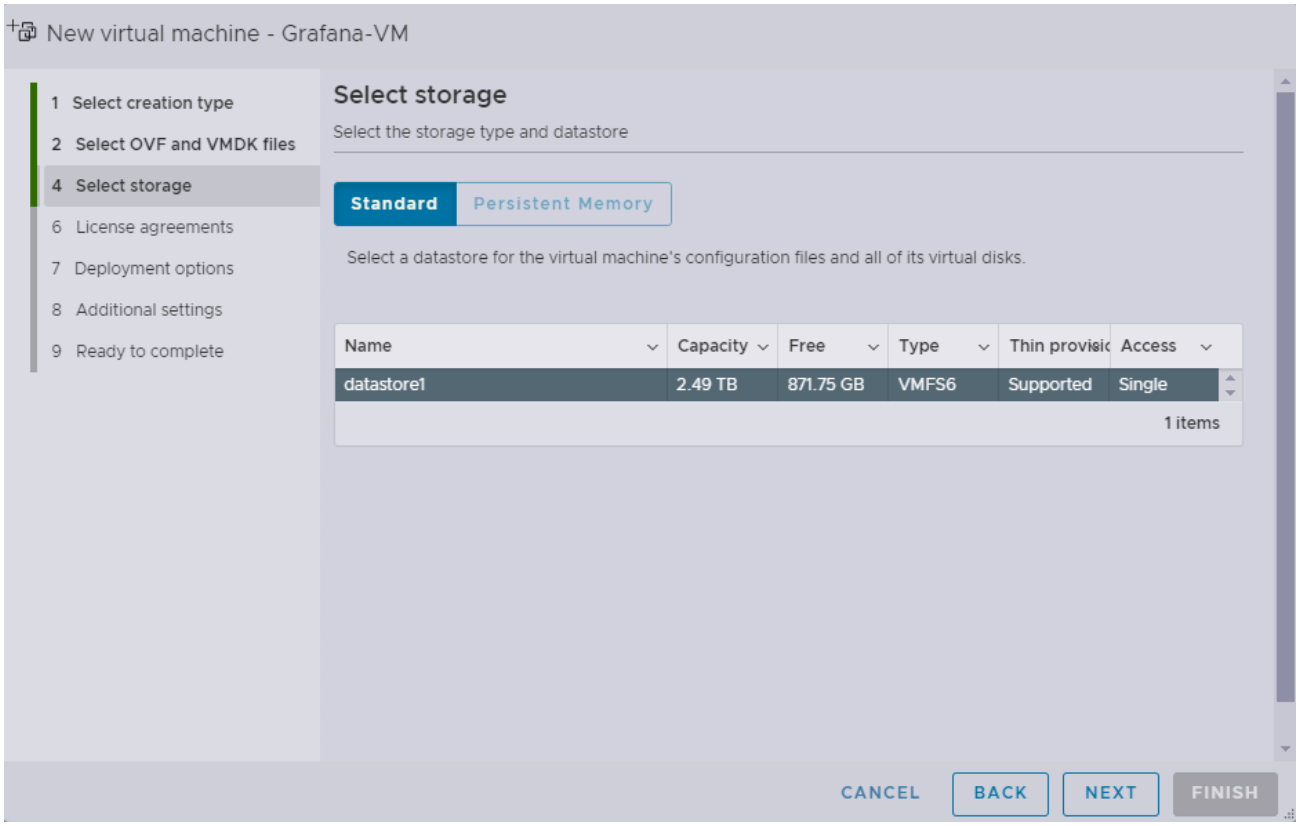


Рисунок 44. Выбор хранилища

6. Выберите способ маппинга интерфейсов на подсети виртуализации.

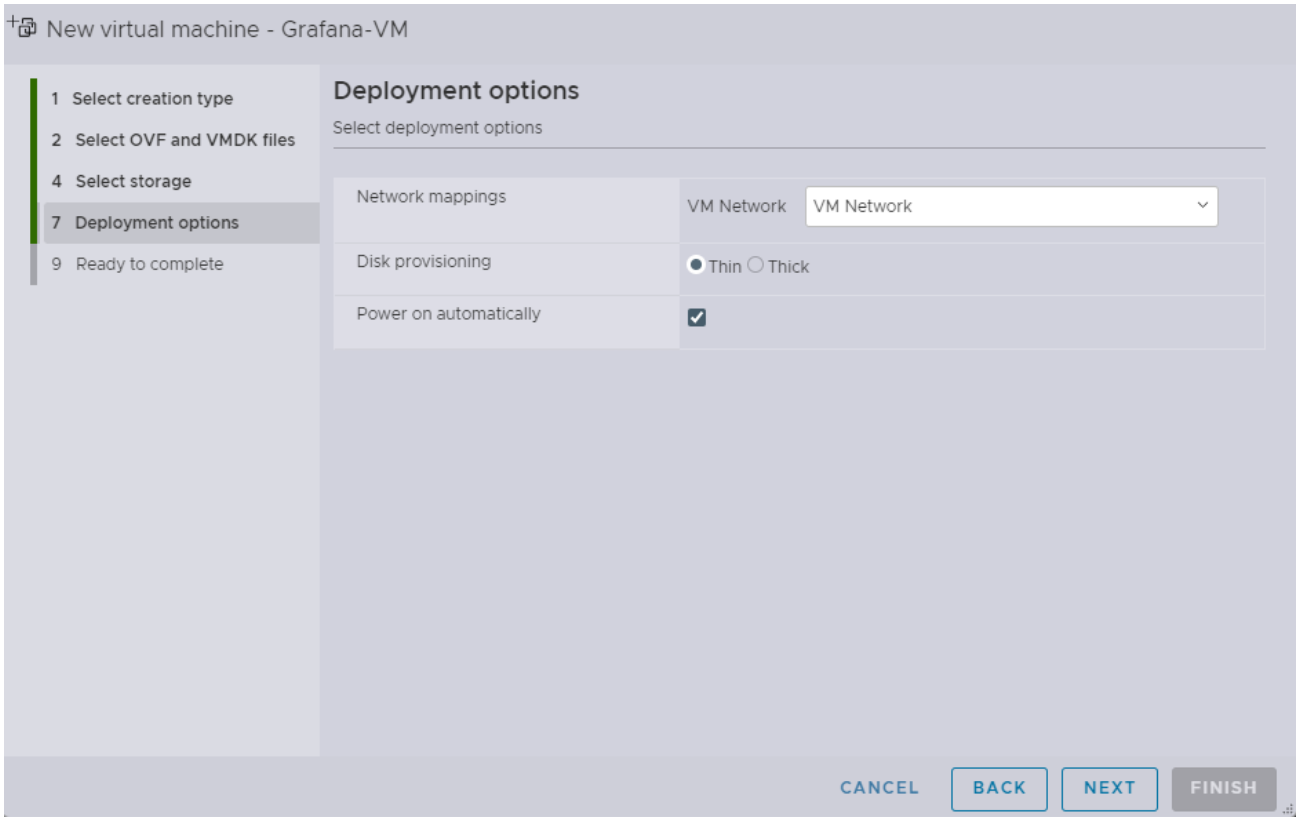


Рисунок 45. Выбор способа маппинга интерфейсов

7. Нажмите **FINISH**.

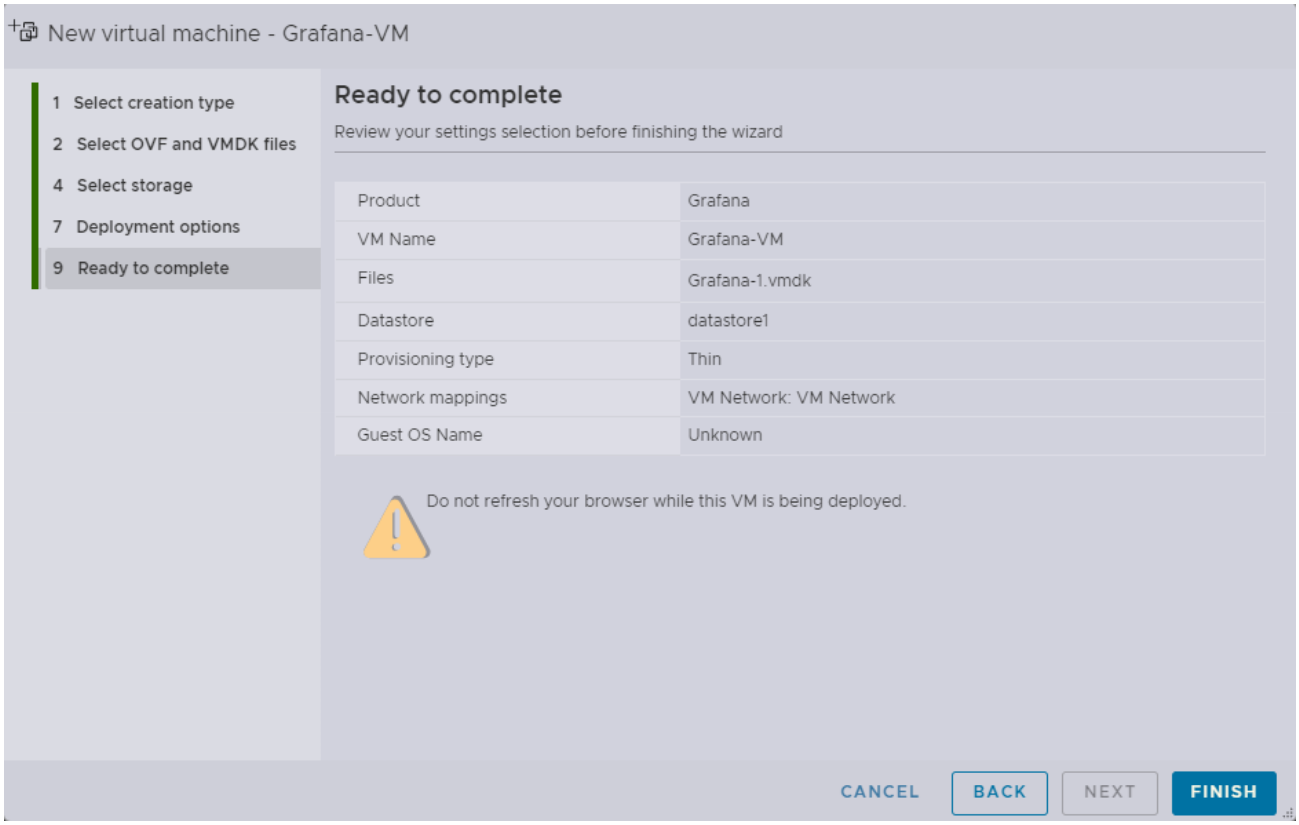


Рисунок 46. Завершение развертывания виртуальной машины в среде ESXi

4.4.2. Настройка интерфейса управления (MGMT)

- Чтобы настроить интерфейс управления:

  1. Подключитесь к консоли управления виртуальной машины.
  2. Войдите в учетную запись ОС, используя логин `ngfw` и пароль `p0sitive`.
  3. Измените параметры сетевого интерфейса ens192:

     ```
     sudo nano /etc/network/interfaces
     ```

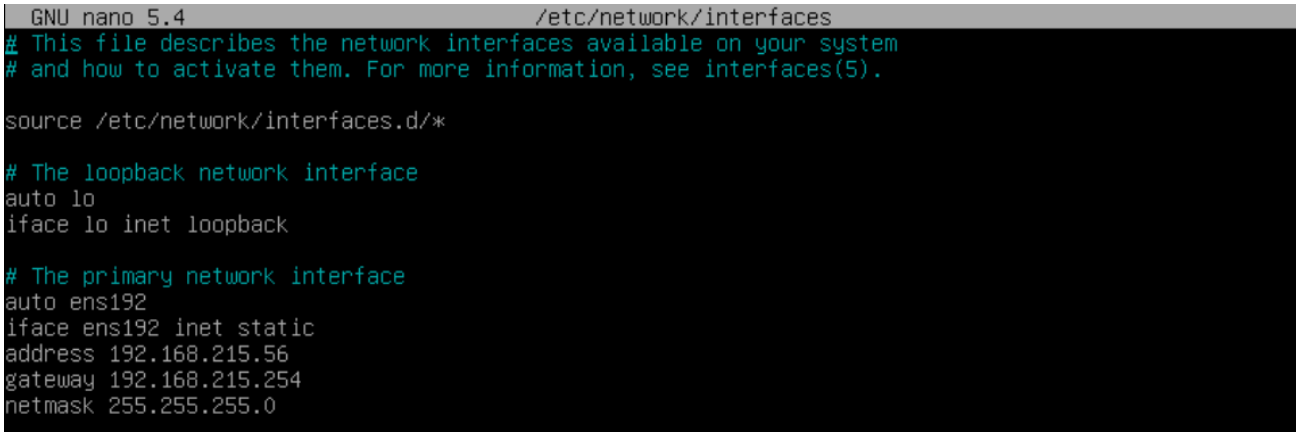


Рисунок 47. Параметры сетевого интерфейса ens192

4. Перезапустите сервис, чтобы изменения вступили в силу:
   `sudo systemctl restart networking.service`

4.4.3. Настройка DNS-сервера в ОС

Настройка DNS-сервера нужна для корректной работы сервисов. Для этого необходимо указать в параметрах внутренний или внешний DNS-сервер.

- Чтобы настроить DNS-сервер:

1. Откройте конфигурационный файл `resolv.conf`:
   `sudo nano /etc/resolv.conf`
2. Добавьте DNS-сервер.

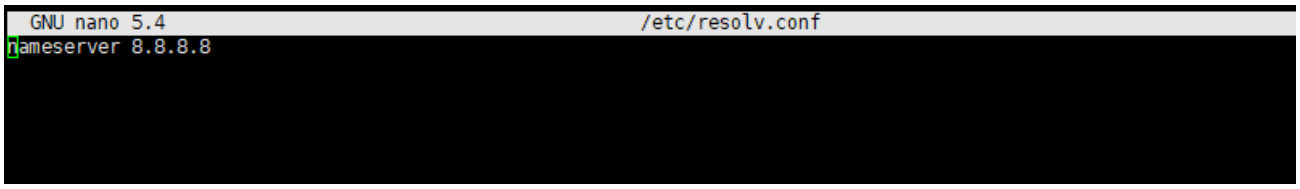


Рисунок 48. Содержимое файла `resolv.conf`

> **Примечание.** Адрес указанного DNS-сервера (серверов) используется базовой операционной системой и не влияет на разрешение FQDN в политиках безопасности процессом PT NGFW.

4.4.4. Настройка синхронизации времени с NTP-сервером

Для корректной работы систем журналирования и мониторинга необходимо синхронизировать время. Для этого используются NTP-серверы.

- Чтобы настроить синхронизацию времени с NTP-сервером:

  1. Откройте конфигурационный файл `timesyncd.conf`:
     ```
     sudo nano /etc/systemd/timesyncd.conf
     ```
  2. Раскомментируйте строку `NTP` и введите адрес NTP-сервера по своему усмотрению.

```
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See timesyncd.conf(5) for details.

[Time]
NTP=ntp.test.ru
#FallbackNTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
#RootDistanceMaxSec=5
#PollIntervalMinSec=32
#PollIntervalMaxSec=2048
```

Рисунок 49. Содержимое файла `timesyncd.conf`

  3. Перезапустите сервис, чтобы изменения вступили в силу:
     ```
     sudo systemctl restart systemd-timesyncd
     ```
     Вы можете проверить работоспособность службы с помощью команды:
     ```
     timedatectl timesync-status
     ```

4.4.5. Первоначальная настройка

- После успешного развертывания:

  1. Запустите виртуальную машину с развернутой системой мониторинга.
  2. Подключитесь к консоли управления виртуальной машины.
  3. Выполните настройку системы мониторинга (см. раздел 5.4).

5. Подготовка к работе

Этот раздел поможет вам подготовить PT NGFW к работе и настроить его основные подсистемы. Раздел содержит данные, необходимые для организации взаимодействия между компонентами PT NGFW и смежными системами, а также сведения о монтаже аппаратных платформ в серверную стойку.

В этом разделе

Настройка необходимых сетевых доступов (см. раздел 5.1)

Настройка системы управления (см. раздел 5.2)

Настройка межсетевого экрана (см. раздел 5.3)

Настройка системы мониторинга (см. раздел 5.4)

Настройка выделенного сборщика журналов (см. раздел 5.5)

5.1. Настройка необходимых сетевых доступов

Для взаимодействия компонентов и подсистем PT NGFW необходимо обеспечить прохождение IP-пакетов между ними. В зависимости от развернутых в вашей сети компонентов PT NGFW и конфигурации сети, настройте сетевые доступы, используя таблицы ниже.

Таблица 5. Взаимодействие компонентов PT NGFW

№	Источник			Назначение			Описание взаимодействия
	Наименование	Интерфейс	Порт и протокол	Наименование	Интерфейс	Порт и протокол	
1	Система управления	mgmt	Динамический, TCP	Межсетевой экран	mgmt	443, TCP	Управление и настройка межсетевых экранов по протоколу HTTPS
2	Межсетевой экран	mgmt	Динамический, TCP	Система управления	mgmt	5570, TCP	Получение информации о пользователях Active Directory. Обращение к службе User Agent
3	Межсетевой экран	mgmt	Динамический, TCP	Система управления	mgmt	7002, TCP	Отправка журналов событий безопасности
4	Межсетевой экран	mgmt	Динамический, TCP	Система мониторинга	mgmt	8086, TCP	Передача телеметрической информации в подсистему мониторинга. Обращение к службе InfluxDB
5	Межсетевой экран	mgmt	Динамический, TCP	Портал аутентификации	mgmt	80, 443, TCP	Выполнение авторизации пользователей через веб-страницу (форму) для получения доступа к сетевым ресурсам
6	Межсетевой экран	sync	5650, TCP	Межсетевой экран	sync	5650, TCP	Обмен информацией между межсетевыми экранами, объединенными в кластер

№	Источник			Назначение			Описание взаимодействия
	Наименование	Интерфейс	Порт и протокол	Наименование	Интерфейс	Порт и протокол	
7	Система управления	mgmt	Динамический, TCP	Система управления	mgmt	5432, TCP	Порт службы PostgreSQL. Должен быть открыт как для основной, так и для резервной системы управления
8	Система управления	mgmt	Динамический, TCP	Система управления	mgmt	8040, TCP	Порт API системы управления. Должен быть открыт как для основной, так и для резервной системы управления
9	Система управления	mgmt	Динамический, TCP	Система управления	mgmt	8230, TCP	Порт объектного хранилища. Должен быть открыт как для основной, так и для резервной системы управления
10	Система управления	mgmt	Динамический, TCP	Сборщик журналов	mgmt	7015, TCP	Порт API сборщика журналов
11	Межсетевой экран	mgmt	Динамический, TCP	Сборщик журналов	mgmt	7002, TCP	Отправка журналов событий безопасности
12	Межсетевой экран	mgmt	Динамический, TCP	Система управления	mgmt	6090, TCP	Загрузка обновлений на межсетевой экран

Таблица 6. Взаимодействие PT NGFW со смежными системами

№	Источник			Назначение			Описание взаимодействия
	Наименование	Интерфейс	Порт и протокол	Наименование	Интерфейс	Порт и протокол	
1	Рабочая станция оператора	—	Динамический, TCP	Система управления	BMC	22, TCP	Удаленное подключение к системе управления аппаратной платформой (IPMI) по протоколу SSH. Неприменимо для ПАК PT NGFW 1005, 1010, 1020, 1050
				Межсетевой экран			
2	Рабочая станция оператора	—	Динамический, TCP	Система управления	BMC	443, TCP	Удаленное подключение к системе управления аппаратной платформой (IPMI) по протоколу HTTPS. Неприменимо для ПАК PT NGFW 1005, 1010, 1020, 1050
				Межсетевой экран			
3	Рабочая станция оператора	—	Динамический, TCP	Система управления	BMC	3900, TCP	Для удаленного подключения к виртуальной консоли системы управления аппаратной платформой (внеполосное управление через KVM-подключение). Неприменимо для ПАК PT NGFW 1005, 1010, 1020, 1050
				Межсетевой экран			
4	Рабочая станция оператора	—	Динамический, TCP	Система управления	mgmt	22, TCP	Удаленное подключение к CLI серверов с установленными компонентами PT NGFW по протоколу SSH
				Система мониторинга			
				Межсетевой экран			

№	Источник			Назначение			Описание взаимодействия
	Наименование	Интерфейс	Порт и протокол	Наименование	Интерфейс	Порт и протокол	
5	Рабочая станция оператора	—	Динамический, TCP	Система управления	mgmt	443, TCP	Удаленное подключение к системе управления PT NGFW по протоколу HTTPS
6	Рабочая станция оператора	—	Динамический, TCP	Система мониторинга	mgmt	3000, TCP	Удаленное подключение к подсистеме мониторинга PT NGFW по протоколу HTTP(S)
7	Система управления	mgmt	Динамический, UDP	syslog-сервер	—	514, UDP	Передача syslog-событий на внешний сервер
8	Сборщик журналов	mgmt	Динамический, UDP	syslog-сервер	—	514, UDP	Передача syslog-событий на внешний сервер
9	Система управления	mgmt	Динамический, TCP	Контроллер домена Active Directory	—	389, TCP	Получение информации о пользователях из Active Directory, используется протокол LDAP + StartTLS
10	Система управления	mgmt	Динамический, TCP	Контроллер домена Active Directory	—	636, TCP	Получение информации о пользователях из Active Directory по протоколу LDAPs
11	Система управления	mgmt	Динамический, TCP	Контроллер домена Active Directory	—	5986, TCP	Обращение к журналу безопасности (Security) контроллера домена и загрузка информации об аутентификации пользователей Active Directory по WinRM

№	Источник			Назначение			Описание взаимодействия
	Наименование	Интерфейс	Порт и протокол	Наименование	Интерфейс	Порт и протокол	
12	Межсетевой экран	mgmt	Динамический, TCP	ICAP-сервер	—	1344, TCP	Отправка объектов, извлеченных из трафика, на внешний ICAP-сервер
13	Система управления	mgmt	Динамический, UDP	NTP-сервер	—	123, UDP	Синхронизация времени с NTP-сервером
	Система мониторинга	mgmt					
	Межсетевой экран	mgmt					
14	Система управления	mgmt	Динамический, UDP	DNS-сервер	—	53, UDP	Разрешение имен серверов смежных систем, таких как серверы обновления, прокси и контроллеры домена
			Динамический, TCP			53, TCP	
15	Межсетевой экран	mgmt	Динамический, UDP	DNS-сервер	—	53, UDP	Разрешение имен объектов с FQDN
			Динамический, TCP			53, TCP	
16	Межсетевой экран	ethX / aeX	500, UDP	VPN-шлюз	—	500, UDP	Обмен IKEv2-сообщениями для построения IPsec site-to-site VPN (без NAT)

№	Источник			Назначение			Описание взаимодействия
	Наименование	Интерфейс	Порт и протокол	Наименование	Интерфейс	Порт и протокол	
17	Межсетевой экран	ethX / aeX	IP/ESP	VPN-шлюз	—	IP/ESP	Передача данных при использовании IPsec site-to-site VPN (без NAT)
18	VPN-шлюз		500, UDP	Межсетевой экран	ethX / aeX	500, UDP	Обмен IKEv2-сообщениями для построения IPsec site-to-site VPN (без NAT)
19	VPN-шлюз	—	IP/ESP	Межсетевой экран	ethX / aeX	IP/ESP	Передача данных при использовании IPsec site-to-site VPN (без NAT)
20	Межсетевой экран	ethX / aeX	4500, UDP	VPN-шлюз	—	4500, UDP	Построение site-to-site VPN с использованием протокола IPsec NAT Traversal (NAT-T)
21	VPN-шлюз	—	4500, UDP	Межсетевой экран	ethX / aeX	4500, UDP	Построение site-to-site VPN с использованием протокола IPsec NAT Traversal (NAT-T)
22	Межсетевой экран	mgmt	Динамический, UDP	SNMP-сервер	—	162, UDP	Асинхронное уведомление от межсетевого экрана на SNMP-сервер
23	SNMP-сервер	—	Динамический, UDP	Межсетевой экран	mgmt	161, UDP	Запрос от SNMP-сервера на межсетевой экран для получения значения переменной или списка переменных
24	Рабочая станция оператора (внешняя система)	—	Динамический, TCP	Межсетевой экран	mgmt	443, TCP	Выгрузка телеметрической информации в стороннюю систему в формате JSON

Таблица 7. Доступ, необходимый при установке компонентов

Источник			**Назначение**			**Описание взаимодействия**
Наименование	**Интерфейс**	**Порт, протокол**	**Наименование**	**Интерфейс**	**Порт, протокол**	
Система управления	mgmt	Динамический, TCP	Межсетевой экран	mgmt	22, TCP	Доступ по SSH-протоколу к межсетевому экрану для установки компонентов

5.2. Настройка системы управления

Для настройки системы управления подключитесь к ней и выполните вход в ОС, используя логин `ngfw` и пароль `p0sitive`. Подключение выполняется одним из способов:

— Через интерфейс управления устройством BMC или VGA — при использовании ПАК NGFW MNGT.

— Через консоль управления виртуальной машины — при использовании виртуализированной системы управления.

Внимание! Перед использованием виртуализированной системы управления разверните его на платформе виртуализации согласно инструкции (см. раздел 4.2).

В этом разделе

Настройка интерфейса управления (MGMT) (см. раздел 5.2.1)

Настройка синхронизации времени с NTP-сервером (см. раздел 5.2.2)

Настройка IP-адреса сетевого интерфейса узла системы управления для возможности загрузки обновлений на межсетевые экраны (см. раздел 5.2.3)

Настройка сборщиков журналов (см. раздел 5.2.4)

См. также

Развертывание системы управления (см. раздел 4.2)

5.2.1. Настройка интерфейса управления (MGMT)

Вход в учетную запись

► Чтобы войти в учетную запись ОС:

1. Подключитесь к консоли управления виртуальной машины.
2. Введите логин `ngfw` и пароль `p0sitive`.

Перед началом настройки

Настройка интерфейса управления осуществляется через подсистему systemd.

```
ngfw@ngfw-1: ~
 GNU nano 5.4                                    /etc/network/interfaces
#   ################
#   # ! ВНИМАНИЕ ! #
#   # ! WARNING  ! #
#   ################
#
# Данная система использует службу systemd-networkd
# This system using systemd-networkd service
#
# Пожалуйста редактируйте файлы ".network" в каталоге:
# Please edit ".network" files in:
#
#   /etc/systemd/network/
#
# Настройка через данный файл также работает, но в любом случае требуется
#   отключение службы:
# Setting up through this file also works, but in any case you need
#   service disable:
#
#  sudo systemctl disable --now systemd-networkd
#
```

Рисунок 50. Справочная информация в файле `/etc/network/interfaces`

В первую очередь необходимо определить интерфейс, который будет взаимодействовать с сетью, а также проверить наличие необходимых файлов.

- Чтобы подготовить систему к настройке:

  1. Выполните команду `ip a` для определения интерфейса, который будет взаимодействовать с сетью.

```
ngfw@ngfw:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: mgmt1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:84:3d:be brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.103/24 brd 192.168.1.255 scope global dynamic mgmt1
       valid_lft 25164sec preferred_lft 25164sec
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:e2:d8:91:48 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

Рисунок 51. Пример вывода команды `ip a`

Примечание. В выводе команды выше это интерфейс `mgmt1`. Далее он будет использоваться в качестве примера.

2. Выполните команду `ls -la /etc/systemd/network` для проверки наличия файлов `10-mgmt1.link` и `10-mgmt1.network`.

```
ngfw@ngfw:~$ ls -la /etc/systemd/network
total 16
drwxr-xr-x 2 root root 4096 Nov 21 10:46 .
drwxr-xr-x 6 root root 4096 Nov 20 14:37 ..
-rw-r--r-- 1 root root   49 Nov 21 10:46 10-mgmt1.link
-rw-r--r-- 1 root root  252 Nov 21 10:46 10-mgmt1.network
```

Рисунок 52. Пример вывода команды с файлами `10-mgmt1`

```
ngfw@ngfw:/etc/systemd/network$ ls
50-default-dhcp.network
```

Рисунок 53. Пример вывода команды без файлов `10-mgmt1`

3. В зависимости от результатов проверки настройте интерфейс управления по одной из инструкций ниже.

Настройка интерфейса при наличии файлов 10-mgmt1

- Чтобы настроить интерфейс управления:

1. Откройте файл `10-mgmt1.network`:
   ```
   sudo nano /etc/systemd/network/10-mgmt1.network
   ```
2. Измените параметры интерфейса управления `mgmt1`:
   ```
   [Match]
   Name=mgmt1


   [Network]
   # For autoconfig
   # Для автонастройки
   #DHCP=yes
   # Пример статической конфигурации:
   # Static config example:
   #
   Address=10.10.18.3/24
   Gateway=10.10.18.254
   DNS=10.10.22.31
   DNS=10.10.22.21
   ```

Примечание. Адрес указанного DNS-сервера (серверов) используется базовой операционной системой и не влияет на разрешение FQDN в политиках безопасности процессом PT NGFW.

3. Узнайте PCI-адрес устройства с помощью команды `lspci -D | grep -i eth`.

   Примечание. В выводе команды необходимо обратить внимание на первый адрес в списке. Например, `0000:03:00.0`.

4. Откройте файл `10-mgmt1.link`:

   ```
   sudo nano /etc/systemd/network/10-mgmt1.link
   ```

   В файле должны быть указаны корректные PCI-адрес и название интерфейса, например:

   ```
   [Match]
   Path=pci-0000:03:00.0


   [Link]
   Name=mgmt1
   ```

5. Перезапустите сервис, чтобы изменения вступили в силу:

   ```
   sudo systemctl restart systemd-networkd
   ```

Настройка интерфейса при отсутствии файлов 10-mgmt1

- Чтобы настроить интерфейс управления:

  1. Создайте и откройте файл `10-mgmt1.network`:

     ```
     sudo nano /etc/systemd/network/10-mgmt1.network
     ```

  2. Измените параметры интерфейса управления `mgmt1`:

     ```
     [Match]
     Name=mgmt1


     [Network]
     # For autoconfig
     # Для автонастройки
     #DHCP=yes
     # Пример статической конфигурации:
     # Static config example:
     #
     Address=10.10.18.3/24
     Gateway=10.10.18.254
     DNS=10.10.22.31
     DNS=10.10.22.21
     ```

  3. Узнайте PCI-адрес устройства с помощью команды `lspci -D | grep -i eth`.

     Примечание. В выводе команды необходимо обратить внимание на первый адрес в списке. Например, `0000:03:00.0`.

4. Создайте и откройте файл `10-mgmt1.link`:
   ```
   sudo nano /etc/systemd/network/10-mgmt1.link
   ```
5. Внесите в него изменения, указав PCI-адрес из предыдущего шага и название интерфейса, например:
   ```
   [Match]
   Path=pci-0000:03:00.0


   [Link]
   Name=mgmt1
   ```
6. Удалите остальные файлы из каталога `/etc/systemd/network` при их наличии, например:
   ```
   sudo rm /etc/systemd/network/50-default-dhcp.network
   ```
7. Перезагрузите устройство, чтобы изменения вступили в силу:
   ```
   sudo reboot
   ```

5.2.2. Настройка синхронизации времени с NTP-сервером

Для корректной работы систем журналирования и мониторинга необходимо синхронизировать время. Для этого используются NTP-серверы.

- Чтобы настроить синхронизацию времени с NTP-сервером:

1. Откройте конфигурационный файл `timesyncd.conf`:
   ```
   sudo nano /etc/systemd/timesyncd.conf
   ```
2. Раскомментируйте строку `NTP` и введите адрес NTP-сервера по своему усмотрению.

```
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See timesyncd.conf(5) for details.

[Time]
NTP=ntp.test.ru
#FallbackNTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
#RootDistanceMaxSec=5
#PollIntervalMinSec=32
#PollIntervalMaxSec=2048
```

Рисунок 54. Содержимое файла `timesyncd.conf`

3. Перезапустите сервис, чтобы изменения вступили в силу:
   ```
   sudo systemctl restart systemd-timesyncd
   ```

Вы можете проверить работоспособность службы с помощью команды:

```
timedatectl timesync-status
```

5.2.3. Настройка IP-адреса сетевого интерфейса узла системы управления для возможности загрузки обновлений на межсетевые экраны

- Чтобы настроить IP-адрес сетевого интерфейса узла системы управления для возможности загрузки обновлений на межсетевые экраны:

  1. Откройте для редактирования конфигурационный файл `config.toml`:

     ```
     sudo nano /opt/pt-ngfw/ngfw-ms-backend/config/config.toml
     ```

  2. Задайте значение `externalAddress`:

     ```
     ...
     [server]
     skipAuth = false
     maxLoginAttempts = 4
     externalAddress = "10.10.10.1:6090"
     ...
     ```

  3. Перезапустите службу pt-ngfw-ms-backend.

     ```
     sudo systemctl restart pt-ngfw-ms-backend
     ```

  4. Нажмите **Отправить на устройства**, чтобы изменения вступили в силу.

5.2.4. Настройка сборщиков журналов

Настройка сборщиков журналов осуществляется в пользовательском интерфейсе системы управления PT NGFW. Подробнее см. в разделе «Настройка сборщиков журналов (см. раздел 39.1)».

См. также

Настройка сборщиков журналов (см. раздел 39.1)

5.3. Настройка межсетевого экрана

Для настройки межсетевого экрана PT NGFW подключитесь к нему и выполните вход в ОС, используя логин `ngfw` и пароль `p0sitive`. Подключение выполняется одним из способов:

— Ко всем исполнениям на базе аппаратных платформ — через интерфейс Serial Console с параметрами 115200 8n1.

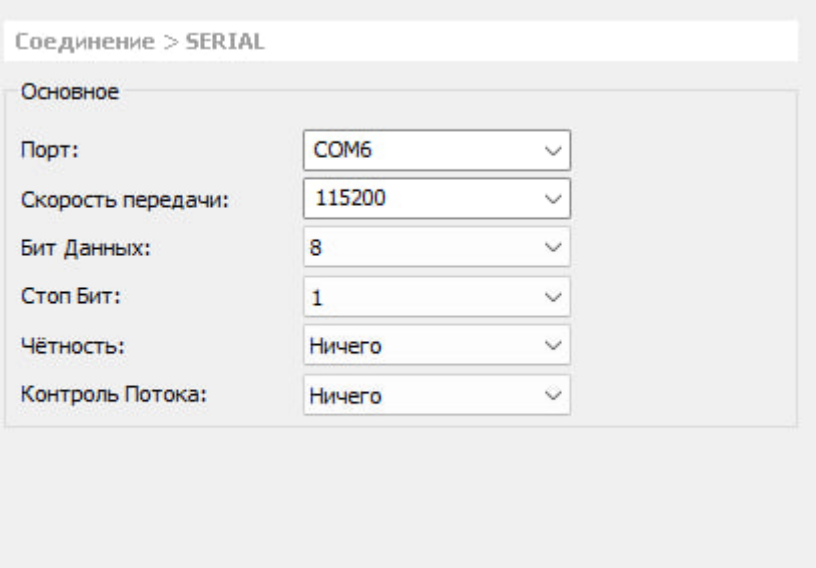


Рисунок 55. Пример подключения через Serial Console

— К виртуальному исполнению PT NGFW — через консоль управления виртуальной машины.

  Внимание! Перед использованием виртуального исполнения PT NGFW разверните его на платформе виртуализации согласно инструкции (см. раздел 4.3).

— К исполнениям на базе аппаратных платформ PT NGFW 1005, 1010, 1020, 1050 — с помощью SSH-клиента через интерфейсы управления (сетевой порт № 5 на модели PT NGFW 1005, порт № 8 на модели PT NGFW 1010 и сетевой порт № 1 на моделях PT NGFW 1050 и PT NGFW 1020). На этих портах по умолчанию настроен DHCP-клиент.

— К исполнениям на базе аппаратных платформ PT NGFW 2010, 2020, 2050, 3010, 3040, 3050 — с помощью SSH-клиента через интерфейсы управления (сетевые порты №1 или №2 в отсеке OCP0_1 или через интерфейс BMC).

Если ваш PT NGFW работает под управлением ОС Astra Linux, то при авторизации в поле **Integrity Level** (уровень доступа) укажите значение 63.

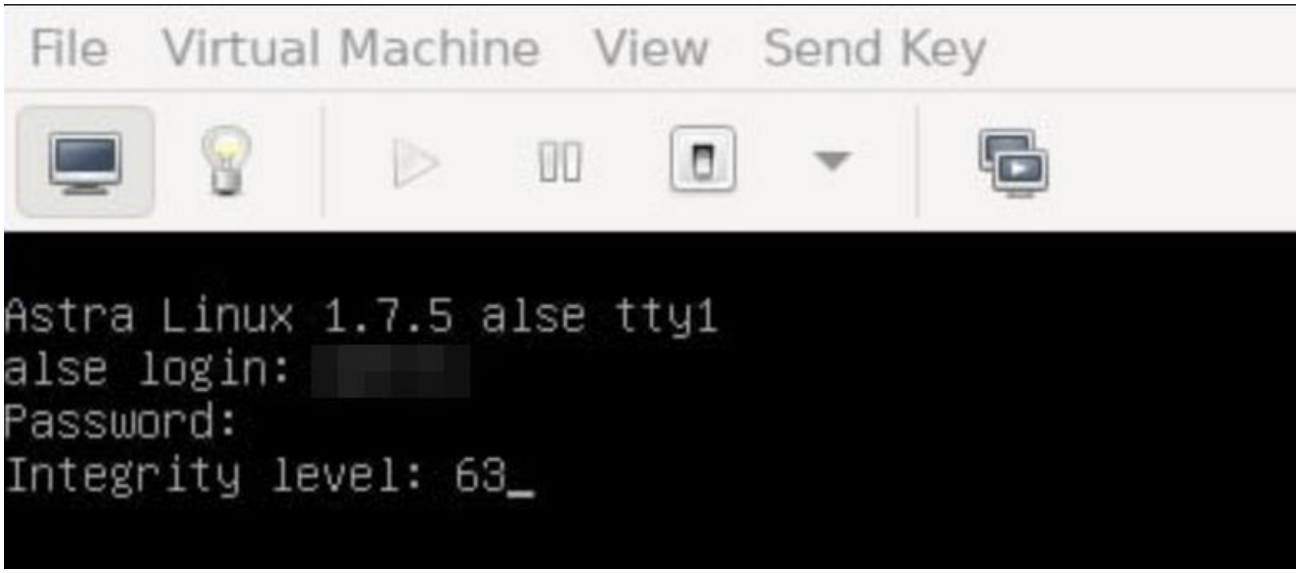


Рисунок 56. Ввод значения **Integrity level**

Примечание. Драйвер для комплектного кабеля можно скачать по ссылке.

В этом разделе

Изменение имени хоста (hostname) (см. раздел 5.3.1)

Настройка интерфейса управления (MGMT) (см. раздел 5.3.2)

Подключение межсетевого экрана к DNS-серверу (серверам) для разрешения FQDN в политиках безопасности (см. раздел 5.3.3)

Настройка синхронизации времени с NTP-сервером (см. раздел 5.3.4)

Подключение межсетевого экрана к системе управления (см. раздел 5.3.5)

Первичная настройка интерфейсов (см. раздел 5.3.6)

5.3.1. Изменение имени хоста (hostname)

При необходимости вы можете изменить имя хоста.

> **Внимание!** При создании кластера из двух межсетевых экранов (см. раздел 30.11) убедитесь, что имена хостов этих устройств не совпадают.

Чтобы изменить имя хоста:

1. Если требуется, проверьте текущее имя хоста с помощью команды `hostnamectl`.
2. Задайте новое имя хоста с помощью команды:
   ```
   sudo hostnamectl set-hostname <Новое имя хоста>
   ```
3. Обновите строку с именем хоста в файле `/etc/hosts`:

- Откройте файл в любом текстовом редакторе (например, nano):
  `sudo nano /etc/hosts`
- В строке `hostname` замените текущее имя хоста на новое.
- Сохраните изменения.

4. Выполните команду `hostnamectl` для проверки изменений.

5.3.2. Настройка интерфейса управления (MGMT)

► Чтобы настроить интерфейс управления:

1. Подключитесь к консоли управления виртуальной машины.
2. Введите логин `ngfw` и пароль `p0sitive`.

   Настройка интерфейса управления осуществляется через подсистему systemd.

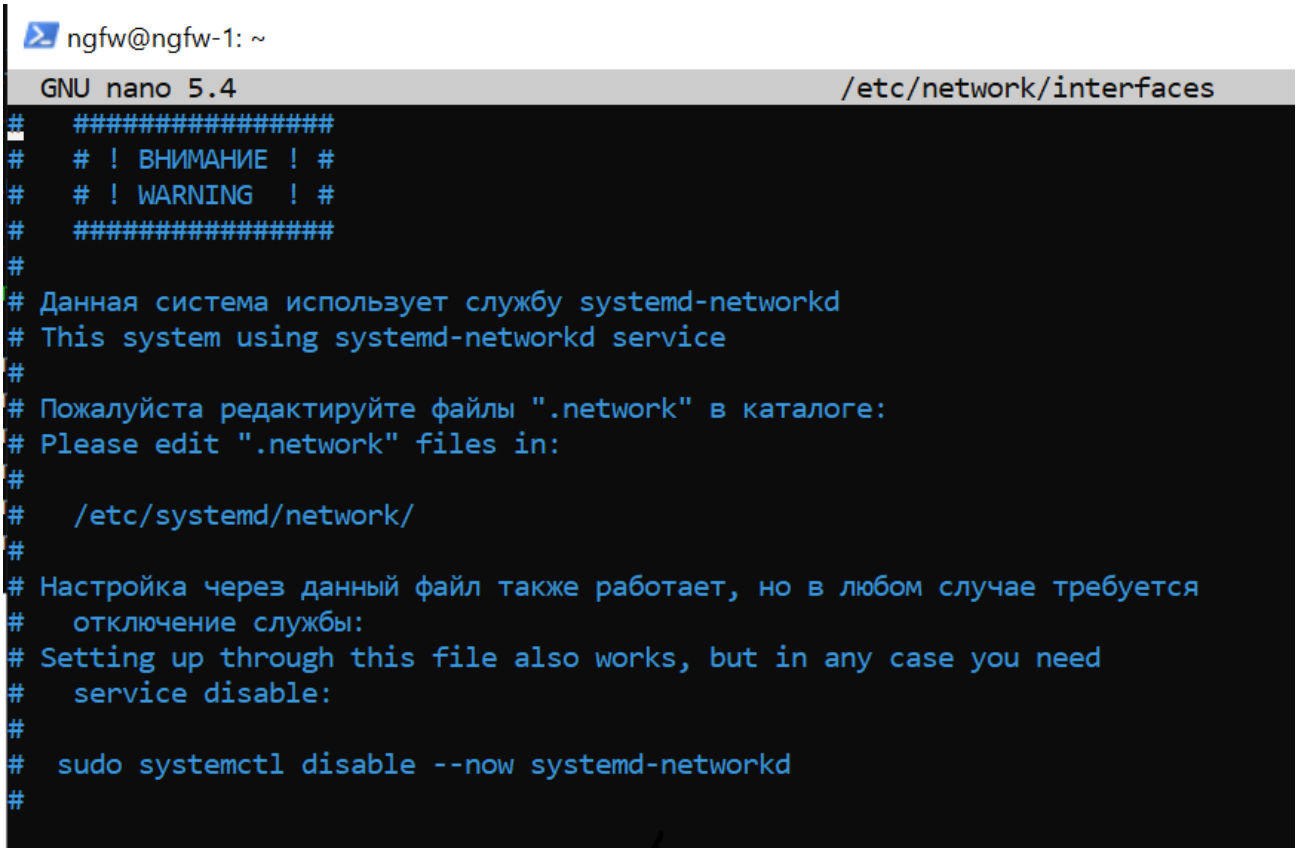


Рисунок 57. Справочная информация в файле `/etc/network/interfaces`

3. Откройте файл `10-mgmt1.network`:
   `sudo nano /etc/systemd/network/10-mgmt1.network`
4. Измените параметры интерфейса управления `mgmt1`:

```
[Match]
Name=mgmt1


[Network]
# For autoconfig
# Для автонастройки
#DHCP=yes
# Пример статической конфигурации:
# Static config example:
#
Address=10.10.18.3/24
Gateway=10.10.18.254
DNS=10.10.22.31
DNS=10.10.22.21
```

Примечание. Адрес указанного DNS-сервера (серверов) используется базовой операционной системой и не влияет на разрешение FQDN в политиках безопасности процессом PT NGFW.

5. Перезапустите сервис, чтобы изменения вступили в силу:
   ```
   sudo systemctl restart systemd-networkd
   ```

5.3.3. Подключение межсетевого экрана к DNS-серверу (серверам) для разрешения FQDN в политиках безопасности

- Чтобы подключить межсетевой экран к DNS-серверу (серверам):

1. В конфигурационном файле `pt-ngfw.conf` в блоке `dns_resolver` укажите параметр `servers`:
   ```
   sudo nano /opt/pt-ngfw/ngfw-core/etc/config/pt-ngfw.conf
   ```

   Примечание. Если DNS-серверов несколько, их адреса вводятся через запятую без пробелов.

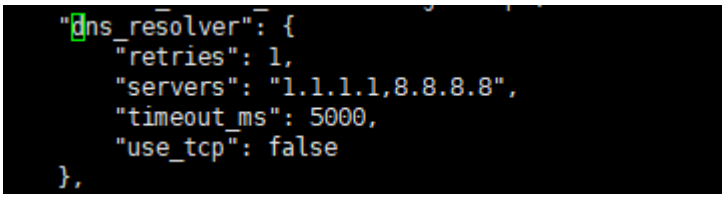


Рисунок 58. Содержимое файла `pt-ngfw.conf`

2. Перезапустите сервис, чтобы изменения вступили в силу:
   ```
   sudo systemctl restart pt-ngfw-core.service
   ```

5.3.4. Настройка синхронизации времени с NTP-сервером

Для корректной работы систем журналирования и мониторинга необходимо синхронизировать время. Для этого используются NTP-серверы.

- Чтобы настроить синхронизацию времени с NTP-сервером:

  1. Откройте конфигурационный файл `timesyncd.conf`:
     ```
     sudo nano /etc/systemd/timesyncd.conf
     ```
  2. Раскомментируйте строку `NTP` и введите адрес NTP-сервера по своему усмотрению.

```
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See timesyncd.conf(5) for details.

[Time]
NTP=ntp.test.ru
#FallbackNTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
#RootDistanceMaxSec=5
#PollIntervalMinSec=32
#PollIntervalMaxSec=2048
```

Рисунок 59. Содержимое файла `timesyncd.conf`

  3. Перезапустите сервис, чтобы изменения вступили в силу:
     ```
     sudo systemctl restart systemd-timesyncd
     ```
     Вы можете проверить работоспособность службы с помощью команды:
     ```
     timedatectl timesync-status
     ```

5.3.5. Подключение межсетевого экрана к системе управления

- Чтобы подключить межсетевой экран к системе управления:

  1. Подключитесь к веб-интерфейсу системы управления, используя логин `admin` и пароль `admin`.

     При первом входе в систему потребуется сменить пароль.
  2. На странице **Devices** нажмите **Add device**.

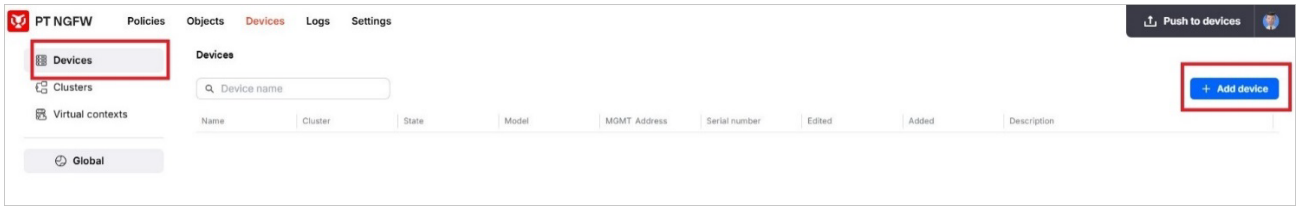


Рисунок 60. Добавление устройств

3. Введите серийный номер устройства.
4. Введите IP-адрес интерфейса управления устройства или FQDN.

   Примечание. Разрешение FQDN происходит в соответствии с системными параметрами ОС.

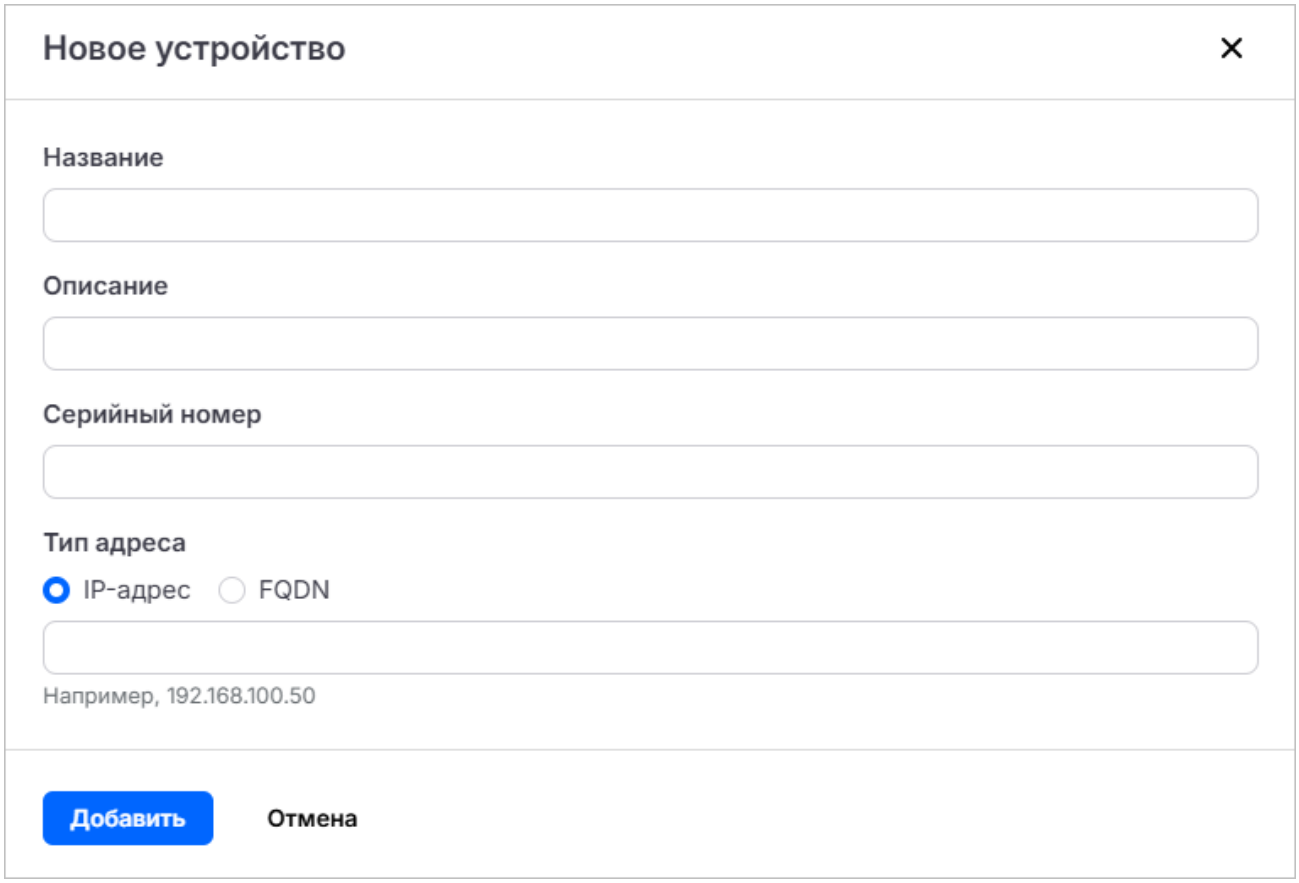


Рисунок 61. IP-адрес и серийный номер межсетевого экрана

5. Нажмите **Push to devices**, чтобы изменения вступили в силу.

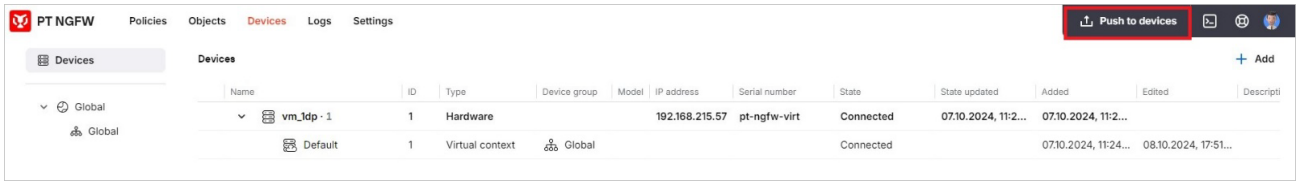


Рисунок 62. Завершение подключения межсетевого экрана к системе управления

5.3.6. Первичная настройка интерфейсов

- Чтобы произвести первичную настройку интерфейсов:

1. Подключитесь к веб-интерфейсу системы управления.
2. На странице **Devices** выберите подключенное устройство.
3. В контекстном меню нужного сабинтерфейса нажмите **Edit**.

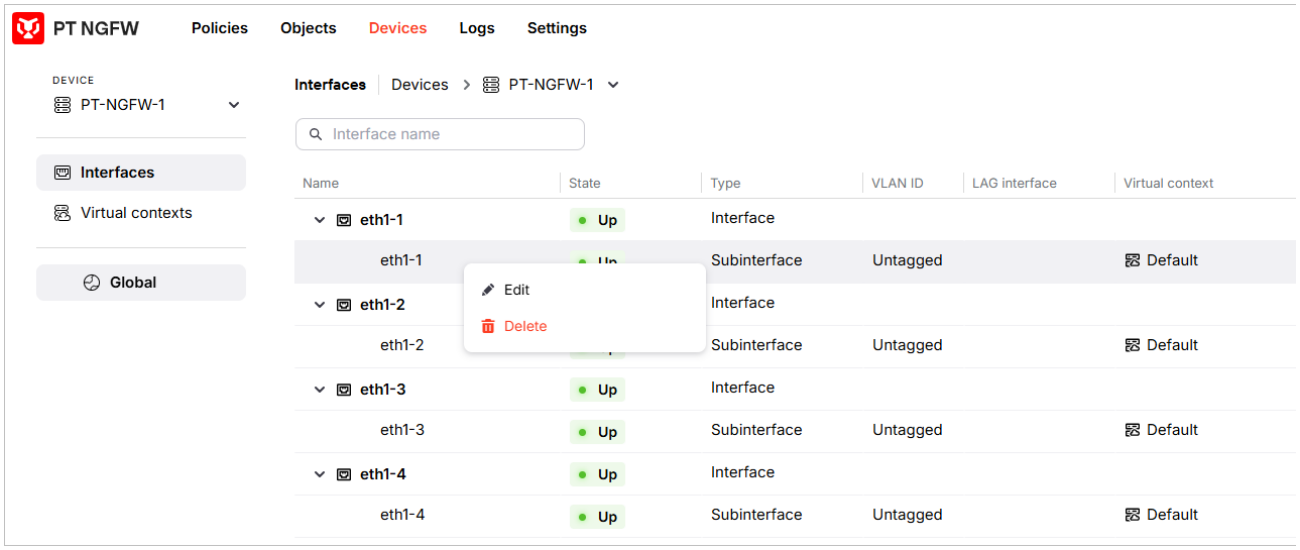


Рисунок 63. Выбор сабинтерфейса

4. Укажите обязательные параметры сабинтерфейса: **Mode**, **IP address**, **Virtual context** и **Security zone**.

   Примечание. Зона безопасности **Local** является служебной и не предусмотрена для назначения сабинтерфейсам.

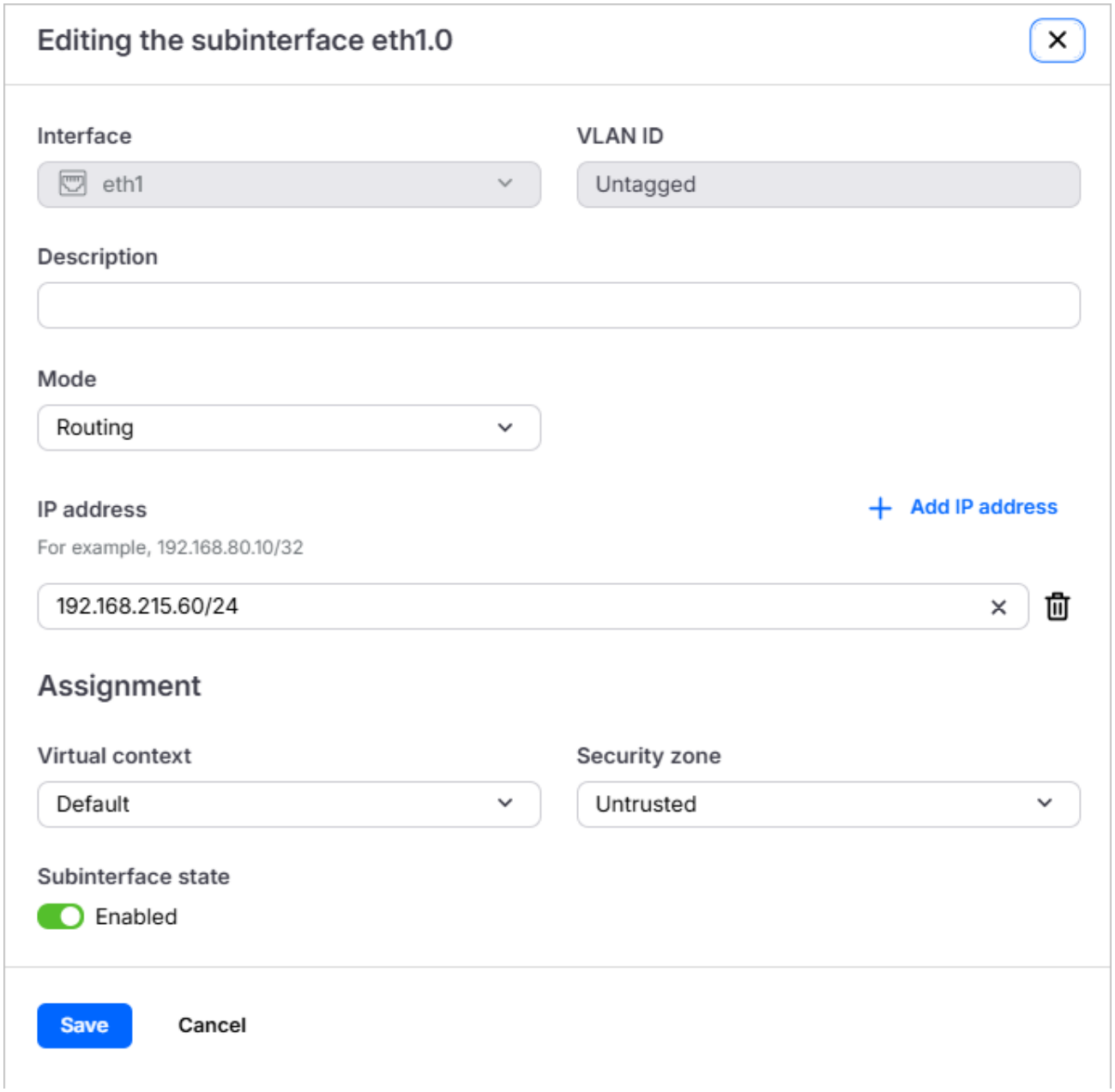


Рисунок 64. Параметры сабинтерфейса

5. Нажмите **Push to devices**, чтобы изменения вступили в силу.

5.4. Настройка системы мониторинга

Внимание! Перед использованием системы мониторинга разверните ее на платформе виртуализации согласно инструкции (см. раздел 4.4).

Настройка системы мониторинга состоит из двух этапов — настройки сервера СУБД и визуализации и настройки клиента.

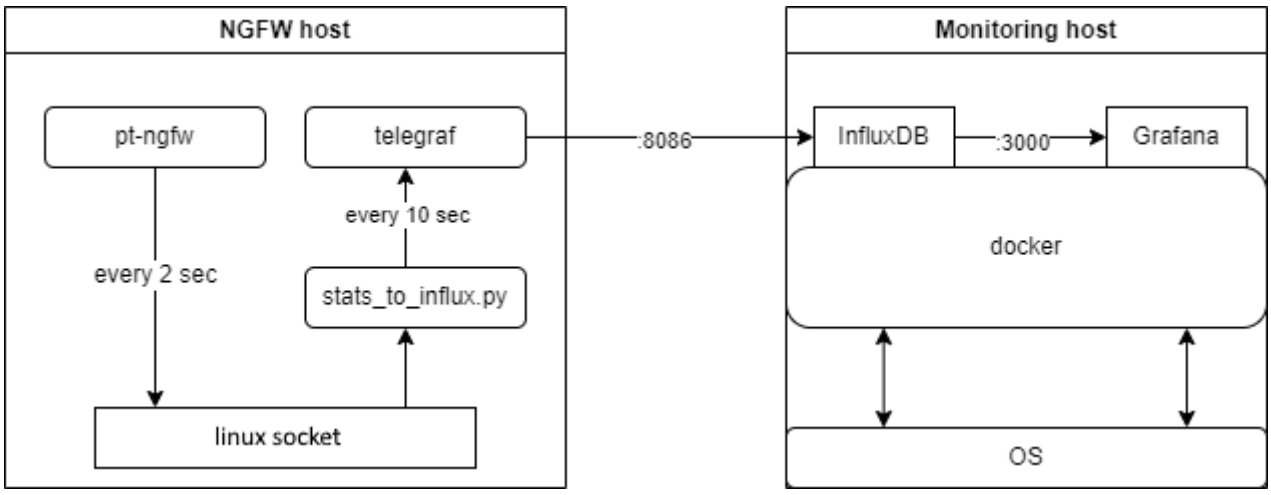


Рисунок 65. Схема взаимодействия межсетевого экрана и системы мониторинга

Внимание! Сначала необходимо настроить сервер СУБД и визуализацию, а затем клиент.

В этом разделе

Настройка сервера СУБД и визуализации (см. раздел 5.4.1)

Установка и настройка клиента (см. раздел 5.4.2)

5.4.1. Настройка сервера СУБД и визуализации

- Чтобы настроить сервер СУБД и визуализацию:

1. Выполните вход в веб-интерфейс Grafana по адресу `http://<IP-адрес сервера Grafana>:3000`, используя логин `admin` и пароль `p0sitive`.

   Примечание. В начале адреса используется `http`, а не `https`.

2. Если в системе уже есть источник данных, удалите его:
   - Перейдите в раздел **Connections** → **Data Sources**.
   - Нажмите **Explore** напротив источника, который хотите удалить.

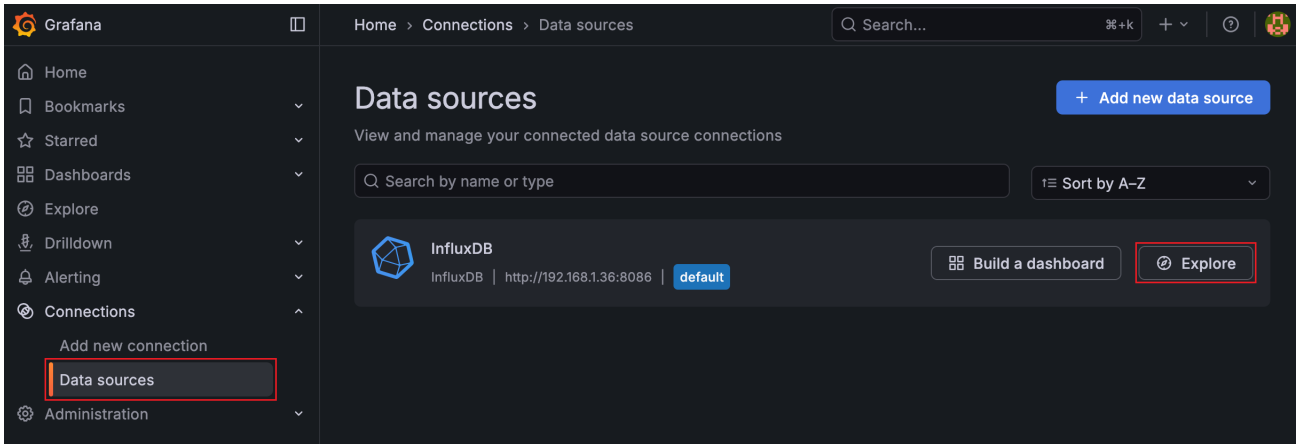


Рисунок 66. Страница **Data sources**

- Нажмите **Delete**.

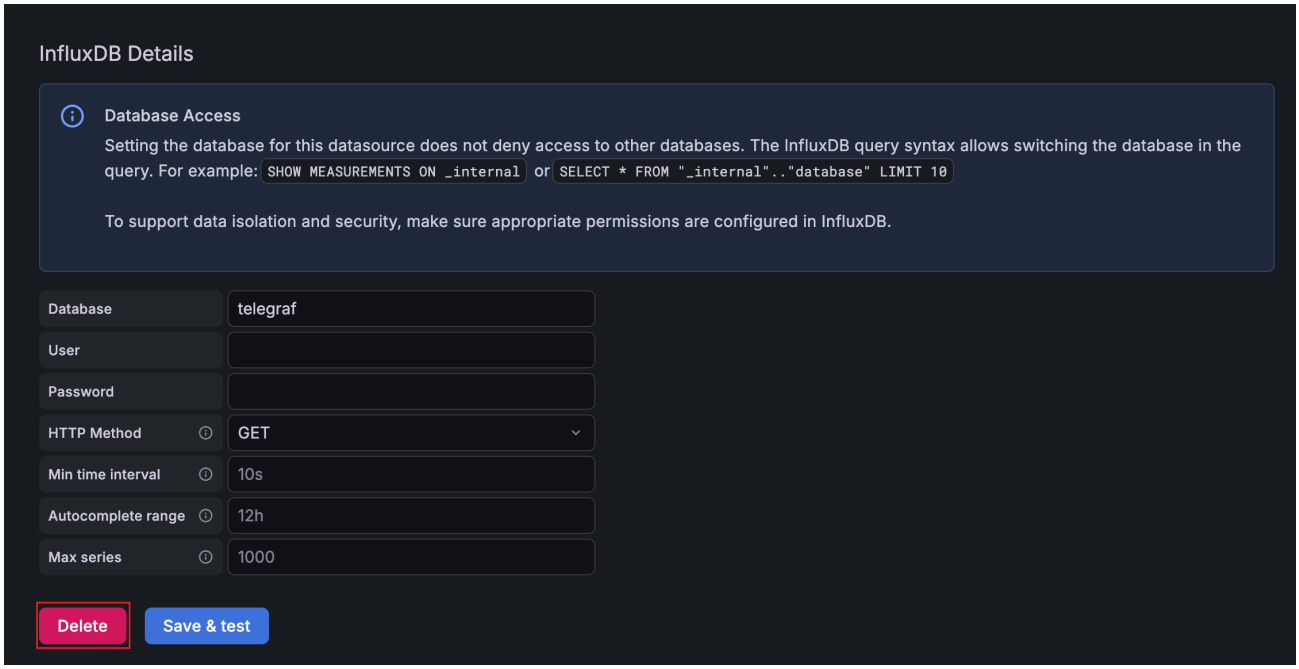


Рисунок 67. Удаление источника данных

3. Подключите источник данных InfluxDB:
   - Перейдите в раздел **Connections** → **Data Sources**.
   - Нажмите **Add data source**.

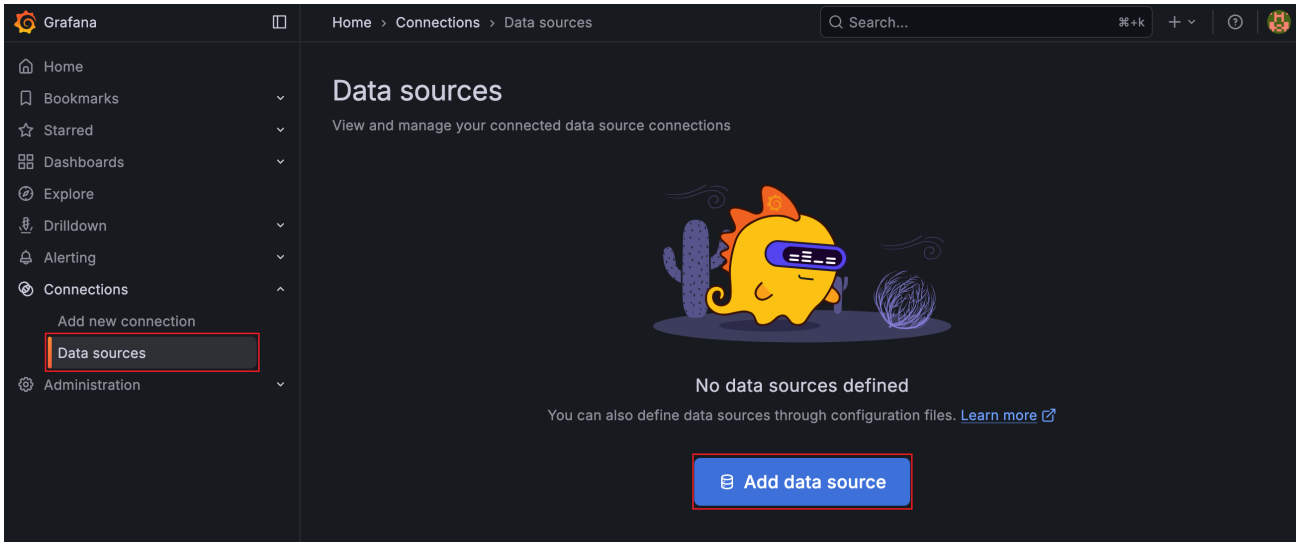


Рисунок 68. Добавление источника данных

- Выберите **InfluxDB**.

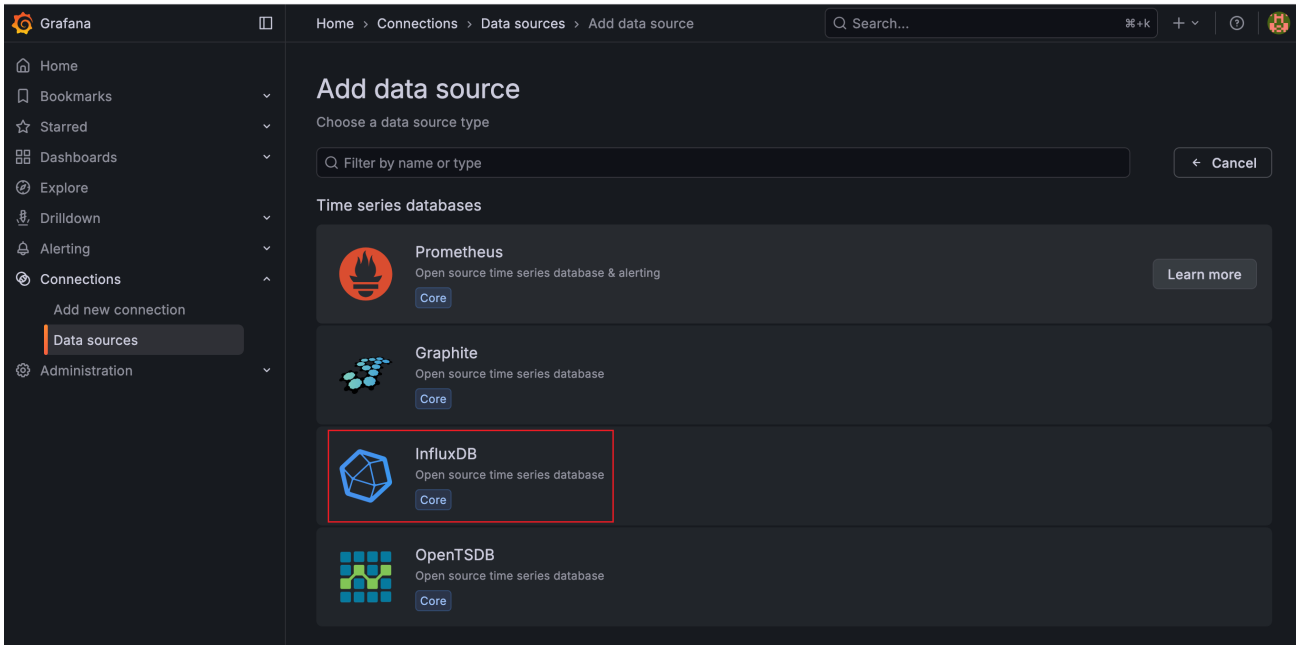


Рисунок 69. Выбор типа источника данных InfluxDB

- Введите имя базы данных.

  Примечание. В примере используется имя `InfluxDB-1`.

- Включите параметр **Default**, чтобы сделать этот источник данных по умолчанию.
- В поле URL введите `http://<IP-адрес сервера Grafana>:8086`.

  Примечание. В начале адреса используется `http`, а не `https`.

- Включите параметр **Basic Auth**.
- В поле **User** введите логин, в поле **Password** введите пароль.

  Примечание. Данные должны совпадать с логином и паролем, вводимыми при настройке клиента (см. раздел 5.4.2).

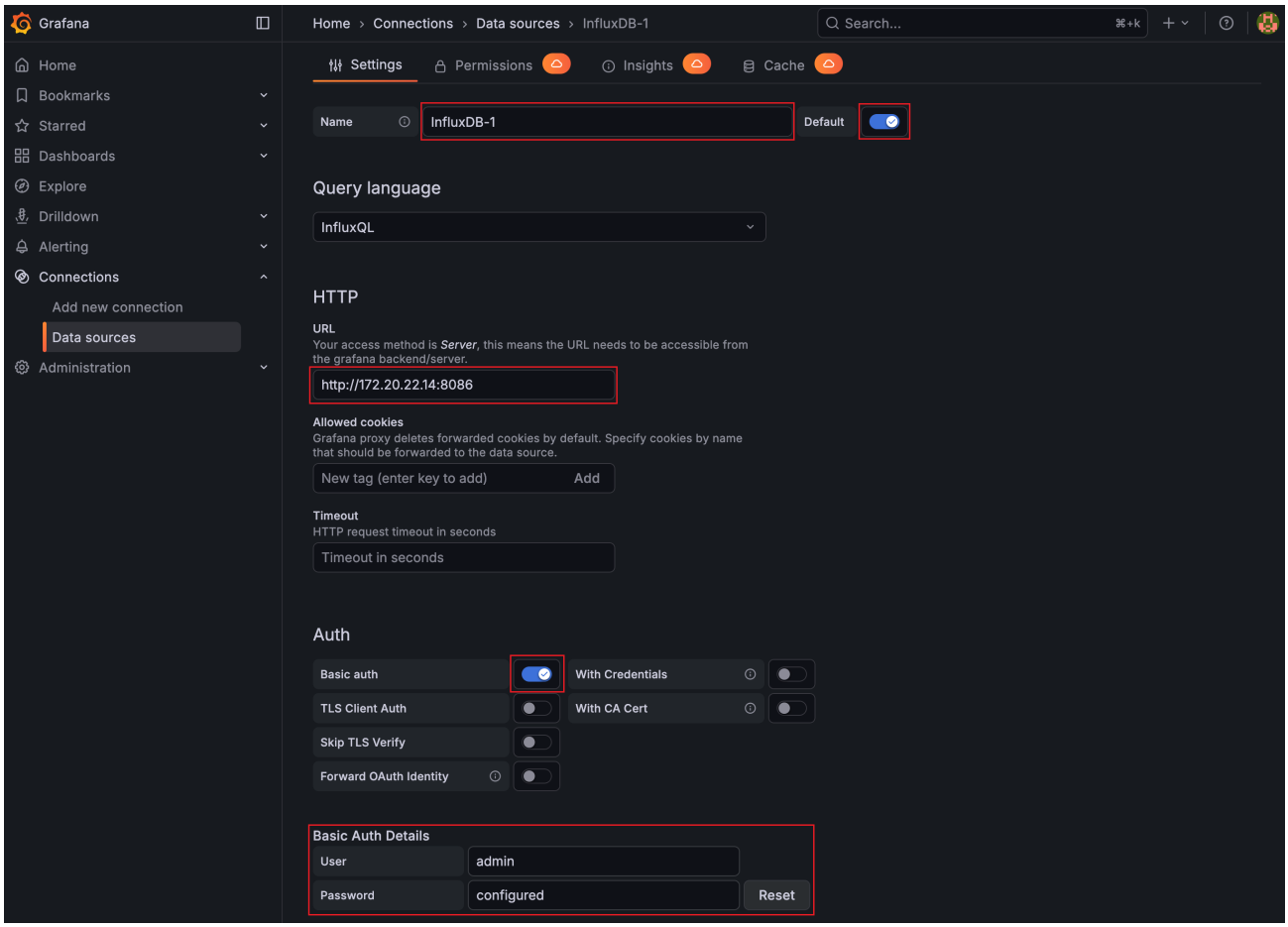


Рисунок 70. Настройка параметров источника данных

- В поле **Database** введите имя базы данных.

  Примечание. В примере используется имя `telegraf`.
- Для параметра **HTTP Method** выберите значение **GET**.
- Для параметра **Min time interval** задайте значение `10`.
- Для параметра **Max series** задайте значение `10000`.

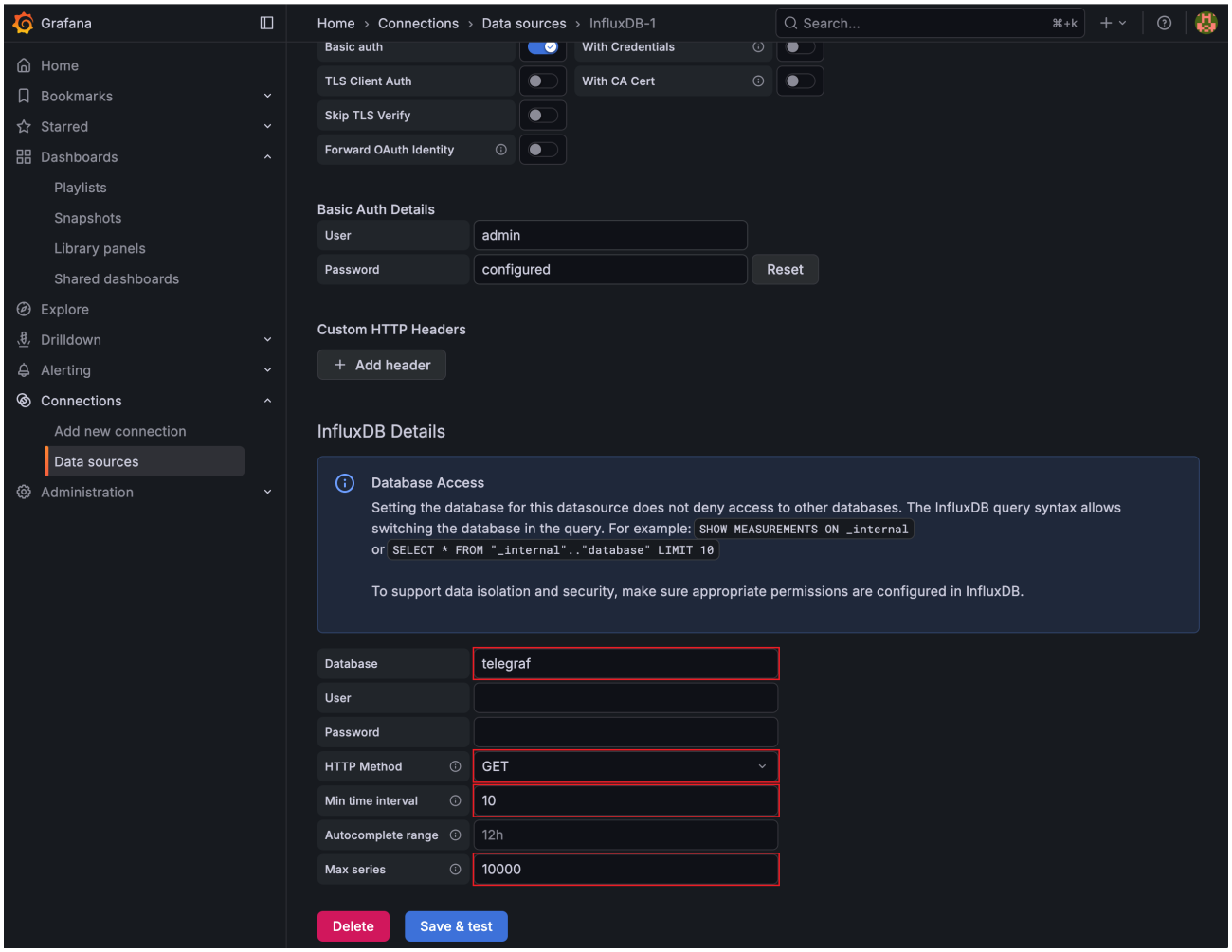


Рисунок 71. Настройка параметров базы данных

4. Нажмите **Save & Test** для сохранения параметров и проверки успешного подключения к БД.

   Примечание. При успешной настройке отобразится оповещение с текстом **datasource is working**.

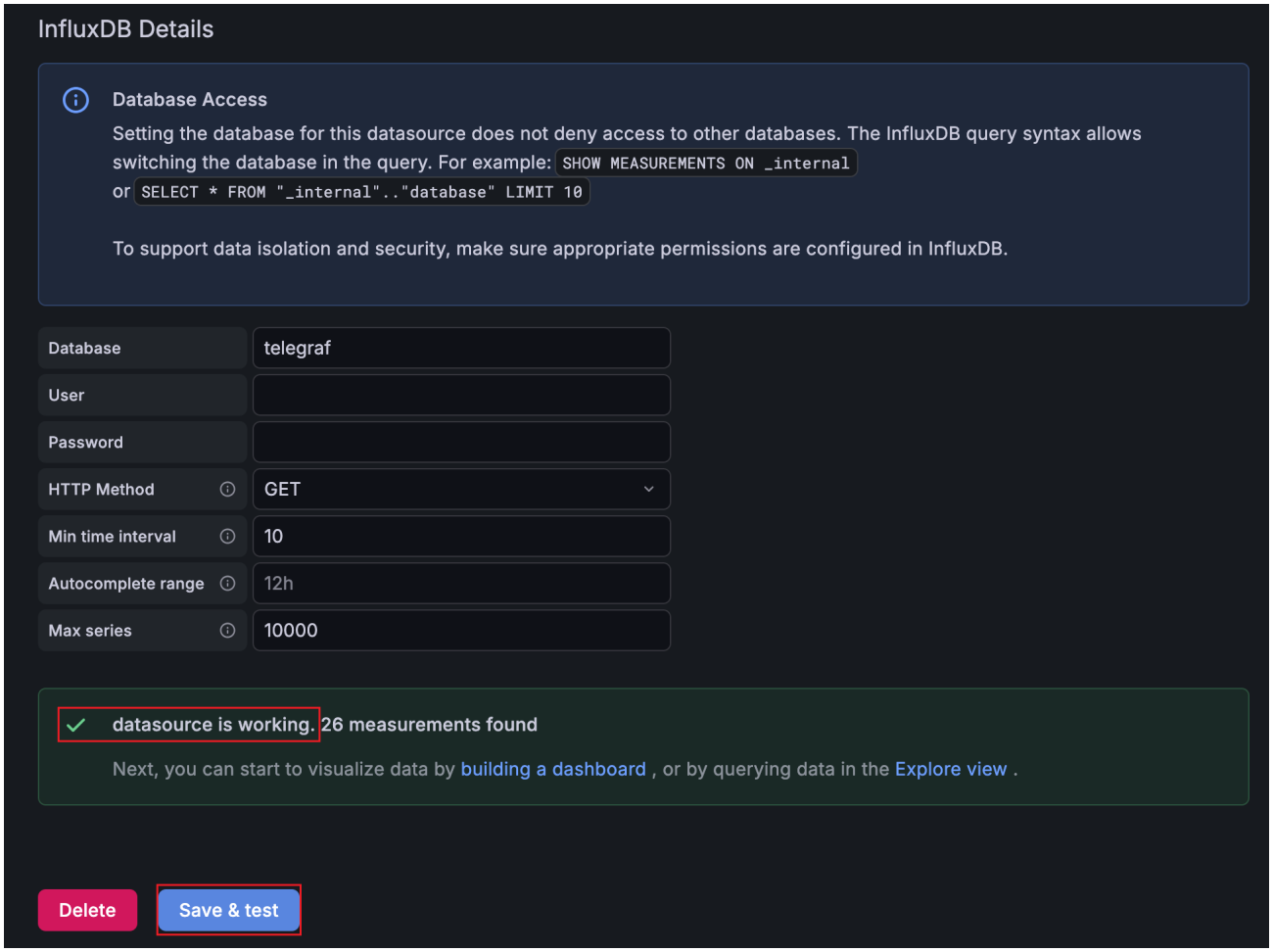


Рисунок 72. Сохранение параметров и проверка успешного подключения к БД

5. Удалите устаревшие дашборды, если они есть:
   - Перейдите в раздел **Dashboards**.
   - Установите флажки напротив всех дашбордов.
   - Нажмите **Delete**.

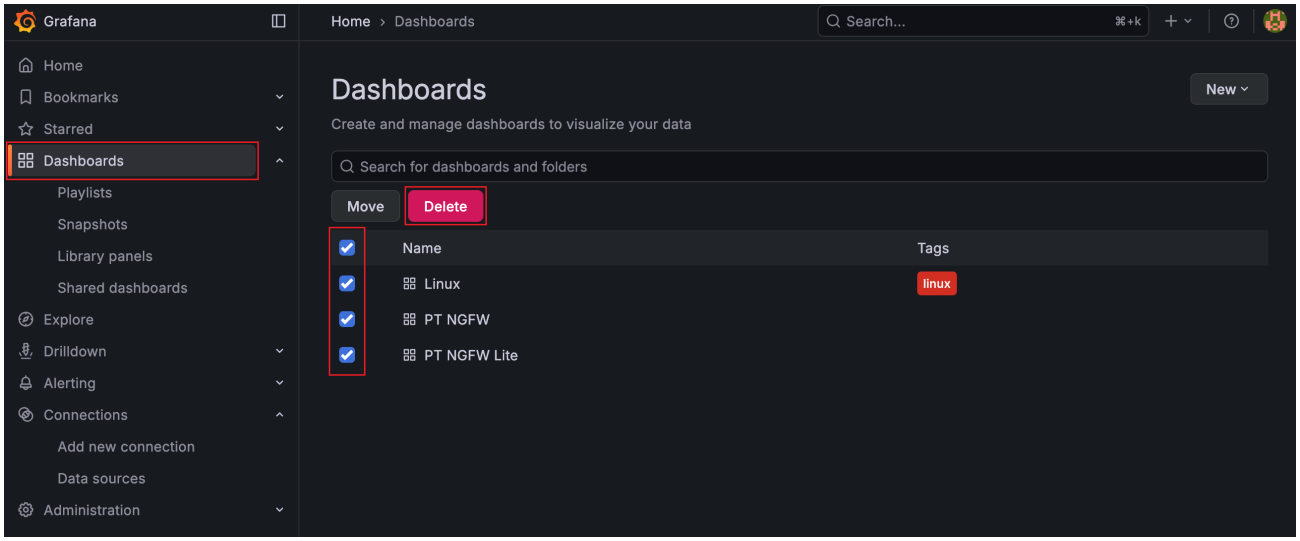


Рисунок 73. Удаление устаревших дашбордов

6. Скачайте архив с дашбодами по метрикам ОС и PT NGFW.

   В архиве содержатся следующие дашборды:

   - `linux.json` — дашборд с виджетами по метрикам ОС;
   - `pt-ngfw.json` — дашборд с виджетами по метрикам PT NGFW;
   - `pt-ngfw-lite.json` — облегченный дашборд с виджетами по метрикам (см. раздел 40) PT NGFW.

7. Импортируйте скачанные дашборды в Grafana:

   - Перейдите в раздел **Dashboards**.
   - Нажмите **New** → **Import**.

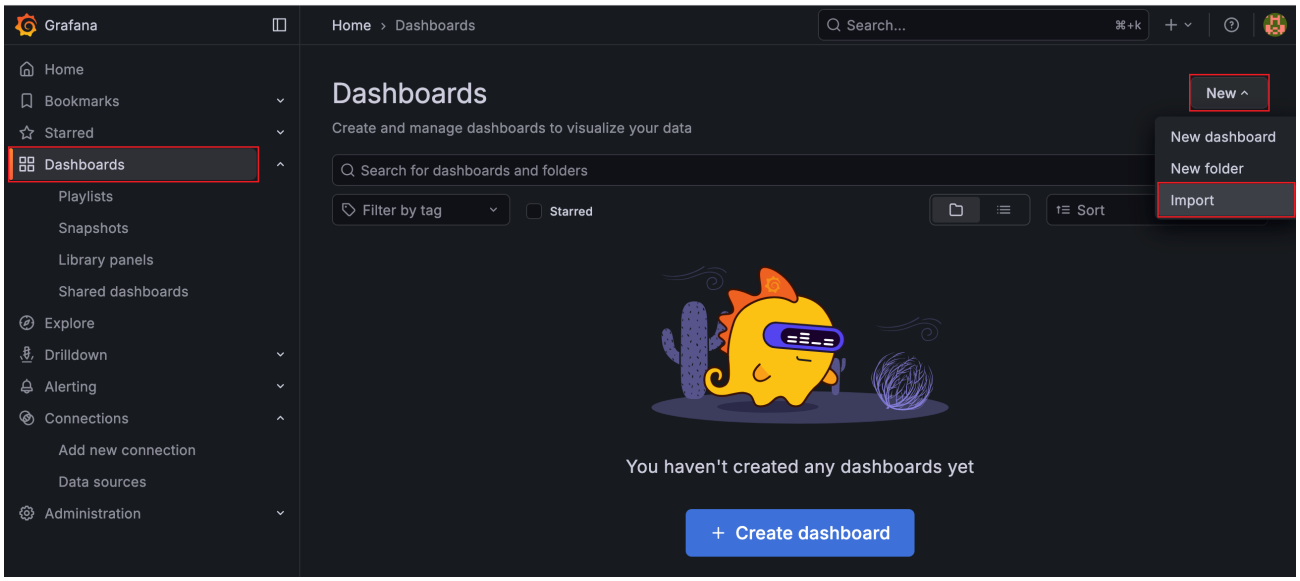


Рисунок 74. Импортирование дашборда

- Перетащите JSON-файл одного из дашбордов в область загрузки.

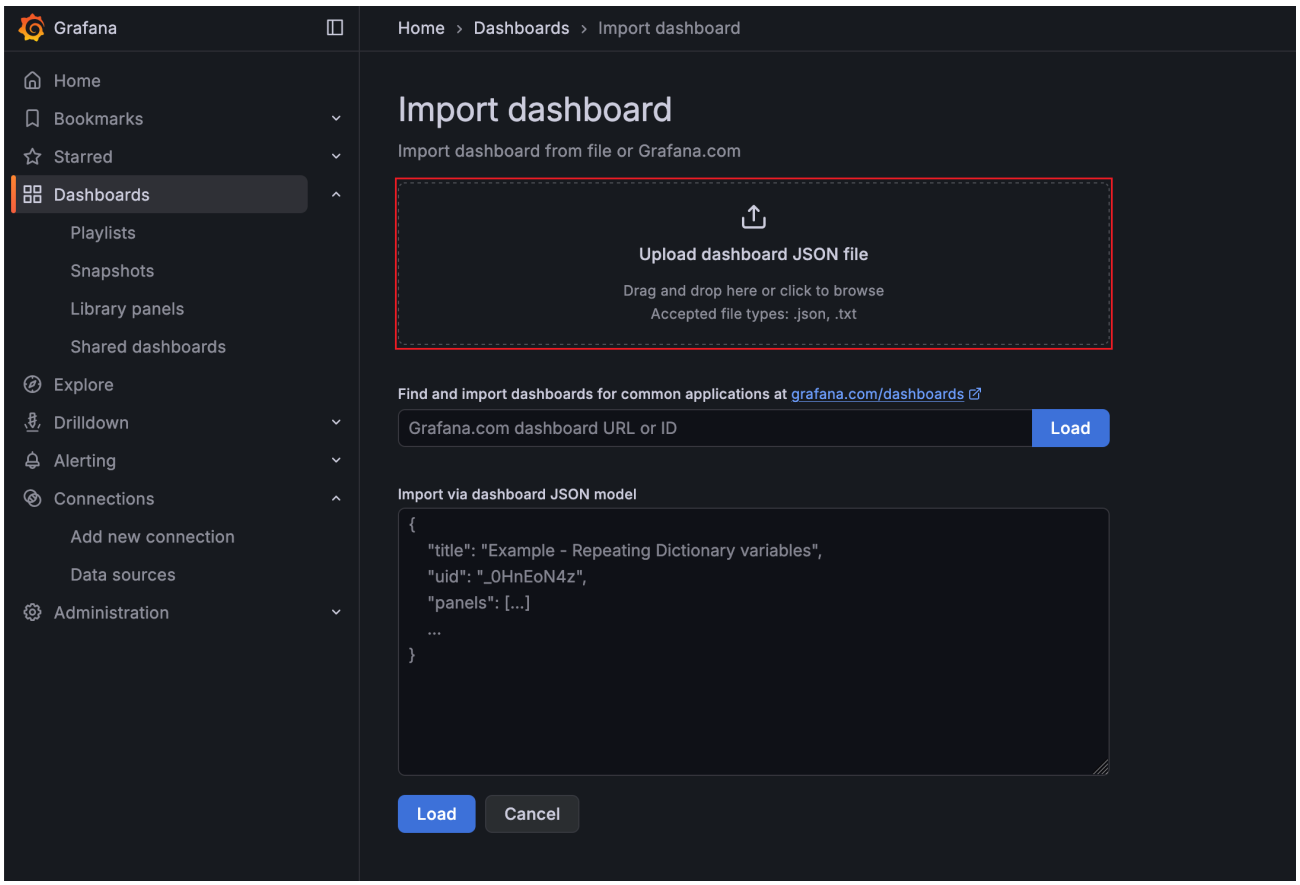


Рисунок 75. Загрузка JSON-файла

- Выберите ранее созданный источник данных (в примере — `InfluxDB-1`).

- Нажмите **Import**.

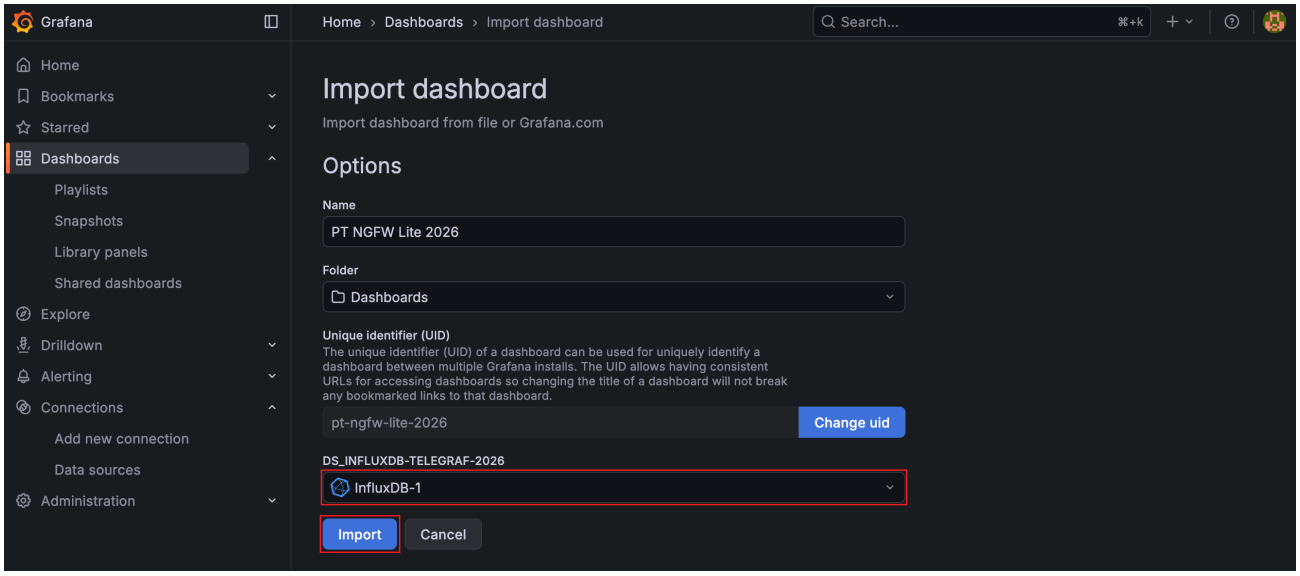


Рисунок 76. Завершение импортирования дашборда

- Повторите процедуру импортирования с остальными JSON-файлами.

Примечание. Ошибка **Database not found** означает, что PT NGFW еще не настроен на отдачу телеметрии, и графики не будут отображаться. Для этого необходимо настроить клиент (см. раздел 5.4.2).

5.4.2. Установка и настройка клиента

Примечание. Ниже в командах и их выводах в качестве примера используется пользователь с именем ngfw.

Перед началом настройки

В первую очередь необходимо проверить, установлен ли Telegraf на узле PT NGFW.

- Чтобы проверить наличие установленного Telegraf:

1. Войдите в командный интерфейс базовой операционной системы узла PT NGFW в качестве пользователя с правами sudo.
2. Введите команду `dpkg --get-selections | grep telegraf`.

   Пример вывода команды, если Telegraf не установлен:

   ```
   ngfw@NGFW1:~$ dpkg --get-selections | grep telegraf
   ngfw@NGFW1:~$
   ```

Пример вывода команды, если Telegraf установлен:

```
ngfw@NGFW1:~$ dpkg --get-selections | grep telegraf
telegraf install
ngfw@NGFW1:~$
```

3. Если Telegraf не установлен, установите его (см. раздел 5.4.2).
4. Если Telegraf установлен, настройте его (см. раздел 5.4.2).

Установка Telegraf

- Чтобы установить Telegraf:

1. Скачайте архив с клиентом для ОС Debian или ОС Astra Linux.
2. Поместите архив `telegraf_offline_debian_11.zip` в домашний каталог пользователя (в этом примере — в каталог `/home/ngfw`) и перейдите в него:

   ```
   ngfw@NGFW1:~$ cd ~
   ```

3. Проверьте наличие файла `telegraf_offline_debian_11.zip`:

   ```
   ngfw@NGFW1:~$ ls -la
   total 3382980
   ...
   -rw-r--r-- 1 ngfw ngfw 72038053 Apr 8 14:08 telegraf_offline_debian_11.zip
   ...
   ```

4. Установите утилиту unzip для распаковки архива, если она не установлена:

   ```
   ngfw@NGFW1:~$
   ngfw@NGFW1:~$ sudo apt-get install unzip
   Reading package lists... Done
   Building dependency tree... Done
   Reading state information... Done
   Suggested packages:
   zip
   The following NEW packages will be installed:
   unzip
   0 upgraded, 1 newly installed, 0 to remove and 20 not upgraded.
   Need to get 172 kB of archives.
   After this operation, 393 kB of additional disk space will be used.
   Get:1 http://deb.debian.org/debian bullseye/main amd64 unzip amd64 6.0-26+deb11u1 [172 kB]
   Fetched 172 kB in 1s (227 kB/s)
   Selecting previously unselected package unzip.
   (Reading database ... 62810 files and directories currently installed.)
   Preparing to unpack .../unzip_6.0-26+deb11u1_amd64.deb ...
   Unpacking unzip (6.0-26+deb11u1) ...
   Setting up unzip (6.0-26+deb11u1) ...
   Processing triggers for mailcap (3.69) ...
   Processing triggers for man-db (2.9.4-2) ...
   ngfw@NGFW1:~$
   ```

5. Распакуйте архив в локальный каталог:

```
ngfw@NGFW1:~$ unzip telegraf_offline_debian_11.zip
Archive: telegraf_offline_debian_11.zip
creating: telegraf_offline_debian_11/
inflating: telegraf_offline_debian_11/lm-sensors_1%3a3.6.0-7_amd64.deb
creating: telegraf_offline_debian_11/python-pip/
inflating: telegraf_offline_debian_11/python-pip/jsonpath_ng-1.7.0-py3-none-any.whl
inflating: telegraf_offline_debian_11/python-pip/python3-pkg-
resources_52.0.0-4+deb11u2_all.deb
inflating: telegraf_offline_debian_11/python-pip/python3-lib2to3_3.9.2-1_all.deb
inflating: telegraf_offline_debian_11/python-pip/flatten_json-0.1.14-py3-none-any.whl
inflating: telegraf_offline_debian_11/python-pip/six-1.17.0-py2.py3-none-any.whl
inflating: telegraf_offline_debian_11/python-pip/python3-pip_20.3.4-4+deb11u1_all.deb
inflating: telegraf_offline_debian_11/python-pip/python-pip-whl_20.3.4-4+deb11u1_all.deb
inflating: telegraf_offline_debian_11/python-pip/python3-
setuptools_52.0.0-4+deb11u2_all.deb
inflating: telegraf_offline_debian_11/python-pip/python3-distutils_3.9.2-1_all.deb
inflating: telegraf_offline_debian_11/python-pip/ply-3.11-py2.py3-none-any.whl
inflating: telegraf_offline_debian_11/python-pip/python3-wheel_0.34.2-1_all.deb
inflating: telegraf_offline_debian_11/check_install.sh
inflating: telegraf_offline_debian_11/telegraf_1.32.1-1_amd64.deb
inflating: telegraf_offline_debian_11/инструкция.txt
inflating: telegraf_offline_debian_11/libsensors-config_1%3a3.6.0-7_all.deb
inflating: telegraf_offline_debian_11/sysstat_12.5.2-2+deb11u1_amd64.deb
inflating: telegraf_offline_debian_11/libsensors5_1%3a3.6.0-7_amd64.deb
inflating: telegraf_offline_debian_11/ethtool_1%3a5.9-1_amd64.deb
ngfw@NGFW1:~$
```

6. Перейдите в каталог `telegraf_offline_debian_11`:

```
ngfw@NGFW1:~$ cd telegraf_offline_debian_11
```

7. Установите пакеты, выполнив следующие команды:

```
sudo dpkg -i ethtool_1%3a5.9-1_amd64.deb
sudo dpkg -i libsensors-config_1%3a3.6.0-7_all.deb
sudo dpkg -i libsensors5_1%3a3.6.0-7_amd64.deb
sudo dpkg -i sysstat_12.5.2-2+deb11u1_amd64.deb
sudo dpkg -i lm-sensors_1%3a3.6.0-7_amd64.deb
sudo dpkg -i telegraf_1.32.1-1_amd64.deb
```

8. Перейдите в каталог `python-pip`:

```
ngfw@NGFW1:~/telegraf_offline_debian_11$ cd python-pip
ngfw@NGFW1:~/telegraf_offline_debian_11/python-pip$
```

9. Установите пакеты, выполнив следующие команды:

```
sudo dpkg -i python3-lib2to3_3.9.2-1_all.deb
sudo dpkg -i python3-distutils_3.9.2-1_all.deb
sudo dpkg -i python3-pkg-resources_52.0.0-4+deb11u2_all.deb
sudo dpkg -i python3-setuptools_52.0.0-4+deb11u2_all.deb
sudo dpkg -i python-pip-whl_20.3.4-4+deb11u1_all.deb
sudo dpkg -i python3-wheel_0.34.2-1_all.deb
```

```
sudo dpkg -i python3-pip_20.3.4-4+deb11u1_all.deb
sudo pip3 install ./flatten_json-0.1.14-py3-none-any.whl
sudo pip3 install ./six-1.17.0-py2.py3-none-any.whl
sudo pip3 install ./ply-3.11-py2.py3-none-any.whl
sudo pip3 install ./jsonpath_ng-1.7.0-py3-none-any.whl
```

10. Выполните следующие действия, чтобы проверить, что пакеты успешно установлены:

    - Перейдите в каталог на уровень выше:
      `ngfw@NGFW1:~/telegraf_offline_debian_11/python-pip$ cd ..`
    - Запустите проверочный скрипт:
      `ngfw@NGFW1:~/telegraf_offline_debian_11$ sudo ./check_install.sh`

      Система выполнит проверку обязательных зависимостей. По окончании проверки будет выведено значение `installed [OK]` при успешной установке и `NOT installed [NO]` — при неуспешной установке.

      Пример вывода выполнения скрипта при успешной установке:

```
ngfw@NGFW1:~/telegraf_offline_debian_11$ sudo ./check_install.sh
Check install packages + depends:
ethtool:
status: installed [OK]
depends:
libc6: installed [OK]
libmnl0: installed [OK]


libsensors5:
status: installed [OK]
depends:
libsensors-config: installed [OK]
libc6: installed [OK]


libsensors-config:
status: installed [OK]
depends: (none)


lm-sensors:
status: installed [OK]
depends:
sed: installed [OK]
lsb-base: installed [OK]
libc6: installed [OK]
libsensors5: installed [OK]
<perl:any>: NOT installed [NO]


sysstat:
status: installed [OK]
depends:
```

```
lsb-base: installed [OK]
ucf: installed [OK]
xz-utils: installed [OK]
<debconf-2.0>: NOT installed [NO]
libc6: installed [OK]
libsensors5: installed [OK]

telegraf:
status: installed [OK]
depends: (none)

python3-distutils:
status: installed [OK]
depends:
<python3:any>: NOT installed [NO]
<python3:any>: NOT installed [NO]
python3-lib2to3: installed [OK]

python3-pip:
status: installed [OK]
depends:
ca-certificates: installed [OK]
python3-distutils: installed [OK]
python3-setuptools: installed [OK]
python3-wheel: installed [OK]
python-pip-whl: installed [OK]
<python3:any>: NOT installed [NO]

python3-pkg-resources:
status: installed [OK]
depends:
<python3:any>: NOT installed [NO]

python3-setuptools:
status: installed [OK]
depends:
python3-pkg-resources: installed [OK]
python3-distutils: installed [OK]
<python3:any>: NOT installed [NO]

python3-wheel:
status: installed [OK]
depends:
<python3:any>: NOT installed [NO]
```

```
python-pip-whl:
status: installed [OK]
depends:
ca-certificates: installed [OK]

python3-lib2to3:
status: installed [OK]
depends:
<python3:any>: NOT installed [NO]
<python3:any>: NOT installed [NO]

ngfw@NGFW1:~/telegraf_offline_debian_11$
```

Настройка клиента

- Чтобы настроить клиент:

1. Перейдите в каталог `/home/ngfw/`.
   ```
   ngfw@NGFW1:~$ cd ~
   ```
2. Проверьте наличие архива с набором скриптов и конфигурационных файлов на узле PT NGFW:
   ```
   ngfw@NGFW1:~$ ls -la
   total 3382984
   ...
   -rw-r--r-- 1 ngfw ngfw 2388480 Apr 8 05:31 trex-perf-main-telegraf.tar.gz
   ```
3. Если архива нет, скачайте его по ссылке и поместите в каталог `/home/ngfw/`.
4. Выполните команду для распаковки архива:
   ```
   ngfw@NGFW1:~$ tar -xvf trex-perf-main-telegraf.tar.gz
   ./trex-perf-main-telegraf/
   ./trex-perf-main-telegraf/telegraf/
   ./trex-perf-main-telegraf/telegraf/linux.json
   ./trex-perf-main-telegraf/telegraf/pt-ngfw-lite.json
   ./trex-perf-main-telegraf/telegraf/pt-ngfw.json
   ./trex-perf-main-telegraf/telegraf/scripts/
   ./trex-perf-main-telegraf/telegraf/scripts/ethtool-stats-for-debug.py
   ./trex-perf-main-telegraf/telegraf/scripts/ethtool-stats.py
   ./trex-perf-main-telegraf/telegraf/scripts/stats_to_influx.py
   ./trex-perf-main-telegraf/telegraf/scripts/thread_stat.py
   ./trex-perf-main-telegraf/telegraf/telegraf.conf
   ./trex-perf-main-telegraf/telegraf/telegraf.d/
   ./trex-perf-main-telegraf/telegraf/telegraf.d/influx.conf
   ./trex-perf-main-telegraf/telegraf/telegraf.d/linux.conf
   ./trex-perf-main-telegraf/telegraf/telegraf.d/ngfw.conf
   ngfw@NGFW1:~$
   ```

5. Подготовьте структуру каталогов для работы с файлами конфигурации:
   - Очистите стандартный каталог конфигурации:
     `sudo rm -r /etc/telegraf/*`
   - Создайте каталог для дополнительных конфигурационных файлов:
     `sudo mkdir /etc/telegraf/telegraf.d`
6. Перейдите в каталог с распакованными файлами конфигурации Telegraf:
   `cd ~/trex-perf-main-telegraf/telegraf/`
7. Откройте конфигурационный файл в этом каталоге для редактирования:
   `nano ./telegraf.conf`
8. Измените IP-адрес InfluxDB в файле `telegraf.conf` на тот, который используется для InfluxDB:
   `urls = ["http://<IP-адрес сервера Grafana>:8086"]`
9. Если база уже создана, задайте параметру `skip_database_creation` значение `true` и введите имя базы данных для параметра `database`.

```
  GNU nano 5.4                          ./telegraf.conf

# # Configuration for sending metrics to InfluxDB
 [[outputs.influxdb]]
#   ## The full HTTP or UDP URL for your InfluxDB instance.
#   ##
#   ## Multiple URLs can be specified for a single cluster, only ONE of the
#   ## urls will be written to each interval.
#   # urls = ["unix:///var/run/influxdb.sock"]
 urls = ["http://172.20.22.14:8086"]
#   # urls = ["http://127.0.0.1:8086"]
#
#   ## The target database for metrics; will be created as needed.
#   ## For UDP url endpoint database needs to be configured on server side.
 database = "telegraf"
#
#   ## The value of this tag will be used to determine the database.  If this
#   ## tag is not set the 'database' option is used as the default.
#   # database_tag = ""
#
#   ## If true, the 'database_tag' will not be included in the written metric.
#   # exclude_database_tag = false
#
#   ## If true, no CREATE DATABASE queries will be sent.  Set to true when using
#   ## Telegraf with a user without permissions to create databases or when the
#   ## database already exists.
 skip_database_creation = true
#
```

Рисунок 77. Изменение параметра `skip_database_creation`

10. Укажите логин и пароль, которые вы указывали при настройке СУБД. Например:

```
username = "admin"
password = "321admin"
```

```
 GNU nano 5.4                                          ./telegraf.conf *
#   ## the default retention policy.  Only takes effect when using HTTP.
 retention_policy = ""
#
#   ## The value of this tag will be used to determine the retention policy.  If this
#   ## tag is not set the 'retention_policy' option is used as the default.
#   # retention_policy_tag = ""
#
#   ## If true, the 'retention_policy_tag' will not be included in the written metric.
#   # exclude_retention_policy_tag = false
#
#   ## Write consistency (clusters only), can be: "any", "one", "quorum", "all".
#   ## Only takes effect when using HTTP.
 write_consistency = "any"
#
#   ## Timeout for HTTP messages.
 timeout = "5s"
#
#   ## HTTP Basic Auth
 username = "admin"
 password = "321admin"
#
#   ## HTTP User-Agent
#   # user_agent = "telegraf"
#
#   ## UDP payload size is the maximum packet size to send.
#   # udp_payload = "512B"
#
#   ## Optional TLS Config for use on HTTP connections.
```

Рисунок 78. Пример логина и пароля

11. Обновите конфигурацию Telegraf, измените параметры его запуска и перезагрузите настройки системного менеджера служб:

```
sudo cp ./telegraf.conf /etc/telegraf/telegraf.conf
sudo sed -i 's/User=telegraf/User=root/g' /usr/lib/systemd/system/telegraf.service
sudo systemctl daemon-reload
```

12. Добавьте статистику Linux metrics:

```
sudo apt-get update && sudo apt-get install -y sysstat lm-sensors
```

13. Включите параметр sysstat в конфигурационном файле `/etc/default/sysstat`:

    Откройте файл `sysstat`:

```
ngfw@NGFW1:~/trex-perf-main-telegraf/telegraf$ cd ~
ngfw@NGFW1:~$ sudo nano /etc/default/sysstat
```

    Измените значение параметра `ENABLED` на `"true"`.

```
  GNU nano 5.4                          /etc/default/sysstat
#
# Default settings for /etc/init.d/sysstat, /etc/cron.d/sysstat
# and /etc/cron.daily/sysstat files
#

# Should sadc collect system activity informations? Valid values
# are "true" and "false". Please do not put other values, they
# will be overwritten by debconf!
ENABLED="true"
```

Рисунок 79. Включение параметра `sysstat`

14. Перезапустите sysstat:

    ```
    sudo systemctl restart sysstat
    ```

15. Перейдите в каталог `trex-perf-main-telegraf/telegraf/` и добавьте конфигурационный файл Telegraf Linux:

    ```
    ngfw@NGFW1:~$ cd ~/trex-perf-main-telegraf/telegraf/
    ngfw@NGFW1:~/trex-perf-main-telegraf/telegraf$ sudo cp ./telegraf.d/linux.conf /etc/
    telegraf/telegraf.d
    ```

16. Перезапустите Telegraf:

    ```
    sudo systemctl restart telegraf
    ```

17. Добавьте статистику PT-NGFW metrics:

    ```
    sudo ln -s "$PWD/scripts" /etc/telegraf/scripts
    sudo cp ./telegraf.d/ngfw.conf /etc/telegraf/telegraf.d
    sudo chmod +x -R /etc/telegraf/scripts/*
    sudo systemctl restart telegraf
    ```

    Вы можете проверить отображение данных телеметрии на узле межсетевого экрана в графическом интерфейсе Grafana на странице **Dashboards**.

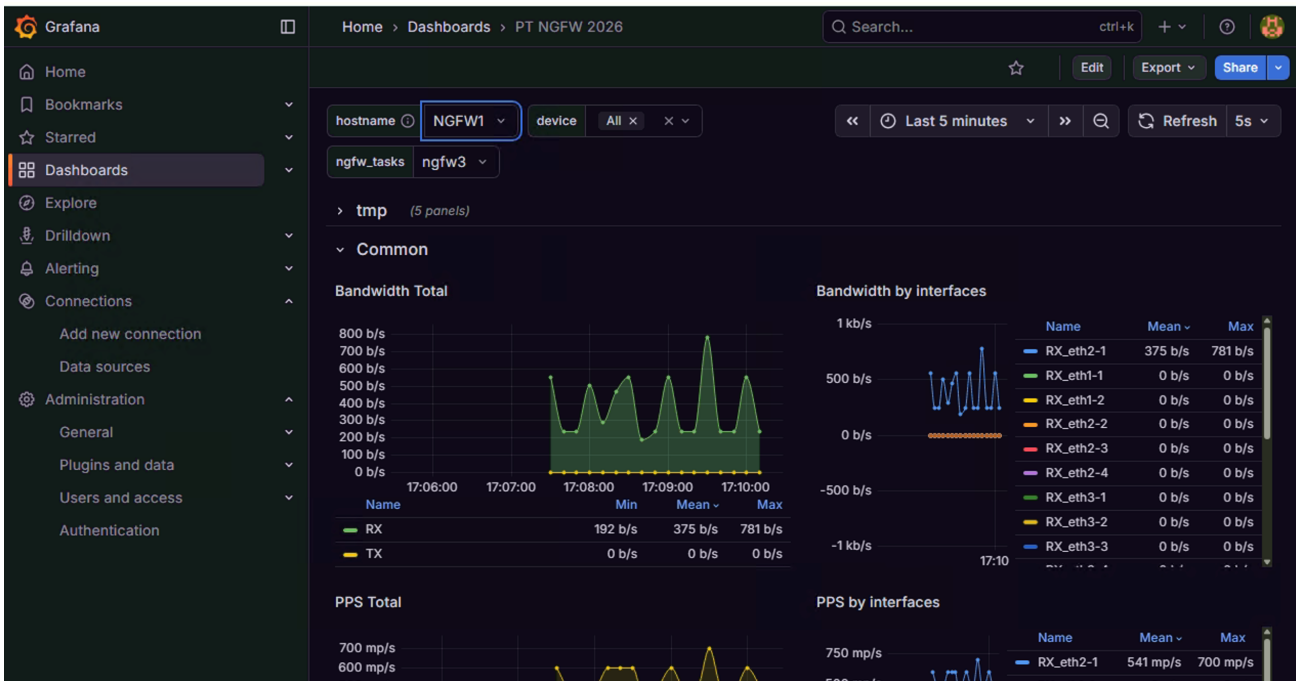


Рисунок 80. Страница **Dashboards** в Grafana

Подробнее про описание графиков (только дашборд PT NGFW Lite) см. в разделе «Описание графиков дашборда PT NGFW Lite (см. раздел 40)»

См. также

Описание графиков дашборда PT NGFW Lite (см. раздел 40)

5.5. Настройка выделенного сборщика журналов

В этом разделе описаны шаги по настройке выделенного сборщика журналов на ПАК PT NGFW LOG.

- Чтобы настроить выделенный сборщик журналов:

  1. Подключитесь к ПАК PT NGFW LOG через интерфейс управления устройством BMC или VGA.
  2. Выполните вход в ОС, используя логин `ngfw` и пароль `p0sitive`.

В этом разделе

Настройка интерфейса управления (MGMT) (см. раздел 5.5.1)

Настройка синхронизации времени с NTP-сервером (см. раздел 5.5.2)

5.5.1. Настройка интерфейса управления (MGMT)

Перед началом настройки

Настройка интерфейса управления осуществляется через подсистему systemd.

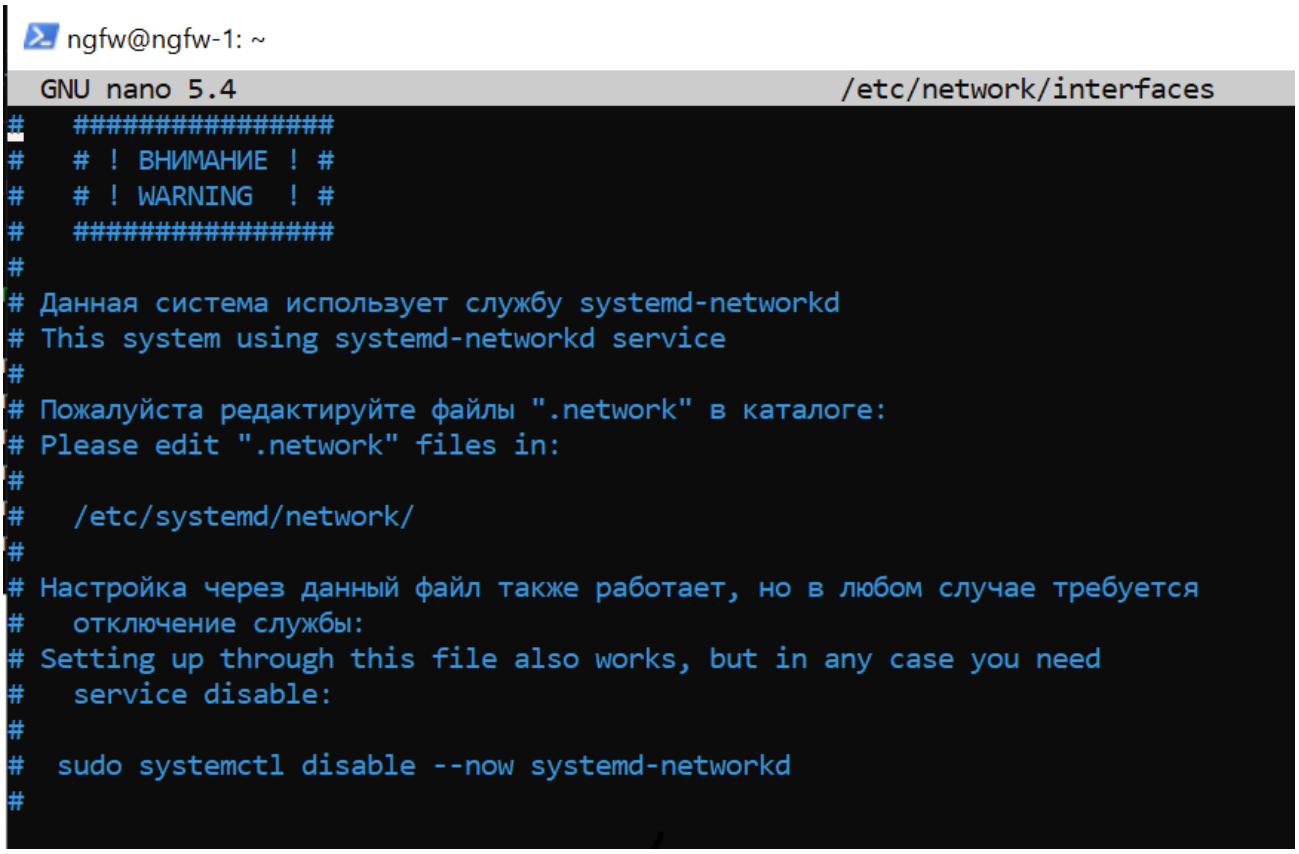


Рисунок 81. Справочная информация в файле `/etc/network/interfaces`

В первую очередь необходимо определить интерфейс, который будет взаимодействовать с сетью, а также проверить наличие необходимых файлов.

- Чтобы подготовить систему к настройке:

  1. Выполните команду `ip a` для определения интерфейса, который будет взаимодействовать с сетью.

```
ngfw@ngfw:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
2: mgmt1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:84:3d:be brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.103/24 brd 192.168.1.255 scope global dynamic mgmt1
       valid_lft 25164sec preferred_lft 25164sec
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
    link/ether 02:42:e2:d8:91:48 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
       valid_lft forever preferred_lft forever
```

Рисунок 82. Пример вывода команды `ip a`

Примечание. В выводе команды выше это интерфейс `mgmt1`. Далее он будет использоваться в качестве примера.

2. Выполните команду `ls -la /etc/systemd/network` для проверки наличия файлов `10-mgmt1.link` и `10-mgmt1.network`.

```
ngfw@ngfw:~$ ls -la /etc/systemd/network
total 16
drwxr-xr-x 2 root root 4096 Nov 21 10:46 .
drwxr-xr-x 6 root root 4096 Nov 20 14:37 ..
-rw-r--r-- 1 root root   49 Nov 21 10:46 10-mgmt1.link
-rw-r--r-- 1 root root  252 Nov 21 10:46 10-mgmt1.network
```

Рисунок 83. Пример вывода команды с файлами `10-mgmt1`

```
ngfw@ngfw:/etc/systemd/network$ ls
50-default-dhcp.network
```

Рисунок 84. Пример вывода команды без файлов `10-mgmt1`

3. В зависимости от результатов проверки настройте интерфейс управления по одной из инструкций ниже.

Настройка интерфейса при наличии файлов 10-mgmt1

- Чтобы настроить интерфейс управления:

1. Откройте файл `10-mgmt1.network`:
   ```
   sudo nano /etc/systemd/network/10-mgmt1.network
   ```
2. Измените параметры интерфейса управления `mgmt1`:
   ```
   [Match]
   Name=mgmt1


   [Network]
   # For autoconfig
   # Для автонастройки
   #DHCP=yes
   # Пример статической конфигурации:
   # Static config example:
   #
   Address=10.10.18.3/24
   Gateway=10.10.18.254
   DNS=10.10.22.31
   DNS=10.10.22.21
   ```
   Примечание. Адрес указанного DNS-сервера (серверов) используется базовой операционной системой и не влияет на разрешение FQDN в политиках безопасности процессом PT NGFW.
3. Узнайте PCI-адрес устройства с помощью команды `lspci -D | grep -i eth`.

   Примечание. В выводе команды необходимо обратить внимание на первый адрес в списке. Например, `0000:03:00.0`.
4. Откройте файл `10-mgmt1.link`:
   ```
   sudo nano /etc/systemd/network/10-mgmt1.link
   ```
   В файле должны быть указаны корректные PCI-адрес и название интерфейса, например:
   ```
   [Match]
   Path=pci-0000:03:00.0


   [Link]
   Name=mgmt1
   ```
5. Перезапустите сервис, чтобы изменения вступили в силу:
   ```
   sudo systemctl restart systemd-networkd
   ```

Настройка интерфейса при отсутствии файлов 10-mgmt1

- Чтобы настроить интерфейс управления:

1. Создайте и откройте файл `10-mgmt1.network`:
   ```
   sudo nano /etc/systemd/network/10-mgmt1.network
   ```
2. Измените параметры интерфейса управления `mgmt1`:
   ```
   [Match]
   Name=mgmt1


   [Network]
   # For autoconfig
   # Для автонастройки
   #DHCP=yes
   # Пример статической конфигурации:
   # Static config example:
   #
   Address=10.10.18.3/24
   Gateway=10.10.18.254
   DNS=10.10.22.31
   DNS=10.10.22.21
   ```
3. Узнайте PCI-адрес устройства с помощью команды `lspci -D | grep -i eth`.

   Примечание. В выводе команды необходимо обратить внимание на первый адрес в списке. Например, `0000:03:00.0`.
4. Создайте и откройте файл `10-mgmt1.link`:
   ```
   sudo nano /etc/systemd/network/10-mgmt1.link
   ```
5. Внесите в него изменения, указав PCI-адрес из предыдущего шага и название интерфейса, например:
   ```
   [Match]
   Path=pci-0000:03:00.0


   [Link]
   Name=mgmt1
   ```
6. Удалите остальные файлы из каталога `/etc/systemd/network` при их наличии, например:
   ```
   sudo rm /etc/systemd/network/50-default-dhcp.network
   ```
7. Перезагрузите устройство, чтобы изменения вступили в силу:
   ```
   sudo reboot
   ```

5.5.2. Настройка синхронизации времени с NTP-сервером

Для корректной работы систем журналирования и мониторинга необходимо синхронизировать время. Для этого используются NTP-серверы.

- Чтобы настроить синхронизацию времени с NTP-сервером:

  1. Откройте конфигурационный файл `timesyncd.conf`:
     ```
     sudo nano /etc/systemd/timesyncd.conf
     ```
  2. Раскомментируйте строку `NTP` и введите адрес NTP-сервера по своему усмотрению.

```
#  This file is part of systemd.
#
#  systemd is free software; you can redistribute it and/or modify it
#  under the terms of the GNU Lesser General Public License as published by
#  the Free Software Foundation; either version 2.1 of the License, or
#  (at your option) any later version.
#
# Entries in this file show the compile time defaults.
# You can change settings by editing this file.
# Defaults can be restored by simply deleting this file.
#
# See timesyncd.conf(5) for details.

[Time]
NTP=ntp.test.ru
#FallbackNTP=0.debian.pool.ntp.org 1.debian.pool.ntp.org 2.debian.pool.ntp.org 3.debian.pool.ntp.org
#RootDistanceMaxSec=5
#PollIntervalMinSec=32
#PollIntervalMaxSec=2048
```

Рисунок 85. Содержимое файла `timesyncd.conf`

  3. Перезапустите сервис, чтобы изменения вступили в силу:
     ```
     sudo systemctl restart systemd-timesyncd
     ```
     Вы можете проверить работоспособность службы с помощью команды:
     ```
     timedatectl timesync-status
     ```

6. Принцип работы

Для эффективного развертывания, настройки и эксплуатации продукта в корпоративной среде необходимо понимание принципов работы PT NGFW.

PT NGFW анализирует трафик пользовательских сессий, состоящих из потоков данных двух типов:

— исходящий трафик — поток данных от клиента локальной сети к внешнему сетевому ресурсу. Как правило, клиент инициирует соединение путем запроса на адрес внешнего ресурса;

— входящий трафик — поток данных от внешнего ресурса, адресованный клиенту локальной сети.

В основу работы PT NGFW положены следующие принципы:

— Глубокая инспекция пакетов (Deep Packet Inspection, DPI) — PT NGFW анализирует не только заголовки, но и содержимое (payload) каждого пакета. Это позволяет идентифицировать конкретные приложения, в том числе работающие на нестандартных портах.

— Контроль состояния сессий (Stateful Packet Inspection, SPI) — PT NGFW отслеживает состояние сетевых соединений чтобы принимать решения о фильтрации на основе контекста всего диалога, а не отдельных пакетов.

— Идентификация пользователей и приложений — PT NGFW связывает сетевой трафик с конкретными пользователями и приложениями, что позволяет создавать гранулярные политики безопасности.

— Механизм предотвращения вторжений (IPS) — в режиме реального времени сравнивает проходящий трафик с базами сигнатур атак и поведенческими аномалиями, чтобы активно обнаруживать и нейтрализовать попытки вторжений.

— Инспекция зашифрованного трафика — PT NGFW может расшифровывать, SSL/TLS-трафик. Это позволяет анализировать защищенные соединения на наличие угроз.

— Антивирусная проверка трафика — встроенный в межсетевой экран потоковый антивирус позволяет обнаружить в передаваемом трафике зараженный файл и предотвратить его передачу.

Ниже детально описаны специфичные принципы и подходы, связанные с архитектурой и программной реализацией PT NGFW.

В этом разделе

Режимы работы сетевых интерфейсов (см. раздел 6.1)

Принципы обработки трафика (см. раздел 6.2)

Инспекция SSL/TLS-трафика (см. раздел 6.3)

Правила межсетевого экрана (см. раздел 6.4)

Группы устройств (см. раздел 6.5)

Виртуальные контексты (см. раздел 6.6)

Виртуальные роутеры (см. раздел 6.7)

Зоны безопасности (см. раздел 6.8)

Ролевая модель (см. раздел 6.9)

6.1. Режимы работы сетевых интерфейсов

PT NGFW поддерживает разделение физического сетевого интерфейса на сабинтерфейс — логические интерфейсы, которые используют родительский интерфейс для приема и передачи данных и наследуют его MAC-адрес.

Настройка сабинтерфейсов выполняется аналогично физическим интерфейсам. Например, на одном физическом интерфейсе можно создать несколько сабинтерфейсов и назначить им IP-адреса из разных подсетей чтобы маршрутизировать трафик между этими подсетями. Также вы можете назначить сабинтерфейсам VLAN-метки и использовать их для маршрутизации трафика между VLAN, либо создать зеркальный порт для дублирования IP-пакетов во внешние системы анализа трафика.

Вы можете создать для физического интерфейса до 4094 сабинтерфейсов, каждый из которых может работать в одном из следующих режимов:

— **Маршрутизация** (Routing) — передача трафика осуществляется согласно таблице маршрутизации, при этом отбрасывается широковещательный трафик и трафик протоколов, отличных от IP.

— **Виртуальное соединение** (vWire) — в этом режиме сабинтерфейсы могут быть объединены, образуя сетевой мост между сегментами сети. При передаче трафика через виртуальное соединение при необходимости выполняется преобразование VLAN-меток, поэтому его можно использовать для объединения разных VLAN.

— **Зеркалирование** (Decryption mirroring) — этот режим используется для зеркалирования (дублирования) проходящего расшифрованного трафика с целью его передачи во внешние системы.

По умолчанию каждый физический интерфейс PT NGFW имеет сабинтерфейс, работающий в режиме маршрутизации и предназначенный для обработки нетегированного трафика.

6.2. Принципы обработки трафика

PT NGFW выполняет анализ и фильтрацию трафика с учетом состояния сессий (SPI — Stateful Packet Inspection). Если IP-пакет принадлежит к ранее установленной сессии, то он дополнительно анализируется с учетом текущего состояния и направления потоков сессии. Такие проверки позволяют защитить сеть от несанкционированного проникновения в момент закрытия сессии или с помощью поддельных IP-пакетов.

При обработке сетевых протоколов, не устанавливающих соединение (например, UDP), началом сессии считается первый пакет, удовлетворяющий условиям одного из правил политики безопасности. В этом случае PT NGFW завершает сессию по истечении тайм-аута (см. раздел 26) — определенного времени допустимой неактивности сетевого узла.

Чтобы правильно настроить правила межсетевого экрана (см. раздел 6.4), ознакомьтесь со схемой и порядком обработки трафика в PT NGFW:

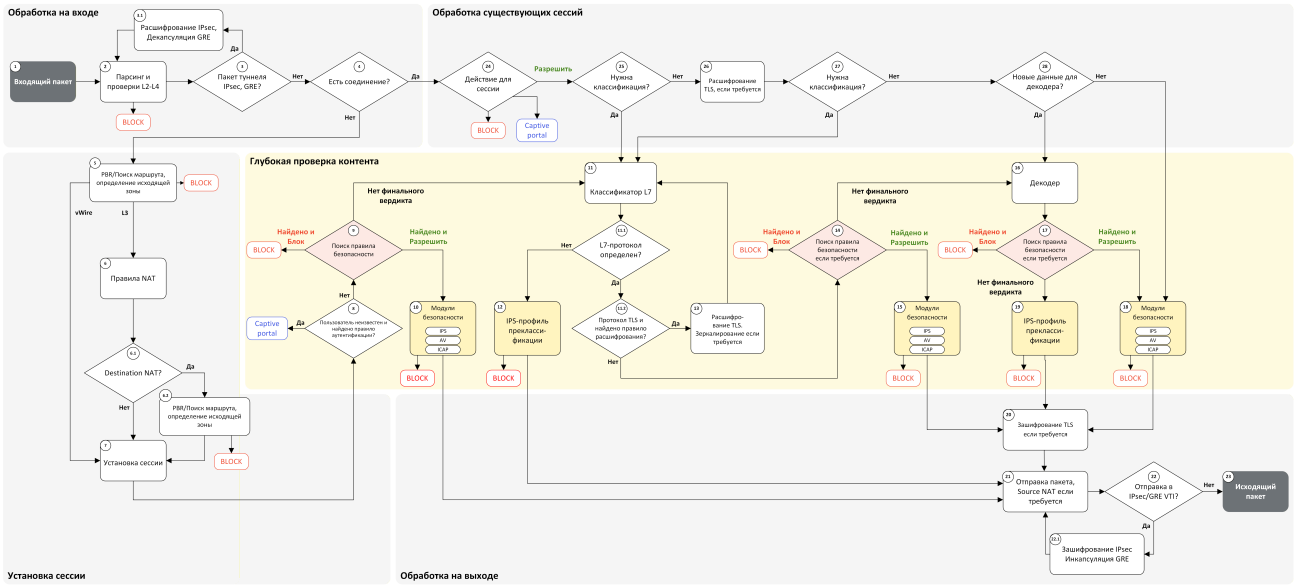


Рисунок 86. Схема обработки трафика

Блокировка (**Блок**) трафика выполняется, в зависимости от настроек (модуля, правила безопасности, IPS- или других профилей), одним из способов:

— Сброс — заблокированный трафик отбрасывается без уведомления клиента и сервера.

— Сброс с отправкой RST — трафик отбрасывается с отправкой сообщения TCP RST (клиенту, серверу или обоим) для принудительного прерывания TCP-сессии.

Порядок обработки трафика в PT NGFW

1. Входящий Ethernet-кадр поступает на сетевой интерфейс.
2. Выполняется парсинг[1] и проверка заголовков (L2, L3-L4, если есть), проверка контрольных сумм, корректность адреса источника и соответствие установленных в пакете флагов, проверка ассоциации Ethernet-кадра с интерфейсом[2]. Выполняется сборка фрагментированного трафика, а также проверка встроенным средством антиспуфинга —

1 **Парсинг** — поиск и извлечение содержимого полей сетевых кадров, пакетов, сегментов.

2 **Проверка ассоциации Ethernet-кадра с интерфейсом** — проверка, что на физическом интерфейсе присутствует сабинтерфейс для обработки нетегированного трафика либо трафика с VLAN ID, указанным в заголовке входящего Ethernet-кадра.

проверяется, что IP-адрес источника достижим через тот интерфейс, на который поступил пакет. Если проверка не пройдена, то дальнейшая обработка прекращается, а соответствующий Ethernet-кадр, IP-пакет или сегмент отбрасывается.

3. Если пакет принадлежит соединению IPsec Site-to-Site (в том числе туннельному интерфейсу Remote Access VPN), то выполняется обработка заголовков IPsec, расшифрование данных IPsec и проверка расшифрованных пакетов. Если пакет принадлежит соединению GRE, то выполняется обработка заголовков GRE и декапсуляция исходного пакета.

   Примечание. Начальные пакеты IPsec и GRE также проходят проверку правилами безопасности до расшифрования данных.

   ***Пример**: В начале IPsec-соединения сессия еще не идентифицирована и PT NGFW выполняет проверку IP-пакетов, включая идентификацию протокола и поиск подходящего правила безопасности, без их расшифрования. После установления IPsec-соединения PT NGFW расшифровывает IP-пакеты для последующего анализа.

4. Устанавливается принадлежность IP-пакета существующему сетевому соединению (сессии). Если IP-пакет принадлежит существующей сессии, то обработка трафика выполняется в соответствии с порядком обработки сессии (шаг 24), иначе переходит к следующему шагу.

5. Выполняется проверка связи IP-пакета с интерфейсом:

   - Если пакет поступил на сабинтерфейс Layer 3 (режим маршрутизации), то выполняется поиск по таблице маршрутизации и политикам PBR (policy based routing).
   - Если пакет поступил на сабинтерфейс vWire, то поиск правила NAT пропускается.
   - Определяется исходящий интерфейс и связанная с ним зона безопасности.
   - Если пакет не связан ни с одним интерфейсом, не найден подходящий маршрут, сабинтерфейс vWire, либо пакет блокируется правилом PBR, то он отбрасывается.

6. Выполняется поиск подходящего правила NAT

   6.1. Если пакет подпадает под правило NAT с настроенной трансляцией адресов назначения (Destination NAT), то выполняется трансляция адреса и порта назначения. Если в правиле NAT настроена трансляция адресов источника (Source NAT), то параметры трансляции запоминаются и используются на финальной стадии отправки пакета.

   Примечание. Дальнейший поиск подходящих правил безопасности, расшифрования и прочих правил выполняется, используя значения адреса и порта источника (source) до трансляции, а адреса и порта назначения (destination) — после трансляции. Это дает возможность проверять трафик последующими правилами, используя фактические адреса и порты клиента и сервера.

   6.2. Если IP-адрес или порт назначения изменились, то выполняется повторный поиск маршрута в таблице маршрутизации или правила маршрутизации по политикам PBR. Определяется исходящий интерфейс и связанная с ним зона безопасности. Если пакет не ассоциирован ни с одним интерфейсом, не найден подходящий маршрут или найдено правило PBR с блокирующим действием, то пакет отбрасывается.

7. Выполняется установление TCP-сессии: для TCP-трафика выполняется проверка, что это первый пакет сессии (TCP SYN). Пакеты неизвестных TCP-сессий, начинающихся не с TCP SYN, отбрасываются. Также на данном шаге выполняется поиск соответствия IP-адреса источника пользователю.

   Примечание. Принадлежность входящих IP-пакетов к ранее установленным сессиям определяется комбинацией значений: IP-адрес и порт отправителя, IP-адрес и порт получателя, номер IP-протокола. Запоминаются зоны безопасности источника и назначения. Таблица сессий каждого виртуального контекста является независимой от таблиц сессий других виртуальных контекстов. При получении последующих пакетов сессии проверяется их зона безопасности для прямого и обратного потоков. Если зоны отличаются от тех, которые были определены в момент установления сессии, то такие пакеты отбрасываются.

8. Если пользователь неизвестен (не найдено соответствие IP-адреса источника пользователю), то выполняется поиск подходящего правила аутентификации. Если оно найдено, то сессия помечается для обработки модулем Captive portal (см. раздел 29).

   Примечание. Трафик помеченной сессии пропускается только в адрес Captive portal, при этом трафик DNS и HTTP/HTTPS пропускается, а остальной —отбрасывается. При срабатывании правила аутентификации PT NGFW в ответ на DNS-запрос от клиента отправляет DNS-ответ с коротким TTL (Time to Live), в котором для запрошенного клиентом FQDN возвращается IP-адрес Captive portal.

   ***Пример**: Клиент обращается к веб-сайту ya.ru и на первом шаге отправляет DNS-запрос (выполняет разрешение FQDN ya.ru в IP-адрес), который перехватывается NGFW. В DNS-ответе NGFW возвращает IP-адрес Captive portal для ресурса ya.ru вместо реального IP-адреса ya.ru. Затем клиент выполняет HTTPS-запрос в IP-адрес Captive portal. После успешной аутентификации пользователя на Captive portal NGFW получает связку IP-адреса источника и пользователя и последующие сессии этого клиента уже не подпадают под правило аутентификации.

9. Выполняется поиск подходящего правила безопасности. На данном этапе итоговое правило может быть найдено при условии, если нет более приоритетных правил, требующих определения вышестоящего протокола/приложения.

   ***Пример**: Обрабатываемый пакет соответствует нескольким правилам безопасности по параметрам заголовков L3-L4, а также зонам безопасности и приоритетным (первым по списку) является правило, в котором указано приложение **Любое**. В этом случае какое бы приложение ни было идентифицировано, текущая сессия подпадет под это правило безопасности.

   Таким образом, на данном этапе правило может сработать на основе L3-L4-заголовков (разрешить или заблокировать сессию) если критерием правила является приложение **Любое**.

   Примечание. Определение приложения осуществляется независимо от нахождения на этом шаге итогового правила.

10. Если трафик разрешен сработавшим правилом безопасности и в нем указаны модули безопасности, то он проверяется теми модулями, которые могут быть использованы на данном этапе обработки. Далее пакеты передаются в блок выходной обработки (шаг 21).

11. Если на шаге 9 не удалось найти подходящее итоговое правило безопасности из-за необходимости определения вышестоящего протокола или приложения, то пакет передается модулю классификации[3] для определения вышестоящего протокола.

    ***Пример**: Обрабатываемый пакет соответствует нескольким правилам безопасности по параметрам заголовков L3-L4, а также зонам безопасности, но в каждом правиле указаны различные приложения. Таким образом, на шаге 9 было невозможно однозначно определить итоговое правило безопасности.

    11.1. Если данных для идентификации протокола пока недостаточно, то пакет передается в блок выходной обработки с проверкой на шаге 12.

    11.2. Если протокол удалось определить и это не TLS, либо TLS, но сессия не подходит ни под одно правило расшифрования, то обработка переходит на шаг 14.

    Примечание. Если на шаге 9 не удалось найти итоговое правило безопасности, то обязательным условием перехода алгоритма обработки трафика к шагу 11 является наличие как минимум одного правила-кандидата: правила безопасности, параметры L3-L4, а также зоны безопасности которого соответствуют обрабатываемому пакету, указано приложение и правило может потенциально разрешить обрабатываемые данные сессии после определения вышестоящего протокола или приложения (подприложения).

12. Если данных для определения вышестоящего протокола пока недостаточно, например, обрабатывается один из начальных пакетов TCP-рукопожатия, где не передается никаких данных приложения или данные приложения есть в пакете, но их недостаточно для определения итогового правила безопасности, то пакет передается в блок выходной обработки и проверяются модулем IPS если активирован IPS-профиль преклассификации.

    Примечание. Профиль IPS-преклассификации обеспечивает защиту от атак на этапе, когда NGFW требуется пропустить некоторое количество данных для идентификации вышестоящего протокола/приложения.

13. Если пакет относится к протоколу TLS и он подпадает под правило расшифрования, то трафик TLS-сессии расшифровывается и отправляется на классификацию (шаг 11).

    Если указан профиль зеркалирования, то копия расшифрованного трафика отправляется с интерфейса, указанного в профиле зеркалирования, и в Ethernet-кадрах копии расшифрованного трафика устанавливается MAC-адрес назначения, заданный в профиле.

14. После идентификации прикладного протокола выполняется поиск подходящего правила безопасности, если оно не было найдено ранее. На данном этапе правило безопасности может быть найдено при условии, если нет более приоритетных правил, требующих определения специфического приложения.

---

3 **Классификация** — определение протокола прикладного уровня, данные которого передаются в рамках анализируемой сетевой сессии.

*__Пример__: Обрабатываемый IP-пакет сессии HTTP соответствует нескольким правилам безопасности по параметрам L3, L4 и L7, а также зонам безопасности и самым приоритетным (первым по списку) является правило, в котором указано приложение «HTTP». В этом случае итоговое решение принимается на основе заголовков L3, L4, данных о прикладном протоколе и зонах безопасности.

Примечание. Определение приложения и подприложения выполняется независимо от нахождения на этом шаге итогового правила.

15. Если трафик разрешен правилом безопасности и в нем указаны модули безопасности (IPS, Антивирус, ICAP), то он проверяется этими модулями. Далее пакеты передаются в блок выходной обработки (шаг 20).
16. Если на шаге 14 не удалось найти подходящее правило безопасности из-за необходимости определения специфического приложения, то пакет передается в модуль декодера, который выполняет парсинг полей данных идентифицированного прикладного протокола, идентифицирует приложение и подприложение (функцию приложения).
17. Если финальное правило безопасности не было найдено ранее на шаге 14, то выполняется поиск подходящего правила безопасности.

    *__Пример__: Обрабатываемый IP-пакет соответствует нескольким правилам безопасности по параметрам L3, L4 и L7, а также зонам безопасности и в каждом правиле указаны различные приложения: в первом правиле — `Yandex-Disk-Upload`, во втором — `Yandex-Disk-Download`. Поскольку оба приложения работают поверх протокола HTTP, то на шаге 14 было невозможно определить итоговое правило, т.к. требовался анализ данных прикладного протокола.
18. Если трафик разрешен правилом безопасности и в нем указаны модули безопасности (IPS, Антивирус, ICAP), то он проверяется этими модулями. Далее пакеты передаются в блок выходной обработки (шаг 20).
19. Если имеющихся данных еще недостаточно для определения приложения, то пакет передается в блок выходной обработки и проверяется модулем IPS (если активирован IPS-профиль преклассификации).

    *__Пример__: Обрабатывается один из начальных пакетов TCP-рукопожатия, где не передается данных приложения, либо пакет содержит данные приложения, но их недостаточно для идентификации прикладного протокола или приложения (подприложения) и определения итогового правила безопасности.

    Примечание. Профиль IPS-преклассификации обеспечивает защиту от атак на этапе, когда NGFW требуется пропустить некоторое количество данных для идентификации приложения.
20. Если данные сессии подпадают под правило расшифрования TLS (выполнялось расшифрование на шаге 13), то выполняется их зашифрование перед отправкой в сеть.
21. Если пакет сессии подпадает под правило NAT с настроенной трансляцией адреса источника, то выполняется замена адреса и порта источника согласно настроенному в правиле NAT действию.

22. Если пакет принадлежит соединению IPsec Site-to-Site, то выполняется зашифрование данных.

    Внимание. Пакеты соединений GRE over IPsec перед шифрованием инкапсулируются в GRE-туннель.

23. IP-пакету устанавливаются новые заголовки L2 и L3 в соответствии с NAT, ARP и таблицей маршрутизации, после чего исходящий Ethernet-кадр отправляется в соответствующий сетевой интерфейс.

24. Если IP-пакет принадлежит существующей сессии, то выполняется действие согласно сработавшему правилу безопасности: заблокировать или разрешить трафик сессии, либо перенаправить на Captive portal.

    Примечание. Для Captive portal такой сессией может быть HTTP/HTTPS-соединение, инициированное клиентом в адрес Captive portal.

25. Если пакеты сессии разрешены, то, в зависимости от стадии установления соединения, принимается решение о необходимости дальнейшей классификации данных сессии.

    ***Пример**: Получен пакет TCP SYN-ACK, TCP ACK или первый пакет с данными после успешного установления сессии TCP. На этом этапе протокол L7 и приложение еще не известны и выполняется классификация данных.

    Таким образом, для данных пакета может начаться классификация (переход к шагу 11), либо (если вышестоящий протокол уже определен) — дальнейшая обработка. Если правило безопасности еще не найдено, то поиск подходящего правила безопасности выполняется после классификации (шаг 14) или, если потребуется, то после декодирования[4] (шаг 17).

    Если выполняется классификация и выполняется переход к шагу 11, но при этом итоговое правило уже было определено ранее на шаге 9, то далее поиск правила безопасности (шаги 14 или 17) не выполняется за исключением ситуации, когда изменилось приложение (подприложение) и выполняется повторный поиск правила безопасности (шаг 28).

    ***Пример**: На шаге 9 найдено итоговое правило безопасности, в котором задано приложение **Любое** и параметры L3 — L4 соответствуют пакетам сессии. Несмотря на это, идентификация прикладного протокола и приложения продолжится.

26. Если сессия уже была классифицированы как TLS-сессия, а также сработало правило расшифрования, то данные сессии расшифровываются. Выполняется зеркалирование расшифрованных данных, если это указано в правиле расшифрования.

4 **Декодирование** — поиск, анализ структуры и извлечение содержимого отдельных полей сообщений протоколов начиная от сеансового уровня и выше.

27. Проверяется требуется ли классификация для расшифрованных данных.

    - Если требуется — переход к классификации (шаг 11). Если после получения новых данных правило безопасности еще не найдено, то выполняется поиск подходящего правила безопасности на шаге 14 или, если потребуется, то на шаге 17.
    - Если протокол уже идентифицирован — выполняется переход к следующему шагу.

28. Выполняется декодирование данных приложения:

    - Если приложение или подприложение не изменилось, то трафик проверяется модулями безопасности (IPS, Антивирус, ICAP), заданными в правиле безопасности (шаг 18). После этого пакеты передаются для выходной обработки (шаг 20).
    - Если изменилось приложение или подприложение (например, если в одной TCP-сессии сначала передавались данные одного приложения, а затем произошло переключение на другое приложение), то данные отправляются в модуль декодера (шаг 16). После получения данных от декодера и, если итоговое правило безопасности еще не было найдено, либо было обнаружено изменение приложения (подприложения), то выполняется поиск подходящего правила безопасности (шаг 17).

    Если при этом выполняется переход к шагу 16, но итоговое правило уже было определено ранее на шаге 9 или 14, то далее (шаг 17) поиск правила безопасности не выполняется за исключением ситуации, когда изменилось приложение или подприложение и выполняется повторный поиск правила безопасности (шаг 28).

    ***Пример**: На шаге 14 найдено итоговое правило безопасности, в котором задано приложение **HTTP** и параметры L3-L4 соответствуют пакетам сессии. Несмотря на это, идентификация приложения (подприложения) продолжится.

Особенности обработки трафика

— Если сессия не была явно разрешена ни одним из правил безопасности, то она блокируется правилом по умолчанию с действием **Отбросить**, которое всегда неявно располагается самым последним в списке правил безопасности.

— Если в процессе идентификации изменилось приложение (подприложение), то ранее найденное правило безопасности может перестать соответствовать сессии. В таком случае поиск правила безопасности будет выполняться заново.

— При проектировании сети необходимо исключить повторное прохождение IP-пакета через сетевые интерфейсы одного виртуального контекста (вне зависимости от режима работы этих интерфейсов). В ходе установления сессии PT NGFW запоминает зону безопасности источника (входящая зона) и назначения (исходящая зона). В случае повторного прохождения IP-пакета через сетевые интерфейсы одного виртуального контекста зона безопасности источника и/или назначения будет отличаться от зоны/зон, которые были зафиксированы на этапе установления сессии и пакет будет отброшен.

См. также

IPS (система предотвращения вторжений) (см. раздел 22)

Антивирусная проверка трафика (см. раздел 23)

6.3. Инспекция SSL/TLS-трафика

Значительная часть корпоративного трафика передается по защищенным протоколам (TLS 1.2/1.3, HTTPS и другие). PT NGFW использует механизм прозрачного TLS-прокси (TLS Decrypt) для контролируемого расшифрования проходящего трафика и его анализа модулями безопасности. Это позволяет применять правила межсетевого экрана на основе приложений и прикладных протоколов, использующих зашифрованный трафик.

Инспекция SSL/TLS-трафика позволяет:

— обнаруживать вирусы и вредоносное ПО внутри HTTPS-сессий;

— блокировать доступ к запрещенным страницам (контентная фильтрация);

— выявлять утечки данных (в связке с DLP-системами);

— обнаруживать и предотвращать атаки на уровне приложений.

PT NGFW встраивается в TLS-сессию между клиентом и сервером: устанавливает отдельное TLS-соединение с клиентом, подменяя сертификат сервера на сертификат, подписанный корневым центром сертификации (CA) организации, и отдельное TLS-соединение с сервером назначения. Расшифрованный трафик передается во внутренний конвейер обработки и обрабатывается политиками и модулями безопасности, после этого повторно зашифровывается и направляется получателю. Подробнее об обработке трафика см. в разделе Принципы обработки трафика (см. раздел 6.2).

При необходимости PT NGFW может зеркалировать (см. раздел 27) расшифрованный трафик — при этом копия расшифрованного трафика направляется во внешнюю систему анализа (например, в DLP-систему).

Сертификат для инспекции

Для инспекции PT NGFW использует сертификат, которым подписывает сертификаты анализируемых сессий. По умолчанию используется самоподписанный сертификат, который можно заменить на собственный (см. раздел 11.3) (например, сертификат, подписанный корпоративным центром сертификации).

Правила расшифрования

По умолчанию PT NGFW не расшифровывает зашифрованный трафик. Инспекцию SSL/TLS-трафика включают правила расшифрования (см. раздел 6.4), определяющих параметры обработки шифрованного трафика и действия с ним:

— **Условия срабатывания** — адреса источника и назначения, пользователи сети (при интеграции с Active Directory), сетевые сервисы и категории URL.

— **Действие** — расшифровывать или не расшифровывать трафик, подпадающий под условия правила. Действие **Не расшифровывать** позволяет создавать исключения из инспекции, если для заданных веб-ресурсов расшифрование трафика невозможно или не требуется.

Примечание. Чтобы создать правило для исключения из расшифрования отдельных ресурсов, необходимо создать для этих ресурсов URL-категорию и перечислить FQDN исключаемых ресурсов в поле **URL-адреса**.

— **Параметры зеркалирования** — выбор профиля зеркалирования, определяющего сабинтерфейсы, на которые будет направляться копия расшифрованного трафика.

— **Журналирование** — включает или выключает регистрацию срабатываний правила расшифрования в журнале **Расшифрование**.

Рекомендации по использованию

При настройке SSL/TLS-инспекции используйте следующие подходы и рекомендации:

— Планирование производительности: TLS-инспекция требует дополнительных вычислительных ресурсов. Учитывайте объем зашифрованного трафика в сети при выборе модели PT NGFW.

— Управление сертификатами: рекомендуется использовать сертификаты, подписанные корпоративным центром сертификации, и распространять корневой сертификат на все клиентские системы централизовано (например, через групповые политики) для беспрерывной работы пользователей.

— Гранулированные политики: создавайте отдельные правила расшифрования для разных типов трафика и приложений, чтобы гибко управлять процессом инспекции.

— Мониторинг и аудит: регулярно анализируйте журналы расшифрования для выявления просроченных или отозванных сертификатов, нестандартных алгоритмов шифрования и потенциальных угроз.

— Интеграция с другими системами: используйте зеркалирование расшифрованного трафика для передачи данных во внешние системы анализа при создании комплексной системы мониторинга информационной безопасности.

Особенности инспекции SSL/TLS-трафика в PT NGFW

— Для работы инспекции требуется распространить корневой сертификат PT NGFW на конечные устройства организации.

— Для защиты собственных серверов организации требуется загрузка сертификата и закрытого ключа защищаемого сервера на конечное устройство.

— PT NGFW не поддерживает расшифрование трафика приложений, использующих SSL Pinning (например, банковские приложения). Для таких приложений требуется создать исключения, чтобы не нарушать их работу.

— PT NGFW не поддерживает расшифрование трафика ресурсов с client-certificate-аутентификацией, так как не имеет доступа к пользовательскому сертификату. Для таких ресурсов следует создать исключения.

— При создании политик безопасности для расшифрованного трафика следует вместо HTTPS указывать приложение HTTP.

— При расшифровании трафика TLS 1.3 информация о сертификатах и доменах шифруется, поэтому PT NGFW использует данные из поля SNI сообщения TLS client hello.

— Изменения в профиле зеркалирования действуют только для новых сессий.

6.4. Правила межсетевого экрана

Для обработки и фильтрации трафика PT NGFW использует правила межсетевого экрана четырех типов:

1. **Правила аутентификации** — определяют условия и параметры перенаправления пользователей сети на портал аутентификации. Правила аутентификации выполняется до проверки правилами безопасности и только для неаутентифицированных пользователей.
2. **Правила безопасности** — задают параметры фильтрации трафика и определяют действия с ним: разрешить или заблокировать, проверить системой предотвращения вторжений (IPS) и потоковым антивирусом, либо передать на внешний ICAP-сервер для анализа.
3. **Правила трансляции адресов (NAT)** — предназначены для преобразование IP-адресов одной сети в IP-адреса другой сети в соответствии с RFC 2663. PT NGFW может выполнять: трансляцию адреса источника (динамическая трансляция, маскарадинг), трансляцию адреса назначения (статическая трансляция, перенаправление портов), одновременную трансляцию адресов источника и назначения.
4. **Правила расшифрования** — управляют расшифрованием HTTPS-трафика для его последующего анализа и проверки службой IPS и антивирусом.

Правила межсетевого экрана назначаются группам устройств, при этом в состав правил, применяемых к группе, также входят правила, наследуемые из родительской группы. Правила в каждой группе разделены на два блока:

— **Предправила** — обрабатываются до правил дочерней группы.

— **Постправила** — обрабатываются после правил дочерней группы.

Итоговый список правил определяется иерархией групп устройств и обрабатывается в следующем порядке:

1. Предправила родительской группы.
2. Правила дочерней группы (ее пред- и постправила).
3. Постправила родительской группы.

IP-пакеты последовательно проверяются на соответствие правилам и к ним применяется первое правило, все условия которого соответствуют характеристикам трафика, после чего проверка IP-пакета правилами прекращается.

Порядок поиска соответствия правилам

Пользователь PT NGFW располагает правила, учитывая порядок поиска подходящего правила межсетевыми экранами. Поиск происходит начиная с первого правила до нахождения полного соответствия полученного трафика условиям в одном из правил. После нахождения соответствия над трафиком выполняются действия, указанные в правиле. В связи с этим менее общие правила рекомендуется располагать выше более общих. Например: правило безопасности, разрешающее трафик для конкретных IP-адресов из какой-либо подсети, обычно должно находиться выше правила, запрещающего трафик для всей этой подсети.

Между условиями срабатывания одного типа работает логическое ИЛИ. Между условиями срабатывания разных типов работает логическое И. Пример: адрес источника «А» или «Б» и пользователь «А» или «Б» и приложение «А».

Общие рекомендации по настройке правил межсетевого экрана

— Используя правила безопасности, вы можете разрешить или запретить дальнейшую передачу трафика, проверить трафик системой предотвращения вторжений и потоковым антивирусом.

— Используя правила расшифрования, вы можете указать признаки трафика, который должен быть расшифрован или исключен из процесса расшифрования. Расшифрование трафика требуется для возможности распознания внутри него приложения при проверке правилами безопасности и для анализа трафика системой предотвращения вторжений и антивирусом. Для расшифрования трафика используется механизм прямого прозрачного TLS-прокси.

— С помощью правил NAT вы можете указать признаки трафика, для которого выполненяется трансляция сетевых адресов.

— Используя правила аутентификации, вы можете настроить перенаправление пользователей на портал аутентификации, которая осуществляется в домене Active Directory, связанном с межсетевым экраном. Прохождение пользователями аутентификации позволяет применять к ним правила межсетевого экрана. Проверка трафика правилами аутентификации выполняется до проверки правилами безопасности и только для неаутентифицированных пользователей. Действием правила аутентификации может быть перенаправление или исключение трафика из процесса перенаправления. Адрес портала указывается в правиле аутентификации в виде профиля аутентификации.

Предустановленные правила безопасности

PT NGFW поставляется с двумя постправилами безопасности: **Default-Local-Out-Allow** и **Default-Block-All**.

Правило **Default-Local-Out-Allow** разрешает любой трафик, генерируемый самим PT NGFW, то есть, трафик, исходящий из зоны безопасности **Local** (например, трафик OSPF, BFD или пакеты для проверки доступности узлов). Правило **Default-Block-All** располагается непосредственно ниже правила **Default-Local-Out-Allow** и запрещает (выполняется действие **Отбросить**) любой трафик. Срабатывания правил по умолчанию не журналируются. Вы можете изменить режим журналирования, если требуется.

Необходимо учитывать, что PT NGFW также содержит неявное правило, отбрасывающее любой трафик и всегда находящееся самым последним. По этой причине любая сессия, не подпадающая ни под одно разрешающее правило, блокируется. Срабатывания этого правила не журналируются.

6.5. Группы устройств

Группы устройств предназначены для объединения виртуальных контекстов (см. раздел 6.6) (устройств), требующих одинаковых правил. Это упрощает централизованное управление большим количеством межсетевых экранов, поскольку правила межсетевого экрана назначаются не отдельным виртуальным контекстам, а группе устройств.

Вы можете объединять контексты в группы по любому удобному признаку, как, например, территориальное местоположение или функция. Все виртуальные контексты внутри группы автоматически используют правила, назначенные этой группе.

Группы устройств могут также включать другие группы устройств, образуя иерархию «родитель-потомок», где дочерние группы наследуют все правила от родительской. Одна группа может быть одновременно и родительской, и дочерней. По умолчанию PT NGFW поставляется с группой **Global**, которая является вершиной иерархии правил.

Используя иерархию групп, вы можете создавать общие политики безопасности на верхнем уровне и уточнять их на нижних.

Пример иерархии:

Организация → **Регионы** → **Филиал**.

Здесь группа **Филиал** наследует правила от группы **Регионы**, а **Регионы**, в свою очередь — от группы **Организация**.

В итоге, к группе **Филиал** будут применены правила всех групп выше себя.

6.6. Виртуальные контексты

PT NGFW позволяет создавать виртуальные контексты — логические межсетевые экраны. Виртуальные контексты предназначены для административного разделения физического межсетевого экрана на несколько логических. Каждому виртуальному контексту назначаются сабинтерфейсы. По умолчанию каждый физический межсетевой экран имеет виртуальный контекст **Default**, которому автоматически назначаются все сабинтерфейсы физического межсетевого экрана.

Виртуальные контексты изолированы друг от друга — каждый из них имеет собственную таблицу состояний и таблицы маршрутизации. В разных виртуальных контекстах могут существовать сессии с одинаковыми параметрами, при этом они будут обрабатываться как независимые.

> **Примечание.** Принадлежность входящих IP-пакетов к сессиям в рамках виртуального контекста определяется по следующим параметрам: IP-адрес и порт отправителя, IP-адрес и порт получателя, протокол. Также для каждой сессии запоминаются входящая и исходящая зоны безопасности.

Если в сценариях использования PT NGFW вашей организации отсутствует необходимость в виртуальных контекстах, то контекст **Default** можно рассматривать как контекст, означающий физический межсетевой экран. Возможность удаления этого виртуального контекста не предусмотрена.

Виртуальные контексты добавляются в группы устройств.

В рамках виртуального контекста создаются виртуальные роутеры (см. раздел 6.7) и виртуальные соединения (vWire).

Рисунок ниже содержит пример разделения устройства на виртуальные контексты и показывает, как взаимосвязаны виртуальный контекст, виртуальный роутер (маршрутизатор) и виртуальное соединение (vWire).

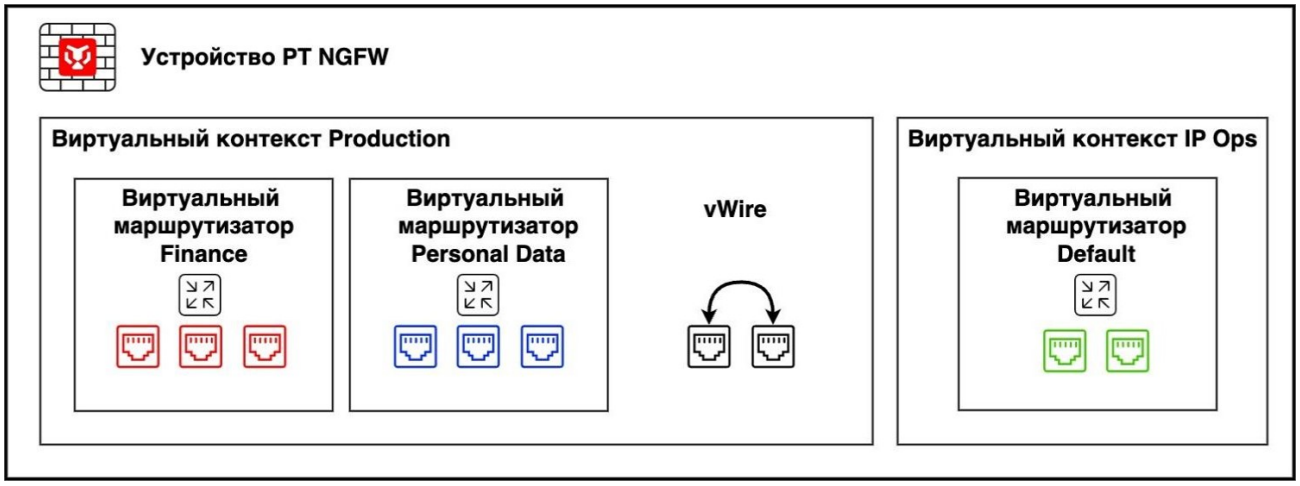


Рисунок 87. Пример разделения на контексты

6.7. Виртуальные роутеры

Виртуальный роутер в PT NGFW — программное обеспечение, эмулирующее работу физического маршрутизатора.

Виртуальные роутеры имеют независимые таблицы маршрутизации и изолированы один от другого. Каждый виртуальный роутер создается в рамках виртуального контекста. К виртуальному роутеру могут быть привязаны только те сабинтерфейсы, которым назначен режим работы маршутизатора. Один сабинтерфейс может принадлежать только одному виртуальному роутеру. Любой сабинтерфейс, предназначенный для маршрутизации, должен быть привязан к виртуальному роутеру. При подключении межсетевого экрана к системе управления в виртуальном контексте **Default** автоматически создается виртуальный роутер **Default**, не подлежащий удалению.

6.8. Зоны безопасности

Зона безопасности — это один или несколько сабинтерфейсов с общими параметрами безопасности. Зона безопасности должна быть назначена любому сабинтерфейсу и может быть указана в правиле межсетевого экрана как условие для его срабатывания. В правиле может быть указана зона безопасности источника трафика и зона безопасности назначения трафика. Каждому сабинтерфейсу может быть назначена только одна зона безопасности.

> **Примечание.** Зона безопасности Local является служебной и не предусмотрена для назначения сабинтерфейсам.

По умолчанию в PT NGFW предустановлены 4 зоны безопасности: Local, DMZ, Trusted и Untrusted. Вы можете создавать новые зоны безопасности, а также редактировать и удалять все зоны, кроме Local.

Зона безопасности Local является служебной и может использоваться в правилах безопасности для разрешения или ограничения трафика, предназначенного для самого межсетевого экрана, а также его защиты от атак в трафике, поступающем в его адрес.

Например, для проверки с помощью модуля IPS внешних запросов, поступающих в адрес одного из сабинтерфейсов межсетевого экрана. Также зона Local может использоваться в правилах политики NAT, когда адресом назначения исходного пакета, подлежащего трансляции, является адрес сабинтерфейса межсетевого экрана.

6.9. Ролевая модель

В PT NGFW используется ролевая модель доступа. Предусмотрены следующие роли пользователей: **Суперадминистратор**, **Администратор межсетевого экрана**, **Администратор системы**, **Администратор безопасности**, **Оператор**.

В таблице ниже перечислены доступы, которые имеет каждая из ролей к той или иной функции.

Доступы бывают пяти типов:

- L — доступ на просмотр списка сущностей;
- C — доступ на создание новой сущности;
- R — доступ на просмотр карточки со всеми атрибутами сущности;
- U — доступ на изменение сущности;
- D — доступ на удаление сущности.

Примечание. Возможность создания дополнительных ролей отсутствует.

Таблица 8. Роли пользователей и доступные функции

Сущность	Администратор безопасности	Администратор межсетевого экрана	Администратор системы	Суперадминистратор	Оператор
Группы устройств	L	L	LCUD	LCUD	L
Правила безопасности	—	LCUD	—	LCUD	L
Правила NAT	—	—	LCUD	LCUD	L
Правила расшифрования	—	LCUD	—	LCUD	L
Правила аутентификации	—	LCUD	—	LCUD	L
Применение изменений	—	CU	—	CU	—
Объекты «Приложение»	—	L	—	L	L
Объекты «Пользователь»	—	L	—	L	L
Объекты «Сервис»	—	L	LCUD	LCUD	L
Объекты «Адрес»	—	L	LCUD	LCUD	L
Объекты «Зона»	—	L	LCUD	LCUD	L

Сущность	Администратор безопасности	Администратор межсетевого экрана	Администратор системы	Супер-администратор	Оператор
Объекты «Категория URL»	—	L	LCUD	LCUD	L
IPS-профили и группы	LCUD	L	—	LCUD	L
Профили аутентификации	—	L	LCUD	LCUD	L
Профили зеркалирования	—	L	LCUD	LCUD	L
ICAP-профили и серверы	—	L	LCUD	LCUD	L
Устройства	—	L	LCUD	LCUD	L
Самотестирование	—	CU	—	CU	—
Параметры. Тайм-ауты	—	L	LCUD	LCUD	L
Сборщик журналов	—	LU	LU	LU	L
SNMP	—	LCUD	—	LCUD	L
Сабинтерфейсы	—	L	LCUD	LCUD	L
Виртуальные контексты	—	L	LCUD	LCUD	L
Remote Access VPN	—	L	LCUD	LCUD	L
GRE	—	L	LCUD	LCUD	L
Виртуальные соединения	—	L	LCUD	LCUD	L
Виртуальные роутеры	—	L	LCUD	LCUD	L
Маршрутизация (статическая, OSPF, BGP, PBR)	—	L	LCUD	LCUD	L
Профили проверки доступности	—	L	LCUD	LCUD	L
BFD-профили	—	L	LCUD	LCUD	L
IPsec VPN	—	L	LCUD	LCUD	L
DHCP relay	—	L	LCUD	LCUD	L
Журналы	LR	LR	—	LR	LR
Сборщик журналов	LR	LCRUD	LCRUD	LCRUD	LR
Отправка syslog-сообщений	—	LCUD	—	LCUD	LR
Учетные записи пользователей	—	LCUD	—	LCUD	LR
Обновление баз контента	—	LCUD	—	LCUD	L
Резервное копирование и восстановление	—	LCUD	—	LCUD	LR

7. Вход в PT NGFW

При первом входе в учетную запись вам потребуется сменить пароль.

- Чтобы войти в систему управления:

  1. Введите в адресной строке браузера https://<FQDN системы управления>.
  2. Введите логин и пароль вашей учетной записи.
  3. Нажмите кнопку **Войти**.

     Примечание. Для первого входа в системную учетную запись пользователя используйте логин `admin` и пароль `admin`.

  Вход в систему управления выполнен.

  Примечание. При первом входе в систему управления отобразится сообщение об ошибке проверки сертификата. Ошибка связана с тем, что сертификат, предоставляемый системой управления, подписан самой системой управления, и может быть проигнорирована.

8. Интерфейс PT NGFW

Интерфейс системы управления состоит из главного меню, рабочей области и кнопки **Применить на устройствах**.

> **Внимание!** В зависимости от роли вашей учетной записи некоторые из описанных элементов интерфейса могут быть недоступны.

Главное меню

Главное меню содержит разделы для перехода к страницам интерфейса.

Страница «Политики»

Страница **Политики** позволяет настраивать правила межсетевого экрана. Ее рабочая область содержит иерархический список групп устройств и вкладки **Безопасность**, **NAT**, **Расшифрование** и **Аутентификация**. При выборе вкладки и группы отображается таблица, строкам которой соответствуют правила определенного типа этой группы.

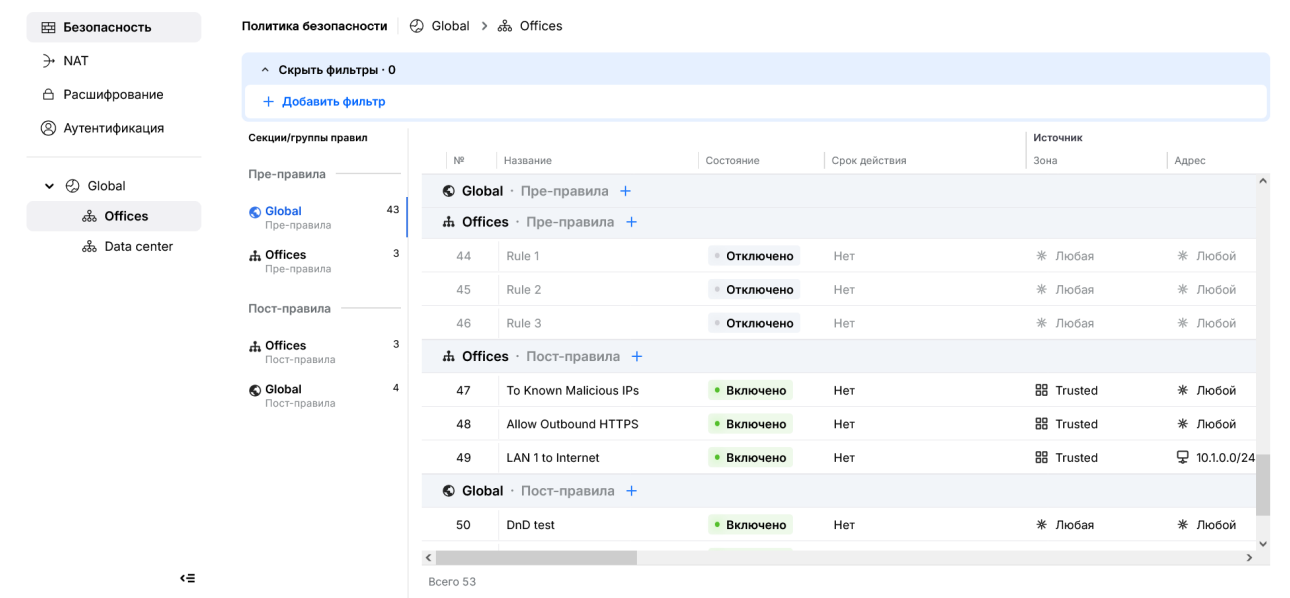


Рисунок 88. Страница «Политики»

Страница «Объекты»

Страница **Объекты** позволяет работать с объектами. Рабочая область страницы **Объекты** содержит несколько вкладок в левом верхнем углу. На каждой из вкладок отображаются объекты определенного типа.

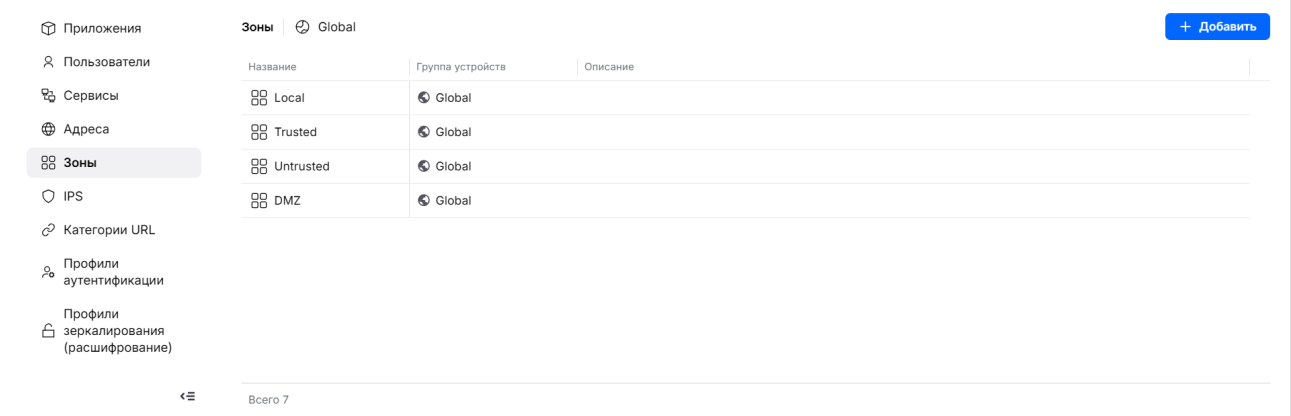


Рисунок 89. Страница «Объекты»

Страница «Устройства»

На странице **Устройства** вы можете просматривать и добавлять межсетевые экраны, настраивать сетевые интерфейсы и маршрутизацию, добавлять виртуальные соединения, группы устройств, виртуальные роутеры и виртуальные контексты.

Страница «Журналы»

На странице **Журналы** приводится информация о событиях, подлежащих журналированию, например о срабатываниях правил безопасности или действиях пользователей в системе управления.

Страница «Параметры»

Страница **Параметры** позволяет управлять учетными записями администраторов системы управления, настраивать отправку syslog-сообщений, осуществлять резервное копирование (см. раздел 41), настраивать работу со сборщиками журналов (см. раздел 39.1), менять язык интерфейса, просматривать пользовательскую документацию, лицензионное соглашение и спецификацию API, а также получать информацию о текущей версии.

Кнопка «Применить на устройствах»

Кнопка **Применить на устройствах** позволяет передать изменения конфигурации из системы управления на межсетевые экраны.

9. Начало работы

Этапы начала работы с PT NGFW включают:

1. Добавление межсетевого экрана в систему управления (см. раздел 12). В результате добавления в системе управления появляется сущность «устройство» и связанный с ней виртуальный контекст (см. раздел 6.6) **Default**. Последний автоматически привязывается к поставляемой вместе с PT NGFW группой устройств (см. раздел 6.5) **Global**. Также для каждого физического интерфейса устройства автоматически добавляется один сабинтерфейс и назначается виртуальному контексту **Default**.
2. Настройку сабинтерфейсов (см. раздел 13). На этом этапе происходит выбор режимов работы сабинтерфейсов (см. раздел 6.1), назначение сабинтерфейсу виртуального роутера (см. раздел 6.7) (для сабинтерфейсов в режиме маршрутизации) и зоны безопасности (см. раздел 6.8), а также, если это необходимо, добавление дополнительных сабинтерфейсов.
3. Настройку маршрутизации (см. раздел 14), если это необходимо.
4. Добавление виртуального соединения (см. раздел 15) (vWire), если это необходимо.
5. Добавление правил межсетевого экрана (см. раздел 16).
6. Применение изменений путем нажатия на кнопку **Применить на устройствах**.

10. Управление учетными записями

Управление учетными записями подразумевает добавление, изменение, удаление и блокирование учетных записей, а также сброс паролей. Управление доступно для ролей **Администратор межсетевого экрана** и **Суперадминистратор**.

Управление учетными записями происходит на странице **Параметры** → **Администраторы**.

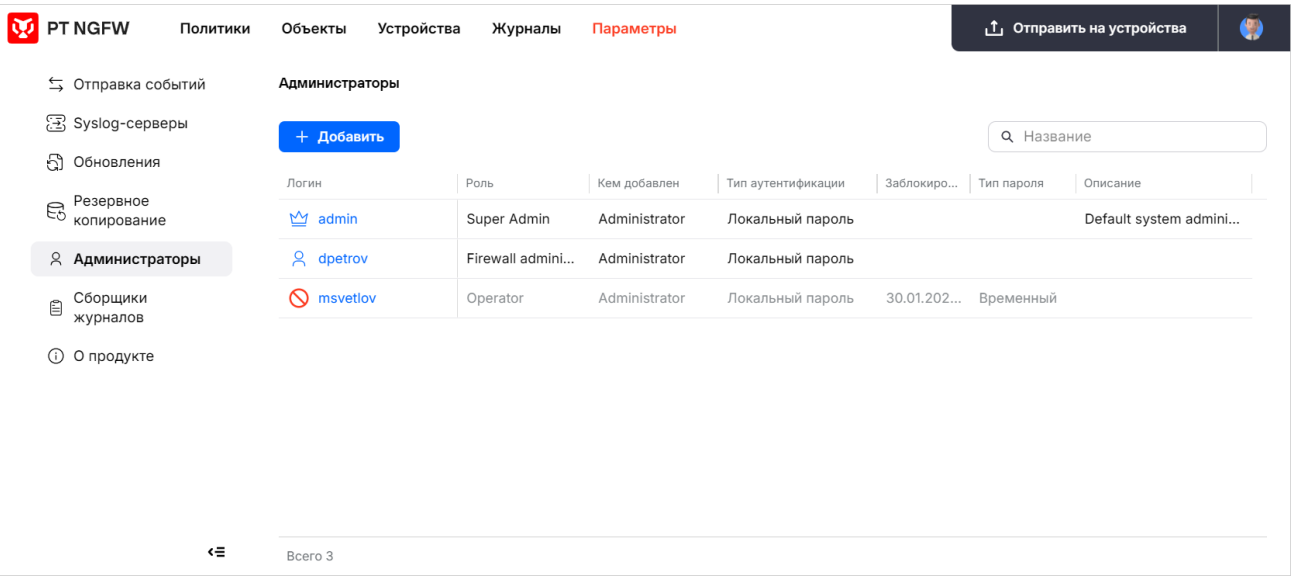


Рисунок 90. Страница **Администраторы**

Добавление учетной записи

- Чтобы добавить учетную запись:

  1. В главном меню выберите **Параметры**.
  2. Выберите вкладку **Администраторы**.
  3. Нажмите **Добавить**.
  4. Выберите роль пользователя.

     Примечание. Подробнее о доступных ролях см. в разделе «Ролевая модель».
  5. Введите логин учетной записи.
  6. Если требуется, введите описание.
  7. Укажите тип аутентификации: **Локальный пароль**, **LDAP** или **RADIUS**.

     Примечание. В случае выбора типа аутентификации LDAP или RADIUS, убедитесь, что подключение к LDAP или RADIUS настроено в агенте Identity Control (см. раздел 28.4).
  8. Введите временный пароль учетной записи.

Примечание. Владельцу учетной записи с типом аутентификации **Локальный пароль** потребуется сменить временный пароль при первом входе в систему.

9. Нажмите **Добавить**.

Вы можете изменить или удалить учетную запись, используя контекстное меню.

Блокирование или разблокирование учетной записи

Заблокированная учетная запись не может быть использована для входа в систему управления. В списке учетных записей заблокированные выделены серым цветом.

- Чтобы заблокировать или разблокировать учетную запись:

  1. В главном меню выберите **Параметры**.
  2. Выберите вкладку **Администраторы**.
  3. В контекстном меню учетной записи выберите **Заблокировать** или **Разблокировать**.

Сброс пароля учетной записи

- Чтобы сбросить пароль учетной записи:

  1. В главном меню выберите **Параметры**.
  2. В контекстном меню учетной записи выберите **Сброс пароля**.
  3. Введите временный пароль учетной записи.

     Примечание. Владельцу учетной записи с типом аутентификации **Локальный пароль** потребуется сменить временный пароль при первом входе в систему.
  4. Нажмите **Сбросить**.

См. также

Настройка PT NGFW для подключения к агенту (см. раздел 28.4.1)

11. Работа с сертификатами

PT NGFW использует цифровые сертификаты для безопасной передачи данных с помощью технологии шифрования с открытым ключом. Сертификаты устанавливаются в локальное хранилище и применяются для расшифрования SSL/TLS-трафика, защиты взаимодействия PT NGFW с системами управления и мониторинга, а также для защиты веб-трафика системы управления и портала аутентификации. Также сертификаты используются для защиты взаимодействия ключевых компонентов PT NGFW с помощью механизма mTLS (Mutual TLS Authentication).

В этом разделе

Установка собственного сертификата для веб-интерфейса системы управления (см. раздел 11.1)

Настройка mTLS для защиты взаимодействия PT NGFW с системой управления (см. раздел 11.2)

Установка собственного сертификата для расшифрования TLS/SSL-трафика (см. раздел 11.3)

Установка сертификата удостоверяющего центра на сетевых узлах пользователей (см. раздел 11.4)

11.1. Установка собственного сертификата для веб-интерфейса системы управления

По умолчанию для защиты веб-интерфейса системы управления используется самоподписанный сертификат. Вы можете установить собственный PEM-сертификат, например корпоративный или выпущенный внешним удостоверяющим центром.

- Чтобы установить собственный сертификат для веб-интерфейса системы управления:

  1. Подключитесь к интерфейсу командной строки узла системы управления.
  2. Скопируйте файл сертификата и его закрытый ключ в каталог `/opt/pt-ngfw/traefik/config/certs`

     Примечание. Файлы сертификата и закрытого ключа должны называться `main.crt` и `main.key`, соответственно. Закрытый ключ сертификата не должен быть защищен парольной фразой.
  3. Перезапустите службу `traefik`:

     ```
     ~# sudo systemctl restart pt-ngfw-traefik
     ```

11.2. Настройка mTLS для защиты взаимодействия PT NGFW с системой управления

Механизм взаимной проверки подлинности mTLS реализует двустороннюю TLS-аутентификацию сервера и клиента. Он обеспечивает устойчивость ко многим видам сетевых атак и по умолчанию используется для защиты взаимодействия между компонентами PT NGFW. Вы можете установить и использовать собственные PEM-сертификаты для взаимной проверки подлинности, например, если этого требует политика безопасности вашей компании.

Поскольку mTLS–соединение инициирует система управления, то при взаимодействии она выступает в роли клиента, а узел PT NGFW — в роли сервера. Установка клиентского и серверного сертификатов, а также настройка mTLS выполняется на узлах PT NGFW и на узле системы управления.

- Чтобы настроить использование mTLS на узле PT NGFW:

  1. Подключитесь к интерфейсу командной строки узла PT NGFW.
  2. Скопируйте в каталог `/opt/pt-ngfw/ngfw-core/etc/config/mtls/` следующие файлы:

     — PEM-сертификат узла PT NGFW;

     — закрытый ключ сертификата PT NGFW;

     Внимание! Закрытый ключ сертификата не должен быть защищен парольной фразой.

     — корневой сертификат центра сертификации (промежуточного центра сертификации), которым подписан сертификат системы управления.
  3. Откройте для редактирования конфигурационный файл `pt-ngfw.conf`:

     ```
     ~$ sudo nano /opt/pt-ngfw/ngfw-core/etc/config/pt-ngfw.conf
     ```
  4. Отредактируйте конфигурационный файл `pt-ngfw.conf` и задайте в нем пути к сертификатам в секции `[web_server]`:

     ```
     "web_server": {
     "address": "0.0.0.0",
     ...
     "server_certificate": "<путь к сертификату узла NGFW>",
     "server_private": "<путь к закрытому ключу>",
     "client_certificate": "<путь к корневому сертификату, которым подписан сертификат системы управления>",
     ...
     ```

     Внимание. Пути к файлам сертификатов необходимо указывать относительно каталога `/opt/pt-ngfw/ngfw-core/`. Например, если полный путь к файлу сертификата `/opt/pt-ngfw/ngfw-core/etc/config/mtls/NGFW-CA.crt`, то в файле конфигурации укажите: `"client_certificate": "etc/config/mtls/NGFW-CA.crt"`

5. Сохраните изменения **Ctrl+O** и закройте редактор **Ctrl+X**.
6. Перезапустите службу `pt-ngfw-core.service`:

   ```
   ~$ sudo systemctl restart pt-ngfw-core.service
   ```

- Чтобы настроить использование mTLS на узле системы управления:

1. Подключитесь к интерфейсу командной строки узла системы управления.
2. Скопируйте в каталог `/opt/pt-ngfw/ngfw-ms-backend/config/certs/` следующие файлы:

   — PEM-сертификат системы управления;

   — закрытый ключ сертификата системы управления;

   Внимание! Закрытый ключ сертификата не должен быть защищен парольной фразой.

   — корневой сертификат центра сертификации (промежуточного центра сертификации), которым подписан сертификат узла PT NGFW.
3. Откройте для редактирования конфигурационный файл `config.toml`:

   ```
   ~$ sudo nano /opt/pt-ngfw/ngfw-ms-backend/config/config.toml
   ```
4. Отредактируйте конфигурационный файл `config.toml` и задайте в нем пути к сертификатам в секции `[ngfw]`:

   ```
   ....
   [ngfw]
   tlsCert = "<путь к сертификату системы управления>"
   tlsKey = "<путь к закрытому ключу сертификата системы управления>"
   tlsCA = "<путь к корневому сертификату>"
   ....
   insecure = false
   serverName = "<имя узла>"
   port = 443
   ...
   ```

   Внимание. Пути к файлам сертификатов необходимо указывать относительно каталога `/opt/pt-ngfw/ngfw-ms-backend`. Например, если полный путь к файлу сертификата `/opt/pt-ngfw/ngfw-ms-backend/config/certs/ca-cert.crt`, то в файле конфигурации укажите: `tlsCA = "/config/certs/ca-cert.pem"`
5. Сохраните изменения **Ctrl+O** и закройте редактор **Ctrl+X**.
6. Перезапустите службу `pt-ngfw-ms-backend`:

   ```
   ~$ sudo systemctl restart pt-ngfw-ms-backend
   ```

11.3. Установка собственного сертификата для расшифрования TLS/SSL-трафика

PT NGFW использует при расшифровании трафика заранее сформированный сертификат, которым подписываются сертификаты анализируемых сессий. По умолчанию в PT NGFW установлен самоподписанный сертификат, вместо которого вы можете установить и использовать собственный.

> **Примечание.** Сертификат для расшифрования трафика должен иметь полномочия на подписывание сертификатов, для этого убедитесь, что в нем установлен атрибут `Basic Constraints CA:TRUE`. Закрытый ключ не должен быть защищен парольной фразой.

- Чтобы установить собственный сертификат для расшифрования трафика:

  1. Подключитесь к интерфейсу командной строки узла PT NGFW.
  2. Удалите текущий сертификат и его закрытый ключ:
     ```
     sudo rm /opt/pt-ngfw/ngfw-core/etc/config/mitm/root.crt
     sudo rm /opt/pt-ngfw/ngfw-core/etc/config/mitm/root.key
     ```
  3. Скопируйте файл сертификата и его закрытый ключ в каталог `/opt/pt-ngfw/ngfw-core/etc/config/mitm`

     > **Примечание.** Файлы сертификата и закрытого ключа должны называться `root.crt` и `root.key`, соответственно.
  4. Перезапустите службу `pt-ngfw-core.service`:
     ```
     ~$ sudo systemctl restart pt-ngfw-core.service
     ```

  Внимание. После смены сертификата браузеры и сетевые приложения пользователей сети могут выдавать предупреждение о подмене сертификата (`net::ERR_CERT_AUTHORITY_INVALID`). Для корректной работы сетевых приложений установите на сетевых узлах пользователей корневой сертификат удостоверяющего центра (сертификат, которым был подписан установленный для расшифрования трафика сертификат).

11.4. Установка сертификата удостоверяющего центра на сетевых узлах пользователей

Сертификат удостоверяющего центра необходимо добавить в хранилище доверенных корневых центров сертификации на каждом узле, чей SSL/TLS-трафик вы хотите анализировать. Способ установки сертификата зависит от используемого ПО. Некоторые сетевые приложения (например, браузеры) имеют собственные хранилища сертификатов, поэтому для них процедура установки отличается. Ниже описана установка сертификата для распространенных браузеров.

- Чтобы установить сертификат для браузеров Edge, Chrome в ОС Windows:

  1. Откройте папку, куда вы скопировали PEM-сертификат, измените его расширение на `*.der` и дважды щелкните по нему.

     Следуйте рекомендациям мастера импорта сертификатов.
  2. В окне информации нажмите **Установить сертификат**.
  3. В окне выбора хранилища сертификата нажмите **Обзор** и выберите **Доверенные корневые центры сертификации**, после чего нажмите **ОК**.
  4. Нажмите **Готово**.
  5. В окне **Предупреждение о безопасности** нажмите **Да**.

- Чтобы установить сертификат для браузеров Safari, Chrome в ОС MacOS:

  1. Откройте папку, куда вы скопировали PEM-сертификат, дважды щелкните по нему.
  2. В открывшемся приложении **Связка ключей** введите имя пользователя и пароль, затем нажмите **Изменить связку ключей**.
  3. На вкладке **Сертификаты** выберите установленный сертификат, затем раскройте вкладку **Доверие** и выберите **Всегда доверять**.
  4. В открывшемся окне настроек доверия введите имя пользователя и пароль, затем нажмите **Обновить настройки**.

- Чтобы установить сертификат в хранилище браузера Firefox:

  1. Откройте окно настройки браузера Firefox. Для этого в окне браузера выберите **Инструменты** → **Настройки**.
  2. Выберите **Приватность и защита** → **Просмотр сертификатов**.
  3. Нажмите **Импортировать** и укажите путь к скачанному PEM-сертификату.
  4. В окне **Загрузка сертификата** выберите **Доверять при идентификации веб-сайтов**.
  5. Нажмите **ОК**.

12. Добавление устройств

Чтобы иметь возможность настраивать различные функции устройства и получать от него данные журналов, устройство необходимо добавить в систему управления. При добавлении устройства в нем автоматически создается виртуальный контекст **Default** и несколько (по числу физических интерфейсов) сабинтерфейсов. Последние автоматически назначаются виртуальному контексту **Default**. Когда виртуальный контекст **Default** является единственным, его можно рассматривать как само устройство. Возможность удаления виртуального контекста **Default** не предусмотрена.

> **Примечание.** В PT NGFW устройствами называются физические устройства с установленным компонентом межсетевого экрана.

- Чтобы добавить устройство:

1. В главном меню выберите **Устройства**.
2. Нажмите **Добавить устройство**.
3. Введите название устройства в системе управления.
4. Если требуется, введите описание.
5. Введите серийный номер устройства.
6. Введите IP-адрес интерфейса управления устройства или FQDN.

   > **Примечание.** Разрешение FQDN происходит в соответствии с системными параметрами ОС.

7. Нажмите **Добавить**.

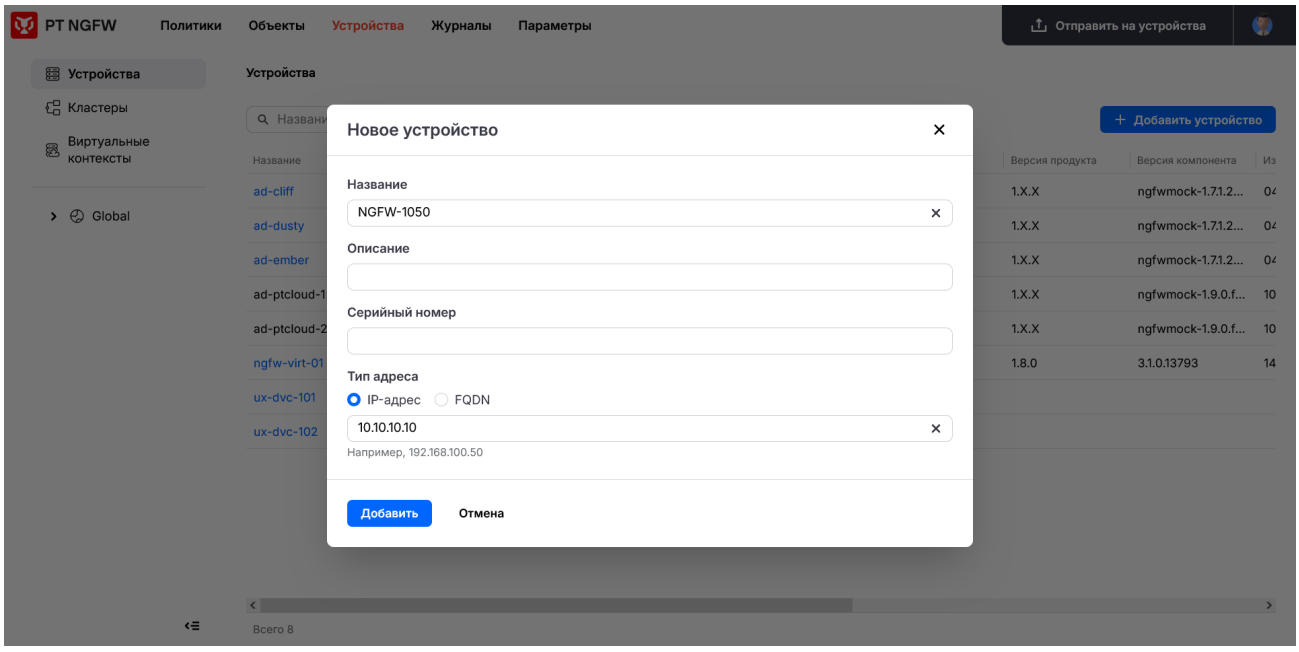


Рисунок 91. Добавление устройства

Сразу после добавления устройство находится в состоянии **Подключение**. В это время система управления подключается к устройству, проверяет совпадение серийного номера и при обнаружении совпадения получает с устройства перечень интерфейсов и их MAC-адресов. Затем устройство переходит в состояние **Подключено**.

Устройство может быть изменено или удалено — в контекстном меню устройства на вкладке **Устройства**.

> **Внимание!** Устройство нельзя удалить, если оно входит в состав кластера. Прежде чем удалить устройство, необходимо исключить его из кластера.

При удалении устройства из системы управления, конфигурация на самом устройстве не сбрасывается. Устройство нельзя удалить, если на нем созданы пользовательские виртуальные контексты.

Настройка MTU для добавленного устройства или кластера

По умолчанию для добавленного устройства устанавливается размер MTU, равный 1500 байт. Это значение наследуется сетевыми интерфейсами, если для них не задано собственное значение. Вы можете изменить размер MTU чтобы оптимизировать передачу данных.

- Чтобы изменить MTU для устройства:

1. Нажмите **Устройства** → **Устройства**, затем выберите название устройства.

   Примечание. Если устройство работает в кластере A/S, нажмите **Устройства** → **Кластеры**, затем выберите название кластера.

2. Выберите **Общие** → **Изменить**.

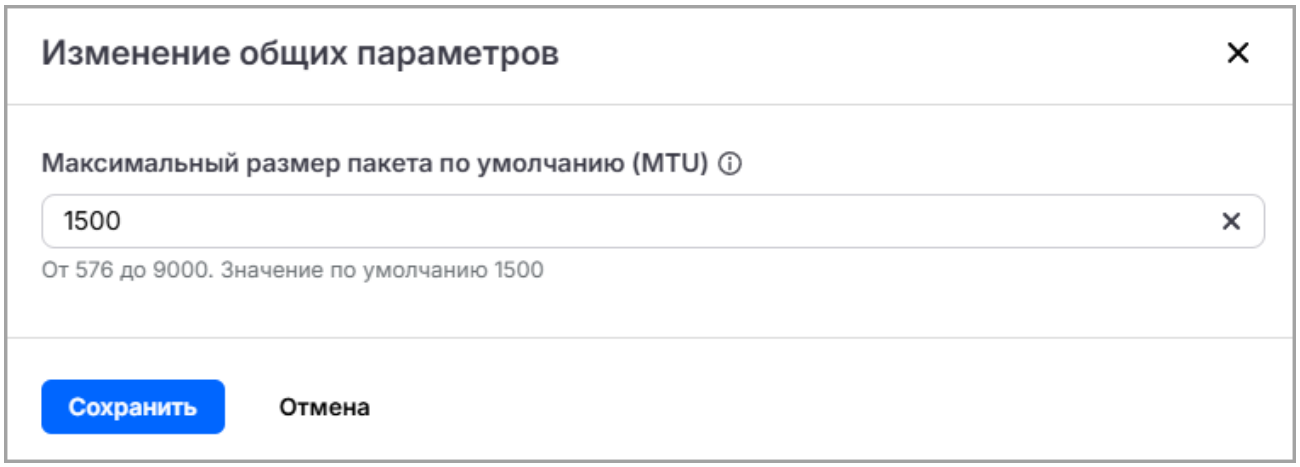


Рисунок 92. Настройка MTU

3. Задайте новое значение MTU в диапазоне от 576 до 9216 байт (до 9000 для виртуального исполнения PT NGFW).
4. Нажмите **Сохранить**.

Внимание! Значения MTU и MSS в сети должны быть согласованы. Иначе в сети могут возникать ошибки, связанные с обработкой фрагментированных IP-пакетов.

13. Настройка сетевых интерфейсов

Настройка сетевых интерфейсов предполагает добавление, изменение или удаление сабинтерфейсов — логических интерфейсов, между которыми осуществляется передача данных. При добавлении сабинтерфейсов физический интерфейс делится на несколько логических. При подключении устройства к системе управления для каждого физического интерфейса автоматически создается один сабинтерфейс, предназначенный для приема и передачи кадров, не имеющих VLAN-метки, и не подлежащий удалению.

Внимание! Привязывание сабинтерфейса к виртуальному роутеру возможно только при добавлении или изменении виртуального роутера.

- Чтобы добавить сабинтерфейс:

1. В главном меню выберите **Устройства**.
2. Выберите устройство, для которого вы хотите добавить сабинтерфейс.
3. Нажмите **Добавить** → **Новый сабинтерфейс**.
4. Выберите физический интерфейс, для которого вы хотите добавить сабинтерфейс.
5. Укажите VLAN-метку, трафик с которой сабинтерфейс должен принимать и отправлять.
6. Если требуется, введите описание сабинтерфейса.
7. Если вы хотите, чтобы сабинтерфейс работал в режиме маршрутизации, укажите IP-адрес сабинтерфейса (или адреса).

   Внимание! Все сабинтерфейсы, состоящие во включенных виртуальных роутерах, должны иметь настроенные IP-адреса, в противном случае установка такой конфигурации на устройство завершится ошибкой.
8. Если вы хотите, чтобы сабинтерфейс работал в режиме vWire или Зеркалирование (расшифрованного трафика), выберите соответствующий режим.
9. Назначьте сабинтерфейсу виртуальный контекст.
10. Назначьте сабинтерфейсу зону безопасности.

    Внимание! Не указывайте в качестве зоны безопасности зону **Local**.
11. По умолчанию значение MTU сабинтерфейса наследуется из устройства (см. раздел 12). Чтобы оптимизировать передачу данных, вы можете изменить размер MTU. Для этого на вкладке **Дополнительные** снимите флажок **Наследуется из устройства** и введите новое значение MTU.

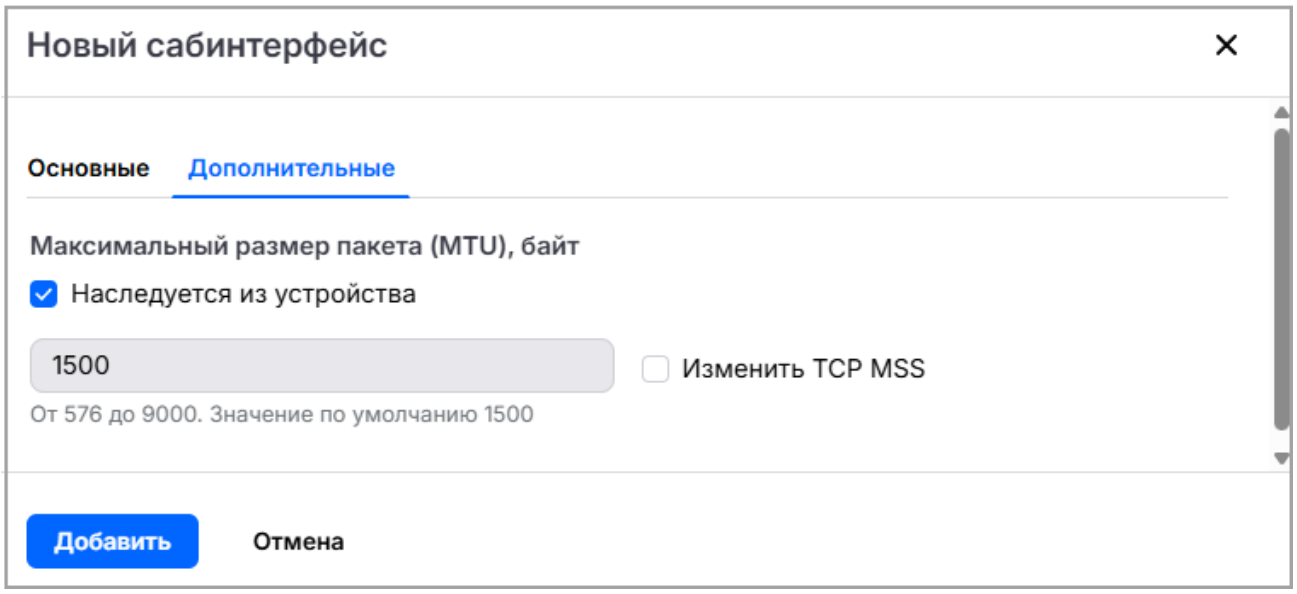


Рисунок 93. Настройка MTU для сабинтерфейса

Примечание. Если требуется автоматическое согласование MSS, установите флажок **Изменить TCP MSS**. При установленном флажке размер MSS будет определяться по формуле: MSS = MTU – 40.

12. Нажмите **Добавить**.

    Сразу после добавления и до применения конфигурации на устройстве сабинтерфейс находится в состоянии **Не применен**.

Примечание. Названия сабинтерфейсов формируются автоматически и соответствуют номеру метки VLAN, трафик которой сабинтерфейс обрабатывает. Например, если сабинтерфейс интерфейса **eth1-1** обрабатывает трафик VLAN 10, то его названием будет **eth1-1.10**. Названия сабинтерфейсов, предназначенных для приема и передачи нетегированных кадров, имеют названия вида <название интерфейса>.0.

Добавленный сабинтерфейс может быть изменен или удален — в контекстном меню сабинтерфейса.

14. Настройка маршрутизации

В разделе прилагаются инструкции по настройке статической и динамической маршрутизации, маршрутизации по политикам (PBR) и связанных функций.

В этом разделе

Статическая маршрутизация (см. раздел 14.1)

Динамическая маршрутизация (см. раздел 14.2)

Маршрутизация по политикам (PBR) (см. раздел 14.3)

Профили проверки доступности (см. раздел 14.4)

BFD (см. раздел 14.5)

14.1. Статическая маршрутизация

Когда PT NGFW работает в режиме маршрутизатора, трафик из одного сабинтерфейса передается в другой в соответствии с информацией в таблице FIB (Forwarding Information Base). Таблица FIB формируется на основе таблицы машрутизации RIB (Routing information base). В RIB попадают маршруты, полученные по протоколам OSPF, BGP, а также статические маршруты, указанные администратором. На основе административной дистанции (AD) выбираются лучшие маршруты, которые заносятся в FIB.

Настройка статической маршрутизации предполагает добавление статических маршрутов.

- Чтобы добавить статический маршрут:

  1. В главном меню выберите **Устройства**.
  2. Выберите устройство, для которого вы хотите добавить маршрут.
  3. Выберите вкладку **Виртуальные контексты**.
  4. Нажмите на название виртуального контекста, для которого вы хотите добавить маршрут.
  5. Выберите вкладку **Виртуальные роутеры**.
  6. Выберите виртуальный роутер, для которого вы хотите добавить маршрут.
  7. Выберите вкладку **Статические маршруты**.
  8. Нажмите **Добавить маршрут**.
  9. Если требуется, отключите маршрут.
  10. В поле **Назначение** укажите сеть, до которой нужен маршрут.

Примечание. Указав в качестве назначения 0.0.0.0/0, вы создадите маршрут по умолчанию. Маршрут по умолчанию используется тогда, когда не найдены более специфичные маршруты к пункту назначения.

11. Если требуется, введите описание маршрута.
12. Укажите IP-адрес шлюза, через который указанная сеть будет доступна, или исходящий интерфейс.

    Примечание. В текущей версии в качестве исходящего интерфейса может быть выбран только туннельный интерфейс (VTI).

13. Если требуется, укажите значение административной дистанции, отличное от значения по умолчанию для статических маршрутов в текущем виртуальном роутере.

    Примечание. Когда установлен флажок **Наследовано из виртуального роутера**, маршрут имеет административную дистанцию, равную административной дистанции по умолчанию для статических маршрутов в виртуальном роутере.

14. Если требуется, выберите BFD-профиль.

    Примечание. Подробнее см. в разделе «BFD (см. раздел 14.5)».

15. Если требуется, выберите профиль проверки доступности.

    Примечание. Подробнее см. в разделе «Профили проверки доступности (см. раздел 14.4)».

16. Нажмите **Создать**.

Маршрут может быть изменен или удален через контекстное меню маршрута на вкладке **Статические маршруты**.

Маршрут с указанием туннельного интерфейса может быть перераспределен в протоколы динамической маршрутизации. При перераспределении в BGP автоматически указывается next-hop-self; при перераспределении в OSPF в качестве forwarding address в LSA 5, 7 автоматически указывается 0.0.0.0 — для того чтобы OSPF-сосед пересылал пакеты до данного узла межсетевого экрана по аналогии с next-hop self.

14.2. Динамическая маршрутизация

Динамическая маршрутизация — это процесс, в ходе которого маршрутизаторы с помощью протокола динамической маршрутизации непрерывно обмениваются информацией и на ее основе заполняют и обновляют свои таблицы маршрутизации. Отличие динамической маршрутизации от статической в том, что при динамической маршрутизации таблица маршрутизации заполняется автоматически, а не вручную. Протоколы динамической маршрутизации бывают внешними (exterior gateway protocols, EGP), к которым относится протокол BGP, и внутренними (interior gateway protocols, IGP), например OSPF или RIP. Внешние протоколы используются для построения маршрутизации в интернете, а внутренние — для маршрутизации во внутренних сетях (например, в корпоративной сети).

PT NGFW поддерживает маршрутизацию по протоколам BGP и OSPF версии 2.

В этом разделе

Настройка OSPF (см. раздел 14.2.1)

Настройка BGP (см. раздел 14.2.2)

Перераспределение маршрутов (см. раздел 14.2.3)

14.2.1. Настройка OSPF

OSPF — это один из протоколов для динамической маршрутизации внутренних сетей (например, корпоративной сети).

Протокол имеет следующий принцип работы:

— Каждый маршрутизатор создает объявление о состоянии каналов (link-state advertisement, LSA) и описывает в нем состояние своих каналов (интерфейсов). Например, объявление маршрутизатора с подключениями только типа «точка — точка» содержит собственный идентификатор маршрутизатора, адреса и маски подключенных сетей, IP-адреса маршрутизатора, идентификаторы маршрутизаторов в подключенных сетях, а также стоимость отправки данных с интерфейса. Маршрутизатор передает объявление своим непосредственно подключенным маршрутизаторам, а те — своим. Таким образом, в каждом устройстве формируется идентичная база данных объявлений (link-state database, LSDB) с информацией о топологии сети.

  Примечание. Тип подключения указывается для каждого интерфейса при настройке маршрутизатора. PT NGFW поддерживает два наиболее часто используемых типа: «точка — точка» и широковещательный. Первый предназначен для использования, когда интерфейс подключается к сети с одним маршрутизатором, второй — с несколькими (посредством коммутатора).

— На основе имеющихся данных маршрутизаторы наполняют свои таблицы маршрутизации, учитывая при этом стоимость отправки данных по каждому из возможных путей к сети назначения для выбора наиболее оптимального пути. Стоимость пути складывается из стоимости отправки данных с интерфейсов, через которые проходит путь. Стоимость отправки данных с определенного интерфейса может быть задана администратором вручную или рассчитана автоматически, исходя из пропускной способности интерфейса. При наличии нескольких возможных путей до целевой сети будет выбран маршрут с минимальной стоимостью.

— При изменениях в состоянии каналов маршрутизатор пересоздает с учетом изменений объявление о состоянии каналов, и оно передается всем остальным устройствам.

Передача объявлений от одного устройства к другому происходит только после установления между ними отношений соседства. Условием установления соседства является совпадение ряда параметров соответствующих интерфейсов: маски сети, версии протокола, интервалов отправки Hello- и Dead-сообщений, типа подключения, идентификатора области и ее типа, типа аутентификации и пароля, а также MTU. Кроме того, оба маршрутизатора должны иметь уникальные идентификаторы (в домене маршрутизации).

Домен маршрутизации (совокупность всех OSPF-маршрутизаторов) может быть разделен на несколько областей для снижения требований к ресурсам сети и маршрутизаторов. Домен должен всегда состоять хотя бы из одной области, а в конфигурации более чем с одной областью включать область с идентификатором 0 или 0.0.0.0 и типом Standard, которая называется магистральной. Любой интерфейс, который должен участвовать в маршрутизации по протоколу OSPF, должен быть привязан к какой-либо области и может быть привязан только к одной области.

Поддержка OSPF в PT NGFW имеет следующие особенности:

— Реализована поддержка OSPF версии 2 в соответствии с RFC 2328.

— Протокол настраивается индивидуально для каждого виртуального роутера.

— Идентификатор маршрутизатора указывается вручную.

— Поддерживается только широковещательный тип подключений и «точка — точка».

— Стоимость отправки данных с интерфейса указывается вручную.

Настройка OSPF в PT NGFW состоит из следующих этапов:

1. Настройка основных параметров (см. раздел 14.2.1) — включение процесса OSPF-маршрутизации в виртуальном роутере и указание идентификатора маршрутизатора.
2. Добавление как минимум одной области (см. раздел 14.2.1), что позволит добавить в нее (привязать к ней) интерфейс маршрутизатора.
3. Добавление интерфейсов в область (см. раздел 14.2.1).
4. Настройка параметров интерфейсов (см. раздел 14.2.1) (типа подключения, стоимости, интервалов отправки Hello- и Dead-сообщений и др.).
5. Настройка аутентификации (см. раздел 14.2.1) — на уровне интерфейса, области или маршрутизатора (если требуется).

Настройка основных параметров

► Чтобы настроить основные параметры маршрутизации OSPF:

1. В главном меню выберите **Устройства**.
2. Выберите устройство, для которого вы хотите выполнить настройку.
3. Выберите вкладку **Виртуальные контексты**.
4. Нажмите на название виртуального контекста, для которого вы хотите выполнить настройку.
5. Выберите вкладку **Виртуальные роутеры**.
6. Выберите виртуальный роутер, для которого вы хотите выполнить настройку.
7. Выберите вкладку **OSPF**.

8. Введите уникальный идентификатор маршрутизатора OSPF в формате IP-адреса (например, 1.1.1.1).
9. Включите OSPF-маршрутизацию.

   Примечание. Один виртуальный роутер поддерживает не более одного процесса OSPF-маршрутизации.
10. Если требуется отключить режим graceful restart, снимите соответствующий флажок.

    Примечание. Graceful restart — режим работы маршрутизатора, позволяющий сохранить состояние маршрутизации на время запланированной перезагрузки OSPF-процесса. Когда режим включен, маршрутизатор в момент перезагрузки OSPF-процесса уведомляет непосредственно подключенные устройства о том, что будет недоступен в течение определенного времени. Сохранение маршрутизации возможно, только если на соседних устройствах включен режим graceful restart helper и во время перезагрузки не изменяется LSDB.

    Примечание. Режим graceful restart работает только внутри кластера. Режим помощника graceful restart работает как внутри кластера, так и на отдельном (некластерном) устройстве. Подробнее см. в разделе «Graceful restart (OSPF, BGP) (см. раздел 30.6)».
11. Если требуется, укажите grace-период в секундах.

    Примечание. Указанное значение объявляется соседнему маршрутизатору-помощнику. Определяет ожидаемую длительность перезапуска узла PT NGFW и время (в секундах), в течение которого маршрутизатор-помощник должен сохранять маршруты и OSPF LSA от межсетевого экрана, необходимые для пересылки трафика.
12. Если требуется включить режим помощника (graceful restart helper), установите соответствующий флажок.

    Примечание. В этом режиме межсетевой экран продолжает пересылку трафика, не разрывает OSPF-соседство и содействует перезапускающемуся соседнему маршрутизатору, который использует механизм graceful restart.
13. Нажмите **Создать**.

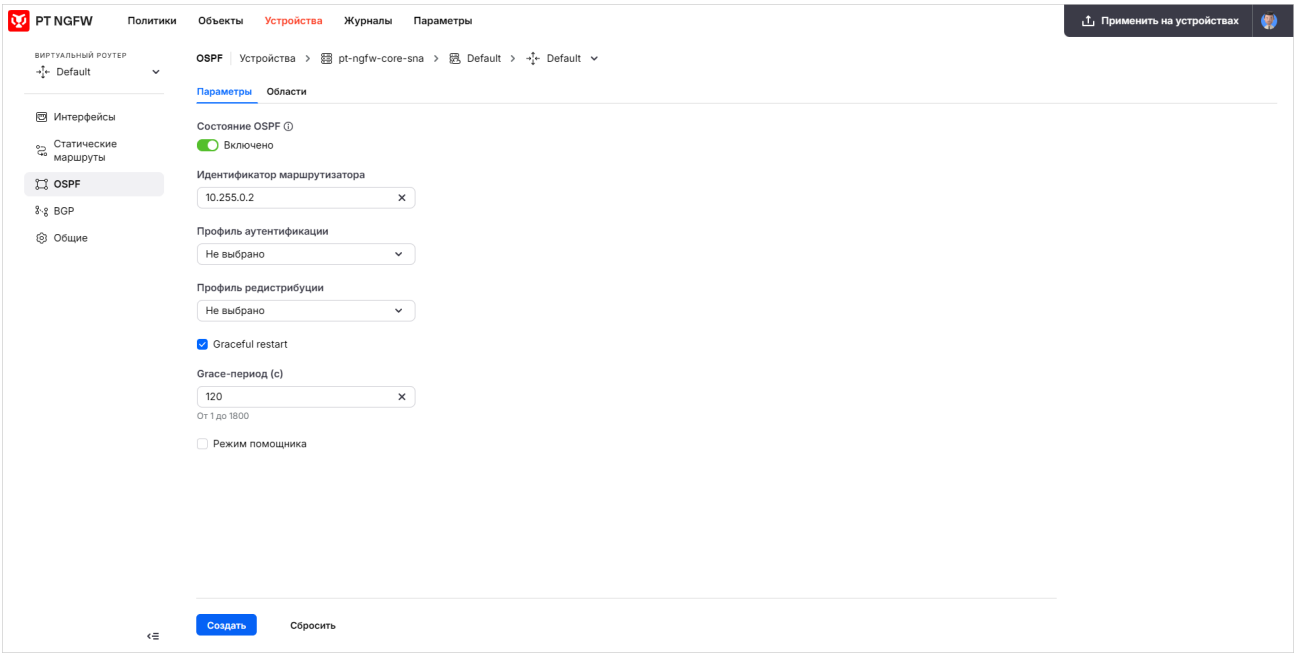


Рисунок 94. Настройка основных параметров OSPF

Добавление области

Область (area) — это совокупность сетевых интерфейсов с одинаковым идентификатором области. Идентификатор должен быть присвоен любому интерфейсу для его участия в OSPF-маршрутизации. Маршрутизаторы могут взаимодействовать, только если соответствующие интерфейсы привязаны к одной области (имеют одинаковый идентификатор). Один маршрутизатор может иметь интерфейсы, привязанные к разным областям. Конфигурация более чем с одной областью должна включать область с идентификатором 0 и типом Standard, которая называется магистральной. С магистральной областью посредством пограничного маршрутизатора (area border router, ABR) должна быть соединена любая другая область — для предотвращения петель маршрутизации.

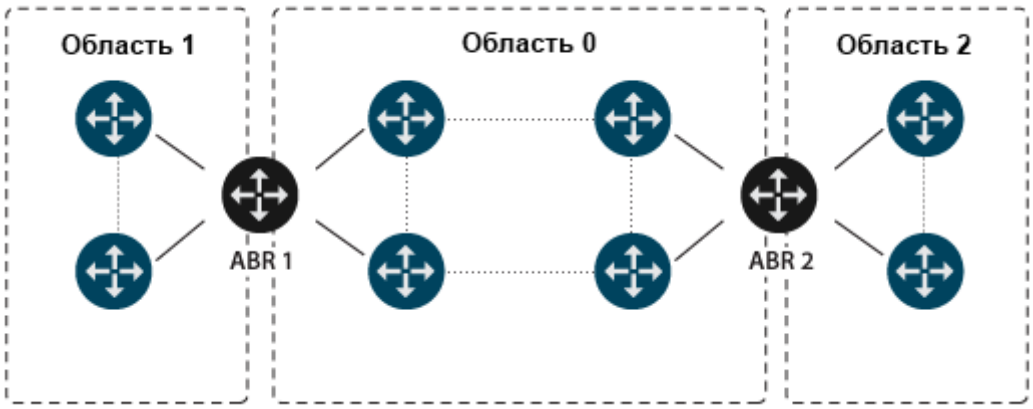


Рисунок 95. Пример разделения сети на области

При разделении домена маршрутизации на области маршрутизаторам, принадлежащим к одной области, неизвестна подробная информация о топологии других областей. Разделение на области позволяет:

— уменьшить размер таблиц маршрутизации за счет суммирования маршрутов на границах областей;

— уменьшить размер базы данных объявлений (LSDB) и, следовательно, потребление устройством оперативной памяти: каждая область имеет свою базу данных, в которой не содержатся объявления первого и второго типов (LSA 1—2) из других областей;

Примечание. Когда у маршрутизатора есть интерфейсы в нескольких областях, у него есть несколько баз данных (по одной на область).

— снизить требования к ресурсам маршрутизаторов за счет уменьшения количества расчетов по алгоритму SPF.

Добавление области производится на странице виртуального роутера (на вкладке **OSPF**).

► Чтобы добавить область:

1. Выберите вкладку **Области**.
2. Нажмите **Добавить область**.
3. Если вы хотите добавить магистральную область, установите соответствующий флажок.
4. Если вы хотите добавить немагистральную область, введите в формате IP-адреса ее идентификатор (например, 0.0.0.1) и выберите тип.

   Примечание. Маршрутизаторы могут стать соседями только в том случае, если идентификатор и тип области соответствующих интерфейсов совпадают.
5. Если вы хотите добавить область типа Stub и запретить в ней любые LSA третьего типа (Summary LSA), кроме маршрута по умолчанию, выберите соответствующий тип и установите флажок **no-summary**.

   Примечание. Этот шаг следует выполнять только на пограничном маршрутизаторе (ABR).
6. Если вы хотите добавить область типа NSSA, распространить в области маршрут по умолчанию, используя LSA третьего типа, и запретить в ней все LSA третьего типа, кроме маршрута по умолчанию, выберите соответствующий тип и установите флажок **no-summary**.

   Примечание. Этот шаг следует выполнять только на пограничном маршрутизаторе (ABR).
7. Если вы хотите добавить область типа NSSA и распространить в ней маршрут по умолчанию, используя LSA седьмого типа, выберите соответствующий тип области, установите флажок **nssa default-information originate** и укажите тип метрики и метрику (стоимость маршрута).
8. Нажмите **Добавить**.

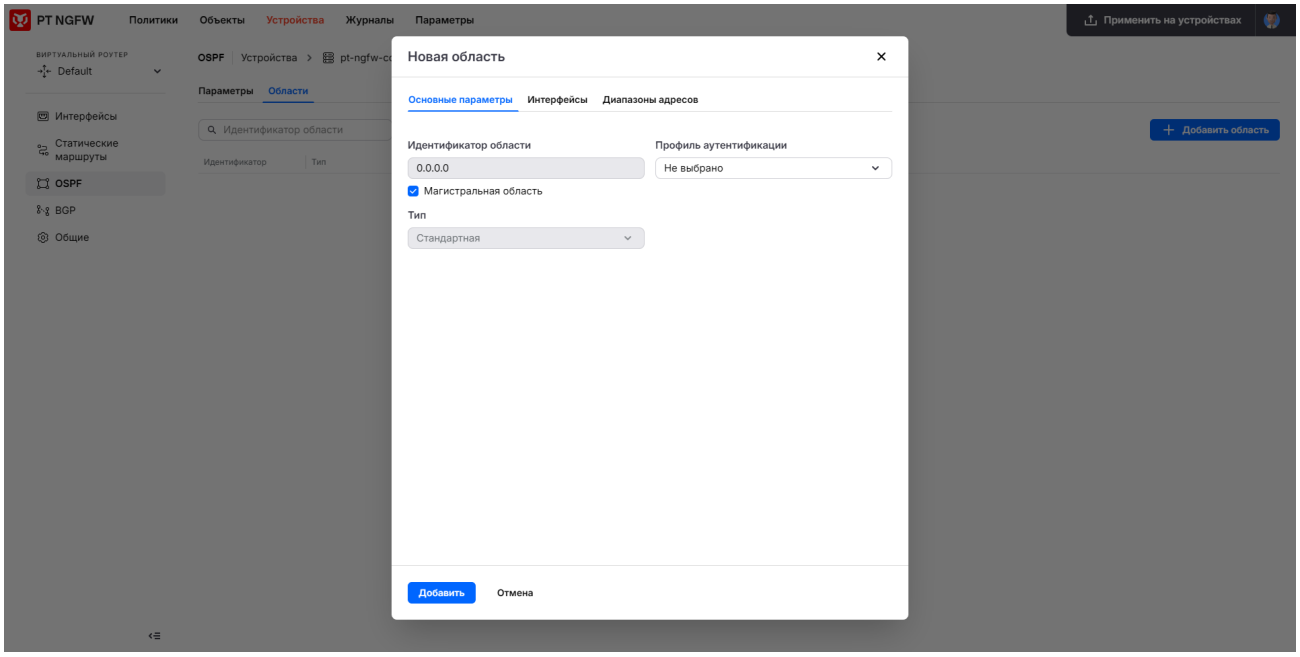


Рисунок 96. Добавление области

Добавление интерфейса в область

Перед добавлением интерфейса в область необходимо добавить область.

> **Примечание.** Добавление интерфейса в область производится на странице виртуального роутера (на вкладке **OSPF**).

- Чтобы добавить интерфейс в область OSPF:

1. Выберите вкладку **Области**.
2. Выберите область.
3. Выберите вкладку **Интерфейсы**.
4. Нажмите **Добавить интерфейс**.
5. Установите флажок напротив каждого сабинтерфейса, который вы хотите добавить.
6. Нажмите **Добавить**.

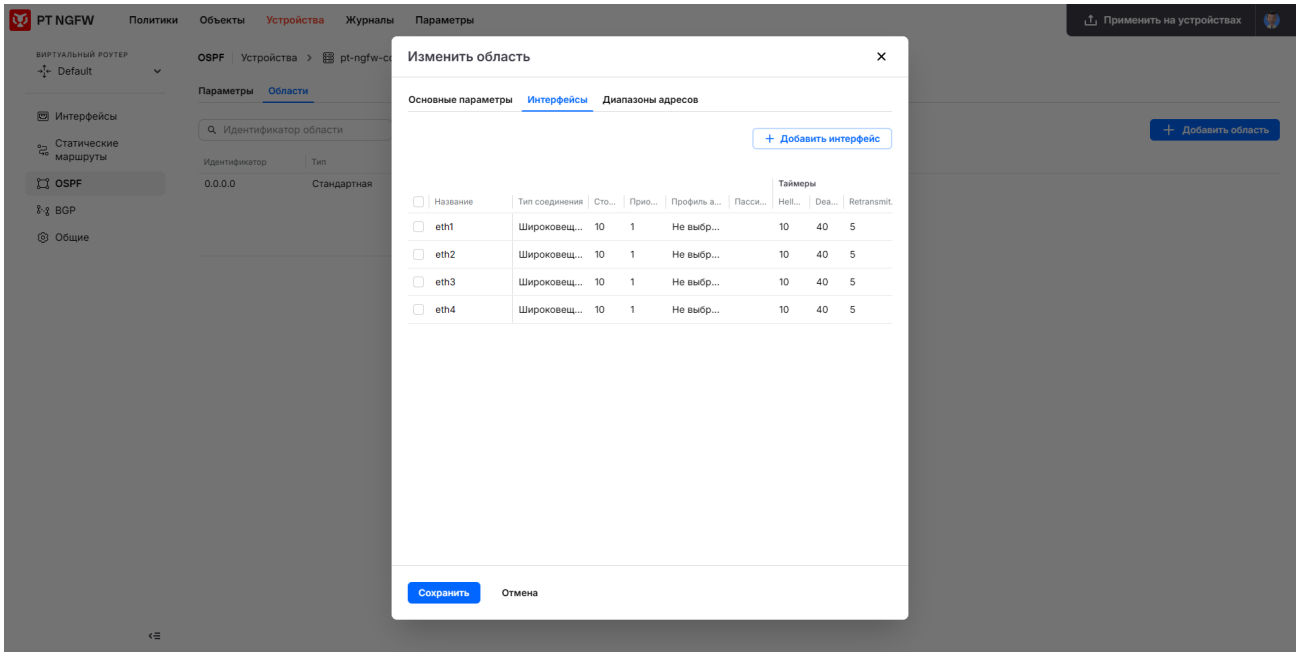


Рисунок 97. Добавление интерфейсов в область

Настройка суммирования

Если маршрутизатор является пограничным (ABR) (имеет интерфейсы в разных областях), то вы можете настроить суммирование сетей — вместо передачи множества LSA третьего типа (по одному на сеть) пограничный маршрутизатор будет передавать LSA третьего типа с суммированной сетью. Передача LSA с суммированной сетью будет производиться, только если существует хотя бы одна сеть, входящая в суммированную. Использование механизма суммирования позволяет уменьшить нагрузку на процессор и память маршрутизаторов. Настройка суммирования выполняется путем добавления диапазона адресов на странице виртуального роутера (на вкладке **OSPF**).

- Чтобы настроить суммирование маршрутов:

  1. Выберите вкладку **Области**.
  2. Выберите область, для которой вы хотите выполнить настройку.
  3. Выберите вкладку **Диапазоны адресов**.
  4. Нажмите **Добавить диапазон**.
  5. Укажите суммированную сеть.

     Примечание. Стоимость суммированной сети будет равна стоимости вложенной сети с наибольшей стоимостью.

  6. Если вы хотите, чтобы суммированная сеть и любые вложенные исключались из рассылки, выберите действие **Не объявлять**.
  7. Нажмите **Добавить**.

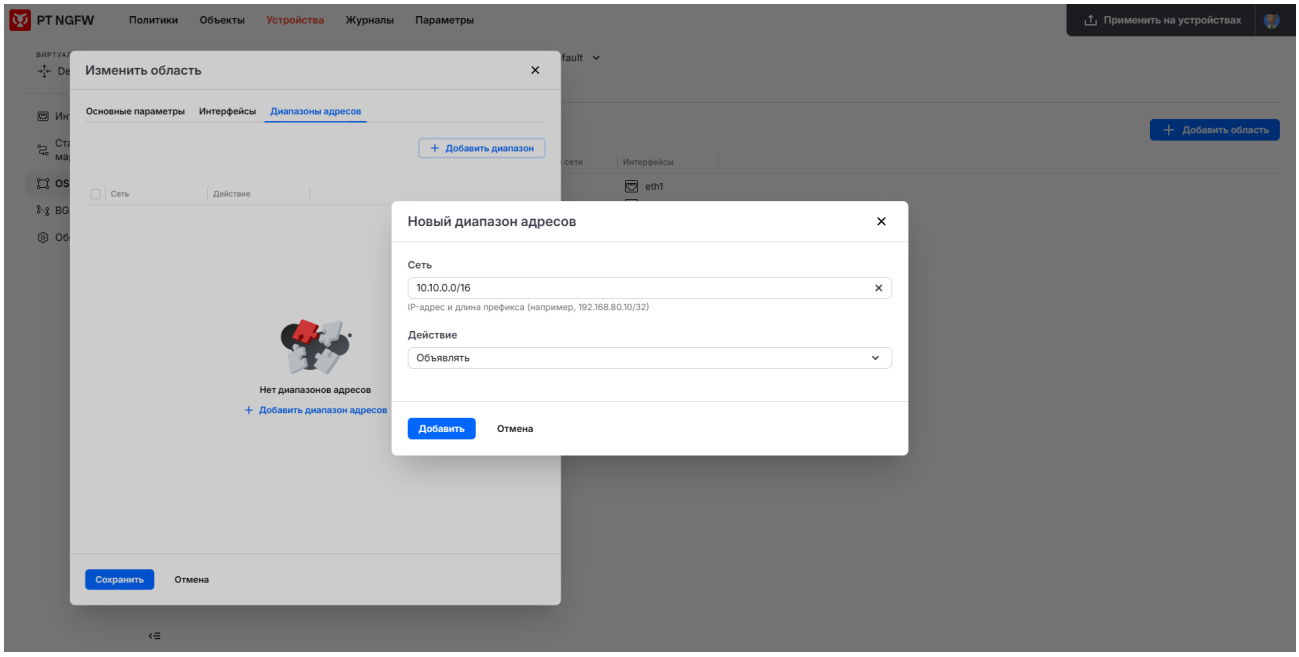


Рисунок 98. Настройка суммирования

Настройка параметров интерфейса

Настройка параметров интерфейса производится на странице виртуального роутера (на вкладке **OSPF**).

- Чтобы настроить параметры интерфейса:

1. Выберите вкладку **Области**.
2. Выберите область.
3. Выберите вкладку **Интерфейсы**.
4. В контекстном меню интерфейса выберите **Изменить**.
5. Если требуется, включите пассивный режим.

   Примечание. В пассивном режиме интерфейс не формирует отношения соседства, поскольку не отправляет Hello-сообщения. Рекомендуется использовать в тупиковых сетях (не имеющих других маршрутизаторов).

6. Если требуется, выберите тип соединения, отличный от широковещательного.

   Примечание. Используйте тип «точка — точка», если интерфейс подключается к сети с одним маршрутизатором, или широковещательный , если с несколькими (посредством коммутатора).

7. Если требуется, укажите приоритет интерфейса, отличный от 1.

Примечание. Чем выше приоритет, тем выше вероятность того, что маршрутизатор будет выбран в роли выделенного (DR) или резервного выделенного маршрутизатора (BDR). Приоритет 0 означает, что маршрутизатор не будет выбран ни в одной роли.

8. Если требуется, укажите стоимость отправки данных с интерфейса, отличную от 10.
9. Если требуется, в раскрывающемся списке **Профиль BFD** выберите BFD-профиль.

   Примечание. Подробнее см. в разделе «Поддержка BFD».
10. Если требуется, в поле **Hello-интервал** введите интервал отправки устройством Hello-сообщений, отличный от 10 секунд.

    Примечание. Маршрутизаторы становятся соседями, только если интервалы отправки Hello-сообщений соответствующих интерфейсов совпадают.
11. Если требуется, в поле **Dead-интервал** введите время, отличное от 40 секунд, по истечении которого отношения с соседним маршрутизатором будут разорваны, если от него не было получено Hello-сообщение.

    Примечание. Маршрутизаторы становятся соседями, только если соответствующие интерфейсы имеют одинаковый Dead-интервал.
12. Если требуется, в поле **Retransmit-интервал** введите время между повторными передачами LSA-сообщений, отличное от 5 секунд.

    Примечание. Маршрутизатор передает LSA повторно, когда не получает сообщение LSAck.
13. Если требуется, в поле **Задержка передачи** укажите примерное время, требуемое для передачи LSA, отличное от 1 секунды.

    Примечание. Каждое LSA имеет возраст, увеличивающийся на 1 в секунду, но во время передачи он не меняется. Указанное в поле значение будет добавлено к возрасту LSA перед его отправкой. Изменение значения по умолчанию может потребоваться для очень медленных соединений.
14. Если требуется, исключите интерфейс из OSPF-маршрутизации.
15. Нажмите **Сохранить**.

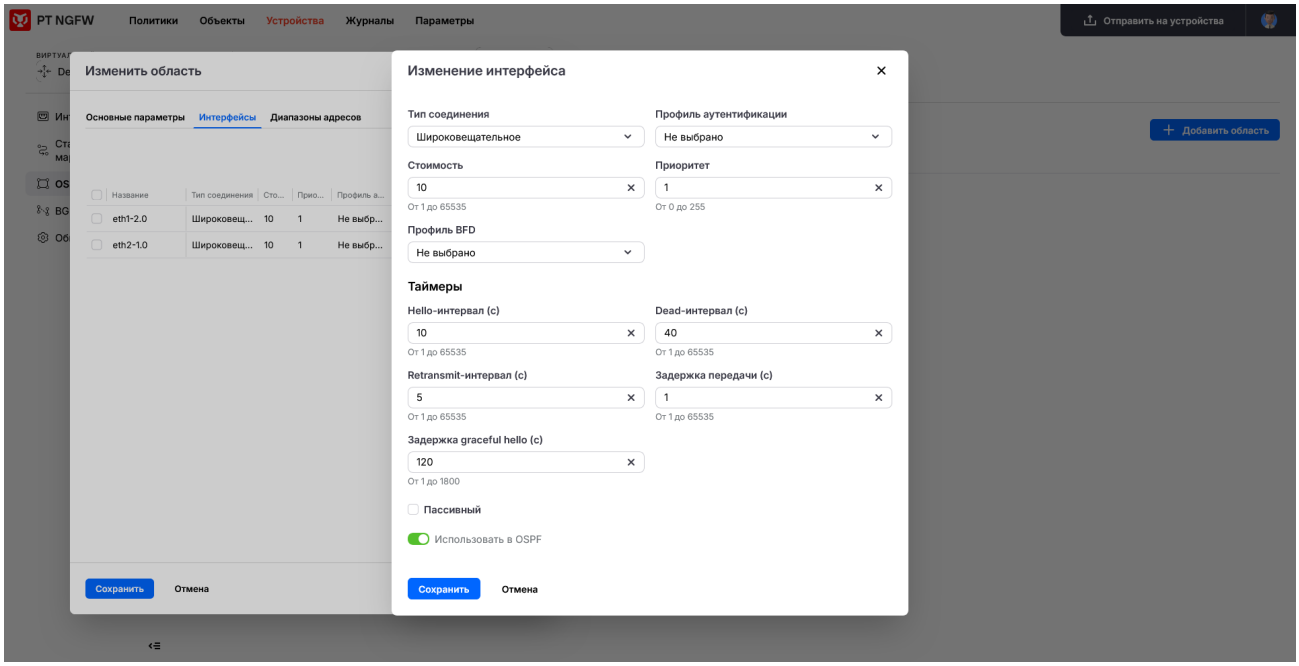


Рисунок 99. Настройка параметров интерфейса

Настройка аутентификации

Маршрутизаторы, работающие по протоколу OSPF, принимают маршрутную информацию только от маршрутизаторов с теми же параметрами аутентификации. Аутентификация используется для защиты сети от злоумышленников, рассылающих ложную маршрутную информацию с целью обмануть устройства и получить возможность перехвата и модификации данных или просто нарушить работу сети. Аутентификация может быть настроена для интерфейса, области или маршрутизатора через добавление профиля аутентификации и назначения его интерфейсу, области или маршрутизатору. Более специфичная настройка аутентификации имеет приоритет над менее специфичной: настройка аутентификации для области переопределяется таковой для интерфейса, но имеет приоритет над настройкой на уровне маршрутизатора.

Поддерживаются три типа аутентификации:

— Парольная. При такой аутентификации пароль передается по сети в виде открытого текста.

— MD5. При такой аутентификации передается хеш-сумма содержимого OSPF-пакета и пароля, идентификатор ключа, состоящего из пароля и идентификатора, и неубывающий порядковый номер. Получатель OSPF-пакета должен иметь ключ с тем же идентификатором и паролем. Возможна смена пароля без потери соседства путем добавления второго ключа на обоих устройствах и последующего удаления старых ключей.

— Keychain — тип аутентификации, отличающийся от предыдущего поддержкой HMAC-SHA и возможностью установить время, в течение которого устройство должно принимать и отправлять пакеты с определенным ключом.

- Чтобы добавить профиль аутентификации:

  1. В главном меню выберите **Устройства**.
  2. Выберите устройство, в котором находится виртуальный роутер.
  3. Выберите вкладку **Виртуальные контексты**.
  4. Нажмите на название виртуального контекста, в котором находится виртуальный роутер.
  5. Выберите вкладку **Профили OSPF**.
  6. Нажмите **Добавить профиль**.
  7. Введите название профиля.
  8. Если требуется, введите описание.
  9. Выберите тип аутентификации.
  10. Укажите пароль или добавьте один или несколько ключей.
  11. Нажмите **Сохранить**.

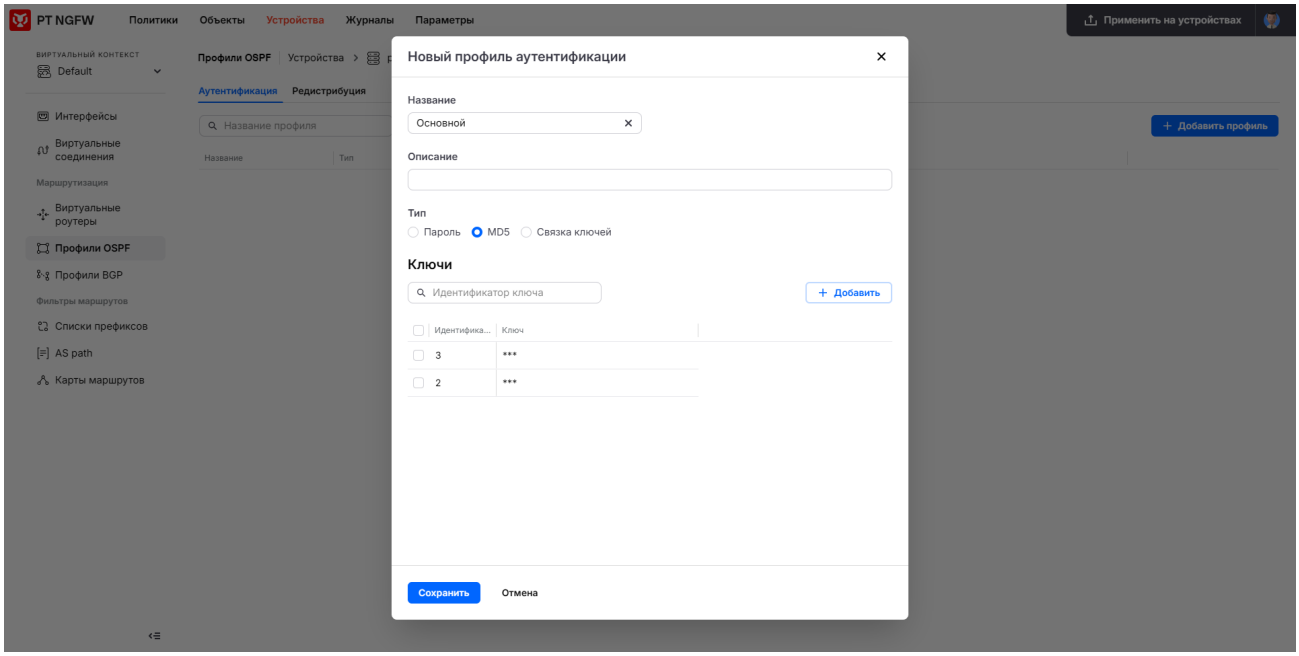


Рисунок 100. Добавление профиля аутентификации

- Чтобы назначить профиль аутентификации интерфейсу,

  выберите профиль на странице настройки OSPF-параметров интерфейса.

- Чтобы назначить профиль аутентификации области,

  выберите профиль на странице настройки области.

► Чтобы назначить профиль аутентификации маршрутизатору,

выберите профиль на странице виртуального роутера (на вкладке **OSPF**).

14.2.2. Настройка BGP

BGP — протокол динамической маршрутизации, предназначенный для обмена информацией между автономными системами. После установки соединения BGP-маршрутизатор передает пирам (соседним маршрутизаторам) информацию о маршрутах, предназначенных для экспорта. На основе полученной информации пиры выбирают лучшие маршруты и вносят их в свои таблицы маршрутизации.

Маршрутизация BGP имеет следующие особенности:

— BGP включается глобально для маршрутизатора, а не каждого интерфейса (как, например, в OSPF);

— для установления отношений соседства сосед настраивается вручную;

— BGP функционирует поверх протокола транспортного уровня TCP (порт 179);

— обновления отправляются только после изменений в сети (нет периодических обновлений);

— по умолчанию BGP отправляет keepalive-сообщения каждые 60 секунд;

— в таблице BGP хранятся все известные маршруты, а в таблице маршрутизации — лучшие;

— лучший маршрут выбирается на основании набора поочередно сравниваемых атрибутов пути (path attributes), которые можно гибко изменять политиками маршрутизации;

— протокол позволяет обмениваться информацией о маршрутах внутри одной автономной системы (такой вариант использования BGP называется внутренним — iBGP) и между различными автономными системами (внешний BGP, eBGP).

В PT NGFW BGP настраивается индивидуально для каждого виртуального роутера. Для начала настройки потребуется выбрать виртуальный роутер и на вкладке **BGP** включить BGP-маршрутизацию. Дальнейшие шаги включают настройку основных параметров BGP-маршрутизации, добавление одного или нескольких пиров, настройку анонсирования сетей и (или) редистрибуции.

В PT NGFW для обмена маршрутными сообщениями установка фильтров не является обязательной.

Настройка основных параметров

► Чтобы настроить основные параметры BGP-маршрутизации:

1. В главном меню выберите **Устройства**.
2. Выберите устройство, для которого вы хотите выполнить настройку.
3. Выберите вкладку **Виртуальные контексты**.

4. Нажмите на название виртуального контекста, для которого вы хотите выполнить настройку.
5. Выберите вкладку **Виртуальные роутеры**.
6. Выберите виртуальный роутер, для которого вы хотите выполнить настройку.
7. Выберите вкладку **BGP**.
8. Включите BGP-маршрутизацию.
9. Введите в форме IP-адреса уникальный идентификатор маршрутизатора BGP (например, 1.1.1.1).
10. Введите номер локальной автономной системы (автономной системы виртуального роутера).
11. Если требуется, укажите в форме IP-адреса идентификатор RR-кластера.
12. Если требуется, настройте следующие параметры:
    - **Проверять номер первой AS** — отбрасывать сообщение Update, полученное от внешнего узла BGP (eBGP), если тот не указал номер своей автономной системы в начале атрибута AS path;
    - **Всегда сверять MED** — сравнивать атрибут MED маршрутов, полученных из разных автономных систем (по умолчанию сравнение происходит только для маршрутов из одной и той же автономной системы);
    - **Детерминированный MED** — рассчитывать лучший маршрут среди соседей из одной AC до сравнения с маршрутами из других AC;
    - **Graceful shutdown** — используется для минимизации или устранения потерь трафика в сети при проведении планового технического обслуживания маршрутизатора;
    - **Локальное предпочтение по умолчанию** — применяется для маршрутов, не имеющих атрибута local preference.
13. Если требуется, включите режим graceful restart и настройте параметры его работы:
    - **Restart-таймер** — указанное значение объявляется соседнему маршрутизатору-помощнику. Оно определяет ожидаемую длительность перезапуска узла PT NGFW и время (в секундах), в течение которого маршрутизатор-помощник должен сохранять маршруты от PT NGFW, необходимые для пересылки трафика;
    - **Stale-path-таймер** — максимальное время удержания устаревших путей перезагружаемого пира (в секундах). Команда актуальна, если межсетевой экран работает в режиме помощника graceful restart;
    - **Deferral-таймер** — время, по истечении которого новый активный узел кластера выполнит выбор маршрутов на основании данных, полученных от маршрутизатора-помощника, в случае если узел кластера не получил от него сообщение BGP End-of-RIB (в секундах).

Примечание. Режим graceful restart работает только внутри кластера. Режим помощника graceful restart работает как внутри кластера, так и на отдельном (некластерном) устройстве. Подробнее см. в разделе «Graceful restart (OSPF, BGP) (см. раздел 30.6)».

Примечание. При включении режима graceful restart автоматически включается режим помощника (graceful restart helper).

14. Нажмите **Сохранить**.

Добавление пира

Добавление пира позволяет установить отношения соседства в целях обмена маршрутной информацией. При добавлении пира вы можете указать профиль фильтрации, позволяющий производить фильтрацию входящих и исходящих маршрутов в отношении этого пира, и профиль аутентификации. Добавление пира производится на странице виртуального роутера (вкладке **BGP**).

- Чтобы добавить пир:

1. Выберите вкладку **Пиры**.
2. Нажмите **Добавить пир**.
3. Если требуется, отключите пир.
4. Введите название пира.
5. Введите номер удаленной автономной системы (автономной системы пира).
6. Выберите сабинтерфейс, предназначенный для связи с пиром, и IP-адрес из назначенных сабинтерфейсу адресов.
7. Введите IP-адрес пира.
8. Если требуется, выберите профиль фильтрации.
9. Если требуется, выберите профиль аутентификации.
10. Если требуется, выберите BFD-профиль.

    Примечание. Подробнее см. в разделе «Поддержка BFD».

11. Если требуется, настройте таймеры:

    - **Keepalive-интервал** — интервал времени между отправкой сообщений keepalive (в секундах);
    - **Hold-time-интервал** — интервал времени, по истечении которого пир будет считаться недоступным (в секундах);
    - **Reconnect-интервал** — интервал времени, контролирующий время ожидания BGP между попытками подключения к пиру (в секундах);

- **Задержка сообщения Open** — интервал времени для задержки между открытием TCP-соединения с пиром и отправкой первого сообщения BGP Open для установления BGP-соединения (в секундах);
- **Advertisement-интервал** — интервал времени (минимальное время), которое должно пройти между двумя последовательными сообщениями Update (в секундах).

12. Если требуется, настройте дополнительные параметры:

- **Вес (weight)** — вес по умолчанию для маршрутов пира;

  Примечание. Вес имеет только локальное значение (в пределах маршрутизатора) и не передается в обновлениях. Чем больше вес, тем предпочтительнее маршрут.

- **Multihop** — позволяет устанавливать сессии с соседями eBGP, если они находятся на расстоянии нескольких прыжков;
- **Next hop self** — позволяет менять адрес следующего узла (next hop) на свой при передаче маршрута;

  Примечание. Значение **Нет** означает отключение функции, **Self** — адрес локального BGP-маршрутизатора будет установлен в качестве next-hop для анонсируемых маршрутов, полученных через eBGP, **Self force** — значение next-hop будет принудительно перезаписываться для маршрутов, изученных через eBGP и iBGP.

- **Отправка Community** — позволяет отправить пиру атрибут community;
- **Неизменяемый атрибут** — атрибуты, которые должны оставаться неизменными для объявлений, отправляемых пиру;
- **Клиент отражателя маршрутов** — позволяет сделать пира клиентом отражателя маршрутов;
- **Мягкая реконфигурация** — исключает необходимость в сбросе сессии после обновления параметров пира;
- **Перезапись номера AS** — в объявлениях, отправляемых пиру, в атрибуте AS path заменять номер АС пира на номер локальной АС;
- **Максимальное количество префиксов** — максимально допустимое количество префиксов, принятых от пира (после возможной фильтрации);
- **Форсирование макс. количества префиксов** — учитывать все префиксы, а не только принятые;
- **Объявление маршрута по умолчанию** — объявлять маршрут по умолчанию при соблюдении условий карты маршрутов.

13. Нажмите **Сохранить**.

Пир может быть удален или изменен — в контекстном меню пира на вкладке **Пиры**.

Добавление профиля фильтрации

Вы можете добавить профиль фильтрации, чтобы применять фильтры маршрутов к определенному пиру. Профиль может содержать фильтр на основе AS path, список префиксов и карту маршрутов. Один профиль фильтрации может быть назначен сразу нескольким пирам и пирам разных виртуальных роутеров. Порядок фильтрации для входящего трафика — карта маршрутов, фильтр AS path, список префиксов, для исходящего — список префиксов, фильтр AS path, карта маршрутов. Если в результате проверки одним из фильтров маршрут разрешается, он проверяется следующим фильтром. Добавление профиля производится на странице виртуального контекста.

- Чтобы добавить профиль фильтрации:

  1. Выберите вкладку **Профили BGP**.
  2. Нажмите **Добавить профиль**.
  3. Введите название профиля.
  4. Если требуется, введите описание.
  5. Выберите фильтры.
  6. Нажмите **Сохранить**.

Профиль фильтрации может быть изменен или удален — в контекстном меню профиля на вкладке **Профили BGP**.

> **Примечание.** Вы можете назначить профиль фильтрации пиру при добавлении или изменении пира.

Добавление списка префиксов

Список префиксов представляет собой список разрешенных или запрещенных сетей, который обрабатывается последовательно. При получении или отправке информации о сети, точно соответствующей записи в списке, прохождение информации разрешается или запрещается (в зависимости от указанного действия), и проверка на соответствие оставшимся записям списка не выполняется.

> **Внимание!** В конце списка префиксов находится неотображаемая запись, запрещающая любые сети.

Добавление списка производится на странице виртуального контекста. Для применения списка префиксов его необходимо добавить в профиль фильтрации и назначить профиль фильтрации пиру.

- Чтобы добавить список префиксов:

  1. Выберите вкладку **Списки префиксов**.
  2. Нажмите **Добавить список префиксов**.
  3. Введите название списка.

4. Если требуется, введите описание.
5. Добавьте правило (запись), указав значения следующих параметров:
   - **Порядковый номер** — правило с меньшим порядковым номером будет всегда располагаться выше правила с большим порядковым номером, и, соответственно, проверка на соответствие правилу с меньшим порядковым номером будет происходить раньше;
   - **Действие** — разрешить или запретить сеть;
   - **Сеть** — адрес сети и длина префикса;
   - **Длина префикса (необязательный параметр)** — диапазон допустимых длин префиксов у маршрута (например, при указании сети 10.0.0.0/8 и 11 в качестве значения параметра LE будут разрешены или запрещены сети, у которых первый октет равен 10, а длина префикса находится в диапазоне 8—11).
6. Нажмите **Сохранить**.

Список префиксов может быть изменен или удален — в контекстном меню списка на вкладке **Списки префиксов**.

Добавление фильтра AS path

Фильтр AS path позволяет управлять обновлениями маршрутизации на основе пути автономной системы. Например, вы можете запретить обновление, исходящее из определенной автономной системы или проходящее через нее. Фильтр состоит из правил, и при прохождении обновления через фильтр, обновление проверяется на соответствие каждому из правил, начиная с первого правила. Когда соответствие обнаружено, обновление в зависимости от действия правила разрешается или запрещается и проверка остальными правилами фильтра не происходит.

> **Внимание!** В конце фильтра AS path находится неотображаемое правило, запрещающее прохождение любых обновлений.

Добавление фильтра производится на странице виртуального контекста. Для применения фильтра его необходимо добавить в профиль фильтрации и назначить профиль фильтрации пиру.

► Чтобы добавить фильтр AS path:

1. Выберите вкладку AS path.
2. Нажмите **Добавить фильтр AS path**.
3. Введите название фильтра.
4. Если требуется, введите описание.
5. Добавьте правило, указав значения следующих параметров:

- **Порядковый номер** — правило с меньшим порядковым номером будет всегда располагаться выше правила с большим порядковым номером, и, соответственно, проверка на соответствие правилу с меньшим порядковым номером будет происходить раньше;
- **Действие** — разрешить или запретить обновление;
- **Регулярное выражение** — используется для фильтрации информации в атрибуте AS path.

  Примечание. Примеры регулярных выражений: _67$ — маршруты отправленные из АС 67, _67_ — маршруты проходящие через АС 67, ^67$ — маршруты из непосредственно присоединенной АС 67.

6. Нажмите **Сохранить**.

Фильтр AS path может быть изменен или удален — в контекстном меню фильтра на вкладке **AS path**.

Добавление карты маршрутов

Карта маршрута состоит из списка правил; каждое правило позволяет разрешить или запретить маршрут, соответствующий условиям правила, и дополнительно изменить информацию, связанную с маршрутом. Проверка маршрута на соответствие правилу происходит начиная с первого правила в списке. Когда соответствие обнаружено, маршрут в зависимости от действия правила разрешается или запрещается и проверка остальными правилами карты не происходит.

Внимание! В конце карты маршрутов находится неотображаемое правило, запрещающее прохождение любых маршрутов.

Добавление карты маршрутов производится на странице виртуального контекста. Для применения карты ее необходимо добавить в профиль фильтрации и назначить профиль фильтрации пиру.

► Чтобы добавить карту маршрутов:

1. Выберите вкладку **Карты маршрутов.**
2. Нажмите **Добавить карту**.
3. Введите название карты.
4. Если требуется, введите описание.
5. Выберите тип (назначение) карты маршрутов (**Фильтрация**).
6. Нажмите **Добавить**, чтобы добавить правило.
7. Укажите основные параметры правила.

   Примечание. Правило с меньшим порядковым номером будет всегда располагаться выше правила с большим порядковым номером, и, соответственно, проверка на соответствие правилу с меньшим порядковым номером будет происходить раньше.

8. Если требуется, укажите условия для выполнения действия.
9. Если требуется, укажите атрибуты маршрута.
10. Сохраните изменения.

Карта маршрутов может быть изменена или удалена — в контекстном меню карты на вкладке **Карты маршрутов**.

Добавление списков сообществ BGP (BGP community lists)

С помощью списков сообществ BGP (BGP community lists) вы можете разрешать или запрещать маршруты с определенными сообществами, включая использование регулярных выражений. Сообщества BGP подразделяются на 3 типа: обычный (standard), расширенный (extended) и большой (large). Для каждого из типов можно задать значение в двух форматах: стандартном и развернутом. Список сообществ BGP организован как список последовательных записей и состоит из порядкового номера, действия (разрешить или отклонить) и значения. Список сообществ можно указать в карте маршрутов в качестве условия выполнения действия.

Добавление списков сообществ BGP производится на странице виртуального контекста.

► Чтобы добавить список сообществ BGP:

1. Выберите вкладку **Списки сообществ** (**Community lists**).
2. Нажмите **Добавить**.
3. Введите название списка.
4. Если требуется, введите описание.
5. Выберите тип.
6. Выберите формат.
7. Добавьте правило, указав значения следующих параметров:
   - **Порядковый номер** — правило с меньшим порядковым номером будет всегда располагаться выше правила с большим порядковым номером, и, соответственно, проверка на соответствие правилу с меньшим порядковым номером будет происходить раньше;
   - **Действие** — разрешить или запретить маршрут;
   - Значение или регулярное выражение (в зависимости от выбранного типа и формата).

Фильтр по спискам сообществ может быть изменен или удален — в контекстном меню фильтра на вкладке **Списки сообществ** (**Community lists**).

Таблица 9. Типы BGP communities

Тип	Формат	Компоненты и их описание	Примеры корректных значений	Примеры некорректных значений
Обычный (Standard)	AS:VAL	AS и VAL — 16-битные беззнаковые целые числа (допустимый диапазон от 0 до 65535). Оба числа должны быть разделены одним двоеточием	`1234:5678`	`70000:10` — превышение допустимого значения для AS; `10:20:30` — нарушение структуры, лишний компонент
Расширенный (Extended)	TYPE SOURCE:VALUE	TYPE — тип атрибута, допустимые значения: — rt — Route Target; — nt — Node Target; — soo — Site of Origin; — color — Color. SOURCE — идентификатор источника, который может быть: — AS-номером (16-битное беззнаковое целое число, допустимый диапазон от 0 до 65535); — IP-адресом. VALUE — числовое значение, зависит от типа SOURCE: — если SOURCE — AS-номер, то VALUE — 32-битное беззнаковое целое	`rt 65001:1000` — AS-номер 65001, значение 1000; `soo 192.0.2.1:500` — IP-адрес 192.0.2.1, значение 500; `color 65535:4294967295` — AS-номер 65535, значение 4294967295	`rt 70000:10` — превышение допустимого значения для AS; `soo 192.0.2.1:70000` — значение 70000 недопустимо для IP-источника

Тип	Формат	Компоненты и их описание	Примеры корректных значений	Примеры некорректных значений
		(допустимый диапазон от 0 до 4294967295; — Если SOURCE — IP-адрес, то VALUE — 16-битное беззнаковое целое (допустимый диапазон от 0 до 65535)		
Большой (Large)	AS:VAL1:VAL2	AS — 32-битное беззнаковое целое число (допустимый диапазон от 0 до 4294967295); VAL1, VAL2 — 32-битные беззнаковые целые числовые значения (допустимый диапазон от 0 до 4294967295)	`64512:100:200` — AS 64512, значения 100 и 200	`5000000000:10:20` — превышение допустимого значения для AS; `64512:100` — отсутствует VAL2

Допустимые регулярные выражения BGP communities:

— обычный (standard) — regex1:regex2;

— расширенный (extended) — regex1:regex2;

— большой (large) — regex1:regex2:regex3.

Добавление профиля аутентификации

В профиле указывается пароль, предназначенный для аутентификации. Профиль аутентификации может быть назначен одному или нескольким пирам при добавлении или изменении пира. Один профиль фильтрации может быть назначен пирам разных виртуальных роутеров. Добавление профиля производится на странице виртуального контекста.

> **Примечание.** PT NGFW поддерживает аутентификацию BGP с использованием TCP-опции 19 (TCP-MD5) в соответствии с RFC 2385.

- Чтобы добавить профиль аутентификации:

  1. Выберите вкладку **Профили BGP**.
  2. Выберите вкладку **Аутентификация**.
  3. Нажмите **Добавить профиль**.
  4. Введите название профиля.
  5. Введите пароль.
  6. Если требуется, введите описание.
  7. Нажмите **Сохранить**.

Профиль аутентификации может быть изменен или удален — в контекстном меню профиля на вкладке **Аутентификация**.

Настройка анонсирования сетей

Настройка позволяет указать, о каких сетях необходимо объявлять пирам по протоколу BGP. Настройка осуществляется путем добавления сети, о которой требуется объявлять.

> **Примечание.** Добавление сети производится на странице виртуального роутера (вкладке **BGP**).

- Чтобы добавить сеть:

  1. Выберите вкладку **Сети**.
  2. Нажмите **Добавить сеть**.
  3. Укажите сеть, о которой требуется объявлять пирам.
  4. Нажмите **Сохранить**.

Сеть может быть изменена или удалена — в контекстном меню сети на вкладке **Сети**.

См. также

Graceful restart (OSPF, BGP) (см. раздел 30.6)

14.2.3. Перераспределение маршрутов

Под перераспределением (редистрибуцией) маршрутов подразумевается передача маршрутов в динамический протокол маршрутизации. В PT NGFW перераспределение маршрутов выполняется путем добавления и назначения виртуальному роутеру (протоколу) профиля редистрибуции. В профиле редистрибуции указываются типы маршрутов, которые необходимо перераспределить, и атрибуты, которые должны быть установлены в перераспределяемые маршруты. Для каждого типа маршрутов вы также можете выбрать карту

маршрутов типа **Редистрибуция**. Такая карта маршрутов позволяет указать, какие маршруты выбранного типа должны перераспределяться, а какие — нет, и (или) установить дополнительные атрибуты.

Добавление профиля редистрибуции

- Чтобы добавить профиль редистрибуции:

  1. В главном меню выберите **Устройства**.
  2. Выберите устройство, в котором находится виртуальный роутер.
  3. Выберите вкладку **Виртуальные контексты**.
  4. Нажмите на название виртуального контекста, в котором находится виртуальный роутер.
  5. Выберите вкладку **Профили <название протокола>**, в который выполняется перераспределение>.
  6. Выберите вкладку **Редистрибуция**.
  7. Нажмите **Добавить профиль**.
  8. Введите название профиля.
  9. Если требуется, введите описание.
  10. Выберите типы маршрутов, которые вы хотите перераспределять.
  11. Если требуется, укажите атрибуты маршрутов, отличные от атрибутов по умолчанию, и (или) карту маршрутов.

      Примечание. Всегда перераспределять — флажок, который позволяет перераспределить маршрут по умолчанию, даже если маршрут по умолчанию отсутствует в таблице маршрутизации.

  12. Нажмите **Сохранить**.

Профиль редистрибуции может быть изменен или удален — в контекстном меню профиля на вкладке **Редистрибуция**.

> **Примечание.** Настройка атрибутов карты маршрутов имеет приоритет над таковой профиля редистрибуции. То есть, если выбрана карта маршрутов, то в перераспределяемые маршруты будут установлены атрибуты, указанные в карте маршрутов.

Добавление карты маршрутов для перераспределения

Карта маршрута для перераспределения состоит из списка правил; каждое правило позволяет разрешить или запретить перераспределение маршрута, соответствующего условиям правила, и дополнительно установить атрибуты маршрута. Проверка маршрута на

соответствие правилу происходит начиная с первого правила в списке. Когда соответствие обнаружено, маршрут в зависимости от действия правила перераспределяется или не перераспределяется и проверка остальными правилами карты маршрутов не происходит.

Внимание! В конце карты маршрутов находится неотображаемое правило, запрещающее перераспределение любых маршрутов.

Добавление карты маршрутов производится на странице виртуального контекста.

- Чтобы добавить карту маршрутов для перераспределения:

1. Выберите вкладку **Карты маршрутов**.
2. Нажмите **Добавить карту**.
3. Введите название карты.
4. Если требуется, введите описание.
5. Выберите тип (назначение) карты маршрутов (**Редистрибуция**).
6. Выберите протокол, из которого будут перераспределяться маршруты (тип маршрутов).
7. Выберите протокол, в который будет происходить перераспределение.
8. Нажмите **Добавить**, чтобы добавить правило.
9. Укажите основные параметры правила.

   Примечание. Правило с меньшим порядковым номером будет всегда располагаться выше правила с большим порядковым номером, и, соответственно, проверка на соответствие правилу с меньшим порядковым номером будет происходить раньше.
10. Если требуется, укажите условия для выполнения действия.
11. Если требуется, укажите атрибуты маршрута.
12. Сохраните изменения.

Карта маршрутов для перераспределения может быть изменена или удалена — в контекстном меню карты на вкладке **Карты маршрутов**.

14.3. Маршрутизация по политикам (PBR)

Маршрутизация по политикам (policy-based routing, PBR) — это маршрутизация на основе специальных правил. Такие правила имеют приоритет над таблицей маршрутизации. Любое правило позволяет указать адрес следующего узла (next hop) для трафика, соответствующего определенным критериям. В качестве таких критериев правило может использовать L3-сабинтерфейс, включая туннельный, зону безопасности, из которой поступил IP-пакет, адрес источника и (или) назначения и другое.

Примеры использования:

— перенаправление видеопотоков или IP-телефонии через один канал, а остального трафика — через другой, что позволяет регулировать нагрузку на сеть и (или) провайдера;

— перенаправление трафика конкретного пользователя или сервиса в VPN-туннель;

— тонкая настройка маршрутизации.

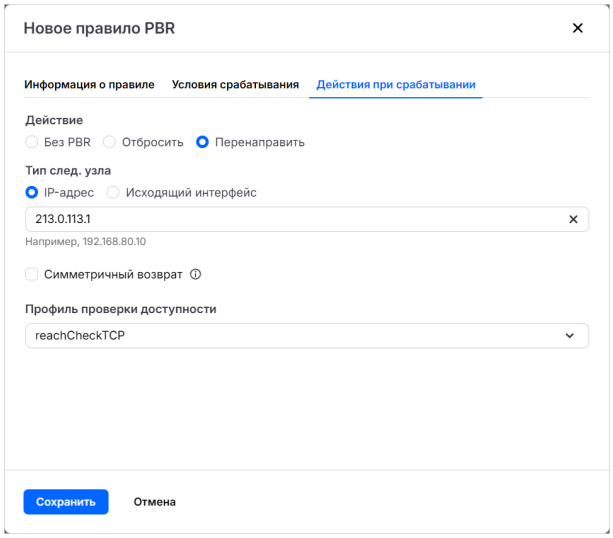


Рисунок 101. Добавление правила PBR

При добавлении правила PBR вам потребуется указать критерии и действие, которое должно быть выполнено при получении межсетевым экраном трафика, соответствующего этим критериям. Действием правила может быть:

— Перенаправление на указанный IP-адрес или с указанного туннельного интерфейса (VTI).

— Отбрасывание сетевого пакета.

— Исключение трафика из процесса маршрутизации по политикам — в этом случае для перенаправления будет использоваться таблица маршрутизации.

Поиск подходящего правила PBR происходит так же, как и поиск других правил: начиная с первого правила до нахождения полного соответствия полученного трафика критериям в одном из правил (сверху вниз). После нахождения соответствия выполняется действие, указанное в правиле.

Маршрутизация по политикам выполняется после трансляции сетевых адресов назначения (DNAT) и до трансляции сетевых адресов источника (SNAT).

Поскольку PBR-правила имеют приоритет над таблицей маршрутизации, их создание происходит на уровне виртуального роутера.

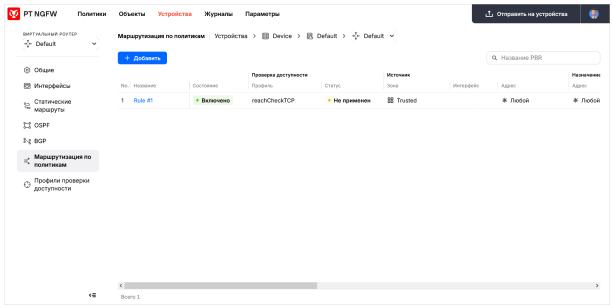


Рисунок 102. Страница **Маршрутизация по политикам**

Симметричный возврат

Функция симметричного возврата (symmetric return) доступна при выборе в качестве действия перенаправления или **Без PBR**. Она позволяет отправлять ответы сервера через те интерфейсы, на которых были получены запросы клиента.

Работа в кластере

В кластере при обновлении версий возможны сценарии, при которых сессии PBR не будут синхронизированы между узлами кластера.

Например, при обновлении кластера с версии 1.8 до 1.9 вначале обновляется резервный узел, а затем происходит переключение, для того чтобы резервный узел стал активным и продолжил обрабатывать текущие сессии пользователей. Если в этот момент администратор попробует применить правила PBR для существующих сессий, то они не будут применены, так как межсетевому экрану недостаточно информации для перенаправления трафика с учетом правила PBR. В частности, неизвестно, на какой интерфейс пришел первый пакет от клиента, неизвестны MAC-адреса соседних устройств, на которые при включенной функции симметричного возврата необходимо будет выполнить обработку обратного трафика. В этом случае у администратора есть возможность при помощи CLI-команды `clear session` удалить необходимые сессии, чтобы они начались заново и PT NGFW получил всю необходимую информацию для выполнения политик перенаправления PBR.

Подробнее о команде `clear session` см. в разделе «Интерфейс командной строки (CLI) (см. раздел 46)».

Добавление правила PBR

Правила PBR добавляются на странице виртуального роутера.

- Чтобы добавить правило PBR:

  1. Выберите вкладку **Маршрутизация по политикам**.
  2. Нажмите **Добавить**.
  3. Введите название правила.
  4. Укажите условия срабатывания (критерии трафика, обрабатываемого правилом):

- зону безопасности (объект «Зона»), из которой поступил сетевой пакет;
- сабинтерфейс, работающий в режиме маршрутизации, на котором был получен пакет;
- адрес источника и (или) адрес назначения (объект «Адрес»);
- L4-протокол, порт источника и (или) порт назначения (объект «Сервис»).

5. Укажите действие при срабатывании (при получении трафика, соответствующего критериям):
   - **Без PBR** — исключение трафика из процесса маршрутизации по политикам; маршрутизация будет происходить в соответствии с таблицей.
   - **Отбросить** — отбрасывание сетевого пакета.

     Примечание. Отбрасывание будет зафиксировано в журнале **Трафик**.
   - **Перенаправить** — перенаправление на указанный IP-адрес или с указанного туннельного интерфейса.
6. Если требуется, включите симметричный возврат, установив соответствующий флажок.

   Примечание. Когда функция включена, маршрут ответного пакета равен маршруту входящего. В противном случае маршрут ответного пакета определяется текущей таблицей маршрутизации.
7. Если требуется, выберите профиль проверки доступности.

   Примечание.Подробнее см. в разделе «Профили проверки доступности (см. раздел 14.4)».
8. Нажмите **Сохранить**.

Правило может быть изменено, удалено или отключено в контекстном меню правила.

При разрешении или блокировании трафика, подпадающего под правило PBR, в журнале **Трафик** создается запись, содержащая название правила PBR. Пункт **Перейти к журналу трафика** позволяет быстро увидеть все записи в журнале, соответствующие правилу.

14.4. Профили проверки доступности

Профили проверки доступности позволяют управлять маршрутизацией на основе измерения качества сети в реальном времени. Для оценки качества сети используется проверка доступности указанного узла по протоколам ICMP и TCP. Функция может быть использована при наличии нескольких альтернативных маршрутов до узла назначения, например при подключении к интернету через нескольких провайдеров.

Примечание. Функция является близким аналогом IP SLA в программном обеспечении Cisco IOS.

Принцип работы

На уровне виртуального роутера вы можете добавить один или несколько профилей проверки доступности.

В профиле проверки доступности настраиваются параметры проверки доступности:

- **Протокол.** В зависимости от выбранного протокола (ICMP или TCP) проверка будет выполняться путем отправки ICMP-сообщений echo request или установления TCP-соединений.
- **Адрес назначения.** IP-адрес узла, доступность которого требуется проверять.
- **Порт назначения.** Параметр указывается, если выбран протокол TCP.
- **Интерфейс-источник.** Сабинтерфейс текущего виртуального роутера, IP-адрес которого требуется использовать как IP-адрес источника в тестовых пакетах.
- **Интервал.** Интервал отправки тестовых пакетов (в секундах).
- **Число попыток.** Число последовательных проверок, в ходе которых не было получено ICMP-сообщение echo reply или TCP-сообщение SYN-ACK, при достижении которого узел считается недоступным.

Профиль может быть применен к статическим маршрутам и (или) правилам PBR, если их действием является **Перенаправить** (**Forward**), в текущем виртуальном роутере. Устройство будет выполнять проверку доступности указанного узла в соответствии с параметрами профиля.

> **Внимание!** Путь для отправки тестовых пакетов определяется текущей таблицей маршрутизации.

При обнаружении недоступности указанного узла:

- связанный с профилем статический маршрут будет исключен из таблицы маршрутизации;
- связанное с профилем правило PBR будет отключено.

После обнаружения недоступности узла проверка доступности продолжится. Узел будет снова считаться доступным при достижении числа последовательных успешных проверок равному значению параметра **Число попыток**.

Когда указаный узел вновь станет доступным:

- связанный с профилем маршрут будет возвращен в таблицу маршрутизации;
- связанное с профилем правило PBR будет включено.

Межсетевой экран передает в систему управления изменения статуса доступности маршрутов и правил PBR.

> **Внимание!** Для успешной проверки доступности тестовый трафик должен быть разрешен правилами безопасности. В правиле безопасности в качестве зоны безопасности источника потребуется указать зону **Local**.

Статусы проверки доступности

Статический маршрут и правило PBR могут иметь следующие статусы проверки доступности:

- **Не применен (Not pushed).** Маршрут, правило или связанный профиль имеет изменения, не примененные на устройствах.
- **Ожидание (Waiting).** От устройства ожидается статус проверки доступности.
- **Доступен (Up).** Проверка доступности успешна.
- **Недоступен (Down).** Проверка доступности неуспешна.
- **Отключен (Disabled).** Связанный с маршрутом или правилом профиль отключен.

Добавление профиля проверки доступности

Вы можете добавить профиль на странице виртуального роутера.

- Чтобы добавить профиль проверки доступности:

  1. Выберите вкладку **Профили проверки доступности**.
  2. Нажмите **Добавить**.
  3. Если требуется, отключите профиль.
  4. Введите название профиля.
  5. Если требуется, введите описание.
  6. Выберите протокол для проверки доступности — ICMP или TCP.
  7. Введите IP-адрес узла, доступность которого требуется проверять.
  8. Если вы выбрали проверку по TCP, введите порт назначения.
  9. Выберите интерфейс-источник — IP-адрес выбранного сабинтерфейса (первый адрес в списке адресов сабинтерфейса при наличии нескольких адресов) будет использоваться как адрес источника в тестовых пакетах.

     Примечание. Параметр не влияет на выбор устройством исходящего интерфейса при отправке тестовых пакетов.
  10. Укажите число попыток — число последовательных неуспешных или успешных проверок доступности, при достижении которого узел считается недоступным или вновь доступным, соответственно.
  11. Укажите интервал отправки тестовых пакетов в секундах.
  12. Нажмите **Сохранить**.

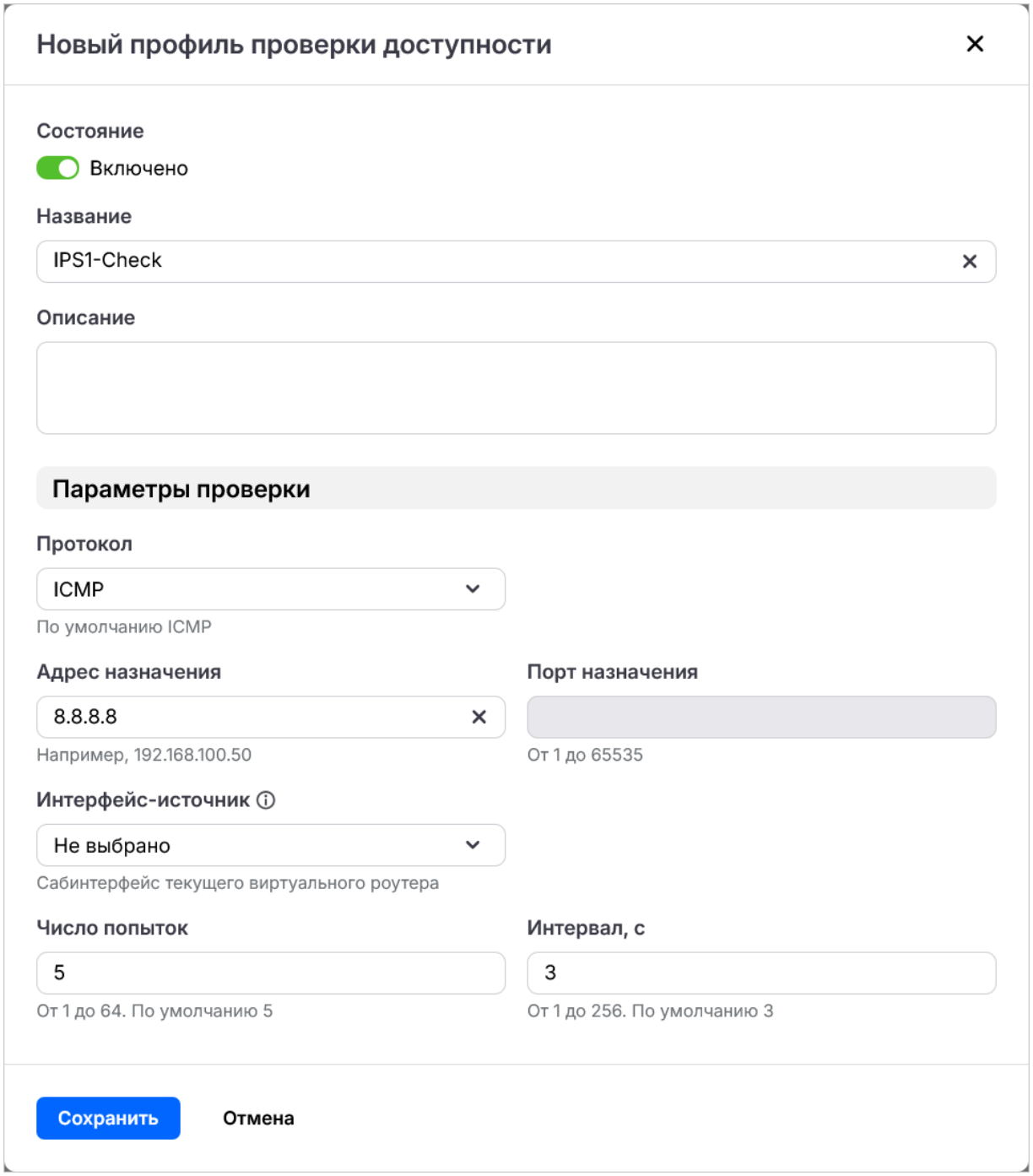


Рисунок 103. Добавление профиля проверки доступности

Вы можете изменить или удалить профиль, используя контекстное меню.

Применение профиля к маршруту или правилу

- Чтобы применить профиль к статическому маршруту или правилу PBR, в карточке маршрута или правила выберите этот профиль.

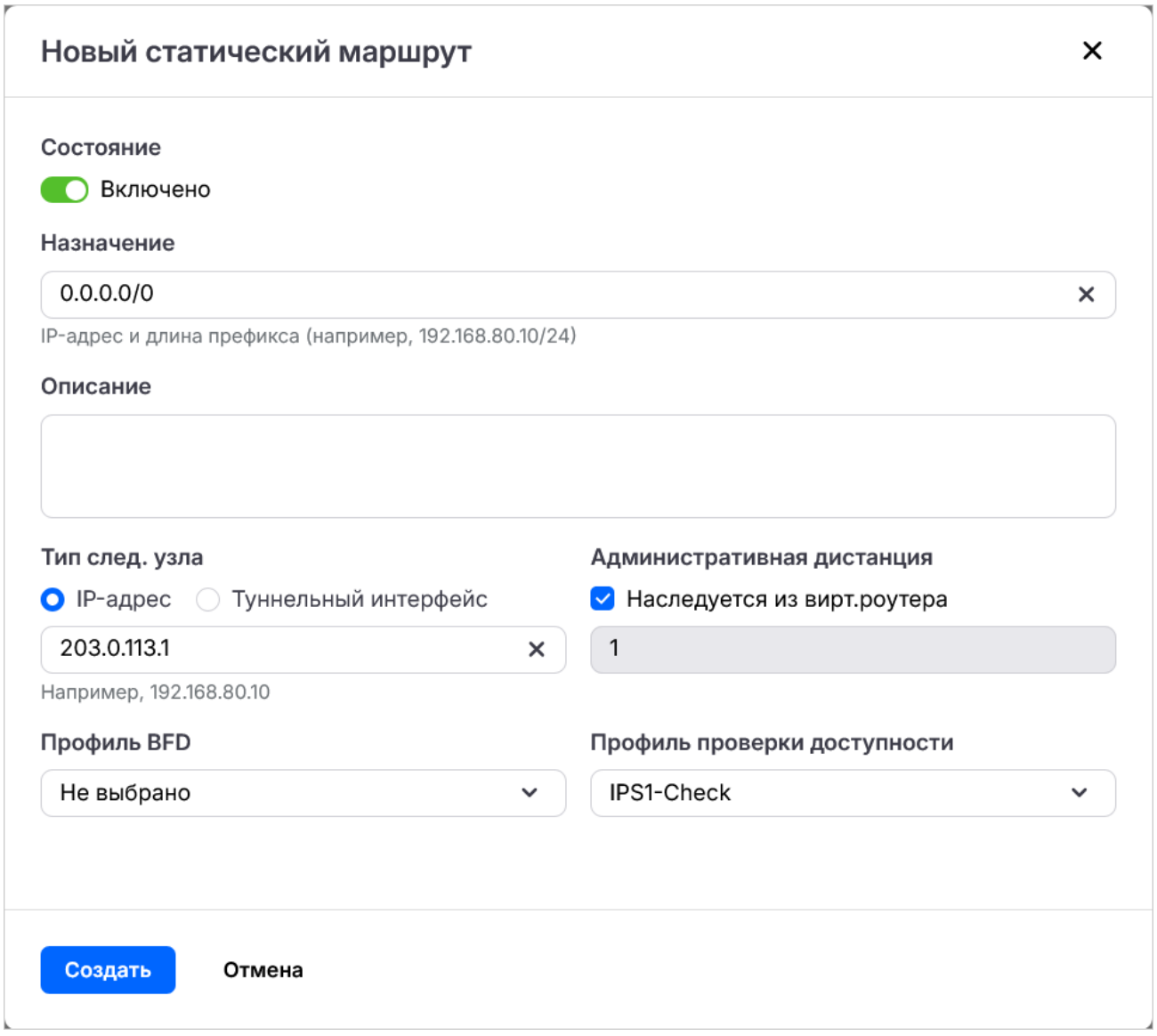


Рисунок 104. Добавление маршрута с привязанным профилем

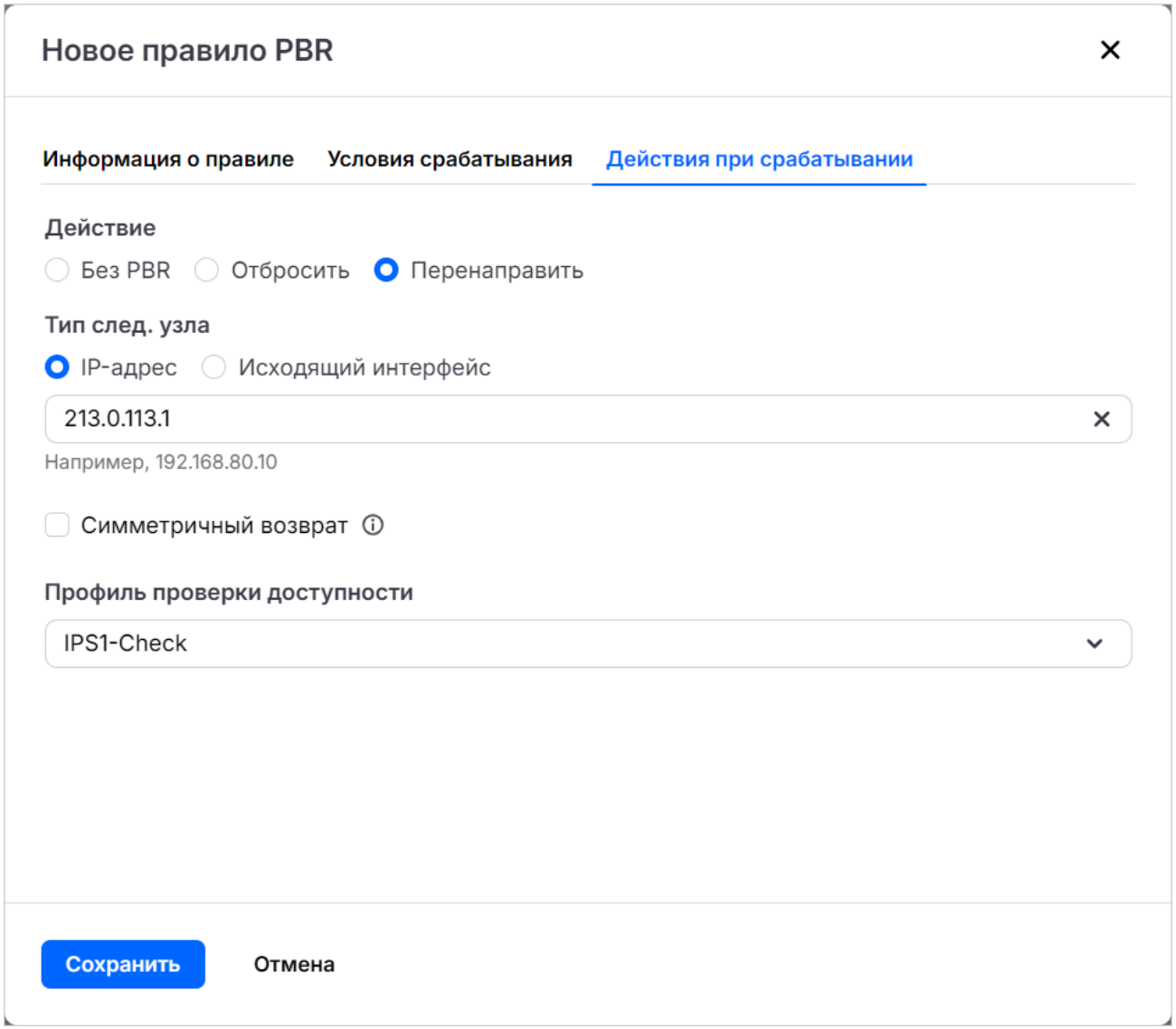


Рисунок 105. Добавление правила PBR с привязанным профилем

14.5. BFD

BFD (Bidirectional Forwarding Detection) — это механизм, позволяющий протоколам динамической маршрутизации обнаруживать потерю связности с соседними устройствами быстрее, чем позволяют их встроенные механизмы. За счет быстрого обнаружения сбоя (на уровне сотен миллисекунд) маршрутизатор может быстрее переключиться на резервный путь передачи данных, что сокращает время простоя. По сравнению со встроенными механизмами (например, Hello-сообщениями в OSPF), BFD оказывает значительно меньшую нагрузку на процессор. BFD может быть полезен в инфраструктуре, где важна быстрая реакция на сбои, например в сетях, передающих VoIP-трафик.

BFD может быть использован для проверки доступности следующего узла (next hop) статического маршрута. Если для маршрута включен BFD, то при обнаружении недоступности следующего узла маршрут удаляется. Когда следующий узел снова становится доступным, маршрут восстанавливается.

Поддержка BFD в текущей версии PT NGFW имеет следующие ограничения:

— Поддерживается только асинхронный режим — режим «по требованию» (demand mode) не поддерживается.

— Не реализована синхронизация статуса BFD между узлами A/S-кластера.

— Аутентификация BFD-пакетов не поддерживается.

— Эхо-функция не поддерживается.

Принцип работы

Между двумя устройствами устанавливается BFD-сессия, в рамках которой каждое устройство с заданным интервалом передает другому пакеты BFD. Если в течение времени обнаружения (detection time) соседнее устройство не присылает BFD-пакет, это воспринимается как сбой — BFD-сессия разрывается и связанные протоколы маршрутизации оповещаются о проблеме.

BFD работает поверх UDP-протокола. BFD-пакеты — это unicast-пакеты со случайным портом источника (в диапазоне 49152—65535) и портом назначения 3784 — для обычных пакетов, 3785 — для эхо-пакетов (не поддерживается в текущей версии PT NGFW) и 4784 — для обычных пакетов в режиме multi-hop.

PT NGFW поддерживает работу между удалёнными устройствами (multi-hop) (RFC 5883), что может быть полезно при BGP-маршрутизации. Для BGP-пира соответствующий режим работы (multi-hop) включается автоматически при определении такой необходимости. Для OSPF-интерфейсов возможность использования режима multi-hop не предусмотрена. Для статического маршрута режим multi-hop включается вручную, если требуется.

Настройка в PT NGFW

Настройка BFD в PT NGFW предполагает создание BFD-профиля, в котором указываются параметры работы BFD, и его последующее применение к BGP-пиру (пирам), OSPF-интерфейсу (интерфейсам) или (и) статическому маршруту (маршрутам). Параметры профиля будут действительны для этого пира, интерфейса или (и) статического маршрута.

► Чтобы добавить BFD-профиль:

1. В главном меню выберите **Устройства**.
2. Выберите устройство, для которого вы хотите выполнить настройку.
3. Выберите виртуальный контекст, для которого вы хотите выполнить настройку.
4. Выберите вкладку **Профили BFD**.

5. Нажмите **Добавить**.
6. Если требуется, отключите профиль.

   Примечание. При отключении BFD-профиля PT NGFW информирует соответствующих BFD-соседей об административном отключении, что не приводит к ошибочному обнаружению постоянного сбоя.
7. Введите название профиля.
8. Выберите режим работы:
   - **Активный** — устройство будет инициировать создание BFD-сессии;
   - **Пассивный** — устройство не будет самостоятельно инициировать создание BFD-сессии (инициатором должно выступить соседнее устройство).
9. В поле **Желаемый минимальный интервал отправки пакетов (мс)** укажите интервал отправки BFD-пакетов в миллисекундах (transmit interval, MinTxInt).
10. В поле **Необходимый минимальный интервал получения пакетов (мс)** укажите ожидаемый интервал получения BFD-пакетов в миллисекундах (receive interval, MinRxInt).

    Примечание. Указанное значение будет использовано для расчета времени обнаружения сбоя текущим устройством. Это время рассчитывается путем умножения этого интервала на число, указанное в поле **Макс. число пропущенных пакетов**.
11. В поле **Макс. число пропущенных пакетов** укажите множитель, используемый для расчета времени обнаружения сбоя текущим устройством.
12. Нажмите **Сохранить**.

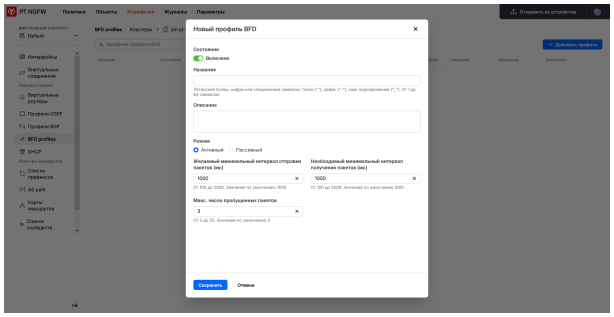


Рисунок 106. Добавление BFD-профиля

- Чтобы назначить BFD-профиль BGP-пиру,

  выберите BFD-профиль на странице создания или изменения BGP-пира.
- Чтобы назначить BFD-профиль OSPF-интерфейсу,

  выберите BFD-профиль на странице изменения параметров OSPF-интерфейса.

- Чтобы назначить BFD-профиль статическому маршруту,

  выберите BFD-профиль на странице создания или изменения статического маршрута.

15. Виртуальные соединения (vWire)

Виртуальное соединение образуется при объединении двух сабинтерфейсов с режимом работы vWire. Кадры, поступающие на один из сабинтерфейсов виртуального соединения, всегда передаются на другой сабинтерфейс этого соединения. Изучение MAC-адресов и ведение ARP-таблицы в таком режиме не выполняется, так как это не требуется. Когда vWire-сабинтерфейсу назначена VLAN-метка, он принимает трафик только из соответствующей виртуальной локальной сети и, если трафик передается с другого сабинтерфейса, помечает этой меткой передаваемый кадр.

- Чтобы добавить виртуальное соединение:

  1. В главном меню выберите **Устройства**.
  2. Выберите устройство, в которое вы хотите добавить соединение.
  3. Выберите вкладку **Виртуальные контексты**.
  4. Выберите виртуальный контекст, в который вы хотите добавить соединение.
  5. Выберите вкладку **Виртуальные соединения**.
  6. Нажмите **Добавить**.
  7. Введите название соединения.
  8. Если требуется, введите описание.
  9. Выберите сабинтерфейсы, между которыми должны передаваться кадры.

     Примечание. В списках сабинтерфейсов находятся только те сабинтерфейсы, которым назначен режим работы vWire.
  10. Нажмите **Добавить**.

Вы можете изменить или удалить виртуальное соединение, используя контекстное меню.

16. Работа с правилами межсетевого экрана

Работа с правилами происходит на странице **Политики**. На странице отображается иерархический список групп устройств. При выборе группы отображаются правила этой группы. Правила группы состоят из пред- и постправил этой группы и пред- и постправил родительских групп. Правила отображаются в том порядке, в котором они будут обрабатываться виртуальными контекстами выбранной группы.

> **Примечание.** Дополнительную информацию о правилах содержит раздел «Принцип работы (см. раздел 6.4)».

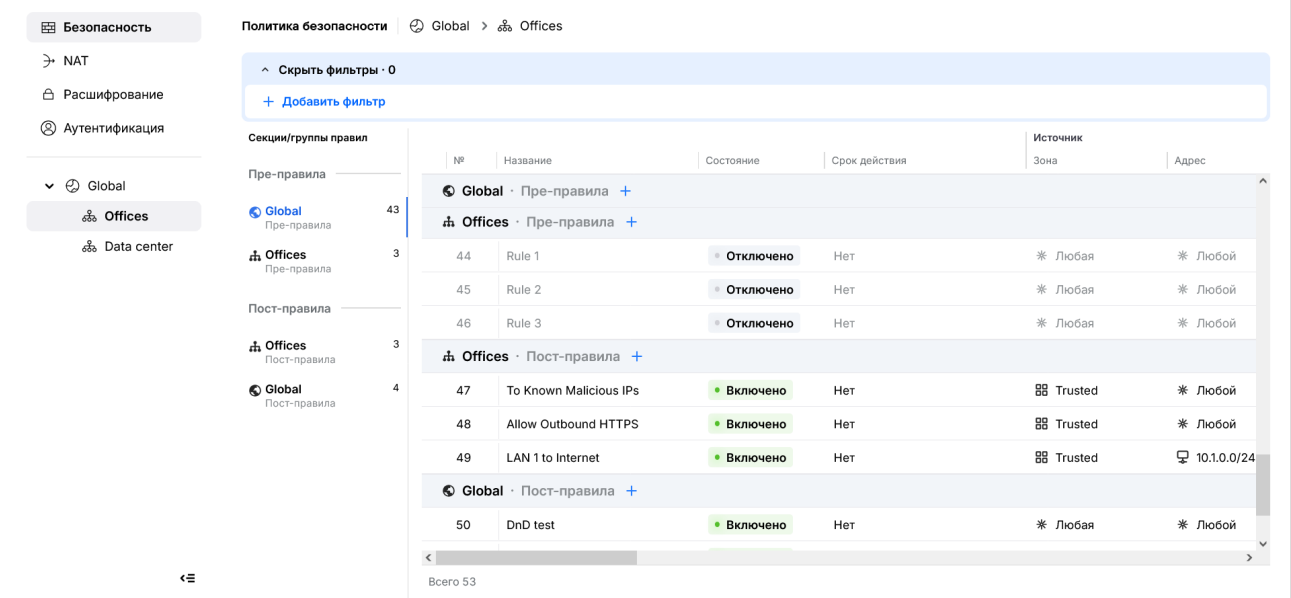


Рисунок 107. Страница **Политики**

Добавление правила безопасности

Используя правило безопасности, вы можете разрешить или запретить дальнейшую передачу трафика, проверить трафик системой предотвращения вторжений (IPS) и потоковым антивирусом, передать на внешний ICAP-сервер трафик HTTP-приложений.

► Чтобы добавить правило безопасности:

1. В главном меню выберите раздел **Политики**.
2. Выберите группу устройств, в которую вы хотите добавить правило.
3. Наведите курсор мыши на название блока пред- или постправил и нажмите +.
4. Введите название правила.
5. Если требуется, укажите период действия правила.
6. Если требуется, укажите условия срабатывания правила, отличные от условий по умолчанию, выбрав объект соответствующего типа:

Примечание. Между условиями срабатывания одного типа работает логическое ИЛИ. Между условиями срабатывания разных типов работает логическое И. Пример: адрес источника «А» или «Б» или «В» и пользователь «А» или «Б» и приложение «А».

- зону безопасности источника и (или) зону безопасности назначения трафика;
- адрес источника и (или) адрес назначения трафика — IP-адрес, полное доменное имя (FQDN) или географическое местоположение (GeoIP) (возможно указание группы адресов);
- пользователя — учетную запись Active Directory (возможно указание группы пользователей);

  Примечание. Правило, в котором указан объект «Пользователь», срабатывает при получении трафика, адрес источника которого совпадает с IP-адресом в указанном объекте.
- сервис — L4-протокол, порт источника или назначения трафика (возможно указание группы сервисов);
- приложение — протокол прикладного уровня или приложение, которые были определены в трафике;
- категорию URL-адресов — множество URL-адресов, относимых на основе содержимого соответствующих веб-ресурсов к одной категории.

7. Если требуется, укажите действие при обнаружении трафика, отличное от действия по умолчанию:
   - **Разрешить** — разрешение передачи сетевого пакета;
   - **Отбросить** — запрет передачи сетевого пакета без отправки источнику трафика сообщения;
   - **Отправить RST клиенту** — запрет с отправкой сообщения TCP RST по адресу источника трафика;
   - **Отправить RST серверу** — запрет с отправкой сообщения TCP RST по адресу назначения трафика;
   - **Отправить RST обоим** — запрет с отправкой сообщения TCP RST клиенту и серверу.
8. Если требуется, выберите режим журналирования, отличный от режима по умолчанию:
   - **При срабатывании правила** — запись создается при получении первого пакета сессии, соответствующего правилу (например, при получении пакета TCP SYN);
   - **В начале сессии** — для TCP-сессии запись создается по завершении процедуры TCP-рукопожатия и при получении первого пакета с данными, а для UDP- и ICMP-трафика — при получении первого пакета сессии;
   - **В конце сессии** — сразу после закрытия сессии;
   - **В начале и в конце сессии** — сразу после открытия и закрытия сессии;
   - **Без журналирования** — информация о срабатывании не будет занесена в журнал.

9. Если требуется, укажите профиль (профили) безопасности:
   - IPS-профиль — используется для проверки трафика системой предотвращения вторжений;

     Примечание. Когда выбран IPS-профиль **PT Protect**, при срабатывании сигнатуры создается запись в журнале IPS и выполняется действие, указанное в сигнатурах (в большинстве случаев блокирование трафика). Когда выбран IPS-профиль **PT Detect**, при срабатывании создается запись в журнале IPS и трафик разрешается к передаче. Подробнее см. в разделе «IPS».
   - антивирусный профиль — используется для проверки трафика антивирусом;

     Примечание. Когда выбран профиль **PT Protect**, при обнаружении зараженного файла создается запись в журнале **Антивирус** и трафик блокируется. Когда выбран профиль **PT Detect**, создается запись в журнале **Антивирус** и трафик не блокируется. Подробнее см. в разделе «Антивирусная проверка трафика (см. раздел 23)».
   - ICAP-профиль — используется для отправки трафика на ICAP-сервер.

     Примечание. Подробнее см. в разделе «ICAP (см. раздел 36)».
10. Нажмите **Сохранить**.

Добавление правила NAT

Подробная информация о настройке NAT доступна в разделе «NAT».

- Чтобы добавить правило NAT:
  1. В главном меню выберите раздел **Политики**.
  2. Выберите группу устройств, в которую вы хотите добавить правило.
  3. Выберите вкладку **NAT**.
  4. Наведите курсор мыши на название блока пред- или постправил и нажмите +.
  5. Введите название правила.
  6. Укажите условия срабатывания правила, выбрав объект соответствующего типа:
     - зону безопасности источника и зону безопасности назначения трафика;
     - (если требуется) адрес источника и (или) адрес назначения трафика — IP-адрес, полное доменное имя (FQDN) или географическое местоположение (GeoIP) (возможно указание группы адресов);
     - (если требуется) сервис — L4-протокол, порт источника или назначения трафика (возможно указание группы сервисов).
  7. Если вы хотите транслировать информацию об источнике, настройте соответствующие параметры:
     - **Тип трансляции**;

Примечание. Действие **Без трансляции** позволяет создавать исключения из процесса трансляции.

- **Тип адреса**;
- **Траслированный пул адресов** — массив адресов для трансляции;
- **Транслированные порты** — массив портов для трансляции.

8. Если вы хотите транслировать информацию о назначении, настройте соответствующие параметры:
   - **Тип трансляции**;

     Примечание. Действие **Без трансляции** позволяет создавать исключения из процесса трансляции.

   - **Адрес назначения** — адрес назначения после трансляции;
   - **Транслированный порт**.
9. Нажмите **Сохранить**.

Добавление правила расшифрования

Используя правило расшифрования, вы можете указать признаки трафика, который должен быть расшифрован или исключен из процесса расшифрования. Расшифрование требуется для возможности распознания внутри трафика приложения при проверке правилами безопасности, для анализа трафика модулем IPS, антивирусом и ICAP-сервисом.

► Чтобы добавить правило расшифрования:

1. В главном меню выберите раздел **Политики**.
2. Выберите группу устройств, в которую вы хотите добавить правило.
3. Выберите вкладку **Расшифрование**.
4. Наведите курсор мыши на название блока пред- или постправил и нажмите + .
5. Введите название правила.
6. Если требуется, укажите условия срабатывания правила, отличные от условий срабатывания по умолчанию, выбрав объект соответствующего типа:
   - зону безопасности источника и (или) зону безопасности назначения трафика;
   - адрес источника и (или) адрес назначения трафика — IP-адрес, полное доменное имя (FQDN) или географическое местоположение (GeoIP) (возможно указание группы адресов);
   - пользователя — учетную запись Active Directory (возможно указание группы пользователей);

Примечание. Правило, в котором указан объект «Пользователь», срабатывает при получении трафика, адрес источника которого совпадает с IP-адресом в указанном объекте.

- сервис — L4-протокол, порт источника или назначения трафика (возможно указание группы сервисов);
- категорию URL-адресов — множество URL-адресов, относимых на основе содержимого соответствующих веб-ресурсов к одной категории.

7. Если требуется, укажите действие при обнаружении трафика, отличное от действия по умолчанию.

   Примечание. Действие **Не расшифровывать** позволяет создавать исключения из процесса расшифрования.

8. Если требуется, выберите режим журналирования, отличный от режима по умолчанию:
   - **При срабатывании правила** — запись создается при получении пакета TLS Client Hello;
   - **При успешном TLS-рукопожатии** — при срабатывании правила и успешном установлении TLS-соединения;
   - **При любом TLS-рукопожатии** — сразу после успешного или неуспешного TLS-рукопожатия;
   - **При неуспешном TLS-рукопожатии** — при срабатывании правила и возникновении ошибок при установлении TLS-соединения;
   - **Без журналирования** — информация о срабатывании не будет занесена в журнал.
9. Если требуется, выберите или создайте и выберите профиль зеркалирования.

   Примечание. Подробнее см. в разделе «Зеркалирование расшифрованного трафика (см. раздел 27)».

10. Нажмите **Сохранить**.

Добавление правила аутентификации

Используя правило аутентификации, вы можете настроить перенаправление пользователей на портал аутентификации, которая осуществляется в домене Active Directory, связанном с межсетевым экраном. Подробнее см. в разделе «Аутентификация пользователей (см. раздел 37)».

► Чтобы добавить правило аутентификации:

1. В главном меню выберите раздел **Политики**.
2. Выберите группу устройств, в которую вы хотите добавить правило.
3. Выберите вкладку **Аутентификации**.
4. Наведите курсор мыши на название блока пред- или постправил и нажмите + .

5. Введите название правила.
6. Если требуется, укажите условия срабатывания правила, отличные от условий срабатывания по умолчанию, выбрав объект соответствующего типа:
   - зону безопасности источника и (или) зону безопасности назначения трафика;
   - адрес источника и (или) адрес назначения трафика — IP-адрес, полное доменное имя (FQDN) или географическое местоположение (GeoIP) (возможно указание группы адресов);
   - сервис — L4-протокол, порт источника или назначения трафика (возможно указание группы сервисов).
7. Если требуется, укажите действие при обнаружении трафика (профиль аутентификации или **Без аутентификации**), отличное от действия по умолчанию.

   Примечание. Действие **Без аутентификации** позволяет создавать исключения из процесса перенаправления на портал аутентификации.
8. Если требуется, выберите режим журналирования, отличный от режима по умолчанию:
   - **При срабатывании правила**;
   - **Без журналирования** — информация о срабатывании не будет занесена в журнал.
9. Нажмите **Сохранить**.

Фильтрация правил

Для удобства просмотра и поиска правил вы можете настроить фильтры по одному или нескольким столбцам, отображающие нужные правила и скрывающие остальные.

Вы можете добавить фильтры по кнопке **Добавить фильтр** или нажав  в заголовке столбца.

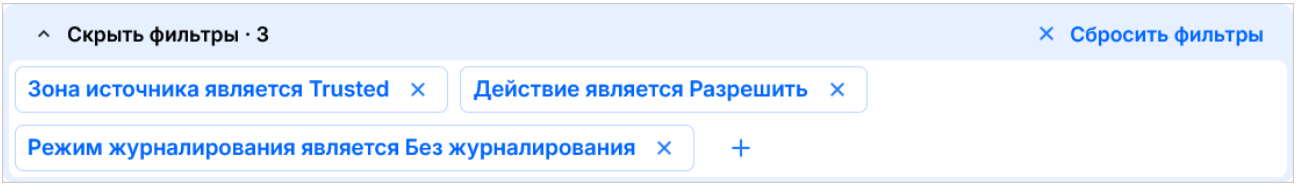


Рисунок 108. Панель фильтров

Примечание. Фильтрация по периоду действия правила безопасности и условиям срабатывания **Транслированные порты** и **Транслированный порт** в правилах NAT не поддерживается.

Другие действия с правилами

Используя контекстное меню правила, вы можете помимо прочего:

— копировать правило — с помощью пунктов **Копировать** и **Вставить строкой ниже** или **Вставить строкой выше**;

— переместить правило в пределах блока пред- или постправил — с помощью пунктов **Вырезать** и **Вставить строкой ниже** или **Вставить строкой выше** или перетаскивания;

— перейти к журналу — посмотреть связанные записи журнала;

— отключить правило;

— сбросить счетчик срабатываний — сделать равным нулю;

Примечание. Действие доступно только для правил безопасности.

— удалить правило.

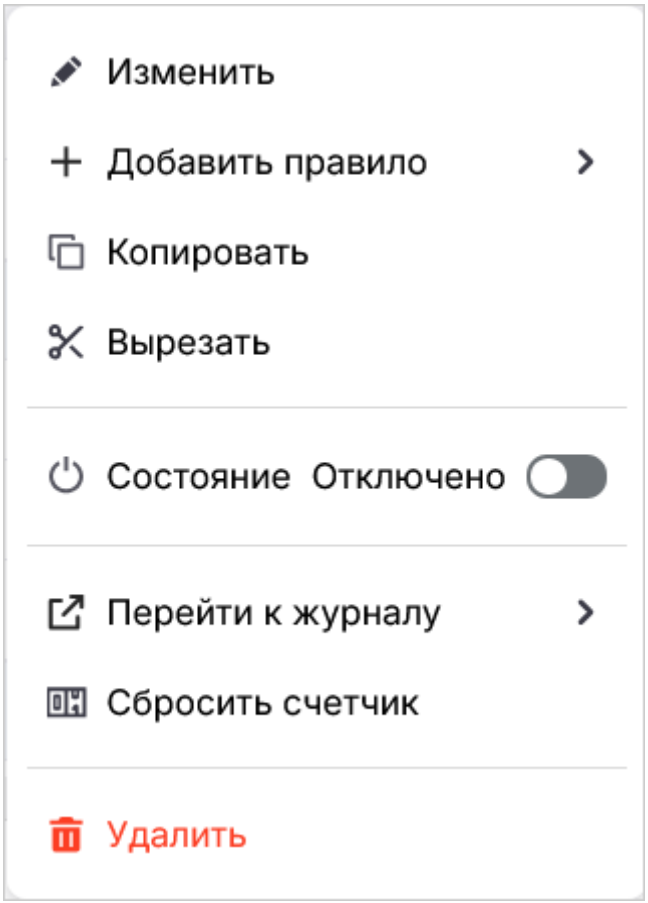


Рисунок 109. Контекстное меню правила

17. Объекты

С помощью объектов настраиваются различные функции PT NGFW. Например, объекты указываются как условия срабатывания при добавлении или изменении правил межсетевого экрана (выполнения действий правила). Такое использование объектов призвано упростить управление межсетевым экраном — изменяя объект, вы изменяете условия срабатывания сразу всех правил, в которых он указан. Объекты некоторых типов могут быть объединены в группу и указаны в правиле в качестве условия срабатывания как группа.

Объекты следующих типов указываются в качестве условий срабатывания: «Приложение», «Пользователь», «Сервис», «Адрес», «Зона», «Категория URL».

Другие типы объектов включают:

— IPS-профили и группы — используются для настройки системы предотвращения вторжений (IPS). Подробнее см. в разделе «Работа с IPS (системой предотвращения вторжений)».

— Профили аутентификации — используются для перенаправления пользователей на портал аутентификации. Подробнее см. в разделе «Аутентификация пользователей (см. раздел 37)».

— Профили зеркалирования — используются для зеркалирования расшифрованного трафика. Подробнее см. в разделе «Зеркалирование расшифрованного трафика (см. раздел 27)».

Объект «Приложение»

Такой объект представляет собой протокол прикладного уровня, приложение или функцию приложения и указывается в качестве условия срабатывания в правилах безопасности. Объекты «Приложение» бывают только предустановленными — возможность добавления пользовательских объектов «Приложение» отсутствует. Вместе с PT NGFW поставляется несколько тысяч таких объектов.

Объект «Пользователь»

Объект этого типа указывается в правилах безопасности и расшифрования и представляет собой учетную запись пользователя Active Directory. Объекты «Пользователь» добавляются автоматически в результате синхронизации межсетевого экрана с Active Directory. Каждый объект содержит информацию о логине пользователя и его текущем IP-адресе. Правило, в котором указан такой объект, срабатывает при получении трафика, адрес источника которого совпадает с IP-адресом из объекта. Эти объекты не могут быть добавлены, изменены или удалены вручную.

Объект «Сервис»

Объект «Сервис» используется для указания в правилах IP-протокола — транспортного (TCP, UDP) и его порта или протокола ICMP. Вместе с PT NGFW поставляется несколько десятков таких объектов.

Объект «Адрес»

Этот объект используется для указания в правилах адреса источника и назначения трафика. Такой объект может содержать IP-адрес в формате CIDR, диапазон IP-адресов, полное доменное имя (FQDN) или географическое местоположение (GeoIP). Когда в правиле указано FQDN, PT NGFW выполняет его разрешение в IP-адрес (адреса), запоминает все IP-адреса, соответствующие указанному FQDN, на период времени жизни (TTL) DNS-записи и использует полученные IP-адреса для поиска подходящего правила. Когда в правиле указано географическое местоположение, PT NGFW определяет IP-адреса, соответствующие стране или региону. Объекты, содержащие географическое местоположение, бывают только предустановленными.

Объект «Зона»

Объект «Зона» подразумевает один или несколько сабинтерфейсов с общими параметрами безопасности. Объект указывается в правилах как зона безопасности источника и назначения трафика.

Объект «Категория URL»

Информация об этом типе объектов доступна в разделе «Категории URL (см. раздел 18)».

Добавление объекта «Сервис», «Адрес», «Зона»

- Чтобы добавить объект «Сервис», «Адрес», «Зона»:

  1. Выберите раздел **Объекты**.
  2. Выберите вкладку, соответствующую типу добавляемого объекта.
  3. Нажмите **Добавить**.
  4. Введите название объекта.
  5. Если требуется, введите описание.
  6. Укажите содержимое объекта, например IP-адрес (при добавлении «Адреса»).

     Внимание! Добавление сабинтерфейса в «Зону» возможно при добавлении или изменении сабинтерфейса. Удаление сабинтерфейса из «Зоны» возможно при его изменении.
  7. Нажмите **Добавить**.

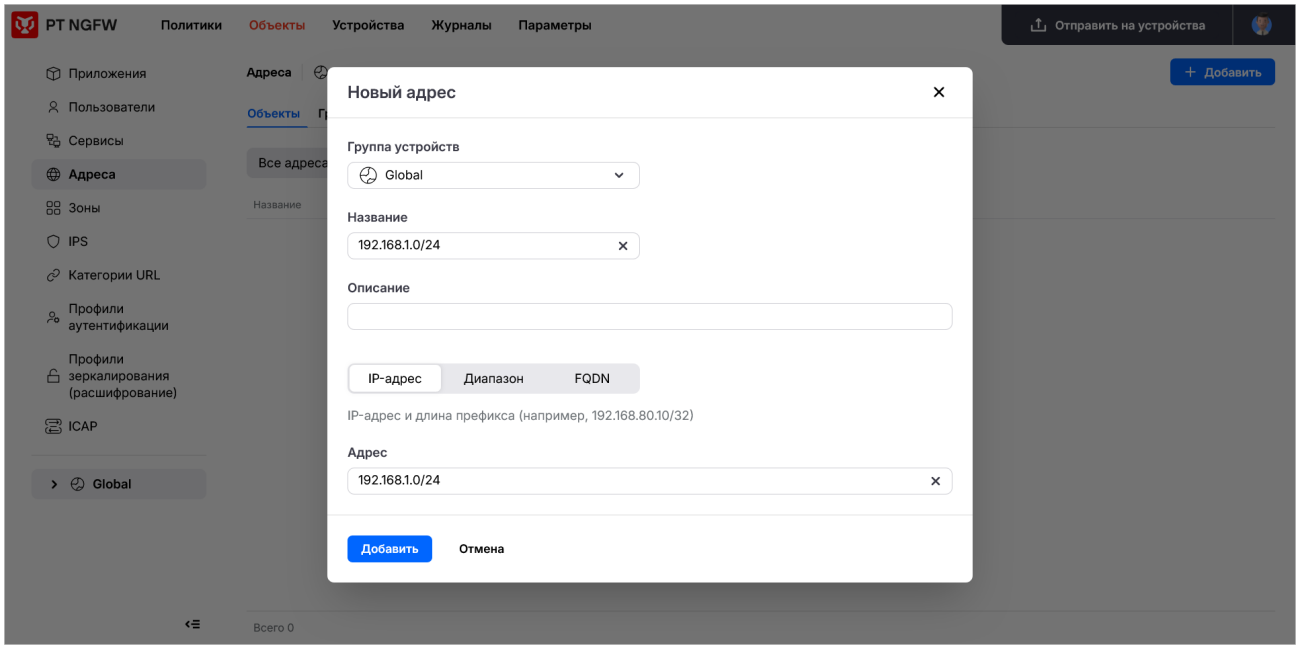


Рисунок 110. Добавление объекта «Адрес»

Добавленный объект может быть изменен или удален через контекстное меню объекта.

Объекты могут быть добавлены не только в разделе **Объекты**, но и при создании или изменении правила.

> **Внимание!** Перед удалением объекта убедитесь, что он не используется в правиле или в группе объектов. Если объект используется, сначала удалите объект из правила или группы, а затем станет возможным удаление самого объекта. Такое ограничение призвано предотвратить неявные изменения политик и групп.

Добавление группы объектов

В группу можно добавить объекты «Сервис» и «Адрес».

- Чтобы добавить группу объектов:

  1. Выберите раздел **Объекты**.
  2. Выберите вкладку, соответствующую типу объектов, которые должна содержать группа.
  3. Выберите вкладку **Группы**.
  4. Нажмите **Добавить**.
  5. Введите название группы.
  6. Если требуется, введите описание.
  7. Выберите объекты, которые должна содержать группа.

Примечание. Возможен выбор других групп объектов. Максимально допустимое количество вложенных групп объектов — 10.

8. Нажмите **Добавить**.

Группа объектов может быть изменена или удалена через контекстное меню объекта.

Группа может быть добавлена не только в разделе **Объекты**, но и при создании или изменении правила.

Примечание. Удаление группы объектов приводит к удалению только самой группы объектов (не приводит к удалению объектов).

18. Категории URL

Категория URL — это объект, представляющий собой один или множество URL. Категория URL может быть указана в правилах безопасности и расшифрования. Сессия считается соответствующей правилу, если категория, к которой была отнесена сессия, совпадает с категорией, указанной в правиле (и если выполняются остальные условия правила). PT NGFW относит сессию к тем или иным категориям согласно принципу, описанному далее в этом разделе.

Категоризация незашифрованного или расшифрованного трафика HTTP определяется на основе URL, а трафика TLS, расшифрование которого не выполнялось или не удалось выполнить, — на основе значения атрибута SNI. Значение SNI передается в сообщении TLS ClientHello.

PT NGFW поставляется с десятками категорий, содержащих миллионы URL. Примеры предустановленных категорий: социальные сети, вредоносные сайты, развлечения. Предустановленные категории нельзя измененить или удалить.

PT NGFW поддерживает создание собственных категорий URL. Это может потребоваться, например, для фильтрации запросов к внутренним URL организации или для переопределения предустановленных категорий. В собственной категории вы можете указывать как URL, так и wildcard-выражения, содержащие подстановочные символы и соответствующие множеству URL и SNI.

Работа с категориями происходит в разделе **Объекты** → **Категории URL**.

Все присвоенные трафику категории отображаются в записях журналов.

В этом разделе

Принцип категоризации трафика (см. раздел 18.1)

Порядок указания URL и выражений (см. раздел 18.2)

Примеры wildcard-выражений (см. раздел 18.3)

Добавление категории URL (см. раздел 18.4)

Предустановленные категории (см. раздел 18.5)

18.1. Принцип категоризации трафика

PT NGFW относит URL или SNI к тем или иным категориям согласно принципу, описанному ниже.

Примечание. Далее в разделе под URL, анализируемом в трафике, подразумевается URL или SNI.

— В одной собственной категории можно указать как специфичные URL, не содержащие подстановочные символы, так и wildcard-выражения. Все они работают через ИЛИ: если URL соответствует любому URL или wildcard-выражению, указанному в категории, то URL присваивается эта категория.

— URL не может быть отнесен и к собственной, и к предустановленной категории. Если для URL задана хотя бы одна собственная категория, то предустановленные категории для такого URL игнорируются.

— Поиск подходящих собственных категорий выполняется среди собственных категорий, привязанных к той же группе устройств, что и виртуальный контекст, через который передается анализируемая сессия, а также к родительским по отношению к группе контекста группам.

— URL не может быть отнесен более чем к пяти категориям.

— Если URL соответствует множеству wildcard-выражений и в итоге более чем пяти собственным категориям, то выбираются те категории, wildcard-выражения в которых наиболее точно соответствуют анализируемому URL.

— Если URL имеет одинаковую степень соответствия нескольким wildcard-выражениям, то из категорий, в которых содержатся эти выражения, будет выбрано несколько случайных категорий — столько, сколько необходимо для достижения максимально допустимого количества присвоенных категорий.

18.2. Порядок указания URL и выражений

Примечание. Любой URL всегда содержит путь, даже если путь не виден пользователю. Когда пользователь вводит в строке браузера example.com, браузер автоматически добавляет путь до корневой директории сервера — example.com/.

Внимание! Атрибут SNI содержит, как правило, только доменное имя и не содержит путь или параметры.

Общий порядок указания как URL, так и wildcard-выражения в собственной категории:

— Следует указывать URL или выражение без схемы (http:// или https://), порта и фрагмента.

— В конец URL или выражения автоматически и неявно добавляется подстановочный символ *, означающий в этом случае, что на его месте может находиться любой набор символов. Например, если вы указали example.com/mail, то этот URL будет неявно изменен на `example.com/mail*`. Выражению `example.com/mail*` соответствуют помимо прочего такие URL, как example.com/mail, example.com/mail/inbox и example.com/mailbox?lang=ru.

Внимание! Символ * не добавляется после подстановочных символов ^ или $ в конце выражения. Подробнее о подстановочных символах см. ниже в разделе «Использование подстановочных символов (см. раздел 18.2)».

— Если URL или выражение указано без пути, то сразу после доменного имени будет автоматически и неявно добавлена косая черта. Например, если вы указали example.com, то этот URL будет неявно изменен на выражение `example.com/*`. Такому выражению (`example.com/*`) будет соответствовать помимо прочего URL example.com/ и SNI example.com.

Внимание! Символы, добавляемые автоматически, не отображаются в карточке категории в системе управления.

Символы, добавляемые автоматически, могут быть добавлены вручную. Например, вы можете ввести example.com (вид после автодополнения — `example.com/*`), example.com/ или `example.com/*`. Добавленные вручную символы будут отображаться в карточке категории.

Примечание. Все три записи из примера выше (example.com, example.com/ и `example.com/*`) являются эквивалентными

Использование подстановочных символов

Вы можете составлять wildcard-выражения с использованием трех подстановочных символов: *, ^ и $.

Перед тем как приступить к составлению выражений, необходимо ознакомиться с понятием токена.

Токен — это набор символов:

— от начала URL без учета схемы до символа-разделителя,

— от символа-разделителя до другого ближайшего символа-разделителя,

— от символа-разделителя до конца URL.

Символы разделители: `. / ? & = ; +`.

К примеру, URL ngfw.ptsecurity.com/path имеет четыре токена: ngfw, ptsecurity, com и path.

Подстановочные символы указывают, в каком месте URL может быть любое значение токена.

Символ *, если находится внутри выражения, то соответствует одному и более токенам. Если находится в самом конце wildcard-выражения (то есть, является самым последним символом в выражении), то соответствует как отсутствию символов, так и любому символу в том числе и символам-разделителям.

Символ ^ соответствует только одному токену.

Символ $ означает конец строки. То есть, тот символ, перед которым указан $, является последним символом URL.

Примечание. Если $ расположен не в конце выражения, то он не является подстановочным символом. Например, выражению `example.com?$news=1$` будет соответствовать URL example.com?$news=1.

Особенности указания URL и выражений

- Одно и то же wildcard-выражение или URL можно указать не более чем в пяти собственных категориях.
- В одном выражении могут использоваться разные подстановочные символы. Пример — `*.example.^/`.
- Выражение может состоять только из подстановочных символов и разделителей. Примеры — `*.^, ^.^.^.^.*/`.
- Подстановочные символы не могут находиться внутри токена. Например, не поддерживаются такие выражения, как `example*.com/`, `example^.com/`, `example.com/news*/media`, `example.com/news^/media` и подобные. Символ * как часть токена может находиться только в самом конце выражения, например `example.com/news/media*`.
- Запрещены выражения с несколькими символами * подряд, например `www.*.*.com/`, `www.example.com/*/*`, `example.*/*` поскольку такое использование подстановочного символа нецелесообразно (все символы * могут быть заменены на один).
- Запрещены выражения, состоящие из единственного подстановочного символа.
- Использование множества символов ^ в одном выражении может негативно повлиять на производительность устройства — в зависимости от модели.
- После символа ^ в конце выражения символ * автоматически не добавляется. Примеры выражений даны ниже под номерами 2.1, 2.6—2.10.

18.3. Примеры wildcard-выражений

Внимание! В примерах в таблице ниже записи вида example.com (без завершающей косой черты) соответствуют значению атрибута TLS SNI.

Таблица 10. Примеры wildcard-выражений с использованием символа *

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
1.1	example.com **или** example.com/ **или** example.com/*	— example.com — example.com/ — example.com/**mail**	— www.example.com — www.example.com/ — abc.example.com/ — example.ru/ — example.ru/news

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
		— example.com/**test/folder2** — example.com/**news/folder2?parameter1&parameter2**	
1.2	***.example.com **или** ***.example.com/ **или** ***.example.com/***	— **www**.example.com — **www.**example.com/ — **docs**.example.com/ — **docs**.example.com/**any-path** — **abc.xyz**.example.com/ — **abc.xyz**.example.com/**any-path**	— www.example.ru — www.example.ru/ — example.com/ — example.com/any-path — other-site.com/folder1?url=www.example.com — other-site.com/folder1?url=www.example.com%2Fpath
1.3	mail.example.*** **или** mail.example.*/	— mail.example.**ru** — mail.example.**ru/** — mail.example.**gov.ru/** — mail.example.**test.co.uk/** — mail.example.**test.co.uk/inbox** — mail.example.**test.co.uk/inbox?parameter1&parameter2**	— docs.example.com — docs.example.com/
1.4	***.mail.example.*** **или** ***.mail.example.*/	— blog.mail.example.com — **blog**.mail.example.**com/** — **blog**.mail.example.**gov.ru/**	— news.example.com — news.example.com/ — 123.docs.example.com/

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
		— **blog.us**.mail.example.**test.co.uk/** — **test.blog.service.uk.any**.mail.example.**test.co.uk/inbox**	
1.5	www.*****.com **или** www.*****.com/ **или** www.*****.com/*****	— www.**example**.com — www.**example**.com/ — www.**xyz.example**.com/ — www.**xyz.example**.com/**any-path**	— abc.xyz.example.com — abc.xyz.example.com/ — www.example.ru/
1.6	example.com/news **или** example.com/news*****	— example.com/news — example.com/news**week** — example.com/news**123** — example.com/news**/** — example.com/news**?** — example.com/news**/folder** — example.com/news**?parameter1**	— example.com/video — example.com/photo/path
1.7	example.com/news/ **или** example.com/news/*****	— example.com/news/ — example.com/news/**any-path**	— example.com/news — example.com/news? — example.com/video — example.com/photo/any-path
1.8	example.com/mail? **или** example.com/mail?*****	— example.com/mail?**parameter1&parameter2** — example.com/mail?**parameter1&parameter2&parameter3**	— example.com/mail/ — example.com/mail& — example.com/test/folder2

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
1.9	example.com/news/***/folder1/ **или** example.com/news/***/folder1/***	— example.com/news/**sports**/folder1/ — example.com/news/**sports/football**/folder1/ — example.com/news/**sports/football/premierligue**/folder1/**any-path**	— example.com/news/folder1/ — example.com/news/sports/folder1? — example.com/news/sports/folder23/
1.10	***.227.58.243 **или** ***.227.58.243/ **или** ***.227.58.243/***	— **1**.227.58.243 — **1**.227.58.243/ — **123**.227.58.243/**any-path**	— 1.227.58.ru — 1.227.58.ru/ — 123.227.58.15/ — sub.112.123.227.58.org/ — 112.123.227.58.243.com/
1.11	12.***.58.34 **или** 12.***.58.34/ **или** 12.***.58.34/***	— 12.**12**.58.34 — 12.**56**.58.34/ — 12.**60**.58.34/**any-path**	— 12.227.58.ru — 12.227.58.ru/ — 12.1.227.58.ru/ — 123.100.58.15/ — 12.888.123.100.58.15.com/
1.12	12.15.58.*** **или** 12.15.58.*/	— 12.15.58.**154** — 12.15.58.**com** — 12.15.58.**154**/ — 12.15.58.**com**/ — 12.15.58.**200**/**any-path**	— 12.227.58.ru — 12.227.58.ru/ — 12.1.227.58.ru/ — 123.100.58.15/ — 12.888.123.100.58.15.com/

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
1.13	188.227.58.243 **или** 188.227.58.243/ **или** 188.227.58.243/*****	— 188.227.58.243 — 188.227.58.243/ — 188.227.58.243/**any-path**	— 190.227.58.ru — 190.227.58.ru/ — 190.227.58.243/news
1.14	188.227.58.243/news **или** 188.227.58.243/news*****	— 188.227.58.243/news — 188.227.58.243/news**week** — 188.227.58.243/news**123** — 188.227.58.243/news**123?query** — 188.227.58.243/news**/any-path** — 188.227.58.243/news**?any-path** — 188.227.58.243/news**&any-path**	— 188.227.58.243/video

Таблица 11. Примеры wildcard-выражений с использованием символа ^

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
2.1	example.com/**^**	— example.com/**mail** — example.com/**news**	— example.com/mail/ — example.com/folder1? — example.com/mail/folder2
2.2	**^**.example.com **или** **^**.example.com/ **или** **^**.example.com/*	— **www.**example.com — **www.**example.com/ — **abc**.example.com/ — **xyz**.example.com/	— www.example.ru — www.example.ru/ — abc.xyz.example.com/ — example.com/

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
		— **xyz**.example.com/any-path — **abc**.example.com/any-path	
2.3	mail.example.**^** **или** mail.example.**^**/ **или** mail.example.**^**/*	— mail.example.**ru** — mail.example.**ru**/ — mail.example.**org**/ — mail.example.**com**/ — mail.example.**com**/any-path — mail.example.**org**/any-path	— mail.example.gov.ru — mail.example.gov.ru/ — mail.example.test.co.uk/ — video.example.ru/
2.4	www.**^**.com **или** www.**^**.com/ или www.**^**.com/*	— www.**example**.com — www.**example**.com/ — www.**abc**.com/ — www.**abc**.com/any-path	— www.abc.example.com — www.abc.example.com/
2.5	www.**^**.**^**.com **или** www.**^**.**^**.com/ **или** www.**^**.**^**.com/*	— www.**abc**.**example**.com — www.**abc**.**example**.com/ — www.**abc**.**example**.com/any-path	— www.abc.xyz.example.com — www.abc.xyz.example.com/
2.6	example.com/mail/**^**	— example.com/mail/**folder1** — example.com//mail/**folder2** — example.com//mail/**folder3**	— example.com/mail/folder1/ — example.com/mail/folder2? — example.com/mail/folder1/folder2

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
			— example.com/mail?p=1 — example.com/mail& — example.com/news/folder2
2.7	example.com/mail?^	— example.com/mail?**parameter1**	— example.com/mail?parameter1&parameter2 — example.com/mail/folder1 — example.com/mail?folder1/
2.8	example.com/mail?parameter1=^&parameter2=^	— example.com/mail?parameter1=**5**&parameter2=**yes** — example.com/mail?parameter1=**no**&parameter2=**15**	— example.com/mail?parameter2=no&parameter1=15
2.9	example.com/mail?^=**5**&^=^	— example.com/mail?**parameter1**=5&**parameter2**=**yes** — example.com/mail?**parameter2**=5&**parameter1**=**15**	— example.com/mail?parameter1=10&parameter2=yes — example.com/mail?parameter2=no&parameter1=15 — example.com/mail?parameter2=5+parameter1=15
2.10	188.227.58.243/^	— 188.227.58.243/**news** — 188.227.58.243/**folder1**	— 188.227.58.243/news/ — 188.227.58.243/sports? — 190.227.58.243/news/folder2

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
2.11	example.com/mail?**^**=10 **или** example.com/mail?**^**=10*****	— example.com/mail?**parameter1**=10**&**parameter2=yes — example.com/mail?**parameter1**=100 — example.com/mail?**parameter1**=10test — example.com/mail?**parameter1**=10**&**any-thing — example.com/mail?**parameter2**=10**+**any-thing — example.com/mail?**parameter3**=10**;**any-thing	— example.com/mail?**parameter1**=**20** — example.com/mail?**parameter1**=**20**&any-thing — example.com/mail
2.12	**^**.227.58.243 **или** **^**.227.58.243/ **или** **^**.227.58.243/*****	— **1**.227.58.243 — **19**.227.58.243/ — **123**.227.58.243/ — **17**.227.58.243/any-path	— 1.227.58.ru — 1.227.58.ru/ — 123.227.58.15/
2.13	**^**.227.58.**^** **или** **^**.227.58.**^**/ **или** **^**.227.58.**^**/*****	— **1**.227.58.**245** — **17**.227.58.**245**/ — **123**.227.58.**1**/ — **123**.227.58.**ru**/ — **157**.227.58.**com**/ — **123**.227.58.**15**/any-path — **13**.227.58.**org**/any-path	— 1.227.50.ru — 1.227.50.ru/ — 123.100.58.15/

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
2.14	188.227.58.243/^/news **или** 188.227.58.243/^/news*	— 188.227.58.243/**folder1**/news — 188.227.58.243/**folder2**/news — 188.227.58.243/**folder3**/newsweek — 188.227.58.243/**folder4**/news/any-path	— 188.227.58.243/video/folder — 188.227.58.243/news/folder

Таблица 12. Примеры wildcard-выражений с использованием символа $

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
3.1	example.com**$** **или** example.com/$	— example.com — example.com/	— example.com/any-path — example.com/?query
3.2	example.com/news**$**	— example.com/news	— example.com/news/ — example.com/news/folder — example.com/newsweek — example.com/news?query — example.com/folder1
3.3	example.com/news/politics**$**	— example.com/news/politics	— example.com/news — example.com/news/politics123 — example.com/news/politics&query — example.com/news/politics?query — example.com/news/politics/folder2

№	Выражение	Соответствующие URL и SNI	Несоответствующие URL и SNI
3.4	example.com/news?query**$**	— example.com/news?query	— example.com/news?query123 — example.com/news?query& — example.com/news?query=param
3.5	example.com/tracker?p=$&p2=5**$**	— example.com/tracker?p=$&p2=5	— example.com/tracker?p=$&p2=5xyz — example.com/tracker?p=$&p2=57
3.6	example.*/**$**	— example.com — example.abc.com — example.abc.def.com — example.abc.def.com/ — example.abc.def.ghi.ru/ — example.abc.def.ghi.jkl.org/	— example.com/any-path — example.abc.def.com/any-path

18.4. Добавление категории URL

Добавление категорий происходит в разделе **Объекты** → **Категории URL**.

► Чтобы добавить категорию URL:

1. Нажмите **Добавить**.
2. Введите название категории.
3. Если требуется, введите описание.
4. Добавьте один или более URL.
5. Сохраните изменения.

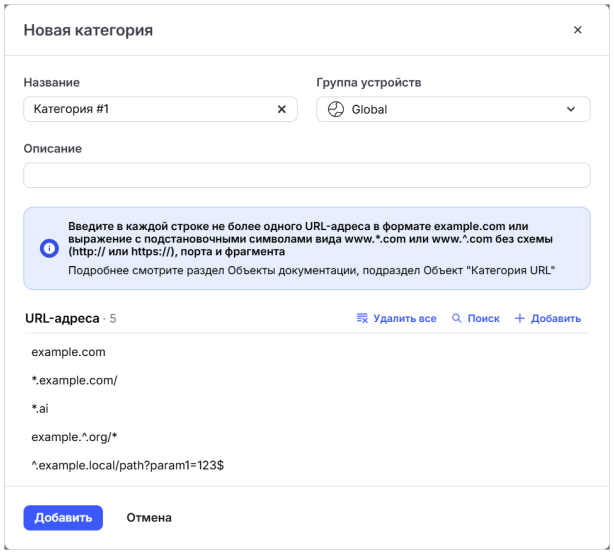


Рисунок 111. Добавление категории URL

18.5. Предустановленные категории

Со списком и описанием предустановленных категорий URL вы можете ознакомиться в соответствующем разделе (см. раздел 42).

19. Работа с группами устройств

Группам устройств (см. раздел 6.5) назначаются виртуальные контексты и правила межсетевого экрана. Правила группы устройств используются всеми назначенными ей виртуальными контекстами.

- Чтобы добавить группу устройств:

  1. В главном меню выберите **Политики**, **Объекты** или **Устройства**.
  2. В контекстном меню группы устройств выберите **Добавить дочернюю группу**.
  3. Введите название группы устройств.
  4. Если требуется, введите описание.

     Примечание. Рекомендуется добавлять описание для упрощения последующей работы с группой.
  5. Нажмите **Добавить**.

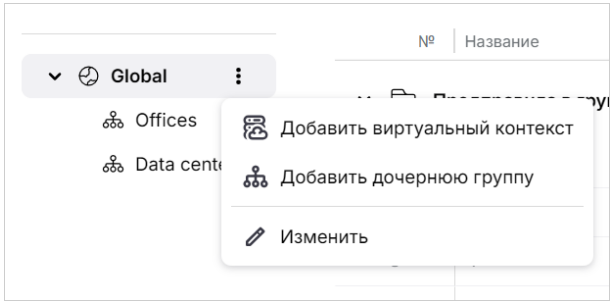


Рисунок 112. Контекстное меню группы устройств

20. Работа с виртуальными контекстами

Виртуальные контексты (см. раздел 6.6) используются для разделения устройства на логические независимые межсетевые экраны. Добавляя виртуальный контекст, пользователь назначает ему сабинтерфейсы и прикрепляет к группе устройств.

- Чтобы добавить виртуальный контекст:

  1. В главном меню выберите **Устройства**.
  2. Выберите устройство, в которое вы хотите добавить виртуальный контекст.
  3. Нажмите **Добавить**.
  4. Введите название виртуального контекста.
  5. Если требуется, введите описание.
  6. Назначьте виртуальному контексту сабинтерфейсы.
  7. Если требуется, на вкладке **Конфигурация** назначьте виртуальному контексту IPS-профиль.

     Примечание. Подробнее об IPS-профиле виртуального контекста см. в разделе «IPS (система предотвращения вторжений) (см. раздел 22)».
  8. Нажмите **Добавить**.

Вы можете изменить или удалить виртуальный контекст, используя контекстное меню.

21. Работа с виртуальными роутерами

Виртуальный роутер — программное обеспечение, эмулирующее работу физического маршрутизатора. Виртуальные роутеры имеют независимые таблицы маршрутизации и изолированы один от другого.

Примечание. Дополнительную информацию о виртуальных роутерах см. в разделе «Принцип работы (см. раздел 6.7)».

- Чтобы добавить виртуальный роутер:

1. В главном меню выберите **Устройства**.
2. Выберите устройство, в которое вы хотите добавить виртуальный роутер.
3. Выберите вкладку **Виртуальные контексты**.
4. Нажмите на название виртуального контекста, в который вы хотите добавить виртуальный роутер.
5. Выберите вкладку **Виртуальные роутеры**.
6. Нажмите **Добавить**.
7. Введите название виртуального роутера.
8. Если требуется, введите описание.
9. Если требуется, включите **ECMP** (Equal-Cost Multi-Path) — режим балансировки, при котором трафик сетевой сессии может передаваться по нескольким маршрутам с одинаковой стоимостью.

   Внимание! Режим ECMP не применяется к маршрутам, полученным по протоколу BGP.

   Примечание. Режим ECMP поддерживает до 16 равнозначных маршрутов.
10. Назначьте виртуальному роутеру сабинтерфейсы.

    Примечание. В списке **Интерфейсы** отображаются только те сабинтерфейсы, которым назначен режим работы маршрутизатора, и сабинтерфейсы, не назначенные другим виртуальным роутерам.
11. Если требуется, измените административные дистанции, которые различные типы маршрутов имеют по умолчанию.

    Примечание. Административная дистанция используется для выбора оптимального маршрута при наличии двух и более маршрутов различных типов до одного и того же пункта назначения. Чем ниже значение, тем предпочтительнее маршрут.
12. Если требуется, отключите виртуальный роутер.
13. Нажмите **Добавить**.

Вы можете изменить параметры роутера или удалить его через контекстное меню роутера на вкладке **Виртуальные роутеры**.

22. IPS (система предотвращения вторжений)

Система предотвращения вторжений (IPS), входящая в состав PT NGFW, позволяет защититься от атак, использующих уязвимости приложений. IPS проверяет проходящий через PT NGFW трафик и при обнаружении подозрительной или вредоносной активности блокирует сессию. Вредоносная или подозрительная активность выявляется путем проверки трафика на соответствие сигнатурам.

Система настраивается на странице **Объекты** → **IPS** путем создания групп сигнатур и профилей:

— Группы содержат сигнатуры, соответствующие различным угрозам. Одна сигнатура может быть добавлена одновременно в несколько групп сигнатур.

— Профиль объединяет группы. Одна группа может быть добавлена одновременно в несколько профилей.

— Профили назначаются правилам безопасности. Когда правилу назначен профиль, трафик, разрешенный к передаче этим правилом, проверяется на соответствие сигнатурам из этого профиля.

Для любой группы на уровне профиля можно указать действие при обнаружении трафика, соответствующего сигнатурам группы. Если действие не указано, то будет выполняться рекомендованное действие, то есть, действие, указанное в сигнатуре. Вы также можете отключить журналирование — тогда обнаружение угрозы не будет сопровождаться созданием записи в журнале **IPS** (по умолчанию журналирование включено).

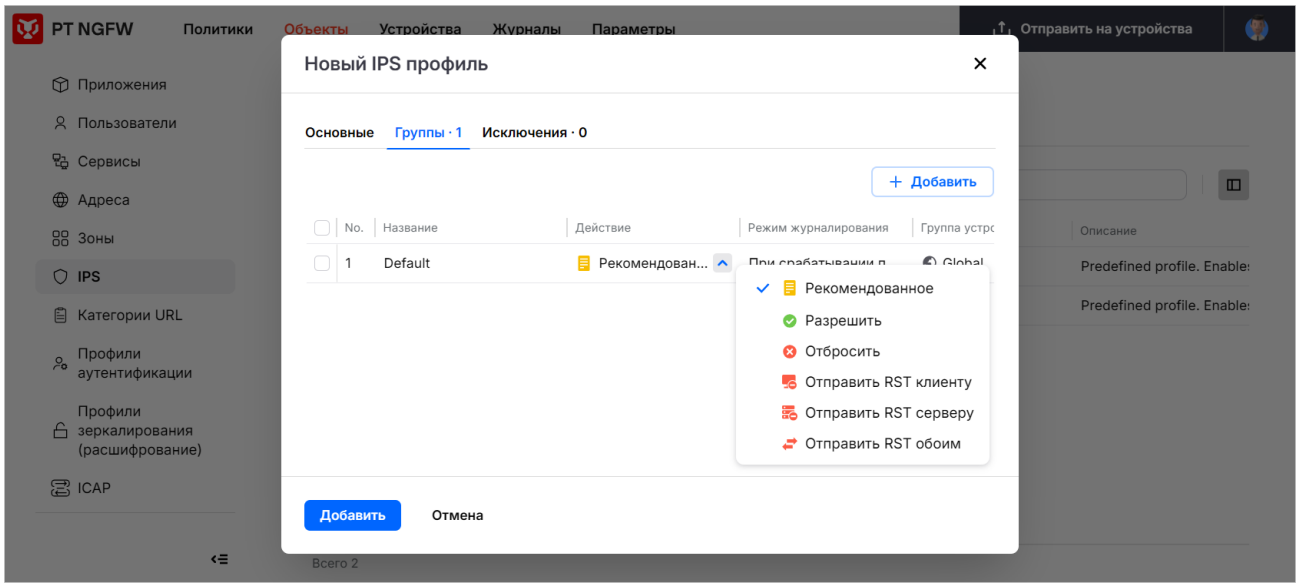


Рисунок 113. Выбор действия для группы профиля

Профили могут содержать не только группы, но и исключения:

— Исключением может быть любая сигнатура.

— Для исключения можно указать действие при обнаружении соответствующего трафика и отключить журналирование.

— При обнаружении трафика, соответствующего исключению, будет всегда производится действие и журналирование исключения.

Исключения могут использоваться, например, для исключения ложных срабатываний, то есть предотвращения блокирования трафика, ошибочно определяющегося как угроза.

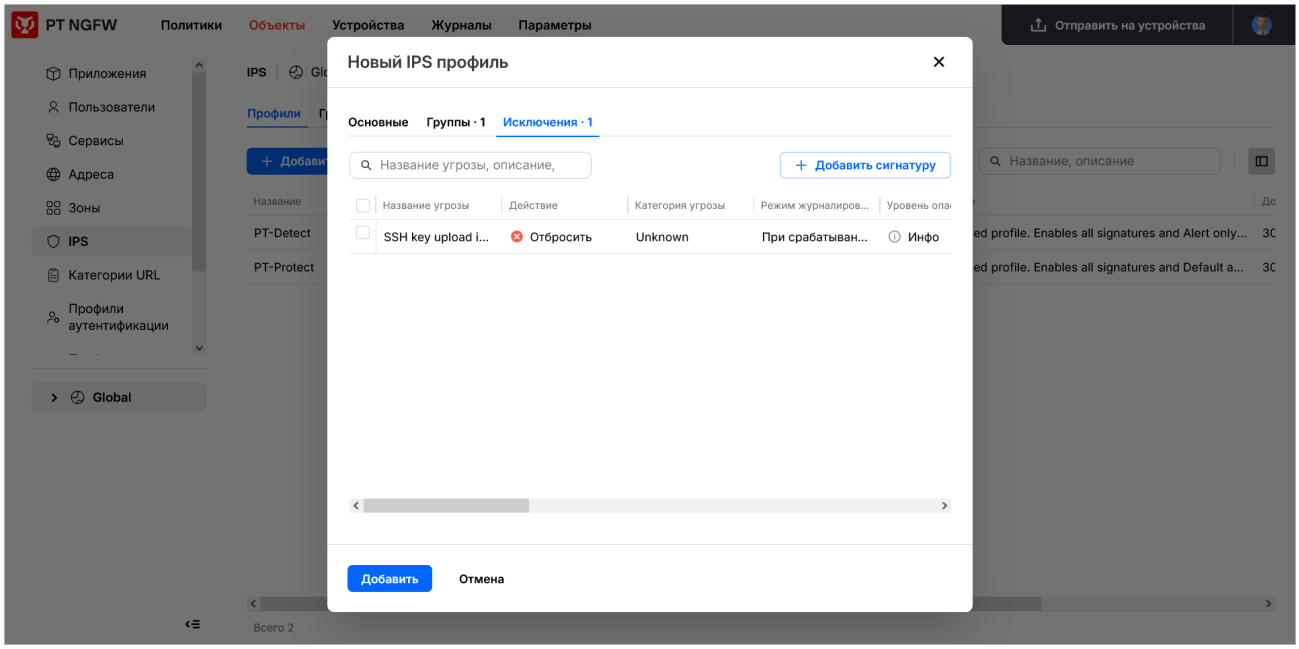


Рисунок 114. Исключения профиля

Профили назначаются правилам безопасности на вкладке **Действие при срабатывании**.

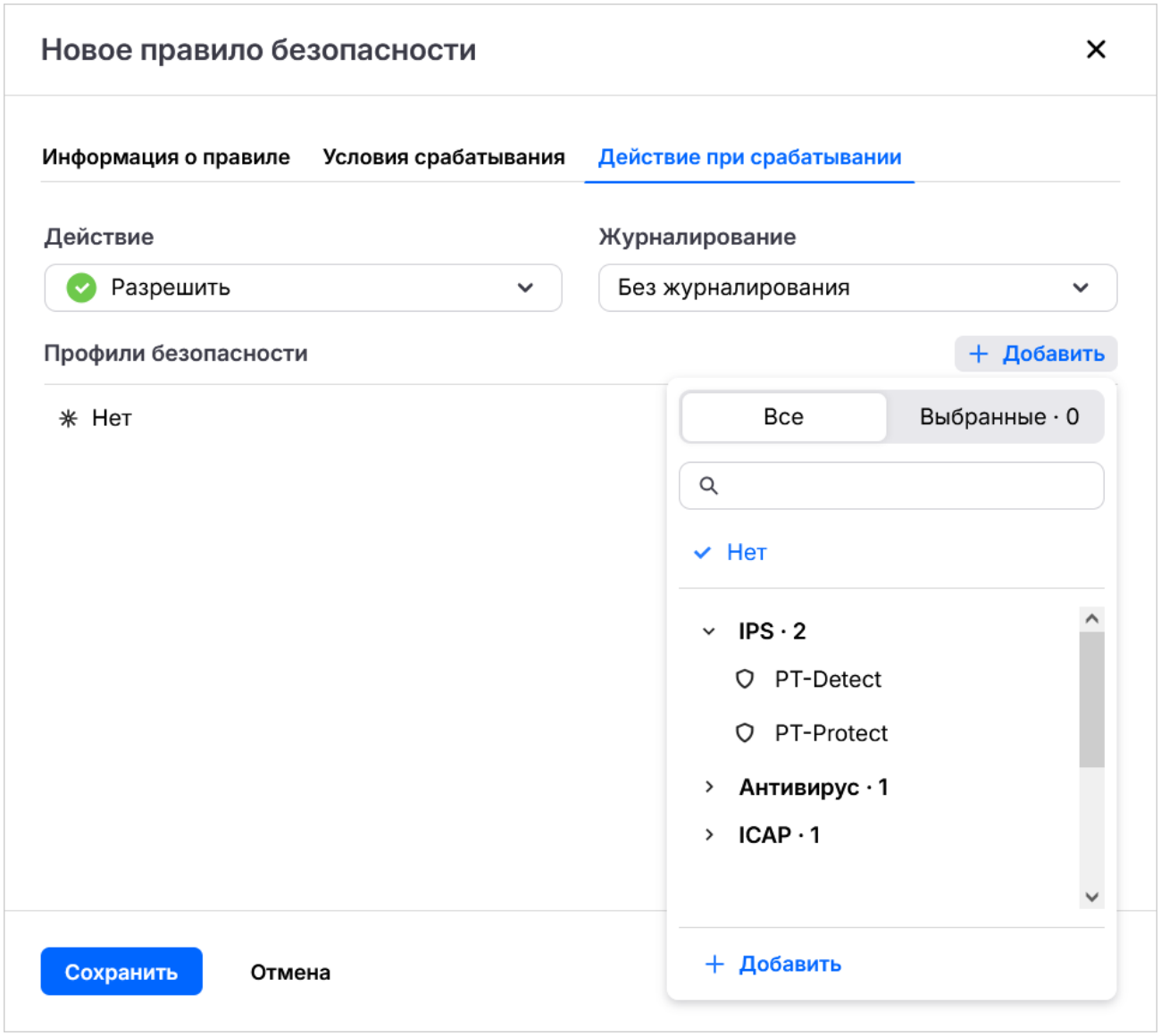


Рисунок 115. Назначение профиля правилу безопасности

Предустановленные группы и профили

PT NGFW поставляется с группой **Default**, содержащей все рекомендуемые сигнатуры. При обновлении PT NGFW группа **Default** будет также автоматически обновлена. Эта группа включена в предустановленные профили **PT-Protect** и **PT-Detect**. В профиле **PT-Protect** действие группы **Default** не переопределяется; в профиле **PT-Detect** действие группы — разрешение трафика.

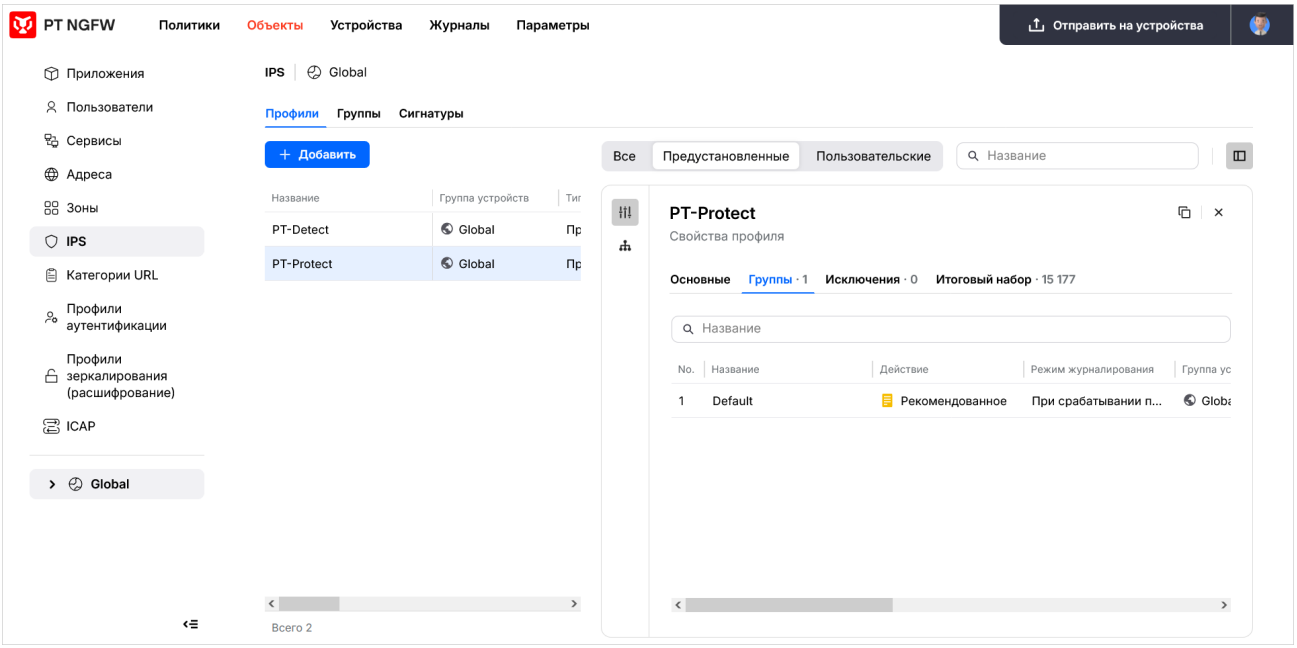


Рисунок 116. Карточка профиля **PT-Protect**

Порядок проверки трафика

Проверка трафика системой происходит следующим образом:

— сначала происходит проверка исключениями;

— затем идет проверка сигнатурами в группах профиля, начиная с первой сигнатуры первой группы сигнатур.

Для профиля из примера ниже сначала будет происходить проверка сигнатурами «группы А», затем сигнатурами «группы Б» и затем сигнатурами «группы В».

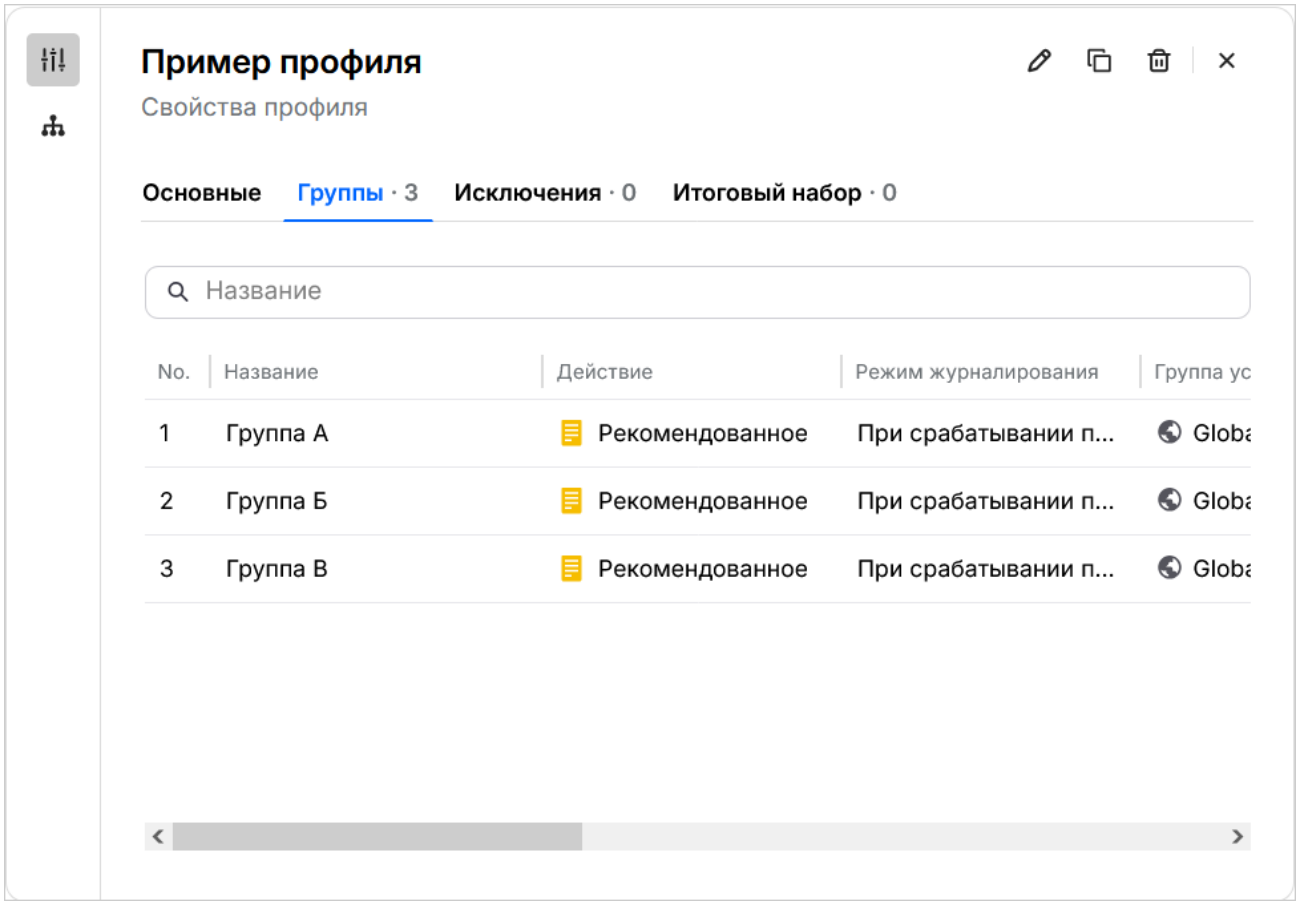


Рисунок 117. Порядок проверки трафика

Примечание. При срабатывании сигнатуры с запрещающим действием дальнейшая проверка трафика не выполняется.

Профиль виртуального контекста (предклассификации)

Вы можете назначить профиль виртуальному контексту.

Такой профиль действует на этапе поиска подходящего правила безопасности, то есть до момента его нахождения (см. также «Порядок обработки трафика».). Если профиль не назначен, то часть атак может быть не обнаружена и не заблокирована. Это связано с тем, что для определения некоторых приложений, указанных в качестве критериев срабатывания правила, межсетевому экрану требуется передать (пропустить) некоторое количество данных сессии. IPS-профиль виртуального контекста позволяет защититься от угроз безопасности, которые могут возникнуть из-за передачи этих данных.

Профиль виртуального контекста, или IPS-профиль предклассификации, может быть назначен при добавлении или изменении контекста (см. раздел 20).

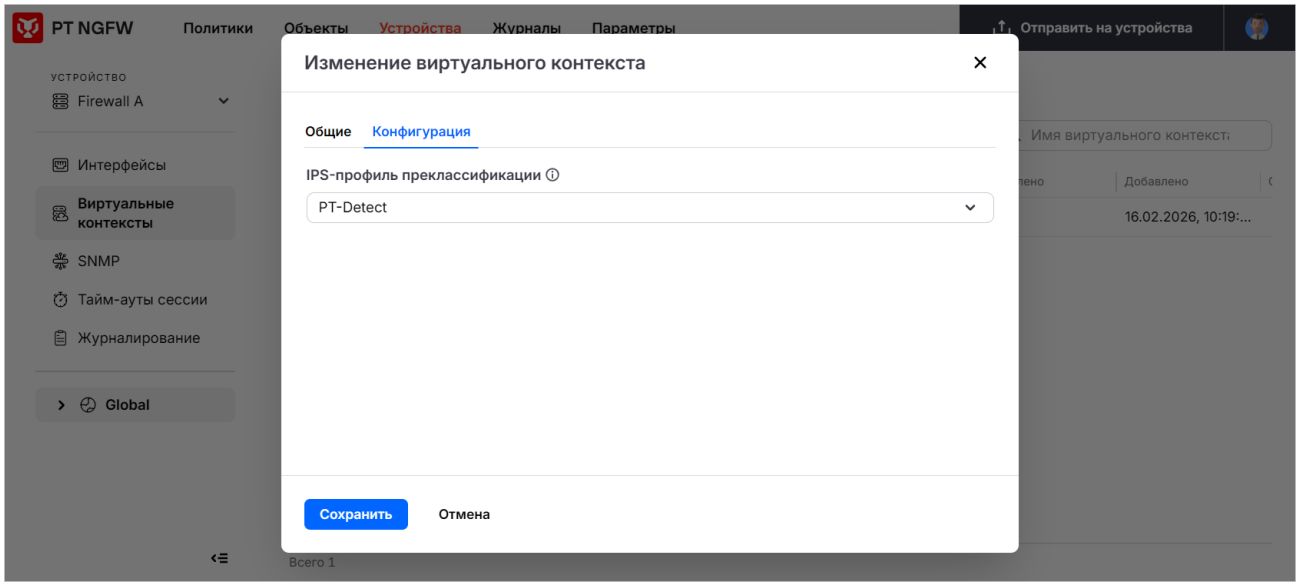


Рисунок 118. Выбор IPS-профиля предклассификации

Добавление группы сигнатур

- Чтобы добавить группу сигнатур:

  1. В главном меню выберите **Объекты**.
  2. Выберите вкладку **IPS**.
  3. Выберите вкладку **Группы**.
  4. Нажмите **Добавить**.
  5. Введите название группы.
  6. Выберите вкладку **Сигнатуры**.
  7. Добавьте сигнатуры.
  8. Нажмите **Добавить**.

Группа сигнатур может быть изменена или удалена — в контекстном меню группы на вкладке **Группы**.

Добавление IPS-профиля

- Чтобы добавить IPS-профиль:

  1. В главном меню выберите **Объекты**.
  2. Выберите вкладку **IPS**.
  3. Нажмите **Добавить**.
  4. Введите название профиля.

5. Добавьте группы сигнатур:
   - Выберите вкладку **Группы**.
   - Добавьте группы.

     Примечание. Вы можете изменить позицию группы в профиле путем ее перетаскивания.
   - Если требуется, переопределите действие группы, выбрав в столбце **Действие** другое действие.
   - Если требуется, отключите журналирование группы, выбрав в столбце **Журналирование** значение **Без журналирования**.
6. Если требуется, добавьте исключения:
   - Выберите вкладку **Исключения**.
   - Добавьте исключения.
   - Если требуется, переопределите действие исключения и (или) отключите журналирование.
7. Нажмите **Добавить**.

IPS-профиль может быть изменен или удален — в контекстном меню профиля на вкладке **Профили**.

Просмотр информации о сигнатурах

На странице **Объекты** → **IPS** → **Сигнатуры** вы можете увидеть полный список сигнатур и информацию о каждой из них.

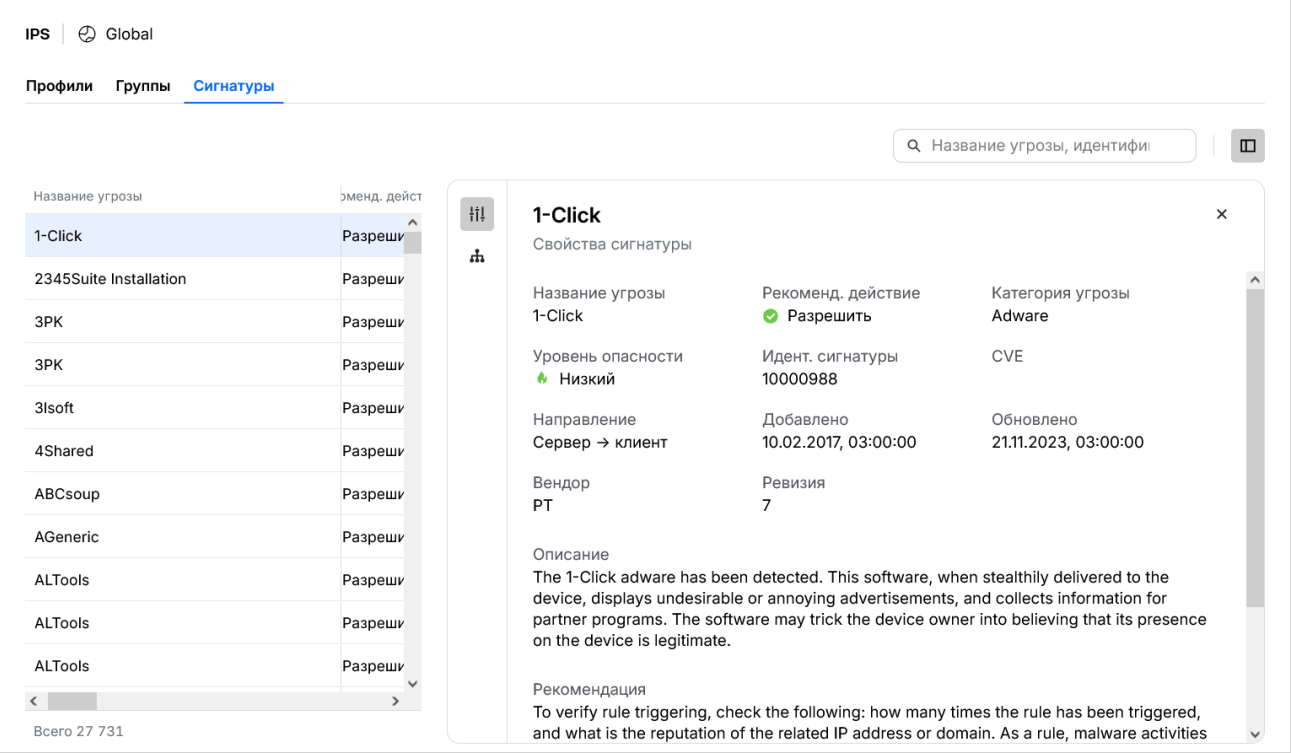


Рисунок 119. Информация о сигнатуре

Примечание. Возможность добавления собственных сигнатур не предусмотрена.

Просмотр списка сигнатур профиля

Вы можете увидеть итоговый набор сигнатур профиля в карточке профиля на вкладке **Итоговый набор**.

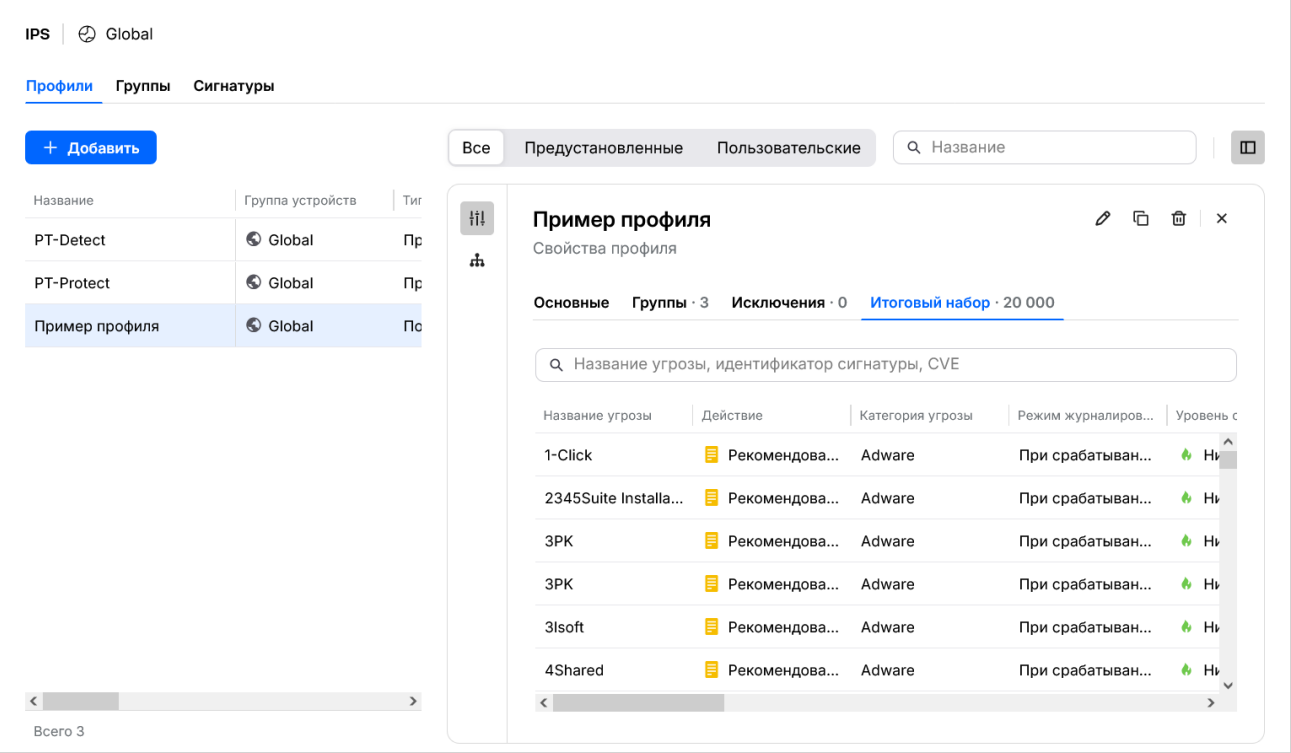


Рисунок 120. Итоговый набор сигнатур профиля

Просмотр связей сущностей

Вы можете увидеть, как связаны между собой сущности IPS, правила безопасности и виртуальные контексты. Например, вы можете увидеть, к каким правилам применен тот или иной IPS-профиль. На рисунке ниже показано отображение связей для сигнатуры, которая добавлена в две группы и не используется как исключение ни в одном из IPS-профилей.

Чтобы увидеть связность, в карточке IPS-профиля, группы сигнатур или сигнатуры, нажмите .

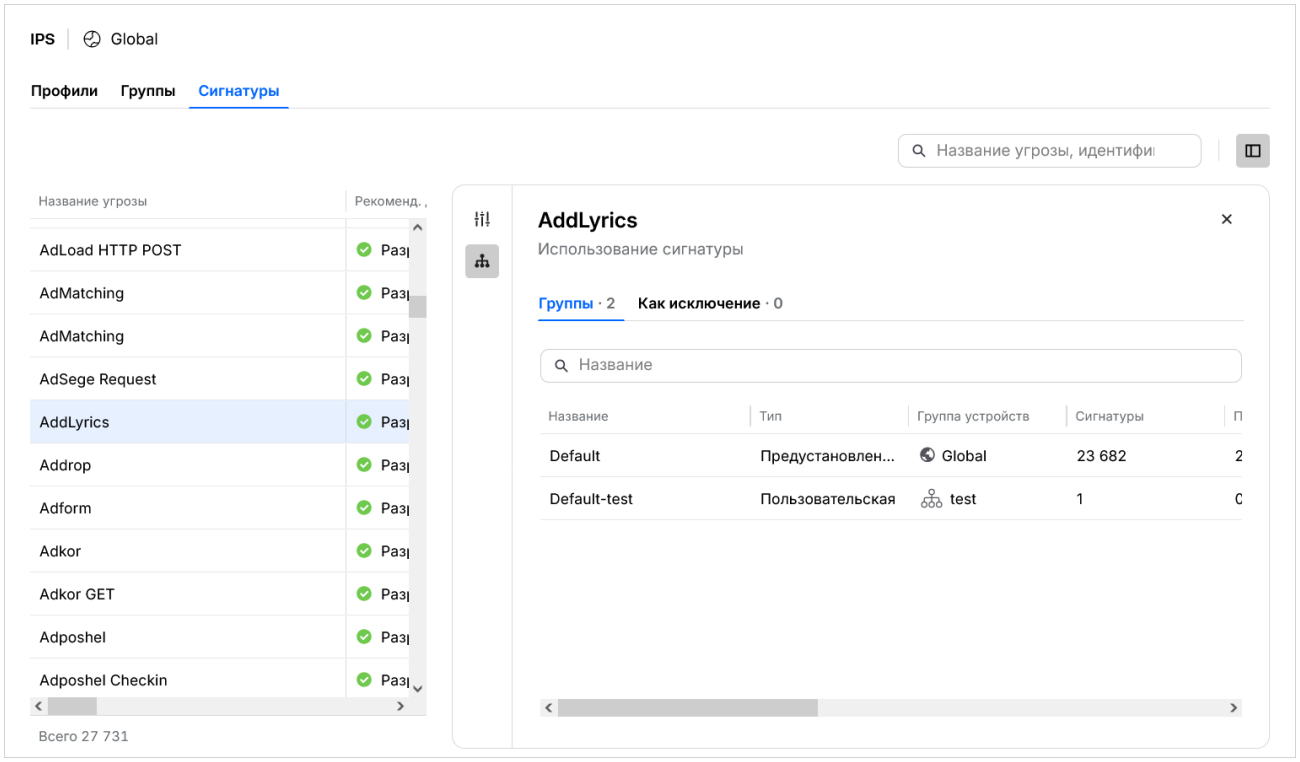


Рисунок 121. Связи сигнатуры

23. Антивирусная проверка трафика

Встроенный в межсетевой экран антивирус позволяет обнаружить в передаваемом через устройство трафике зараженный файл и предотвратить его передачу. Файл считается зараженным, если его хеш-сумма находится в базе данных хеш-сумм зараженных файлов (сигнатур). Проверке (сравнению хеш-сумм) подвергаются файлы, передаваемые по протоколу HTTP. Проверка выполняется путем выбора антивирусного профиля в правиле безопасности. От выбранного профиля зависит, будет ли заблокирован трафик, подпадающий под условия правила и содержащий файл, определяемый как зараженный.

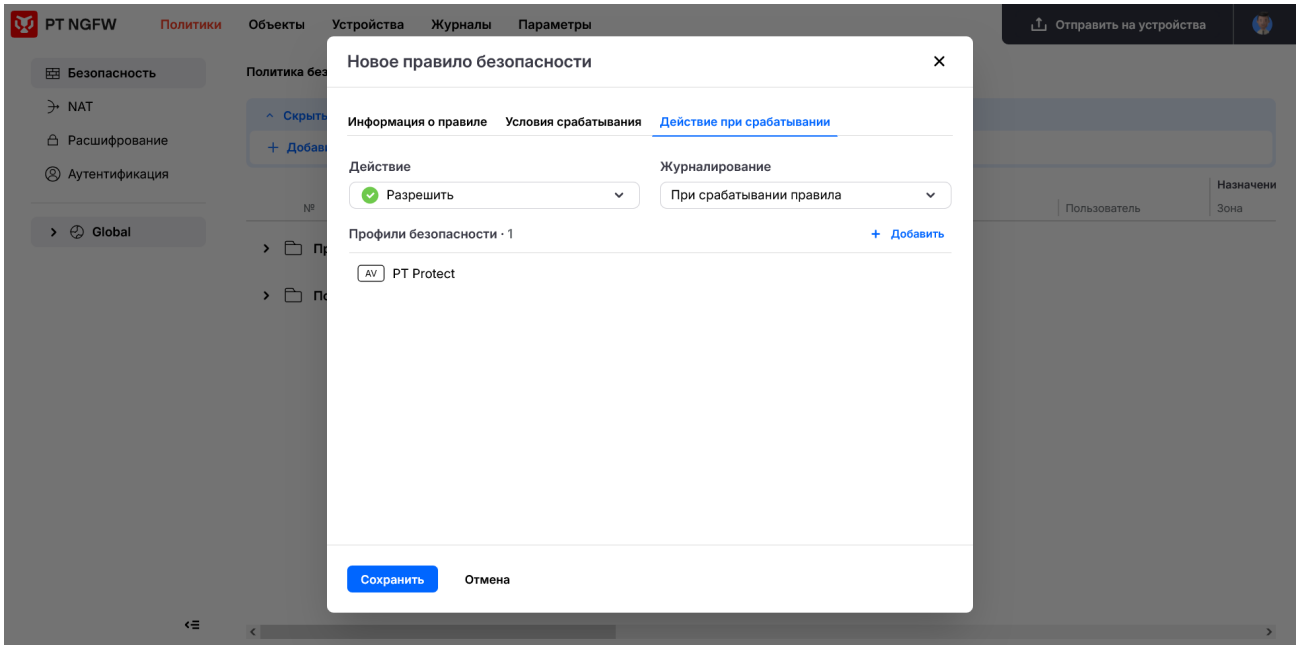


Рисунок 122. Включение антивирусной проверки

Примечание. Обновление базы данных антивирусных сигнатур выполняется через установку пакета экспертизы.

Вы можете выбрать один из двух антивирусных профилей:

— **PT Protect**. Когда выбран этот профиль и обнаруживается угроза, трафик блокируется. Блокирование сопровождается отправкой сообщения TCP RST клиенту и серверу и созданием записи в журнале **Антивирус**.

— **PT Detect**. Когда выбран этот профиль и обнаруживается угроза, трафик не блокируется. В журнале **Антивирус** создается запись об обнаружении.

- Чтобы выполнить антивирусную проверку трафика,

  в правиле безопасности, разрешающем передачу трафика, в блоке параметров **Профили безопасности** нажмите **Добавить** и выберите антивирусный профиль безопасности.

24. NAT

Трансляция сетевых адресов (англ. network address translation, NAT) — это механизм, позволяющий изменить (транслировать) информацию об источнике или (и) назначении в заголовке IP-пакета и заголовках TCP и UDP, а именно IP-адрес или IP-адрес и номер порта источника или (и) назначения. Наиболее частые сценарии применения NAT: предоставление возможности устройствам в частной сети взаимодействовать с устройствами в публичной сети (интернете) без назначения каждому устройству публичного IP-адреса (Source NAT) и предоставление доступа к ресурсам, находящимся во внутренней сети, используя ограниченное количество публичных IP-адресов (Destination NAT).

В PT NGFW настройка NAT производится в разделе **Политики** путем добавления, удаления или изменения правил NAT. Правило NAT позволяет указать, в каком трафике необходимо выполнять трансляцию и ее тип. Параметры трафика, трансляцию адресов и портов которого необходимо выполнить, указываются в разделе **Исходный пакет** правила NAT.

Поиск межсетевым экраном подходящего правила NAT начинается с первого правила и выполняется до нахождения полного соответствия полученного трафика условиям в одном из правил. Правила являются терминальными, то есть при нахождении правила, которому соответствует сетевой пакет, поиск прекращается. Если сетевой пакет не соответствует ни одному правилу, трансляция не выполняется.

Одно правило NAT позволяет выполнять трансляцию IP-адресов и TCP- и UDP-портов источника, назначения, либо одновременно источника и назначения.

Поиск подходящего правила NAT выполняется до проверки трафика правилами безопасности. Если для пакета найдено подходящее правило NAT, то сама трансляция выполняется либо до, либо после проверки трафика правилами безопасности (в зависимости от указанного в правиле NAT действия), либо и до, и после (если в правиле NAT настроена трансляция обоих адресов — источника и получателя).

> **Внимание!** В правилах безопасности следует указывать адрес и порт источника (source) до трансляции, а адрес и порт назначения (destination) — после трансляции, то есть фактические адреса и порты клиента и сервера. Ниже приведены подробное описание и примеры настройки правил безопасности и правил NAT.

Трансляция информации об источнике (Source NAT)

В PT NGFW трансляция информации об источнике может выполняться в адрес исходящего сабинтерфейса или в пул адресов:

— При трансляции в адрес исходящего сабинтерфейса исходный адрес источника заменяется на адрес исходящего сабинтерфейса, а порт заменяется на случайный порт из массива. Исходящий сабинтерфейс определяется на основе таблицы маршрутизации. Для

всех пакетов одной сессии трансляция выполняется в один и тот же IP-адрес и порт источника. Если требуется произвести замену, а свободных портов в массиве нет, пакет отбрасывается.

— При трансляции в пул адресов исходный адрес источника и порт заменяются на случайные адрес из пула и порт из массивов. Замена происходит для всех пакетов одной сессии. Когда требуется произвести трансляцию, а свободных адресов или портов нет, пакет отбрасывается.

Трансляция информации об источнике происходит после проверки пакета правилами безопасности.

PT NGFW выполняет динамическую трансляцию вида Source NAT + PAT (port address translation), то есть адреса (из пула) и порты назначаются динамически, а не зафиксированы статически за транслируемыми адресами. В таблице трансляций NAT PT NGFW запись создается только после инициирования соединения клиентской стороной. В таблице указаны исходные адрес и порт источника, а также адрес и порт источника после трансляции. Такая запись позволяет выполнить обратное преобразование адреса и порта при получении межсетевым экраном ответа от серверной стороны для того, чтобы ответ успешно достиг клиента.

При трансляции в пул адресов PT NGFW обеспечивает резервирование IP-адресов за клиентами, то есть одному и тому же IP-адресу источника будет назначаться один и тот же IP-адрес в ходе выполнения трансляции информации об источнике в рамках одного и того же правила NAT.

Трансляция информации о назначении (Destination NAT)

В PT NGFW при трансляции информации о назначении исходный адрес назначения заменяется на случайный адрес из массива и порт назначения, если требуется, заменяется на указанный. Замена происходит для всех пакетов одной сессии.

Такая трансляция происходит до проверки пакета правилами безопасности. После трансляции адреса назначения (в связи с тем, что он изменился) межсетевой экран выполняет еще один поиск в таблице маршрутизации для определения исходящего интерфейса и, как следствие, зоны назначения (destination zone) за тем, чтобы выполнить дальнейший поиск подходящего правила политики безопасности.

Трансляция исходного IP-адреса назначения и, если требуется, порта назначения выполняется в пул адресов и заданный порт назначения. Пул может включать различное количество IP-адресов: от одного до множества. При этом, если пул содержит множество адресов, то исходный адрес назначения в запросе будет транслироваться в разные адреса назначения.

Для выбора конкретного IP-адреса назначения из пула применяется алгоритм хеширования исходного IP-адреса клиента, который учитывает размер пула. Запросы одного клиента будут транслироваться в один и тот же адрес назначения из пула (при условии, что IP-адрес источника клиента не изменяется от запроса к запросу). Один и тот же клиент (с тем же адресом источника) будет попадать на один и тот же сервер из пула, пока пул не изменится.

Внимание. Если адресом назначения во входящих пакетах является адрес интерфейса PT NGFW, то при настройке правила трансляции зоной назначения должна быть указана зона **Local**. Если адрес назначения во входящих пакетах отличается от адреса интерфейса PT NGFW, то при настройке правила трансляции зоной назначения должна быть указана зона интерфейса, на который поступают подлежащие трансляции пакеты.

Для равномерной балансировки запросы должны поступать от большого количества клиентов с различными адресами. Если запросы поступают от одного и того же клиента, то адрес назначения в его запросах будет транслироваться в один и тот же адрес назначения из пула независимо от размера пула.

Практические сценарии применения Destination NAT см. в разделе Примеры настройки Destination NAT (см. раздел 24.2).

В этом разделе

Пример настройки Source NAT (см. раздел 24.1)

Примеры настройки Destination NAT (см. раздел 24.2)

Пример двойной трансляции (Twice NAT) (см. раздел 24.3)

Пример U-Turn NAT (Hairpin NAT, Loopback NAT, Reflection NAT) (см. раздел 24.4)

Proxy ARP (см. раздел 24.5)

24.1. Пример настройки Source NAT

У организации может не быть возможности назначать каждому внутреннему узлу отдельный публичный адрес. Чтобы обеспечить доступ всех узлов корпоративной сети в интернет вы можете использовать трансляцию адресов источника: все внутренние адреса транслируются в адрес внешнего интерфейса маршрутизатора (или в пул публичных адресов). В этом случае для внешних ресурсов в интернете все подключения от узлов организации выглядят как подключения, исходящие с одного IP-адреса (или с нескольких адресов из пула). Исходный порт источника транслируется в случайный (или случайный порт из заданного диапазона). Изменение портов источника позволяет транслировать более одного внутреннего адреса (если трансляция выполняется в адрес исходящего интерфейса) или более внутренних адресов, чем количество адресов в пуле (если трансляция выполняется в пул адресов).

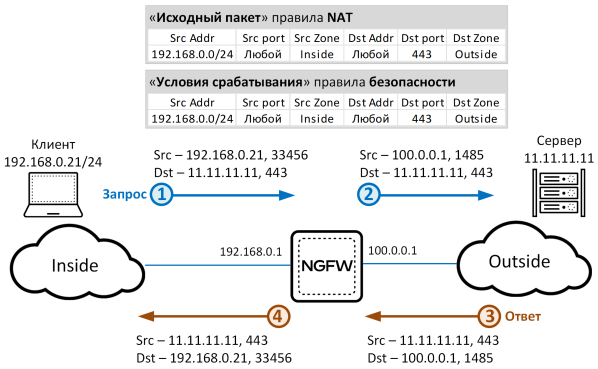


Рисунок 123. Схема Source NAT

На схеме выше внутренний узел с адресом 192.168.0.21 делает запрос к внешнему серверу 11.11.11.11. Адрес внутреннего узла транслируется в адрес внешнего интерфейса межсетевого экрана, 100.0.0.1, а порт заменяется на случайный, 1485. При получении ответного потока трафика из зоны **Outside** с адресом назначения 100.0.0.1 и портом 1485 происходит обратная трансляция.

Для реализации данной схемы:

1. Создайте правило NAT с трансляцией адреса источника как на рисунке ниже.

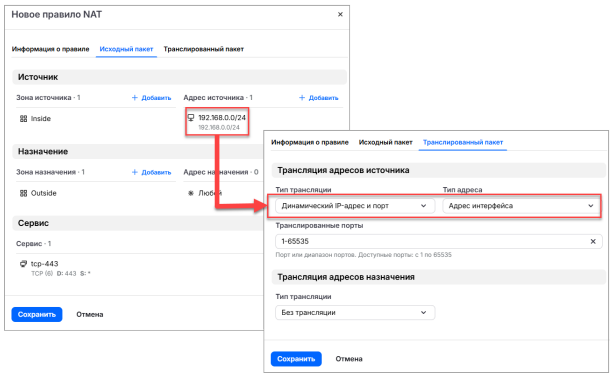


Рисунок 124. Настройка Source NAT

2. Создайте правило безопасности, разрешающее внутренним узлам доступ во внешнюю сеть. Адресом источника является адрес до трансляции, то есть подсеть, которой фактически принадлежат адреса интерфейсов клиентских устройств.

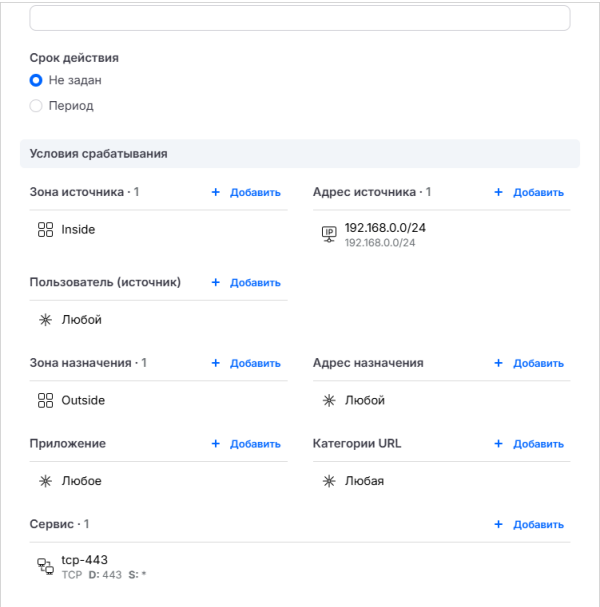


Рисунок 125. Настройка разрешающего правила безопасности

24.2. Примеры настройки Destination NAT

Вы можете использовать трансляцию адресов назначения чтобы предоставлять узлам, находящимся за пределами организации, доступ к внутренним сетевым ресурсам. Ниже приведены примеры настройки Destination NAT в зависимости от того, какой адрес является адресом назначения.

Пример 1. Адресом назначения является адрес интерфейса PT NGFW

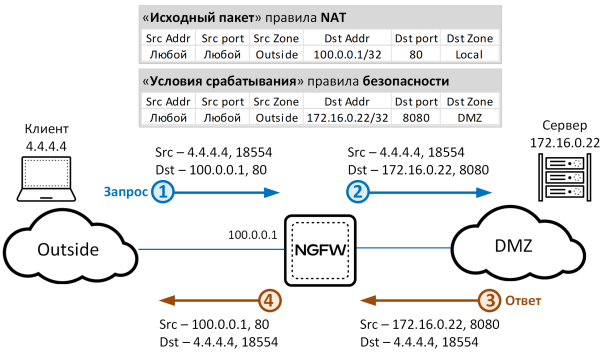


Рисунок 126. Схема Destination NAT, если адресом назначения является адрес интерфейса PT NGFW

В данной схеме узел 4.4.4.4, находящийся в интернете, обращается к веб-серверу организации с адресом 172.16.0.22. Обратиться на фактический адрес веб-сервера узел 4.4.4.4 не может, поскольку адрес сервера принадлежит внутренней сети (информация о доступности которой в интернете отсутствует). Узел 4.4.4.4 обращается на публичный (внешний) адрес интерфейса

межсетевого экрана 100.0.0.1. PT NGFW транслирует адрес назначения в адрес 172.16.0.22 и пересылает запрос веб-серверу. В зависимости от настроек может выполняться трансляция порта назначения. В данном примере порт назначения 80 исходного запроса транслируется в порт 8080.

Для реализации данной схемы:

1. Создайте правило NAT с трансляцией адреса назначения как на рисунке ниже. Поскольку адресом назначения является адрес интерфейса PT NGFW, то в качестве зоны назначения необходимо указывать зону **Local**.

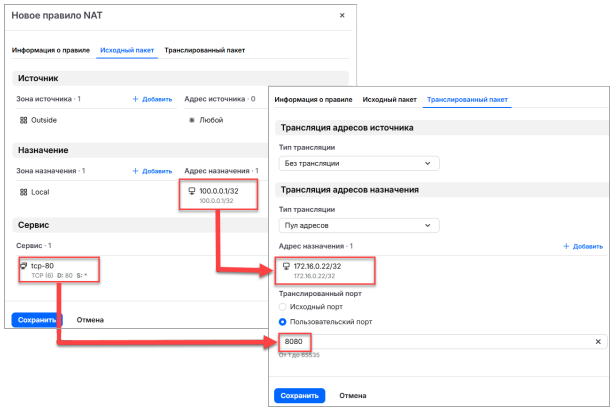


Рисунок 127. Настройка Destination NAT, если адресом назначения является адрес интерфейса PT NGFW

2. Создайте правило безопасности, разрешающее внешним узлам доступ к веб-серверу. Адресом и портом назначения являются IP-адрес и порт после трансляции, то есть фактические IP-адрес и порт веб-сервера.

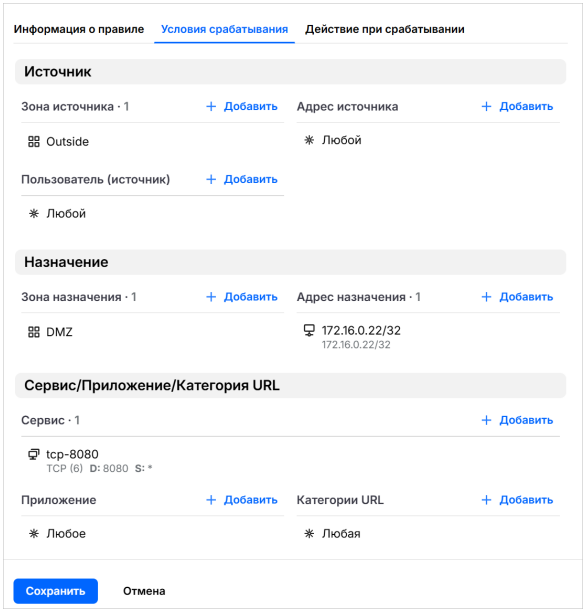


Рисунок 128. Настройка разрешающего правила безопасности

Пример 2. Адресом назначения является адрес из диапазона (пула) адресов

Если адрес назначения во входящих IP-пакетах не является адресом интерфейса PT NGFW, то в качестве зоны назначения необходимо указывать зону интерфейса, на который поступают пакеты.

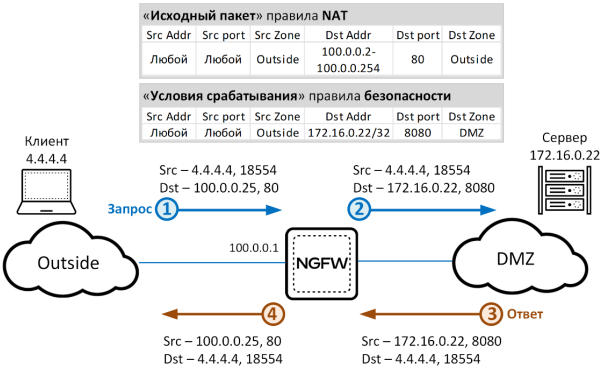


Рисунок 129. Схема Destination NAT, если адресом назначения является адрес из пула адресов

В данной схеме узел с адресом 4.4.4.4, находящийся в интернете, обращается на публичный адрес 100.0.0.25 диапазона (пула) 100.0.0.2-100.0.0.254. Интерфейс, на который поступают пакеты, подлежащие трансляции, имеет адрес 100.0.0.1/24 и находится в зоне безопасности **Outside**. Межсетевой экран выполняет трансляцию адреса назначения в адрес 172.16.0.22 и пересылает запрос веб-серверу. Порт назначения 80 исходного запроса транслируется в порт 8080.

Для реализации данной схемы:

1. Создайте правило NAT с трансляцией адреса назначения как на рисунке ниже. В качестве зоны назначения в правиле NAT необходимо указывать зону **Outside**.

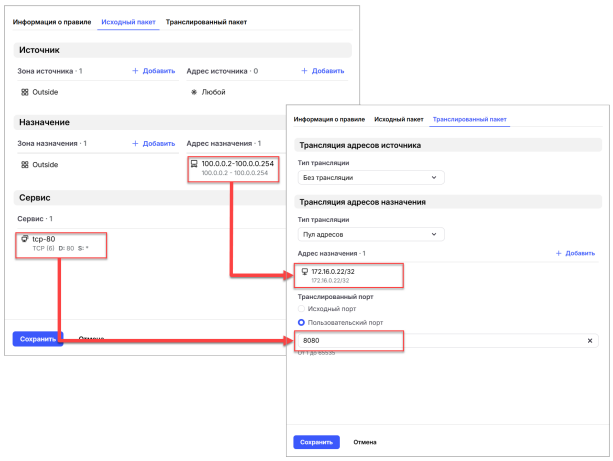


Рисунок 130. Настройка Destination NAT, если адресом назначения является адрес из пула адресов

Создайте правило безопасности, разрешающее внешним узлам доступ к веб-серверу. Адресом и портом назначения являются IP-адрес и порт после трансляции, то есть фактические IP-адрес и порт веб-сервера.

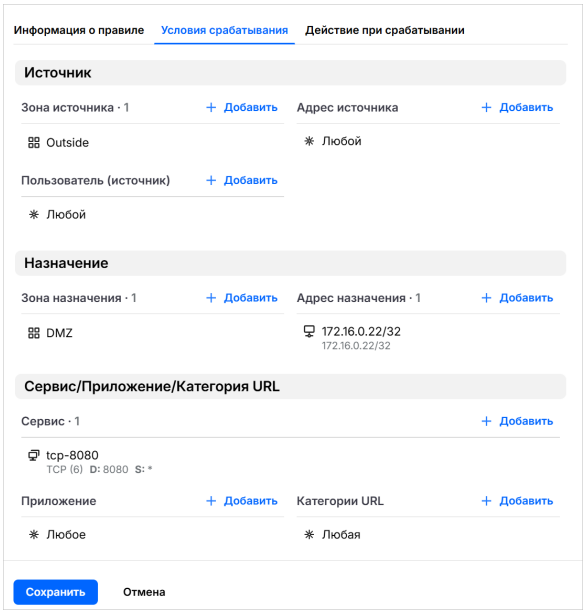


Рисунок 131. Настройка разрешающего правила безопасности

Пример 3. Адресом назначения является адрес подсети интерфейса PT NGFW с трансляцией в пул адресов получателя

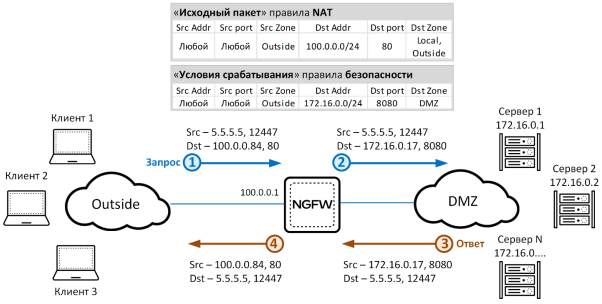


Рисунок 132. Схема Destination NAT, если адресом назначения является адрес подсети интерфейса PT NGFW с трансляцией в пул адресов

В данной схеме множество клиентов, находящийся в интернете, обращаются на один из публичных адресов подсети 100.0.0.0/24 интерфейса PT NGFW. В связи с тем, что адресом назначения может быть как адрес интерфейса PT NGFW (100.0.0.1), так и другие адреса подсети интерфейса, то в правиле NAT необходимо указывать две зоны безопасности назначения: **Local** и **Outside** (ей принадлежит интерфейс, на который поступают пакеты). Трансляция выполняется во множество адресов назначения. Межсетевой экран транслирует адреса назначения в один из адресов пула, включающего все адреса подсети 172.16.0.0/24, и пересылает запрос одному из веб-серверов. Порт назначения 80 исходного запроса транслируется в порт 8080.

Для реализации данной схемы:

1. Создайте правило NAT с трансляцией адреса назначения как на рисунке ниже. В качестве зон назначения в правиле NAT необходимо указывать обе зоны — **Local** и **Outside**.

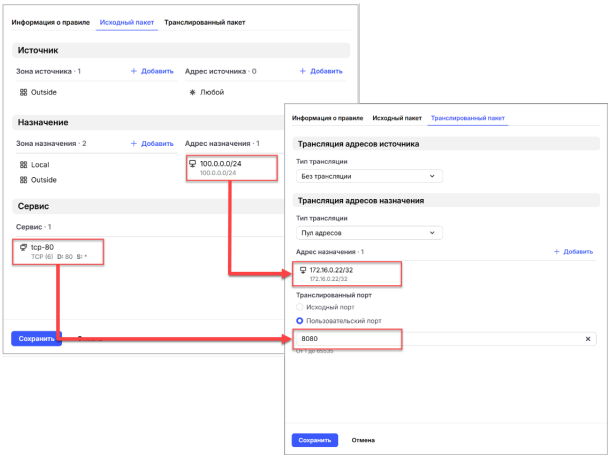


Рисунок 133. Настройка Destination NAT, если адресом назначения является адрес подсети интерфейса с трансляцией в пул адресов

2. Создайте правило безопасности, разрешающее внешним узлам доступ к веб-серверу. Адресом и портом назначения являются адрес подсети пула и порт после трансляции, то есть фактические IP-адреса и порты веб-серверов.

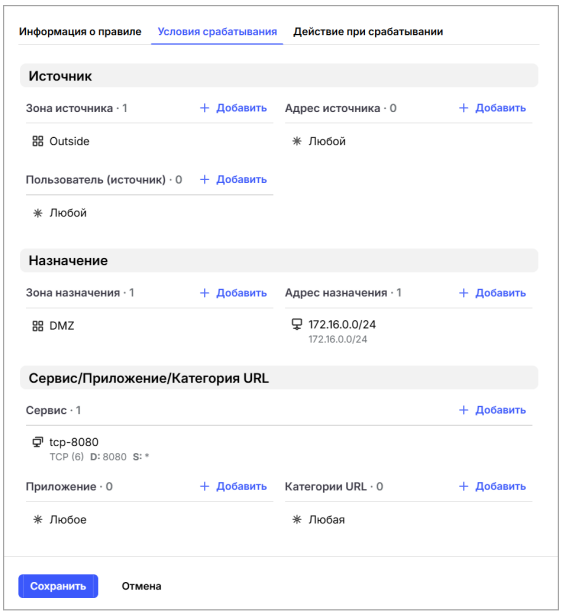


Рисунок 134. Настройка разрешающего правила безопасности

24.3. Пример двойной трансляции (Twice NAT)

PT NGFW позволяет в одном правиле NAT настроить одновременную трансляцию как адресов и портов источника, так и назначения (Twice NAT).

Например, внешние клиенты обращаются на публичный IP-адрес сервера. Межсетевой экран транслирует IP-адреса источников запросов, заменяя их на адрес своего внутреннего интерфейса. Сервер не имеет маршрута в адрес клиентов, например, не имеет маршрута по умолчанию. Таким образом, сервер не инициирует сам сессии в интернет, а отвечает только на запросы, источником которых с его точки зрения является межсетевой экран.

На схеме ниже клиент с IP-адресом 200.200.0.1 отправляет запрос в адрес сервера, 100.0.0.1, и TCP-порт назначения 443. Фактический адрес сервера — 172.20.0.1. В пакете запроса межсетевой экран заменяет адрес назначения с 100.0.0.1 на 172.20.0.1, оставляет исходное значение порта назначения, 443, и изменяет адрес источника с 200.200.0.1 на 172.20.0.254.

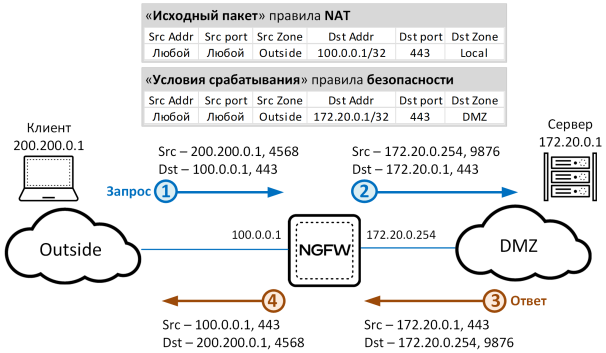


Рисунок 135. Схема трансляции адресов источника и назначения (Twice NAT)

Для реализации схемы Twice NAT:

1. Создайте правило NAT с трансляцией адресов источника и назначения как на рисунке ниже.

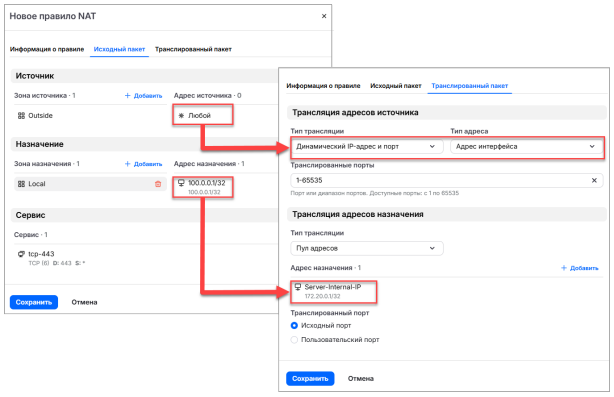


Рисунок 136. Настройка Twice NAT

2. Создайте правило безопасности, разрешающее внешним узлам доступ к веб-серверу.

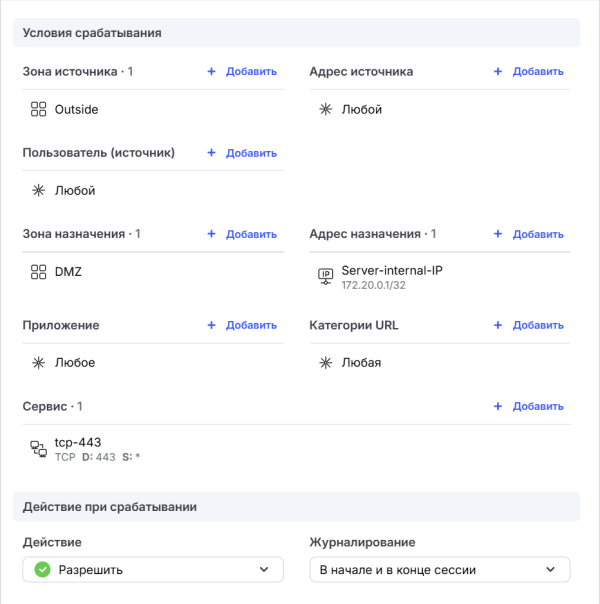


Рисунок 137. Разрешающее правило безопасности для Twice NAT

24.4. Пример U-Turn NAT (Hairpin NAT, Loopback NAT, Reflection NAT)

Конфигурация U-Turn NAT (Hairpin NAT), как правило, требуется, если сервер доступен из публичной сети, но также необходимо, чтобы к серверу был доступ изнутри сети через внешний (публичный) адрес сервера, например, в ситуации, если DNS-сервер, выполняющий преобразование имени сервера в IP-адрес, содержит информацию только о публичном адресе сервера.

Например, клиент, имеющий IP-адрес 172.16.0.1 обращается к серверу, который имеет публичный адрес 2.2.2.2 и TCP-порт 443. В действительности сервер имеет внутренний IP-адрес 172.16.0.2. В пакете запроса межсетевой экран изменят как адрес назначения с 2.2.2.2 на 172.16.0.2 и порт назначения с 443 на 80, так и адрес источника с 172.16.0.1 на 172.16.0.254.

В таком сценарии используется двойная трансляция, так как при использовании только Destination NAT для изменения IP-адреса (порта) назначения сервера сервер отвечал бы клиенту напрямую и в адресе источника ответа значился фактический IP-адрес сервера, 172.16.0.2. Однако клиент делал запрос на публичный адрес сервера, 2.2.2.2, следовательно, клиент отбросил бы ответ сервера, так как он не делал запросы в адрес 172.16.0.2. Поэтому на межсетевом экране также необходимо изменить IP-адрес источника в запросе клиента (выполнить Source NAT) так, чтобы сервер не мог ответить клиенту напрямую (если клиент и сервер находятся в одной подсети или могут взаимодействовать в обход межсетевого экрана) и чтобы ответ всегда шел через межсетевой экран.

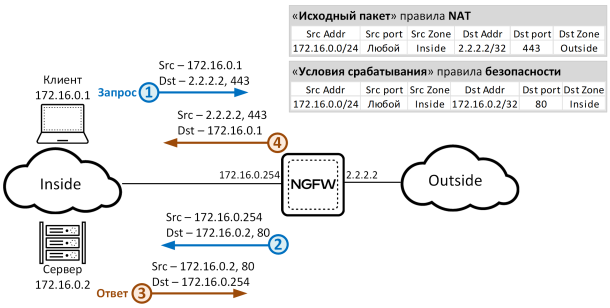


Рисунок 138. Схема U-Turn (Hairpin) NAT, если клиент и сервер находятся в одной зоне безопасности (подсети)

Для реализации данной схемы:

1. Создайте правило NAT как на рисунке ниже.

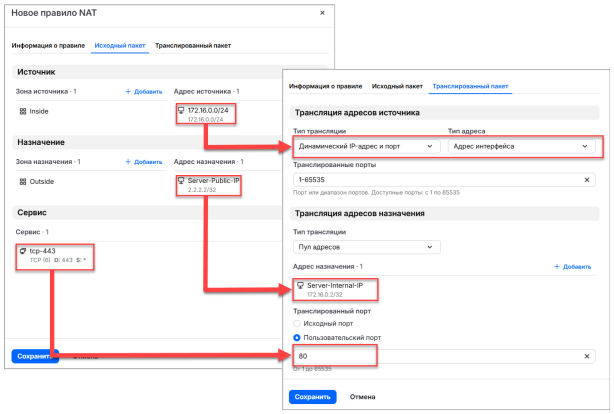


Рисунок 139. Настройка U-Turn (Hairpin) NAT, если клиент и сервер находятся в одной зоне безопасности (подсети)

2. Создайте разрешающее правило безопасности.

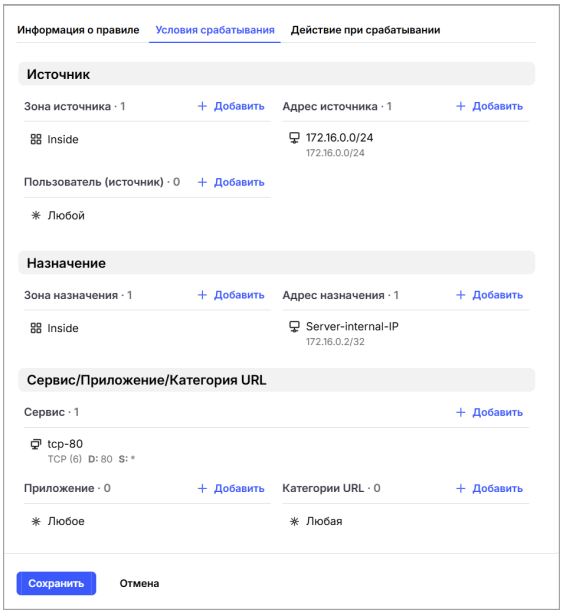


Рисунок 140. Разрешающее правило для U-Turn (Hairpin) NAT, если клиент и сервер находятся в одной зоне безопасности (подсети)

Более вероятным является сценарий, в котором клиент и сервер находятся в разных зонах безопасности и, скорее всего, в разных подсетях. Однако без U-Turn NAT ответ сервера клиенту может идти в обход межсетевого экрана и клиент отбросит пакеты ответа сервера, так как IP-адресом источника в таких пакета будет значиться не тот адрес, куда клиент отправлял запрос.

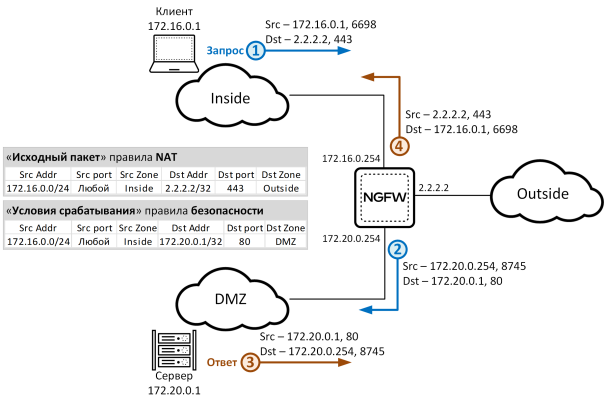


Рисунок 141. Схема U-Turn (Hairpin) NAT, если клиент и сервер находятся в разных зонах безопасности (подсетях)

Для реализации данной схемы:

1. Создайте правило NAT как на рисунке ниже.

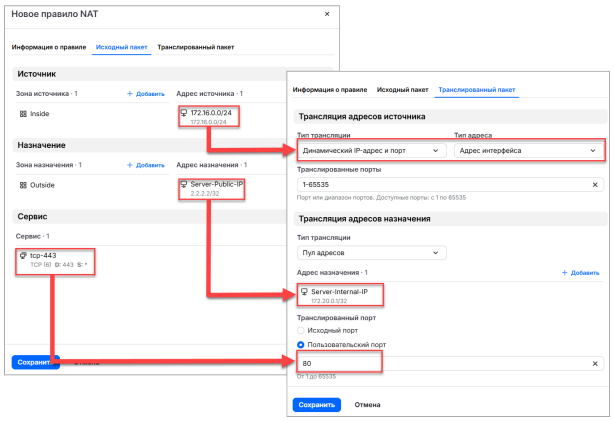


Рисунок 142. Настройка U-Turn (Hairpin) NAT, если клиент и сервер находятся в разных зонах безопасности (подсетях)

2. Создайте разрешающее правило безопасности.

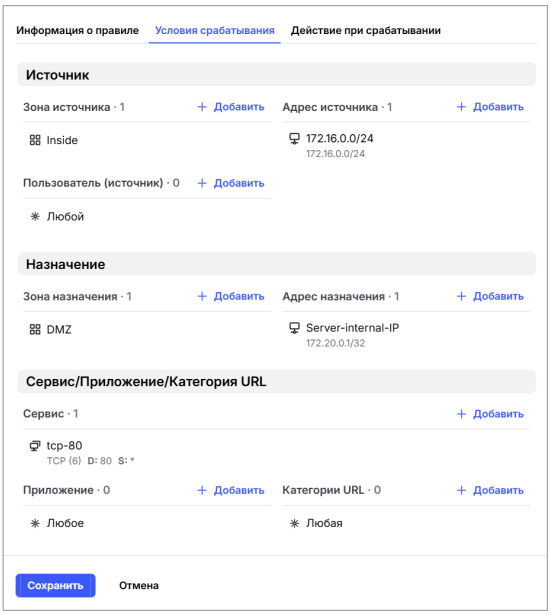


Рисунок 143. Разрешающее правило U-Turn (Hairpin) NAT, если клиент и сервер находятся в разных зонах безопасности (подсетях)

24.5. Proxy ARP

Если трансляция выполняется в пул адресов, либо в транслируемых IP-пакетах адрес назначения отличается от адреса интерфейса межсетевого экрана, то PT NGFW автоматически отвечает на ARP-запросы для таких IP-адресов.

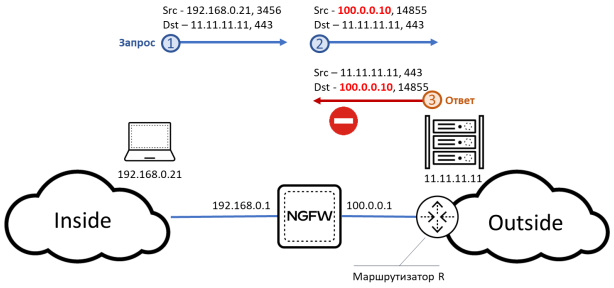


Рисунок 144. Трансляция в пул адресов без применения Proxy ARP

На схеме выше внутренний узел 192.168.0.21 выполняет запрос к внешнему серверу 11.11.11.11. Адрес внутреннего узла транслируется в адрес 100.0.0.10, не являющийся адресом внешнего интерфейса межсетевого экрана, 100.0.0.1, то есть трансляция выполняется в другой, отличный от адреса интерфейса адрес. Маршрутизатор R — это маршрутизатор провайдера, к которому подключен межсетевой экран и через который межсетевой экран имеет доступ во внешние сети. Маршрутизатор R, получив пакет ответа сервера, в котором IP-адресом назначения значится адрес 100.0.0.10, выполнит ARP-запрос, касающийся MAC-адреса для IP-адреса 100.0.0.10, чтобы определить, куда далее переслать пакет.

> **Примечание.** Функция Proxy ARP необходима для пересылки ответных IP-пакетов от маршрутизатора к NGFW. Иначе в приведенной схеме маршрутизатор R будет считать, что получателя не существует и отбросит пакеты.

PT NGFW автоматически отвечает на ARP-запросы для адресов NAT-пула, если эти адреса находятся в одной подсети с адресом интерфейса межсетевого экрана, на который поступил ARP-запрос. В примере выше адрес интерфейса PT NGFW — 100.0.0.1/24. Запрос ARP от маршрутизатора имеет вид «Какой MAC-адрес у узла с IP-адресом 100.0.0.10?». Адрес 100.0.0.10 и адрес интерфейса межсетевого экрана 100.0.0.1 принадлежат одной подсети 100.0.0.0/24. Следовательно, PT NGFW ответит на такой ARP-запрос MAC-адресом своего интерфейса. Явная настройка или включение Proxy ARP на PT NGFW не требуется.

Если трансляция выполняется в адресный пул, принадлежащей отличной от подсети интерфейса подсети, то PT NGFW не отвечает на такие ARP-запросы. В таком случае для успешного прохождения трафика на маршрутизаторе необходимо создать статический маршрут для подсети пула и в качестве next hop указать IP-адрес интерфейса PT NGFW.

25. Агрегирование каналов (LAG, LACP)

Агрегирование каналов — объединение нескольких физических каналов связи в один логический (LAG, Link Aggregation Group) для увеличения пропускной способности сети и повышения ее надежности. Если один из физических каналов выходит из строя, трафик автоматически перераспределяется между оставшимися, что обеспечивает отказоустойчивость LAG.

В PT NGFW вы можете создать агрегированный интерфейс (LAG-интерфейс), включающий от 2 до 8 физических интерфейсов, при этом соответствующие каналы связи объединяются и образуют агрегированный канал. Скорости объединенных каналов суммируются, увеличивая пропускную способность. Созданный LAG-интерфейс настраивается как обычный физический, при этом входящие в него интерфейсы не требуют индивидуальной настройки.

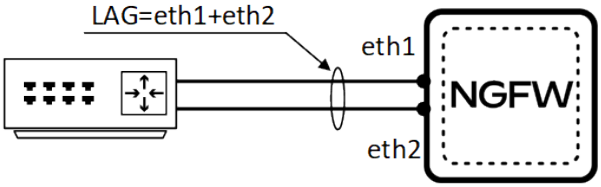


Рисунок 145. Агрегированный канал между PT NGFW и коммутатором

PT NGFW поддерживает два способа агрегирования каналов:

— Статический — канальное оборудование настраивается вручную. Этот способ не требует дополнительных накладных расходов, однако имеет ограничения и не обеспечивает контроль целостности линии;

— Динамический (LACP) — параметры агрегации автоматически согласуются по протоколу LACP (Link Aggregation Control Protocol) в соответствии с IEEE 802.3ax. Это позволяет избегать ошибок коммутации и динамически перераспределять нагрузку при выходе из строя физических каналов. Протокол LACP использует LACPDU-сообщения для согласования параметров агрегированного канала между двумя устройствами.

Особенности работы LACP в PT NGFW

— LAG-интерфейс может работать в двух режимах: активном (отправлять LACPDU-сообщения и инициировать LACP-сессию), либо в пассивном (только отвечать на полученные LACPDU). Для согласования работы LAG, хотя бы один из входящих в агрегацию интерфейсов должен работать в активном режиме.

— При работе PT NGFW в кластере LACP-сессия устанавливается активным узлом, поэтому при переключении кластера требуется время на установление новой LACP-сессии. Вы можете ускорить переключение кластера, включив режим предварительного согласования (**LACP Pre-Negotiation**).

  При этом резервный узел кластера заранее инициирует LACP-сессию и согласует параметры агрегированного интерфейса. При переключении кластера новый активный узел не тратит время на согласование LACP, что минимизирует потери IP-пакетов.

— Физический интерфейс в составе LAG может находиться в одном из состояний: selected (интерфейс участвует в передаче трафика) или standby (интерфейс находится в режиме ожидания и не передает трафик).

— В передаваемых PT NGFW LACPDU-сообщениях значения параметров System Priority и Port Priority равны 32768.

В этом разделе

Создание LAG-интерфейса (см. раздел 25.1)

Агрегирование каналов в кластере (см. раздел 25.2)

Примеры настройки LACP со сторонним оборудованием (см. раздел 25.3)

25.1. Создание LAG-интерфейса

Примечание. Рекомендуется объединять интерфейсы в количестве, равном степени двойки (2, 4, 8), для равномерного распределения трафика.

► Чтобы добавить LAG-интерфейс:

1. В главном меню выберите **Устройства**.
2. Выберите устройство, для которого вы хотите создать LAG-интерфейс.
3. Нажмите **Интерфейсы** → **Добавить** → **LAG-интерфейс**.
4. Введите номер (уникальный идентификатор интерфейса).
5. Если требуется, введите описание.
6. Выберите режим работы интерфейса: **LACP (активный)**, **LACP (пассивный)** или **Статический**.
7. Если требуется, установите частоту передачи LACPDU-сообщений: **Часто** (каждую секунду) или **Редко** (каждые 30 секунд).

   Примечание. Время ожидания ответного LACPDU-сообщения до перехода в состояние standby при значении **Часто** составляет 30 секунд, при значении **Редко** — 90 секунд.
8. При работе PT NGFW в кластере вы можете выбрать режим предварительного согласования с помощью флажка **Предсогласование LACP в кластере A/S**. По умолчанию предварительное согласование включено.
9. Выберите режим балансировки пакетов — балансировку по хеш-сумме на основе IP-адресов и портов источника и назначения, IP- и MAC-адресов источника и назначения или MAC-адресов источника и назначения.
10. Нажмите **+Добавить** и выберите физические интерфейсы, которые должны входить в LAG-интерфейс.

Примечание. Можно указывать только физические интерфейсы с одним сабинтерфейсом Untagged, не связанным с виртуальным роутером, соединением vWire или профилем зеркалирования.

11. Нажмите **Добавить**.

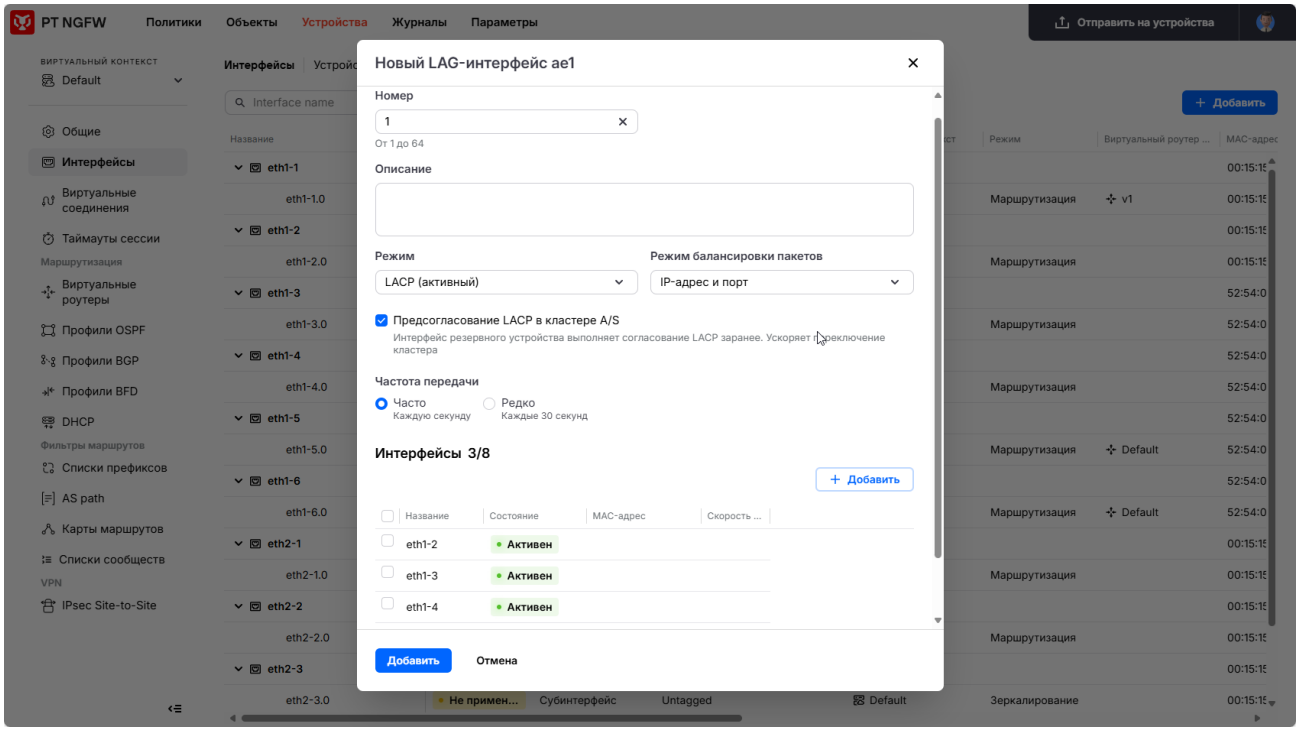


Рисунок 146. Создание LAG-интерфейса

Сразу после добавления LAG-интерфейс находится в состоянии **Не применен**. В процессе передачи и применения конфигурации на устройстве LAG-интерфейс находится в состоянии **Подключение**. Если состояние любого подчиненного физического интерфейса отличается от **Активен**, LAG-интерфейс имеет состояние **Активен частично**.

25.2. Агрегирование каналов в кластере

При работе PT NGFW в кластере рекомендованным способом является динамическое агрегирование с использованием предварительного согласования LACP. В этом случае резервный узел заранее устанавливает соединение с сетевым оборудованием чтобы избежать потерь трафика при переключении кластера.

Возможны следующие схемы подключения кластера PT NGFW к активному оборудованию:

1. Оба узла кластера подключены к одному коммутатору, поддерживающему множественную агрегацию (на котором можно настроить более одной группы агрегации). На коммутаторе настраиваются два отдельных LAG, при этом активный узел подключается к физическим портам одного LAG, а резервный узел — к портам второго.

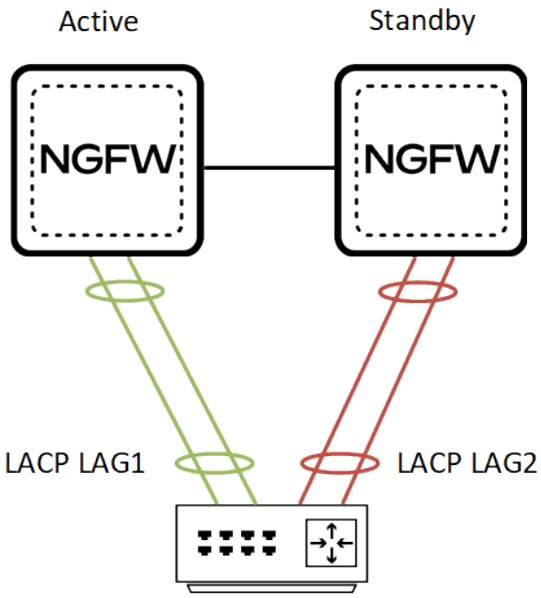


Рисунок 147. Подключение обоих узлов кластера к одному коммутатору

Внимание! Некоторые модели коммутаторов не поддерживают множественную агрегацию, либо их настройки вызывают отключение портов резервного узла. В таком случае данная схема подключения не поддерживается.

2. Подключение узлов кластера к разным коммутаторам. Такая схема не требует поддержки множественной агрегации, однако для ее реализации требуются дополнительный коммутатор.

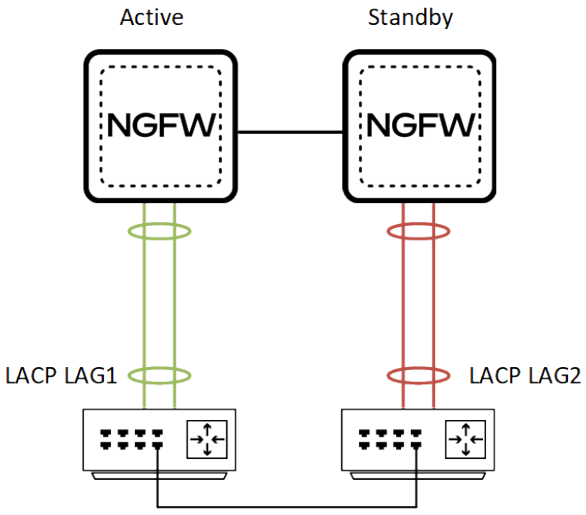


Рисунок 148. Подключение узлов кластера к разным коммутаторам

Внимание! В данной схеме резервируются только физические каналы связи, входящие в LAG, и узлы PT NGFW. Если один из коммутаторов выйдет из строя, агрегированный канал между ним и соответствующим узлом кластера перестанет функционировать.

3. Подключение к разным коммутаторам с использованием MC-LAG. Если активное оборудование поддерживает MC-LAG (Multi-chassis link aggregation group), то вы можете параллельно с агрегированием каналов использовать резервирование коммутаторов для обеспечения отказоустойчивости сети. В этом случае при отказе одного из коммутаторов работа агрегированного канала будет обеспечиваться исправным вне зависимости от того, какой из узлов кластера является активным.

   В группе MC-LAG настраиваются два отдельных LAG, при этом активный узел подключается к физическим портам одного LAG, а резервный узел — к портам второго. Для резервирования коммутаторов в каждый LAG должны входить порты разных шасси из группы MC-LAG.

   Внимание! Запрещено объединять в одном LAG физические каналы активного и резервного узлов кластера.

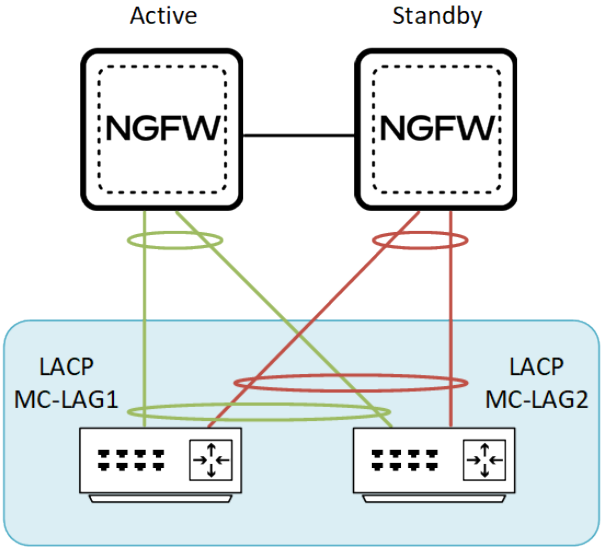


Рисунок 149. Подключение к разным коммутаторам с использованием MC-LAG

25.3. Примеры настройки LACP со сторонним оборудованием

Настройка LACP LAG между PT NGFW и Cisco Catalyst

Рассмотрим пример настройки агрегированного канала LACP LAG между коммутатором Cisco Catalyst и PT NGFW.

Примечание. Настройки приведены для коммутатора Cisco Catalyst 8000-series под управлением Cisco IOS XE v.17.16.01a и PT NGFW, работающем в кластере, с включенной функцией предсогласования LACP (LACP-Prenegotiation). Детальное описание конфигурации и команды диагностики LACP LAG см. в документации к используемой модели коммутатора.

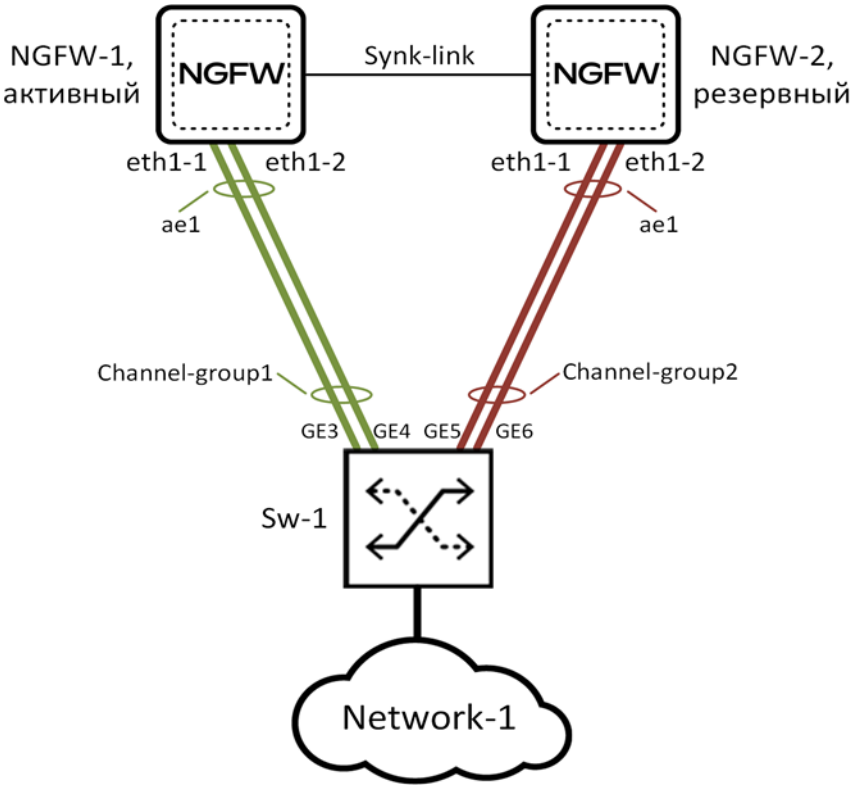


Рисунок 150. Схема подключения узлов кластера к коммутатору

На рисунке выше приведена схема подключения кластера PT NGFW, состоящего из узлов NGFW-1 и NGFW-2 к коммутатору Cisco Catalyst (Sw-1). Для организации агрегированного канала на каждом из узлов кластера создается агрегированный интерфейс `ae1`, включающий физические интерфейсы `eth1-1` и `eth1-2`. Для ускорения переключения кластера используется функция предсогласования LACP (LACP-Prenegotiation).

На коммутаторе Cisco Catalyst настроены два агрегированных интерфейса:

— **Port-channel1** — включает физические интерфейсы GigabitEthernet3 (`GE3`) и GigabitEthernet4 (`GE4`), используется для подключения к агрегированному каналу Channel-group1;

— **Port-channel2** — включает физические интерфейсы GigabitEthernet5 (`GE5`) и GigabitEthernet6 (`GE6`), используется для подключения к агрегированному каналу Channel-group2.

Физические порты узла NGFW-1 подключаются к физическим портам **Port-channel1**, а порты узла NGFW-2 — к портам **Port-channel2**.

Для реализации данной схемы:

1. Настройте (см. раздел 30) кластер PT NGFW.
2. Подключите узлы кластера к коммутатору согласно схеме подключения.
3. Создайте агрегированный интерфейс и настройте его как на рисунке ниже.

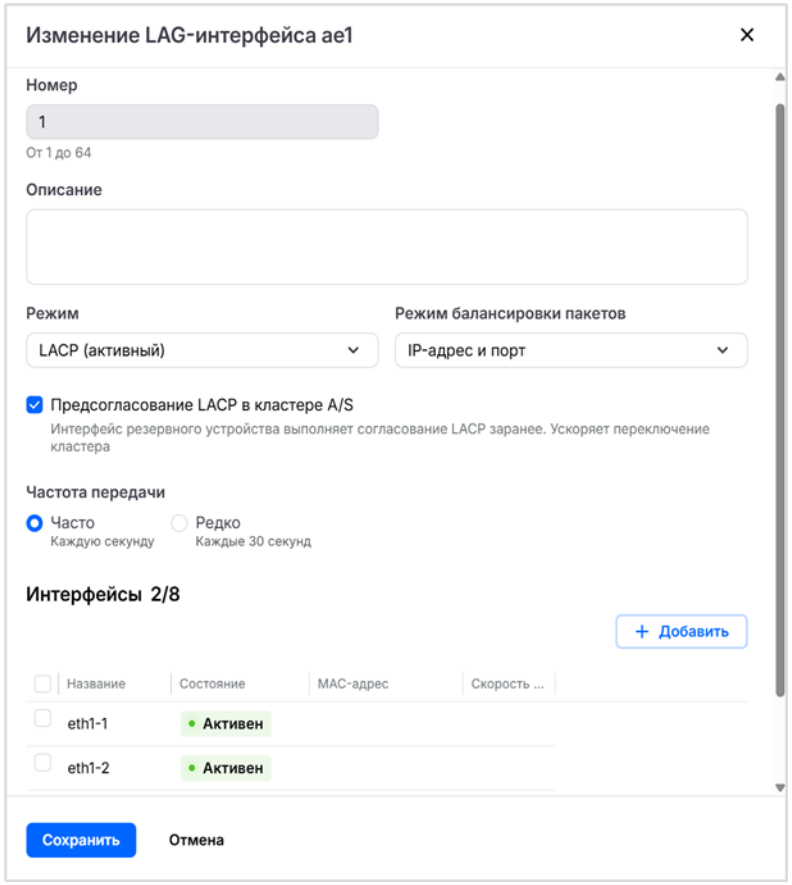


Рисунок 151. Рисунок. Настройка агрегированного интерфейса

4. Настройте подключение к агрегированному каналу на коммутаторе Sw-1 согласно схеме подключения. Ниже приведена конфигурация Cisco Catalyst для рассматриваемого примера:

```
interface Port-channel1
description --LAG-to-NGFW-Node-1--
no ip address
negotiation auto
lacp fast-switchover
service instance 1 ethernet
encapsulation untagged
bridge-domain 1
!
!
interface Port-channel2
```

```
description --LAG-to-NGFW-Node-2--
no ip address
negotiation auto
lacp fast-switchover
service instance 1 ethernet
encapsulation untagged
bridge-domain 1
!
!
interface GigabitEthernet2
description --to-Network-1--
no ip address
negotiation auto
service instance 1 ethernet
encapsulation untagged
bridge-domain 1
!
!
interface GigabitEthernet3
description --to-eth1-1-NGFW-Node-1--
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode active
!
interface GigabitEthernet4
description --to-eth1-2-NGFW-Node-1--
no ip address
negotiation auto
lacp rate fast
channel-group 1 mode active
!
interface GigabitEthernet5
description --to-eth1-1-NGFW-Node-2--
no ip address
negotiation auto
lacp rate fast
channel-group 2 mode active
!
interface GigabitEthernet6
description --to-eth1-2-NGFW-Node-2--
no ip address
negotiation auto
lacp rate fast
channel-group 2 mode active
```

5. Проверьте работоспособность агрегированных каналов. Вывод диагностических команд для рассматриваемого примера на коммутаторе Sw-1 приведен в таблице ниже.

Таблица 13. Примеры вывода диагностических команд

Команда	Пример вывода

`show etherchannel summary`	`Flags: D - down P/bndl - bundled in port-channel`
	`I - stand-alone s/susp - suspended`
	`H - Hot-standby (LACP only)`
	`R - Layer3 S - Layer2`
	`U - in use f - failed to allocate aggregator`
	
	`M - not in use, minimum links not met`
	`u - unsuitable for bundling`
	`w - waiting to be aggregated`
	`d - default port`
	
	`Number of channel-groups in use: 2`
	`Number of aggregators: 2`
	
	`Group Port-channel Protocol Ports`
	`------+-------------+-----------`
	`+-----------------------------------------------`
	`-`
	`1 Po1(SU) LACP Gi3(bndl) Gi4(bndl)`
	`2 Po2(SU) LACP Gi5(bndl) Gi6(bndl)`
	
	`RU - L3 port-channel UP State`
	`SU - L2 port-channel UP state`
	`P/bndl - Bundled`
	`S/susp - Suspended`

`show lacp internal`	`Flags: S - Device is requesting Slow LACPDUs`
	`F - Device is requesting Fast LACPDUs`
	`A - Device is in Active mode P - Device is in Passive mode`

	Channel group 1 LACP port Admin Oper Port Port Port Flags State Priority Key Key Number State Gi3 FA bndl 32768 0x1 0x1 0x4 0x3F Gi4 FA bndl 32768 0x1 0x1 0x5 0x3F Channel group 2 LACP port Admin Oper Port Port Port Flags State Priority Key Key Number State Gi5 FA bndl 32768 0x2 0x2 0x6 0x3F Gi6 FA bndl 32768 0x2 0x2 0x7 0x3F
show lacp neighbor	Flags: S - Device is requesting Slow LACPDUs F - Device is requesting Fast LACPDUs A - Device is in Active mode P - Device is in Passive mode Channel group 1 neighbors LACP port Admin Oper Port Port Port Flags Priority Dev ID Age key Key Number State Gi3 FA 32768 0050.5694.7bc8 0s 0x0 0x7AF4 0x1 0x3F Gi4 FA 32768 0050.5694.7bc8 0s 0x0 0x7AF4 0x2 0x3F Channel group 2 neighbors LACP port Admin Oper Port Port Port Flags Priority Dev ID Age key Key Number State

	Gi5 FA 32768 0050.5694.7bc9 0s 0x0 0x7AF4 0x1 0x3F Gi6 FA 32768 0050.5694.7bc9 0s 0x0 0x7AF4 0x2 0x3F
show interfaces port-channel 1	Port-channel1 is up, line protocol is up Hardware is GEChannel, address is 001e.f629.06c0 (bia 001e.f629.06c0) Description: --LAG-to-NGFW-Node-1-- MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec) ARP type: ARPA, ARP Timeout 04:00:00 No. of active members in this channel: 2 Member 0 : GigabitEthernet3 , Full-duplex, 1000Mb/s Member 1 : GigabitEthernet4 , Full-duplex, 1000Mb/s No. of PF_JUMBO supported members in this channel : 2 . . .
show interfaces port-channel 2	Port-channel2 is up, line protocol is up Hardware is GEChannel, address is 001e.f629.06c1 (bia 001e.f629.06c1) Description: --LAG-to-NGFW-Node-2-- MTU 1500 bytes, BW 2000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec) ARP type: ARPA, ARP Timeout 04:00:00 No. of active members in this channel: 2

	Member 0 : GigabitEthernet5 , Full-duplex, 1000Mb/s Member 1 : GigabitEthernet6 , Full-duplex, 1000Mb/s No. of PF_JUMBO supported members in this channel : 2 . . .

Настройка MC-LAG между PT NGFW и Juniper MX

Рассмотрим пример настройки MC-LAG (Multichassis Link Aggregation Group) между PT NGFW и коммутаторами Juniper MX. Подробнее о технологии MC-LAG см. в разделе Агрегирование каналов в кластере (см. раздел 25).

> **Примечание.** Настройки приведены для коммутаторов Juniper MX, работающих под управлением Junos 18.1R1.9, и PT NGFW, работающем в кластере, с включенной функцией предсогласования LACP (LACP-Prenegotiation). Детальное описание конфигурации и команды диагностики LACP LAG см. в документации к используемой модели коммутаторов.

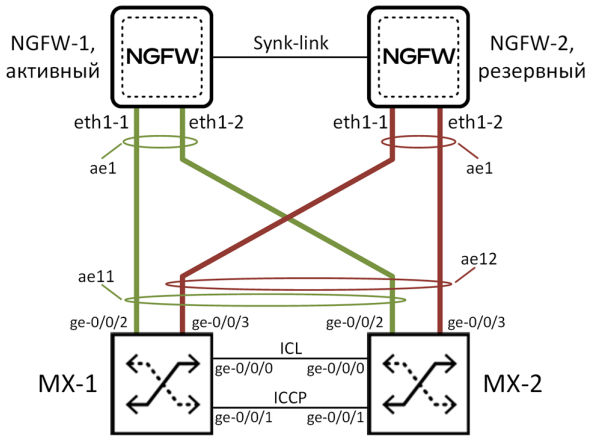


Рисунок 152. Схема подключения MC-LAG

На рисунке выше приведена схема подключения кластера PT NGFW, состоящего из узлов NGFW-1 и NGFW-2, к MC-LAG на базе коммутаторов Juniper MX (узлы MX-1 и MX-2).

Для организации агрегированного канала на каждом из узлов кластера создается агрегированный интерфейс `ae1`, включающий физические интерфейсы `eth1-1` и `eth1-2`. Для ускорения переключения кластера используется функция предсогласования LACP (LACP-Prenegotiation).

На оборудовании Juniper MX настроены два агрегированных интерфейса, в каждый из которых входят физические порты обоих коммутаторов:

— `ae11` — включает физические интерфейсы `ge-0/0/2` узлов MX-1 и MX-2;

— `ae12` — включает физические интерфейсы `ge-0/0/3` узлов MX-1 и MX-2.

Также для взаимодействия коммутаторов в MC-LAG используются дополнительные физические интерфейсы:

— `ge-0/0/0` — для организации InterChassisLink (ICL);

— `ge-0/0/1` — для организации канала Inter-Chassis Control Protocol (ICCP).

Примечание. Механизмы ICL и ICCP используются для организации MC-LAG в оборудовании Juniper Networks. В коммутаторах других производителей настройка MC-LAG может отличаться.

Физические порты, входящие в агрегированный интерфейс (`ae1`) узла NGFW-1, подключаются к физическим портам `ae11`, а узла NGFW-2 — к физическим портам `ae12`.

Для реализации данной схемы:

1. Настройте кластер (см. раздел 30) PT NGFW.
2. Подключите узлы кластера к коммутаторам согласно схеме подключения.
3. Подключите дополнительные интерфейсы, используемых для взаимодействия коммутаторов, согласно схеме подключения.
4. Создайте агрегированный интерфейс и настройте его как на рисунке ниже.

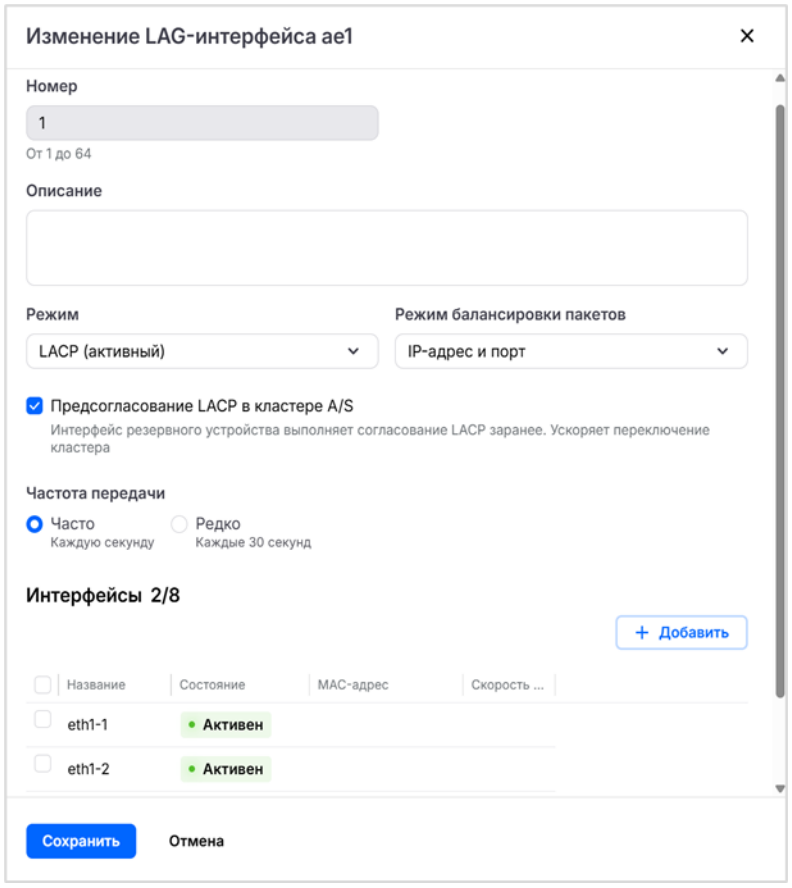


Рисунок 153. Настройка агрегированного интерфейса

5. Настройте агрегированные интерфейсы на коммутаторах Juniper MX согласно схеме подключения. Ниже приведены конфигурации коммутаторов MX-1 и MX-2 для рассматриваемого примера.

MX-1

```
chassis {
aggregated-devices {
ethernet {
device-count 2;
}
}
}
interfaces {
ge-0/0/0 {
description --ICL--;
```

MX-2

```
chassis {
aggregated-devices {
ethernet {
device-count 2;
}
}
}
interfaces {
ge-0/0/0 {
description --ICL--;
```

```
encapsulation ethernet-bridge;
unit 0 {
family bridge {
interface-mode access;
vlan-id 10;
}
}
}
ge-0/0/1 {
description --ICCP--;
unit 0 {
family inet {
address 192.168.55.1/30;
}
}
}
ge-0/0/2 {
description --to-NGFW-1--;
gigether-options {
802.3ad ae11;
}
}
ge-0/0/3 {
description --to-NGFW-2--;
gigether-options {
802.3ad ae12;
}
}
ae11 {
description -AE-to-NGFW-1-;
encapsulation ethernet-bridge;
```

```
encapsulation ethernet-bridge;
unit 0 {
family bridge {
interface-mode access;
vlan-id 10;
}
}
}
ge-0/0/1 {
description --ICCP--;
unit 0 {
family inet {
address 192.168.55.2/30;
}
}
}
ge-0/0/2 {
description --to-NGFW-1--;
gigether-options {
802.3ad ae11;
}
}
ge-0/0/3 {
description --to-NGFW-2--;
gigether-options {
802.3ad ae12;
}
}
ae11 {
description –AE-to-NGFW-1-;
encapsulation ethernet-bridge;
```

```
aggregated-ether-options {
lacp {
active;
periodic fast;
system-id 00:01:02:03:04:05;
admin-key 2;
}
mc-ae {
mc-ae-id 11;
redundancy-group 10;
chassis-id 0;
mode active-active;
status-control active;
init-delay-time 1;
}
}
unit 0 {
family bridge {
interface-mode access;
vlan-id 10;
}
}
}
ae12 {
description -AE-to-NGFW-2-;
encapsulation ethernet-bridge;
aggregated-ether-options {
lacp {
active;
periodic fast;
system-id 00:01:02:03:04:05;
```

```
aggregated-ether-options {
lacp {
active;
periodic fast;
system-id 00:01:02:03:04:05;
admin-key 2;
}
mc-ae {
mc-ae-id 11;
redundancy-group 10;
chassis-id 1;
mode active-active;
status-control standby;
init-delay-time 1;
}
}
unit 0 {
family bridge {
interface-mode access;
vlan-id 10;
}
}
}
ae12 {
description -AE-to-NGFW-2--;
encapsulation ethernet-bridge;
aggregated-ether-options {
lacp {
active;
periodic fast;
system-id 00:01:02:03:04:05;
```

```
admin-key 3;
}
mc-ae {
mc-ae-id 12;
redundancy-group 10;
chassis-id 0;
mode active-active;
status-control active;
init-delay-time 1;
}
}
unit 0 {
family bridge {
interface-mode access;
vlan-id 10;
}
}
}
irb {
unit 10 {
family inet {
address 172.30.130.15/24;
}
}
}
}
multi-chassis {
multi-chassis-protection 192.168.55.2
{
interface ge-0/0/0;
}
```

```
admin-key 3;
}
mc-ae {
mc-ae-id 12;
redundancy-group 10;
chassis-id 1;
mode active-active;
status-control standby;
init-delay-time 1;
}
}
unit 0 {
family bridge {
interface-mode access;
vlan-id 10;
}
}
}
irb {
unit 10 {
family inet {
address 172.30.130.15/24;
}
}
}
}
multi-chassis {
multi-chassis-protection 192.168.55.1
{
interface ge-0/0/0;
}
```

```
}
protocols {
iccp {
local-ip-addr 192.168.55.1;
peer 192.168.55.2 {
redundancy-group-id-list 10;
liveness-detection {
minimum-interval 500;
}
}
}
}
bridge-domains {
br0 {
domain-type bridge;
vlan-id 10;
service-id 2;
mcae-mac-synchronize;
routing-interface irb.10;
}
}
switch-options {
service-id 1;
}
```

```
}
protocols {
iccp {
local-ip-addr 192.168.55.2;
peer 192.168.55.1 {
redundancy-group-id-list 10;
liveness-detection {
minimum-interval 500;
}
}
}
}
bridge-domains {
br0 {
domain-type bridge;
vlan-id 10;
service-id 2;
mcae-mac-synchronize;
routing-interface irb.10;
}
}
switch-options {
service-id 1;
}
```

В результате трафик между узлами кластера PT NGFW и коммутаторами будет идти по агрегированным каналам, в которые входят физические интерфейсы обоих коммутаторов. Такая схема обеспечивает работоспособность при выходе из строя любого узла кластера, физического канала или коммутатора.

Проверить работоспособность (см. раздел 25.3.1) созданных агрегированных каналов вы можете в разделе **Устройства** → **Кластеры**. При необходимости диагностики используйте диагностические команды (см. раздел 25.3.2) на узлах MX-1 и MX-2.

В этом разделе

Диагностика LAG LACP на PT NGFW (см. раздел 25.3.1)

Диагностика LAG LACP на Juniper MX (см. раздел 25.3.2)

25.3.1. Диагностика LAG LACP на PT NGFW

Чтобы проверить работоспособность агрегированного канала и входящих в него интерфейсов:

1. Подключитесь к веб-интерфейсу системы управления.
2. Выберите **Устройства** → **Кластеры** и выберите требуемый кластер.
3. Выберите **Интерфейсы**.
4. Убедитесь, что агрегированный интерфейс **ae1** и физические интерфейсы **eth1-1** и **eth1-2** находятся в состоянии **Активен**.

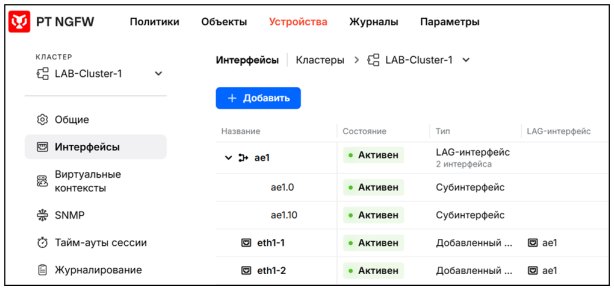


Рисунок 154. Рисунок. Состояние интерфейсов активного узла кластера PT NGFW

5. Выберите **Устройства** → **Кластеры** и выберите требуемый кластер.
6. Выберите **Общие** и выберите активный узел кластера.
7. Убедитесь, что агрегированный интерфейс **ae1** и физические интерфейсы **eth1-1** и **eth1-2** находятся в состоянии **Активен**.

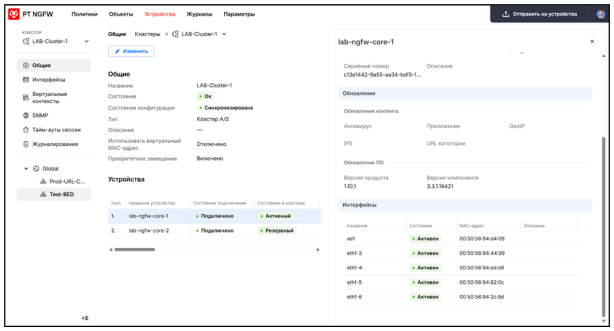


Рисунок 155. Рисунок. Состояние интерфейсов активного узла кластера PT NGFW

8. Выберите резервный узел кластера.

9. Убедитесь, что агрегированный интерфейс **ae1** и физические интерфейсы **eth1-1** и **eth1-2** находятся в состоянии **Активен**.

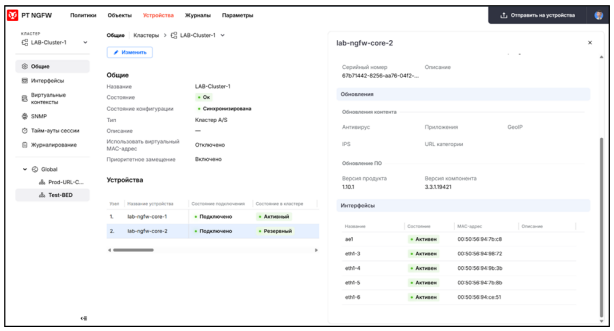


Рисунок 156. Рисунок. Состояние интерфейсов резервного узла кластера PT NGFW

См. также

Кластер межсетевого экрана (см. раздел 30)

Агрегирование каналов (LAG, LACP) (см. раздел 25)

25.3.2. Диагностика LAG LACP на Juniper MX

В таблице ниже приведены диагностические команды Juniper MX и примеры их вывода для описанной схемы MC LAG:

Таблица 14. Примеры вывода диагностических команд

MX-1	MX-2
show lacp interfaces extensive	
Aggregated interface: ae11 LACP state: Role Exp Def Dist Col Syn Aggr Timeout Activity ge-0/0/2 Actor No No Yes Yes Yes Yes Fast Active ge-0/0/2 Partner No No Yes Yes Yes Yes Fast Active LACP protocol: Receive State Transmit State Mux State ge-0/0/2 Current Fast periodic Collecting distributing LACP info: Role System System Port Port Port priority identifier priority number key ge-0/0/2 Actor 127 00:01:02:03:04:05 127 1 2 ge-0/0/2 Partner 32768 00:50:56:94:7b:c8 32768 1 31476 Aggregated interface: ae12	Aggregated interface: ae11 LACP state: Role Exp Def Dist Col Syn Aggr Timeout Activity ge-0/0/2 Actor No No Yes Yes Yes Yes Fast Active ge-0/0/2 Partner No No Yes Yes Yes Yes Fast Active LACP protocol: Receive State Transmit State Mux State ge-0/0/2 Current Fast periodic Collecting distributing LACP info: Role System System Port Port Port priority identifier priority number key ge-0/0/2 Actor 127 00:01:02:03:04:05 127 32769 2 ge-0/0/2 Partner 32768 00:50:56:94:7b:c8 32768 2 31476 Aggregated interface: ae12 LACP state: Role Exp Def Dist Col Syn Aggr Timeout Activity

LACP state: Role Exp Def Dist Col Syn Aggr Timeout Activity ge-0/0/3 Actor No No Yes Yes Yes Yes Fast Active ge-0/0/3 Partner No No Yes Yes Yes Yes Fast Active LACP protocol: Receive State Transmit State Mux State ge-0/0/3 Current Fast periodic Collecting distributing LACP info: Role System System Port Port Port priority identifier priority number key ge-0/0/3 Actor 127 00:01:02:03:04:05 127 2 3 ge-0/0/3 Partner 32768 00:50:56:94:7b:c9 32768 1 31476	ge-0/0/3 Actor No No Yes Yes Yes Yes Fast Active ge-0/0/3 Partner No No Yes Yes Yes Yes Fast Active LACP protocol: Receive State Transmit State Mux State ge-0/0/3 Current Fast periodic Collecting distributing LACP info: Role System System Port Port Port priority identifier priority number key ge-0/0/3 Actor 127 00:01:02:03:04:05 127 32770 3 ge-0/0/3 Partner 32768 00:50:56:94:7b:c9 32768 2 31476
show interfaces terse | match ae	
ge-0/0/2.0 up up aenet --> ae11.0 ge-0/0/3.0 up up aenet --> ae12.0 ae11 up up ae11.0 up up bridge ae12 up up ae12.0 up up bridge	ge-0/0/2.0 up up aenet --> ae11.0 ge-0/0/3.0 up up aenet --> ae12.0 ae11 up up ae11.0 up up bridge ae12 up up ae12.0 up up bridge
show iccp	

Redundancy Group Information for peer 192.168.55.2 TCP Connection : Established Liveliness Detection : Up Redundancy Group ID Status 10 Up Client Application: lacpd Redundancy Group IDs Joined: 10 Client Application: l2ald_iccpd_client Redundancy Group IDs Joined: 10	Redundancy Group Information for peer 192.168.55.1 TCP Connection : Established Liveliness Detection : Up Redundancy Group ID Status 10 Up Client Application: l2ald_iccpd_client Redundancy Group IDs Joined: 10 Client Application: lacpd Redundancy Group IDs Joined: 10
show interfaces mc-ae	
Member Link : ae11 Current State Machine's State: mcae active state Local Status : active Local State : up Peer Status : active Peer State : up Logical Interface : ae11.0	Member Link : ae11 Current State Machine's State: mcae active state Local Status : active Local State : up Peer Status : active Peer State : up Logical Interface : ae11.0

Topology Type : bridge	Topology Type : bridge
Local State : up	Local State : up
Peer State : up	Peer State : up
Peer Ip/MCP/State : 192.168.55.2 ge-0/0/0.0 up	Peer Ip/MCP/State : 192.168.55.1 ge-0/0/0.0 up
Member Link : ae12	Member Link : ae12
Current State Machine's State: mcae active state	Current State Machine's State: mcae active state
Local Status : active	Local Status : active
Local State : up	Local State : up
Peer Status : active	Peer Status : active
Peer State : up	Peer State : up
Logical Interface : ae12.0	Logical Interface : ae12.0
Topology Type : bridge	Topology Type : bridge
Local State : up	Local State : up
Peer State : up	Peer State : up
Peer Ip/MCP/State : 192.168.55.2 ge-0/0/0.0 up	Peer Ip/MCP/State : 192.168.55.1 ge-0/0/0.0 up

26. Тайм-ауты сетевых сессий

Тайм-аут сетевой сессии — максимальное время ожидания на разных этапах двустороннего обмена данными (сетевой сессии), по истечении которого сессия считается истекшей и завершается. В некоторых случаях, например для обеспечения работы специфических сетевых приложений и сервисов, требуется настройка индивидуальных тайм-аутов. В таблице ниже приведены тайм-ауты, которые можно изменить для PT NGFW, и их значения по умолчанию.

Таблица 15. Настраиваемые тайм-ауты сетевых сессий

Наименование тайм-аута	**Диапазон значений, сек.**	**Описание**
TCP-инициализация (TCP Init)	1—60 По умолчанию: 5	Максимальное время между TCP SYN и SYN-ACK при выполнении TCP-рукопожатия
TCP-рукопожатие (TCP Handshake)	1—60 По умолчанию: 10	Максимальное время между получением TCP SYN-ACK и завершающего ACK при выполнении TCP-рукопожатия
TCP-сессия установлена (TCP Established)	1—15 999 999 По умолчанию: 3600	Максимальное время, которое TCP- сессия остается в таблице сессий в установленном состоянии (established) без активности
TCP-сессия частично закрыта (TCP Half closed)	1—604 800 По умолчанию: 60	Максимальное время между получением первого и второго пакета FIN или пакета RST
Ожидание закрытия TCP-сессии (TCP Time wait)	1—600 По умолчанию: 2	Максимальное время, которое TCP-сессия считается активной после получения второго из двух пакетов FIN или после получения пакета RST
UDP	1—1 599 999 По умолчанию: 30	Максимальное время, которое UDP-сессия остается в таблице сессий без активности

В PT NGFW тайм-ауты сетевых сессий можно задать на нескольких уровнях: устройства, виртуального контекста и сервиса. При этом, если на нижестоящих уровнях не заданы собственные тайм-ауты, то значения наследуются с вышестоящего уровня в порядке, указанном на рисунке.



Рисунок 157. Порядок наследования тайм-аутов

Тайм-ауты, заданные на нижестоящем уровне, переопределяют наследуемые значения. Например, вы можете задать общий тайм-аут для всех UDP-сессий на уровне устройства и собственное значение тайм-аута для выбранного сервиса. При этом заданное значение будет использоваться только в политиках безопасности, содержащих в условиях срабатывания выбранный сервис, не влияя на прочие UDP-сессии.

В этом разделе

Настройка тайм-аутов для устройства (см. раздел 26.1)

Настройка тайм-аутов для виртуального контекста (см. раздел 26.2)

Настройка тайм-аутов для сервиса (см. раздел 26.3)

Особенности настройки тайм-аутов для сервисов (см. раздел 26.4)

26.1. Настройка тайм-аутов для устройства

- Чтобы настроить тайм-ауты сессий для устройства:

1. Нажмите **Устройства** → **Устройства**, затем выберите название устройства.

   Примечание. Если устройство работает в кластере A/S, нажмите **Устройства** → **Кластеры**, затем выберите название кластера.

2. Выберите **Тайм-ауты сессии**.

   Будут выведены текущие значения тайм-аутов и их тип: по умолчанию или собственное.

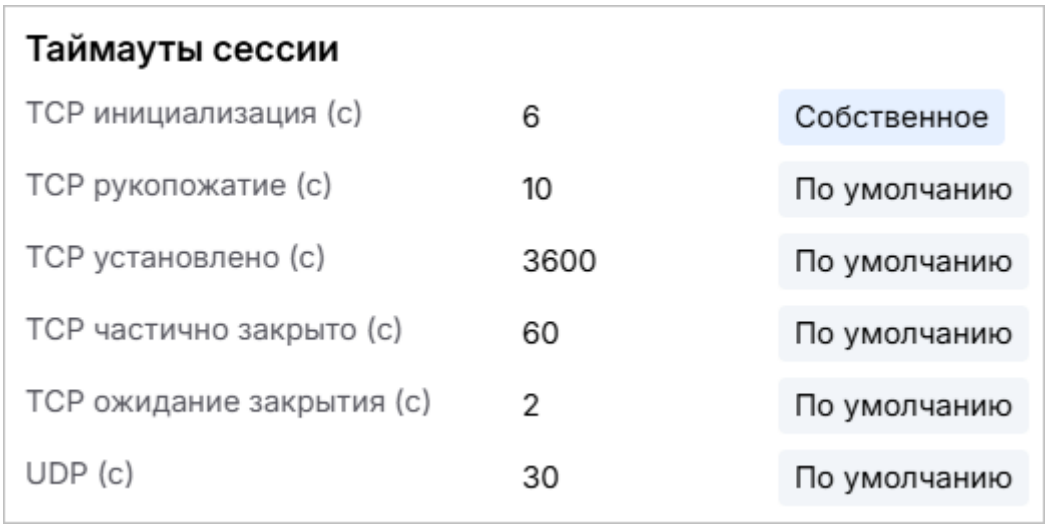


Рисунок 158. Просмотр таймаутов сетевых сессий

3. Нажмите **Редактирование**.

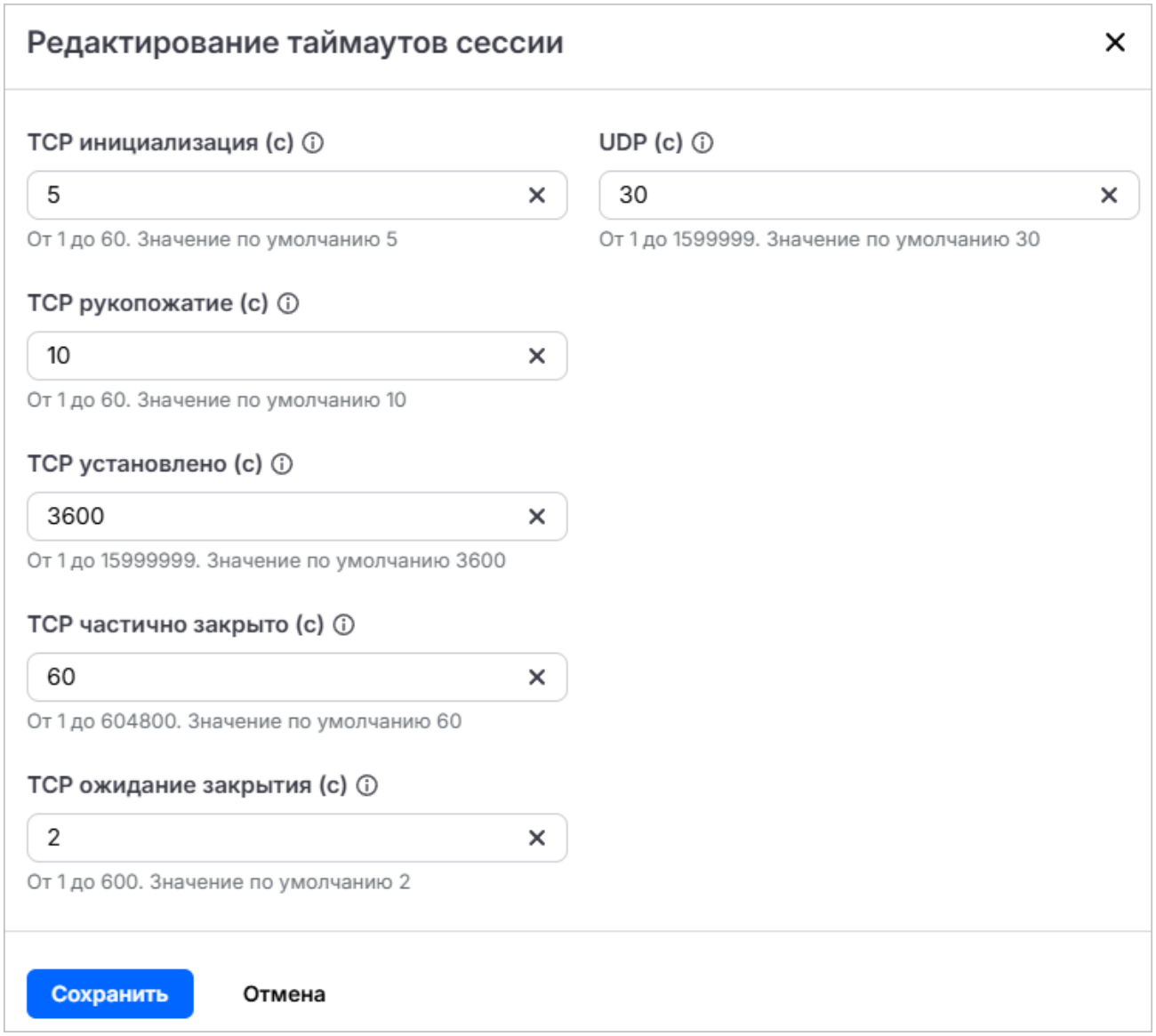


Рисунок 159. Настройка таймаутов сетевой сессии

4. Задайте значения тайм-аутов и нажмите **Сохранить**.

26.2. Настройка тайм-аутов для виртуального контекста

1. Выберите **Устройства** → **Виртуальные контексты**, затем нажмите на название контекста.
2. Выберите **Таймауты сессии**.
3. Нажмите **Редактирование**.

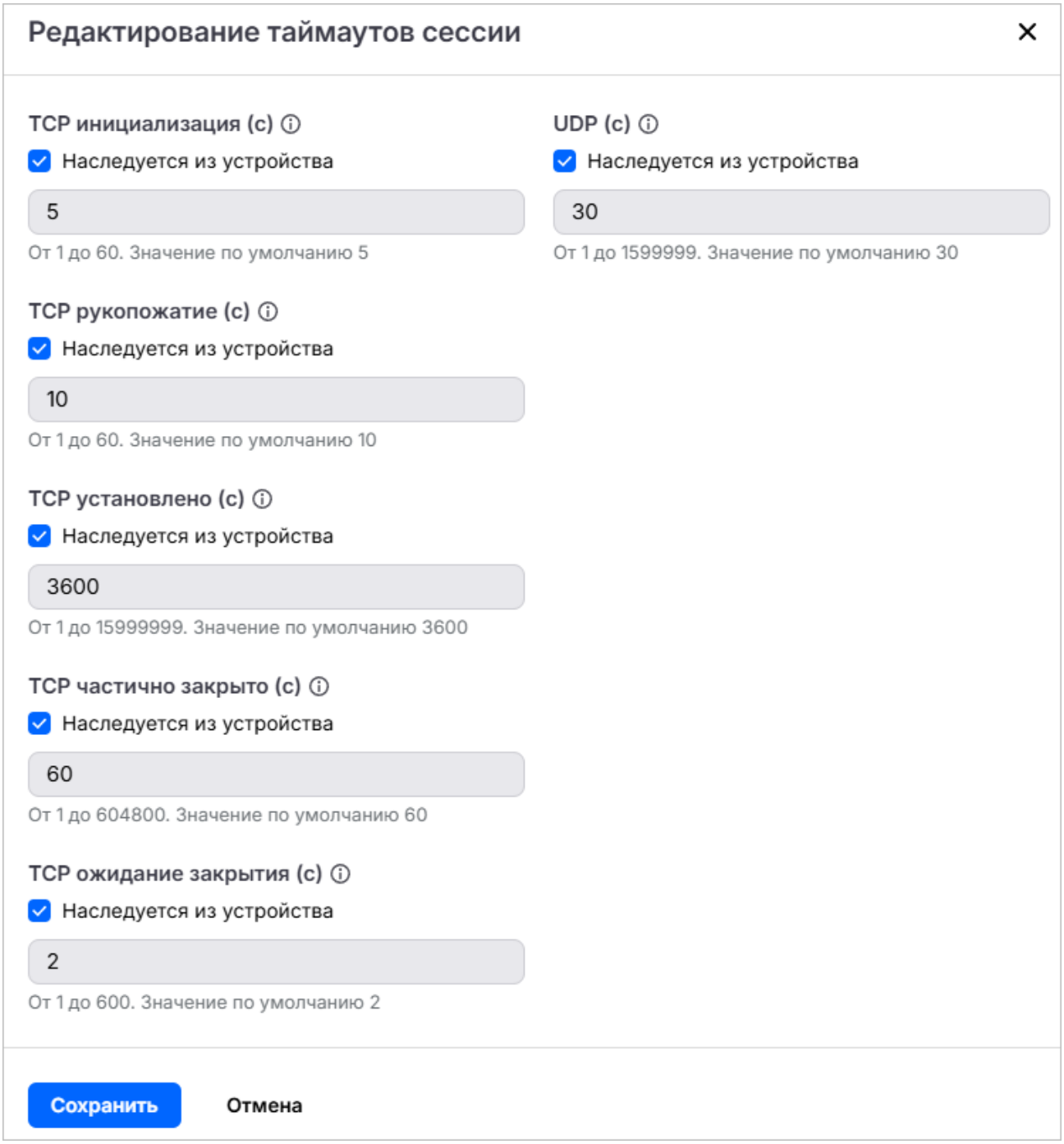


Рисунок 160. Настройка таймаутов сетевых сессий

4. По умолчанию значения таймаутов наследуются из устройства. Чтобы задать собственное значение, снимите флажок **Наследуется из устройства** и введите значение в поле.
5. Нажмите **Сохранить**.

26.3. Настройка тайм-аутов для сервиса

1. Выберите **Объекты → Сервисы → Пользовательские**, затем нажмите на название сервиса.
2. В окне **Изменение сервиса** выберите вкладку **Таймауты сессии**.

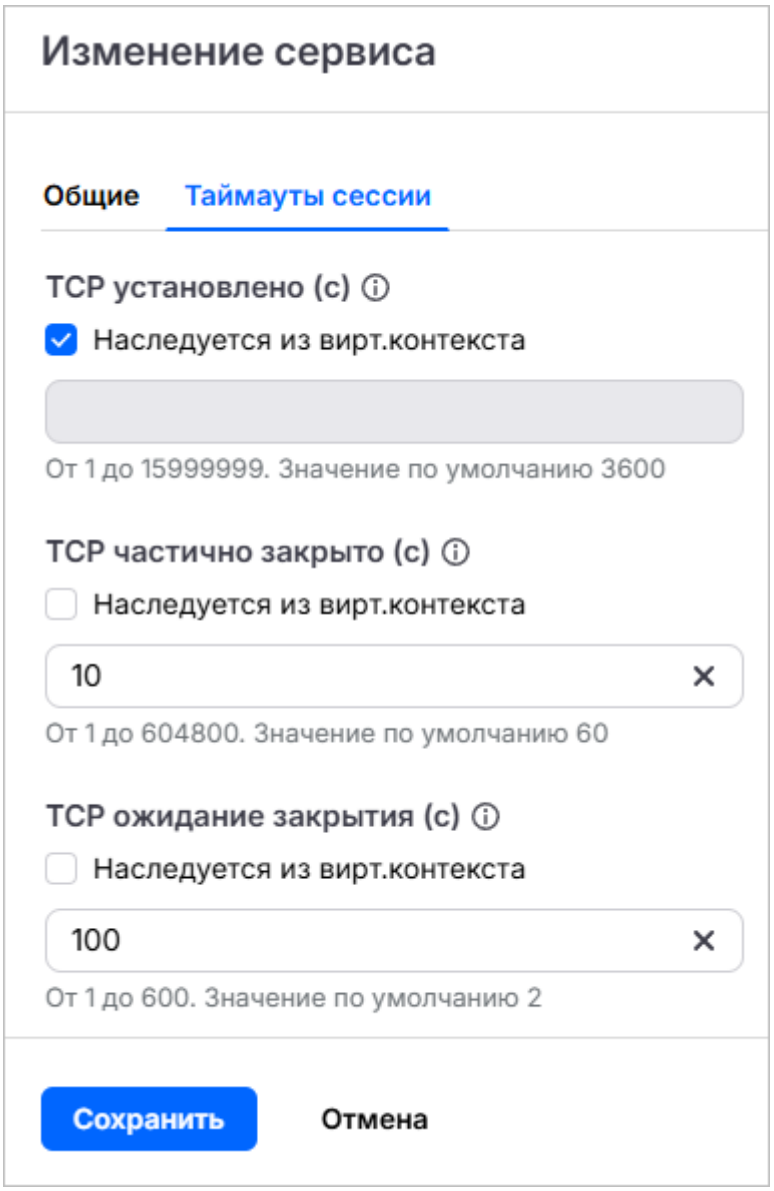


Рисунок 161. Настройка таймаутов сетевой сессии

3. По умолчанию значения таймаутов наследуются из виртуального контекста. Чтобы задать собственное значение, снимите флажок **Наследуется из вирт. контекста** и введите значение в поле.
4. Нажмите **Сохранить**.

26.4. Особенности настройки тайм-аутов для сервисов

— При обработке трафика пользовательский сервис идентифицируется по транспортному протоколу и номеру порта. Если под действие одного правила безопасности подпадает трафик нескольких сервисов, то тайм-ауты каждого сервиса будут применяться к соответствующему ему трафику.

— Не используйте в одном правиле безопасности несколько сервисов с разными значениями тайм-аутов и совпадающими портами (или пересекающимися диапазонами портов). В этом случае сетевая сессия может одновременно соответствовать нескольким сервисам и выбор тайм-аутов будет неопределен.

  Если вы хотите использовать разные сервисы с разными тайм-аутами и пересекающимися диапазонами портов, то создайте отдельные правила безопасности для каждого такого сервиса.

27. Зеркалирование расшифрованного трафика

При зеркалировании расшифрованного трафика PT NGFW отправляет копию расшифрованного TLS-трафика во внешнюю систему сбора или анализа трафика, например систему DLP. Для настройки функции необходимо добавить и указать в правиле расшифрования трафика, который необходимо зеркалировать, профиль зеркалирования. В профиле указываются сабинтерфейсы, через которые нужно передавать копию трафика, и MAC-адрес назначения, который будет установлен в зеркалируемом трафике. Указать можно только те сабинтерфейсы, которым назначен режим работы **Зеркалирование**. MAC-адрес и метка VLAN (при наличии) исходящего сабинтерфейса будут использованы в зеркалируемом трафике как MAC-адрес источника и значение поля VLAN ID.

Примечание. Зеркалирование трафика происходит сразу после его расшифрования.

- Чтобы добавить профиль зеркалирования:

  1. В главном меню выберите **Объекты**.
  2. Выберите вкладку **Профили зеркалирования (расшифрование)**.
  3. Нажмите **Добавить**.
  4. Введите название профиля.
  5. Если требуется, введите описание.
  6. Если требуется, укажите MAC-адрес назначения, отличный от широковещательного.

     Примечание. Этот MAC-адрес назначения будет указан в зеркалируемом трафике.
  7. Нажмите **Добавить** и выберите сабинтерфейсы, в которые должен передаваться расшифрованный трафик.

     Примечание. Вы можете выбрать не более одного сабинтерфейса для одного виртуального контекста.
  8. Нажмите **Добавить**.

Вы можете изменить или удалить профиль зеркалирования в контекстном меню профиля.

Примечание. Изменения в профиле зеркалирования затрагивают только новые сессии.

28. Подключение к Active Directory

В этом разделе описаны шаги по подключению к Active Directory (AD) и настройке подключения к Windows Event Collector (WEC).

В этом разделе

Схема работы (см. раздел 28.1)

Известные ограничения (см. раздел 28.2)

Настройка сервера Microsoft Active Directory (см. раздел 28.3)

Настройка агента Identity Control (IDC) (см. раздел 28.4)

Полезные команды, журналы, статистика (см. раздел 28.5)

Настройка подключения к WEC (см. раздел 28.6)

Пример настройки нескольких подключений LDAP и WinRM (см. раздел 28.7)

28.1. Схема работы

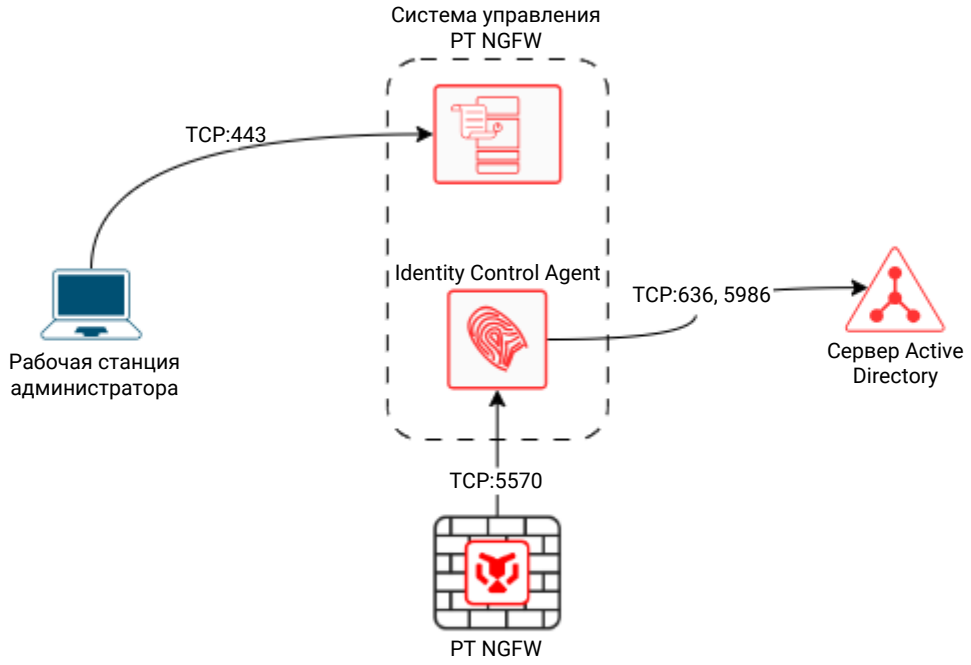


Рисунок 162. Схема работы

Принцип работы агента Identity Control (IDC):

— На PT NGFW поступают пакеты с данными, и среди этих данных и заголовков пакетов нет указания на то, какой пользователь в текущий момент работает на компьютере, и откуда эти пакеты были отправлены.

— PT NGFW ведет таблицу соответствия «IP-адрес ↔ Имя пользователя ↔ Группы, в которые входит пользователь».

— Когда PT NGFW получает первый пакет сессии, и если в правилах политики безопасности в качестве условия срабатывания указан (указаны) пользователь (пользователи) и (или) группа пользователей, то PT NGFW обращается к таблице соответствия, чтобы определить, какому пользователю принадлежит полученный пакет.

  Примечание. Так как устройств PT NGFW может быть много, то, чтобы каждый межсетевой экран не обращался к Active Directory за данными об имени пользователя, его группах и его IP-адресе, предпочтительнее иметь единый сервис, который бы собирал все эти данные, а потом раздавал их межсетевым экранам. Такие функции выполняет сервис Identity Control.

— Для наполнения таблицы соответствия межсетевой экран обращается к агенту Identity Control.

— Агент Identity Control обращается к серверу Active Directory и просматривает журналы сервера для составления таблицы соответствия.

  Примечание. В настоящее время поддерживается WinRM over HTTPS с базовой аутентификацией.

  Примечание. Для работы HTTPS сервис WinRM требует аутентификацию с использованием сертификатов. Механика взаимодействия агента Identity Control межсетевого экрана и контроллера домена MS AD выглядит следующим образом:

— Между агентом Identity Control PT NGFW и контроллером домена MS AD устанавливается соединение TLS (с HTTP внутри, отсюда HTTPS).

— Агент Identity Control PT NGFW подключается к сервису WinRM контроллера домена MS AD используя сервисную учетную запись. Процесс создания сервисной учетной записи описан в разделе про настройку сервера AD (см. раздел 28.3.2). Таким образом, сервер AD идентифицирует и аутентифицирует агента Identity Control.

— В свою очередь агент IDC также идентифицирует и аутентифицирует сервер AD. Для этого он (агент) проверяет сертификат, который присылает ему сервер AD в ходе установления сессии TLS (HTTPS).

— Таким образом, чтобы агент мог идентифицировать и аутентифицировать сервер AD необходимо сгенерировать корректный сертификат и импортировать его на сервер AD, указав сервису WinRM, что последний должен его использовать.

— Сертификат, который будет использоваться сервисом WinRM должен содержать атрибут Server Authentification, что говорит о том, что такой сертификат может использоваться для аутентификации сервера AD (сервиса WinRM),

— Агент IDC должен доверять сертификату, который ему присылает сервер AD (сервис WinRM). Для этого сертификат сервера AD (сервиса WinRM) подписывается корневым сертификатом. Именно этот корневой сертификат должен присутствовать в папке агента IDC и указывается в его конфигурации.

— Таким образом, агент Identity Control идентифицирует сервер AD (сервис WinRM) по имени CN, которое указано в сертификате (в примере ниже это **dc-test.ngfw-lab.local**) и аутентифицирует сервер проверкой доверия к сертификату (проверяет, что присланный сертификат подписан доверенным корневым сертификатом).

Описываемая интеграция для работы требует доступность сетевых портов к Active Directory, указанных в таблице.

Таблица 16. Сетевые порты, необходимые для работы

Адрес источника	**Порт источника**	**Адрес назначения**	**Порт назначения**	**Сервис**
Сетевой адрес системы управления	<random>	Сетевой адрес сервера с ролью контроллера домена	5986/TCP	WinRM HTTPS
Сетевой адрес системы управления	<random>	Сетевой адрес сервера с ролью контроллера домена	636/TCP	LDAP over SSL

28.2. Известные ограничения

Список известных ограничений:

— Минимальная версия Windows Server — 2019.

— Ограничение по числу контроллеров домена, подключаемых по WinRM:

- До версии 1.7.1 — 4.
- Начиная с версии 1.7.1 — 10, с возможностью увеличения до 255. Параметр ограничения вынесен в отдельную опцию `data_sources_limit` в конфигурационный файл `agent.cfg`.

28.3. Настройка сервера Microsoft Active Directory

В этом разделе приводятся инструкции по настройке сервера Microsoft Active Directory.

В этом разделе

Установка роли AD на Windows-сервер (опционально для тестов) (см. раздел 28.3.1)

Создание учетной записи сервисного пользователя (см. раздел 28.3.2)

Добавление учетной записи NETWORK SERVICE в группу безопасности (см. раздел 28.3.3)

Настройка хостового межсетевого экрана на контроллере домена (см. раздел 28.3.4)

Выпуск сертификатов на сервере системы управления (см. раздел 28.3.5)

Запуск службы WinRM (см. раздел 28.3.6)

Настройка журналирования событий безопасности (см. раздел 28.3.7)

28.3.1. Установка роли AD на Windows-сервер (опционально для тестов)

Для установки роли AD на Windows-сервер необходимо настроить сетевой интерфейс сервера: задать IP-адрес, шлюз по умолчанию и DNS-сервера.

- Чтобы настроить сетевой интерфейс сервера:

1. Нажмите **Start** → **Control Panel** → **System** → **Change settings**.

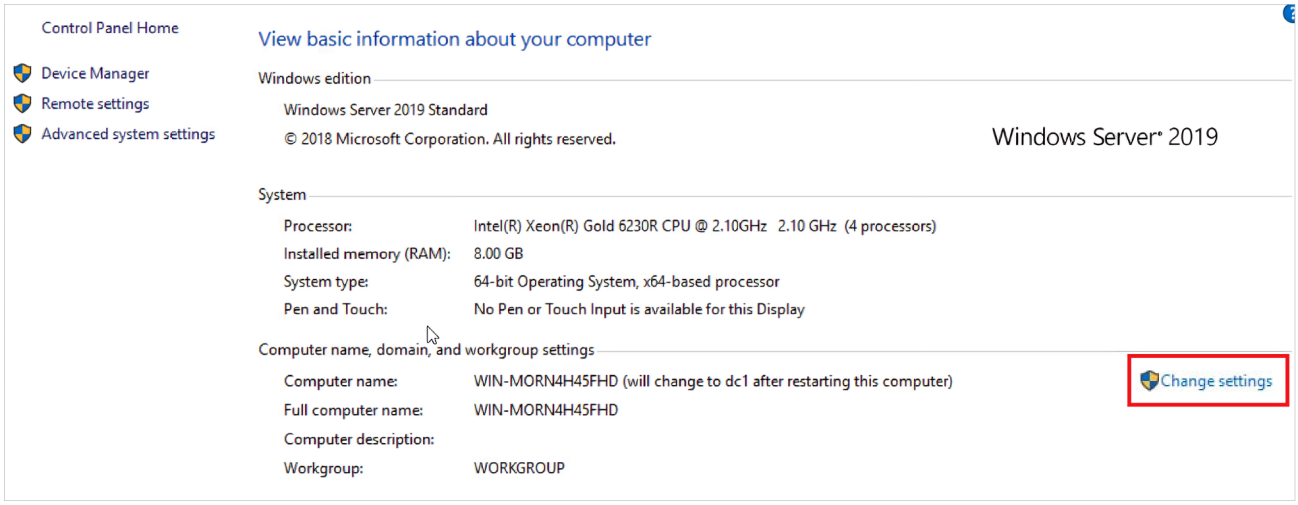


Рисунок 163. Окно **System**

2. В открывшемся окне нажмите **Change**.

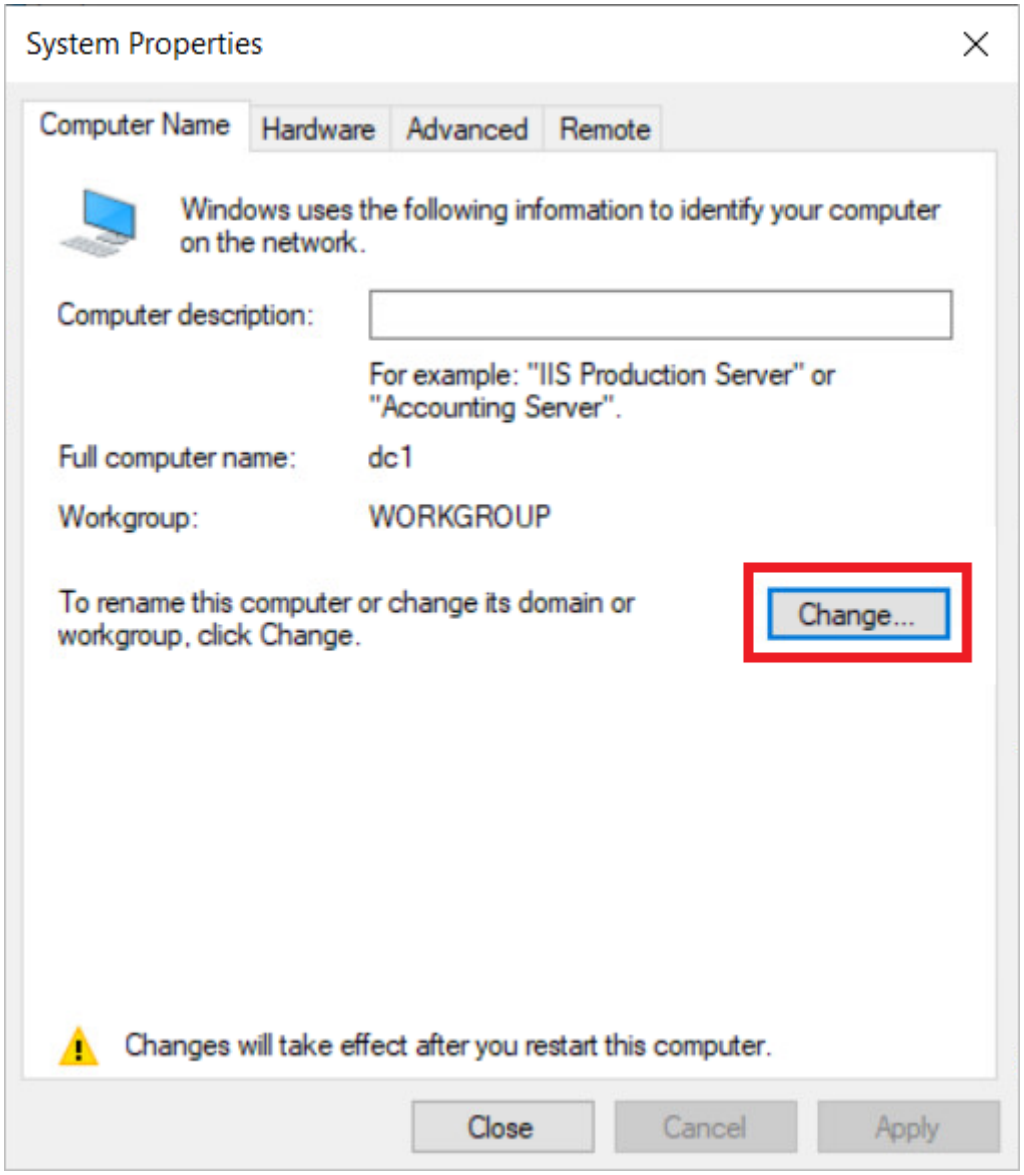


Рисунок 164. Изменение имени компьютера

3. Введите имя компьютера. В примере ниже это **dc1**.
4. Нажмите **OK**.

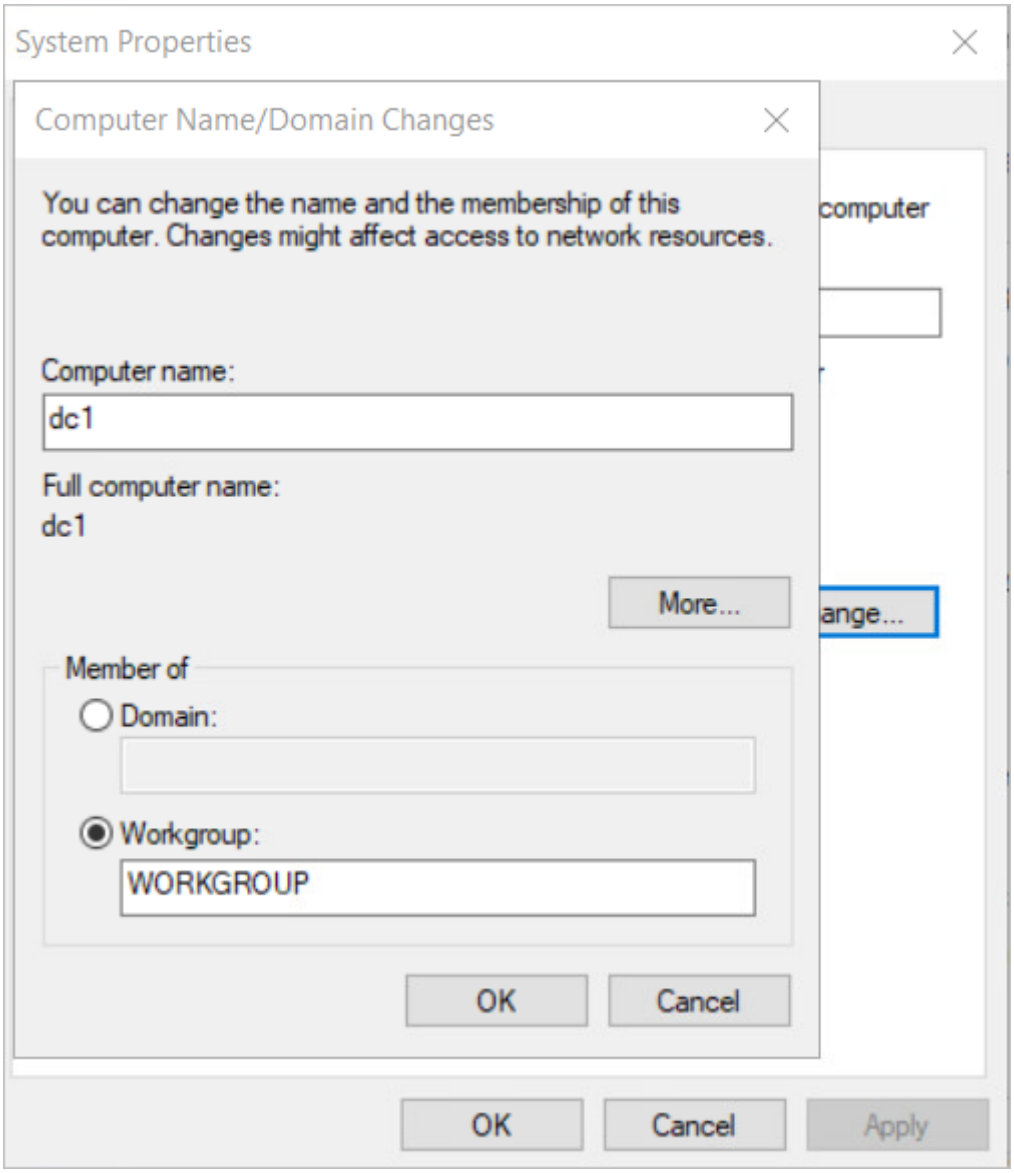


Рисунок 165. Ввод имени компьютера

Система предложит перезагрузить сервер.

5. Нажмите **Restart Now** для перезагрузки сервера.

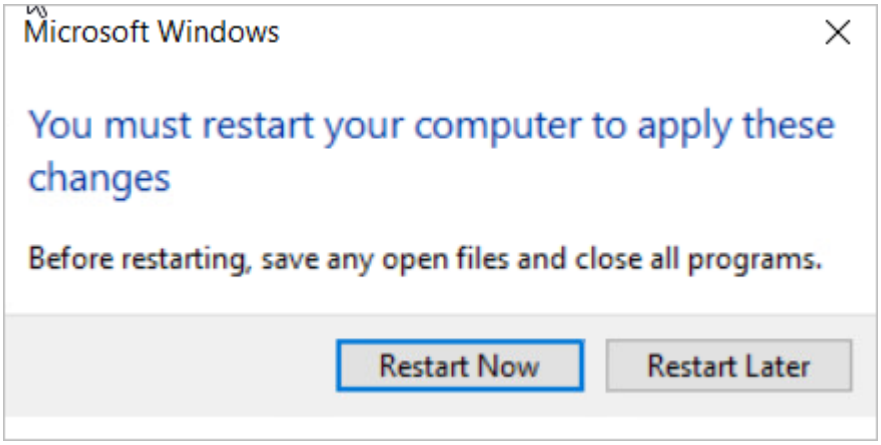


Рисунок 166. Перезагрузка компьютера

6. Включите Active Directory и DNS на сервере. Более подробная инструкция по настройке AD приведена по ссылке.

   На шаге **Server selection** удостоверьтесь, что имя сервера (**dc1** в этом примере) и IP-адрес (**172.28.0.1** в этом примере) корректные и соответствуют тому имени и адресу сервера, которые вы указали на предыдущих шагах.

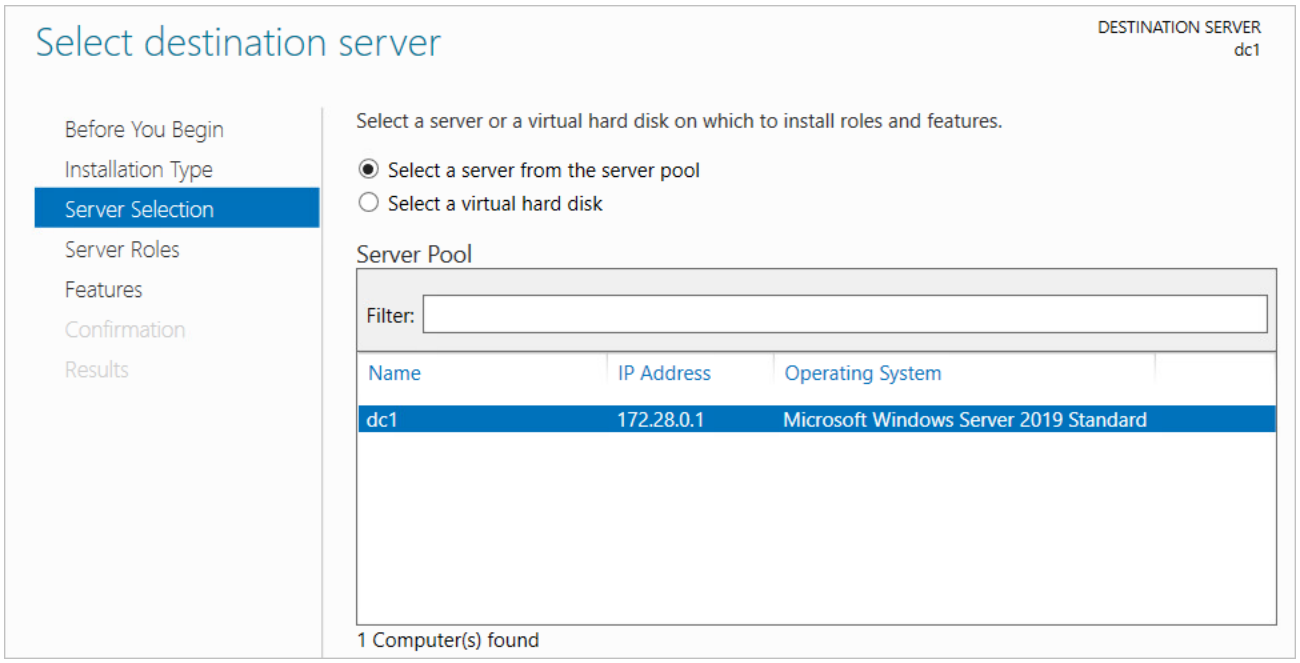


Рисунок 167. Проверка имени и IP-адреса сервера

28.3.2. Создание учетной записи сервисного пользователя

На этом этапе необходимо создать учетную запись сервисного пользователя. Агент Identity Control PT NGFW будет подключаться к серверу AD, используя учетную запись этого пользователя.

- Чтобы создать учетную запись сервисного пользователя:

  1. Введите регистрационные данные в поля, как указано на рисунке ниже.
  2. Введите идентификатор пользователя.

     В примере ниже это пользователь с идентификатором **uagent**.

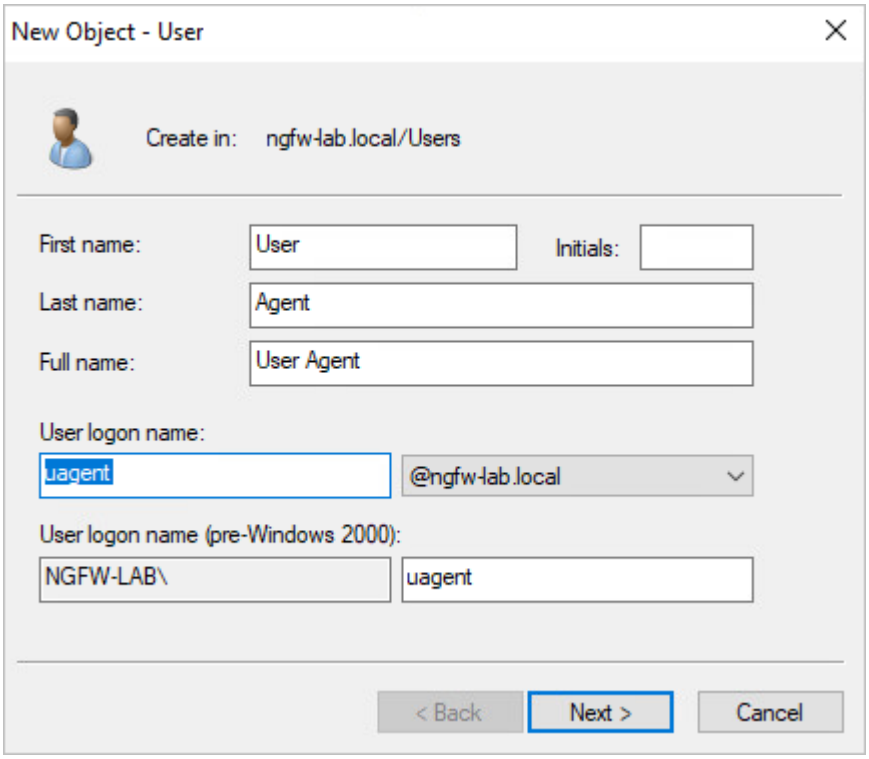


Рисунок 168. Создание сервисного пользователя

  3. Задайте сложный пароль, отвечающий требованиям парольной политики контроллера домена.
  4. Снимите флажок **User must change password at next logon**.
  5. Установите флажки **User cannot change password** (пользователь не может изменить пароль) и **Password never expires** (срок действия пароля не ограничен).

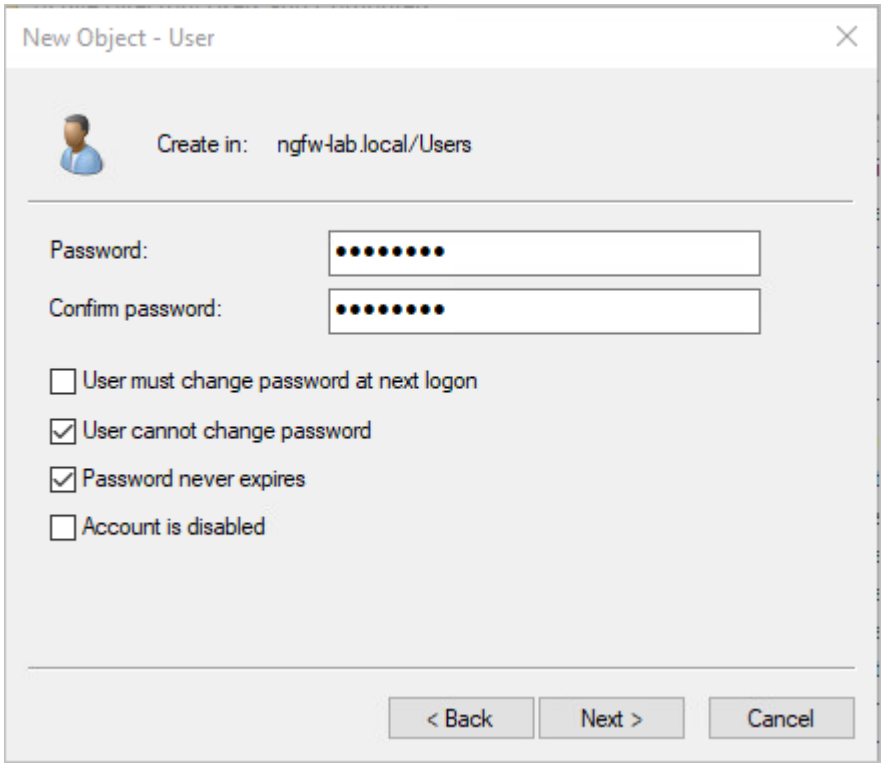


Рисунок 169. Создание пароля

6. Добавьте сервисного пользователя в группы **Event Log Readers** и **Remote Management Users**.

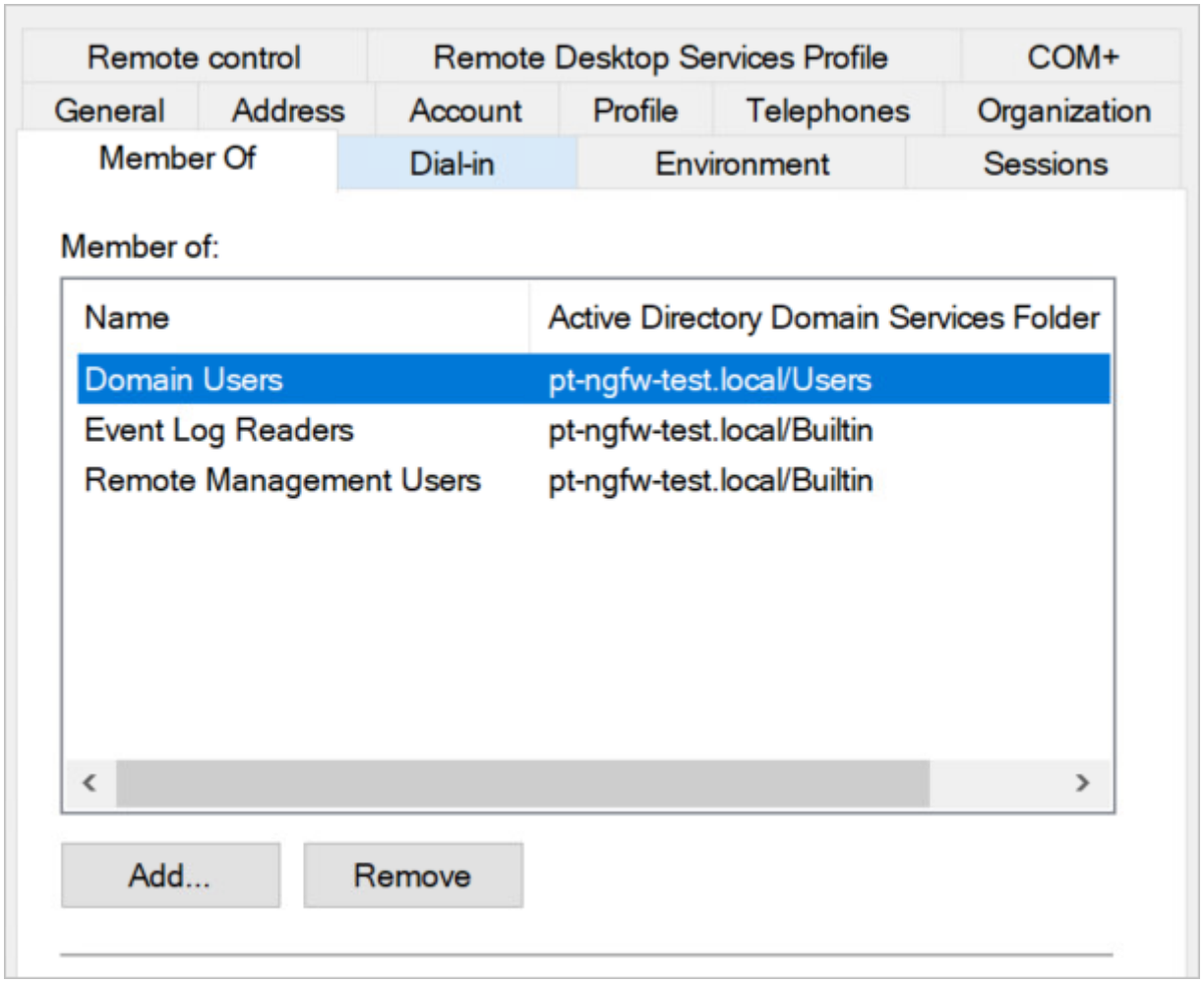


Рисунок 170. Добавление сервисного пользователя в группы

28.3.3. Добавление учетной записи NETWORK SERVICE в группу безопасности

Необходимо добавить предустановленную локальную учетную запись NETWORK SERVICE во встроенную группу (Built-In) Event Log Readers.

Так как эта локальная учетная запись не отображается в списке пользователей домена, ее необходимо найти вручную.

- Чтобы найти учетную запись NETWORK SERVICE:

  1. В перечне **Built-In** объектов AD выберите группу **Event Log Readers**.
  2. В контекстном меню выберите **Properties**.

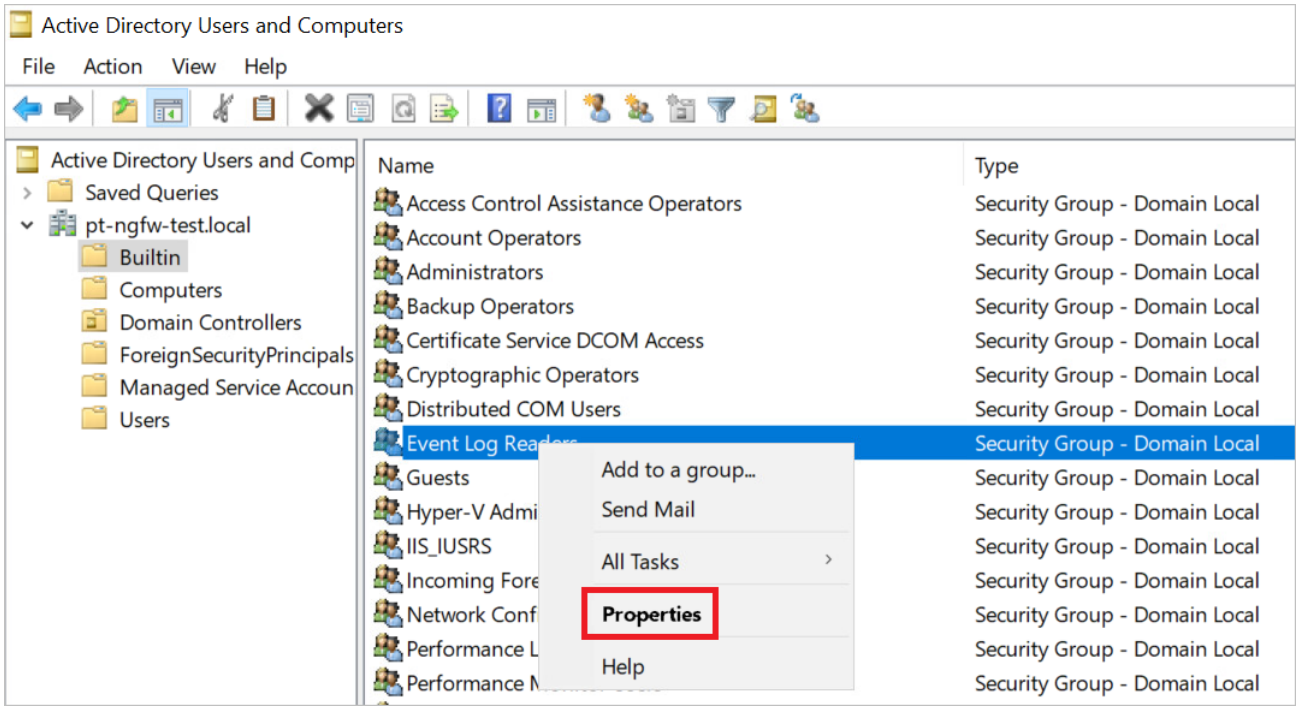


Рисунок 171. Список Builtin-объектов AD

3. На вкладке **Members** нажмите **Add**.

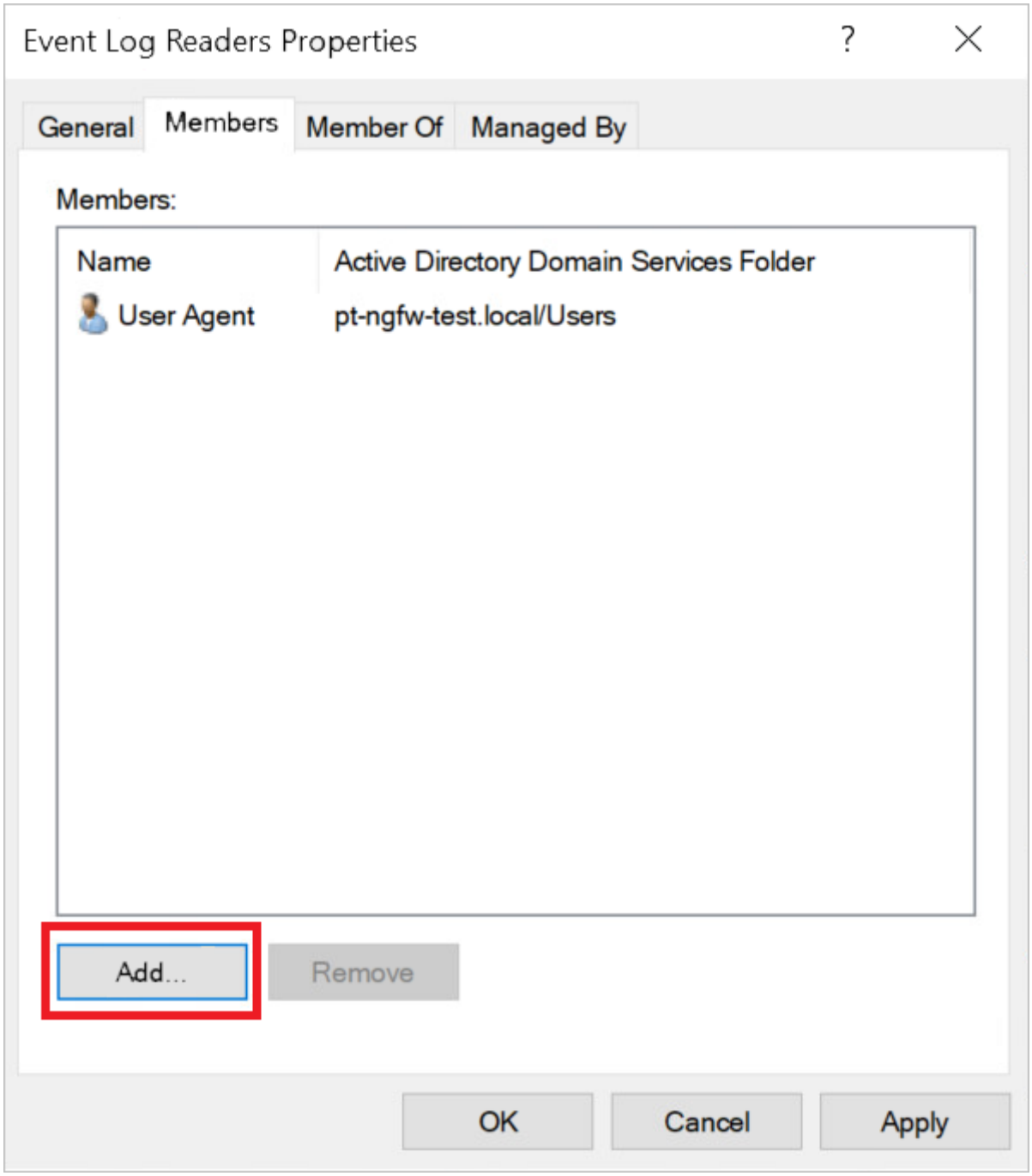


Рисунок 172. Свойства Event Log Readers

4. В открывшемся окне нажмите **Object types** и выберите **Built-in security principals**.

   Это позволит ограничить количество результатов поиска.

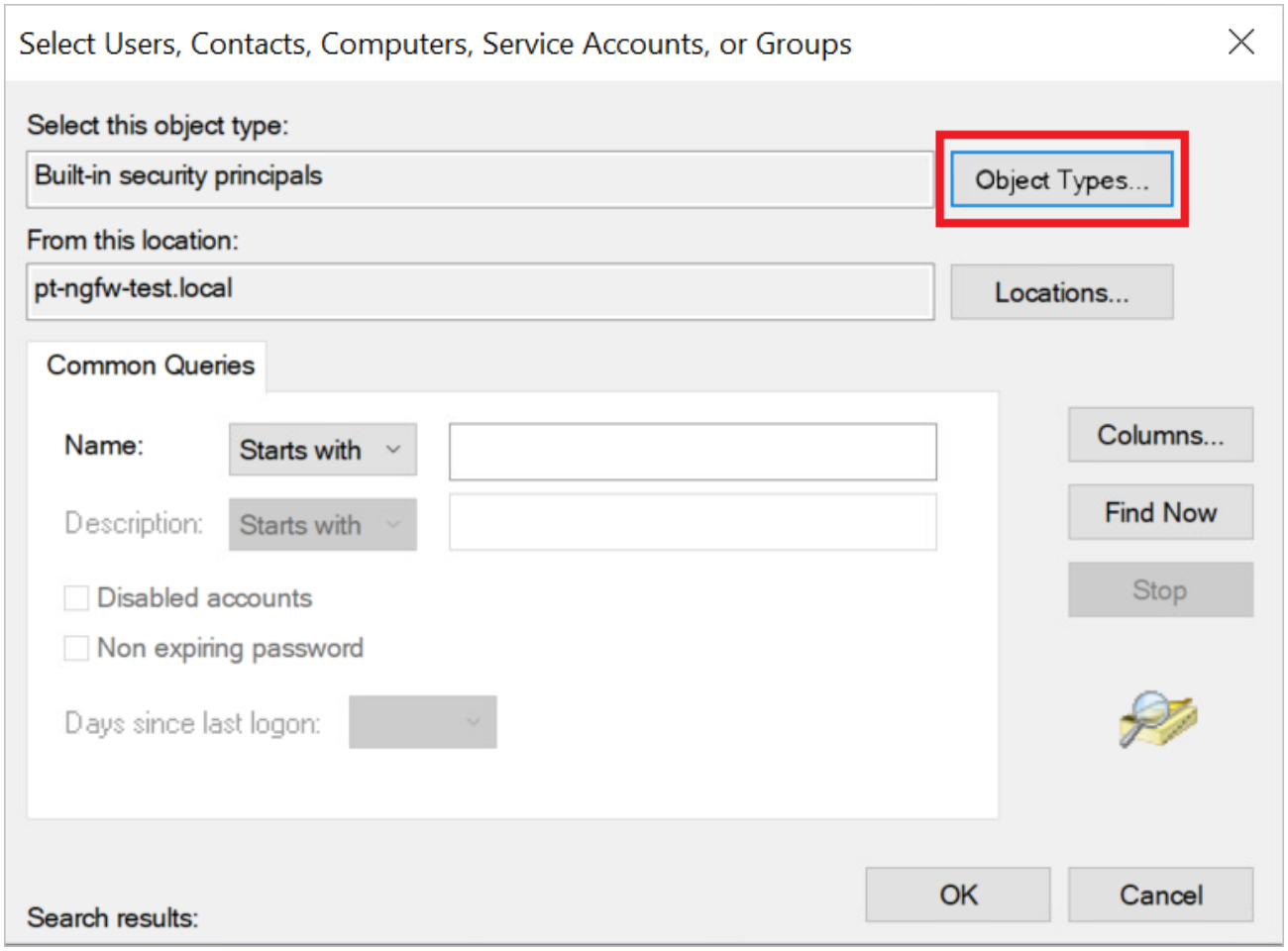


Рисунок 173. Поиск и выбор объектов

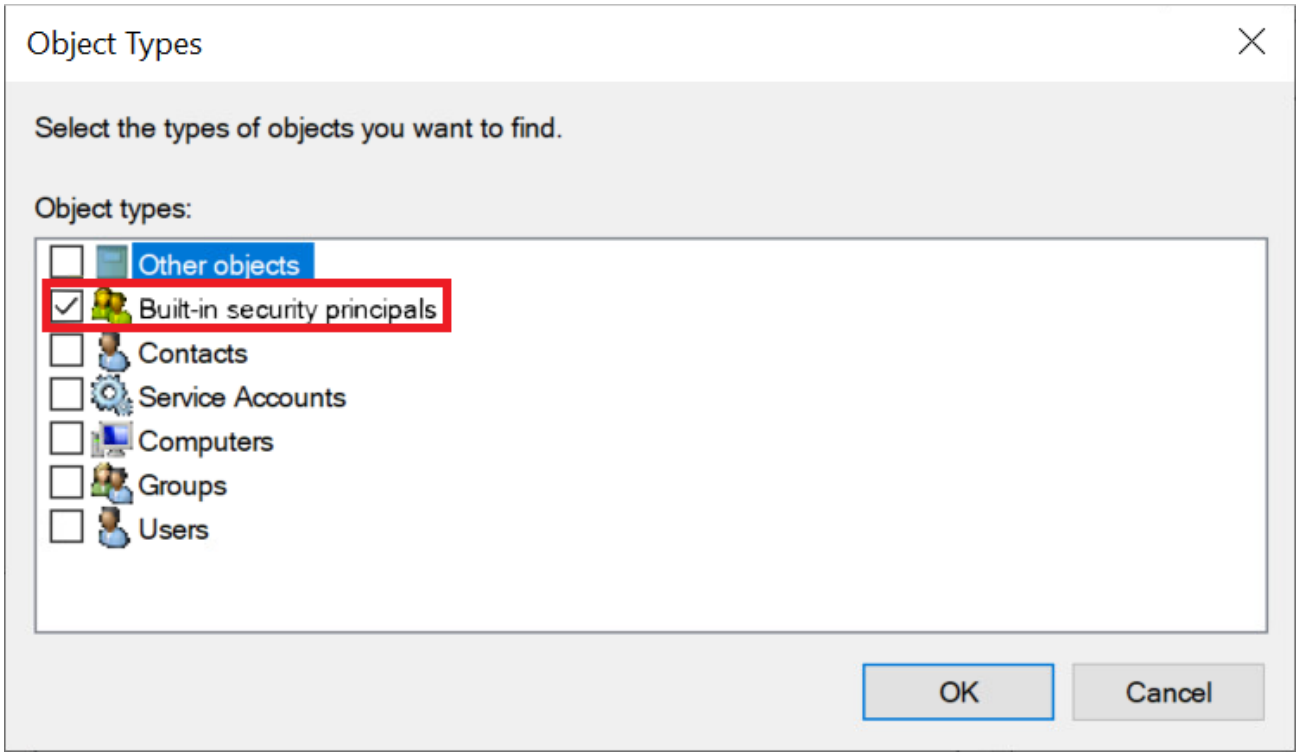


Рисунок 174. Выбор Built-in security principals

5. Нажмите **Advanced** → **Find Now**.

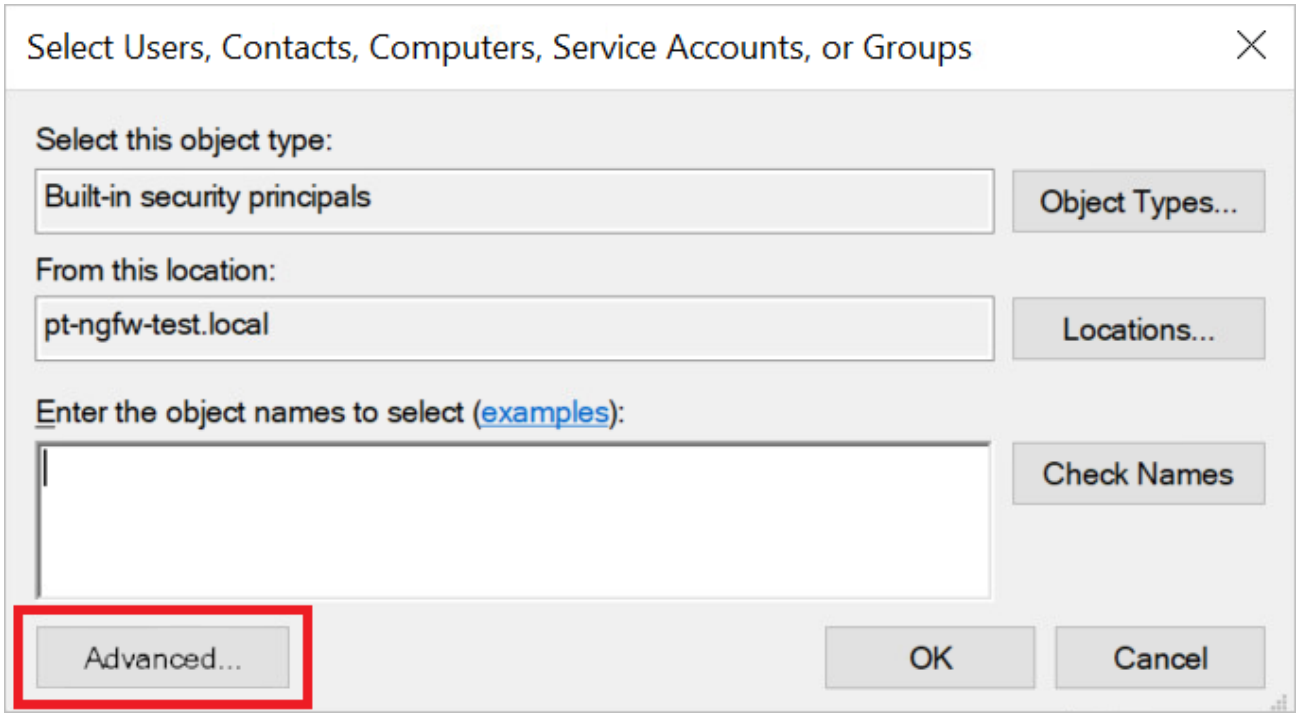


Рисунок 175. Advanced → Find Now

6. Выберите учетную запись **NETWORK SERVICE**.

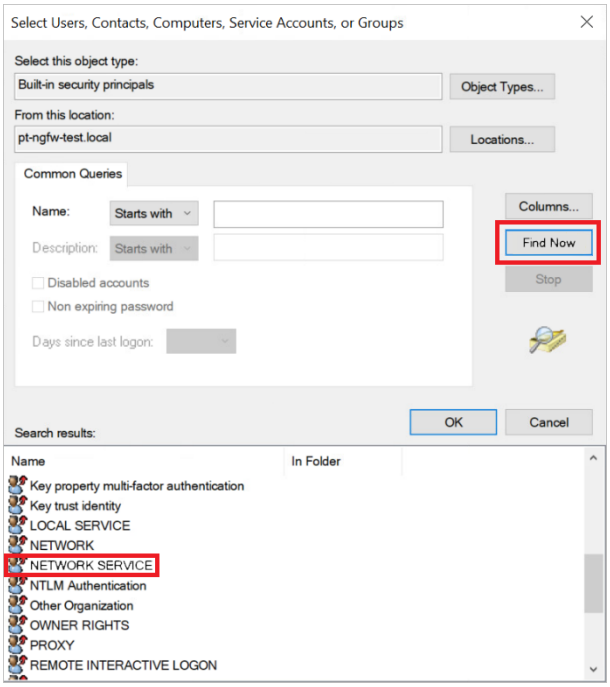


Рисунок 176. Выбор учетной записи NETWORK SERVICE

7. Убедитесь, что учетная запись **NETWORK SERVICE** появилась на вкладке **Members** группы **Event Log Readers**
8. Нажмите **Apply** → **OK**.

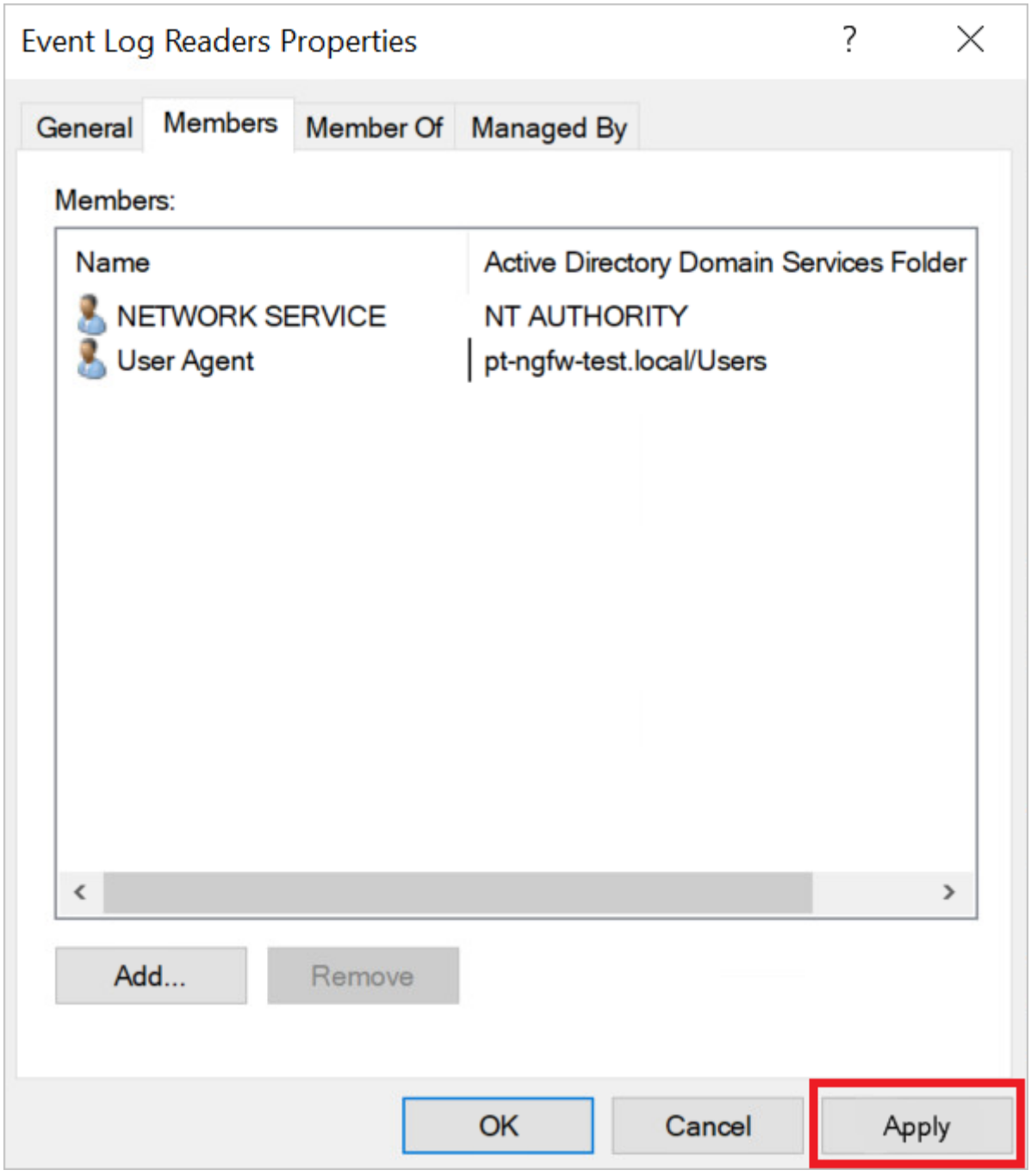


Рисунок 177. Применение изменений

9. Включите для сервисного пользователя (в этом примере это пользователь **uagent**) возможность чтения CIMV2 namespace:
   - Откройте окно **Run**, нажав Win+R
   - Введите `wmimgmt.msc` и нажмите **OK**.

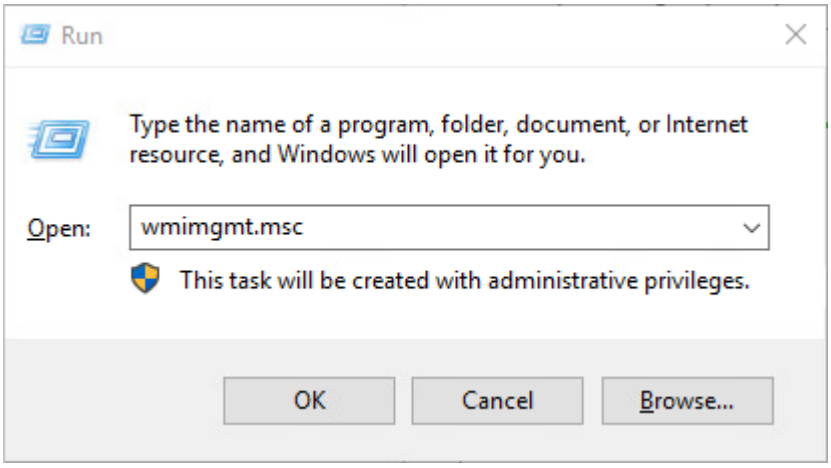


Рисунок 178. Запуск `wmimgmt.msc`

- В открывшемся окне в контекстном меню **WMI Control** выберите **Properties**.

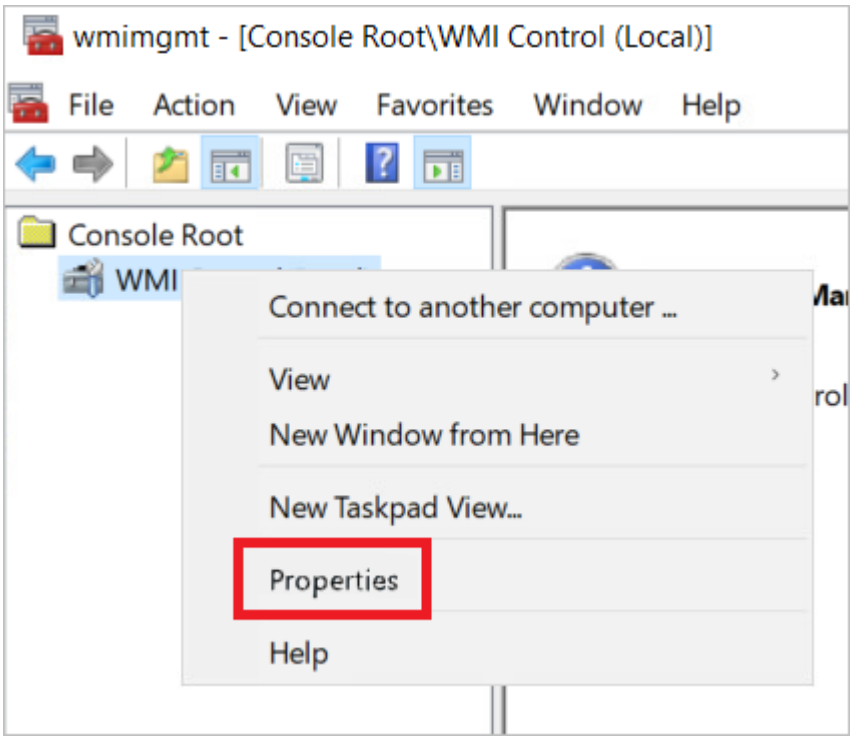


Рисунок 179. Пункт **Properties**

- На вкладке **Security** выберите **Root** → **CIMV2**
- Нажмите **Security**, как указано на рисунке ниже.

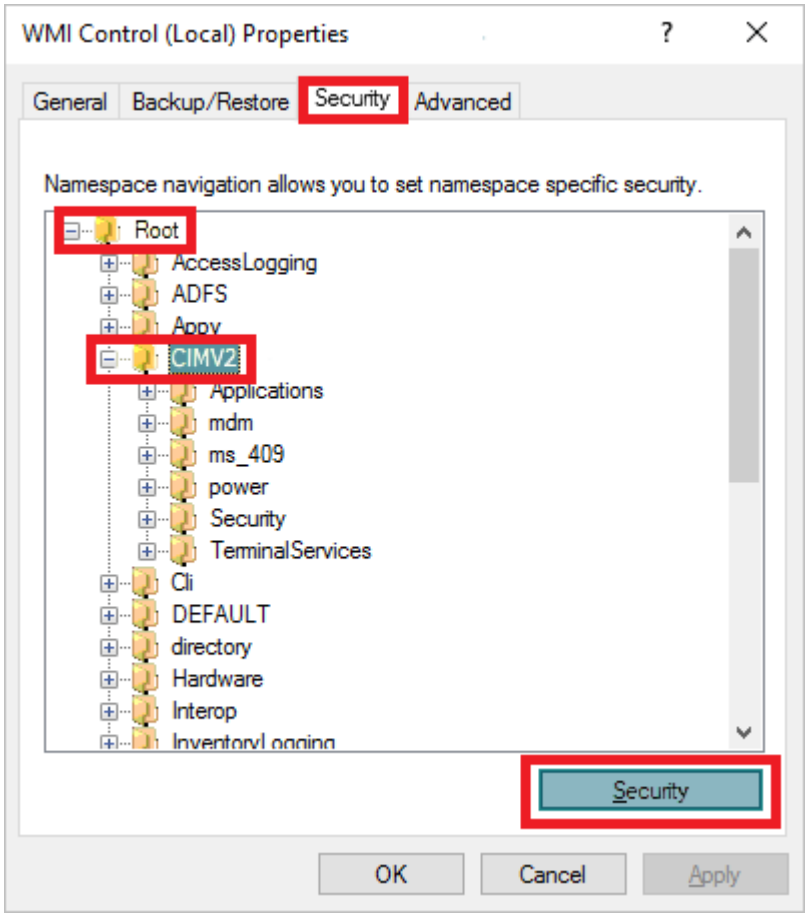


Рисунок 180. Свойства WMI Control (Local)

- Нажмите **Add** для добавления пользователя.
- В столбце **Allow** установите флажки **Enable Account** и **Remote Enable**.
- Нажмите **Apply** → **OK**.

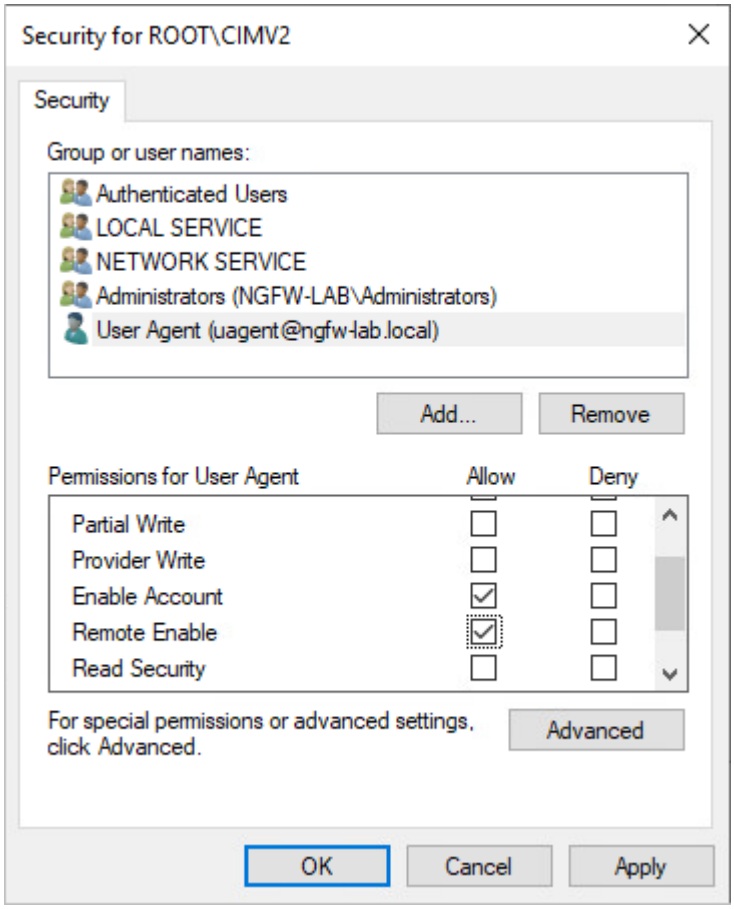


Рисунок 181. Параметры безопасности для ROOT\CIMV2

28.3.4. Настройка хостового межсетевого экрана на контроллере домена

На сервере Active Directory работает межсетевой экран, который по умолчанию запрещает входящие сетевые подключения. Следовательно, если не разрешить подключения от агента Identity Control PT NGFW, то они будут блокироваться, и данные о пользователях и группах получить не удастся.

Если это тестовый стенд, то простым решением является отключение встроенного межсетевого экрана Windows.

Примечание. Не рекомендуется для продуктивной среды.

- Чтобы отключить межсетевой экран:

1. Нажмите **Start** → **Control Panel** → **Windows Defender Firewall**. → **Customize Settings**.
2. Во всех пунктах выберите **Turn off**, как показано на рисунке.

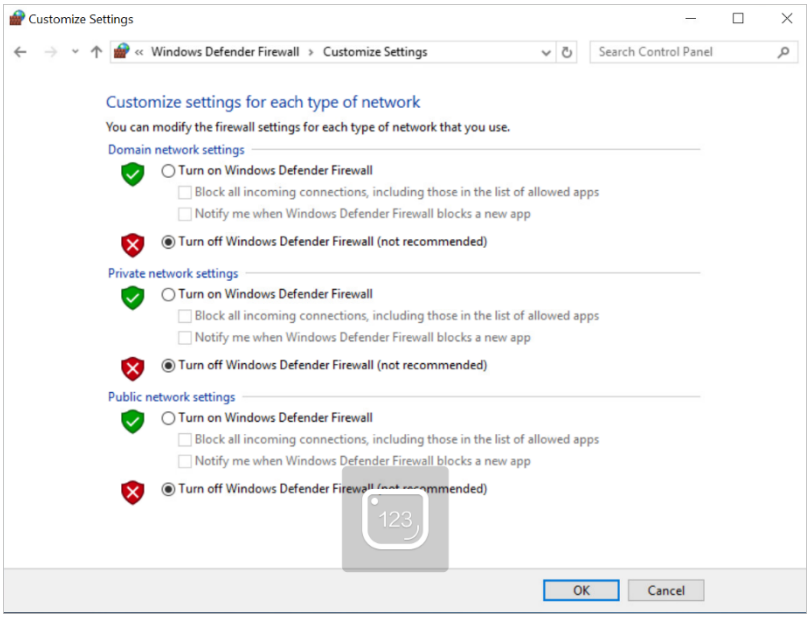


Рисунок 182. Параметры Брандмауэра Защитника Windows

В случае с продуктивной средой разрешите входящие подключения от системы управления PT NGFW, так как агент Identity Control работает на том же узле, что и система управления PT NGFW:

```
New-NetFirewallRule -DisplayName "LDAP over SSL Remote Management" -Name "LDAP over SSL Remote Management" -Profile Any -LocalPort 636 -Protocol TCP
```

28.3.5. Выпуск сертификатов на сервере системы управления

Примечание. Выберите этот вариант развертывания если у вас нет корпоративного центра сертификации или вы не хотите его использовать.

В примере ниже описывается генерация root-сертификата и сертификата для взаимодействия с AD на его основе.

- Чтобы сгенерировать сертификаты:

1. Сгенерируйте приватный ключ Root CA:

   ```
   sudo openssl genrsa -des3 -out root-private.key 2048
   ```

   При генерации будет запрос на создание пароля. Пароль необходимо запомнить.

2. Сгенерируйте Root CA:

   ```
   sudo openssl req -x509 -new -nodes -key root-private.key -sha256 -days 1825 -out root-CA-lab.crt
   ```

   При генерации будет запрос на ввод пароля.

3. Введите пароль, который вы создали на предыдущем шаге.

4. Поля, запрашиваемые при создании сертификата, заполните на свое усмотрение.
5. Сгенерируйте приватный ключ конечного узла (в примере — DC-Test):

   ```
   sudo openssl genrsa -des3 -out dc-test-private.key 2048
   ```

   При генерации будет запрос на создание пароля. Пароль необходимо запомнить.
6. Сгенерируйте CSR (Certificate Request) для будущего сертификата конечного узла (в примере — DC-Test):

   ```
   sudo openssl req -key dc-test-private.key -new -out dc-test.csr
   ```

   При генерации будет запрос на ввод пароля.
7. Введите пароль, который вы создали на предыдущем шаге.
8. Поля, запрашиваемые при создании сертификата, заполните на свое усмотрение.

   Внимание! CN должно совпасть с Hostname Windows сервера с ролью контроллера домена.

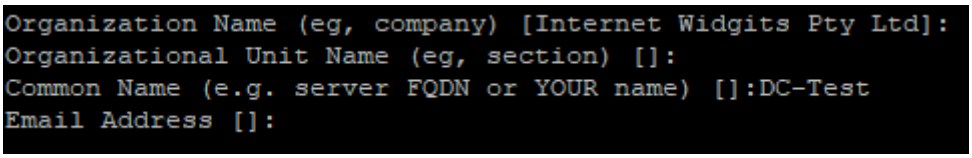


Рисунок 183. Ввод пароля

9. Создайте файл конфигурации для расширений сертификата конечного узла:

   ```
   nano dc1-cert-config.ext
   ```

   Содержимое файла:

   ```
   basicConstraints = critical, CA:FALSE
   subjectKeyIdentifier = hash
   authorityKeyIdentifier = keyid:always, issuer:always
   keyUsage = critical, digitalSignature, keyEncipherment, keyAgreement
   extendedKeyUsage = critical, serverAuth
   subjectAltName = @alt_names
   [alt_names]
   DNS.1 = dc-test.ngfw-lab.local
   IP.1 = 172.28.0.1
   ```

   Комментарии к файлу:

   - DNS.1 — FQDN сервера AD;
   - IP.1 — IP-адрес сервера AD.
10. Сгенерируйте сертификат конечного узла (DC-Test):

    ```
    sudo openssl x509 -req -CA root-CA-lab.crt -CAkey root-private.key -in dc-test.csr -out dc-test.crt -days 1000 -CAcreateserial -extfile dc1-cert-config.ext
    ```
11. Сгенерируйте сертификат с приватным ключом внутри:

    ```
    sudo openssl pkcs12 -export -out dc-test.pfx -inkey dc-test-private.key -in dc-test.crt -certfile root-CA-lab.crt
    ```

При генерации будет запрос на создание пароля. Пароль необходимо запомнить.

12. Созданный корневой сертификат (в примере — `root-CA-lab.crt`) нужно установить в хранилище доверенных корневых сертификатов на Windows Server (хранилище **Local Machine**).

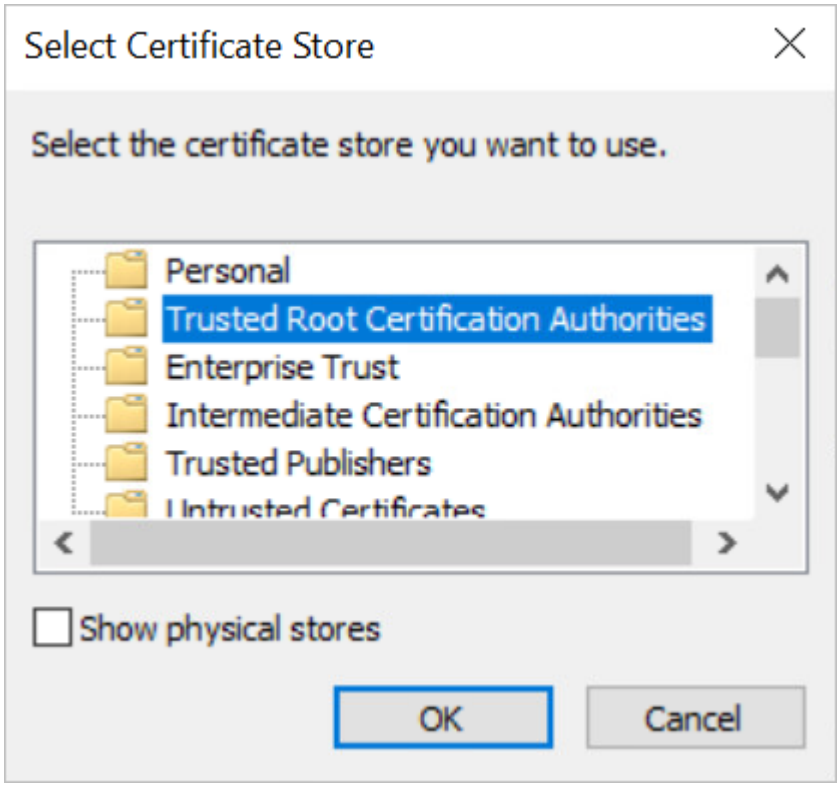


Рисунок 184. Выбор хранилища для сертификатов **Trusted Root Certification Authorities**

Более подробная информация по настройке и включению протокола LDAP через протокол SSL с помощью стороннего центра сертификации приведена по ссылке.

13. Созданный архив сертификата `dc-test.pfx` переместите в папку **personal** (хранилище **Local Machine**).

Внимание! Сертификат `.pfx` содержит приватный ключ. Именно такой сертификат нужно импортировать. Наличие приватного ключа обязательно. Без его наличия нельзя будет настроить службу WinRM на последующих шагах.

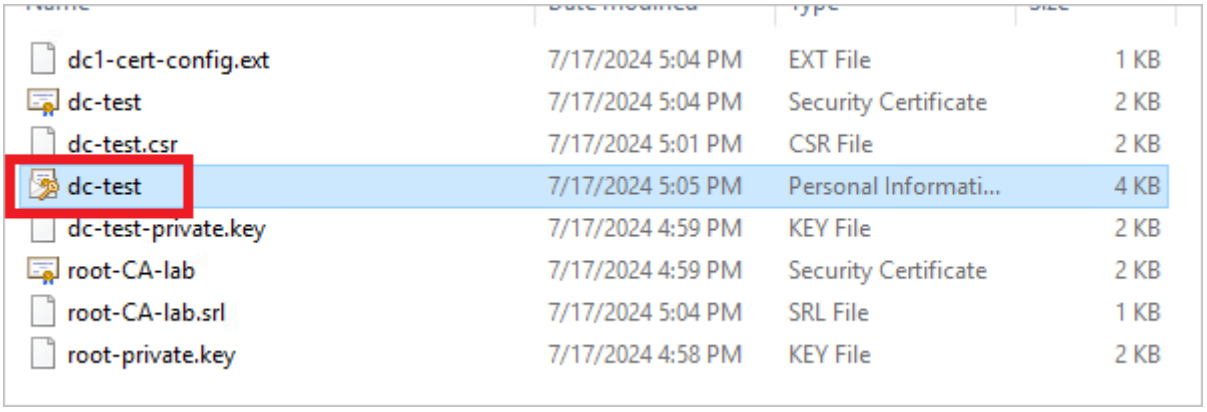


Рисунок 185. Архив сертификата `dc-test.pfx`

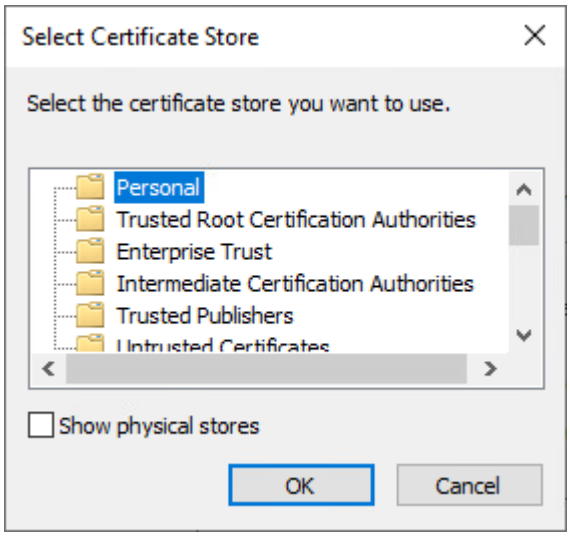


Рисунок 186. Выбор хранилища для сертификатов **Personal**

28.3.6. Запуск службы WinRM

- Чтобы запустить службу WinRM:

1. В командной строке проверьте состояние службы:

```
winrm enumerate winrm/config/listener
```

```
C:\Users\Администратор>winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 172.28.0.1, ::1
```

Рисунок 187. Проверка статуса службы WinRM

На примере рисунка служба запущена с HTTP-транспортом. Это необходимо изменить.

2. Выполните команду:

   `winrm qc`

3. Введите `y`, чтобы подтвердить изменения.

```
C:\Users\Администратор>winrm qc
Служба WinRM уже выполняется на этом компьютере.
Служба WinRM не настроена на разрешение удаленного управления компьютером.
Необходимо внести следующие изменения:

Создайте прослушиватель WinRM на HTTP://* для приема запросов WS-Man на любом из IP-адресов этого компьютера.

Выполнить изменения [y/n]? y

Служба WinRM обновлена для удаленного управления.

Создан прослушиватель WinRM на HTTP://* для приема запросов WS-Man на любом из IP-адресов этого компьютера.
```

Рисунок 188. Создание прослушивателя WinRM

Возможно, что служба уже запущена. В этом случае отобразятся сообщения, что WinRM уже выполняется.

```
C:\Users\Администратор>winrm quickconfig
Служба WinRM уже выполняется на этом компьютере.
Служба WinRM уже настроена для удаленного управления на этом компьютере.
```

Рисунок 189. Сообщение системы при работающей службе WinRM

Полезные ссылки:

- настройка WINRM для HTTPS;
- включение расширенной политики аудита безопасности.

4. Выполните реконфигурирование WinRM на HTTPS-транспорт:

Исходная команда:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS
@{Hostname="<hostname>";CertificateThumbprint="Certificate Thumbprint"}
```

Пример команды (с отпечатком сертификата):

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="DC-
Test";CertificateThumbprint="ab4531c7fed65bc3d1632c82069ec47ef706c4bf"}
```

Примечание. Отпечаток сертификата необходимо скопировать из файла сертификата (не корневого, а хостового. В примере — dc-test.crt).

Примечание. Указывая отпечаток сертификата в команде вы указываете, какой именно сертификат следует использовать при установке HTTPS-соединения.

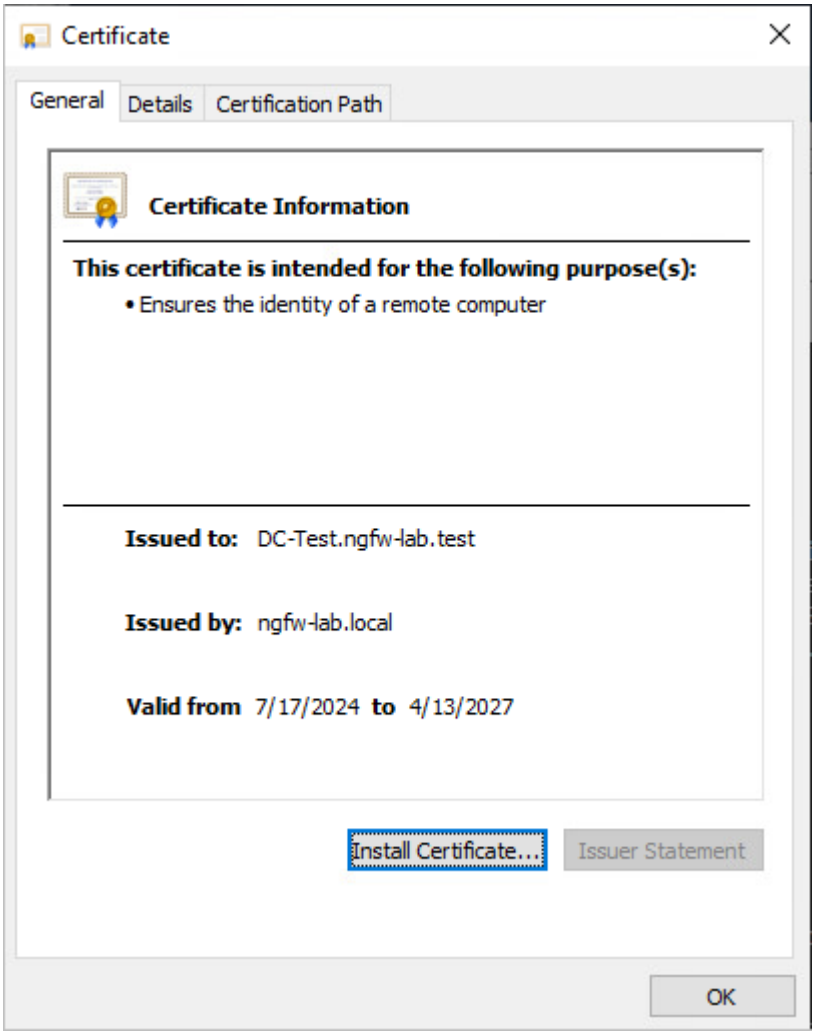


Рисунок 190. Установка сертификата

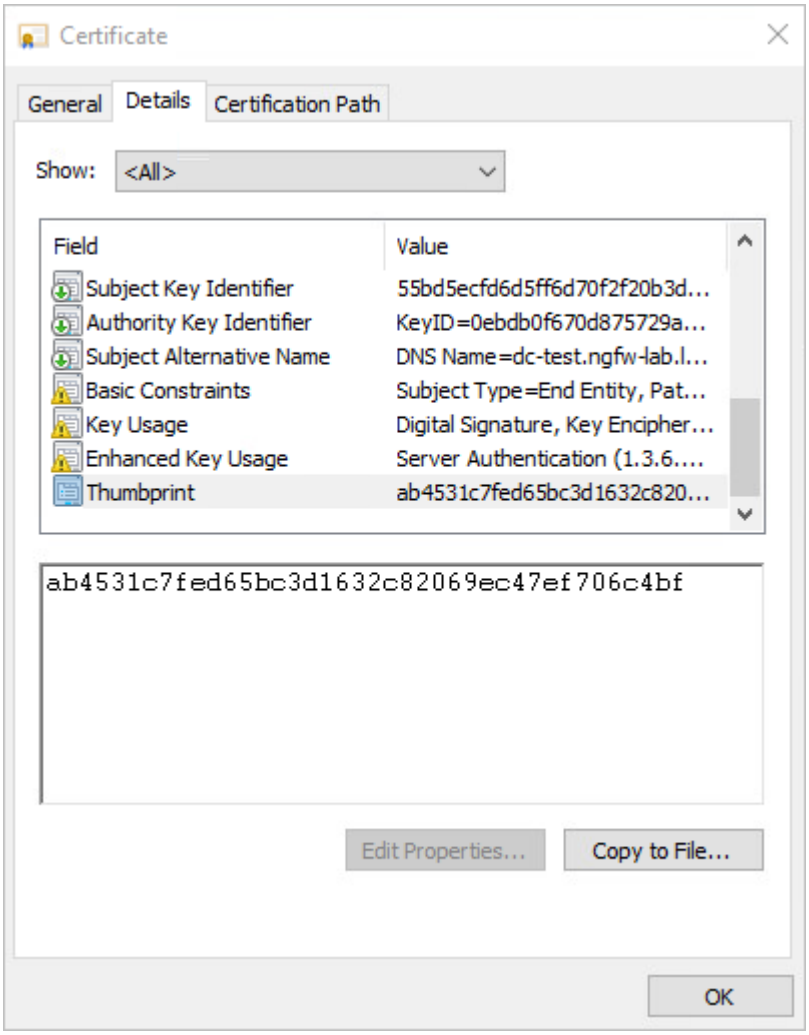


Рисунок 191. Отпечаток сертификата

```
C:\Users\Administrator\Downloads>winrm create winrm/config/Listener?Address=*+Transport=HTTPS @{Hostname="DC-Test";Certi
ficateThumbprint="f983ea2e505d3cb7988bba97ad047754d2f0ccb5"}
ResourceCreated
    Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    ReferenceParameters
        ResourceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener
        SelectorSet
            Selector: Address = *, Transport = HTTPS
```

Рисунок 192. Пример успешного выполнения команды

Далее проверьте, что транспорт HTTPS включен:

```
winrm enumerate winrm/config/listener
```

```
C:\Users\Administrator\Downloads>winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 10.13.169.80, 127.0.0.1, ::1, fe80::b075:a705:77a8:f81d%4

Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = DC-Test
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = f983ea2e505d3cb7988bba97ad047754d2f0ccb5
    ListeningOn = 10.13.169.80, 127.0.0.1, ::1, fe80::b075:a705:77a8:f81d%4
```

Рисунок 193. Проверка успешности включения транспорта HTTPS

5. Включите базовую аутентификацию на стороне клиента:

   `winrm set winrm/config/client/auth @{Basic="true"}`

```
C:\Users\Администратор>winrm set winrm/config/client/auth @{Basic="true"}
Auth
    Basic = true
    Digest = true
    Kerberos = true
    Negotiate = true
    Certificate = true
    CredSSP = false
```

Рисунок 194. Выполнение команды set winrm (клиент)

Включите базовую аутентификацию на стороне службы:

`winrm set winrm/config/service/auth @{Basic="true"}`

```
C:\Users\Администратор>winrm set winrm/config/service/auth @{Basic="true"}
Auth
    Basic = true
    Kerberos = true
    Negotiate = true
    Certificate = false
    CredSSP = false
    CbtHardeningLevel = Relaxed
```

Рисунок 195. Выполнение команды set winrm (служба)

6. Убедитесь, что хостовый межсетевой экран разрешает подключения к службе WinRM.

   Пример правила для хостового межсетевого экрана:

   ```
   New-NetFirewallRule -DisplayName "Winrm HTTPS Remote Management" -Name "Winrm HTTPS Remote Management" -Profile Any -LocalPort 5986 -Protocol TCP
   ```

   Примечание. В лабораторных условиях межсетевой экран можно отключить.

7. Перезапустите службу WinRM.

   Примечание. В лабораторных условиях можно перезагрузить хост Domain Controller.

28.3.7. Настройка журналирования событий безопасности

Как правило, по умолчанию журналирование необходимых событий на сервере AD уже включено, и указанные ниже действия выполнять не нужно. Однако в случае, если User-агент работает, успешно подключается к серверу AD, но данных о пользователях нет — проверьте действительно ли включено журналирование событий на сервере AD. Именно эти события читает User-агент для получения информации о пользователях и их IP-адресах.

- Чтобы включить журналирование необходимых событий безопасности:

  1. В Server manager перейдите в меню **Tools** → **Group Policy Management**.

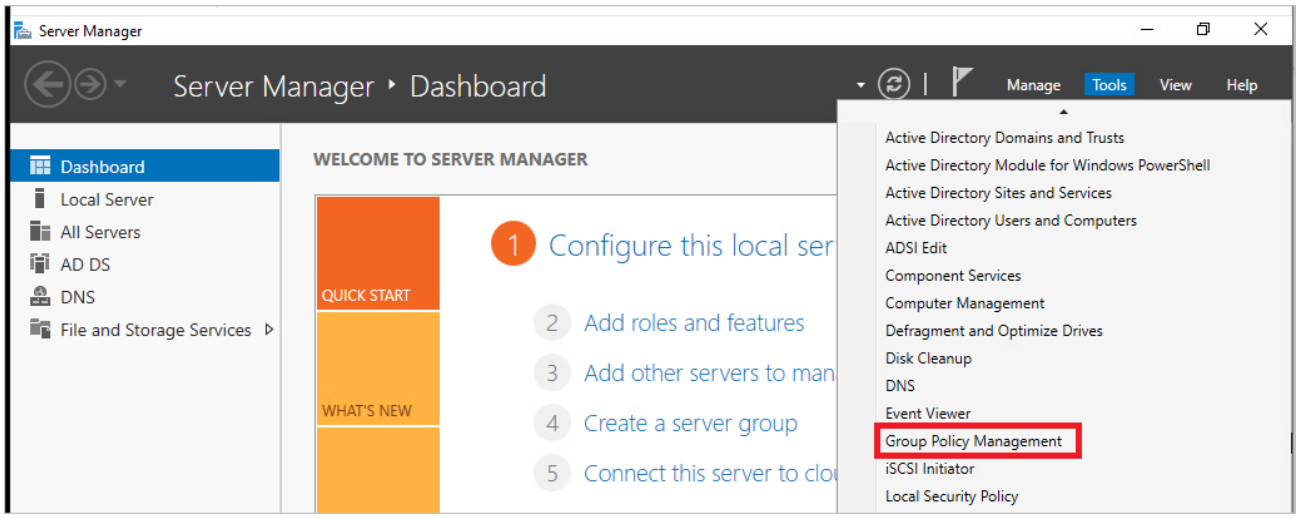


Рисунок 196. Список инструментов Server Manager

  2. Откройте **Forest: <Имя домена>** → **Domains** → **<Имя домена>** → **Domain Controllers**.
  3. В контекстном меню **Default Domain Controllers Policy** выберите **Edit...**.

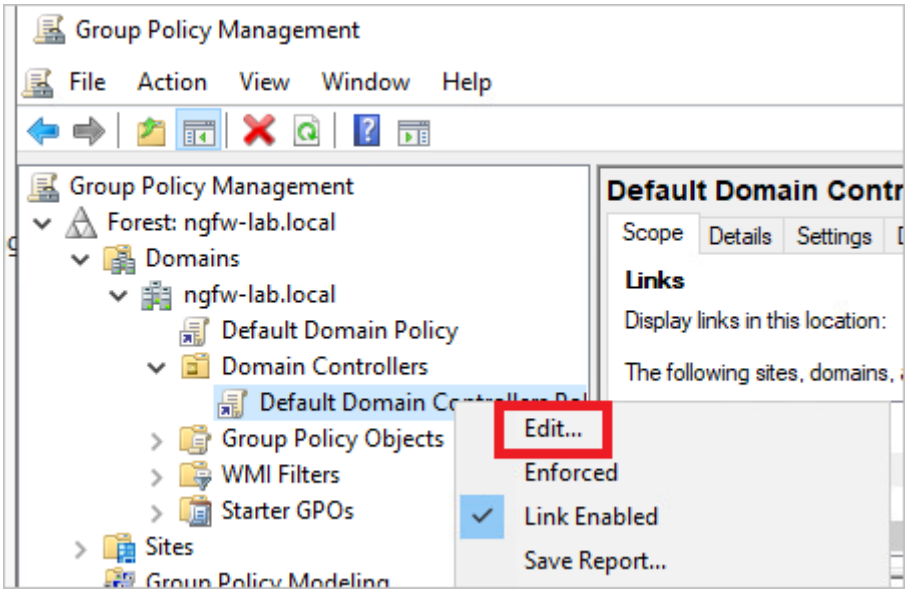


Рисунок 197. Переход в **Default Domain Controllers Policy**

В открывшемся окне перейдите в **Security Settings** → **Advanced Audit Policy Configuration** → **Audit Policies**.

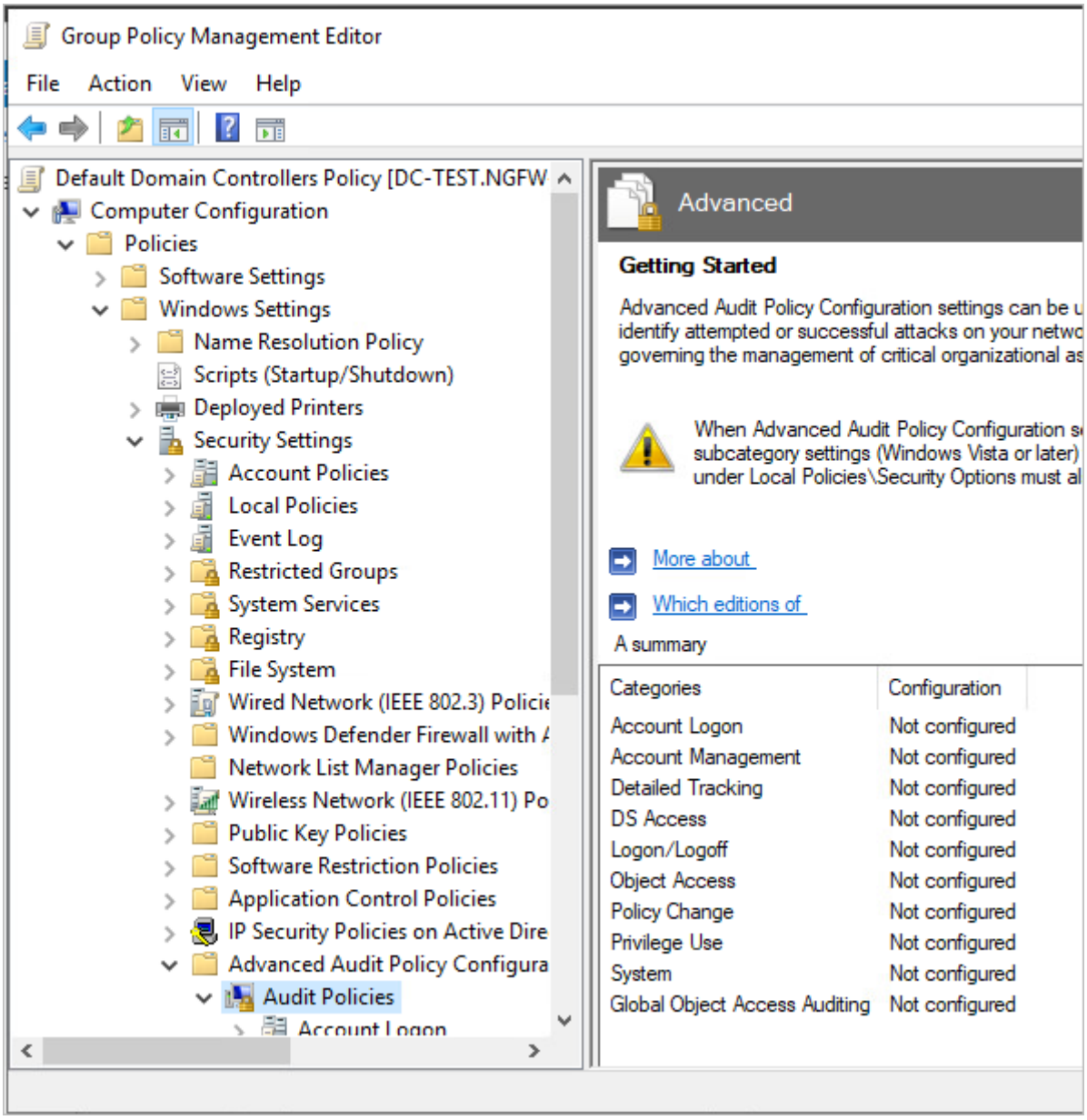


Рисунок 198. Переход в **Audit Policies**

4. Включите журналирование следующих событий:

   - **Success events of Kerberos Authentication Service**, **Kerberos Service Ticket Operations in Account Logon section**;
   - **Success events of Audit Logon in Logon/Logoff section**;
   - **Success events of Audit User Account Management in Account Management section**;
   - **Success events of Audit Security Group Management in Account Management section**;

- **Success events of Audit Directory Service Changes in DS Access section**.

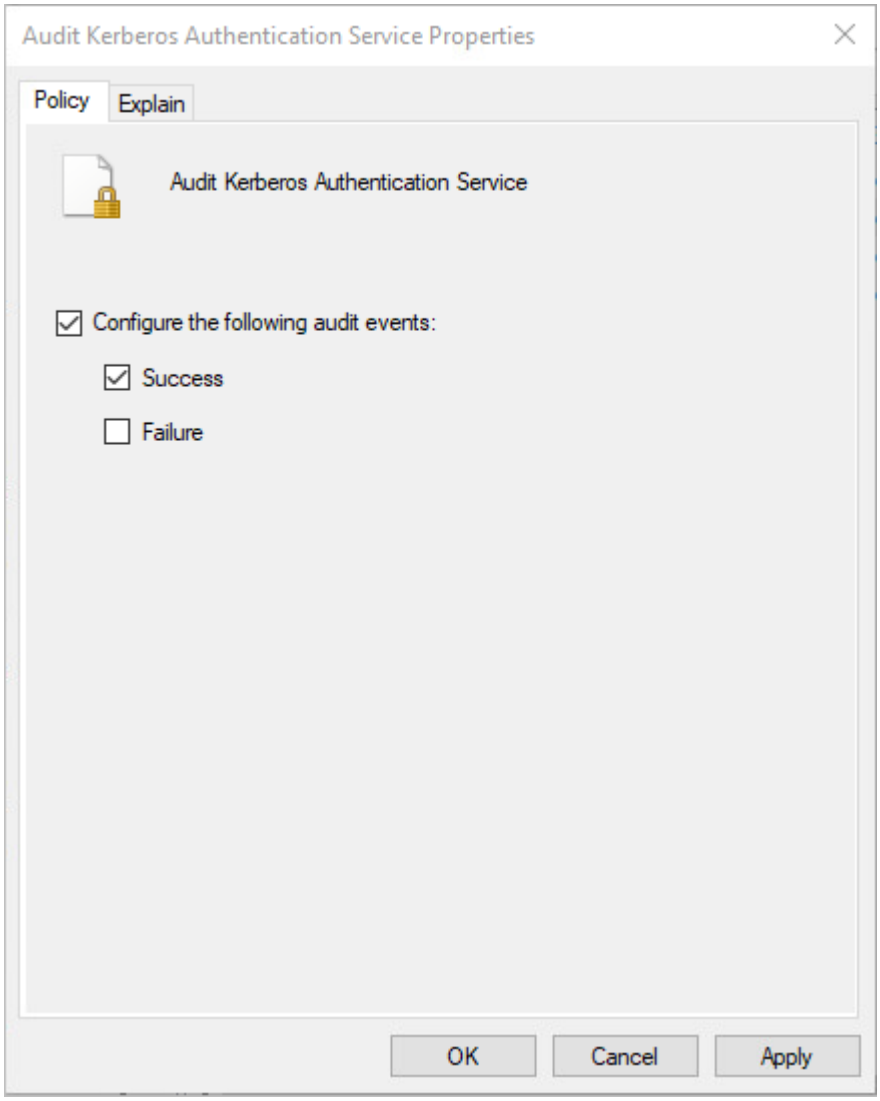


Рисунок 199. Пример включения журналирования событий **Audit Kerberos Authentication Service**

5. Включите аудит лог для пользователей и групп:
   - В меню **Tools** выберите **Active Directory Users and Computers**.

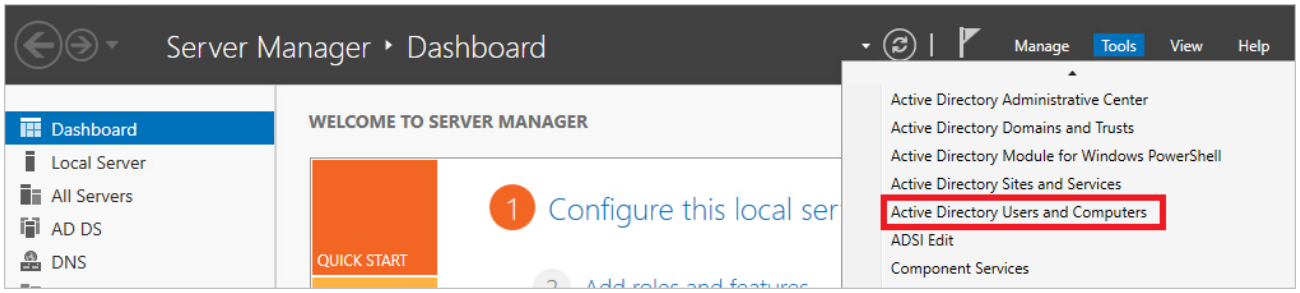


Рисунок 200. Инструменты Server Manager

- В меню **View** выберите **Advanced Features**.

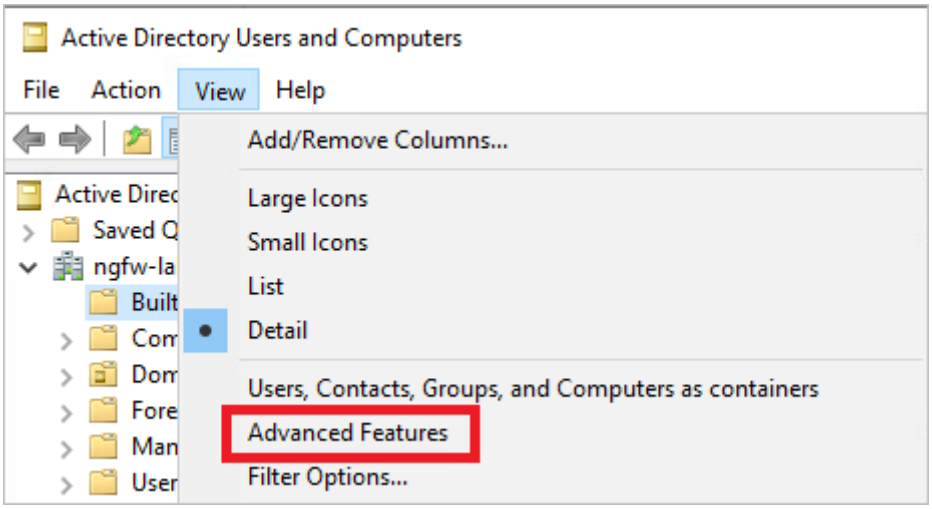


Рисунок 201. Пункт **Advanced Features**

- В контекстном меню домена выберите **Properties**.

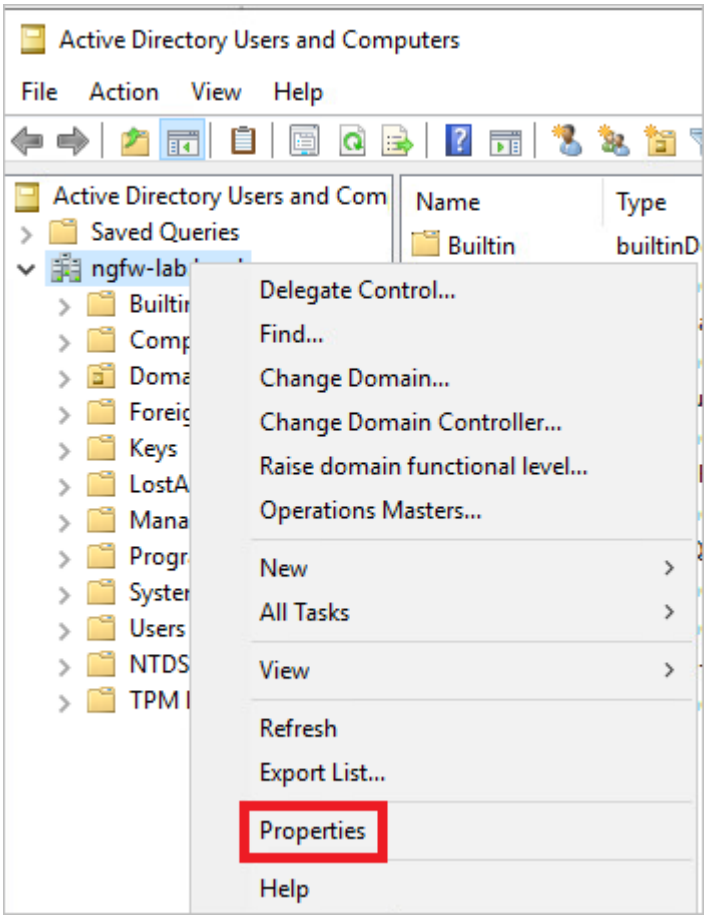


Рисунок 202. Выбор параметров домена

- На вкладке **Security** нажмите **Advanced**.

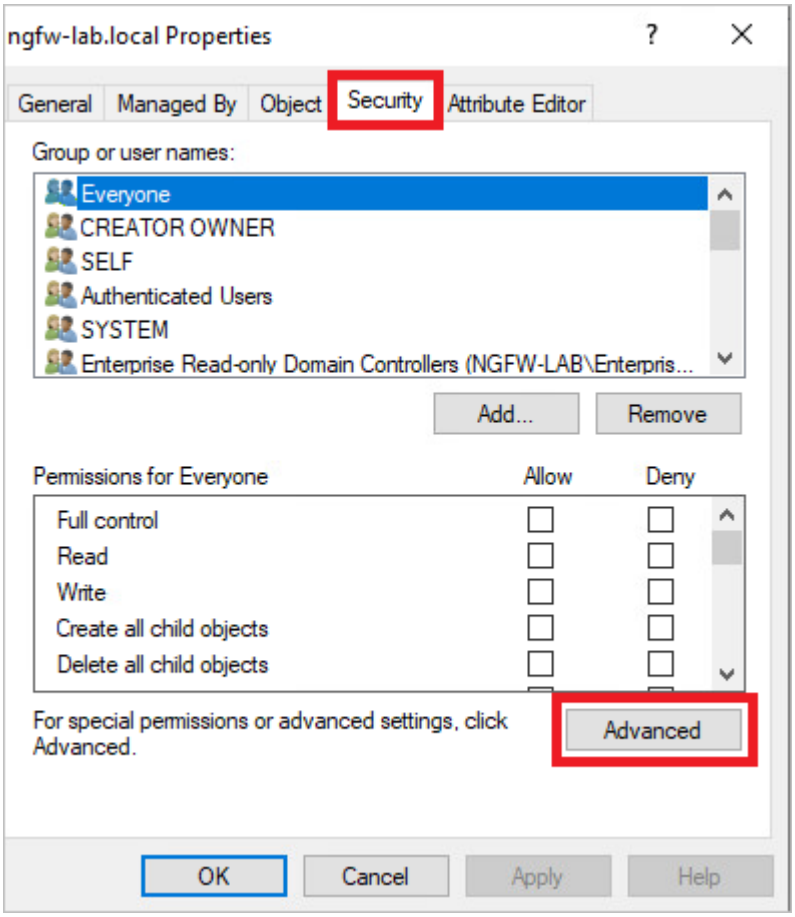


Рисунок 203. Переход в расширенные параметры вкладки **Security**

- На вкладке **Auditing** нажмите **Add**.

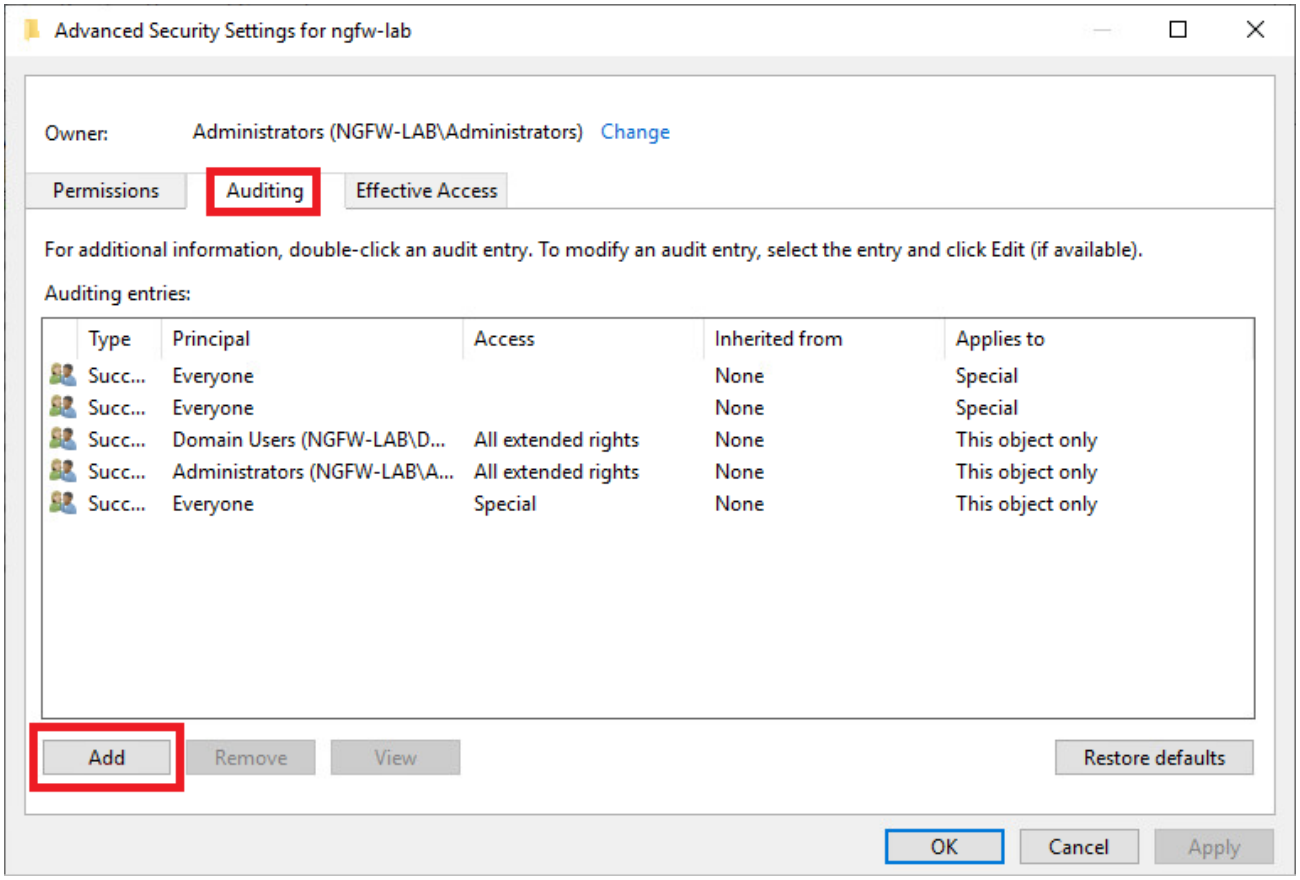


Рисунок 204. Вкладка **Auditing**

- В открывшемся окне перейдите по ссылке **Select Principal**.

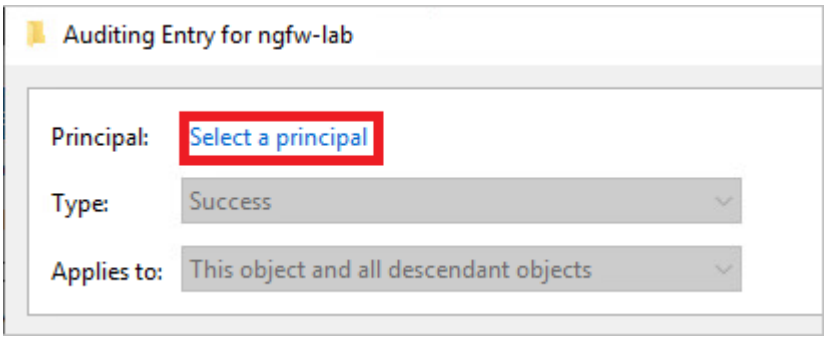


Рисунок 205. Выбор **Select a principal**

- В поле **Enter the object name to select:** введите Everyone и нажмите **OK**.

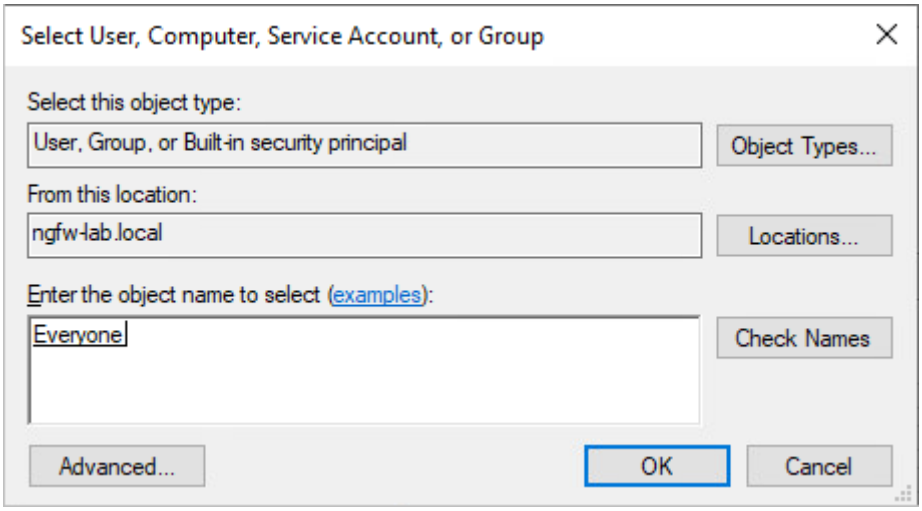


Рисунок 206. Добавление объекта **Everyone**

- В открывшемся окне нажмите **Clear All**.

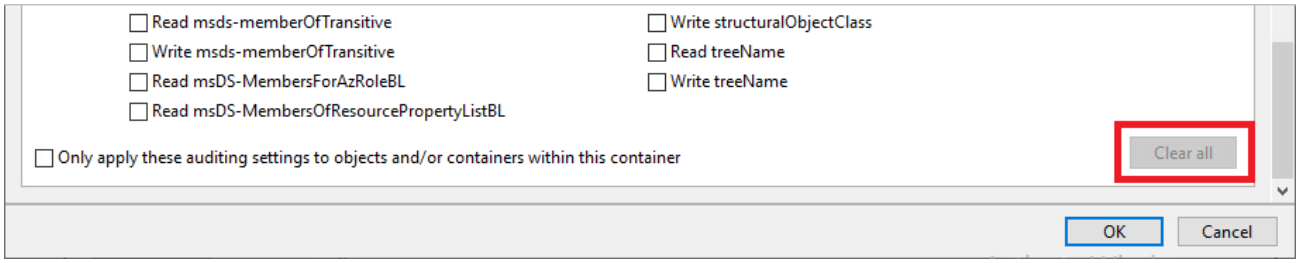


Рисунок 207. Снятие всех флажков по кнопке **Clear All**

- Установите флажки **Create User objects** и **Create Group objects**.
- Нажмите **OK**.

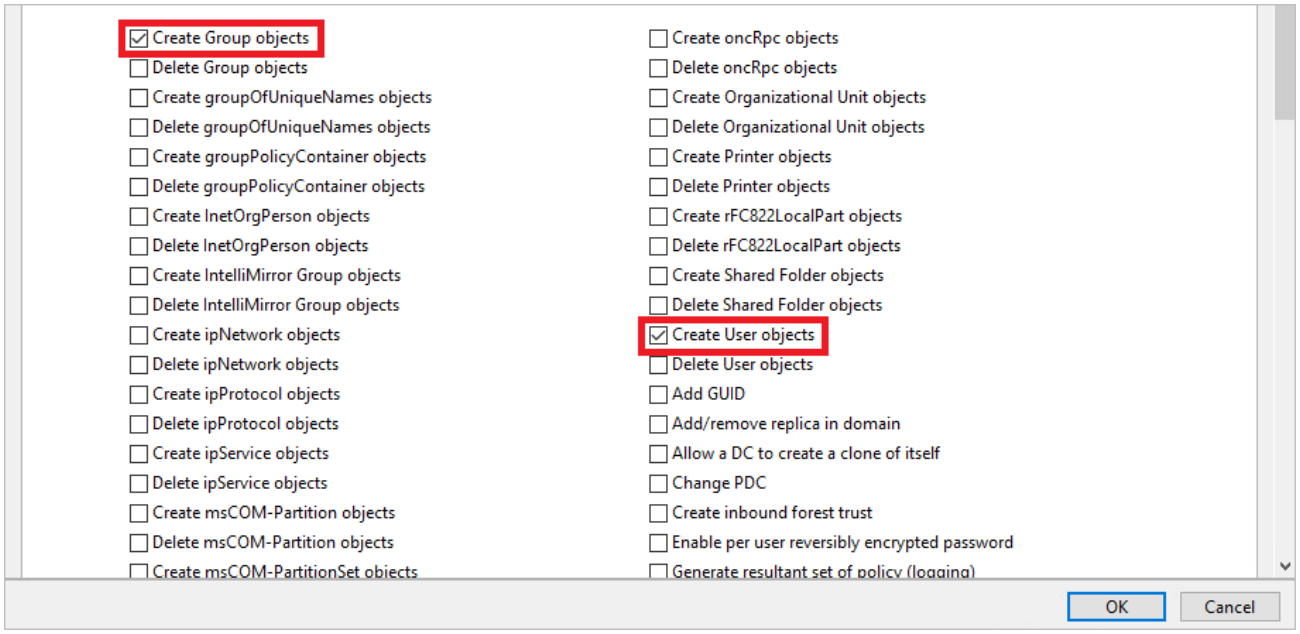


Рисунок 208. Выбор **Create User objects** и **Create Group objects**

- Нажмите **Apply**.

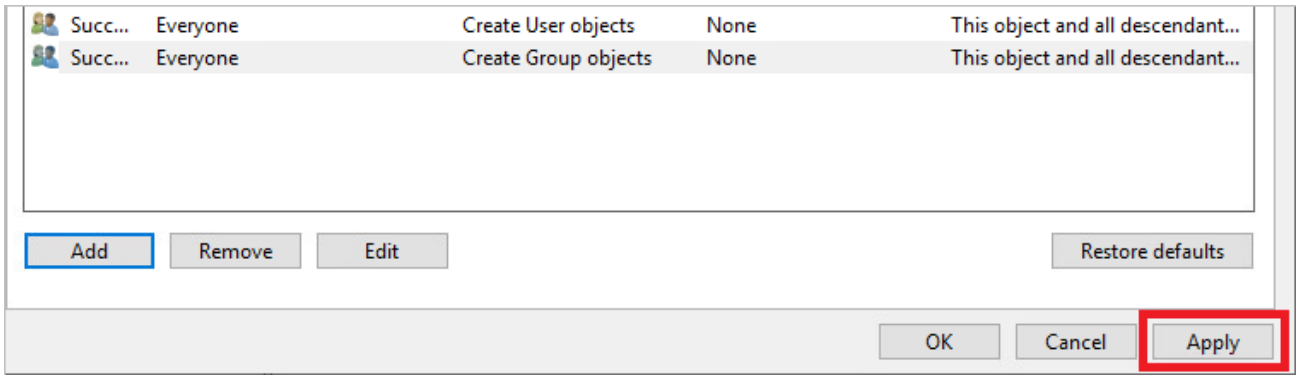


Рисунок 209. Применение параметров

28.4. Настройка агента Identity Control (IDC)

В этом разделе приводятся инструкции по настройке агента Identity Control (IDC).

В этом разделе

Настройка PT NGFW для подключения к агенту (см. раздел 28.4.1)

Настройка агента подключения (на сервере системы управления) (см. раздел 28.4.2)

Настройка RADIUS-серверов в агенте Identity Control (см. раздел 28.4.3)

28.4.1. Настройка PT NGFW для подключения к агенту

- Чтобы настроить PT NGFW для подключения к агенту:

1. В файле конфигурации `/opt/pt-ngfw/ngfw-core/etc/config/pt-ngfw.conf` в блоке `acco` задайте сетевой адрес узла (параметр `address`), на котором находится агент подключения к AD, а также номер порта (параметр `port`).

   По умолчанию это IP-адрес сервера управления и порт 5570.

   Пример:

   ```
   ...
     "acco": {
       "address": "10.13.169.105",
       "port": 5570,
   ...
     },
   ...
   ```

2. После изменения конфигурации перезапустите сервис pt-ngfw-core.service:

   ```
   sudo systemctl restart pt-ngfw-core.service
   ```

28.4.2. Настройка агента подключения (на сервере системы управления)

Внимание! Перед началом настройки убедитесь, что система управления может обратиться к контроллеру домена по FQDN.

- Чтобы настроить агент подключения:

1. Скопируйте сертификат `root` в папку `/opt/pt-ngfw/ngfw-acco-agent/config/certs`

   Например:

   ```
   root@ngfw-mgmt:/opt/pt-ngfw/ngfw-acco-agent/config# cp /home/ngfw/cert/root-CA-lab.crt /
   opt/pt-ngfw/ngfw-acco-agent/config/certs/
   ```

2. Откройте конфигурационный файл `/opt/pt-ngfw/ngfw-acco-agent/config/1/agent.cfg`.

3. В блоках `ldap`, `winrm` и `provider_config` измените следующие параметры:

   - ldap_uri — URL-адрес LDAP-сервера. Поддерживается TLS и StartTLS. Нешифрованные подключения не поддерживаются.
   - cafile — имя (путь) доверенного сертификата агента Identity Control. Путь должен быть относительным — `../certs/cert.pem`.
   - bind_dn — имя пользователя, используемое для аутентификации через операцию bind.
   - bind_pwd — пароль пользователя.

- base_dn — базовый DN, с которого начинается поиск пользователей и групп. Поиск выполняется с областью subtree, то есть, по этому DN и всем его вложенным подразделам. По умолчанию используется корень каталога (root DN). Объекты пользователей, не попавшие в область поиска, обрабатываться не будут. Необязательный параметр.
- filter — фильтр для поиска пользователей. По умолчанию — `sAMAccountType=805306368`. Аналогичен LDAP-фильтру `(&(objectclass=user)(objectclass=person)(!(objectClass=computer)))`.
- timeout_s — тайм-аут LDAP-соединения в секундах.
- ou_support — поддержка использования Organizational Unit в правилах в качестве «псевдогрупп». Сильно увеличивает расход оперативной памяти агентом Identity Control. Не рекомендуется включать. По умолчанию — false.
- winrm_uri — URL-адрес для подключения к службе WinRM.
- user — имя пользователя для аутентификации в WinRM.
- password — пароль пользователя.
- events_read_back_h — время в часах, за которое выполняется чтение информации о прошлых логинах для сопоставления пользователей и IP-адресов. Операция может быть ресурсоемкой на загруженных серверах, поэтому рекомендуется указывать не более шести часов.
- frequency_s — максимальная частота обновления информации в секундах. Параметр контролируется в том числе сервером, поэтому возможны отклонения.
- log_source — имя источника журналов: Security или ForwardedEvents. По умолчанию — Security. Необязательный параметр.

  Пример конфигурационного файла для агента:

```
{
"data_sources": [
    {
      "type": "ad",
      "name": "MS AD",
      "source_config": {
        "ldap": [{
          "ldap_uri": "ldaps://dc-01.rd.pt-ngfw.ru",
          "cafile": "../certs/ca-dc-01.crt",
          "bind_dn": "Administrator@rd.pt-ngfw.ru",
          "bind_pwd": "Qwerty123",
          "base_dn": "OU=DomainObjects,DC=rd,DC=pt-ngfw,DC=ru",
          "filter": "sAMAccountType=805306368",
          "timeout_s": 30,
          "ou_support": false,
          "debug": false,
          "enabled": true
        },
```

```
        {
          "ldap_uri": "ldaps://dc-02.rd.pt-ngfw.ru",
          "cafile": "../certs/ca-dc-02.crt",
          "bind_dn": "Administrator@rd.pt-ngfw.ru",
          "bind_pwd": "Qwerty123",
          "base_dn": "OU=DomainObjects,DC=rd,DC=pt-ngfw,DC=ru",
          "filter": "sAMAccountType=805306368",
          "timeout_s": 30,
          "ou_support": false,
          "debug": false,
          "enabled": true
        }],
        "winrm": [{
          "winrm_uri": "https://dc-01.rd.pt-ngfw.ru:5986/wsman",
          "cafile": "../certs/ca-dc-01.crt",
          "user": "acco@rd.pt-ngfw.ru",
          "password": "Qwerty123",
//        "exclude_filter": ".*\\$$",
//        "exclude_users": [ "user1", "user2" ],
          "events_read_back_h": 0,
          "frequency_s": 30,
          "debug": false,
          "enabled": true,
          "log_source": "Security"
        },
   {
          "winrm_uri": "https://dc-02.rd.pt-ngfw.ru:5986/wsman",
          "cafile": "../certs/ca-dc-02.crt",
          "user": "acco@rd.pt-ngfw.ru",
          "password": "Qwerty123",
//        "exclude_filter": ".*\\$$",
//        "exclude_users": [ "user1", "user2" ],
          "events_read_back_h": 0,
          "frequency_s": 30,
          "debug": false,
          "enabled": true,
          "log_source": "Security"
        }]
      }
    }
  ],
  "data_sources_limit": 10,
  "auth_providers": [
    {
      "name": "ldap_1",
      "type": "ldap",
      "provider_config": {
        "ldap_uri": "ldaps://dc-01.rd.pt-ngfw.ru",
        "cafile": "../certs/ca-dc-01.crt",
```

```
        "bind_timeout_s": 3,
        "debug": false
      }
    }
  ],
  "web_server": {
    "threads": 2,
    "address": "0.0.0.0",
    "port": 4444,
    "session_timeout_sec": 300,
    "server_certificate": "etc/config/certs/web.crt",
    "server_private": "etc/config/certs/web.key",
    "client_certificate": ""
  },
  "acco_server": {
    "address": "0.0.0.0",
    "port": 5570,
    "message_size_soft_limit_kb": 1024,

    // connection parameters
    // "inactivity_timeout_sec": 60,
    // "send_interval_msec": 1000,
    // "socket_send_buffer_size_kb": 8,

    "server_certificate": "etc/config/certs/acco.crt",
    "server_private": "etc/config/certs/acco.key"
  },
  "logger": {
    "name": "common",
    "pattern": "[%Y-%m-%d %T.%f] [%!][%t] [%^%l%$] %v",
    "level": 2,
    "sinks": [
      {
        "type": "console"
      },
      {
        "type": "rotating_logfile",
        "logname": "logs/ngfw_acco_agent.log",
        "max_size": 10000000,
        "files_num": 5
      }
    ]
  }
}
```

Внимание! Убедитесь, что на параметрах `enabled` установлены значения `true`.

```
"enabled": true
```

Примечание. Пример конфигурационного файла для агента Identity Control можно загрузить по ссылке.

4. Если требуется установить тайм-аут действия маппинга «Пользователь — IP-адрес», укажите в секундах значение параметра `user_address_map_timeout_s`.

   Примечание. При значении 0 параметр отключен. Если значение не указано, используется тайм-аут по умолчанию — 86400 секунд (24 часа).

   Примечание. Параметр `user_address_map_timeout_s` может быть полезен в следующих случаях: создание нового маппинга, сброс тайм-аута при получении событий обновления маппинга, удаление маппинга, если в течение заданного тайм-аута не было новых событий обновления маппинга.

   Вы можете установить общий тайм-аут на все источники либо отдельные тайм-ауты на каждый источник, как указано в примерах ниже.

   Общий тайм-аут на все источники:

   ```
   "acco_storage": {
   "user_address_map_timeout_s": 86400
   }
   ```

   Отдельный тайм-аут для источника Captive Portal:

   ```
   "captive_portal": {
   "user_address_map_timeout_s": 86400
   }
   ```

   Отдельный тайм-аут для источника Active Directory:

   ```
   "data_sources": [
      "type": "ad",
   "source_config": {
         ...
         "user_address_map_timeout_s": 86400
       }
     ],
   ```

   Примечание. Параметр, выставленный на отдельных источниках, имеет более высокий приоритет, чем общий параметр.

5. Сохраните изменения и выполните перезапуск агента:

   ```
   sudo systemctl restart pt-ngfw-acco-agent.service
   ```

   Индикатором успешной настройки является сообщение в журнале PT NGFW:

   ```
   ngfw@ngfw-1dp:~$ grep "Policy user" /opt/pt-ngfw/ngfw-core/logs/ngfw.log
   [2024-07-18 09:28:14.119996] [AppConfigurator] [info] Policy user index is successfully
   update
   ```

   Вы также можете настроить уровень журналирования сервиса. Для этого внесите изменения блок `level` в конфигурационном файле агента:

   ```
     "logger": {
       "name": "common",
       "pattern": "[%Y-%m-%d %T.%f] [%!][%t] [%^%l%$] %v",
       "level": 2,
   ```

```
    "sinks": [
      {
        "type": "console"
      }
    ]
  }
}

# уровни логирования:

# 0 - trace, 1 - debug, 2 - info, 3 - warn, 4 - error, 5 - critical, 6 - off
```

28.4.3. Настройка RADIUS-серверов в агенте Identity Control

В агенте Identity Control поддерживается настройка RADIUS-серверов для выполнения аутентификации пользователей. Параметры доступа к RADIUS-серверам задаются в конфигурационном файле агента `agent.cfg` для двух основных сценариев: аутентификации администраторов системы управления и аутентификации пользователей Remote Access VPN.

Аутентификация администраторов СУ

В блоке `auth_providers` определяются параметры доступа к серверам аутентификации (LDAP и RADIUS), используемым для аутентификации администраторов СУ. Кроме того, конфигурация LDAP используется для аутентификации пользователей Captive Portal.

Ниже представлен пример конфигурации с одним LDAP и одним RADIUS-подключением.

```
"auth_providers": [
  {
    "name": "ldap_1",
    "type": "ldap",
    "provider_config": {
      "ldap_uri": "ldaps://ad.example.local",
      "cafile": "../certs/RootCA.cer",
      "bind_timeout_s": 3,
      "debug": false
    }
  },
  {
    "name": "radius_1",
      "type": "radius",
      "provider_config": {
          "address": "192.168.100.101",
          "nas_identifier": "ngfw_acco_agent",
          "shared_secret": "shared_secret",
          "auth_port": 1812,
```

```
            "response_timeout_s": 120,
            "max_retries": 1
        }
    }
```

Описание параметров:

— `name` — имя сервера. Используется при журналировании.

— `type` — тип провайдера. Допустимые значения: `ldap` и `radius`.

— `provider_config` — набор параметров, специфичный для выбранного типа провайдера. Состав параметров зависит от значения `type`.

- При указании типа провайдера `ldap`:
  - `ldap_uri` — URI сервера;
  - `cafile` — путь к сертификату;
  - `bind_timeout_s` — тайм-аут ожидания ответа;
- При указании типа провайдера `radius`:
  - `address` — IP-адрес RADIUS-сервера. Обязательный параметр.
  - `nas_identifier` — идентификатор, используемый RADIUS-сервером для определения клиента, от которого поступает запрос. По умолчанию — `ngfw_acco_agent`.
  - `shared_secret` — значение общего секрета между NAS и RADIUS-сервером, используемого для защиты передаваемых данных. Должен совпадать с секретом, настроенным на RADIUS-сервере. Обязательный параметр.
  - `auth_port` — порт RADIUS-сервера, на который агент отправляет запросы аутентификации (Access-Request). По умолчанию — `1812`.
  - `response_timeout_s` — время ожидания ответа от RADIUS-сервера в секундах. При истечении тайм-аута выполняется попытка авторизации на следующем RADIUS-сервере. По умолчанию — `120`.
  - `max_retries` — максимальное количество повторных попыток авторизации на сервере, если сервер не отвечает. По умолчанию — `1`.

Профили серверов аутентификации

В блоке `auth_server_profiles` определяются параметры доступа к RADIUS-серверам, используемым для аутентификации пользователей Remote Access VPN.

Пример:

```
"auth_server_profiles": [
    {
      "type": "radius",
      "servers": [
        {
```

```
            "address": "192.168.100.101",
            "nas_identifier": "ngfw_acco_agent",
            "shared_secret": "shared_secret",
            "auth_port": 1812,
            "acco_port": 1813,
            "response_timeout_s": 5,
            "max_retries": 5
          }
        ]
      },
    ]
```

Описание параметров:

— `type` — тип профиля сервера аутентификации. Допустимое значение — `radius`.

— `servers` — набор параметров доступа к RADIUS-серверу. В рамках одного профиля поддерживается указание только одного сервера. Параметры доступа:

- `address` — IP-адрес RADIUS-сервера. Обязательный параметр.
- `nas_identifier` — идентификатор, используемый RADIUS-сервером для определения клиента, от которого поступает запрос. По умолчанию — `ngfw_acco_agent`.
- `shared_secret` — значение общего секрета между NAS и RADIUS-сервером, используемого для защиты передаваемых данных. Должен совпадать с секретом, настроенным на RADIUS-сервере. Обязательный параметр.
- `auth_port` — порт RADIUS-сервера, на который агент отправляет запросы аутентификации (Access-Request). По умолчанию — `1812`.
- `acco_port` — номер порта, используемого для отправки сообщений учета сессий. По умолчанию — `1813`.
- `response_timeout_s` — время ожидания ответа от RADIUS-сервера в секундах. По истечении тайм-аута выполняется попытка авторизации на следующем RADIUS-сервере. По умолчанию — `5`.
- `max_retries` — максимальное количество повторных попыток отправки запроса, если сервер не отвечает. По умолчанию — `5`.

28.5. Полезные команды, журналы, статистика

Проверка подключения по LDAP к порту 636 с использованием LDAPS

```
openssl s_client -connect dc-test.ngfw-lab.local:636 -CAfile root-CA-lab.crt
```

```
ngfw@ngfw-mgmt:~/cert$ openssl s_client -connect dc-test.ngfw-lab.local:636 -CAfile root-CA-lab.cr
t
CONNECTED(00000003)
depth=1 C = RU, ST = Some-State, O = Internet Widgits Pty Ltd, CN = ngfw-lab.local
verify return:1
depth=0 C = RU, ST = Some-State, O = Internet Widgits Pty Ltd, CN = DC-Test
verify return:1
---
```

Рисунок 210. Проверка подключения

Просмотр журнала событий

- Чтобы просмотреть журнал событий:

  1. Нажмите Win+R и введите `eventvwr.msc`.
  2. Перейдите в **Application and Services Logs** → **Microsoft** → **Windows** → **WMI-Activity** → **Operational**.

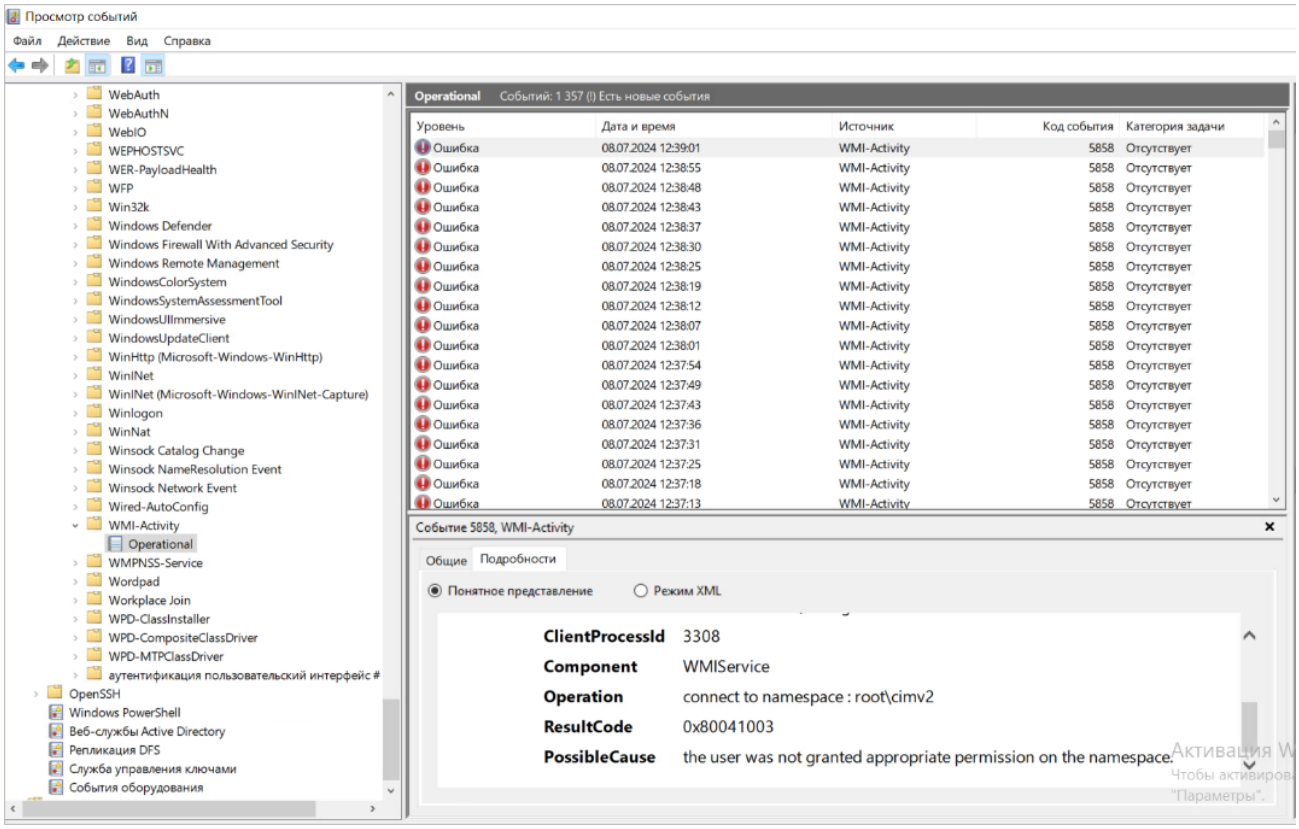


Рисунок 211. Просмотр событий

Статистика работы PT NGFW

```
ngfw@lab-1010:~$ /opt/pt-ngfw/ngfw-core/utils/json2plain_stats.py <(/etc/telegraf/
scripts/stats_to_influx.py https://localhost/stats json) | grep -E "^/acco/" | grep
-v broker
/acco/user_storage_size: 0
```

```
/acco/user_added: 0
/acco/user_removed: 0
/acco/user_update: 0
/acco/group_storage_size: 0
/acco/ipv4_storage_size: 0
/acco/ipv6_storage_size: 0
```

Журнал работы агента

```
root@ngfw-mgmt:~# journalctl -u pt-ngfw-acco-agent.service -e
May 30 08:57:43 ngfw-mgmt pt-ngfw-acco-agent[50834]: > POST /wsman HTTP/2
May 30 08:57:43 ngfw-mgmt pt-ngfw-acco-agent[50834]: Host: DC.ngfwnsk.corp:5986
May 30 08:57:43 ngfw-mgmt pt-ngfw-acco-agent[50834]: authorization: Basic
dXNlcmFnZW50QG5nZnduc2suY29ycDpQMHNpdGl2ZSE=
May 30 08:57:43 ngfw-mgmt pt-ngfw-acco-agent[50834]: accept: */*
May 30 08:57:43 ngfw-mgmt pt-ngfw-acco-agent[50834]: content-type: application/
soap+xml;charset=UTF-8
May 30 08:57:43 ngfw-mgmt pt-ngfw-acco-agent[50834]: user-agent: openwsman 2.2.0
May 30 08:57:43 ngfw-mgmt pt-ngfw-acco-agent[50834]: content-length: 1114
May 30 08:57:43 ngfw-mgmt pt-ngfw-acco-agent[50834]:
May 30 08:57:43 ngfw-mgmt pt-ngfw-acco-agent[50834]: * We are completely uploaded and
fine
May 30 08:58:13 ngfw-mgmt pt-ngfw-acco-agent[50834]: < HTTP/2 200
May 30 08:58:13 ngfw-mgmt pt-ngfw-acco-agent[50834]: < content-type: application/
soap+xml;charset=UTF-8
May 30 08:58:13 ngfw-mgmt pt-ngfw-acco-agent[50834]: < server: Microsoft-HTTPAPI/2.0
May 30 08:58:13 ngfw-mgmt pt-ngfw-acco-agent[50834]: < date: Fri, 30 May 2025
05:58:12 GMT
May 30 08:58:13 ngfw-mgmt pt-ngfw-acco-agent[50834]: < content-length: 739
May 30 08:58:13 ngfw-mgmt pt-ngfw-acco-agent[50834]: <
May 30 08:58:13 ngfw-mgmt pt-ngfw-acco-agent[50834]: * Connection #0 to host
DC.ngfwnsk.corp left intact
May 30 08:58:13 ngfw-mgmt pt-ngfw-acco-agent[50834]: [2025-05-30 05:58:13.451209]
[WsmanClient][8] [info] WsPullRequest got 0 items
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: * Found bundle for host
DC.ngfwnsk.corp: 0x7f3c9c005e80 [can multiplex]
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: * Re-using existing connection!
(#0) with host DC.ngfwnsk.corp
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: * Connected to DC.ngfwnsk.corp
(192.168.216.61) port 5986 (#0)
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: * Server auth using Basic with
user 'useragent@ngfwnsk.corp'
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: * Using Stream ID: d (easy
handle 0x7f3c9c01dfe0)
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: > POST /wsman HTTP/2
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: Host: DC.ngfwnsk.corp:5986
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: authorization: Basic
dXNlcmFnZW50QG5nZnduc2suY29ycDpQMHNpdGl2ZSE=
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: accept: */*
```

```
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: content-type: application/
soap+xml;charset=UTF-8
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: user-agent: openwsman 2.2.0
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: content-length: 1114
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]:
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: * We are completely uploaded and
fine
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <?xml version="1.0"?>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <s:Envelope xmlns:s="http://
www.w3.org/2003/05/soap-envelope" xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/
addressing" xmlns:wsman="http://schemas.dmtf.org/wbe>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <s:Header>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <wsa:Action
s:mustUnderstand="true">http://schemas.xmlsoap.org/ws/2004/09/enumeration/Pull</
wsa:Action>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <wsa:To
s:mustUnderstand="true">https://DC.ngfwnsk.corp:5986/wsman</wsa:To>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <wsman:ResourceURI
s:mustUnderstand="true">http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/*</
wsman:ResourceURI>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <wsa:MessageID
s:mustUnderstand="true">uuid:19928cfd-3654-1654-800b-286383565000</wsa:MessageID>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]:
<wsman:OperationTimeout>PT30.0S</wsman:OperationTimeout>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <wsman:MaxEnvelopeSize>512000</
wsman:MaxEnvelopeSize>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <wsa:ReplyTo>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <wsa:Address>http://
schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous</wsa:Address>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: </wsa:ReplyTo>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: </s:Header>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <s:Body>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <wsen:Pull>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]:
<wsen:EnumerationContext>uuid:D4DB0BE5-4602-4EE2-9C10-4F795166CA98</
wsen:EnumerationContext>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: <wsen:MaxElements>500</
wsen:MaxElements>
May 30 08:58:14 ngfw-mgmt pt-ngfw-acco-agent[50834]: </wsen:Pull>
```

Разное

Агент Identity Control поддерживает LDAPS и StartTLS LDAP.

При подключении через `ldaps://` будет использоваться LDAPS и TCP-порт назначения 636.

При настройке интеграции с AD ошибка при настройке WinRM:

```
WinRM service is already running on this machine.
WSManFault
Message
```

```
ProviderFault
WSManFault
Message = Cannot create a WinRM listener on HTTPS because this machine does not have
an appropriate certificate. To be used for SSL, a certificate must have a CN matching
the hostname, be appropriate for Server Authentication, and not be expired, revoked,
or self-signed.
Error number: -2144108267 0x80338115
Cannot create a WinRM listener on HTTPS because this machine does not have an
appropriate certificate. To be used for SSL, a certificate must have a CN matching
the hostname, be appropriate for Server Authentication, and not be expired, revoked,
or self-signed.
Hostname и CN в сертификате совпадают:
================ Certificate 1 ================
Serial Number: 2a830f1d17b0357bddb8f2dd7893b4546a61b8e4
Issuer: CN=test.local, O=PT, L=Moscow, S=Some-State, C=RU
NotBefore: 14.08.2024 18:04
NotAfter: 11.05.2027 18:04
Subject: CN=winsrv16-ad.test.local, O=Internet Widgits Pty Ltd, S=Some-State, C=AU
Non-root Certificate
Cert Hash(sha1): 25c96c754e369174afddf20a1db72f7f1174e1c0
Key Container = {FFCABE82-1489-4A21-A820-014C644FB769}
Unique container name: 28609504396193deed713bbd32c90396_921feac2-9598-40d0-
ac51-6aebc20c44d1
Provider = Microsoft Enhanced Cryptographic Provider v1.0
Private key is NOT exportable
Encryption test passed
```

Проблема может быть решена через PowerShell с помощью команды:

```
Set-WSManInstance winrm/config/Listener -SelectorSet @{Transport='HTTPS';
Address='*'} -ValueSet @{Hostname="winsrv16-
ad.test.local";CertificateThumbprint="25c96c754e369174afddf20a1db72f7f1174e1c0"}
```

28.6. Настройка подключения к WEC

Настройка подключения агента Identity Control (IDC) к WEC аналогична настройке подключения к контроллеру домена за исключением того, что на текущий момент поддерживаются только локальные учетные записи для WinRM. Способ подключения к LDAP не меняется.

- Чтобы настроить подключение к WEC:

1. Со стороны IDC, в конфигурационном файле укажите CA сертификат, которым подписан сертификат узла WEC, а также укажите журнал, записи которого необходимо читать:

```
"winrm": {
 "winrm_uri": "https://wec.rd.pt-ngfw.ru:5986/wsman",          // HTTPS,WEC
 "cafile": "../certs/ca-dc-01.crt",                            // CA сертификат
 "user": "uagent",                                             // Локальный пользователь W
EC
 "password": "Qwerty123",
```

```
 "events_read_back_h": 2,
 "frequency_s": 30,
 "enabled": true,
//"log_source": "Security"                                    // По умолчанию записи загру
жаются из журнала Security
 "log_source": "ForwardedEvents" // На WEC , по умолчанию все перенаправленные по подписке
 записи помещаются в журнал ForwardedEvents
```

2. Перезапустите сервис:

```
sudo systemctl restart pt-ngfw-acco-agent.service
```

Пример конфигурации WEC-сервера

В рамках этой статьи описывается настройка службы Windows Event Collector. Предполагается, что WEC-сервер состоит в домене и получает записи журналов от машины в домене, в этом случае — от контроллера домена.

Более подробная информация приведена в разделах:

— Настройка подключения к AD (см. раздел 28.3);

— Настройка агента Identity control (IDC) (см. раздел 28.4).

Поскольку IDC не поддерживает типы аутентификации Kerberos и NTLM, используется тип Basic, для которого требуется настроить HTTPS-транспорт, чтобы логин и пароль передавались между агентом Identity Control и WEC в зашифрованном виде.

Требуется выпустить сертификаты для контроллера домена и WEC и подписать их CA-сертификатом, после чего выполнить импорт в хранилище сертификатов Windows (`certlm.msc`).

Процесс выпуска сертификатов описан в рамках статей, указанных выше.

Настройка учетной записи и групп

Поскольку сервер WEC не является контроллером домена, попытка использовать доменную учетную запись в конфигурации агента Identity Control будет приводить к ошибке в журнале сервиса:

```
Internal: Error = 67 (Login denied); user/password wrong or empty.
```

Происходит это потому, что при типе аутентификации Basic поиск учетной записи происходит локально, а не в домене.

Даже если указать учетные данные в формате DOMAIN\\USER, WinRM не распознает домен и будет искать учетную запись локально.

В связи с этим для подключения агента IDC к WinRM будет использоваться локальная учетная запись, а WEC в свою очередь будет использовать доменную учетную запись для подключения к контроллеру домена по WinRM и предоставления своей подписки. Настройка описана в разделе Создание учетной записи сервисного пользователя (см. раздел 28.3.2).

► Чтобы настроить учетную запись:

1. Нажмите Win+R и введите `compmgmt.msc`.
2. В открывшемся окне перейдите в **Local Users and Groups** → **Users**
3. Создайте нового пользователя.

   Примечание. Флажок **User must change password at next logon** должен быть снят.

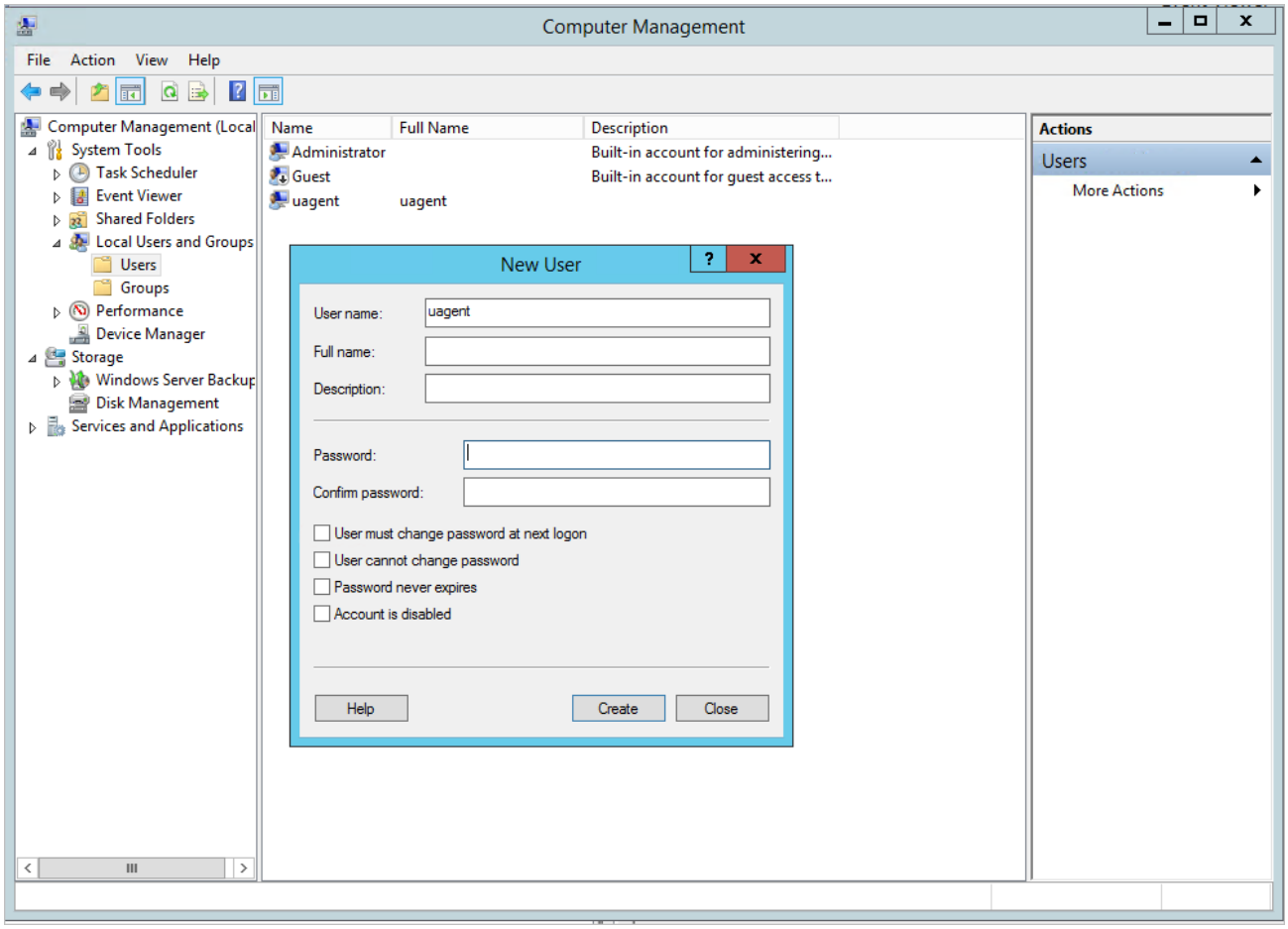


Рисунок 212. Создание локального пользователя

4. Добавьте пользователя в требуемые группы.

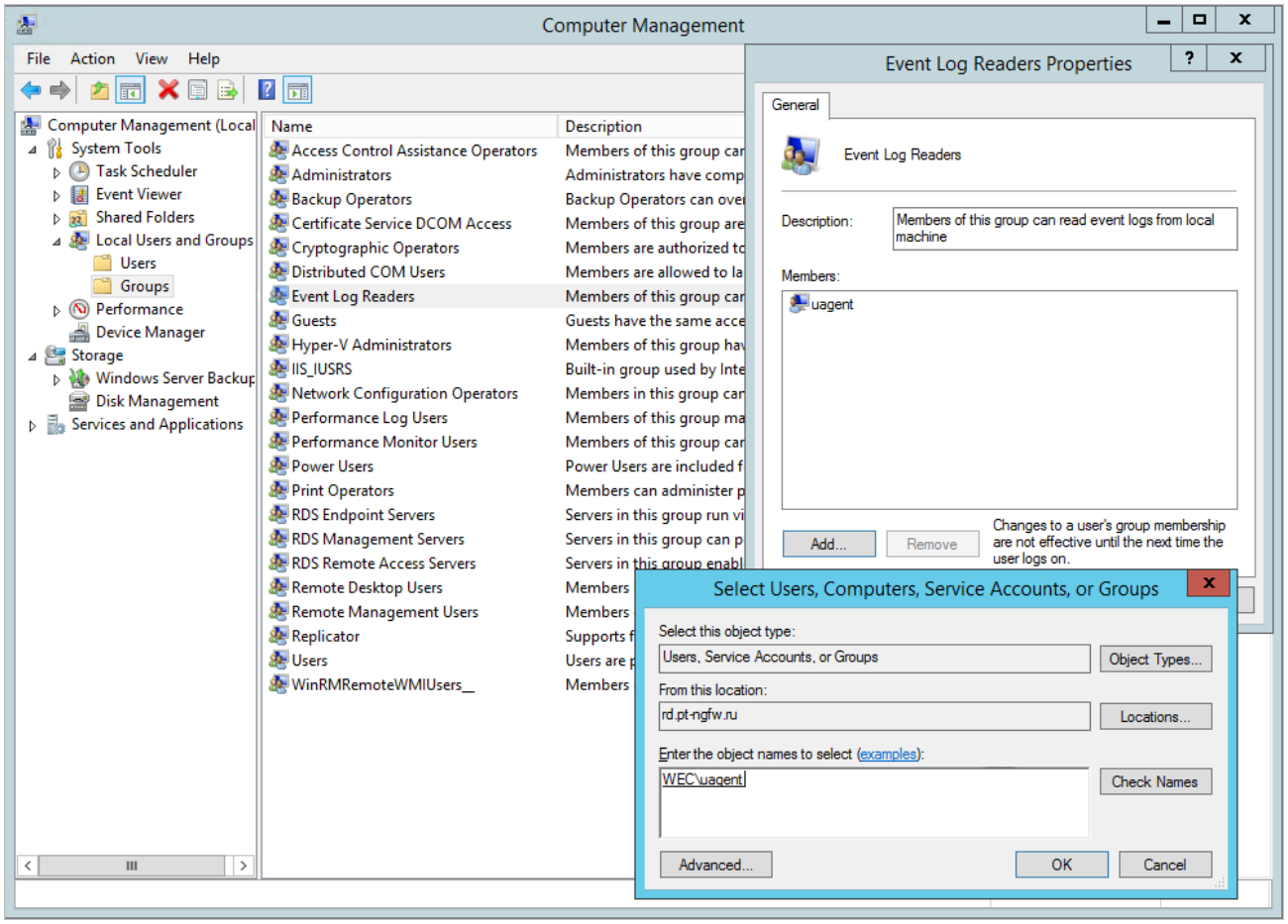


Рисунок 213. Добавление пользователя в требуемые группы

Внимание! В окне выбора имени объекта, который необходимо добавить в группу, поиск происходит в корне доменного дерева, а не в локальном хранилище. Чтобы локальная учетная запись была найдена, нужно либо выбрать путь для поиска вручную, либо к имени пользователя добавить имя компьютера (вместо домена) в формате DOMAIN\NAME.

5. Предоставьте пользователю права на удаленное выполнение WMI запросов.

   Примечание. Если в клиенте IC при попытке подключения к WinRM возникают ошибки **Access Denied**, удостоверьтесь, что права были выданы.

   - Нажмите Win+R и введите `wmimgmt.msc`.
   - В открывшемся окне выберите **WMI Control (Local)** и в контекстном меню перейдите в **Properties**.
   - На вкладке **Security** раскройте список **Root** и выберите папку **CIMV2**.
   - Нажмите кнопку **Security**.
   - Нажмите **Add** для добавления пользователя и добавьте пользователя.
   - В столбце **Allow** установите флажки **Enable Account** и **Remote Enable**.

- Нажмите **OK**.

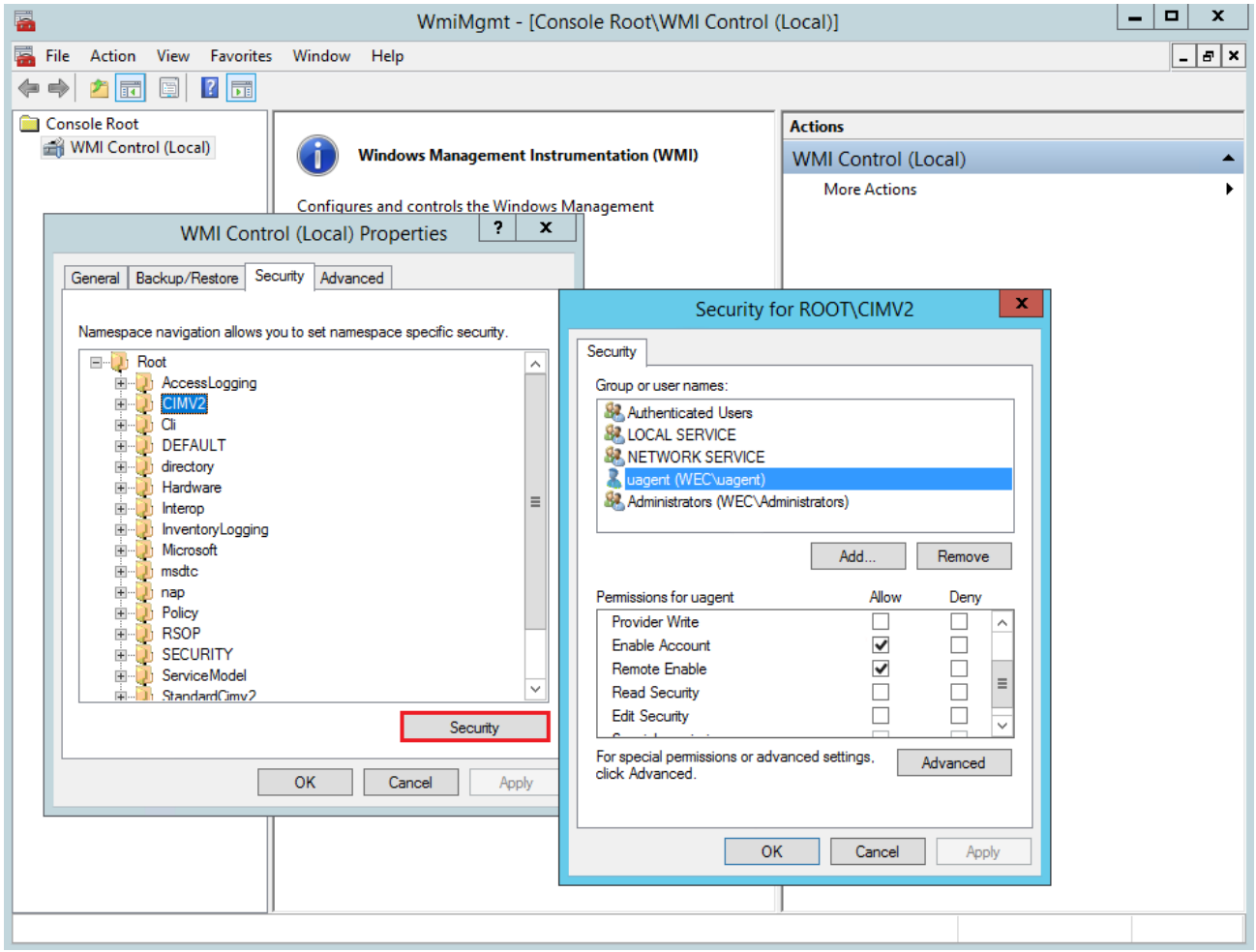


Рисунок 214. Свойства безопасности ROOT/CIMV2

Настройка WinRM

Начиная с версии Windows Server 2008 WinRM включен по умолчанию и прослушивает порт 5985. Проверить список WinRM-прослушивателей можно в командной строке PowerShell или cmd:

```
PS C:\Users\Administrator.RDPTNGFW> winrm enumerate winrm/config/listener
Listener
Address = *
Transport = HTTP
Port = 5985
Hostname
Enabled = true
URLPrefix = wsman
CertificateThumbprint
ListeningOn = 127.0.0.1, 10.16.25.128
```

Необходимо настроить HTTPS-прослушиватель и включить аутентификацию Basic в WinRM. Вам потребуется имя узла и отпечаток сертификата узла, который должен быть подписан CA и добавлен в хранилище сертификатов.

- Чтобы настроить HTTPS-прослушиватель:

  1. Нажмите Win+R и введите `certlm.msc`.
  2. В персональном хранилище найдите сертификат узла, а в нем — имя узла и отпечаток сертификата.

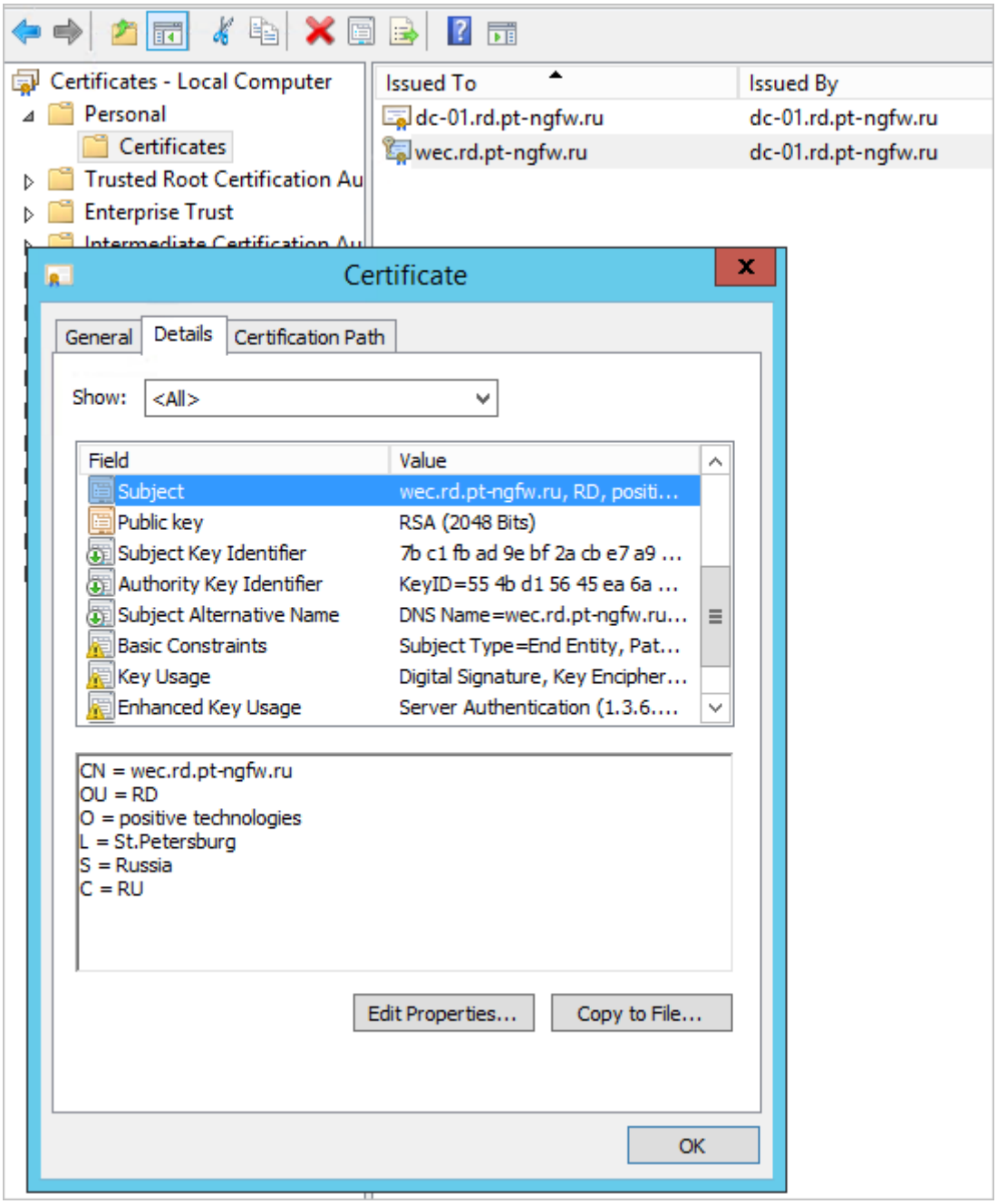


Рисунок 215. Свойства сертификата узла (имя узла)

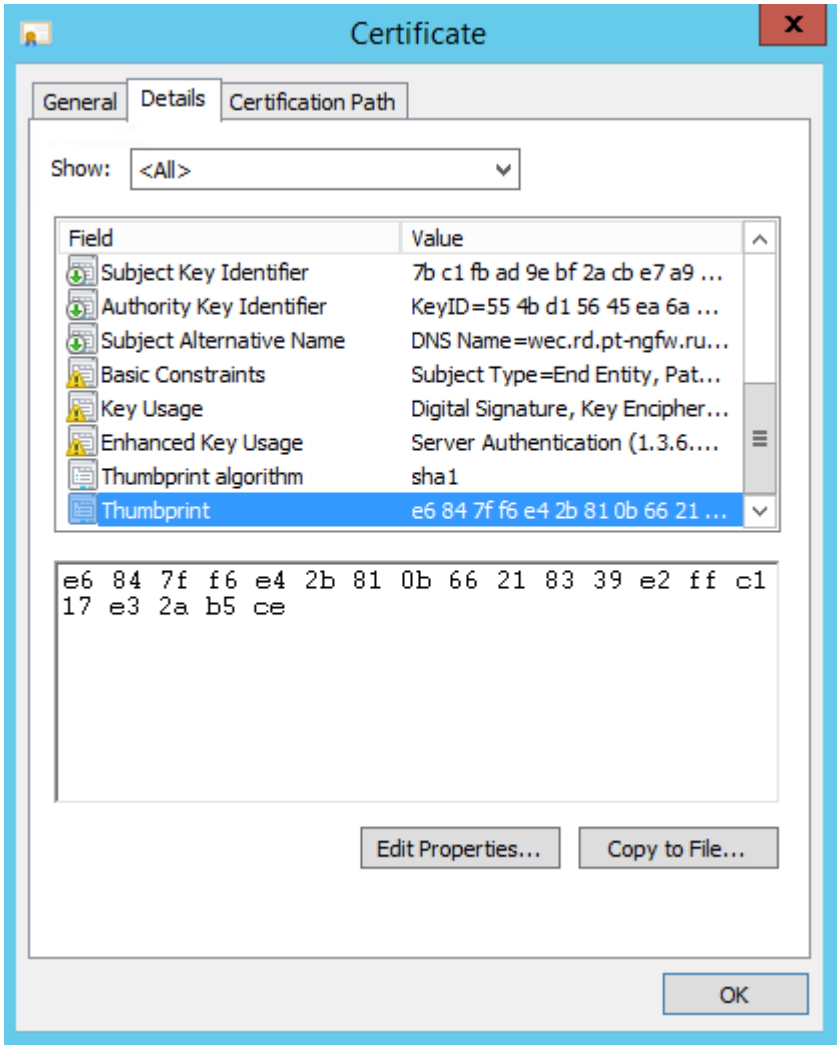


Рисунок 216. Свойства сертификата узла (отпечаток)

3. Добавьте прослушиватель со взятыми из сертификата именем и отпечатком с помощью команды в PowerShell:

```
winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Hostname="HOSTNAME";
CertificateThumbprint="THUMBRPINT"}'
```

4. После добавления проверьте созданный прослушиватель:

```
PS C:\Users\Administrator.RDPTNGFW> winrm enumerate winrm/config/listener
Listener
Address = *
Transport = HTTP
Port = 5985
Hostname
Enabled = true
URLPrefix = wsman
CertificateThumbprint
ListeningOn = 127.0.0.1, 172.16.255.128,
Listener
```

```
Address = *
Transport = HTTPS
Port = 5986
Hostname = wec.rd.pt-ngfw.ru
Enabled = true
URLPrefix = wsman
CertificateThumbprint = e6847ff6e42b810b66218339e2ffc117e32ab5ce
ListeningOn = 127.0.0.1, 10.16.25.128
```

5. Включите basic auth, если нужно для Linux-агента:
   ```
   winrm set winrm/config/service/auth @{Basic="true"}
   ```
6. Разрешите доступ с учетных записей, не входящих в домен (для локальной учетной записи):
   ```
   winrm set winrm/config/service @{AllowUnencrypted="true"}
   ```

Настройка WEC

Для корректной работы Windows Event Collector (WEC) обязательным условием является включенный брандмауэр и наличие правил, разрешающих доступ к служебным портам. Затем требуется включить функции WEC и настроить подписку, которую сервер будет распространять.

Распространение подписки может происходить двумя способами:

1. «Инициировано сборщиком» (**Collector initiated**)

   При использовании этого типа подписки WEC сервер сам будет подключаться к целевой машине и предоставлять подписку.

   Этот тип подписки работает только между машинами, которые находятся в домене. Также этот метод не позволят добавить сразу группу устройств, то есть источники журналов нельзя добавлять группой.

2. «Инициировано исходным компьютером» (**Source computer initiated**)

   При использовании этого типа подписки источники (компьютер или группа) сами перенаправляют события на WEC-сервер.

   Этот тип подписки позволяет получать информацию о событиях, происходящих на машинах как внутри домена, так и за его пределами.

В этой инструкции используется первый способ подписки.

- Чтобы настроить брандмауэр:

  1. Нажмите Win+R и введите `firewall.cpl`.
  2. В открывшемся окне перейдите на вкладку **Включение и отключение Защитника Windows** и включите брандмауэр.

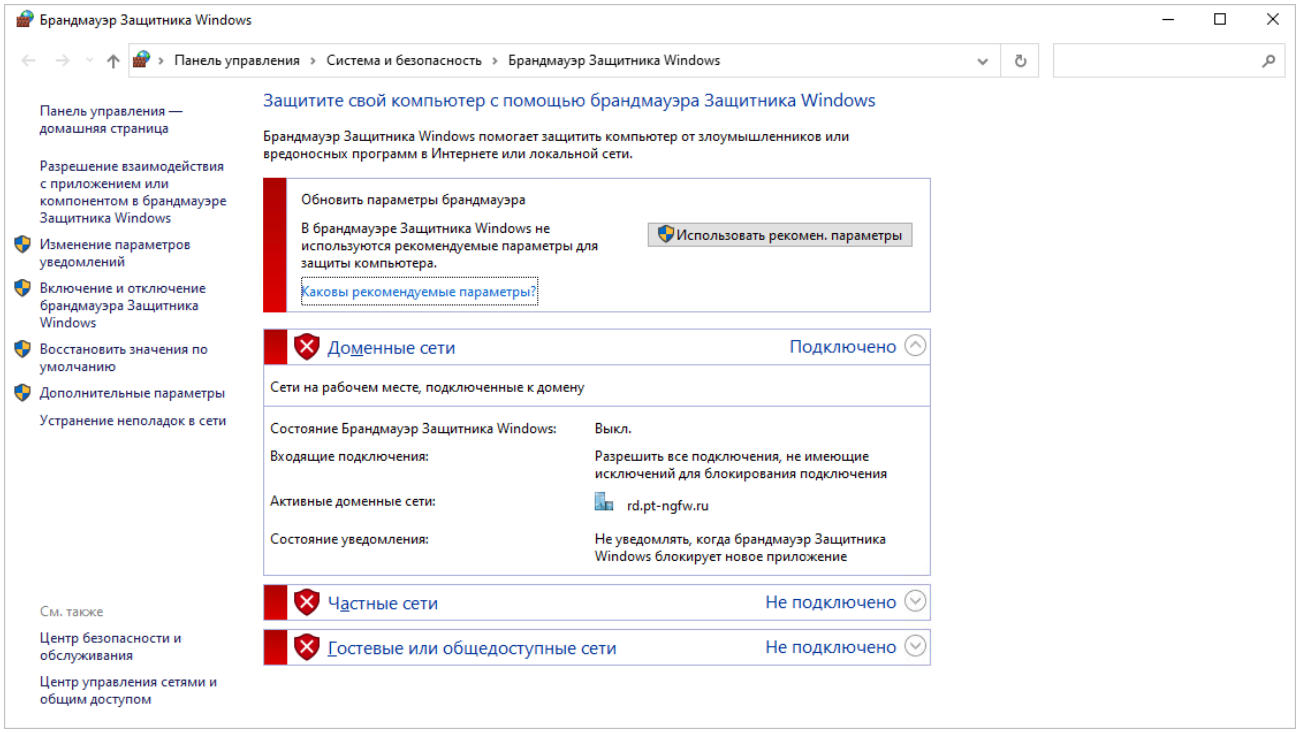


Рисунок 217. Конфигурация брандмауэра

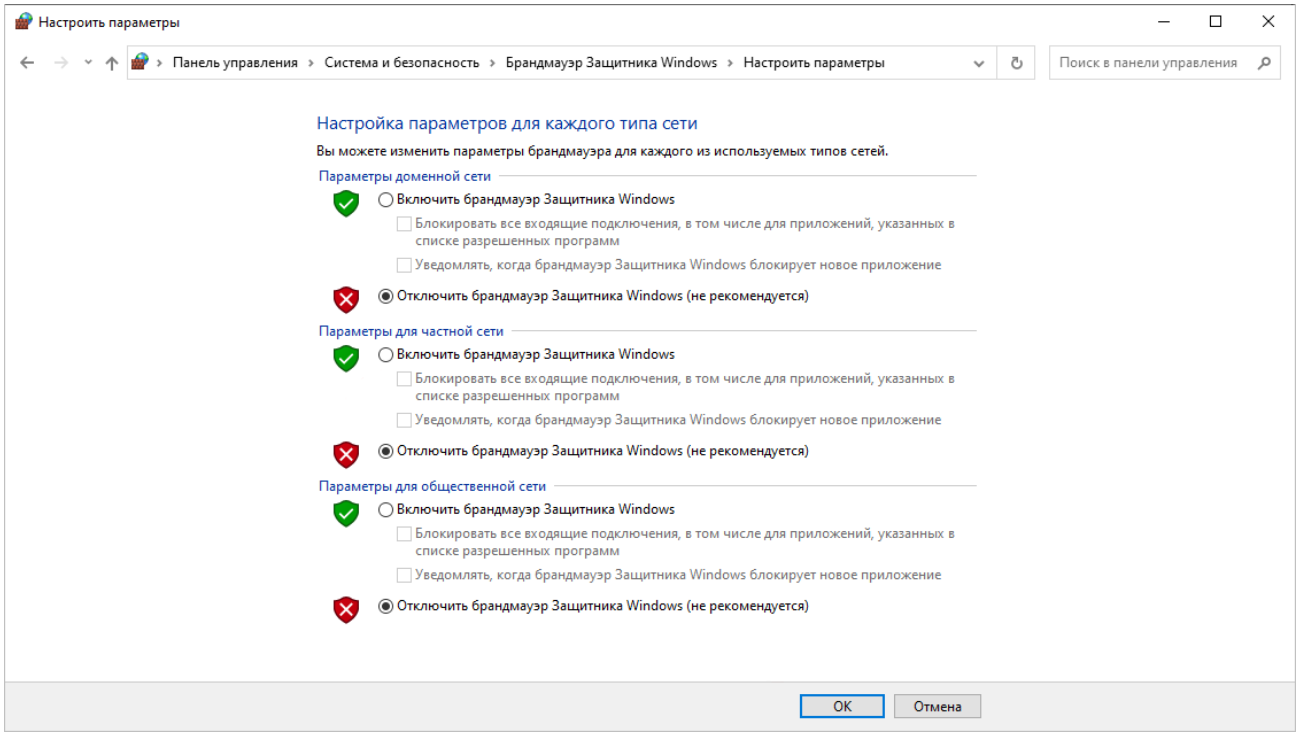


Рисунок 218. Настройка параметров для каждого типа сети

3. Перейдите обратно в **Брандмауэр Защитника Windows** (`firewall.cpl`) → **Дополнительные параметры** для создания разрешающих правил для служб WinRM и Windows Event Collector.

   Примечание. WinRM требует, как минимум два правила: одно для агента Identity Control (входящие соединения), второе — для клиента WinRM, который будет подключаться к целевой машине для предоставления подписки.

   Примечание. В рамках этой инструкции в качестве примеров сделано по одному правилу для обоих направлений, которые разрешают любой трафик.

4. Выберите направление (входящее или исходящее) и нажмите **Создать правило**.

   - На шаге **Тип правила** выберите **Настраиваемые** и нажмите **Далее**.
   - На шагах **Программа**, **Протокол и порты** и **Область** оставьте все параметры без изменений и нажмите **Далее**.
   - На шаге **Действие** выберите **Разрешить подключение**.
   - На шагах **Профиль** и **Имя** оставьте все параметры без изменений и нажмите **Далее**.
   - Нажмите **Готово**.

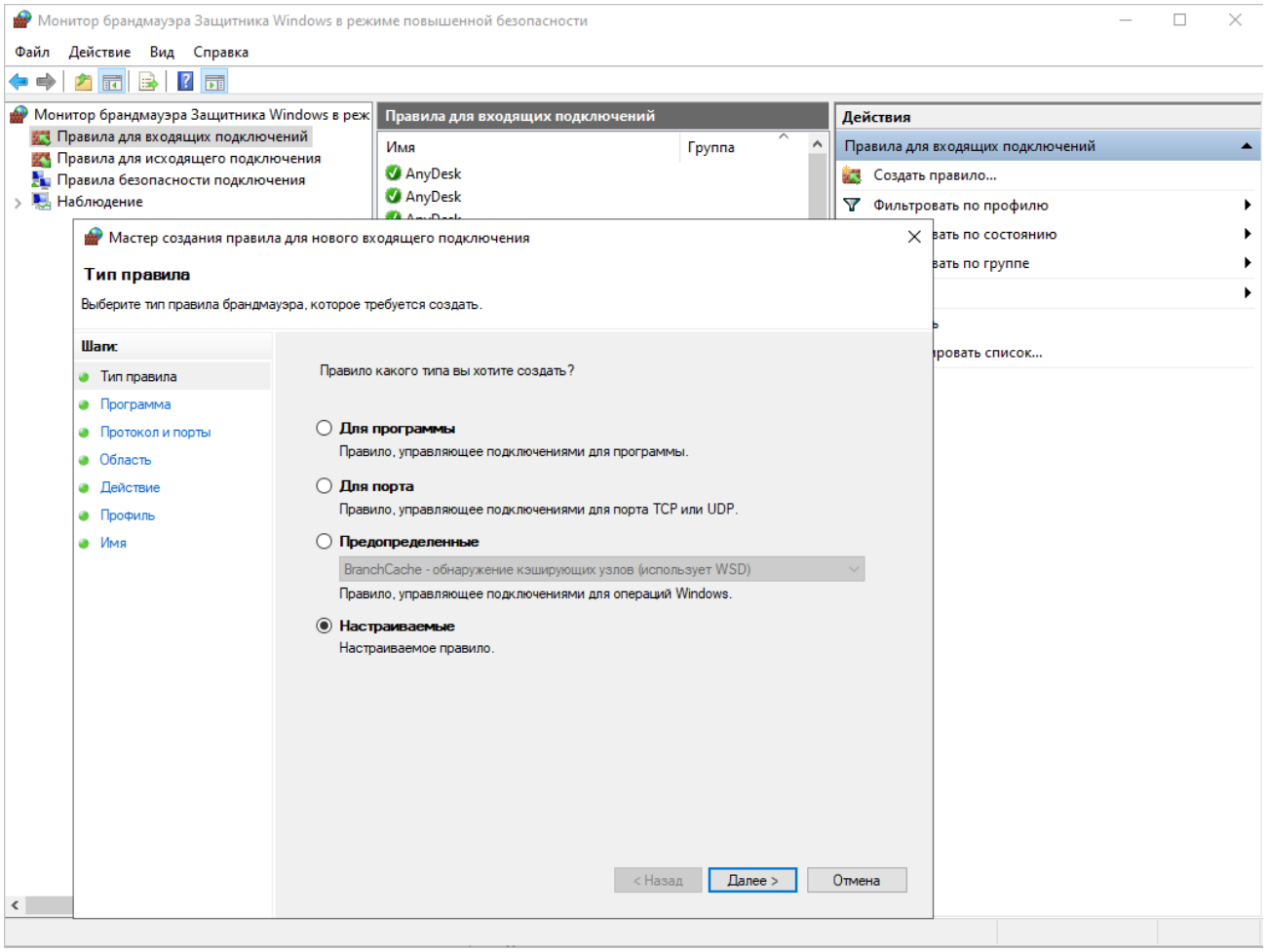


Рисунок 219. Настройка правила для нового входящего подключения

- Чтобы включить WEC и настроить подписку:

  1. Нажмите Win+R и введите `eventvwr.msc`.
  2. Включите WEC (аналог команды `wecutil qc`).

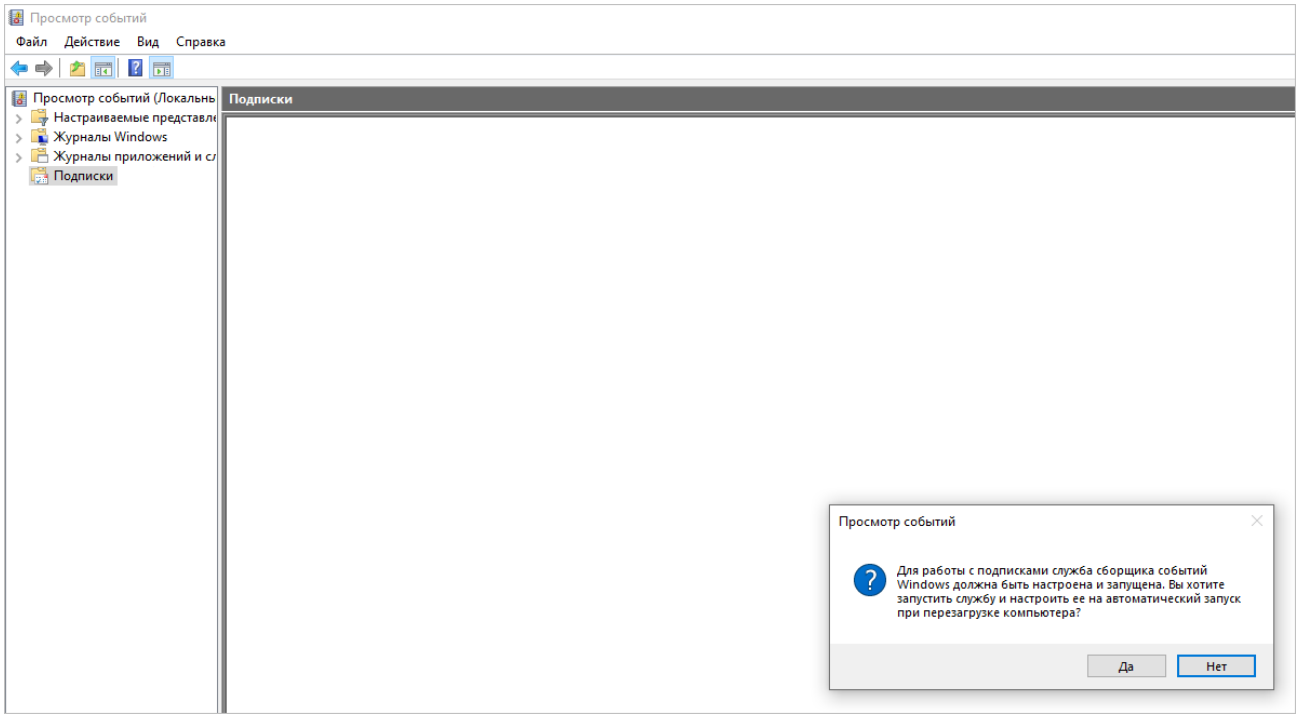


Рисунок 220. Включение WEC

Примечание. Во время включения службы система может работать с задержками. После включения службы в пунтке **Подписки** откроется контекстное меню.

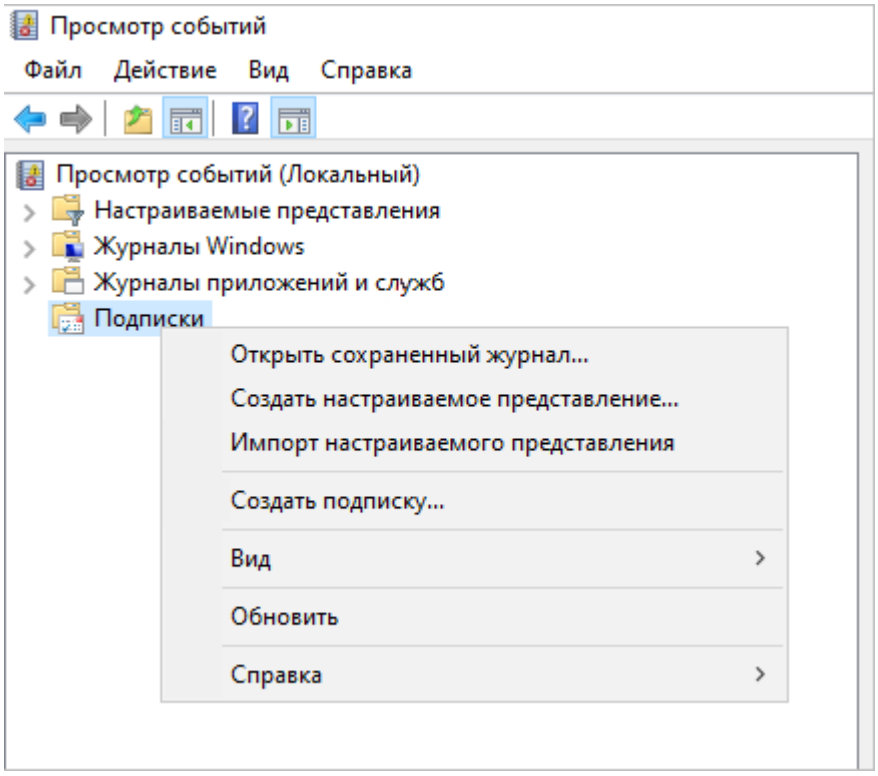


Рисунок 221. Создание подписки

3. В контекстном меню выберите **Создать подписку...**.
4. В открывшемся окне внесите следующие изменения:
   - введите имя подписки (оно будет отображаться в журнале машины, которой эта подписка будет предоставлена);
   - выберите журнал, в который будут попадать перенаправленные события;
   - выберите тип подписки **Инициировано сборщиком**;
   - выберите машины, которым хотите предоставлять подписку;
   - нажмите **Выбрать события** и настройте фильтр, указав, какие события машина должна присылать.

     Примечание. Агент Identity Control обрабатывает события со следующими ID: 4624, 4768, 4769, 4770, 4720, 4726, 4738, 4781, 4727 , 4731, 4754, 4728, 4732, 4756, 4729, 4733, 4757, 4730, 4734, 4758, 5136, 5137, 5139, 5141.
   - нажмите **Дополнительно** и настройте учетную запись, с помощью которой будет происходить подключение к WinRM, а также порт (HTTPS);

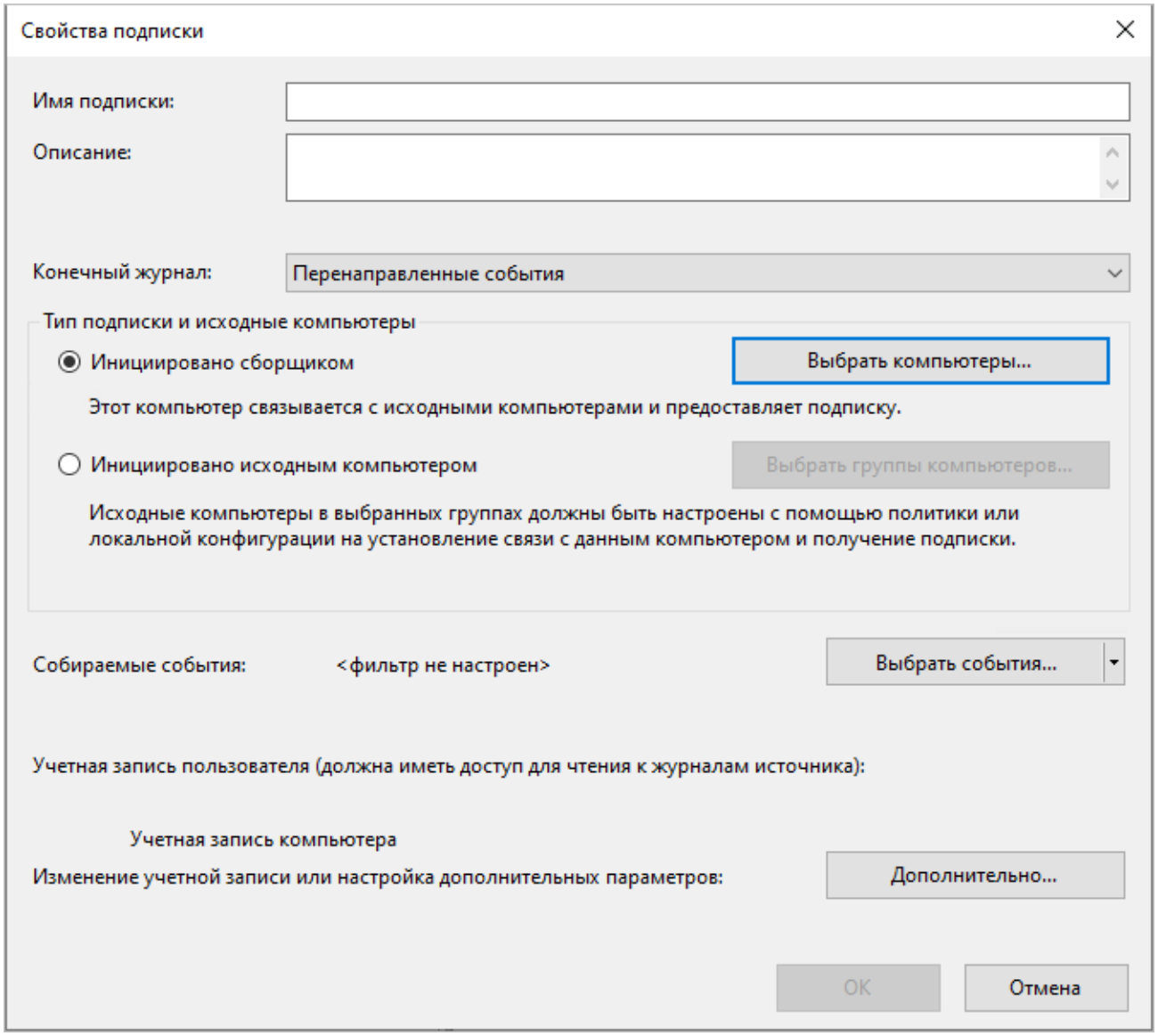


Рисунок 222. Свойства подписки

После создания подписки, ее статус можно проверить в контекстном меню, выбрав пункт **Статус подписки**.

При работающей подписке ее статус будет **Активна**, а в случае ошибки — справа от статуса появится сообщение с подробностями.

Журналы и события

Местоположение журналов служб в Event Viewer (`eventvwr.msc`):

1. Security:

Журналы Windows → **Безопасность** (в том числе для проверки сообщений если агент Identity Control не подключается к WinRM)

2. WinRM:

   Журналы приложений и служб → **Windows** → **Windows Remote Management**

3. Windows Event Collector:

   Журналы приложений и служб → **Windows** → **Eventlog-ForwardingPlugin**

   В этом журнале можно проверить статус и имя подписки.

   Внимание! Если журнал не работает или при открытии журнала возникают ошибки — плагин не работает. Ошибки могут возникать из-за выключенного брандмауэра либо из-за отсутствия обновлений на только что развернутом сервере.

Разное:

Полезные ссылки по настройке WEC:

— Windows Event Collector;

— Сборка и отправка событий Windows с клиента на сервер используя WEC;

— Порты, используемые WinRM по умолчанию, и их изменение.

Схема стенда

На схеме ниже показана приблизительная конфигурация стенда для подключения к WEC

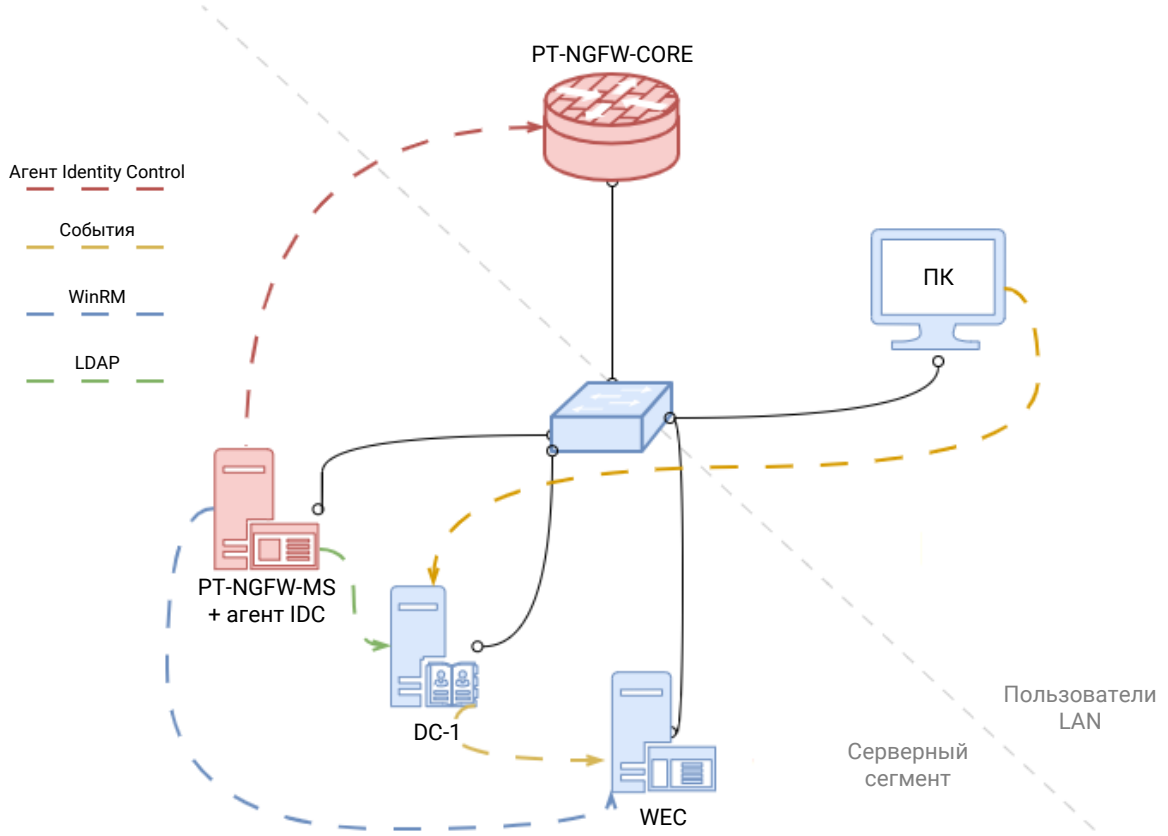


Рисунок 223. Приблизительная схема стенда

28.7. Пример настройки нескольких подключений LDAP и WinRM

Ниже приведен пример конфигурации одного источника данных с несколькими подключениями LDAP и WinRM. Особенности и ограничения такой конфигурации:

— Подключения LDAP работают по принципу резервирования — в источнике данных одновременно используется только одно подключение LDAP из списка, и при его отказе происходит переключение на следующее подключение в списке. Количество подключений не ограничено.

— Максимальное количество подключений WinRM на все источники данных — 255.

— Можно одновременно настроить подключения WinRM для разных типов журналов (например, два подключения WEC и два подключения AD).

— Данные о событиях AD и WEC собираются одновременно со всех настроенных подключений WinRM. Данные о событиях в разных подключениях WinRM одного источника не должны дублироваться.

— Для одного домена можно добавить только один источник данных Active Directory.

```
{
    "type": "ad",
    "name": "MS AD",
    "source_config": {
        "ldap": [
                {
                        "ldap_uri": "ldaps://dc1.example.local",
                        "cafile": "../certs/RootCA.cer",
                        "bind_dn": "user@example.local",
                        "bind_pwd": "secretpassword",
                        "base_dn": "dc=example,dc=local",
                        "filter": "sAMAccountType=805306368",
                        "timeout_s": 30,
                        "ou_support": false,
                        "debug": false,
                        "enabled": true
                },
                {
                        "ldap_uri": "ldaps://dc2.example.local",
                        "cafile": "../certs/RootCA.cer",
                        "bind_dn": "user@example.local",
                        "bind_pwd": "secretpassword",
                        "base_dn": "dc=example,dc=local",
                        "filter": "sAMAccountType=805306368",
                        "timeout_s": 30,
                        "ou_support": false,
                        "debug": false,
                        "enabled": true
                }
                ],
        "winrm": [
                {
                        "winrm_uri": "https://dc1.example.local:5986/wsman",
                        "cafile": "../certs/RootCA.cer",
                        "user": "user@example.local",
                        "password": "secretpassword",
                        "events_read_back_h": 2,
                        "frequency_s": 30,
                        "debug": false,
                        "enabled": true,
                        "log_source": "Security"
```

```
                },
                {
                        "winrm_uri": "https://dc2.example.local:5986/wsman",
                        "cafile": "../certs/RootCA.cer",
                        "user": "user@example.local",
                        "password": "secretpassword",
                        "events_read_back_h": 2,
                        "frequency_s": 30,
                        "debug": false,
                        "enabled": true,
                        "log_source": "Security"
                }
                ]
    }
}
```

Примечание. Пример конфигурационного файла для агента Identity Control можно загрузить по ссылке.

29. Captive Portal

В состав PT NGFW входит служба Captive Portal предназначенная для аутентификации и контроля доступа пользователей сети. С помощью Captive Portal вы можете организовать гостевой доступ в сеть, а также настраивать политики безопасности для устройств, не входящих в домен Active Directory.

Трафик неавторизованных пользователей при обращении к веб-ресурсу или сайту перенаправляется на Captive Portal, который возвращает страницу аутентификации.

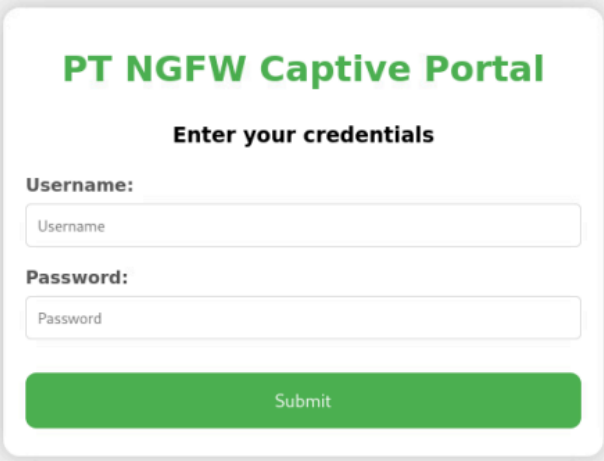


Рисунок 224. Страница аутентификации Captive Portal

После успешной аутентификации доступ к ресурсу будет определяться политиками безопасности PT NGFW.

Порядок аутентификации пользователя

1. Пользователь сети обращается к веб-ресурсу или сайту, при этом он отправляет запрос на DNS-сервер для разрешения доменного имени;
2. PT NGFW перехватывает DNS-запрос и формирует DNS-ответ, в котором доменному имени веб-ресурса сопоставлен IP-адрес Captive Portal;
3. HTTP-запрос пользователя отправляется на IP-адрес Captive Portal, который возвращает страницу аутентификации;
4. Пользователь вводит учетные данные, после чего Captive Portal выполняет его авторизацию в Active Directory по протоколу LDAPs. В случае успешной авторизации на узел передается информация о пользователе Active Directory и его IP-адресе, которая будет использоваться политиками безопасности.

   Внимание! DNS-запросы от пользователей сети должны проходить через узел PT NGFW, при этом IP-адрес Captive Portal должен быть доступен для сетевых узлов, с которых пользователи выполняют аутентификацию.

Настройка Captive Portal

- Чтобы настроить службу аутентификации Captive Portal:

1. Подключитесь к узлу системы управления по SSH.
2. Откройте для редактирования конфигурационный файл `interfaces`:
   ```
   sudo nano /etc/network/interfaces
   ```
3. Настройте дополнительный IP-адрес для работы Captive Portal.

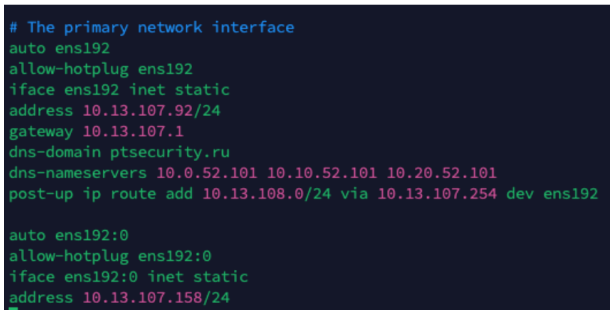


Рисунок 225. Настройка дополнительного адреса

4. Сохраните изменения **Ctrl+O** и закройте файл **Ctrl+X**.
5. Откройте для редактирования конфигурационный файл `traefik.yml`:
   ```
   sudo nano /opt/pt-ngfw/traefik/config/traefik.yml
   ```
6. Настройте точку входа для Captive Portal, используя выделенный ранее IP-адрес. Для этого добавьте в файл `traefik.yml` секции `captive-http` и `captive-https`:
   ```
   captive-http:
   address: <IP-адрес>:80
   transport:
   respondingtimeouts:
   idletimeout: 5m
   forwardedHeaders:
   trustedips:
   - 127.0.0.0/8
   - 10.0.0.0/8
   - 172.16.0.0/12
   - 192.168.0.0/16
   http:
   redirections:
   entrypoint:
   to: captive-https
   scheme: https
   captive-https:
   address: <IP-адрес>:443
   forwardedHeaders:
   trustedips:
   - 127.0.0.0/8
   ```

```
- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
http: tls: {}
```

, где `<IP-адрес>` — адрес, выделенный для работы Captive Portal.

7. Сохраните изменения **Ctrl+O** и закройте файл **Ctrl+X**.
8. Перезапустите службу traefik:
   ```
   sudo systemctl restart pt-ngfw-traefik.service
   ```
9. Подключитесь к веб-интерфейсу системы управления.
10. Создайте адресный объект Captive Portal: **Объекты** → **Адреса** → **Добавить**.
11. В поле **Название** введите название адресного объекта, например, `Captive_Portal`.
12. На вкладке **IP-адрес** введите в IP-адрес, выделенный для работы Captive Portal в формате `<IP-адрес>/32`.

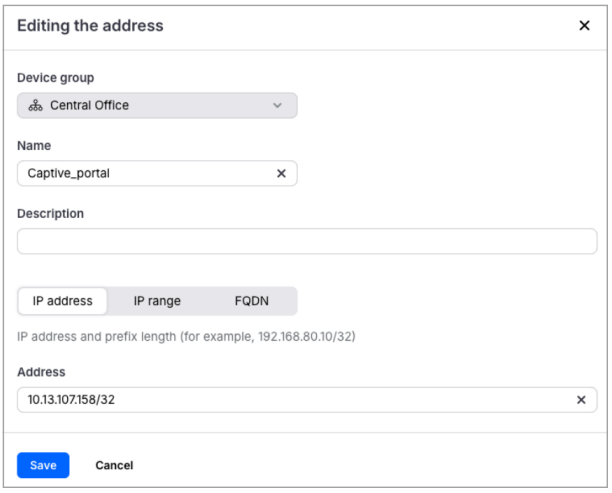


Рисунок 226. Добавление адресного объекта для Captive Portal

13. Нажмите **Сохранить**.
14. Создайте профиль аутентификации Captive Portal: **Объекты** → **Профили аутентификации** → **Добавить**.

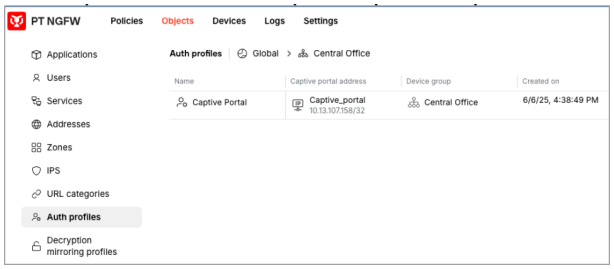


Рисунок 227. Добавление профиля аутентификации

15. В списке **Адрес портала аутентификации** выберите созданный ранее адресный объект `Captive_Portal`.
16. Нажмите **Сохранить**.
17. Для сетевых узлов, которым необходима аутентификация, создайте правила аутентификации (см. раздел 16), используя созданный профиль аутентификации.
18. Обеспечьте сетевую доступность к Captive Portal для сетевых узлов, которым необходима аутентификация. При необходимости создайте разрешающие политики безопасности.
19. Создайте правило аутентификации, разрешающее доступ к IP-адресу Captive Portal со следующими параметрами:
    - **Адрес назначения** — выберите созданный ранее адресный объект.
    - **Сервис** — выберите сервисы **HTTP-default-port** и **HTTPS-default-port**.
    - **Профиль** — выберите **Без аутентификации**.
    - **Режим журналирования** — выберите **При срабатывании правила**.
20. Нажмите **Сохранить**.
21. Нажмите **Отправить на устройство** чтобы разослать конфигурацию на узлы PT NGFW.

Проверка работоспособности Captive Portal

1. На тестовом сетевом узле убедитесь, что в ответ на DNS-запросы возвращается адрес Captive Portal. Для этого вы можете выполнить команду, использующую разрешение доменных имен (например, `ping` или `nslookup`). В выводе команды должен отобразиться IP-адрес, выделенный для Captive Portal.

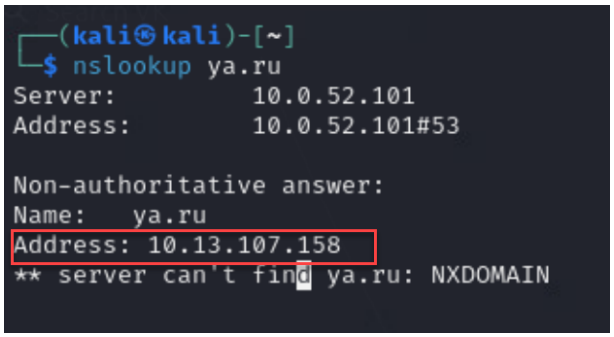


Рисунок 228. Проверка перехвата DNS-запросов с помощью nslookup

2. Откройте тестовый веб-ресурс и убедитесь, что в браузере отображается страница аутентификации Captive Portal.
3. Введите имя пользователя, зарегистрированного в Active Directory, в формате user@domain.local и пароль.

4. После успешной авторизации Captive Portal выводит сообщение **SUCCESS** с указанием IP-адреса авторизованного узла.



Рисунок 229. Сообщение об успешной авторизации

Внимание! Если в сети используется NAT или трафик до Captive Portal попадает под действие политики NAT, изменяющей адрес источника, то выводимый IP-адрес может не соответствовать IP-адресу узла.

5. Если на этапе настройки вы включали регистрацию попыток аутентификации, то проверьте наличие соответствующих записей в журнале событий аутентификации. Для этого подключитесь к системе управления и выберите **Журналы** → **Политика аутентификации**.

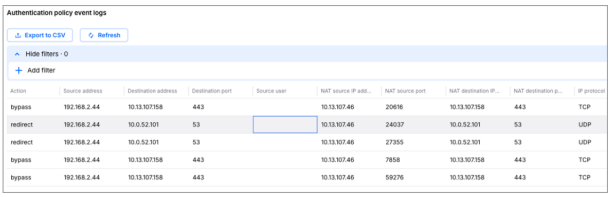


Рисунок 230. Журнал событий аутентификации

При попытке аутентификации в журнале регистрируются две записи:

— пропущенный трафик в сторону Captive Portal (значение **bypass** в столбце **Action**);

— трафик, перенаправленный в интернет в соответствии с политиками аутентификации (значение **redirect** в столбце **Action**).

30. Кластер межсетевого экрана

PT NGFW поддерживает работу в режиме кластера, состоящего из двух межсетевых экранов, типа «активный — резервный» (active-standby, или A/S). Такой кластер также называется отказоустойчивой парой (High Availability, или HA).

В A/S-кластере активное устройство обрабатывает транзитный трафик пользователей, а резервное находится в состоянии готовности начать его обработку. Активное устройство синхронизирует с резервным информацию об обрабатываемом трафике. Устройства имеют одинаковые параметры конфигурации и обмениваются друг с другом информацией о своем текущем состоянии. В случае отказа активного устройства второе берет на себя обработку всего трафика.

Так как межсетевой экран — это устройство, которое обрабатывает сетевой трафик с отслеживанием состояния сессий (stateful), он проверяет, что сессия корректно начинается (это относится к TCP-трафику, в частности — к TCP-рукопожатию), и только в этом случае вносит информацию о сессии в свою таблицу сессий. Если межсетевой экран получает пакеты сессии, о которой у него нет информации (он не зафиксировал TCP-рукопожатие), или если нарушены параметры сессии, то такие пакеты отбрасываются. В этой связи важно, чтобы на резервном устройстве кластера информация о сессиях совпадала с информацией на активном устройстве. В противном случае, когда произойдет переключение кластера и резервное устройство станет активным, оно начнет сбрасывать трафик существующих сессий.

Основное отличие резервирования межсетевых экранов от, например, резервирования коммутаторов или маршрутизаторов в том, что межсетевым экранам необходимо обмениваться друг с другом служебными данными об обрабатываемом трафике и синхронизировать значительно больший объем информации, чтобы при отказе одного из устройств пользовательские сессии, которые им обрабатывались, не прервались после того, как пересылка их трафика продолжилась новым активным межсетевым экраном.

Устройства A/S-кластера синхронизируют друг с другом данные о трафике, конфигурации, а также обмениваются диагностической информацией, чтобы оперативно принимать решение о необходимости переключения, если на соседнем устройстве происходит какой-либо сбой. Для обмена информацией межсетевые экраны кластера соединяются через специальный канал синхронизации — Sync-link. Sync-link — это маршрутизируемое соединение двух узлов, формирующих кластер. Для его создания используются выделенные интерфейсы, работающие в пространстве базовой операционной системы (Debian, Astra Linux).

Основной тип данных, которыми обмениваются устройства в кластере, — это информация об обрабатываемых сессиях транзитного трафика пользователей. Трафик называется транзитным, так как идет через межсетевой экран из одной сети в другую и (или) обратно, то есть транзитом, а не адресован самому межсетевому экрану.

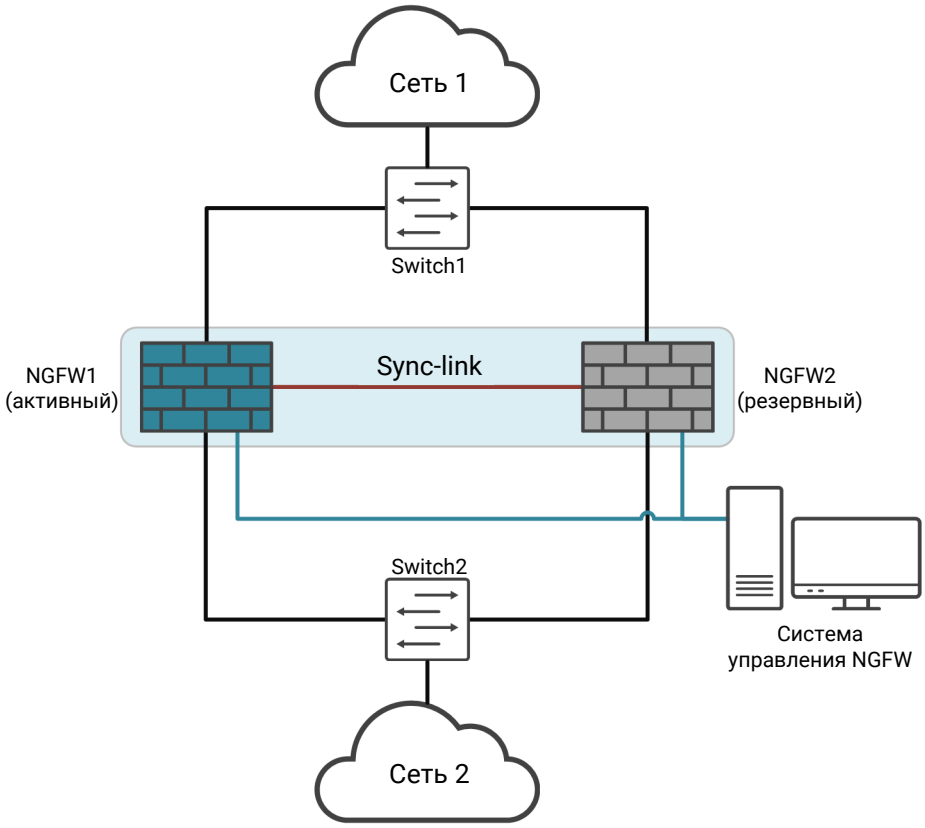


Рисунок 231. Общая схема кластера (отказоустойчивой пары) active-standby

Два устройства, объединенные в кластер, работают, то есть настраиваются и управляются, как единое логическое устройство без необходимости выполнять какую-либо настройку отдельно на каждом из них. Для других сетевых устройств уровня L3 (маршрутизаторы, маршрутизирующие коммутаторы, рабочие станции, серверы) кластер PT NGFW выглядит как одно логическое сетевое устройство, за исключением отдельных пунктов, необходимых для корректной работы некоторых контрольных сетевых протоколов. В режиме vWire кластер PT NGFW выглядит для других сетевых устройств как два пути прохождения трафика, один из которых включен и используется (интерфейсы в состоянии Up), а второй — отключен (интерфейсы в состоянии Down). Это достигается:

— синхронизацией таблиц FIB (forwarding information base);

— синхронизацией конфигурации, которая, среди прочего, обеспечивает неизменность IP-адресов при переключении кластера;

— синхронизацией информации о сессиях и другой информации;

— использованием виртуального MAC-адреса на физических интерфейсах (актуально для сабинтерфейсов, работающих в режиме маршрутизации);

— использованием сообщений Gratuitous ARP (актуально для сабинтерфейсов, работающих в режиме маршрутизации);

— автоматическим переводом интерфейсов резервного узла в выключенное состояние и включением интерфейсов на активном узле (актуально для интерфейсов, имеющих сабинтерфейсы в режиме vWire).

Активное устройство синхронизирует конфигурацию с резервным за исключением параметров базовой ОС.

> **Примечание.** Конфигурация выделенных интерфейсов управления и Sync-link выполняется в пространстве базовой операционной системы (Debian, Astra Linux) и не синхронизируется между устройствами кластера.

> **Примечание.** В PT NGFW поддерживается создание кластера, состоящего из одного устройства. В таком кластере отсутствует возможность резервирования, однако создание такого кластера может требоваться, когда, например, второе устройство будет добавлено в кластер в будущем, а настроить и ввести кластер в эксплуатацию (подготовить и применить кластерную конфигурацию) необходимо уже сейчас.

В этом разделе

Виртуальный MAC-адрес и GARP (см. раздел 30.1)

Работа в виртуальной среде в режиме маршрутизации (см. раздел 30.2)

Режим vWire (см. раздел 30.3)

Приоритет устройств в кластере (см. раздел 30.4)

Приоритетное замещение (Preemption) (см. раздел 30.5)

Graceful restart (OSPF, BGP) (см. раздел 30.6)

Состояния узлов кластера (см. раздел 30.7)

Состояния кластера (см. раздел 30.8)

Состояния конфигурации кластера (см. раздел 30.9)

Требования для создания кластера active-standby (см. раздел 30.10)

Создание кластера (см. раздел 30.11)

Процесс объединения узлов в кластер (см. раздел 30.12)

Изменение параметров кластера (см. раздел 30.13)

Приостановка узла в кластере (Suspend) (см. раздел 30.14)

Мониторинг устройств кластера (см. раздел 30.15)

Split-brain (раскол кластера) (см. раздел 30.16)

Мониторинг интерфейсов кластера (см. раздел 30.17)

Удаление устройств из кластера (см. раздел 30.18)

Добавление устройств в кластер (см. раздел 30.19)

Удаление кластера (см. раздел 30.20)

30.1. Виртуальный MAC-адрес и GARP

Кластер active-standby PT NGFW поддерживает использование виртуального MAC-адреса (vMAC) для сабинтерфейсов, работающих в режиме маршрутизации (уровень L3).

Использование виртуального MAC-адреса имеет следующие преимущества:

— на окружающих сетевых устройствах не требуется обновлять таблицы ARP, обновлять связки IP-адреса и соответствующего ему MAC-адреса;

— отсутствие необходимости обновлять таблицы ARP способствует минимизации потерь сетевых пакетов при переключении кластера, так как такое обновление хотя и происходит быстро, но тем не менее занимает время;

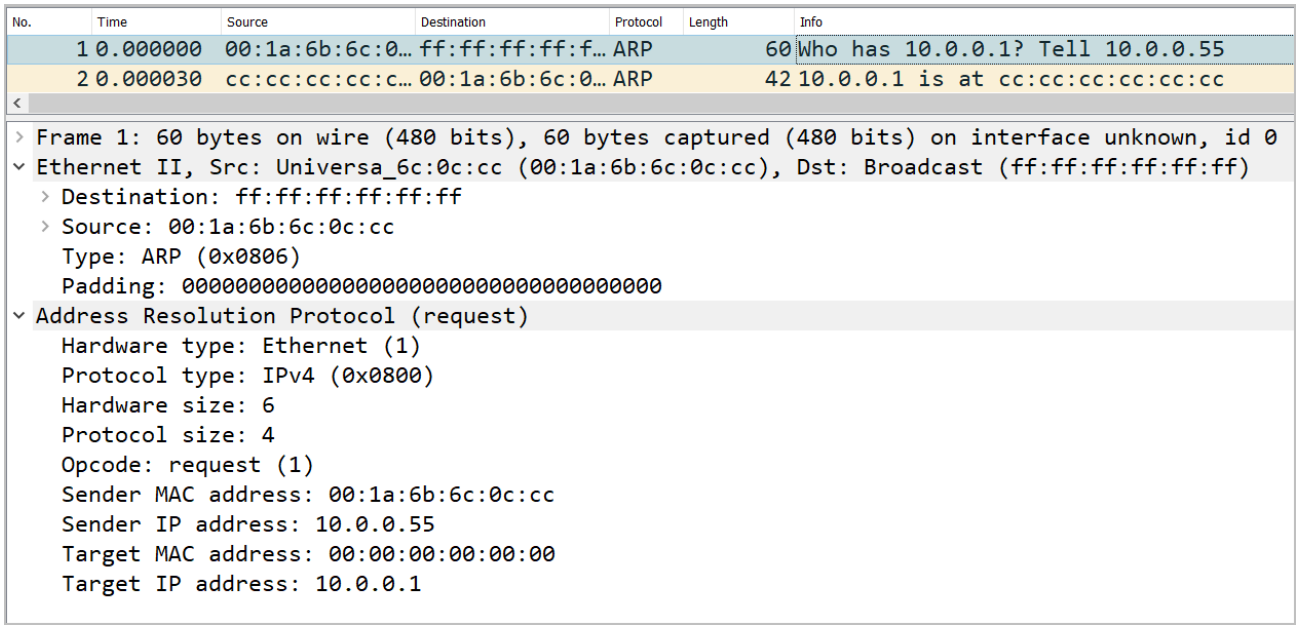
— оконечные сетевые узлы могут не иметь возможности обновить таблицы ARP, так как сообщения GARP блокируются промежуточными или оконечными сетевыми устройствами, например вследствие работы функции защиты от отравления ARP-кэша (anti-ARP poisoning) или игнорируются оконечными сетевыми устройствами.

  Примечание. Отключение виртуального MAC-адреса может требоваться в некоторых сетевых сценариях, но в большинстве случаев его рекомендуется использовать.

Если используется vMAC, то сабинтерфейс активного узла будет использовать виртуальный MAC-адрес вместо реального MAC-адреса интерфейса сетевой карты при отправке и получении кадров Ethernet. Например, на сабинтерфейсе eth1-1.1 настроен IP-адрес 10.0.0.1/8, его реальный MAC-адрес равен AA:AA:AA:AA:AA:AA (далее по тексту AA::AA) и назначенный vMAC имеет значение CC:CC:CC:CC:CC:CC (далее по тексту CC::CC).

Примечание. В действительности MAC-адрес имеет физический интерфейс, а сабинтерфейс его наследует.

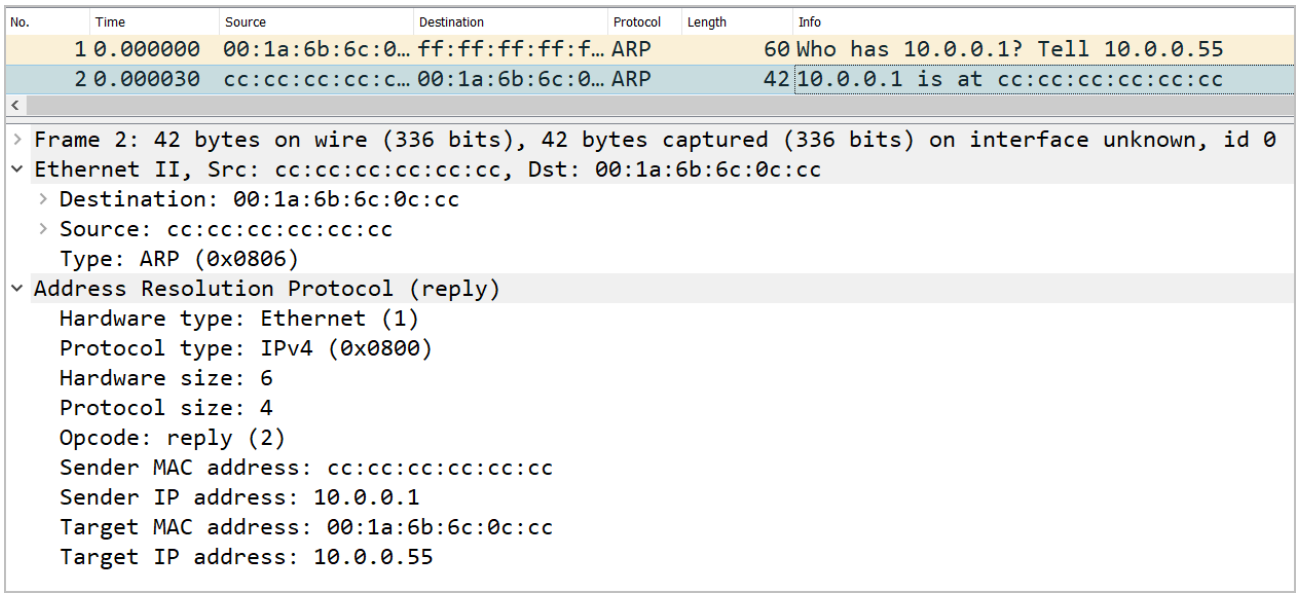
Активный узел кластера (в примере — NGFW1), получая ARP-запросы на сабинтерфейсе eth1-1.1 о MAC-адресе узла с IP-адресом 10.0.0.1, в ARP-ответах будет отправлять значение своего виртуального MAC-адреса — CC::CC. Резервный узел игнорирует все запросы ARP.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:1a:6b:6c:0…	ff:ff:ff:ff:f…	ARP	60	Who has 10.0.0.1? Tell 10.0.0.55
2	0.000030	cc:cc:cc:cc:c…	00:1a:6b:6c:0…	ARP	42	10.0.0.1 is at cc:cc:cc:cc:cc:cc

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface unknown, id 0
v Ethernet II, Src: Universa_6c:0c:cc (00:1a:6b:6c:0c:cc), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: ff:ff:ff:ff:ff:ff
  > Source: 00:1a:6b:6c:0c:cc
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: 00:1a:6b:6c:0c:cc
    Sender IP address: 10.0.0.55
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 10.0.0.1
```

Рисунок 232. Пример запроса ARP, полученного сабинтерфейсом устройства кластера



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:1a:6b:6c:0…	ff:ff:ff:ff:f…	ARP	60	Who has 10.0.0.1? Tell 10.0.0.55
2	0.000030	cc:cc:cc:cc:c…	00:1a:6b:6c:0…	ARP	42	10.0.0.1 is at cc:cc:cc:cc:cc:cc

```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface unknown, id 0
v Ethernet II, Src: cc:cc:cc:cc:cc:cc, Dst: 00:1a:6b:6c:0c:cc
  > Destination: 00:1a:6b:6c:0c:cc
  > Source: cc:cc:cc:cc:cc:cc
    Type: ARP (0x0806)
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: cc:cc:cc:cc:cc:cc
    Sender IP address: 10.0.0.1
    Target MAC address: 00:1a:6b:6c:0c:cc
    Target IP address: 10.0.0.55
```

Рисунок 233. Пример ответа ARP, отправляемого с сабинтерфейса активного устройства

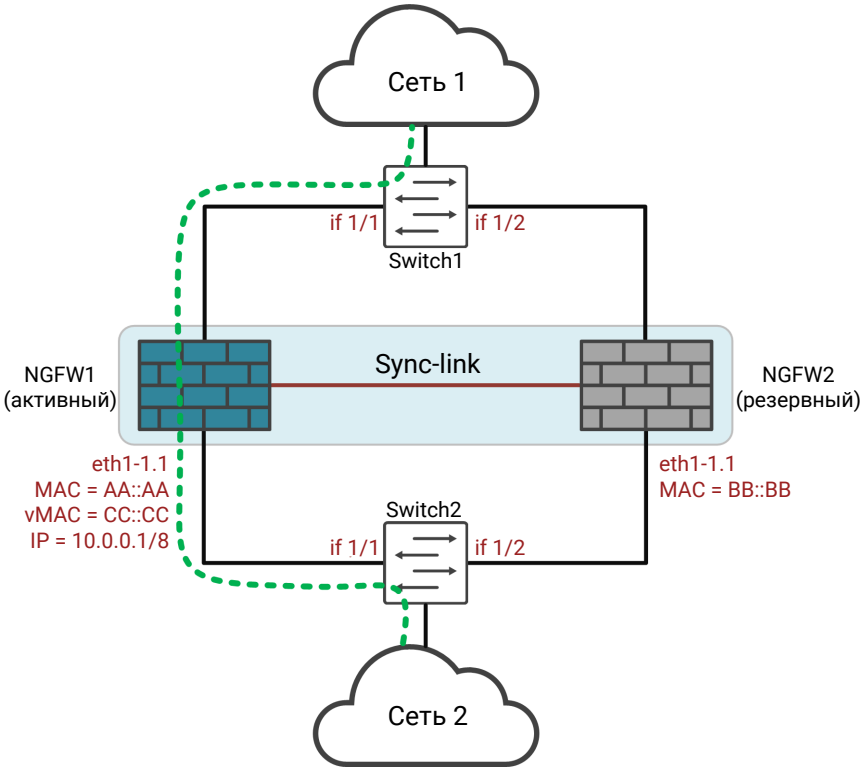


Рисунок 234. Передача трафика через активный узел NGFW1

Ниже пример таблицы MAC-адресов коммутатора Switch2, в котором видно, что адрес CC::CC в этот момент доступен через интерфейс if 1/1.

```
admin@Switch2> show mac-address-table
MAC age-time           : 300 seconds
Number of MAC addresses: 1

MAC Address           VLAN      Type       Interface
-----------------------------------------------------
cc:cc:cc:cc:cc:cc     25        dynamic    1/1
```

После переключения кластера новый активный узел (в примере — NGFW2) рассылает сообщения по протоколу Gratuitous ARP (GARP) со всех своих сабинтерфейсов. В случае, когда используется виртуальный MAC-адрес, рассылка GARP необходима для того, чтобы коммутаторы, к которым подключены кластеры (Switch1 и Switch2 в примере), обновили свои таблицы MAC-адресов и внесли запись, что узел с MAC-адресом CC::CC теперь подключен к другому их интерфейсу (в примере это if 1/2).

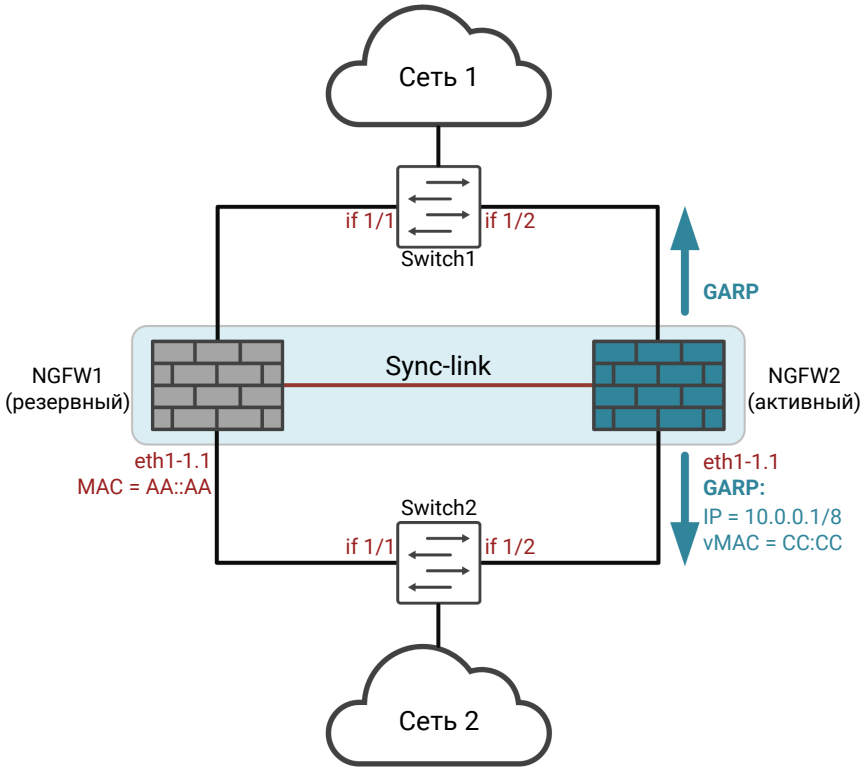


Рисунок 235. Рассылка сообщений GARP с vMAC новым активным узлом NGFW2

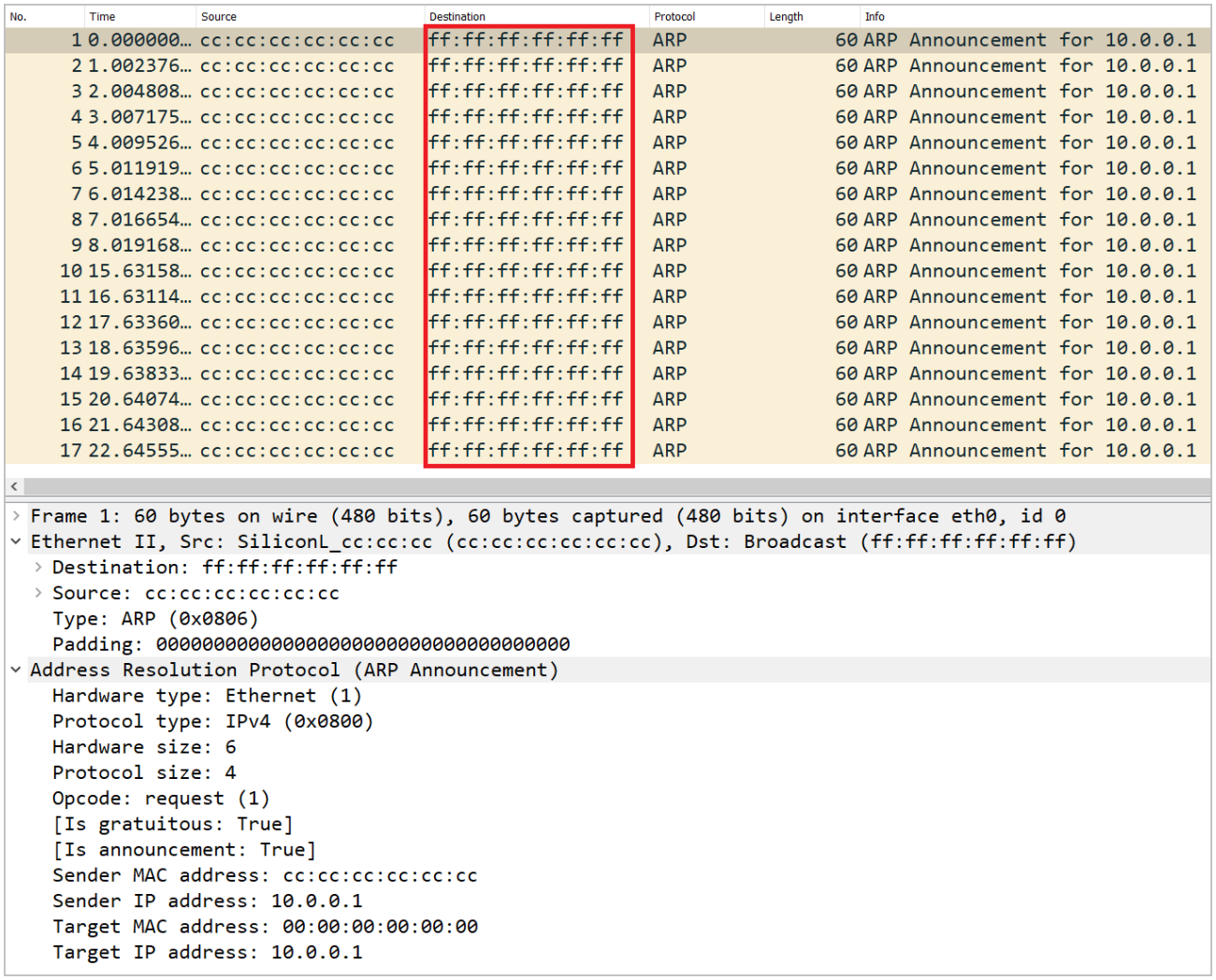


Рисунок 236. Пример сообщения GARP, рассылаемого новым активным узлом кластера

Важно отметить, что сообщения GARP рассылаются с адресом назначения (Destination) FF:FF:FF:FF:FF:FF — это широковещательный адрес, то есть предназначаемый всем узлам в домене широковещательной рассылки. Адрес источника (Source) — CC::CC — это виртуальный MAC-адрес.

Ниже пример таблицы MAC-адресов коммутатора Switch2. Адрес CC::CC теперь доступен через интерфейс if 1/2.

```
admin@Switch2> show mac-address-table
MAC age-time           : 300 seconds
Number of MAC addresses: 1

MAC Address           VLAN      Type       Interface
-----------------------------------------------------
cc:cc:cc:cc:cc:cc     25        dynamic    1/2
```

Для окружающих сетевых узлов в сетях 1 и 2 (таких как рабочие станции, серверы) изменений не произошло, так как связка «IP-адрес и vMAC» осталась прежней. Коммутаторы Switch1 и Switch2 обновили записи в своих таблицах коммутации и теперь пересылают кадры Ethernet с MAC-адресом назначения, равным CC::CC в направлении интерфейса eth1-1 NGFW2 через свои интерфейсы if 1/2.

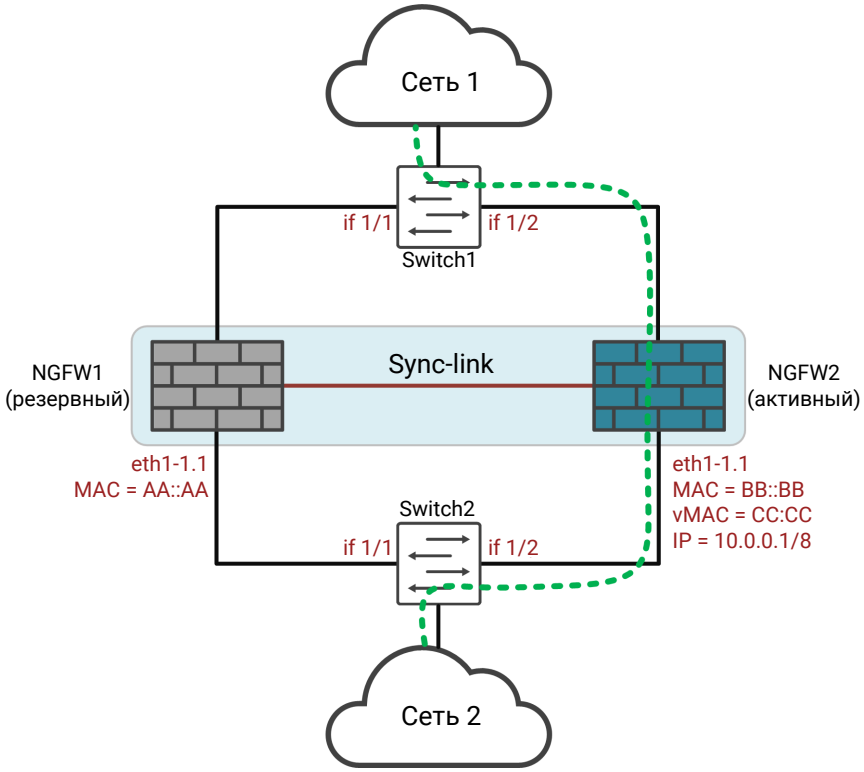


Рисунок 237. Передача трафика через активный узел NGFW2

Виртуальные MAC-адреса назначаются интерфейсам кластера PT NGFW системой централизованного управления из диапазона (пула) 0E:00:5E:00:00:00 — 0E:00:5E:FF:FF:FF.

Начальное значение vMAC — 0E:00:5E:00:00:00. Каждому следующему интерфейсу будет назначен следующий по очереди адрес.

При назначении адресов vMAC интерфейсам очередного (нового) кластера значение не сбрасывается на начальное 0E:00:5E:00:00:00, а назначается следующее очередное значение из пула. Например, интерфейсам кластера Cluster-1 назначены виртуальные MAC-адреса с 0E:00:5E:00:00:00 по 0E:00:5E:00:00:0F. При создании Cluster-2 его интерфейсы получат адреса начиная со следующего значения, то есть начиная с 0E:00:5E:00:00:10 и так далее для последующих создаваемых кластеров.

Удаление кластера никак не влияет на назначаемые виртуальные адреса. Иными словами, адреса vMAC, которые использовались интерфейсами удаляемого кластера, не возвращаются в пул.

При исчерпании пула, то есть когда достигается адрес 0E:00:5E:FF:FF:FF, следующим значением назначаемого vMAC будет 0E:00:5E:00:00:00 и так далее. Назначение адресов vMAC происходит циклическим образом.

Несовпадающие виртуальные MAC-адреса интерфейсов разных кластеров необходимы, чтобы исключить коллизии адресов интерфейсов в одном домене широковещательной рассылки (broadcast domain). Например, пул 0E:00:5E:00:00:00 — 0E:00:5E:FF:FF:FF обеспечивает более 16 миллионов адресов.

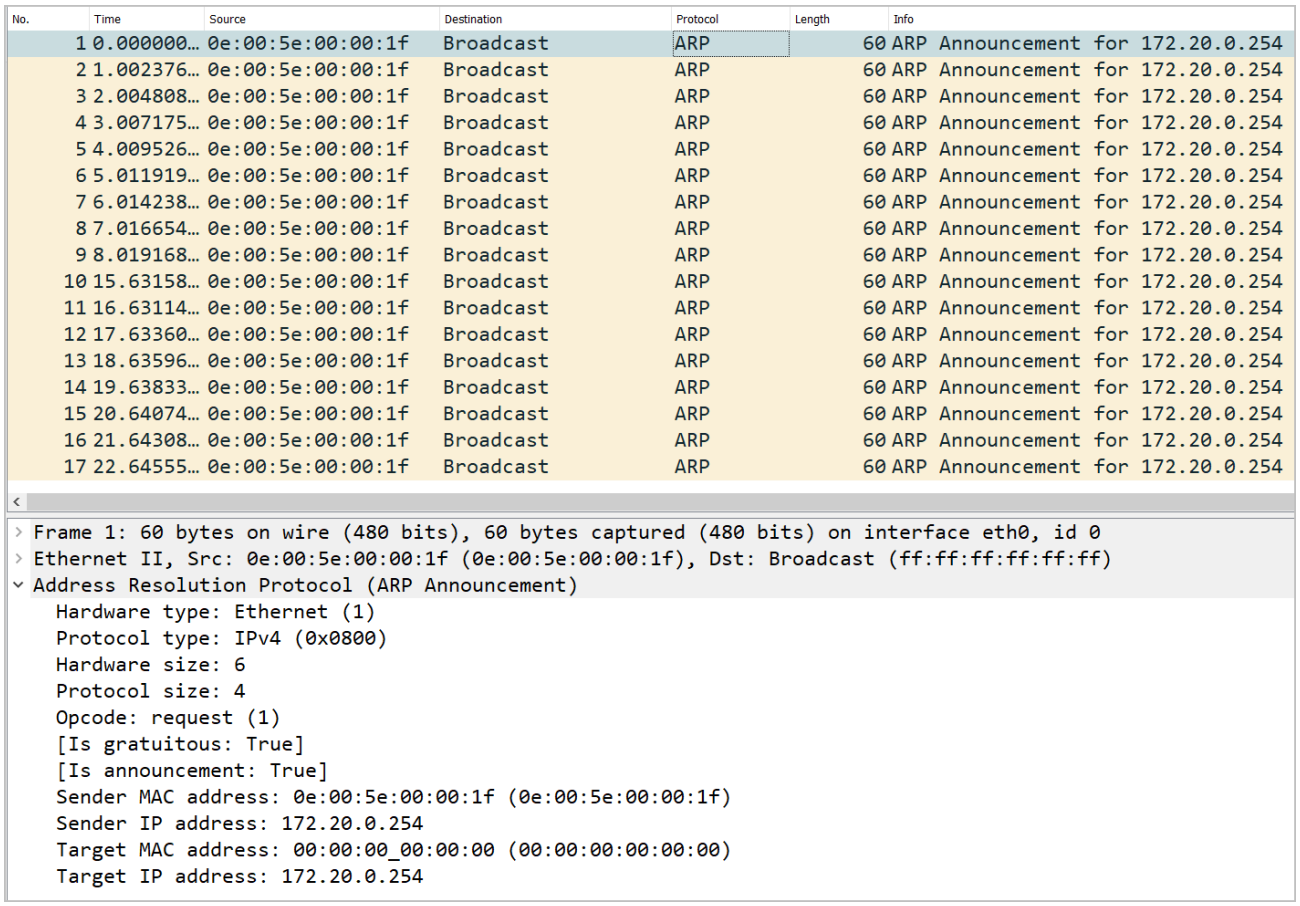


Рисунок 238. Пример рассылки GARP с интерфейса активного узла при переключении кластера

В случае, если использование vMAC отключено в кластере, например, из-за ограничений среды виртуализации, то каждый из узлов кластера будет использовать реальные (назначенные гипервизором) MAC-адреса своих интерфейсов (сабинтерфейсов) для отправки и приема кадров Ethernet. Таким образом, при переключении кластера окружающие сетевые узлы обнаружат, что MAC-адреса его интерфейсов изменились.

Возвращаясь к схеме в примере выше, если использование vMAC отключено, то в кадрах Ethernet, отправляемых активным узлом NGFW1 с сабинтерфейса eth1-1.1, будет указан MAC-адрес AA::AA в качестве адреса источника (Source MAC). Соответственно, в ответах на ARP-запросы узел NGFW1 (активный) будет указывать значение своего реального MAC-адреса — AA::AA.

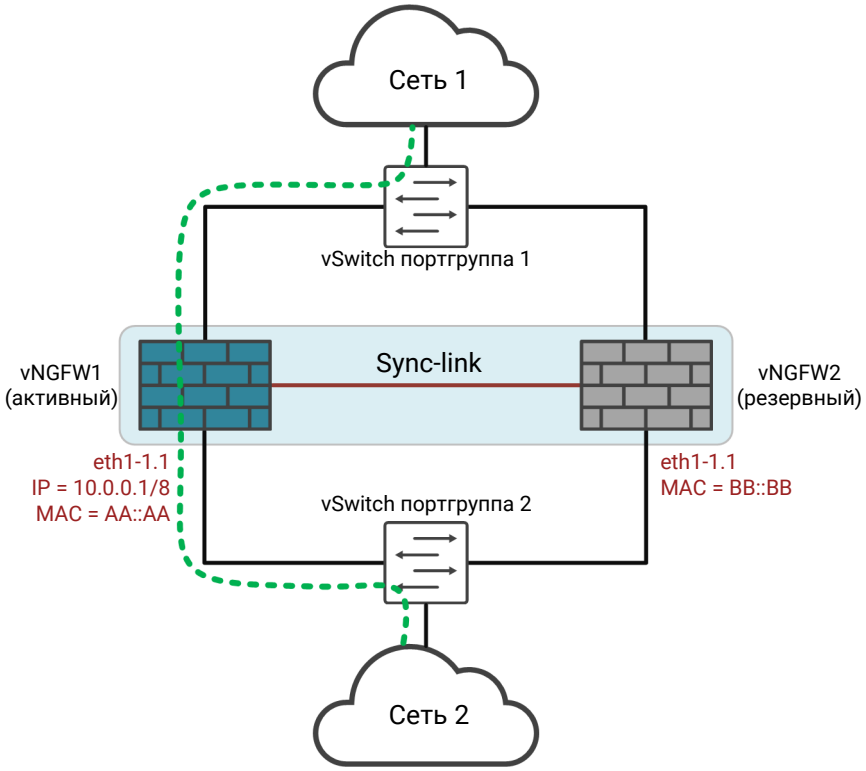


Рисунок 239. Передача трафика через активный узел NGFW1 (vMAC не используется)

В случае переключения кластера новым активным узлом станет NGFW2. Его интерфейсы имеют другие MAC-адреса. Чтобы обновить связку «IP-адрес — MAC-адрес» в таблицах ARP окружающих сетевых узлов (таких как рабочие станции, серверы), а также обновить таблицы коммутации Switch1 и Switch2, новый активный узел рассылает сообщения GARP, в которых указаны реальные MAC-адреса его интерфейсов (в примере — BB::BB).

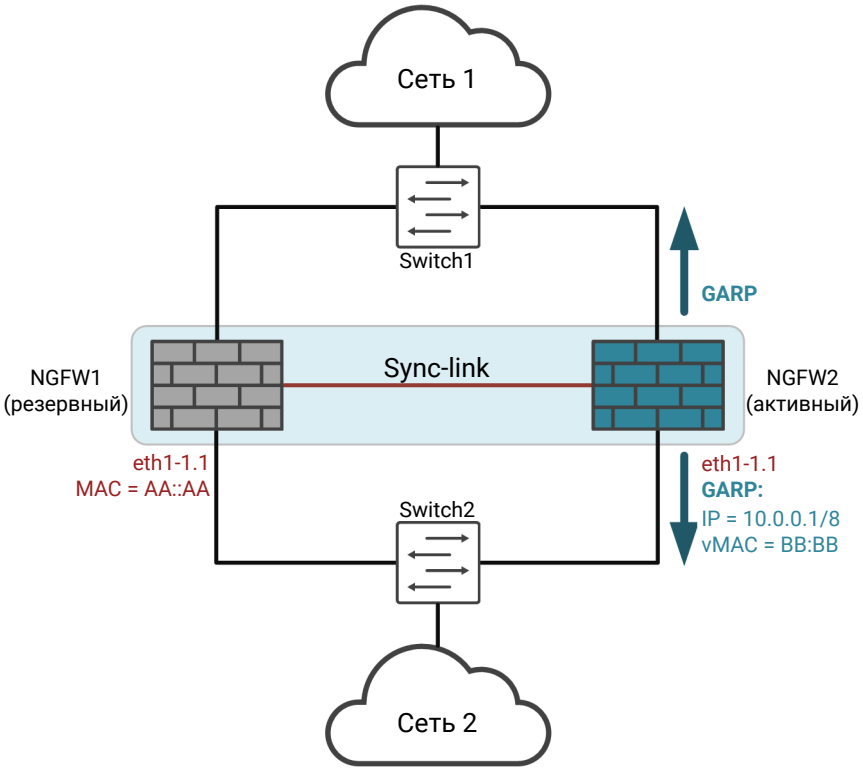


Рисунок 240. Рассылка сообщений GARP с реальным MAC-адресом новым активным узлом NGFW2

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000…	bb:bb:bb:bb:bb:bb	ff:ff:ff:ff:ff:ff	ARP	60	ARP Announcement for 10.0.0.1
2	1.002376…	bb:bb:bb:bb:bb:bb	ff:ff:ff:ff:ff:ff	ARP	60	ARP Announcement for 10.0.0.1

```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
v Ethernet II, Src: bb:bb:bb:bb:bb:bb, Dst: ff:ff:ff:ff:ff:ff
  > Destination: ff:ff:ff:ff:ff:ff
  > Source: bb:bb:bb:bb:bb:bb
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (ARP Announcement)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    [Is announcement: True]
    Sender MAC address: bb:bb:bb:bb:bb:bb
    Sender IP address: 10.0.0.1
    Target MAC address: 00:00:00:00:00:00
    Target IP address: 10.0.0.1
```

Рисунок 241. Пример рассылки GARP с интерфейса активного устройства при переключении кластера (vMAC не используется)

Окружающие сетевые узлы (такие как рабочие станции, серверы) обнаруживают изменения, так как связка «IP-адрес — MAC-адрес» теперь другая.

Коммутаторы Switch1 и Switch2 обновили записи в своих таблицах коммутации и теперь пересылают кадры Ethernet с MAC-адресом назначения, равным BB::BB в направлении интерфейса eth1-1 узла NGFW2.

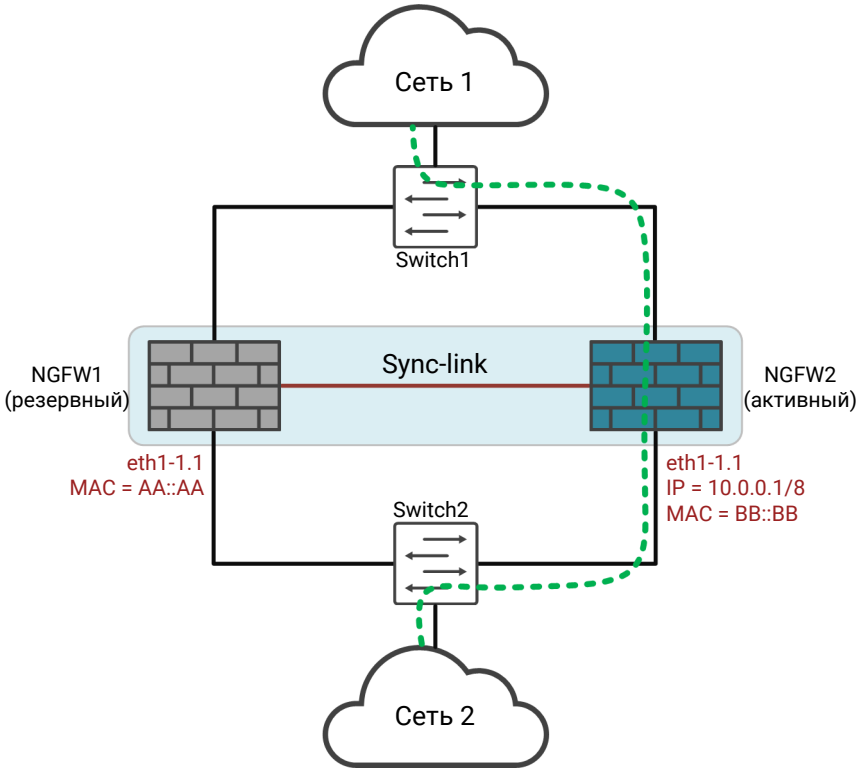


Рисунок 242. Передача трафика через активный узел NGFW2 (vMAC не используется)

В примере ниже активный узел кластера отвечает на запрос ARP клиентского узла. MAC-адрес интерфейса eth1-1 активного узла — 00:50:56:94:95:37, IP-адрес — 172.20.0.254.

```
No.  Time      Source              Destination         Protocol  Length  Info
  29 5.254811… VMware_c6:b7:6c     VMware_94:95:37     ARP         42    Who has 172.20.0.254? Tell 172.20.0.1
  30 5.255019… VMware_94:95:37     VMware_c6:b7:6c     ARP         60    172.20.0.254 is at 00:50:56:94:95:37

> Frame 30: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
v Ethernet II, Src: VMware_94:95:37 (00:50:56:94:95:37), Dst: VMware_c6:b7:6c (00:0c:29:c6:b7:6c)
  > Destination: VMware_c6:b7:6c (00:0c:29:c6:b7:6c)
  > Source: VMware_94:95:37 (00:50:56:94:95:37)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
v Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: VMware_94:95:37 (00:50:56:94:95:37)
    Sender IP address: 172.20.0.254
    Target MAC address: VMware_c6:b7:6c (00:0c:29:c6:b7:6c)
    Target IP address: 172.20.0.1
```

Рисунок 243. Пример ответа ARP, отправляемого с сабинтерфейса активного узла (vMAC не используется)

После переключения кластера новый активный узел рассылает сообщения GARP, в которых MAC-адрес источника (Source MAC) — 00:0c:29:7e:bd:2c. Это MAC-адрес интерфейса eth1-1 нового активного узла. IP-адрес 172.20.0.254 не изменился.

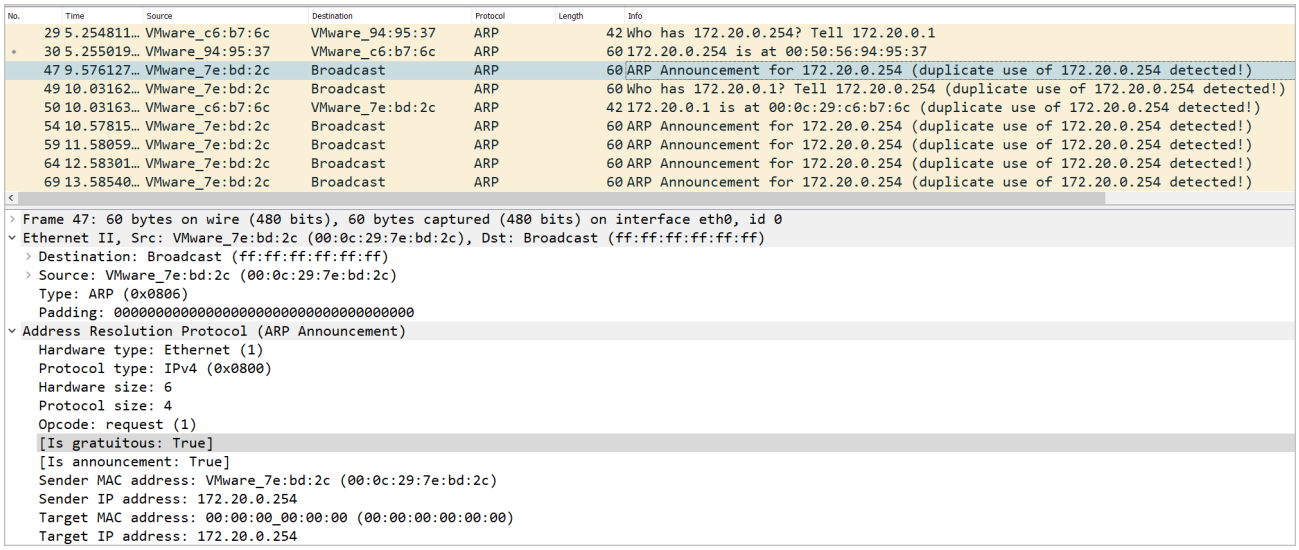


Рисунок 244. Пример рассылки GARP с интерфейса активного узла при переключении кластера (vMAC не используется)

30.2. Работа в виртуальной среде в режиме маршрутизации

При работе в виртуальной среде в режиме маршрутизации (L3), например при развертывании виртуальной машины PT NGFW на базе гипервизора VMware ESXi, виртуальный коммутатор (VMware vSwitch) не выполняет изучение MAC-адресов (MAC-learning). Гипервизор явно назначает MAC-адреса виртуальным сетевым адаптерам (vNIC) виртуальных машин, и, следовательно, в изучении MAC-адресов нет необходимости.

По умолчанию виртуальный коммутатор пересылает кадры Ethernet только с теми MAC-адресами, которые назначены гипервизором и которые известны виртуальному коммутатору. Например, интерфейс виртуальной машины имеет MAC-адрес AA::AA. Виртуальный коммутатор будет пересылать на этот интерфейс и отправлять с этого интерфейса только кадры Ethernet с MAC-адресом назначения (Destination MAC) и MAC-адресом источника (Source MAC), равным AA::AA соответственно. Если в параметрах кластера задано использование виртуального MAC-адреса (vMAC), такие кадры будут отбрасываться, так как MAC-адреса интерфейсов отличаются от назначенных гипервизором.

Для того чтобы кадры с vMAC не блокировались необходимо в параметрах VMware vSwitch или портгруппы, куда подключены vNIC (виртуальные сетевые адаптеры) узлов кластера PT NGFW, разрешить Promiscuous mode, MAC Address Changes и Forged MAC-Transmit.

По различным причинам включение этих параметров может быть невозможно, поэтому необходимо отключить использование виртуального MAC-адреса в кластере.

При отключенном vMAC интерфейсы каждого из узлов кластера используют разные MAC-адреса. При переключении кластера новый активный виртуальный узел рассылает сообщения GARP для того, чтобы окружающие сетевые узлы обновили записи об IP и MAC-адресах интерфейсов межсетевого экрана в своих таблицах ARP. Чтобы окружающие сетевые устройства успешно получали сообщения GARP, рассылаемые новым активным узлом кластера, необходимо убедиться, что сообщения GARP не блокируются и не игнорируются, например, из-за активированной защиты от отравления ARP-кэша (anti-ARP poisoning) на сетевых устройствах.

30.3. Режим vWire

PT NGFW, работающий в режиме vWire, можно представить в виде «логического патч-корда». В этом режиме настраиваются сабинтерфейсы физических интерфейсов. В отличие от режима маршрутизации в режиме vWire:

— через PT NGFW проходят широковещательные запросы;

— не происходит изучение MAC-адресов (MAC Learning);

— сетевые устройства не «замечают» PT NGFW (в части того трафика, который был проверен и разрешен PT NGFW);

— трафик протоколов, не использующих IP (например LACP и STP), проходит прозрачно.

Для обеспечения корректности прохождения сетевого трафика интерфейсы, на которых есть хотя бы один сабинтерфейс, работающий в режиме vWire:

— находятся во включенном состоянии (Up) на активном узле кластера;

— находятся в отключенном состоянии (Down) на узле, который работает в любых других состояниях: резервный (Standby), ошибка (Fatal-Error) или приостановлен (Suspended).

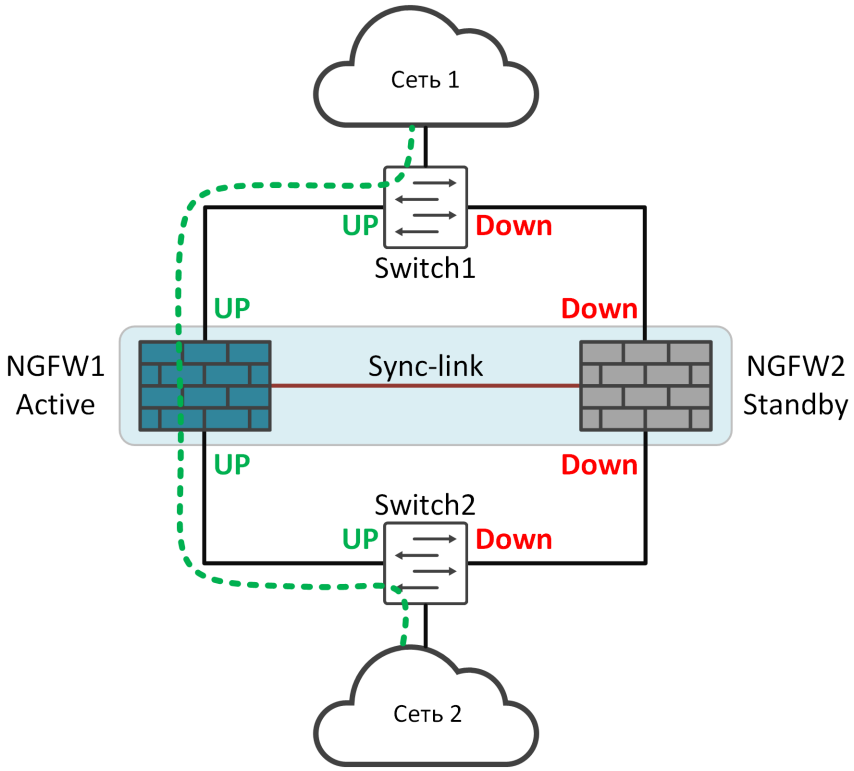


Рисунок 245. Трафик передается через активный узел NGFW1

Таким образом, с точки зрения сетевых устройств кластер PT NGFW выглядит как два пути прохождения трафика (для упрощения не учитываем физические пути в агрегированных группах LAG), один из которых включен и используется (интерфейсы в состоянии Up), а второй — отключен (интерфейсы в состоянии Down).

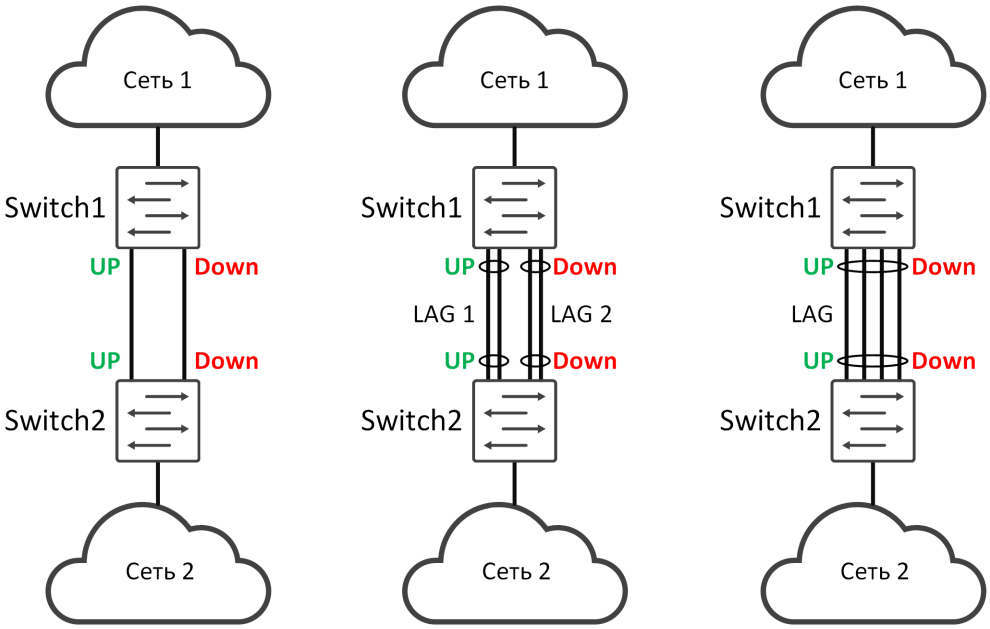


Рисунок 246. Кластер PT NGFW в режиме vWire с точки зрения сетевых устройств

Перевод интерфейсов во включенное состояние (Up) выполняется автоматически, когда узел становится активным. Интерфейсы автоматически отключаются (переходят в состояние Down) если узел стал резервным (Standby), перешел в состояние ошибки (Fatal-Error) или приостановлен (Suspended).

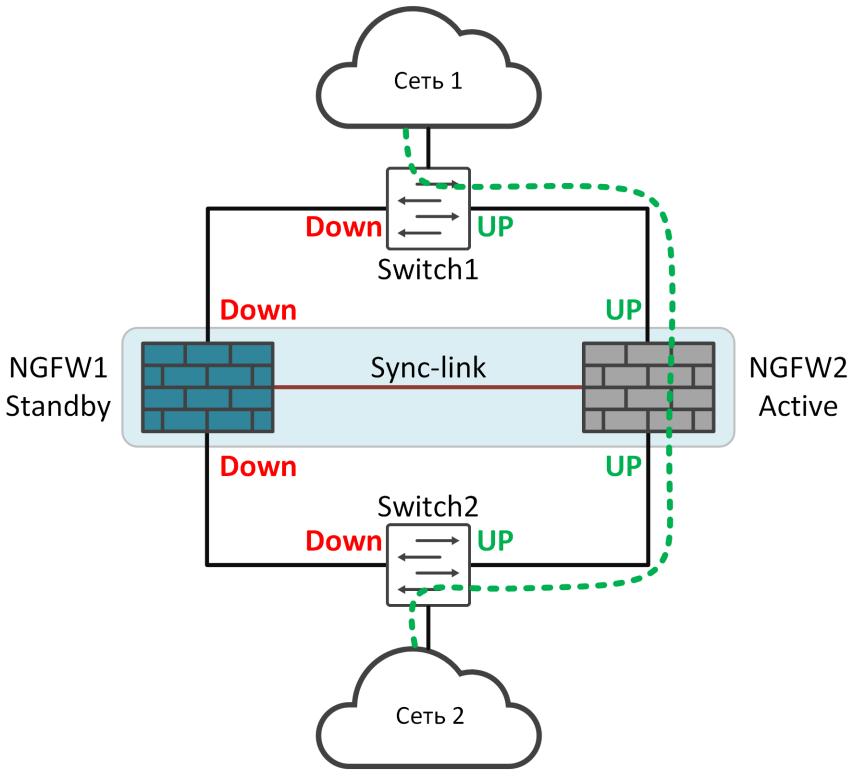


Рисунок 247. Трафик передается через активный узел NGFW2

Отключение интерфейсов (Down) на резервном (включая узел в состоянии ошибки) и приостановленных узлах необходимо, чтобы другие сетевые устройства, к которым подключен кластер PT NGFW, перенаправили трафик через новый активный узел, у которого интерфейсы перешли во включенное состояние (Up).

Если бы отключения интерфейсов на новом резервном устройстве (бывший активный) не производилось и если бы они оставались включенными, то после переключения кластера коммутаторы продолжали бы направлять кадры Ethernet в адрес интерфейсов бывшего активного узла, так как все MAC-адреса в MAC-таблицах коммутаторов продолжали бы значиться как доступные через эти интерфейсы. Все передаваемые кадры терялись бы в связи с тем, что резервный узел не передает трафик. После переключения кластера коммутаторы удаляют записи о MAC-адресах, которые значились доступными через отключенные интерфейсы, фиксируют включение новых интерфейсов и начинают направлять в них кадры Ethernet, поступающие в адрес MAC-адресов, информация о которых была только что удалена (коммутация Unknown unicast трафика). Таким образом, после обмена кадрами между сетевыми узлами в MAC-таблицах коммутаторов MAC-адреса будут значиться как доступные через интерфейсы нового активного узла кластера.

30.4. Приоритет устройств в кластере

Используется для указания более предпочтительного устройства для получения роли активного (Active). Чем ниже значение, тем выше приоритет. Например, если у NGFW1 приоритет 3, а у NGFW2 — 6, то при прочих равных активным будет выбран NGFW1. Если узлы имеют одинаковый приоритет, то при прочих равных активным станет узел с меньшим значением идентификатора узла (UUID). Оно уникальное и генерируется автоматически при первом запуске устройства PT NGFW.

30.5. Приоритетное замещение (Preemption)

В некоторых сценариях требуется, чтобы активным было определенное устройство. При настройке кластера указывается приоритет каждого из устройств. При включенном параметре «Приоритетное замещение (Preemption)» выполняется замещение текущего активного узла новым активным на основе указанного приоритета.

Таблица 17. Поведение кластера при разных состояниях параметра «Приоритетное замещение (Preemption)»

При выключенном параметре	**При включенном параметре**
Приоритет устройств сравнивается: — при начальном объединении узлов в кластер; — если оба устройства находятся в состоянии «Standby (резервный)», например при одновременном перезапуске, включении; — если оба устройства находятся в состоянии «Active (активный)», например после сбоя и восстановления канала синхронизации Sync-link узлы обнаруживают друг друга. Если конфигурация кластера изменилась и текущий резервный узел NGFW2 получил приоритет выше, чем у текущего активного NGFW1, то переключения кластера не произойдет и узлы продолжат работу в прежних рнолях вне зависимости от новых значений приоритетов. Если узел с более высоким приоритетом, например NGFW1, выйдет из строя, то новым активным станет NGFW2, у которого приоритет ниже. Когда узел NGFW1 подключится	Приоритет устройств сравнивается: — в тех же случаях, что и при выключенном параметре; — при изменении приоритетов устройств кластера; — при подключении устройства к кластеру; — при выходе устройства из состояния «Приостановлен (Suspended)». Если конфигурация кластера изменилась и текущий резервный узел NGFW2 получил более высокий приоритет, то он станет новым активным узлом кластера. Если текущий активный узел, у которого был более высокий приоритет, например NGFW1, выйдет из строя, то новым активным станет NGFW2. Когда узел NGFW1 подключится к кластеру после восстановления, то он вернет себе роль активного.

При выключенном параметре	При включенном параметре
к кластеру после восстановления, то он продолжит свою работу в качестве резервного несмотря на более высокий приоритет.	

Примечание. Если нет требования, чтобы определенный узел кластера был активным, например для более оптимального маршрута прохождения трафика в отдельных сетевых сценариях, то рекомендуется отключать параметр «Приоритетное замещение (Preemption)». Это обеспечит меньшее количество переключений кластера и минимизацию потерь трафика.

Примечание. Узел с приоритетом выше становится новым активным узлом по истечении времени Preemption Hold Time (задержка приоритетного замещения). Задержка необходима для стабилизации параметров и полной инициализации всех модулей межсетевого экрана, например в случае загрузки (перезагрузки) устройства с более высоким приоритетом, а также получения и применения актуальной конфигурации текущего активного устройства. В PT NGFW установлено фиксированное значение задержки — 60 секунд.

30.6. Graceful restart (OSPF, BGP)

Узлы в кластере «активный — резервный» поддерживают технологию graceful restart для OSPF и BGP.

При переключении кластера резервный узел становится новым активным устройством и продолжает пересылать транзитный сетевой трафик, используя маршруты в FIB, полученные ранее в рамках синхронизации информации между узлами кластера. Новый активный узел уведомляет соседнее сетевое устройство (graceful restart helper) о перезапуске сетевого процесса и о том, что необходимо продолжать пересылку сетевого трафика, используя имеющиеся маршруты, не удалять маршруты из таблицы маршрутизации, не отправлять уведомления об изменении маршрутной информации. Затем новый активный узел кластера PT NGFW устанавливает отношения смежности BGP или OSPF с соседним сетевым устройством (graceful restart helper), актуализирует таблицу маршрутизации. Все это время пересылка транзитного сетевого трафика продолжается.

Функция graceful restart является одним из механизмов, обеспечивающих минимизацию потерь сетевого трафика при переключении кластера.

Вы можете включить функцию graceful restart и режим помощника (graceful restart helper) в параметрах OSPF и BGP виртуального роутера. В параметрах BGP режим помощника включается автоматически при включении функции graceful restart.

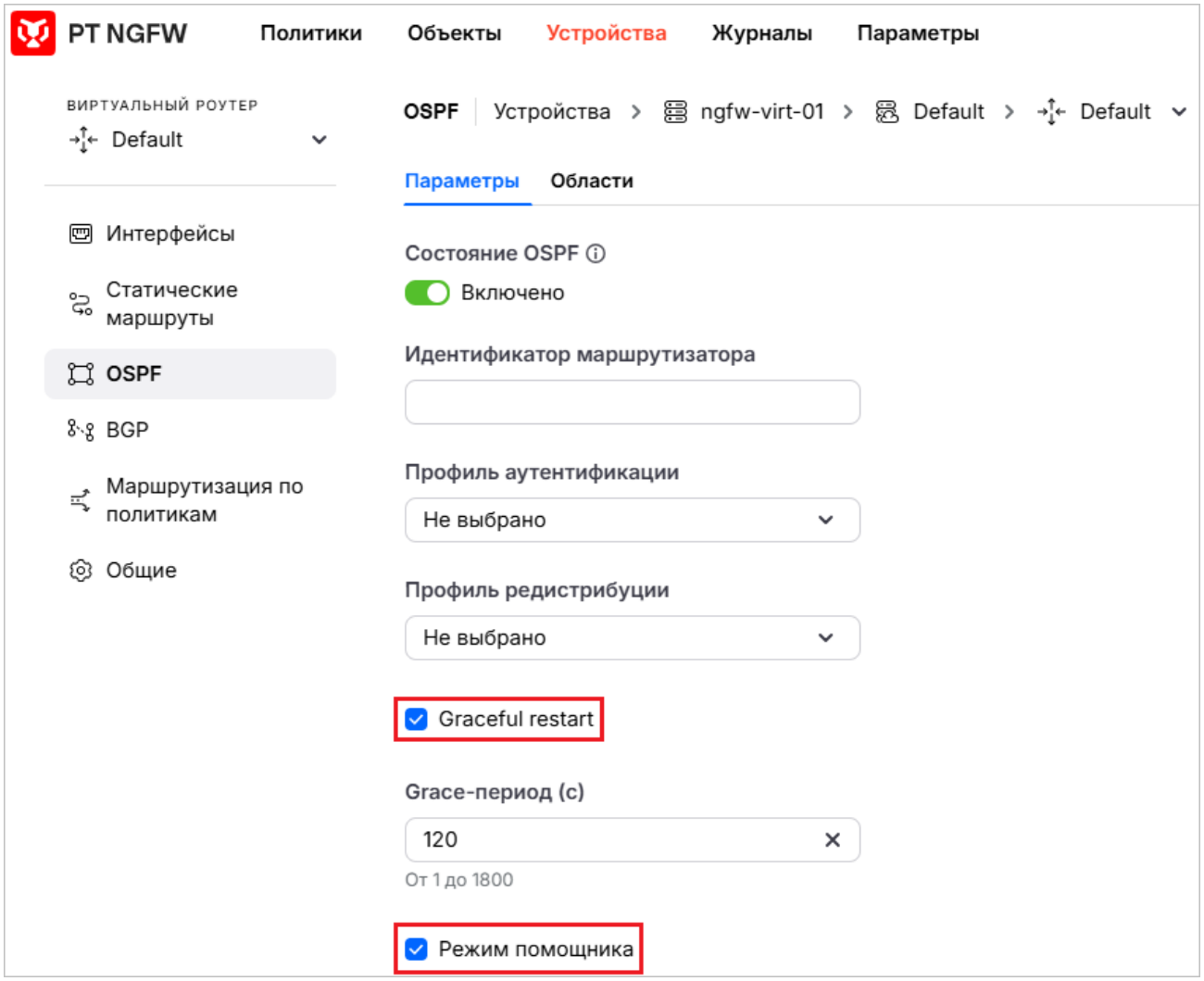


Рисунок 248. Включение функции graceful restart и режима помощника в параметрах OSPF

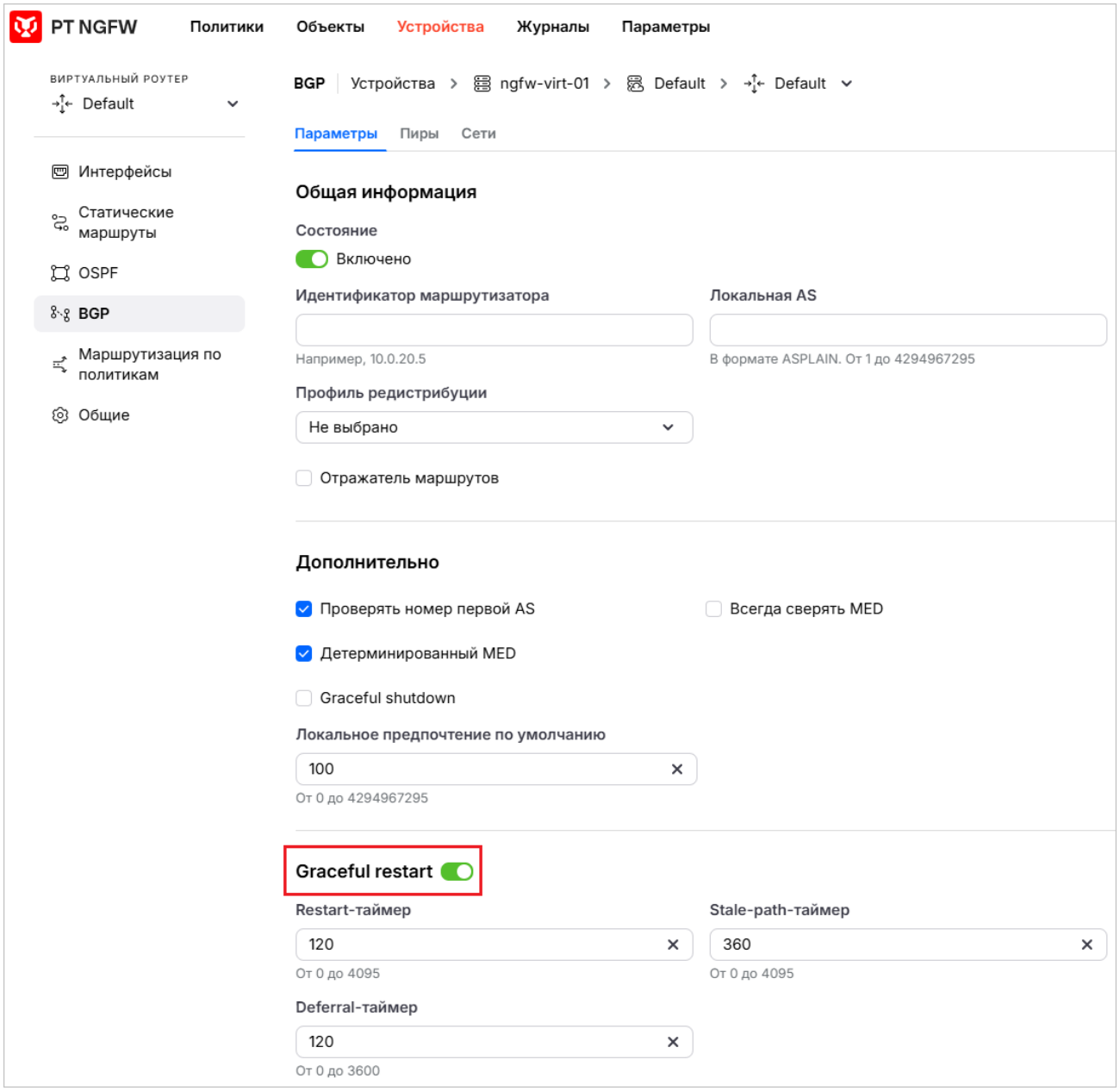


Рисунок 249. Включение функции graceful restart в параметрах BGP (режим помощника при этом включается автоматически)

Подробнее о настройке динамической маршрутизации см. в разделах «Настройка OSPF (см. раздел 14.2.1)» и «Настройка BGP (см. раздел 14.2.2)».

30.7. Состояния узлов кластера

Система управления получает информацию о каждом из узлов кластера как от самих устройств, так и от их соседей по кластеру, то есть узел NGFW1 сообщает информацию о себе и об узле NGFW2; аналогично действует узел NGFW2. Это позволяет получать актуальную информацию о состоянии узлов, даже если у одного из них отсутствует подключение к системе управления.

> **Внимание!** Управление кластером выполняется только при наличии связи системы управления с активным устройством. Ниже приведен список возможных состояний узлов кластера.

Активный (Active)

Устройство передает транзитный пользовательский трафик, участвует в процессах динамической маршрутизации, отслеживает метрики здоровья и состояния интерфейсов, а также обменивается с резервным устройством служебными сообщениями через канал синхронизации Sync-link.

Активный · Внимание (Active · Warning)

Аналогично состоянию «Активный (Active)» за исключением того, что на устройстве зафиксирована деградация метрик здоровья. При этом узел работоспособен, но требует внимания администратора.

Резервный (Standby)

Устройство не передает трафик, отслеживает состояние активного устройства, находится в готовности начать обработку транзитного пользовательского трафика в случае проблем на активном устройстве. В этом состоянии устройство не участвует в процессах динамической маршрутизации, отслеживает метрики здоровья и состояния интерфейсов. Резервное устройство обменивается с активным устройством служебными сообщениями через канал синхронизации Sync-link. Интерфейсы находятся в состоянии «Включено (Up)», но сбрасывают любые поступающие сетевые пакеты. Интерфейсы, на которых настроен хотя бы один сабинтерфейс в режиме vWire, находятся в состоянии «Отключено (Down)». Устройство принимает конфигурацию только от активного узла.

Резервный · Внимание (Standby · Warning)

Аналогично состоянию «Резервный (Standby)» за исключением того, что на устройстве зафиксирована деградация метрик здоровья. Узел требует внимания администратора. Например, на устройстве отказал один из отслеживаемых интерфейсов. При этом устройство находится в приемлемом работоспособном состоянии и готово стать активным в случае выхода из строя текущего активного узла. Устройство принимает конфигурацию только от активного узла.

Пример ситуации, в которой возможно появление устройства в состоянии «Активный · Внимание (Active · Warning)»: у обоих устройств (активного и резервного) отказали отслеживаемые интерфейсы одинакового приоритета, например вследствие выключения коммутатора, к которому они оба подключены. Переключения кластера в этом случае не произойдет, так как на резервном устройстве метрики здоровья равны или хуже, чем на активном. Устройства будут работать в состояниях «Активный · Внимание (Active · Warning)» и «Резервный · Внимание (Standby · Warning)» соответственно.

Резервный · Ошибка (Standby · Fatal-Error)

На устройстве зафиксированы ошибки, делающие невозможным пересылку трафика и переход в состояние активного. Это не всегда является признаком полного выхода устройства из строя. Например, резервное устройство переходит в состояние Fatal-Error если ему не удалось применить конфигурацию, которая успешно применилась на активном устройстве. Резервное устройство переходит в это состояние и требует внимания администратора, чтобы исключить работу устройств одного кластера с разными конфигурациями, так как при переключении кластера это может привести к негативным последствиями в связи с тем, что конфигурации могут значительно отличаться. Устройство принимает конфигурацию только от активного узла.

Находясь в состоянии «Резервный · Ошибка (Standby · Fatal-Error)» узел:

— включен;

— не выполняет синхронизации сессий и другой информации;

— по команде от активного узла пытается синхронизировать с ним конфигурацию;

— обменивается информацией о своем состоянии со вторым устройством и системой управления;

— не передает транзитный пользовательский трафик;

— не участвует в процессе выбора активного устройства, не может стать активным;

Если проблема более не обнаруживается, то узел переходит в состояние резервного, синхронизирует информацию с текущим активным устройством. Только после этого становится полноценным участником кластера с возможными дальнейшими выборами (если включен параметр Preemption) и переходом в состояние активного.

Приостановлен (Suspended)

Участие устройства в кластере приостановлено администратором. Переход узла из состояния «Приостановлен (Suspended)» возможен только по команде администратора.

Находясь в состоянии «Приостановлен (Suspended)» узел:

— включен;

— синхронизирует с активным устройством информацию о сессиях, конфигурации и другие данные;

— обменивается информацией о своем состоянии со вторым устройством и системой управления;

— не передает транзитный пользовательский трафик;

— не участвует в процессе выбора активного устройства и не может стать активным;

— после получения команды выхода из состояния «Приостановлен (Suspended)» переходит в состояние резервного, становится полноценным участником кластера с возможными дальнейшими выборами (если включена опция Preemption) и переходом в состояние активного;

— в случае получения от системы управления команды на выход из кластера устройство переходит в состояние «Отдельный (Standalone)».

Неизвестно (Unknown)

Отсутствует подключение устройства к системе управления, второй узел кластера также не сообщает системе управления никакой информации об устройстве.

Отдельный (Standalone)

Узел не входит в кластер. Статус отображается при первоначальной настройке после добавления устройств в кластер до тех пор, пока не применена конфигурация, а также если устройство было выведено из кластера через интерфейс командной строки (см. раздел «Удаление кластера»).

30.8. Состояния кластера

Ниже приведен список возможных состояний кластера.

Не применен (Pending)

Кластер создан в системе управления, но конфигурация не применена на устройствах. Указывает, что первичная настройка кластера не завершена.

Ок (Ok)

Кластер работает штатно, система управления обнаруживает оба устройства, и при этом одно в состоянии «Активный (Active)», а второе — в состоянии «Резервный (Standby)», включая состояние «Внимание (Warning)» любого или обоих узлов.

Ок · Внимание (Ok · Warning)

Аналогично состоянию «Ок» за исключением того, что одно или оба устройства имеют статус здоровья «Внимание (Warning)». Требует внимания администратора.

Деградация (Degraded)

Система управления обнаруживает оба устройства кластера, но одно из них в состоянии, в котором не передается трафик.

Отказ (Down)

Система управления обнаруживает единственное или оба устройства кластера и при этом узел (узлы) находятся в состоянии, в котором не передается трафик.

Потерян (Lost)

Система управления не обнаруживает ни одного устройства кластера.

Раскол кластера (Split-brain)

Система управления обнаруживает два устройства, и они оба в состоянии «Активный (Active)», включая «Активный · Внимание (Active · Warning)».

Неизвестно (Unknown)

Любые прочие ситуации.

30.9. Состояния конфигурации кластера

Синхронизирована (In sync)

Конфигурация кластера была успешно применена на устройствах при первичной настройке кластера.

Не синхронизирована (Out of sync)

Конфигурация кластера еще не была применена на устройствах при первичной настройке или изменении состава кластера.

Ошибка применения (Failed)

Конфигурацию кластера не удалось применить на устройствах при первичной настройке или изменении состава кластера.

30.10. Требования для создания кластера active-standby

В кластер можно объединить узлы PT NGFW при соблюдении следующих условий:

- одинаковая модель программно-аппаратных PT NGFW или одинаковая модель виртуальных PT NGFW;
- одинаковая версия ядра PT NGFW;
- одинаковая версия базовой ОС;
- одинаковые количество и тип физических интерфейсов или vNIC в случае объединения в кластер двух виртуальных PT NGFW;
- в случае с моделями PT NGFW 2010, 2020, 2050, 3010, 3040 и 3050 узлы должны иметь набор идентичных интерфейсных модулей и их одинаковое расположение в слотах;
- если объединяются два виртуальных PT NGFW, то узлы должны иметь одинаковый объем выделенной оперативной памяти, одинаковое количество выделенных ядер процессора и их распределение между ядрами для обработки данных (dataplane) и функций управления (management, control-plane);
- Значения `hostname` на узлах кластера не должны совпадать. См. подробнее в разделе «Изменение имени хоста (hostname) (см. раздел 5.3.1)».
- рекомендуется иметь одинаковый набор лицензий, а также одинаковую версию баз контента (IPS, антивирус, GeoIP и другие).

Требования обусловлены тем, что при переключении кластера новый активный узел должен продолжить обработку транзитного трафика, который ранее обрабатывался отказавшим узлом, с той же производительностью и тем же уровнем защиты. Конфигурация синхронизируется между узлами кластера, поэтому, например, интерфейс eth1-1.1 нового активного узла продолжит работу с теми же параметрами, с которыми ранее работал интерфейс eth1-1.1 предыдущего активного узла кластера. Это обеспечивается, только если оба устройства, их интерфейсы и их нумерация идентичны.

Обязательным условием для формирования и работы кластера является соединение двух межсетевых экранов между собой через Sync-link.

Схемы соединения моделей PT NGFW 1005, PT NGFW 1010, PT NGFW 1020 и PT NGFW 1050

В моделях PT NGFW 1005, PT NGFW 1010, PT NGFW 1020 и PT NGFW 1050 для Sync-link может использоваться один интерфейс.

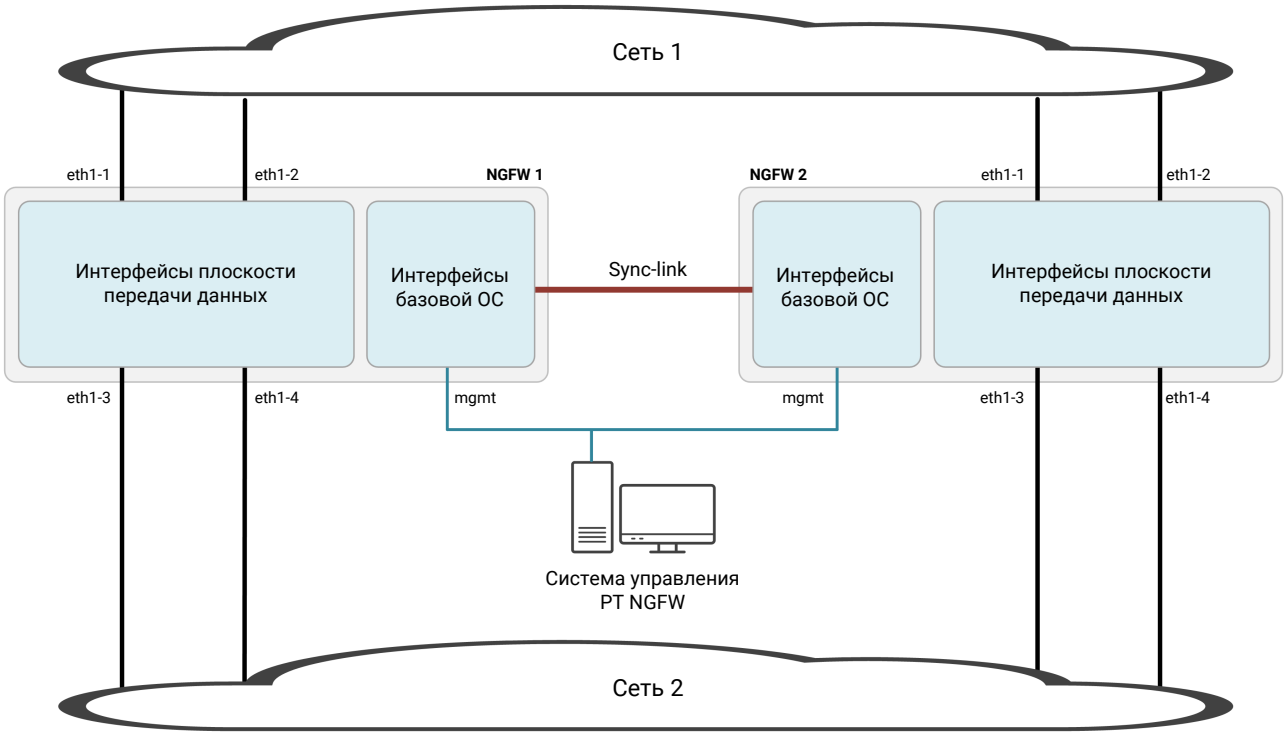


Рисунок 250. Схема распределения интерфейсов моделей PT NGFW 1005, 1010, 1020 и 1050

Примечание. Интерфейс mgmt на рисунке — это выделенный интерфейс для подключения к системе управления.

В модели PT NGFW 1005 для Sync-link используется интерфейс № 4.

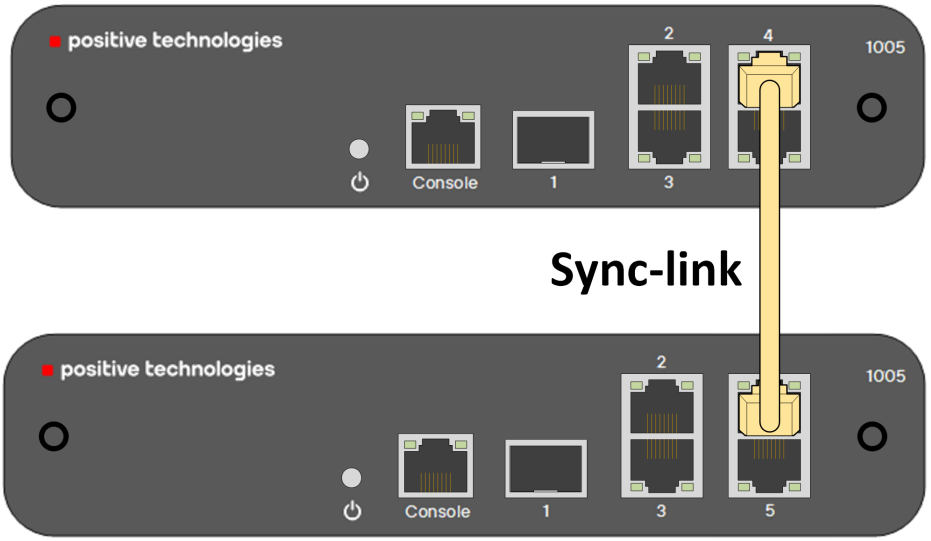


Рисунок 251. Соединение интерфейсов PT NGFW 1005 для формирования Sync-link

В модели PT NGFW 1010 для Sync-link используется интерфейс № 7.

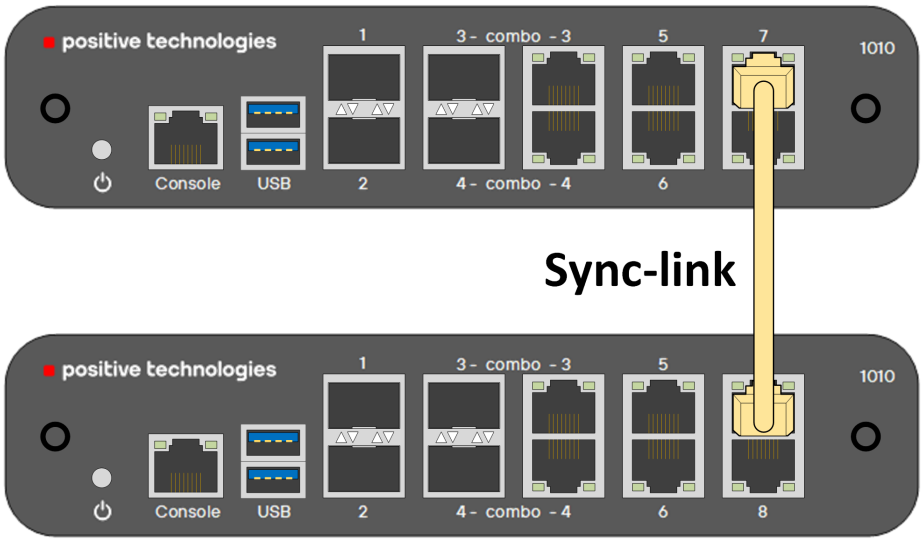


Рисунок 252. Соединение интерфейсов PT NGFW 1010 для формирования Sync-link

В модели PT NGFW 1020 для Sync-link используется интерфейс № 2.

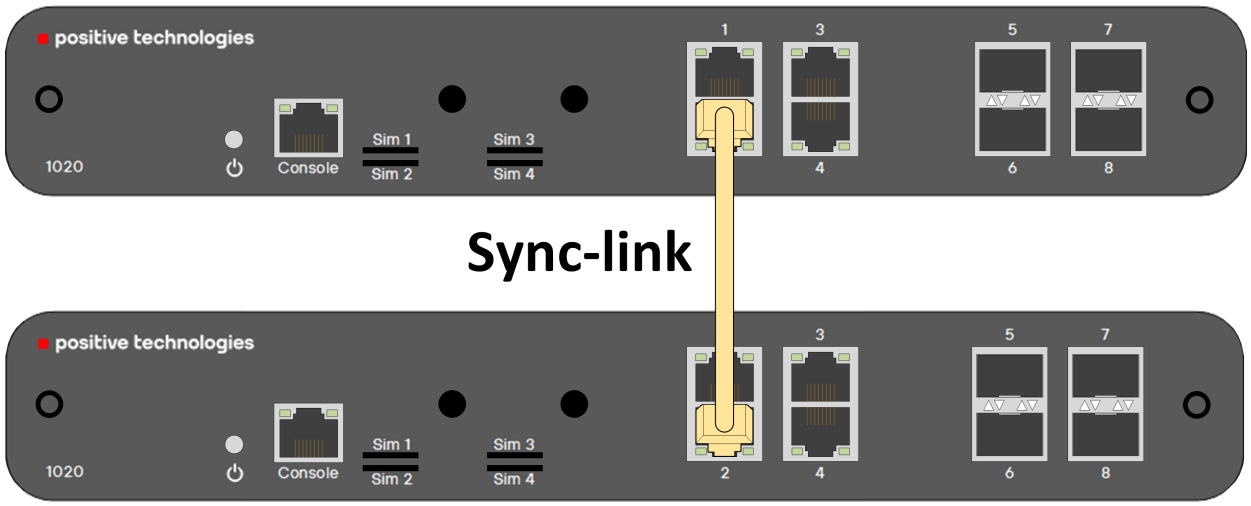


Рисунок 253. Соединение интерфейсов PT NGFW 1020 для формирования Sync-link

В модели PT NGFW 1050 для Sync-link используется интерфейс № 2.

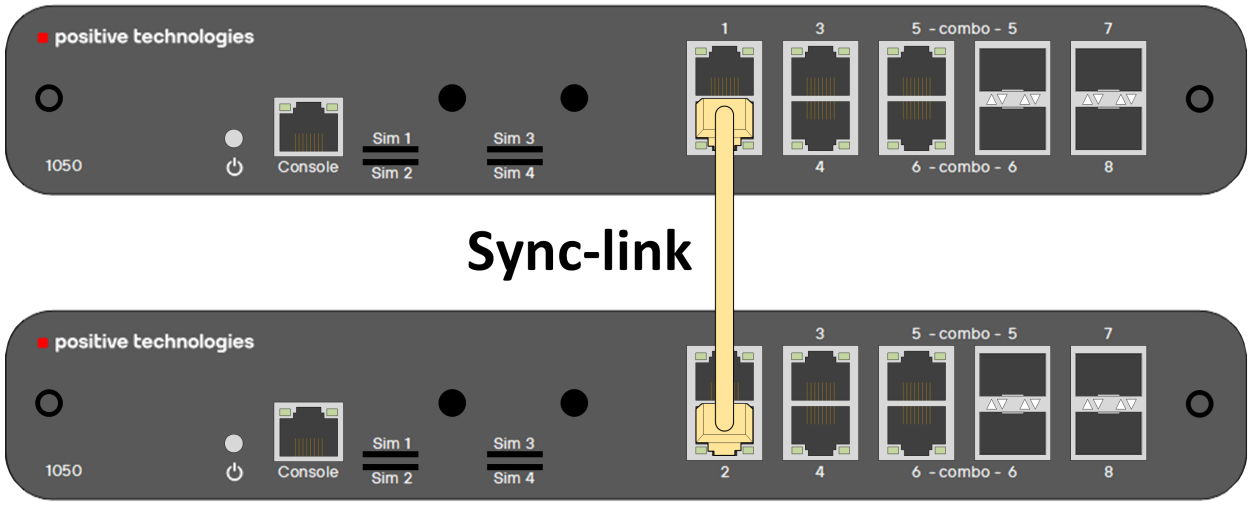


Рисунок 254. Соединение интерфейсов PT NGFW 1050 для формирования Sync-link

Схемы соединения моделей PT NGFW 2010, 2020, 2050, 3010, 3040 и 3050

В моделях PT NGFW 2010, 2020, 2050, 3010, 3040 и 3050 в слоте № 2 (маркировка OCP0_1 на передней панели) установлена интерфейсная карта с четырьмя интерфейсами 10/100/1000Base-T RJ-45.

Для формирования Sync-link следует использовать интерфейс № 3 или № 4.

Внимание! Одновременное использование двух каналов Sync-link не поддерживается.

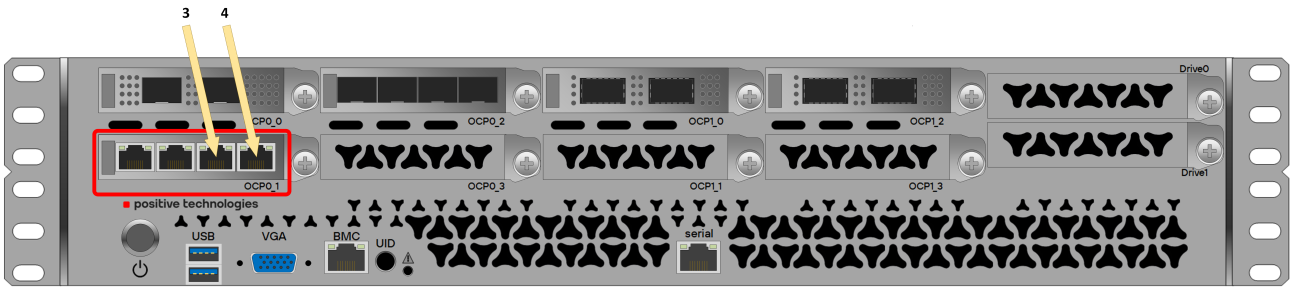


Рисунок 255. Интерфейсы, используемые для формирования Sync-link в моделях PT NGFW 2010, 2020, 2050, 3010, 3040 и 3050

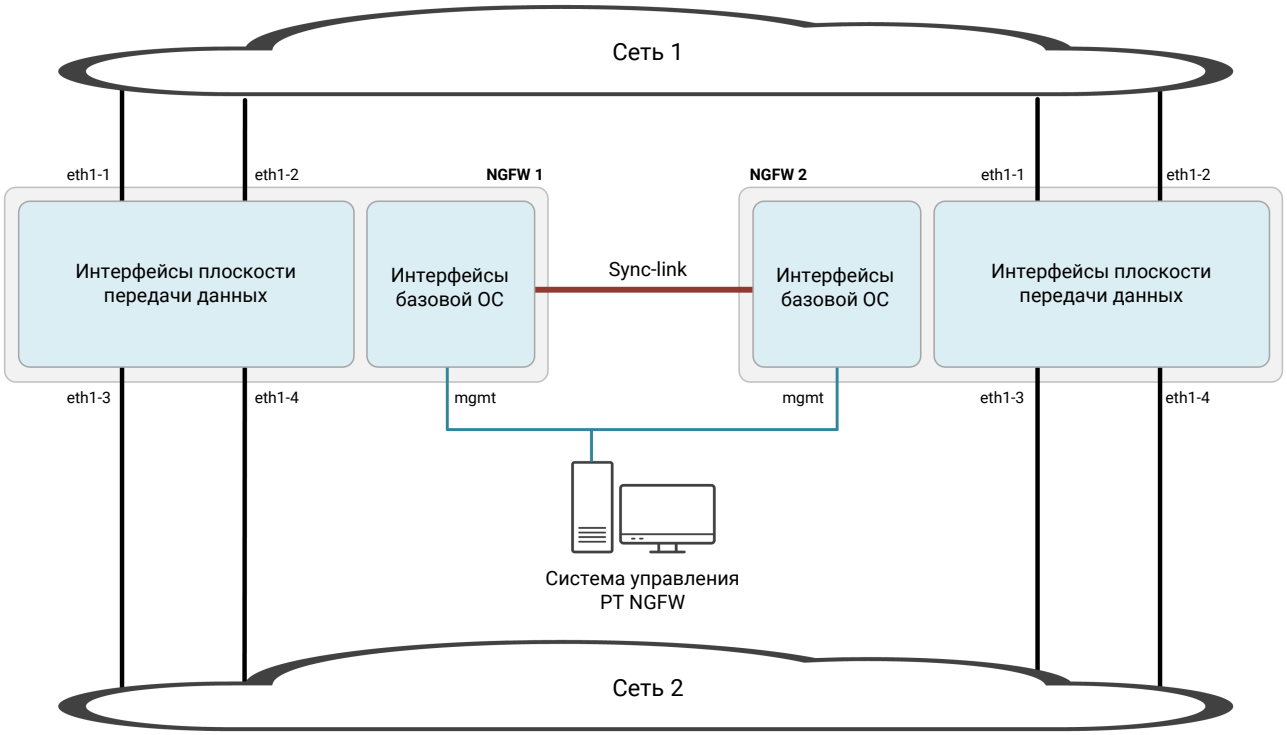


Рисунок 256. Схема распределения интерфейсов моделей PT NGFW 2010, 2020, 2050, 3010, 3040 и 3050

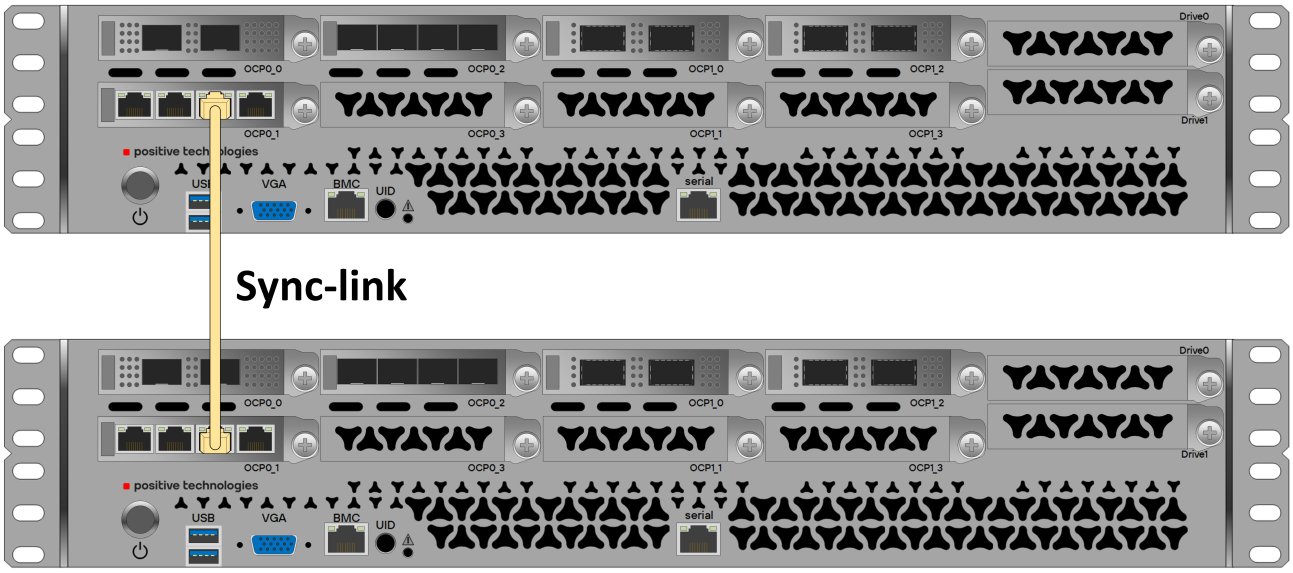


Рисунок 257. Соединение интерфейсов PT NGFW 2010, 2020, 2050, 3010, 3040 и 3050 для формирования Sync-link

При этом в связи с тем, что для Sync-link используются интерфейсы, работающие в пространстве базовой операционной системы (Linux), то интерфейсы № 3 и № 4 слота № 2 можно объединить в агрегированный групповой интерфейс (LAG, bond) средствами базовой

ОС. С точки зрения системы управления PT NGFW такой агрегированный интерфейс выглядит как один интерфейс. Такое соединение обеспечивает лучшую отказоустойчивость в случае выхода из строя одного из интерфейсов или Sync-link, связывающего интерфейсы.

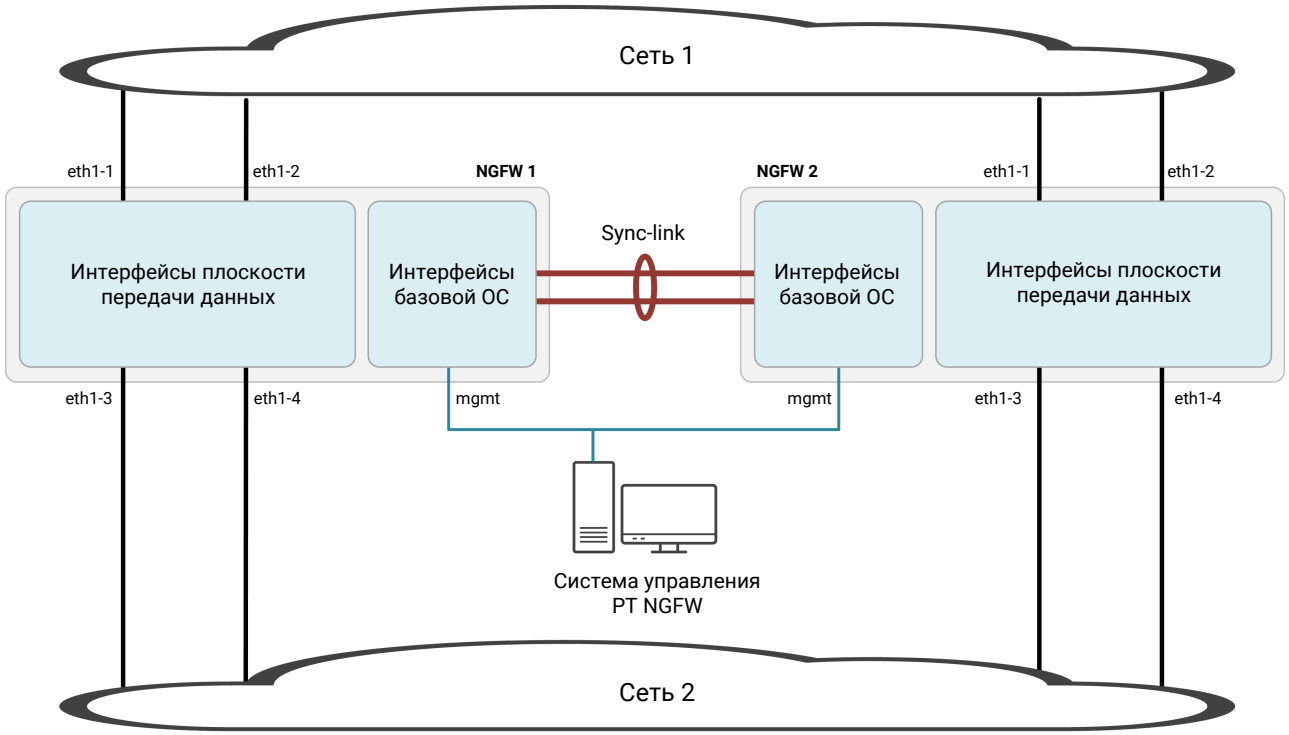


Рисунок 258. Схема распределения интерфейсов моделей PT NGFW 2010, 2020, 2050, 3010, 3040 и 3050 при объединении интерфейсов Sync-link в агрегированную группу

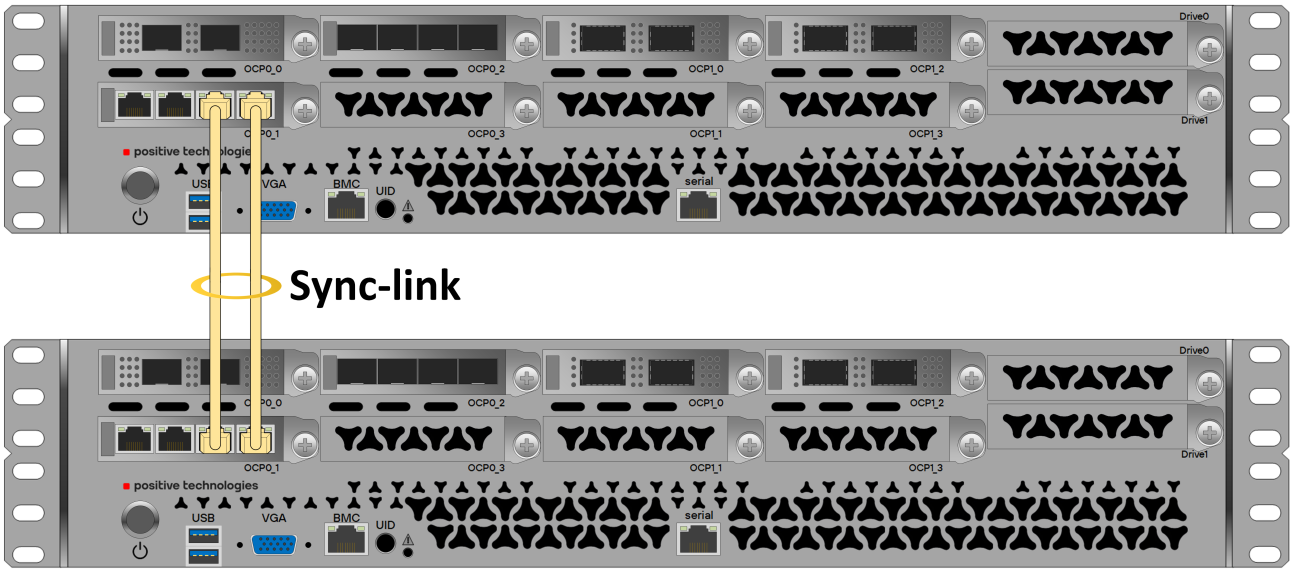


Рисунок 259. Соединение интерфейсов PT NGFW 2010, 2020, 2050, 3010, 3040 и 3050 для формирования Sync-link при объединении интерфейсов канала синхронизации в агрегированную группу

См. также

Изменение имени хоста (hostname) (см. раздел 5.3.1)

30.11. Создание кластера

После соединения двух моделей устройств будущего кластера в соответствии с требованиями к созданию кластера active-standby (см. раздел 30.10) необходимо настроить IP-адреса на интерфейсах каждого из устройств, а затем настроить кластер в системе управления.

Настройка IP-адресов на устройствах

- Чтобы настроить конфигурацию на устройствах:

1. Настройте IP-адреса на сетевых интерфейсах, которые будут формировать Sync-link каждого из устройств PT NGFW будущего кластера:

   - В командном интерфейсе базовой ОС проверьте текущие адреса и имена интерфейсов:

     ```
     ngfw@LAB-Debian-ngfw-node-1:~$ ip a
     1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
     1000
         link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
         inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
     2: mgmt1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
     default qlen 1000
         link/ether 00:50:56:94:35:9e brd ff:ff:ff:ff:ff:ff
         altname enp3s0
         inet 10.0.0.144/24 brd 10.13.107.255 scope global mgmt1
            valid_lft forever preferred_lft forever
     3: sync1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
     default qlen 1000
         link/ether 00:50:56:94:a3:b4 brd ff:ff:ff:ff:ff:ff
         altname enp4s0
         inet 192.168.250.1/24 brd 192.168.250.255 scope global sync1
            valid_lft forever preferred_lft forever
     ```

     В этом примере интерфейсом будущего Sync-link является интерфейс `sync1`, а интерфейс `mgmt1` — это выделенный интерфейс для управления устройством PT NGFW (MGMT-интерфейс).

2. Настройте IP-адрес, создав конфигурационный файл с параметрами интерфейса `sync1` каждого из устройств будущего кластера (настройка интерфейса управления и интерфейса Sync-link осуществляется через подсистему systemd):

   Для node-1:

   ```
   ngfw@LAB-Debian-ngfw-node-1:~$ cd /etc/systemd/network/
   ```

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo nano 10-sync1.network
[Match]
Name=sync1


[Network]
Address=192.168.250.1/24
```

3. Нажмите Ctrl+O (write out) для сохранения изменений, а затем — Ctrl+X для выхода из редактора nano.
4. Перезапустите сервис, чтобы изменения вступили в силу:

   ```
   ngfw@LAB-Debian-ngfw-node-1:~$ sudo systemctl restart systemd-networkd
   ```

   Для node-2:

   ```
   ngfw@LAB-Debian-ngfw-node-2:~$ cd /etc/systemd/network/


   ngfw@LAB-Debian-ngfw-node-2:~$ sudo nano 10-sync1.network
   [Match]
   Name=sync1


   [Network]
   Address=192.168.250.2/24
   ```

5. Нажмите Ctrl+O (write out) для сохранения изменений, а затем — Ctrl+X для выхода из редактора nano.
6. Перезапустите сервис, чтобы изменения вступили в силу:

   ```
   ngfw@LAB-Debian-ngfw-node-2:~$ sudo systemctl restart systemd-networkd
   ```

   В примере выше интерфейсы Sync-link находятся в одной IP-подсети (в одном домене широковещательной рассылки). Адреса 192.168.250.1/24 и 192.168.250.2/24 указаны только в качестве примера и в вашем случае могут быть другими согласно вашей сетевой топологии.

   Sync-link кластера PT NGFW — это L3-соединение. PT NGFW поддерживает сценарий, в котором интерфейсы канала синхронизации могут находиться в разных IP-подсетях. В этом случае в параметры интерфейса синхронизации необходимо добавить статический маршрут, указав соответствующий адрес шлюза, через который осуществляется доступ к интерфейсу синхронизации второго узла, например:

   ```
   [Route]
   Destination=<адрес или подсеть интерфейса Sync-link другого узла>
   Gateway=<адрес шлюза>
   ```

7. Проверьте, вступили ли в силу изменения по настройке IP-адреса интерфейса Sync-link:

   Для node-1:

   ```
   ngfw@LAB-Debian-ngfw-node-1:~$ ip a
   . . .r
   ```

```
3: sync1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 00:50:56:94:a3:b4 brd ff:ff:ff:ff:ff:ff
    altname enp4s0
    inet 192.168.250.1/24 brd 192.168.250.255 scope global sync1
       valid_lft forever preferred_lft forever
```

Для node-2:

```
ngfw@LAB-Debian-ngfw-node-2:~$ ip a
. . .
3: sync1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group
default qlen 1000
    link/ether 00:50:56:94:83:3f brd ff:ff:ff:ff:ff:ff
    altname enp4s0
    inet 192.168.250.2/24 brd 192.168.250.255 scope global sync1
       valid_lft forever preferred_lft forever
```

Настройка кластера в системе управления

- Чтобы настроить кластер в системе управления:

1. На странице **Устройства** → **Кластеры** нажмите **Добавить кластер**.

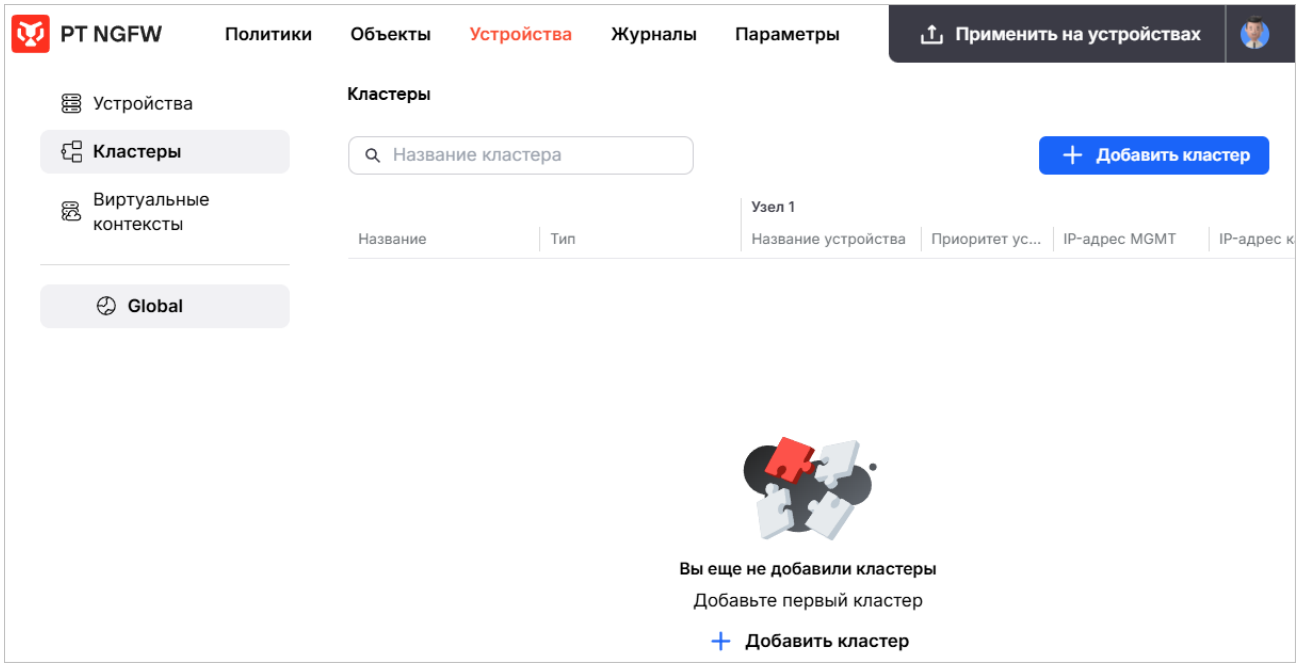


Рисунок 260. Добавление кластера

2. Введите название кластера.

   Примечание. Рекомендуется добавлять описание для упрощения последующей работы с кластером.

3. Нажмите **Добавить**, чтобы выбрать устройства, из которых будет состоять кластер.

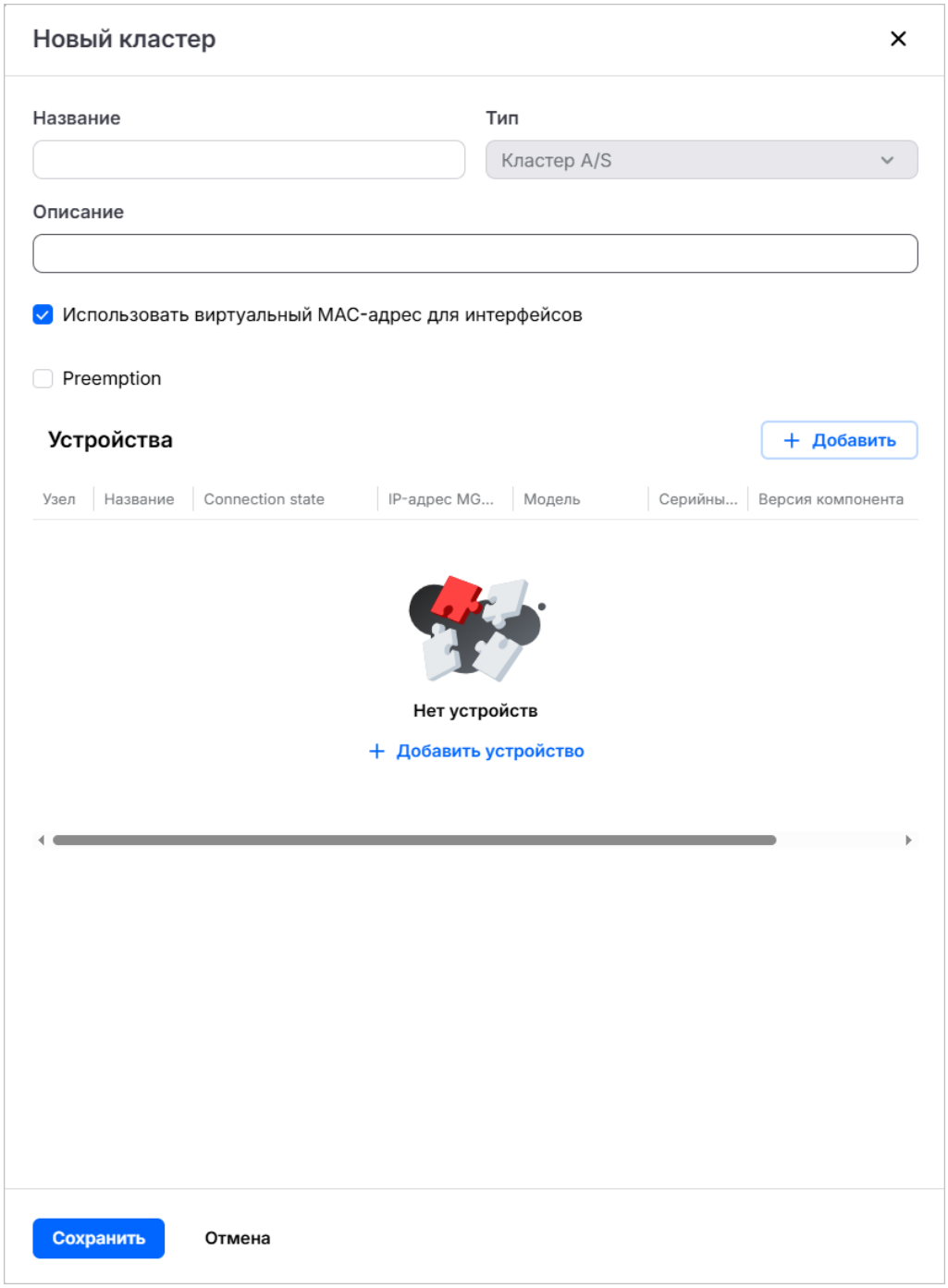


Рисунок 261. Ввод названия и описания кластера

4. Выберите не более двух устройств, которые хотите добавить в кластер.

   Поддерживается возможность создания кластера, состоящего только из одного узла. Второй узел может быть добавлен позже.

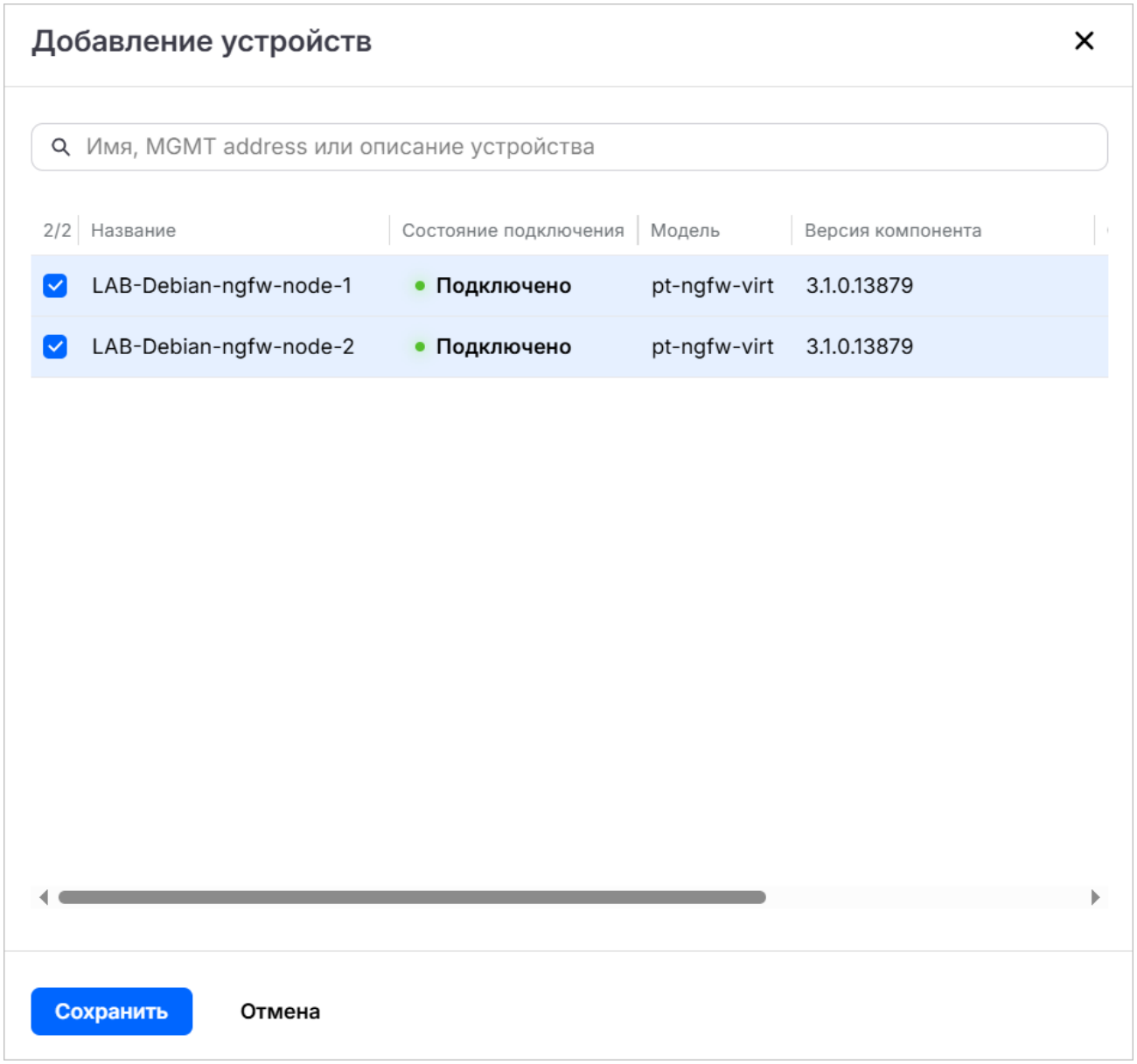


Рисунок 262. Выбор устройств для объединения в кластер

5. Нажмите **Сохранить**.
6. Настройте параметры кластера:
   - Если вы хотите использовать виртуальный MAC-адрес, установите соответствующий флажок.

     Если параметр включен, то одноименные интерфейсы узлов кластера используют одинаковые MAC-адреса (виртуальные MAC-адреса) из пула 0E-00-5E-xx-xx-xx. Если параметр выключен, то на интерфейсах каждого из устройств кластера используются их реальные MAC-адреса.

- Если вы хотите, чтобы кластер работал в режиме приоритетного замещения (Preemption), установите соответствующий флажок.
- Выберите источник начальной конфигурации.

  Примечание. При первоначальной настройке кластера может возникнуть ситуация, при которой одно из устройств, объединяемых в кластер, уже работает в сети, имеет определенную конфигурацию, и требуется, чтобы эта конфигурация сохранилась и далее использовалась в кластере.

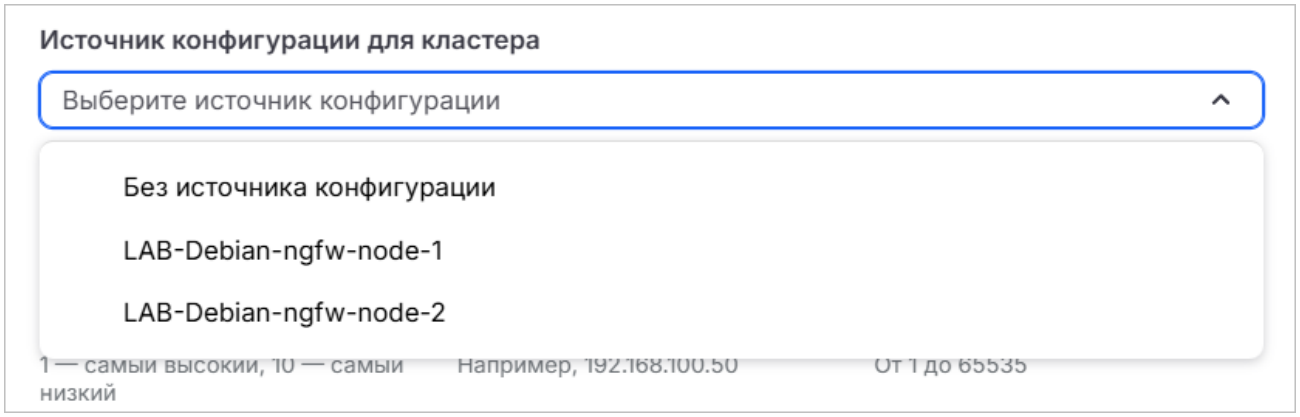


Рисунок 263. Выбор источника конфигурации

Примечание. При выборе **Без источника конфигурации** кластер после успешного формирования будет иметь чистую конфигурацию без каких-либо настроенных параметров.

- Установите приоритет узла в кластере.
- Укажите IP-адрес интерфейса Sync-link.

  Необходимо указать адрес, который был указан при настройке IP-адресов интерфейсов базовой ОС. В примере выше это интерфейсы sync1 и адреса 192.168.250.1 для узла NGFW1 и 192.168.250.2 для узла NGFW2.
- Введите номер порта Sync-link.

  В этом поле указан номер TCP-порта Sync-link. По умолчанию указано значение 5650. Изменение этого значения в большинстве случаев не требуется, но такая необходимость может возникнуть, если между интерфейсами Sync-link расположено фильтрующее устройство, на котором настроена блокировка соединений в адрес порта TCP/5650.

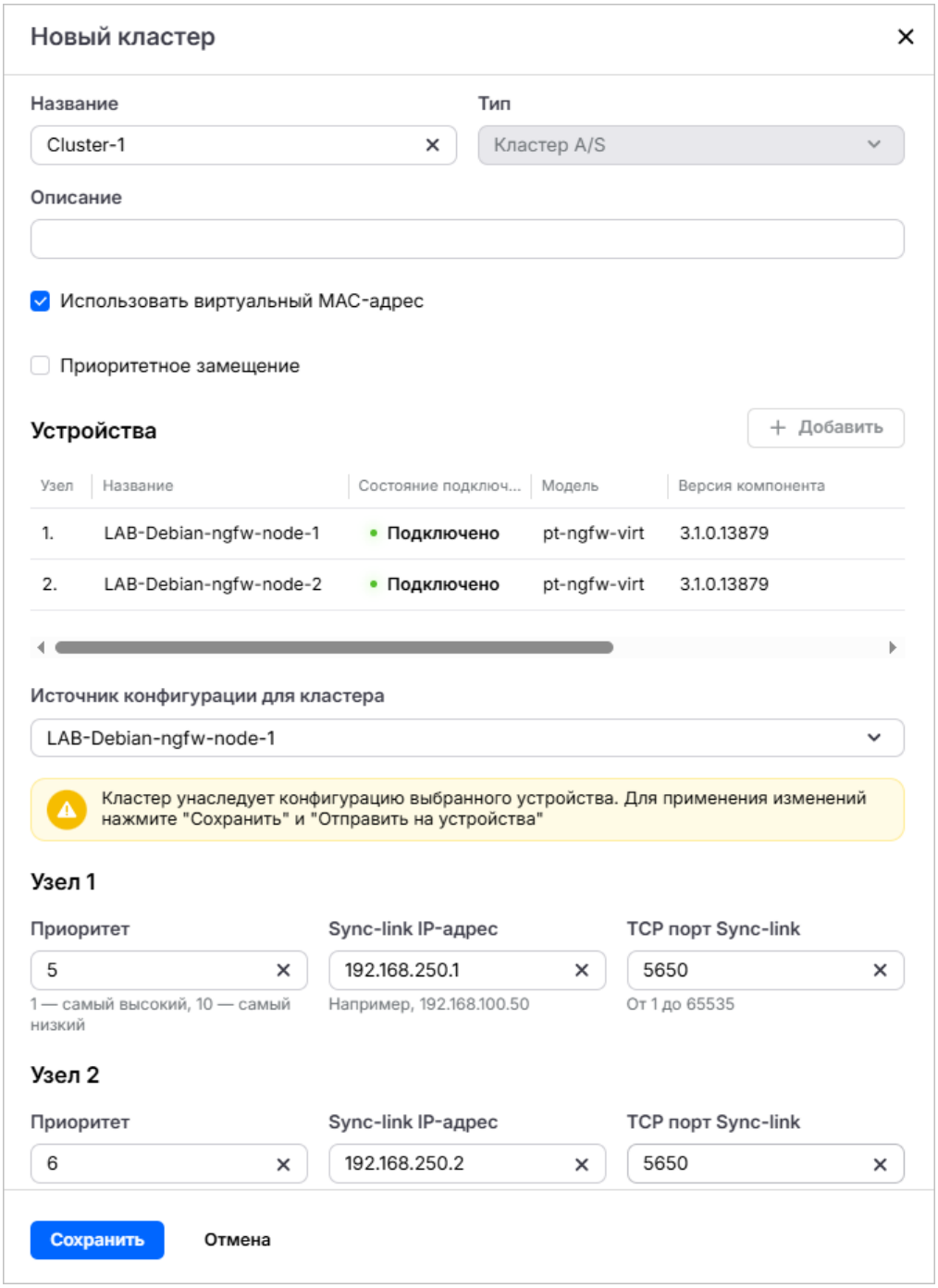


Рисунок 264. Параметры кластера

Примечание. На этом этапе, то есть пока конфигурация не сохранена, вы можете удалить узел из создаваемого кластера. В этом случае конфигурация устройства, которое вы удалили из кластера, не изменится, то есть останется такой, которой она была до добавления устройства.

7. Нажмите **Сохранить**.

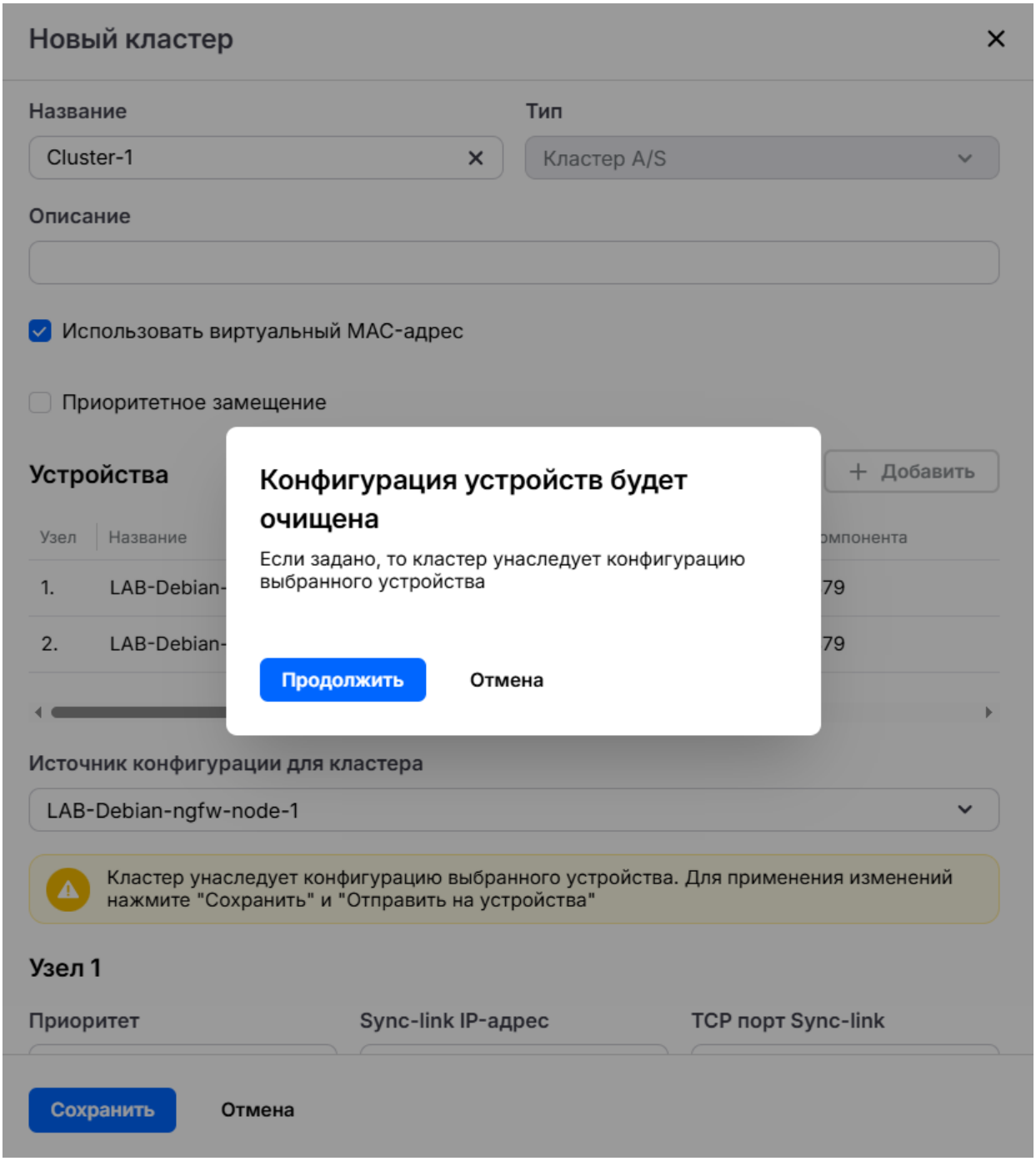


Рисунок 265. Предупреждение о конфигурации устройств

Примечание. Если удалить одно из устройств после сохранения формы создания кластера, то конфигурация этого устройства будет очищена. В настоящее время исходная конфигурация устройства, то есть та конфигурация, которая на нем присутствовала на момент добавления в кластер, не сохраняется. При удалении кластера его конфигурацию можно будет сохранить на второе, оставшееся устройство кластера.

Вы можете просмотреть параметры созданного кластера, выбрав его в списке на странице **Устройства** → **Кластеры**.

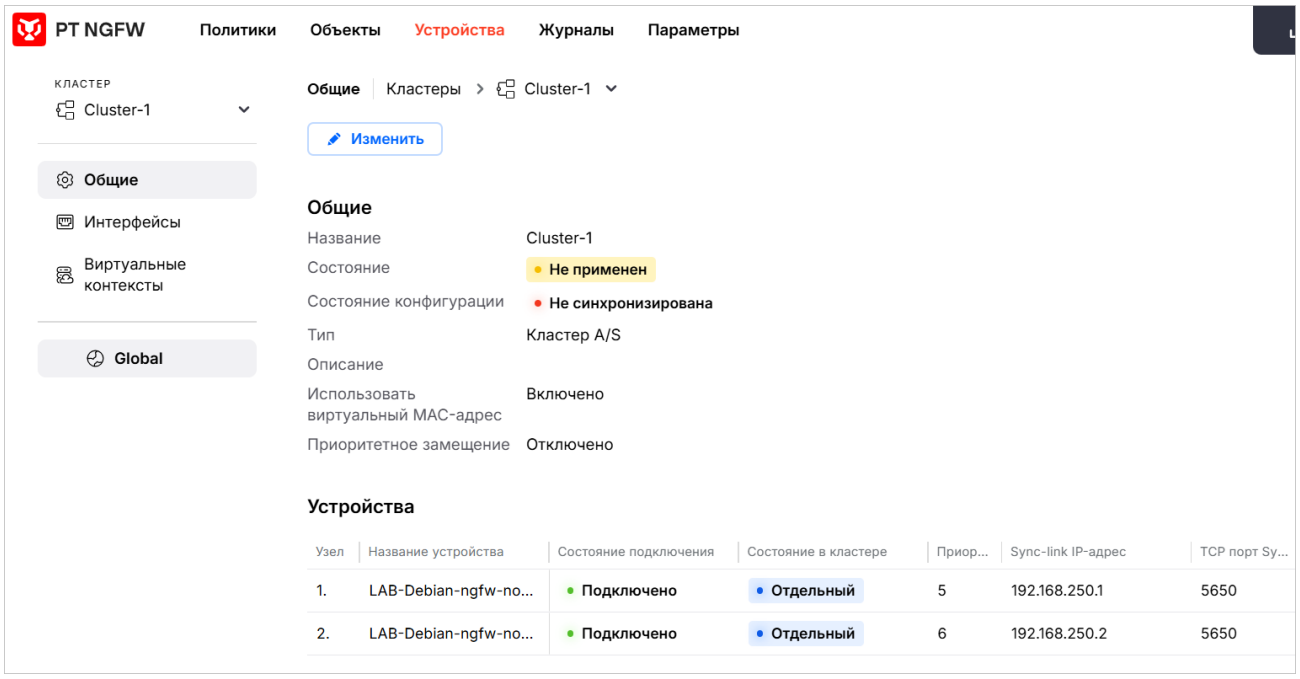


Рисунок 266. Общие параметры созданного кластера, состояние **Pending**

8. Нажмите **Отправить на устройства** для применения конфигурации.

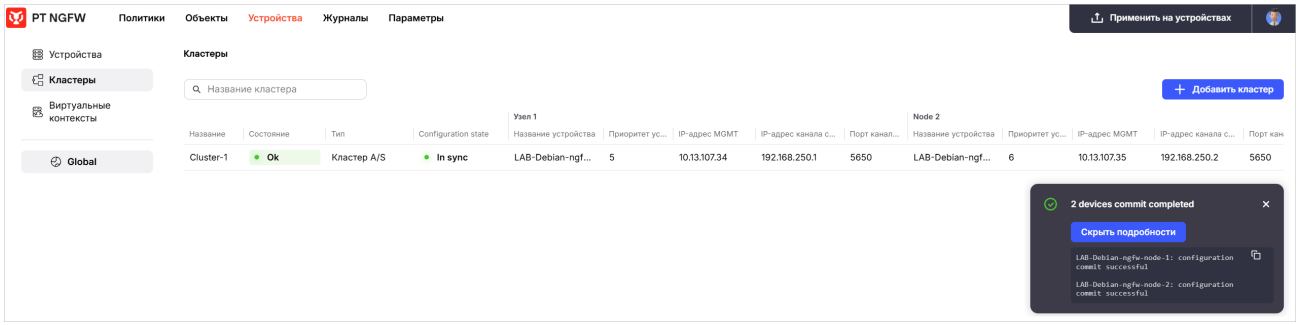


Рисунок 267. Применение конфигурации кластера

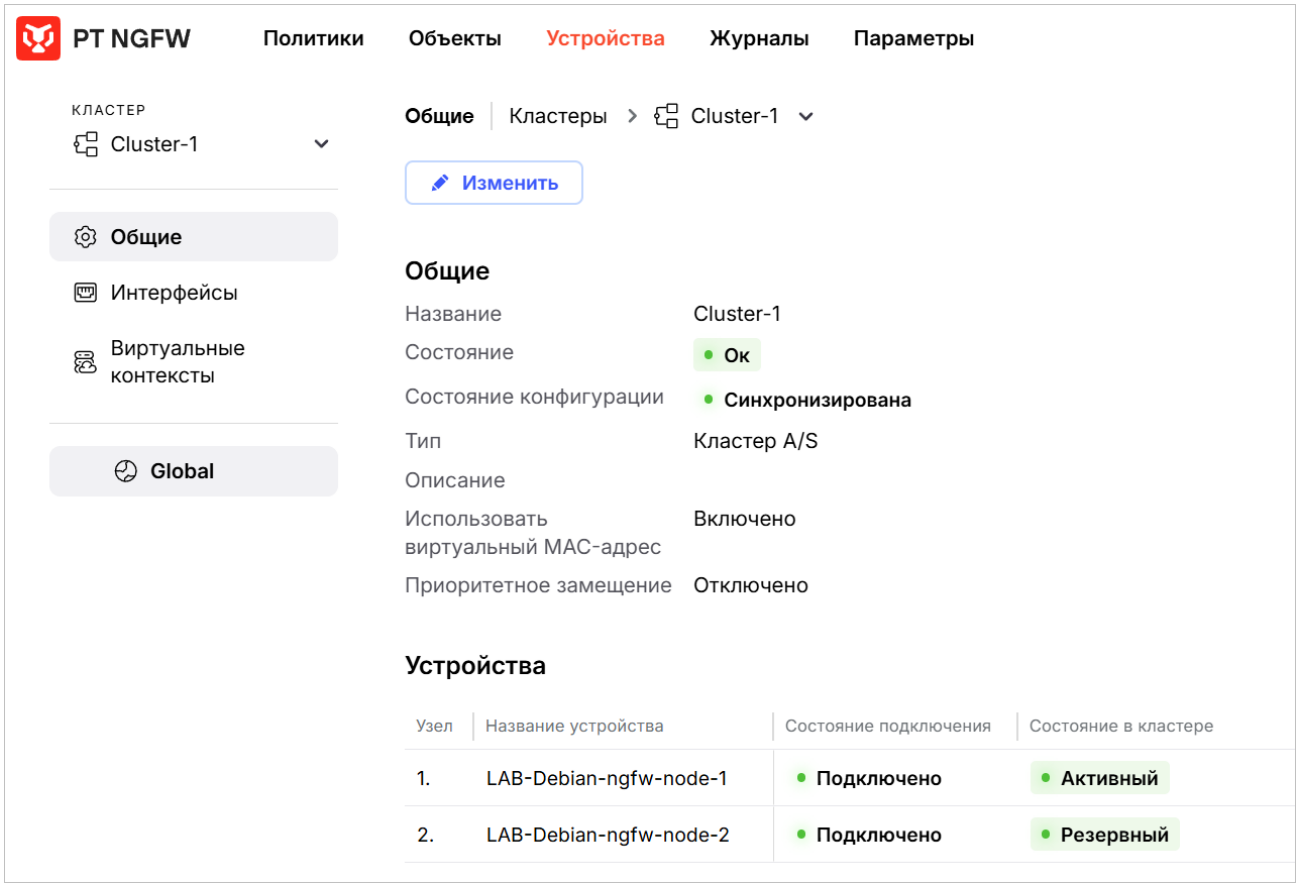


Рисунок 268. Общие параметры созданного кластера, состояние **Ok**

30.12. Процесс объединения узлов в кластер

После того как администратор завершил конфигурирование кластера и применил изменения, нажав **Отправить на устройства** (см. раздел «Создание кластера (см. раздел 30.11)»), система управления отправляет конфигурацию на оба устройства.

В конфигурации, среди прочего, указан идентификатор кластера и идентификаторы каждого из узлов, объединяемых в кластер.

Объединение узлов в кластер происходит следующим образом:

1. Узлы устанавливают канал синхронизации:
   - Каждый из узлов пытается установить соединение и выполнить рукопожатие в течение времени timeout (60 секунд). Попытки соединения повторяются через каждые пять секунд. Если в течение времени timeout не удалось выполнить рукопожатие, то каждый

из узлов остается в прежнем состоянии (отдельный узел, standalone) с прежними параметрами, а в систему управления возвращается ошибка о неуспешном применении конфигурации. Кластер не формируется.

- Если процедура рукопожатия успешна, а именно: установлено сетевое соединение, совпали идентификаторы кластера, ответ пришел от узла с идентификатором, который указан в конфигурации, совпали остальные параметры, то между узлами формируется канал синхронизации Sync-link. На этом шаге конфигурация еще не считается примененной окончательно. Узлы переходят к следующему шагу.

2. Оба узла переходят в состояние «Резервный (Standby)», после чего стартует процедура голосования, в ходе которой узлы обмениваются информацией о своем текущем состоянии, сравнивают приоритеты, значения метрик здоровья и выбирают активный узел. Если ни один из узлов не смог полностью применить конфигурацию, то в систему управления возвращается ошибка о неуспешном применении конфигурации. Кластер не формируется и узлы возвращаются в свое исходное некластерное состояние.
3. Итогом голосования может быть одно из двух состояний кластера:
   - «Активный (Active)» и «Резервный (Standby)» узлы;
   - «Активный (Active)» и «Резервный · Ошибка (Standby · Fatal-Error)», в случае если ему не удалось применить конфигурацию.

Алгоритм формирования кластера представляет собой транзакцию, препятствующую переходу любого из узлов или всего кластера в рассогласованное состояние. Кластер либо формируется целиком, либо не формируется вообще, и узлы возвращаются в исходное состояние с исходной конфигурацией, в котором над ними сохраняется управление, и они продолжают передавать трафик, если это предусматривалось исходной конфигурацией.

Преимущества алгоритма формирования кластера PT NGFW:

— В ходе формирования кластера между узлами может отсутствовать связь через Sync-link, например, если администратор допустил ошибку, указав неверные адреса, если произошел сбой (повреждение) канала связи или блокирование трафика промежуточным сетевым устройством. В текущем подходе каждый из узлов, будучи неспособным связаться с соседом, вернется в свое исходное состояние, о чем уведомит систему управления. После этого администратор может устранить ошибку и повторить сборку кластера.

— При ином подходе каждый из узлов, не получив ответа от соседа в течение timeout и «решив», что второй узел еще не подключен, выключен или не существует, перешел бы в состояние «активный», что в итоге привело бы к состоянию Split-brain (см. раздел 30.16). В таком состоянии каждый узел рассылает сообщения GARP, перетягивая на себя трафик, что может привести к его потерям в сети.

— В ситуации, когда один узел успешно применил конфигурацию и перешел в состояние активного, а второй перешел в состояние «Резервный · Ошибка (Standby · Fatal-Error)», между узлами есть связь через Sync-link, сохраняется управление узлами, однако резервный узел требует внимания администратора для выяснения причин неуспешности применения конфигурации.

Примечание. В PT NGFW поддерживается возможность создания кластера, в который входит только один узел. В этом случае, при получении конфигурации узел фиксирует, что в ней указан только он один в составе кластера и сразу переходит к применению конфигурации, не выполняя попыток установки канала синхронизации Sync-link. После успешного применения конфигурации узел сразу переходит в состояние активного.

Пример записей системного журнала

После получения конфигурации узел NGFW1 устанавливает сетевую сессию с другим узлом кластера и начинает процедуру рукопожатия:

```
[2025-07-23 13:44:33.724852] [cluster][Cluster][2518] [info] initializing AS cluster started [state: Standalone commit_id: 019836f1-9b2e-74fb-8f1e-8766fec2d3f2]
[2025-07-23 13:44:33.724869] [cluster][Cluster][2518] [info] AS cluster sync link initialization started
[2025-07-23 13:44:33.726662] [cluster][Cluster][2513] [info] Peer versions: 14.0,15.0
[2025-07-23 13:44:33.726695] [cluster][Cluster][2513] [info] Selected version: 15.0
[2025-07-23 13:44:33.726708] [cluster][Cluster][2513] [info] peer connected [conn='192.168.250.1:5650'<->'192.168.250.2:5650']
[2025-07-23 13:44:33.737253] [cluster][Cluster][2518] [info] sync link is ready [state: Standalone peer_state: Standalone]
```

После успешного рукопожатия NGFW1 применяет у себя конфигурацию (узел NGFW1 является ведущим), переходит в состояние Standby (резервный), отдает команду второму узлу на применение конфигурации. Конфигурация на соседнем узле также успешно применена:

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log
[2025-07-23 13:44:33.737278] [cluster][Cluster][2518] [info] configuring device as 'Standby'
[2025-07-23 13:44:33.922189] [cluster][Cluster][2518] [info] change state [state: 'Standalone' new_state: 'Standby' reason: 'successful configuration']
[2025-07-23 13:44:33.922202] [cluster][Cluster][2518] [info] configuration has been applied [state: Standby commit_id: 019836f1-9b2e-74fb-8f1e-8766fec2d3f2]
[2025-07-23 13:44:34.115238] [cluster][Cluster][2518] [info] Configuration has been successfully applied on peer [commit_id=019836f1-9b2e-74fb-8f1e-8766fec2d3f2]
```

Узлы перешли к процедуре голосования и сравнению значений метрик здоровья. В записях журнала видно, что узел NGFW1 перешел в статус «активный», так как его приоритет оказался выше (меньшее числовое значение):

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log
[2025-07-23 13:44:34.115489] [cluster][Cluster][2518] [info] Do vote...
[2025-07-23 13:44:34.115506] [cluster][Cluster][2518] [info] compare metrics
[2025-07-23 13:44:34.115515] [cluster][Cluster][2518] [info] self metrics [count=2]
[2025-07-23 13:44:34.115522] [cluster][Cluster][2518] [info] metric [prio=1, name='port_eth1-1', state='ok']
[2025-07-23 13:44:34.115528] [cluster][Cluster][2518] [info] metric [prio=2, name='port_eth1-2', state='ok']
[2025-07-23 13:44:34.115534] [cluster][Cluster][2518] [info] peer metrics [count=2]
[2025-07-23 13:44:34.115540] [cluster][Cluster][2518] [info] metric [prio=1, name='port_eth1-1', state='ok']
[2025-07-23 13:44:34.115547] [cluster][Cluster][2518] [info] metric [prio=2, name='port_eth1-2', state='ok']
```

```
[2025-07-23 13:44:34.115554] [cluster][Cluster][2518] [info] can't select role by
metrics
[2025-07-23 13:44:34.115561] [cluster][Cluster][2518] [info] Vote result
[node='Standby->Active' peer='Standby->Standby' reason='active node has been selected
by priority']
[2025-07-23 13:44:34.115568] [cluster][Cluster][2518] [info] change state [state:
'Standby' new_state: 'Active' reason: 'Vote result']
[2025-07-23 13:44:34.115973] [cluster][Cluster][2518] [info] send configuration to
standby [commit_id: 019836f1-9b2e-74fb-8f1e-8766fec2d3f2]
[2025-07-23 13:44:34.699441] [cluster][Cluster][2518] [info] Configuration has been
successfully applied on peer [commit_id=019836f1-9b2e-74fb-8f1e-8766fec2d3f2]
```

Рукопожатие из записей журнала узла NGFW2:

```
ngfw@LAB-Debian-ngfw-node-2:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-07-23 13:44:34.286124] [cluster][Cluster][43047] [info] initializing AS cluster
started [state: Standalone commit_id: 019836f1-9b2e-74fb-8f1e-8766fec2d3f2]
[2025-07-23 13:44:34.286140] [cluster][Cluster][43047] [info] AS cluster sync link
initialization started
[2025-07-23 13:44:34.287777] [cluster][Cluster][43044] [info] Peer versions:
14.0,15.0
[2025-07-23 13:44:34.287808] [cluster][Cluster][43044] [info] Selected version: 15.0
[2025-07-23 13:44:34.287820] [cluster][Cluster][43044] [info] peer connected
[conn='192.168.250.2:5650'<->'192.168.250.1:5650']
[2025-07-23 13:44:34.298175] [cluster][Cluster][43047] [info] sync link is ready
[state: Standalone peer_state: Standalone]
```

Узел NGFW2 перешел в состояние Standby, прежде чем применил конфигурацию, и остался в этом состоянии по результатам ее успешного применения:

```
ngfw@LAB-Debian-ngfw-node-2:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log
[2025-07-23 13:44:34.484436] [cluster][Cluster][43047] [info] Configuration has been
successfully applied on peer [commit_id=019836f1-9b2e-74fb-8f1e-8766fec2d3f2]
[2025-07-23 13:44:34.484486] [cluster][Cluster][43047] [info] configuring device as
'Standby'
[2025-07-23 13:44:34.674056] [cluster][Cluster][43047] [info] change state [state:
'Standalone' new_state: 'Standby' reason: 'successful configuration']
[2025-07-23 13:44:34.674070] [cluster][Cluster][43047] [info] configuration has been
applied [state: Standby commit_id: 019836f1-9b2e-74fb-8f1e-8766fec2d3f2]
[2025-07-23 13:44:34.677968] [cluster][Cluster][43047] [info] configuring AS cluster
started [state: Standby commit_id: 019836f1-9b2e-74fb-8f1e-8766fec2d3f2]
[2025-07-23 13:44:34.677982] [cluster][Cluster][43047] [info] configuring device as
'Standby'
```

Один из узлов после применения у себя конфигурации еще раз инициирует процедуру голосования, так как в результате применения конфигурации могли измениться какие-либо параметры, например, приоритетов узлов в кластере, отслеживаемые интерфейсы. По результатам голосования роли узлов не изменились. Это видно в журнале NGFW1:

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-07-23 13:45:33.922528] [cluster][Cluster][2518] [info] Do vote...
[2025-07-23 13:45:33.922588] [cluster][Cluster][2518] [info] compare metrics
```

```
[2025-07-23 13:45:33.922598] [cluster][Cluster][2518] [info] self metrics [count=2]
[2025-07-23 13:45:33.922607] [cluster][Cluster][2518] [info] metric [prio=1,
name='port_eth1-1', state='ok']
[2025-07-23 13:45:33.922614] [cluster][Cluster][2518] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-07-23 13:45:33.922620] [cluster][Cluster][2518] [info] peer metrics [count=2]
[2025-07-23 13:45:33.922626] [cluster][Cluster][2518] [info] metric [prio=1,
name='port_eth1-1', state='ok']
[2025-07-23 13:45:33.922633] [cluster][Cluster][2518] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-07-23 13:45:33.922640] [cluster][Cluster][2518] [info] can't select role by
metrics
[2025-07-23 13:45:33.922647] [cluster][Cluster][2518] [info] Vote result
[node='Active->Active' peer='Standby->Standby' reason='nothing changed']
```

30.13. Изменение параметров кластера

При получении обновленной конфигурации, в которой среди прочих изменились параметры канала синхронизации Sync-link (адреса, порты), активный узел пересылает ее на резервный. Затем, прежде чем применить конфигурацию, узлы проверяют, сохранится ли связность через Sync-link, если применить новые параметры. В новой конфигурации изменились IP-адреса интерфейсов Sync-link и (или) значения TCP-портов и другие параметры, влияющие на связность через Sync-link. Устройства кластера выполняют тестовое соединение через Sync-link, используя новые параметры. Если соединение неуспешно, то применение конфигурации не выполняется, устройства кластера остаются с прежними параметрами, а в адрес системы управления направляется сообщение об ошибке применения конфигурации.

Такой подход позволяет предотвратить потерю связи через Sync-link в случае ошибок в конфигурации, например, если администратор ввел некорректные значения новых IP-адресов интерфейсов Sync-link или других параметров, влияющих на сетевую связность.

Если узлы фиксируют, что связь через Sync-link не потеряется, то выполняется применение конфигурации. В случае, если активный узел не смог ее применить, то он отправляет на резервный узел команду отмены, и устройства кластера остаются с прежними параметрами, а в адрес системы управления направляется сообщение об ошибке.

При успешном применении новых параметров активный узел еще раз пересылает на резервный узел конфигурацию вместе с командой на ее применение. Резервный узел, получив конфигурацию от активного устройства, применяет ее у себя. В случае успеха узлы кластера продолжают работу в штатном режиме. В случае ошибки применения резервный узел переходит в состояние Standby · Fatal-Error.

Если после успешной проверки связи через Sync-link резервный узел не получает от активного устройства команду на применение новой конфигурации в течение таймера ожидания, то резервный узел остается с прежней конфигурацией.

При получении обновленной конфигурации, в которой не изменились параметры канала синхронизации Sync-link (адреса, порты), активный узел не пересылает ее на резервный, а сразу применяет у себя. Далее процедура аналогична описанной выше с последующей пересылкой конфигурации соответственно.

Пример записей системного журнала

Применение новой конфигурации и ее синхронизация между узлами кластера (активный узел NGFW1):

```
ngfw@LAB-Debian-ngfw-node-1:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log
[2025-07-23 14:59:30.990534] [cluster][Cluster][2518] [info] configuring AS cluster
started [state: Active commit_id: 01983736-3aa0-7079-b954-5258af85c5ad]
[2025-07-23 14:59:30.990554] [cluster][Cluster][2518] [info] configuring device as
'Active'
[2025-07-23 14:59:31.076606] [cluster][Cluster][2518] [info] configuration has been
applied [state: Active commit_id: 01983736-3aa0-7079-b954-5258af85c5ad]
[2025-07-23 14:59:31.076671] [cluster][Cluster][2518] [info] send configuration to
standby [commit_id: 01983736-3aa0-7079-b954-5258af85c5ad]
[2025-07-23 14:59:31.159602] [cluster][Cluster][2518] [info] Configuration has been
successfully applied on peer [commit_id=01983736-3aa0-7079-b954-5258af85c5ad]
[2025-07-23 14:59:31.159708] [cluster][Cluster][2518] [info] Configuration has been
successfully applied on peer [commit_id=01983736-3aa0-7079-b954-5258af85c5ad]
```

Применение новой конфигурации и ее синхронизация между узлами кластера (резервный узел NGFW2):

```
ngfw@LAB-Debian-ngfw-node-2:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log
[2025-07-23 14:59:31.642894] [cluster][Cluster][43047] [info] configuring AS cluster
started [state: Standby commit_id: 01983736-3aa0-7079-b954-5258af85c5ad]
[2025-07-23 14:59:31.642911] [cluster][Cluster][43047] [info] configuring device as
'Standby'
[2025-07-23 14:59:31.722630] [cluster][Cluster][43047] [info] configuration has been
applied [state: Standby commit_id: 01983736-3aa0-7079-b954-5258af85c5ad]
```

30.14. Приостановка узла в кластере (Suspend)

Вы можете перевести один из узлов кластера в состояние «Приостановлен (Suspended)», например при необходимости провести его обслуживание и (или) обновление либо с целью исключить сценарий, при котором устройство может стать активным в этот период, а также в случае необходимости тестирования переключения кластера.

- Чтобы перевести узел кластера в состояние «Приостановлен (Suspended)»:

  1. На странице **Устройства** → **Кластеры** выберите интересующий вас кластер.

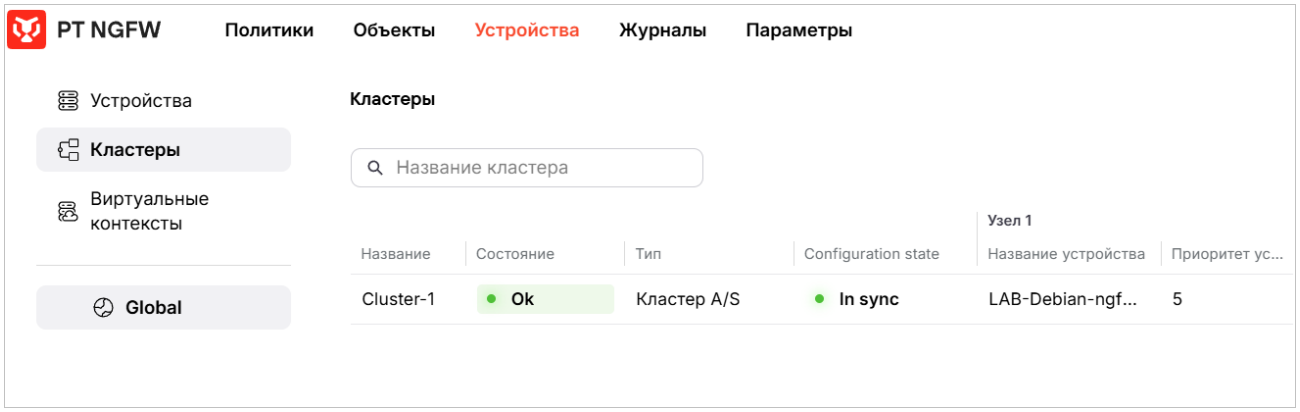


Рисунок 269. Страница **Кластеры**

2. Выполните одно из следующих действий:

   - В контекстном меню устройства, которое требуется перевести в состояние «Приостановлен (Suspended)», выберите **Приостановить** (**Suspend**).

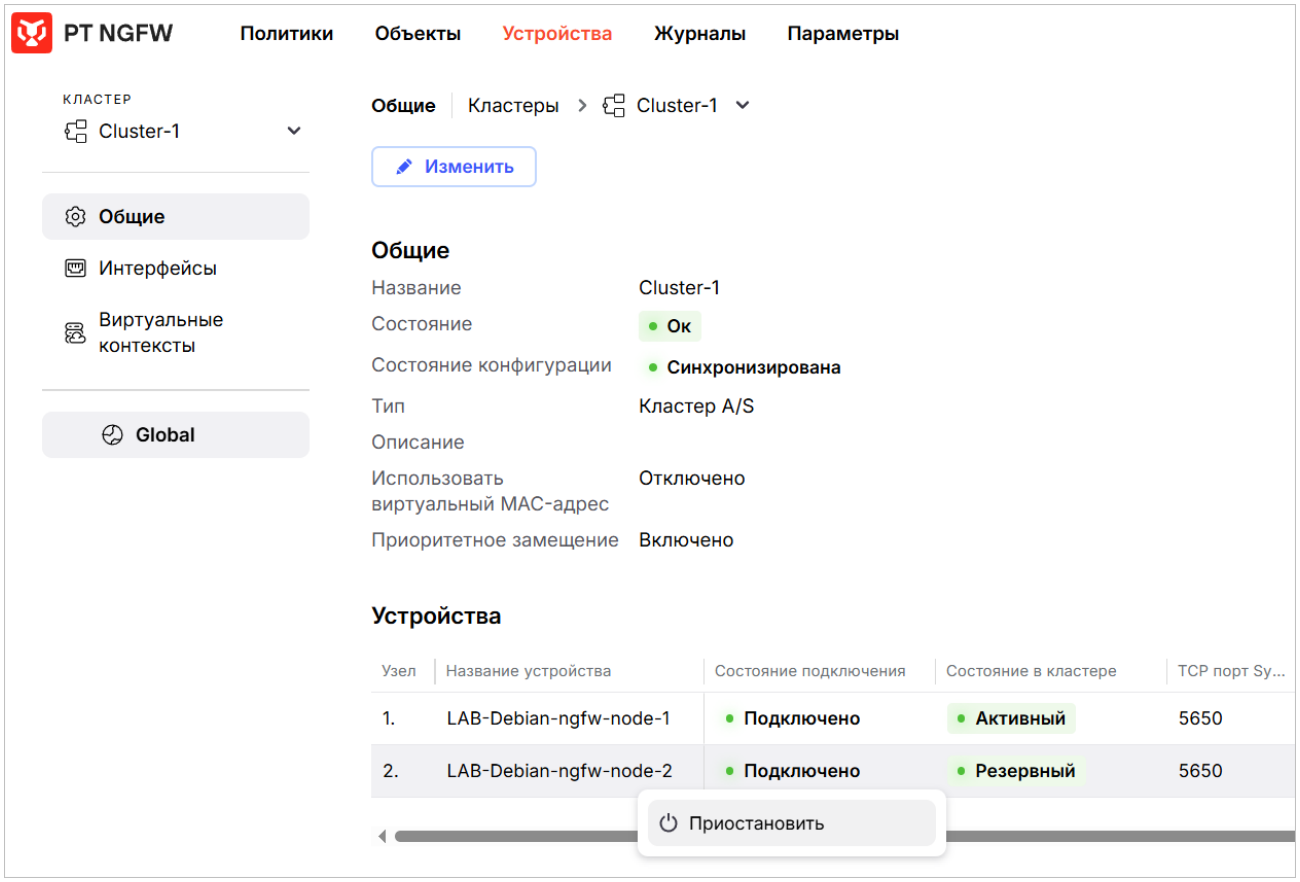


Рисунок 270. Выбор действия **Suspend** в контекстном меню

   - Выберите устройство, которое требуется перевести в состояние «Приостановлен (Suspended)».

- В карточке устройства нажмите **Приостановить** (**Suspend**).

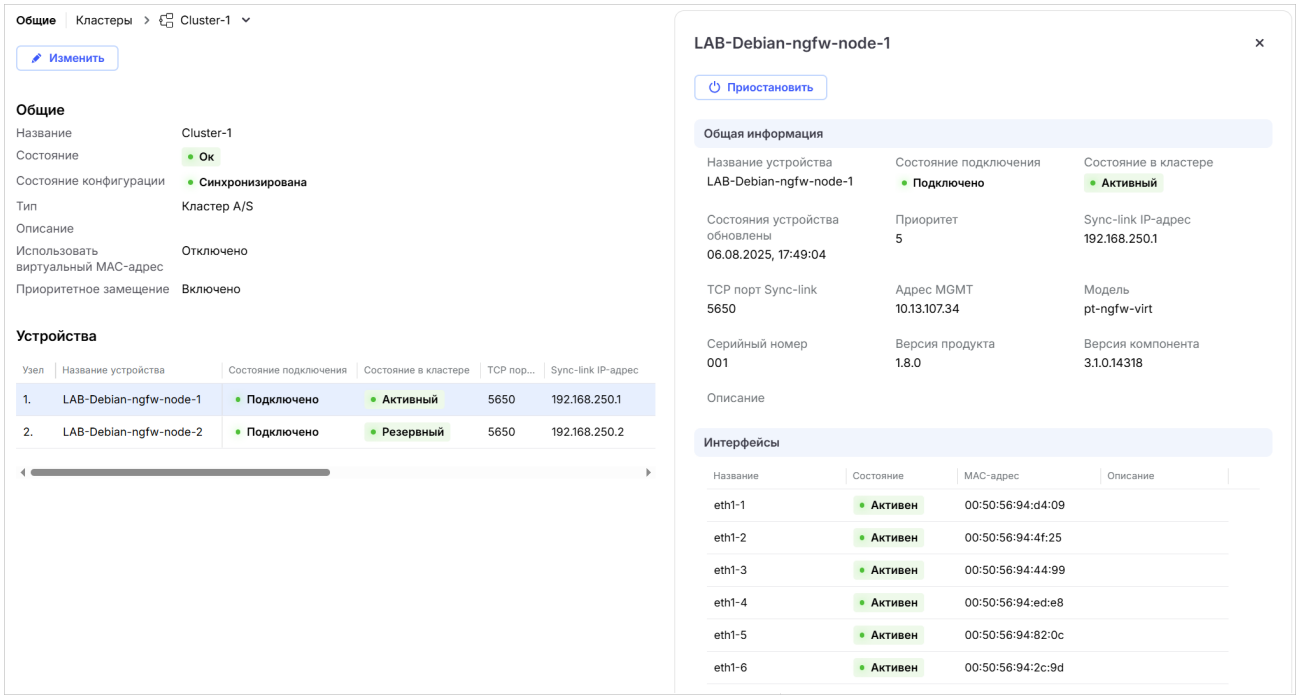


Рисунок 271. Выбор действия **Suspend** в карточке устройства

Пример записей системного журнала

Перевод устройства NGFW1 в состояние «Приостановлен (Suspended)»:

```
ngfw@LAB-Debian-ngfw-node-1:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log | grep cluster
[2025-07-23 15:01:42.868824] [cluster][Cluster][2518] [info] Suspended mode has changed [suspended mode='Enabled']
[2025-07-23 15:01:42.868900] [cluster][Cluster][2518] [info] change state [state: 'Active' new_state: 'Standby' reason: 'Switch to suspended mode']
[2025-07-23 15:01:42.869466] [cluster][Cluster][2518] [info] Do vote...
[2025-07-23 15:01:42.869481] [cluster][Cluster][2518] [info] Vote result [node='Standby->Standby' peer='Standby->Active' reason='current node couldn't be active']
```

NGFW2 становится новым активным устройством:

```
ngfw@LAB-Debian-ngfw-node-2:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log | grep cluster
[2025-07-23 15:01:43.434611] [cluster][Cluster][43047] [info] change state [state: 'Standby' new_state: 'Active' reason: 'Vote result']
```

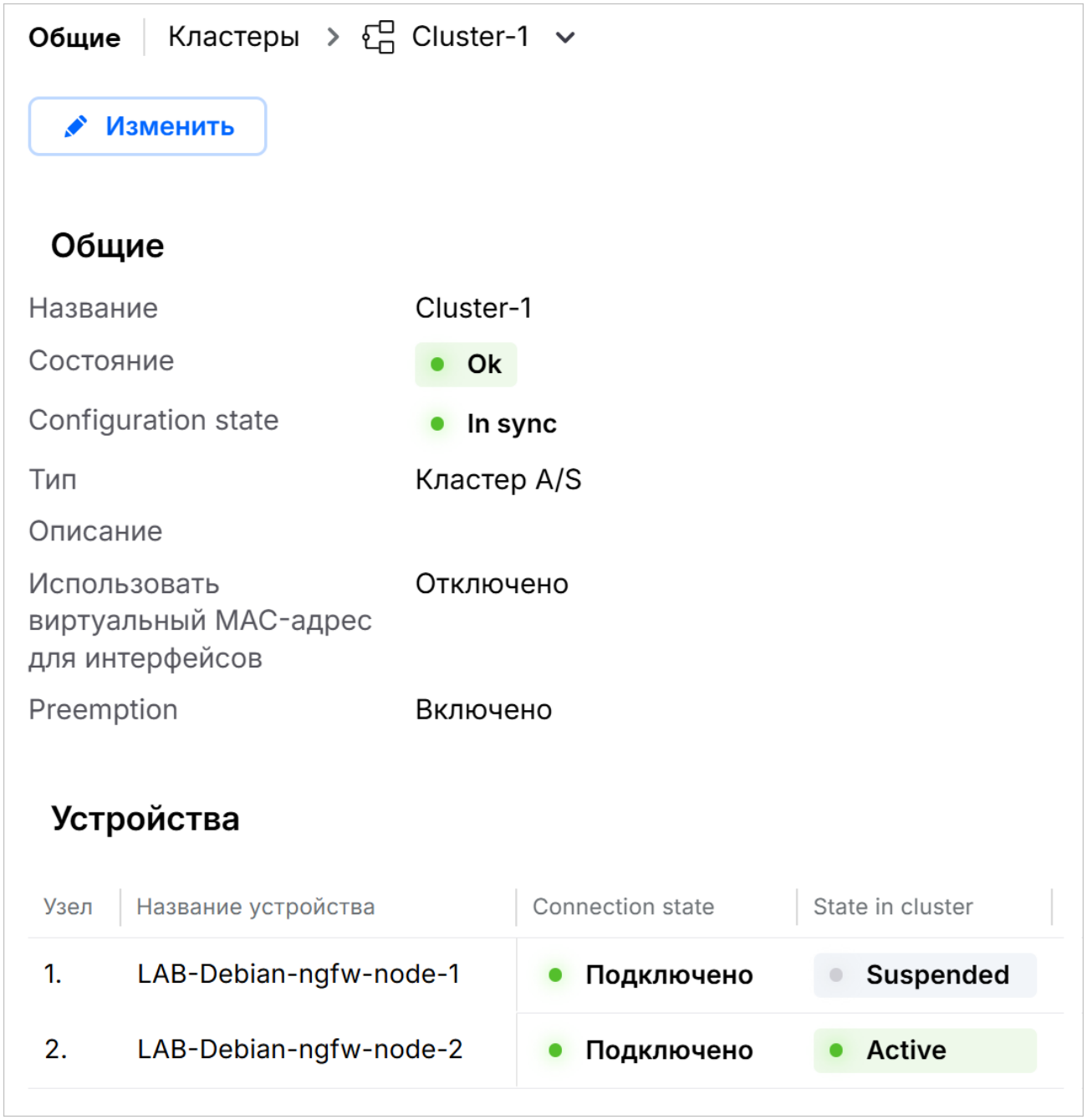


Рисунок 272. Переход узла NGFW2 в состояние активного

Вы можете вывести узел из состояния «Приостановлен (Suspended)» аналогичными способами, нажав **Возобновить** (**Unsuspend**).

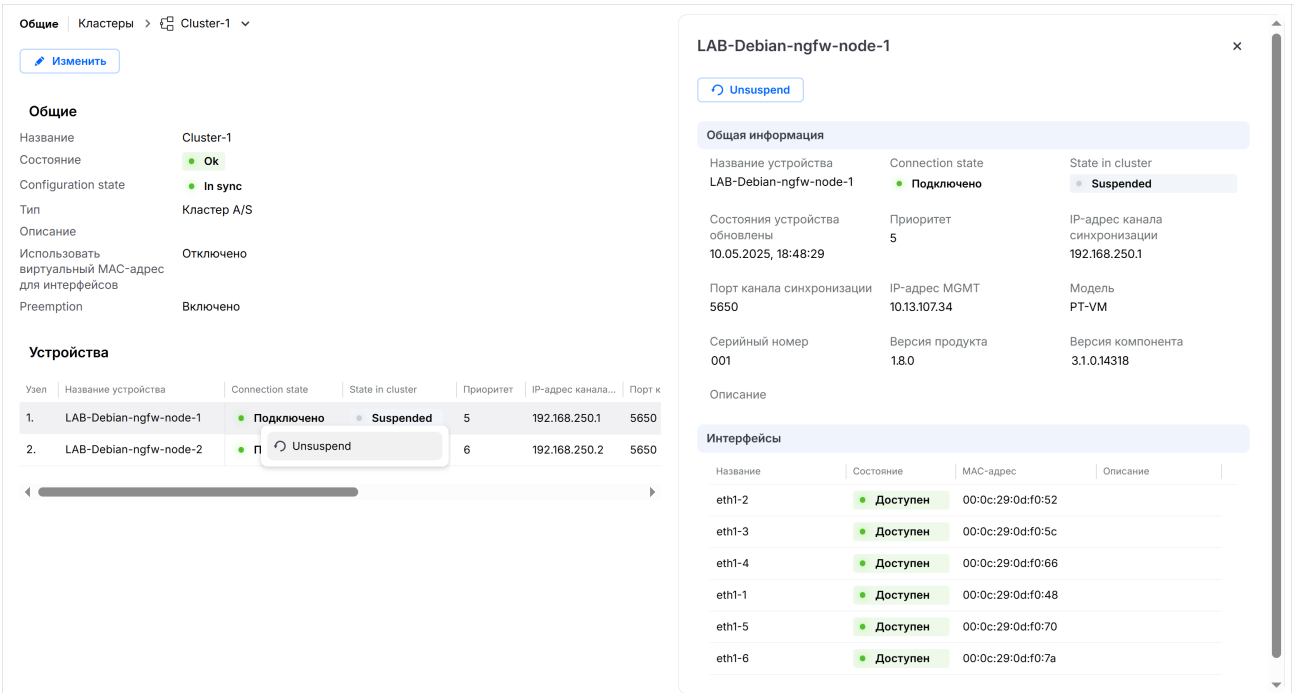


Рисунок 273. Вывод устройства из состояния Suspended

Пример записей системного журнала

Вывод устройства NGFW1 из состояния «Приостановлен (Suspended)». Узел становится активным, так как его приоритет выше и включен режим приоритетного замещения (Preemption):

```
ngfw@LAB-Debian-ngfw-node-1:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log | grep cluster
[2025-07-23 15:02:49.327193] [cluster][Cluster][2518] [info] Suspended mode has changed [suspended mode='Disabled']
[2025-07-23 15:02:49.327466] [cluster][Cluster][2518] [info] Do vote...
[2025-07-23 15:02:49.327486] [cluster][Cluster][2518] [info] compare metrics
[2025-07-23 15:02:49.327495] [cluster][Cluster][2518] [info] self metrics [count=2]
[2025-07-23 15:02:49.327504] [cluster][Cluster][2518] [info] metric [prio=1, name='port_eth1-1', state='ok']
[2025-07-23 15:02:49.327510] [cluster][Cluster][2518] [info] metric [prio=2, name='port_eth1-2', state='ok']
[2025-07-23 15:02:49.327524] [cluster][Cluster][2518] [info] peer metrics [count=2]
[2025-07-23 15:02:49.327531] [cluster][Cluster][2518] [info] metric [prio=1, name='port_eth1-1', state='ok']
[2025-07-23 15:02:49.327537] [cluster][Cluster][2518] [info] metric [prio=2, name='port_eth1-2', state='ok']
[2025-07-23 15:02:49.327543] [cluster][Cluster][2518] [info] can't select role by metrics
```

```
[2025-07-23 15:02:49.327552] [cluster][Cluster][2518] [info] Vote result
[node='Standby->Active' peer='Active->Standby' reason='active node has been selected
by priority']
[2025-07-23 15:02:49.327707] [cluster][Cluster][2518] [info] change state [state:
'Standby' new_state: 'Active' reason: 'Vote result']
```

После голосования NGFW2 становится резервным, так как его приоритет ниже и включен режим приоритетного замещения (Preemption):

```
ngfw@LAB-Debian-ngfw-node-2:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log | grep
cluster
[2025-07-23 15:02:49.892737] [cluster][Cluster][43047] [info] change state [state:
'Active' new_state: 'Standby' reason: 'Vote result']
```

30.15. Мониторинг устройств кластера

Узлы кластера обмениваются сообщениями Keepalive через Sync-link. Если резервный узел не получает сообщений от соседа в течение заданного времени, то он констатирует отказ активного узла и переходит в состояние «активный», рассылает сообщения GARP и начинает передавать транзитный пользовательский трафик.

> **Примечание.** Значения таймеров фиксированы в конфигурации PT NGFW. Переключение происходит если от соседа нет ответных сообщений Keepalives через Sync-link в течение 600 мс. Рекомендуется использовать таймеры, заданные по умолчанию в конфигурации.

Пример записей системного журнала

Узел NGFW1 (текущий активный) вышел из строя, и активным узлом стал NGFW2:

```
ngfw@LAB-Debian-ngfw-node-2:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-02-27 18:43:16.832760] [cluster][Cluster][1048] [error] closing connection due
to an error: conn='192.168.250.2:5650'<->'192.168.250.1:5650' reason=RW error
[2025-02-27 18:43:16.832834] [cluster][Cluster][1048] [error] sync link is broken
[2025-02-27 18:43:16.832859] [cluster][Cluster][1053] [error] Sync connection has
been lost
[2025-02-27 18:43:16.832887] [cluster][Cluster][1053] [info] change state [state:
'Standby' new_state: 'Active' reason: 'sync connection was closed']
[2025-02-27 18:43:53.950388] [cluster][Cluster][1048] [info] peer connected
[conn='192.168.250.2:5650'<->'192.168.250.1:5650']
[2025-02-27 18:43:53.953637] [cluster][Cluster][1053] [info] sync link is ready
[2025-02-27 18:43:53.954596] [cluster][Cluster][1053] [info] send configuration to
standby [commit_id: 01954771-c6df-7391-8b10-b255ee7bc3fb]
[2025-02-27 18:43:53.954613] [cluster][Cluster][1053] [info] notify standby to apply
new configuration
[2025-02-27 18:43:54.035566] [cluster][Cluster][1053] [info] Standby node is
successfully configured [commit_id: 01954771-c6df-7391-8b10-b255ee7bc3fb]
```

Проблема на узле NGFW1 устранена, и он подключается к кластеру, переходит в состояние резервного после голосования:

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-02-27 18:43:53.926665] [cluster][Cluster][4157] [info] initializing AS cluster
started
[2025-02-27 18:43:53.926683] [cluster][Cluster][4157] [info] AS cluster sync link
initialization started
[2025-02-27 18:43:53.929211] [cluster][Cluster][4154] [info] peer connected
[conn='192.168.250.1:5650'<->'192.168.250.2:5650']
[2025-02-27 18:43:53.932530] [cluster][Cluster][4157] [info] sync link is ready
[2025-02-27 18:43:53.932546] [cluster][Cluster][4157] [info] Sync connection accepted
by remote node [remote node uid: '01954684-3cbf-7d7c-711b-7f0d35b3fe2e']
[2025-02-27 18:43:53.932759] [cluster][Cluster][4157] [info] Do vote...
[2025-02-27 18:43:53.932770] [cluster][Cluster][4157] [info] Vote result
[self='Standalone->Standby' peer='Active->Active' reason='connecting to active node']
[2025-02-27 18:43:53.932913] [cluster][Cluster][4157] [info] change state [state:
'Standalone' new_state: 'Standby' reason: 'Vote result']
[2025-02-27 18:43:53.933032] [cluster][Cluster][4157] [info] node had commanded to
apply device configuration
[2025-02-27 18:43:53.933039] [cluster][Cluster][4157] [info] sync link commit new
endpoints
[2025-02-27 18:43:53.933059] [cluster][Cluster][4157] [info] configuring device
[2025-02-27 18:43:54.013665] [cluster][Cluster][4157] [info] configuration was
succeed [state: Standby commit_id: 01954771-c6df-7391-8b10-b255ee7bc3fb]
[2025-02-27 18:45:23.933056] [cluster][Cluster][4157] [info] Do vote...
[2025-02-27 18:45:23.933100] [cluster][Cluster][4157] [info] compare metrics
[2025-02-27 18:45:23.933107] [cluster][Cluster][4157] [info] self metrics [count=12]
[2025-02-27 18:45:23.933113] [cluster][Cluster][4157] [info] metric [prio=1,
name='port_eth1-1', state='ok']
[2025-02-27 18:45:23.933117] [cluster][Cluster][4157] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-02-27 18:45:23.933156] [cluster][Cluster][4157] [info] peer metrics [count=2]
[2025-02-27 18:45:23.933160] [cluster][Cluster][4157] [info] metric [prio=1,
name='port_eth1-1', state='ok']
[2025-02-27 18:45:23.933164] [cluster][Cluster][4157] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-02-27 18:45:23.933202] [cluster][Cluster][4157] [info] can't select role by
metrics
[2025-02-27 18:45:23.933207] [cluster][Cluster][4157] [info] Vote result
[self='Standby->Standby' peer='Active->Active' reason='nothing changed']
```

Текущий активный узел NGFW2 отправил узлу NGFW1, который подключился к кластеру, конфигурацию и команду на ее применение:

```
ngfw@LAB-Debian-ngfw-node-2:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-02-27 18:43:53.950388] [cluster][Cluster][1048] [info] peer connected
[conn='192.168.250.2:5650'<->'192.168.250.1:5650']
[2025-02-27 18:43:53.953637] [cluster][Cluster][1053] [info] sync link is ready
```

```
[2025-02-27 18:43:53.954596] [cluster][Cluster][1053] [info] send configuration to
standby [commit_id: 01954771-c6df-7391-8b10-b255ee7bc3fb]
[2025-02-27 18:43:53.954613] [cluster][Cluster][1053] [info] notify standby to apply
new configuration
[2025-02-27 18:43:54.035566] [cluster][Cluster][1053] [info] Standby node is
successfully configured [commit_id: 01954771-c6df-7391-8b10-b255ee7bc3fb]
```

Примечание. При подключении узла к существующему кластеру он не может сразу получить роль активного. Узел сначала получает роль резервного, применяет актуальную конфигурацию, и только после этого возможно повторное голосование. Такое поведение исключает ситуацию, при которой к существующему кластеру подключается узел со старой конфигурацией и заменяет на нее текущую конфигурацию.

В случае выключения или перезагрузки узлов, в том числе одновременной, после успешного запуска NGFW обнаружит соседнее устройство через Sync-link, после чего будет установлено соединение, выполнено рукопожатие с последующим голосованием для выбора активного узла.

Ниже приведены примеры записей журналов при одновременном перезапуске узлов.

NGFW1:

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-03-18 17:50:42.464841] [cluster][Cluster][965] [info] initializing AS cluster
started
[2025-03-18 17:50:42.464865] [cluster][Cluster][965] [info] AS cluster sync link
initialization started
[2025-03-18 17:50:42.489201] [cluster][Cluster][963] [info] peer connected
[conn='192.168.250.1:5650'<->'192.168.250.2:5650']
[2025-03-18 17:50:42.497673] [cluster][Cluster][965] [info] sync link is ready
[2025-03-18 17:50:42.525205] [cluster][Cluster][965] [info] change state [state:
'Standalone' new_state: 'Active' reason: 'Vote result']
[2025-03-18 17:50:42.525223] [cluster][Cluster][965] [info] configuring device
[2025-03-18 17:50:42.579373] [cluster][Cluster][965] [info] notify standby to apply
new configuration
[2025-03-18 17:50:42.579382] [cluster][Cluster][965] [info] sync link commit new
endpoints
[2025-03-18 17:50:42.579390] [cluster][Cluster][965] [info] configuration was succeed
[state: Active commit_id: 0195a899-f141-7e07-9638-c57cf0be4566]
[2025-03-18 17:50:42.645246] [cluster][Cluster][965] [info] Standby node is
successfully configured [commit_id: 0195a899-f141-7e07-9638-c57cf0be4566]
```

NGFW2:

```
ngfw@LAB-Debian-ngfw-node-2:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-03-18 17:50:39.332976] [cluster][Cluster][945] [info] initializing AS cluster
started
[2025-03-18 17:50:39.332997] [cluster][Cluster][945] [info] AS cluster sync link
initialization started
[2025-03-18 17:50:42.727286] [cluster][Cluster][943] [info] peer connected
[conn='192.168.250.2:5650'<->'192.168.250.1:5650']
[2025-03-18 17:50:42.743313] [cluster][Cluster][945] [info] sync link is ready
```

```
[2025-03-18 17:50:42.743342] [cluster][Cluster][945] [info] Sync connection accepted
by remote node [remote node uid: '01959af3-8167-7788-70e9-60aeee3588f2']
[2025-03-18 17:50:42.755278] [cluster][Cluster][945] [info] Do vote...
[2025-03-18 17:50:42.755293] [cluster][Cluster][945] [info] Vote result
[self='Standalone->Standby' peer='Standalone->Active' reason='active node has been
selected by priority']
[2025-03-18 17:50:42.771297] [cluster][Cluster][945] [info] change state [state:
'Standalone' new_state: 'Standby' reason: 'Vote result']
[2025-03-18 17:50:42.823272] [cluster][Cluster][945] [info] node had commanded to
apply device configuration
[2025-03-18 17:50:42.823298] [cluster][Cluster][945] [info] sync link commit new
endpoints
[2025-03-18 17:50:42.823308] [cluster][Cluster][945] [info] configuring device
[2025-03-18 17:50:42.879500] [cluster][Cluster][945] [info] configuration was succeed
[state: Standby commit_id: 0195a899-f141-7e07-9638-c57cf0be4566]
[2025-03-18 17:51:42.755548] [cluster][Cluster][945] [info] Do vote...
[2025-03-18 17:51:42.755598] [cluster][Cluster][945] [info] Vote result
[self='Standby->Standby' peer='Active->Active' reason='nothing changed']
```

30.16. Split-brain (раскол кластера)

Split-brain (раскол кластера) — это состояние, в котором каждое устройство кластера считает себя активным. Оно возникает, если устройства не определяют друг друга, но при этом оба находятся в работоспособном и активном (Active) состоянии, расценивая состояние соседа как вышедшее из строя.

Это происходит, когда между устройствами кластера по какой-то причине нет связи: резервное устройство не определяет текущее активное устройство и тоже переходит в активное состояние. Это приводит к проблемам в передаче транзитного пользовательского трафика, так как каждое из устройств перетягивает трафик на себя, рассылая сообщения GARP, устанавливая соседство по протоколам LACP, OSPF и BGP, если они заданы в конфигурации. Такое появление в сети двух устройств — копий друг друга с одинаковыми параметрами приводит к потерям пользовательского трафика.

Потеря сообщений Keepalives может происходить по ряду причин, не связанных с отказом устройства PT NGFW, например:

- неверная конфигурация интерфейсов Sync-link (некорректные адреса и (или) маршруты);
- отказ физического интерфейса, который используется для формирования Sync-link;
- нарушение сетевой связности между интерфейсами Sync-link, например, поврежден патч-корд, повреждена линия связи, промежуточное устройство блокирует трафик;
- большие потери на линии связи между интерфейсами Sync-link, например, из-за сбоев работы интерфейса, трансивера, потерь на промежуточных устройствах, перегрузки канала связи.

30.17. Мониторинг интерфейсов кластера

Узлы кластера отслеживают состояние интерфейсов друг друга, через которые передается транзитный пользовательский трафик.

При переходе одного из отслеживаемых интерфейсов активного узла в состояние Down (пропадание связи) активный узел уведомляет об этом резервный узел и передает ему роль активного. Происходит переключение кластера.

При этом, если настроен перечень отслеживаемых интерфейсов и заданы их приоритеты, то:

— Сначала сравниваются состояния отслеживаемых интерфейсов, которые имеют приоритет 1. Если интерфейс с приоритетом 1 активного узла перешел в состояние Down, то происходит переключение, и сравнение интерфейсов более низкого приоритета не выполняется.

— Если состояние интерфейсов приоритета 1 на обоих узлах одинаково, то сравниваются интерфейсы с приоритетом 2 и т. д.

Таким образом, например в ситуации, когда на активном узле отказывает интерфейс с приоритетом 2 и одновременно с этим на резервном узле — интерфейс с приоритетом 1, то переключения кластера не происходит, так как ситуация на резервном узле хуже, чем на активном.

В конфигурационном файле узла PT NGFW в секции `cluster` перечисляются интерфейсы, которые следует использовать для выбора активного узла, и их приоритеты. Иными словами, это интерфейсы, выход из строя которых должен приводить к переключению кластера. Секция `health_monitor` является опциональной. Она предназначена для того, чтобы задать имена отслеживаемым интерфейсам. В примере ниже интерфейсу eth1-1 задается имя port_eth1-1 и это имя используется далее в секции `cluster`.

Если секция `cluster` отсутствует, то:

— выполняется отслеживание всех интерфейсов кластера;

— отказ любого интерфейса активного узла кластера будет вызывать выборы нового активного узла;

— каждый узел кластера сообщает статус состояния здоровья «Внимание (Warning)» при отказе любого своего интерфейса.

Если секция `cluster` присутствует, но не заполнена, то мониторинг интерфейсов кластера не выполняется. Отказы интерфейсов не вызывают выборов нового активного узла и, следовательно, переключения кластера.

Если в секции `cluster` указаны конкретные интерфейсы, то:

— выполняется отслеживание перечисленных интерфейсов;

— отказ одного из перечисленных интерфейсов активного узла кластера запускает выборы нового активного узла с учетом приоритетов интерфейсов;

— каждый узел кластера сообщает статус состояния здоровья «Внимание (Warning)» при отказе любого из перечисленных интерфейсов.

Внимание! Существуют ограничения по сравнению количества отказавших интерфейсов одного приоритета. Если несколько интерфейсов имеют одинаковый приоритет, то количество интерфейсов не отслеживается и не влияет на оценку работоспособности узла. Например, если на NGFW1 отказал один интерфейс с приоритетом 1, а на NGFW2 отказало два интерфейса также с приоритетом 1, то такие узлы кластера будут считаться равнозначными по метрикам и одинаково работоспособными. Переключение кластера выполняться не будет.

Ниже указаны примеры конфигурации в секциях `health_monitor` и `cluster`, а также сценарии переключений для такой конфигурации.

Пример секции `health_monitor`:

```
$ cat /opt/pt-ngfw/ngfw-core/etc/config/pt-ngfw.conf
{
  "health_monitor": {
    "check_period_ms": 100,
    "metrics": [
      {
        "name": "port_eth1-1",
        "type": "dpdk_port",
        "port": "eth1-1"
      },
      {
        "name": "port_eth1-2",
        "type": "dpdk_port",
        "port": "eth1-2"
      }
    ]
  },
<Другие секции конфигурационного файла>
}
```

Пример секции `cluster`:

```
  "cluster":{
    "metrics":[
       {"name": "port_eth1-1", "prio": 1},
       {"name": "port_eth1-2", "prio": 2}
     ]
  },
```

```
<Другие секции конфигурационного файла>
}
```

Внимание! Содержимое секций `health_monitor` и `cluster` должно быть полностью идентично на обоих устройствах кластера.

Сценарий 1

Исходное состояние. Узел NGFW1 находится в состоянии «активный», NGFW2 — «резервный». На обоих устройствах все интерфейсы в состоянии Up.

Изменение интерфейсов. На активном узле отказывает интерфейс eth-1-2 с приоритетом 2.

Переключение. NGFW1 переходит в состояние «резервный», NGFW2 — в состояние «активный».

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-03-05 17:48:30.479903] [cluster][Cluster][14991] [info] Do vote...
[2025-03-05 17:48:30.479932] [cluster][Cluster][14991] [info] compare metrics
[2025-03-05 17:48:30.479946] [cluster][Cluster][14991] [info] self metrics [count=2]
[2025-03-05 17:48:30.479954] [cluster][Cluster][14991] [info] metric [prio=1,
name='port_eth1-1', state='ok']
[2025-03-05 17:48:30.479960] [cluster][Cluster][14991] [info] metric [prio=2,
name='port_eth1-2', state='error']
[2025-03-05 17:48:30.480017] [cluster][Cluster][14991] [info] peer metrics [count=2]
[2025-03-05 17:48:30.480021] [cluster][Cluster][14991] [info] metric [prio=1,
name='port_eth1-1', state='ok']
[2025-03-05 17:48:30.480026] [cluster][Cluster][14991] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-03-05 17:48:30.480081] [cluster][Cluster][14991] [info] Vote result
[self='Active->Standby' peer='Standby->Active' reason='Peer node is better choice:
failed metric [prio='2' self='ok' peer='failed']']
[2025-03-05 17:48:30.480086] [cluster][Cluster][14991] [info] change state [state:
'Active' new_state: 'Standby' reason: 'Vote result']
```

Примечание. В этом сценарии не важен приоритет отказавшего интерфейса в связи с тем, что на NGFW2 (изначально резервный) все интерфейсы находятся в состоянии Up. Поэтому переключение кластера будет происходить при отказе любого из отслеживаемых интерфейсов активного узла.

```
ngfw@LAB-Debian-ngfw-node-2:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-03-05 17:48:30.479180] [cluster][Cluster][2503] [info] change state [state:
'Standby' new_state: 'Active' reason: 'Vote result']
```

Сценарий 2

Исходное состояние. Узел NGFW1 находится в состоянии «активный», NGFW2 — «резервный». На обоих устройствах все интерфейсы в состоянии Up.

Изменение интерфейсов. На активном узле отказывает интерфейс eth-1-2 с приоритетом 2, а на резервном узле — интерфейс eth1-1 с приоритетом 1.

Переключение. Роли узлов не изменяются, так как на активном узле интерфейс eth1-1 более высокого приоритета находится в состоянии Up, на резервном — в Down.

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-03-05 18:00:49.539506] [cluster][Cluster][15812] [info] Do vote...
[2025-03-05 18:00:49.539540] [cluster][Cluster][15812] [info] compare metrics
[2025-03-05 18:00:49.539558] [cluster][Cluster][15812] [info] self metrics [count=2]
[2025-03-05 18:00:49.539565] [cluster][Cluster][15812] [info] metric [prio=1,
name='port_eth1-1', state='ok']
[2025-03-05 18:00:49.539571] [cluster][Cluster][15812] [info] metric [prio=2,
name='port_eth1-2', state='error']
[2025-03-05 18:00:49.539575] [cluster][Cluster][15812] [info] peer metrics [count=2]
[2025-03-05 18:00:49.539580] [cluster][Cluster][15812] [info] metric [prio=1,
name='port_eth1-1', state='error']
[2025-03-05 18:00:49.539584] [cluster][Cluster][15812] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-03-05 18:00:49.539592] [cluster][Cluster][15812] [info] Vote result
[self='Active->Active' peer='Standby->Standby' reason='current node is better choice:
failed metric [prio='1' self='failed' peer='ok']']
```

Сценарий 3

Исходное состояние. Узел NGFW1 находится в состоянии «активный», NGFW2 — «резервный». На узле NGFW1 все интерфейсы в состоянии Up. На узле NGFW2 интерфейс eth1-1 (приоритет 1) в состоянии Down.

Изменение интерфейсов. На активном узле отказывает интерфейс eth-1-1 с приоритетом 1.

Переключение. Переключения кластера не происходит, так как с точки зрения метрик на обоих узлах имеет место равнозначный отказ.

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-03-05 18:31:19.100533] [cluster][Cluster][14991] [info] Do vote...
[2025-03-05 18:31:19.100567] [cluster][Cluster][14991] [info] compare metrics
[2025-03-05 18:31:19.100576] [cluster][Cluster][14991] [info] self metrics [count=2]
[2025-03-05 18:31:19.100583] [cluster][Cluster][14991] [info] metric [prio=1,
name='port_eth1-1', state='error']
[2025-03-05 18:31:19.100588] [cluster][Cluster][14991] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-03-05 18:31:19.100658] [cluster][Cluster][14991] [info] peer metrics [count=2]
[2025-03-05 18:31:19.100663] [cluster][Cluster][14991] [info] metric [prio=1,
name='port_eth1-1', state='error']
[2025-03-05 18:31:19.100668] [cluster][Cluster][14991] [info] metric [prio=2,
name='port_eth1-2', state='ok']
```

```
[2025-03-05 18:31:19.100730] [cluster][Cluster][14991] [info] can't select role by
metrics
[2025-03-05 18:31:19.100737] [cluster][Cluster][14991] [info] Vote result
[self='Active->Active' peer='Standby->Standby' reason='nothing changed']
```

Сценарий 4

Исходное состояние. Узел NGFW1 находится в состоянии «активный», NGFW2 — «резервный». На каждом устройстве интерфейс eth1-1 (приоритет 1) находится в состоянии Down.

Изменение интерфейсов. На активном узле интерфейс eth-1-1 переходит в состояние Up.

Переключение. Изменений не происходит, так как у активного узла ситуация лучше, и он уже активный.

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-03-05 18:33:43.937871] [cluster][Cluster][14991] [info] Do vote...
[2025-03-05 18:33:43.937912] [cluster][Cluster][14991] [info] compare metrics
[2025-03-05 18:33:43.937920] [cluster][Cluster][14991] [info] self metrics [count=2]
[2025-03-05 18:33:43.937927] [cluster][Cluster][14991] [info] metric [prio=1,
name='port_eth1-1', state='ok']
[2025-03-05 18:33:43.937932] [cluster][Cluster][14991] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-03-05 18:33:43.937936] [cluster][Cluster][14991] [info] metric [prio=1,
name='port_eth1-3', state='ok']
[2025-03-05 18:33:43.937986] [cluster][Cluster][14991] [info] peer metrics [count=2]
[2025-03-05 18:33:43.937991] [cluster][Cluster][14991] [info] metric [prio=1,
name='port_eth1-1', state='error']
[2025-03-05 18:33:43.937995] [cluster][Cluster][14991] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-03-05 18:33:43.938052] [cluster][Cluster][14991] [info] Vote result
[self='Active->Active' peer='Standby->Standby' reason='current node is better choice:
failed metric [prio='1' self='failed' peer='ok']']
```

Сценарий 5

Исходное состояние. Узел NGFW1 находится в состоянии «резервный», NGFW2 — «активный». На каждом узле интерфейс eth1-1 (приоритет 1) находится в состоянии Down.

Изменение интерфейсов. Интерфейс eth1-1 узла NGFW1 восстанавливается и переходит в Up.

Переключение. Узел NGFW1 становится новым активным по причине лучшего состояния метрик.

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-03-05 18:46:26.371534] [cluster][Cluster][14991] [info] Do vote...
[2025-03-05 18:46:26.371571] [cluster][Cluster][14991] [info] compare metrics
[2025-03-05 18:46:26.371580] [cluster][Cluster][14991] [info] self metrics [count=2]
```

```
[2025-03-05 18:46:26.371592] [cluster][Cluster][14991] [info] metric [prio=1,
name='port_eth1-1', state='ok']
[2025-03-05 18:46:26.371606] [cluster][Cluster][14991] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-03-05 18:46:26.371661] [cluster][Cluster][14991] [info] peer metrics [count=2]
[2025-03-05 18:46:26.371665] [cluster][Cluster][14991] [info] metric [prio=1,
name='port_eth1-1', state='error']
[2025-03-05 18:46:26.371671] [cluster][Cluster][14991] [info] metric [prio=2,
name='port_eth1-2', state='ok']
[2025-03-05 18:46:26.371760] [cluster][Cluster][14991] [info] Vote result
[self='Standby->Active' peer='Active->Standby' reason='current node is better choice:
failed metric [prio='1' self='failed' peer='ok']']
[2025-03-05 18:46:26.372036] change state [state: 'Standby' new_state: 'Active'
reason: 'Vote result']
```

Узел NGFW2 переходит в состояние «резервный»:

```
ngfw@LAB-Debian-ngfw-node-2:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-03-05 18:46:26.372340] [cluster][Cluster][3190] [info] change state [state:
'Active' new_state: 'Standby' reason: 'Vote result']
```

30.18. Удаление устройств из кластера

- Чтобы удалить устройство из кластера:

  1. На странице **Устройства** → **Кластеры** выберите кластер, из которого хотите удалить устройство.
  2. Нажмите **Изменить**.

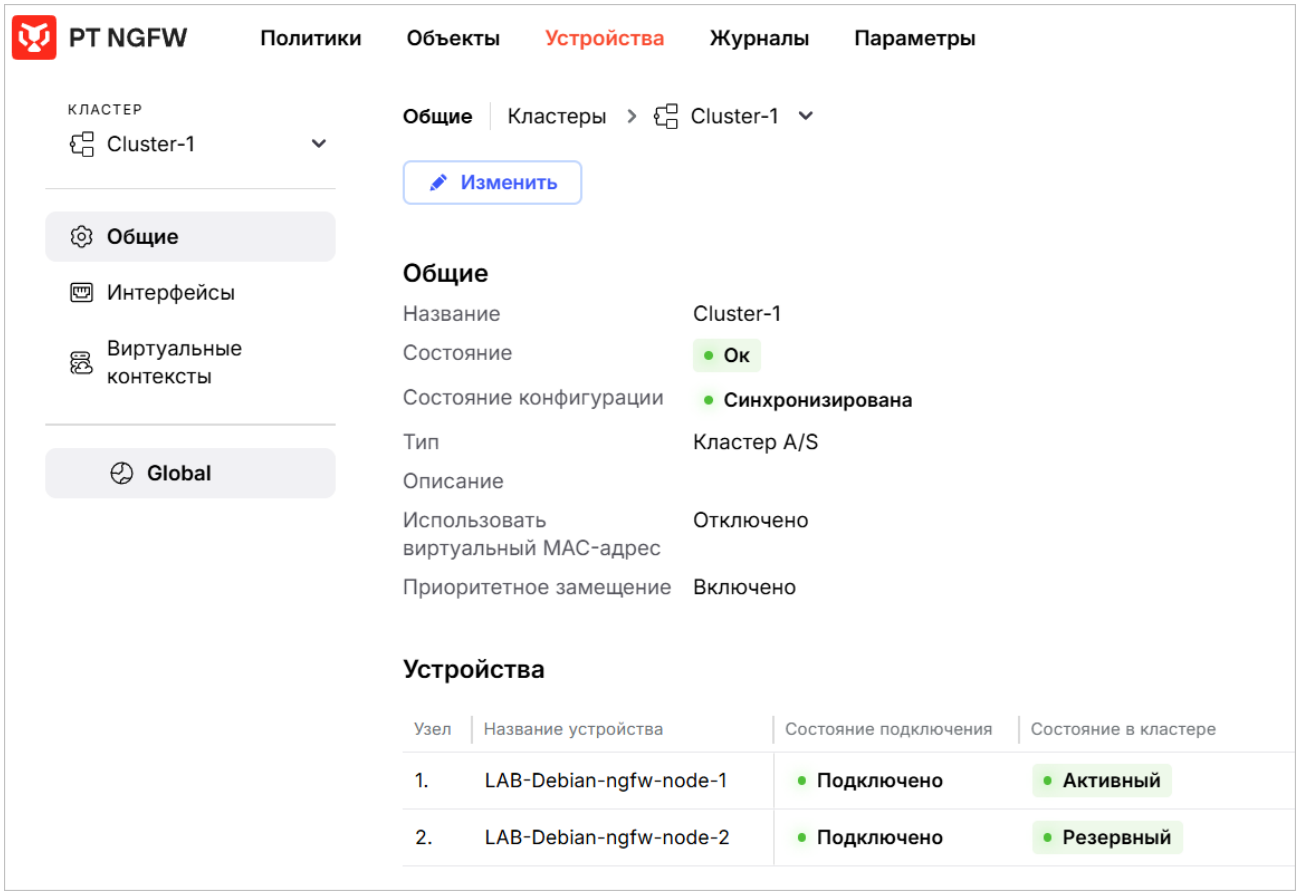


Рисунок 274. Общие параметры кластера

3. В блоке **Устройства** в контекстном меню удаляемого устройства нажмите **Удалить**.

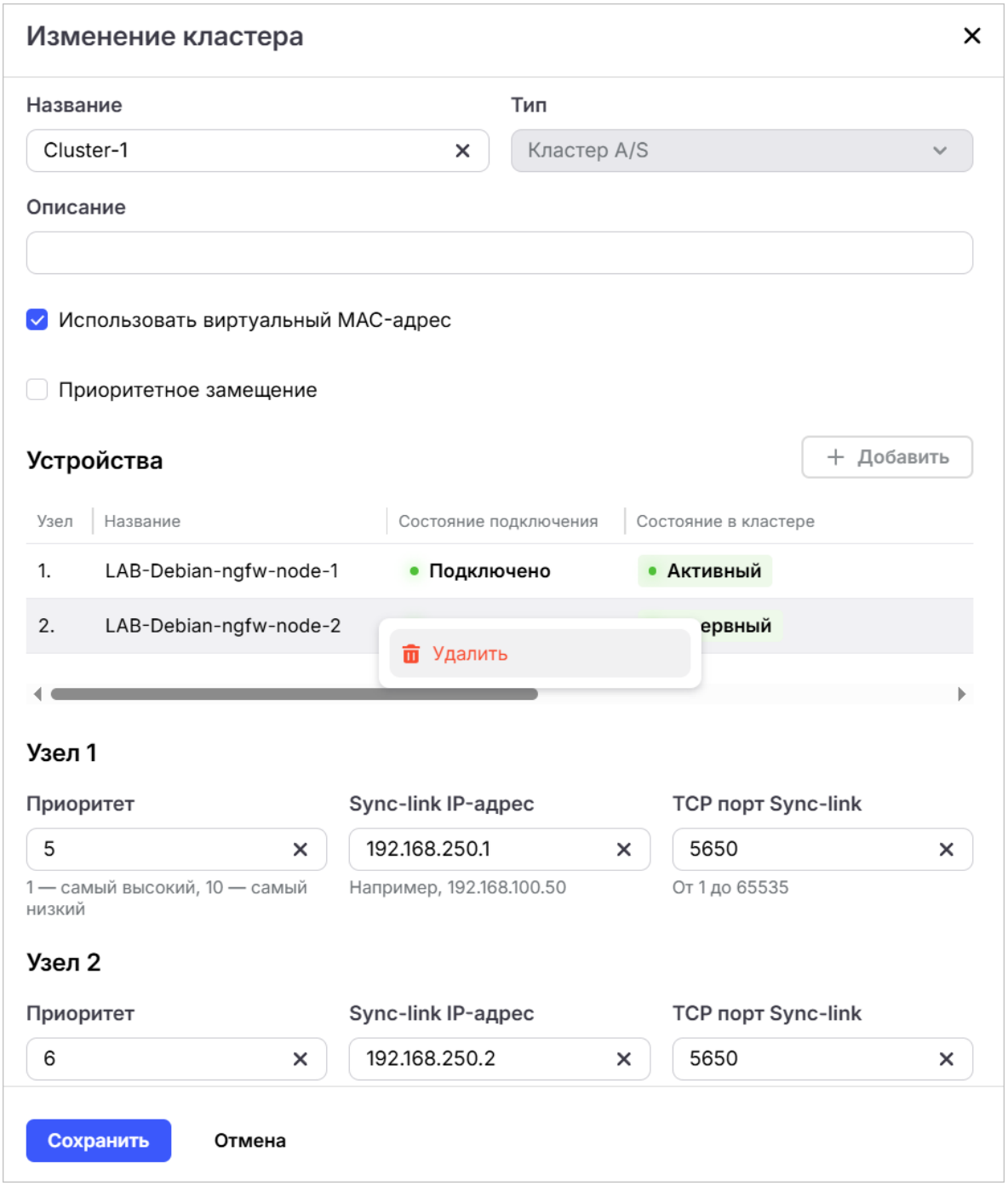


Рисунок 275. Удаление устройства из кластера

Устройство помечается значком , который означает, что устройство будет удалено после сохранения параметров кластера и применения конфигурации.

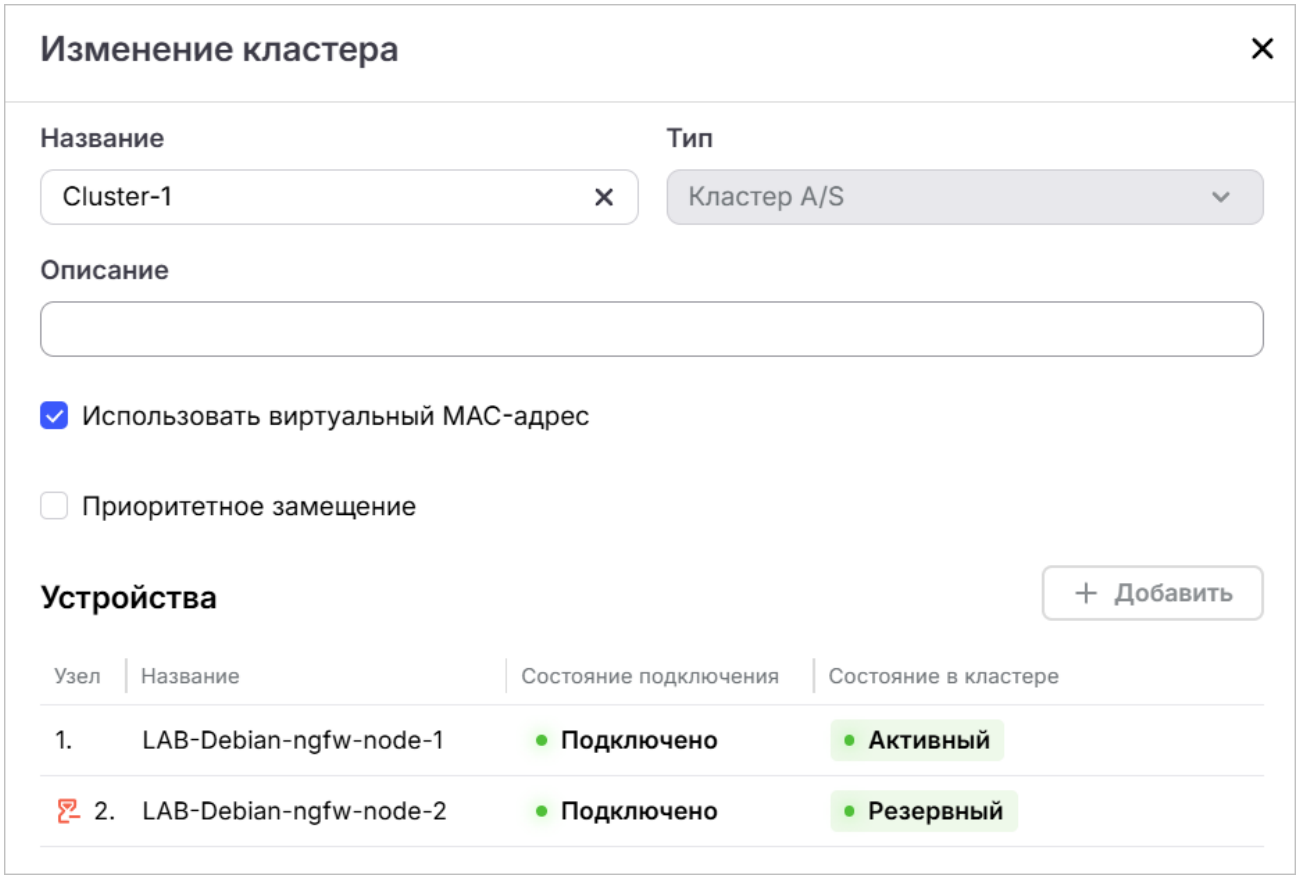


Рисунок 276. Устройство, помеченное к удалению

Примечание. Вы можете отменить удаление, выбрав соответствующий пункт в контекстном меню устройства.

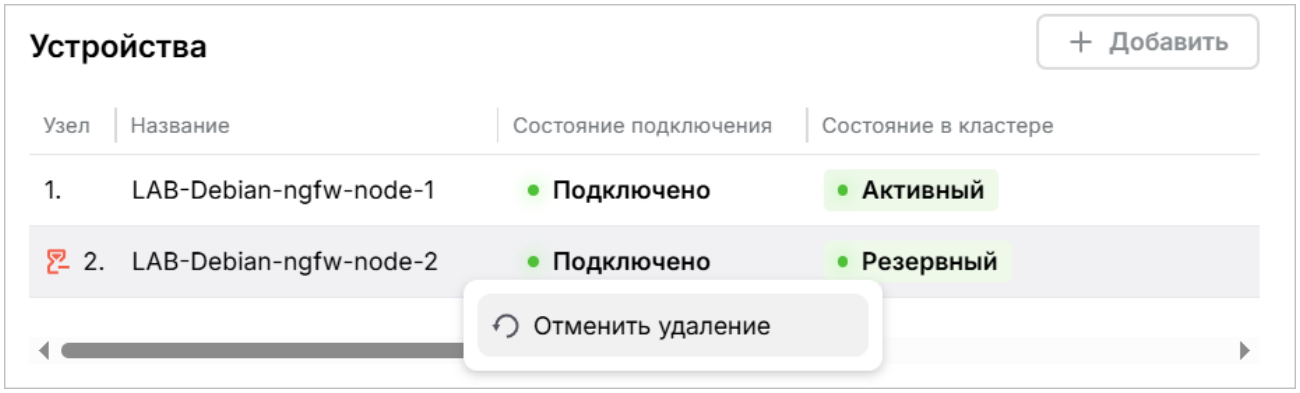


Рисунок 277. Отмена удаления

4. Нажмите **Сохранить**.
5. Нажмите **Отправить на устройства**, чтобы применить конфигурацию.

Внимание! После удаления устройства из кластера и применения изменений конфигурация удаленного устройства будет очищена. Это необходимо для предотвращения присутствия в сети двух устройств с одинаковой конфигурацией.

После успешного применения конфигурации и удаления устройства на странице с общими параметрами кластера будет отображаться его обновленный статус.

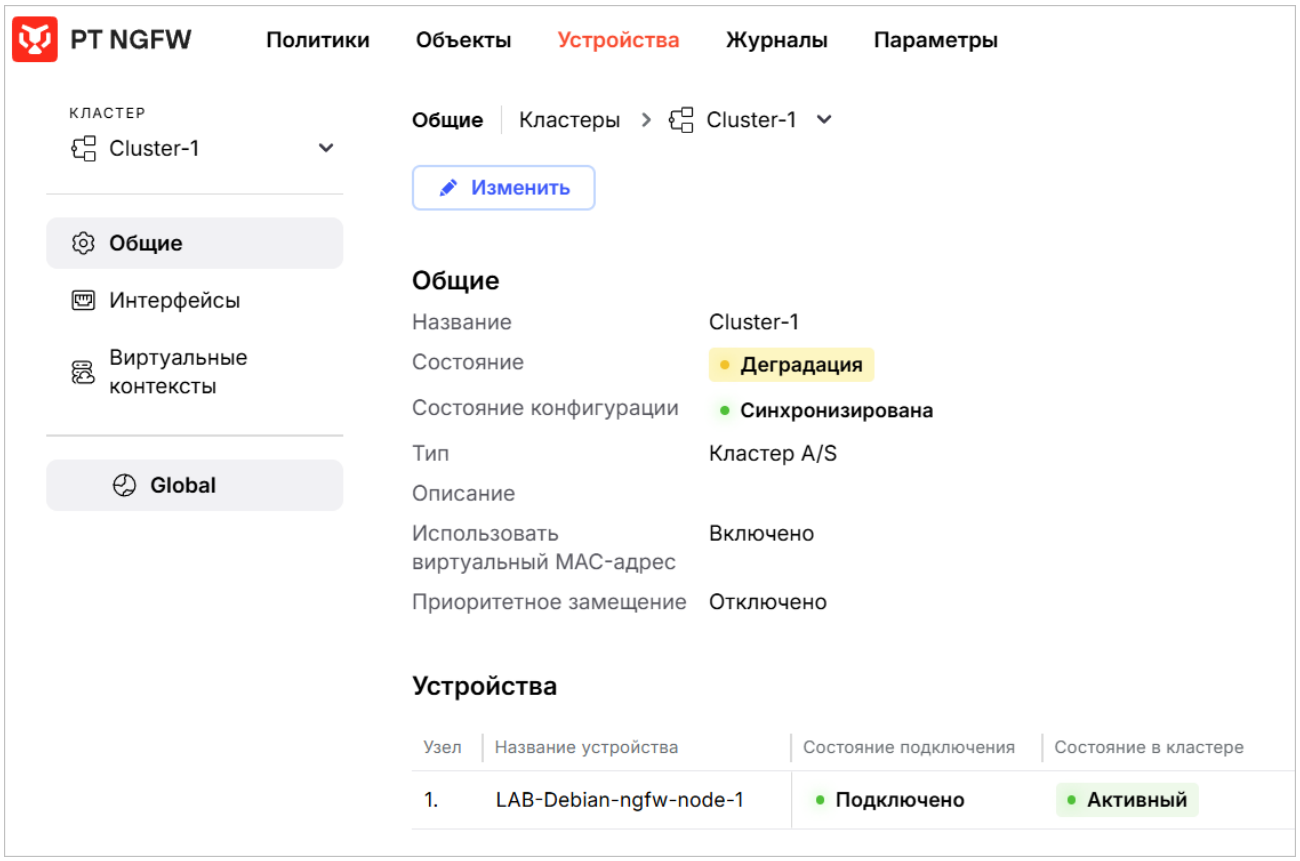


Рисунок 278. Обновленный статус кластера

Пример записей системного журнала

Вывод устройства NGFW1 (активный, остается в кластере):

```
ngfw@LAB-Debian-ngfw-node-1:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log | grep cluster
[2025-07-23 15:19:43.132757] [cluster][Cluster][2518] [info] configuring AS cluster started [state: Active commit_id: 01983748-b9d6-7e04-af64-09df02c3ed97]
[2025-07-23 15:19:43.132773] [cluster][Cluster][2518] [info] configuring device as 'Active'
[2025-07-23 15:19:43.297261] [cluster][Cluster][2518] [info] configuration has been applied [state: Active commit_id: 01983748-b9d6-7e04-af64-09df02c3ed97]
[2025-07-23 15:19:43.297371] [cluster][Cluster][2518] [info] send configuration to standby [commit_id: 01983748-b9d6-7e04-af64-09df02c3ed97]
[2025-07-23 15:19:43.345885] [cluster][Cluster][2512] [error] closing connection due to an error: conn='192.168.250.1:5650'<->'192.168.250.2:5650' reason=RW error
```

```
[2025-07-23 15:19:43.345959] [cluster][Cluster][2518] [error] Sync link has been
broken
[2025-07-23 15:19:43.346134] [cluster][Cluster][2518] [info] peer has left AS cluster
```

Вывод устройства NGFW2 (удалено из кластера):

```
ngfw@LAB-Debian-ngfw-node-1:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log | grep
cluster
[2025-07-23 15:19:43.865098] [cluster][Cluster][43047] [info] configuring AS cluster
started [state: Standby commit_id: 01983748-b9d6-7e04-af64-09df02c3ed97]
[2025-07-23 15:19:43.865119] [cluster][Cluster][43047] [info] standby node has been
excluded from AS cluster
[2025-07-23 15:19:43.865132] [cluster][Cluster][43047] [info] change state [state:
'Standby' new_state: 'Standalone' reason: 'reset configuration']
```

30.19. Добавление устройств в кластер

- Чтобы добавить устройство в кластер:

1. На странице **Устройства** → **Кластеры** выберите кластер, в который хотите добавить устройство.
2. Нажмите **Изменить**.

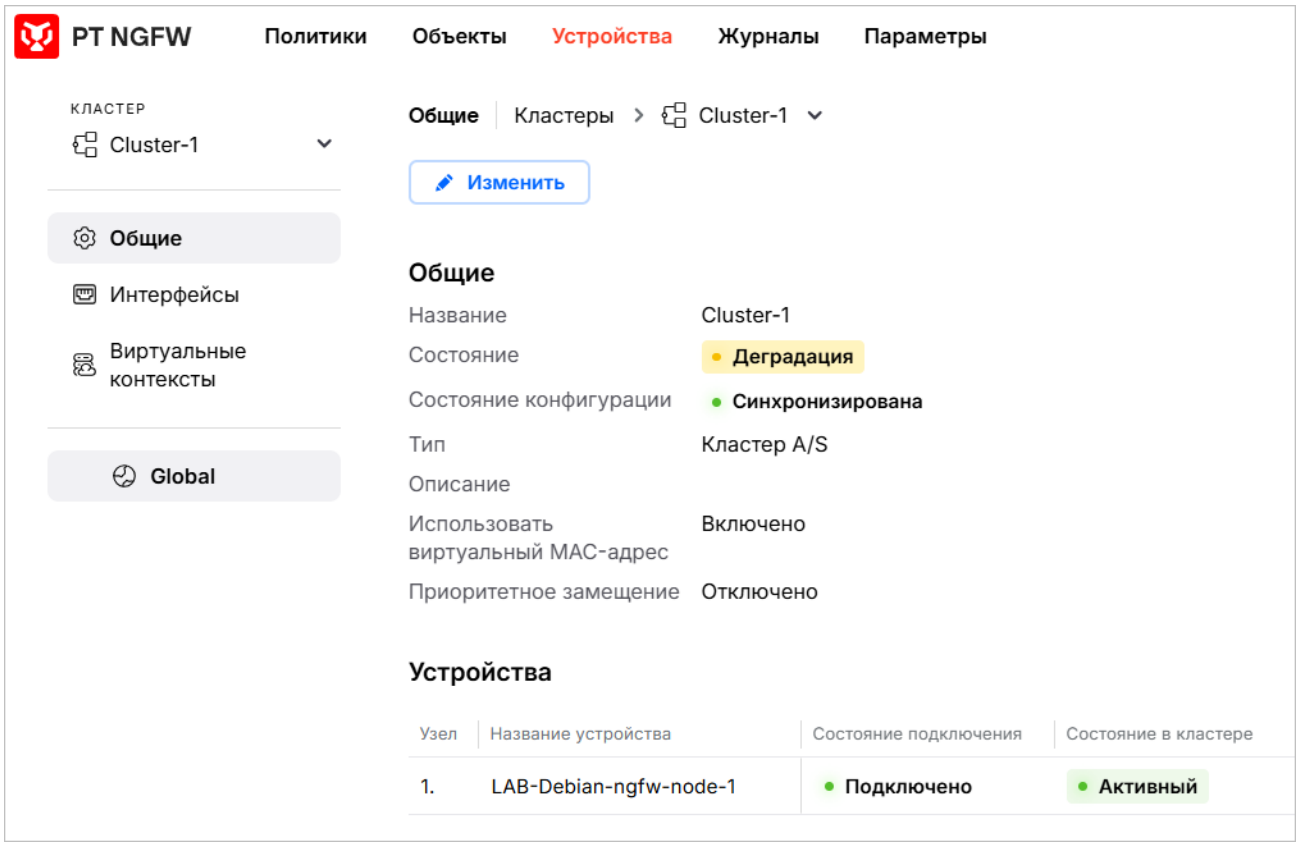


Рисунок 279. Общие параметры кластера

3. В окне с параметрами кластера в блоке **Устройства** нажмите **Добавить**.

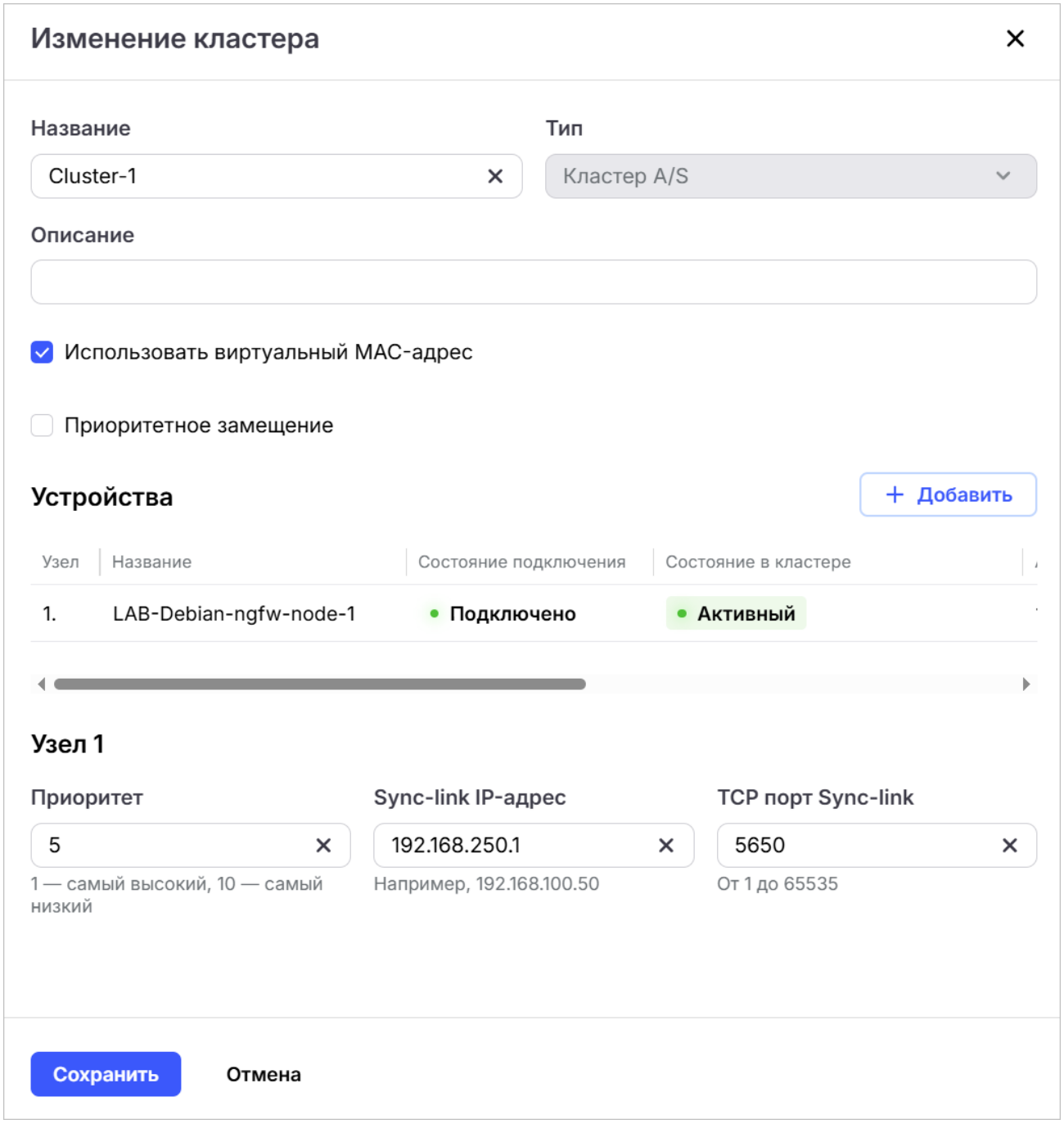


Рисунок 280. Добавление устройства в кластер

4. Выберите устройство для добавления в кластер.

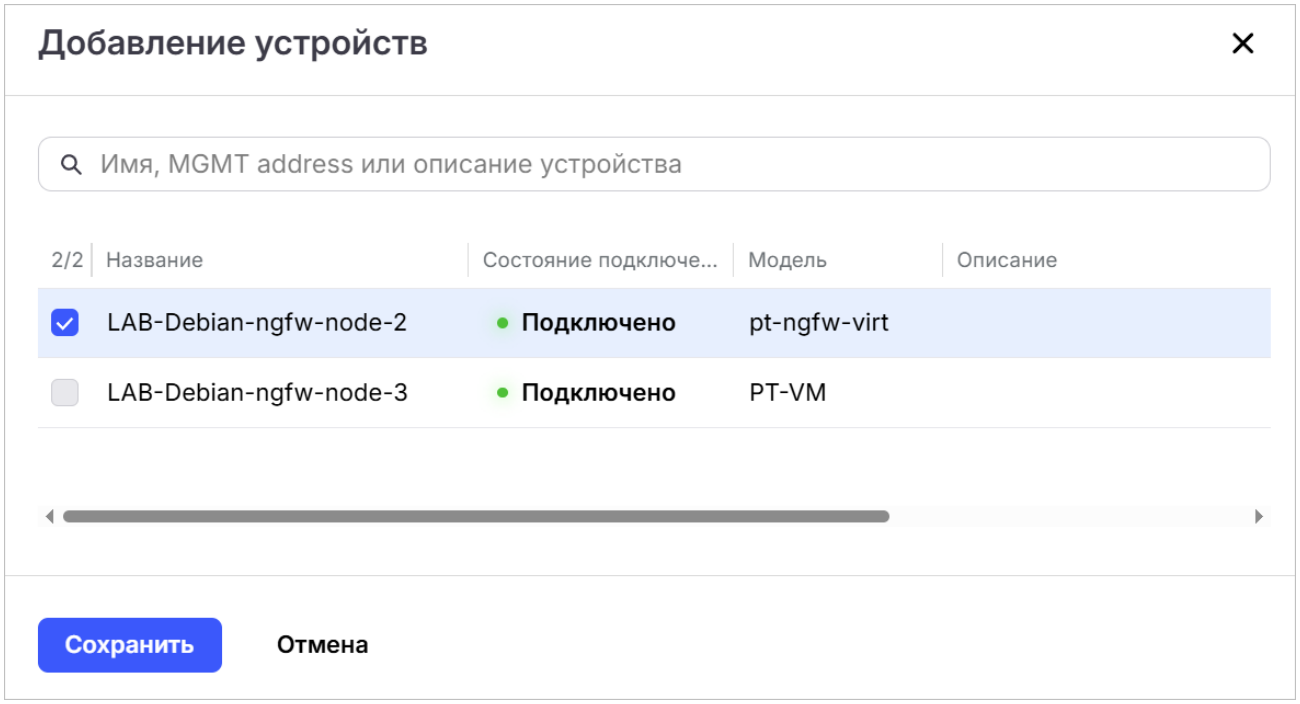


Рисунок 281. Выбор устройства

5. Нажмите **Сохранить**.
6. Укажите приоритет и адрес IP-интерфейса Sync-link добавляемого узла.

   Добавляемый узел помечается значком , который означает, что он будет добавлен в кластер только после сохранения изменений и применения конфигурации.
7. Нажмите **Сохранить**.

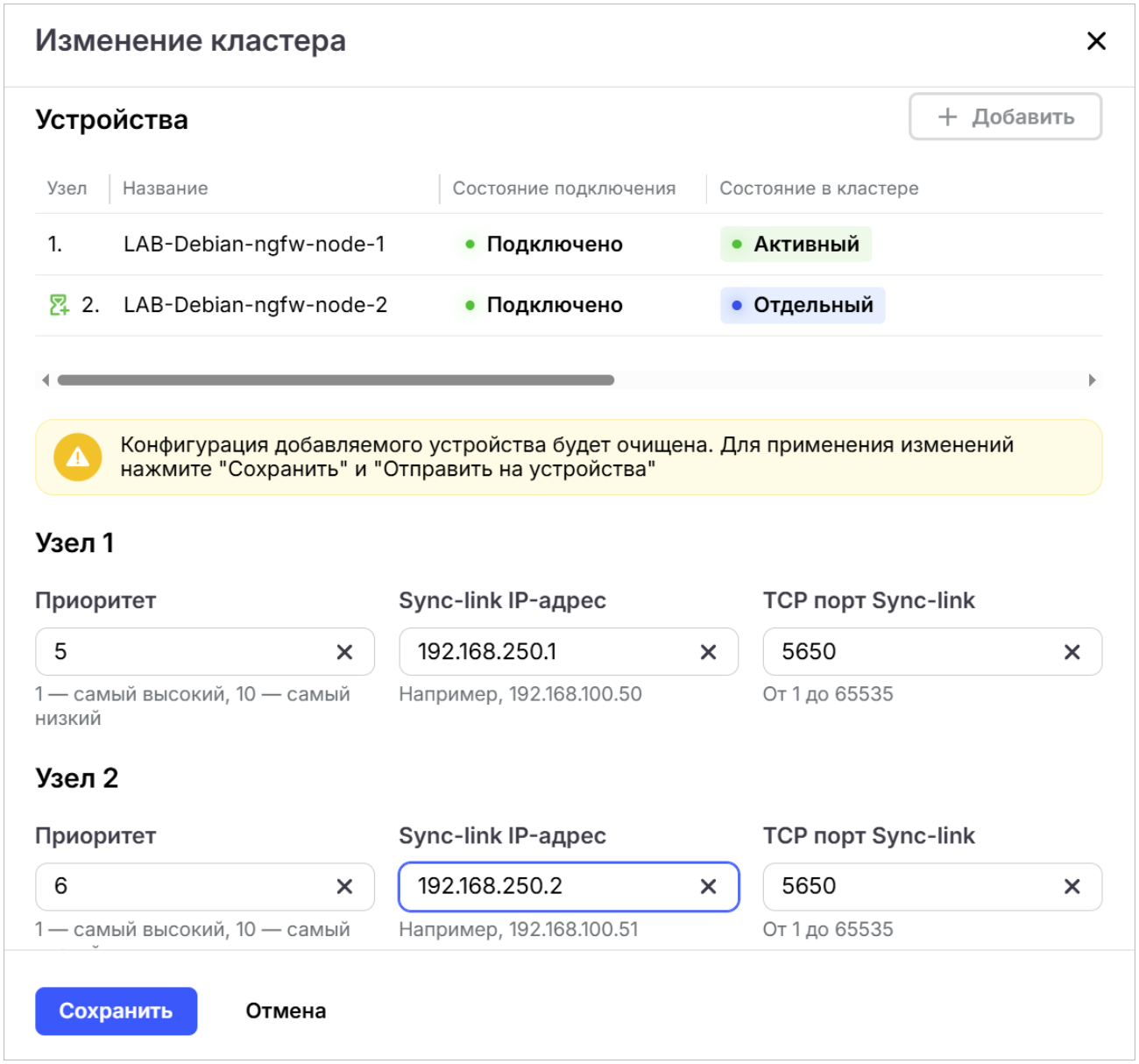


Рисунок 282. Сохранение параметров кластера

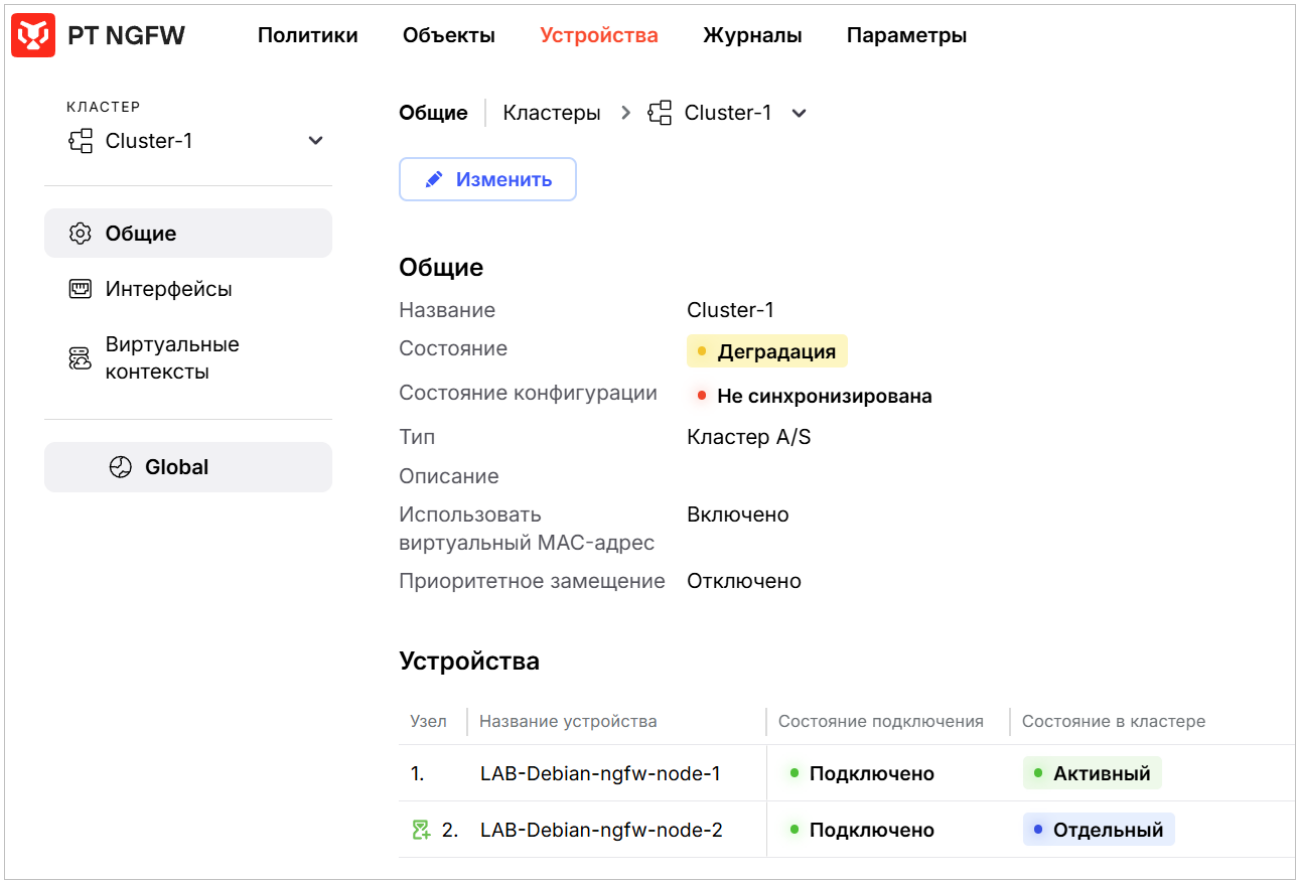


Рисунок 283. Общие параметры кластера

8. Нажмите **Отправить на устройства**, чтобы применить конфигурацию.

   После успешного применения конфигурации и добавления устройства на странице с общими параметрами кластера будет отображаться его обновленный статус.

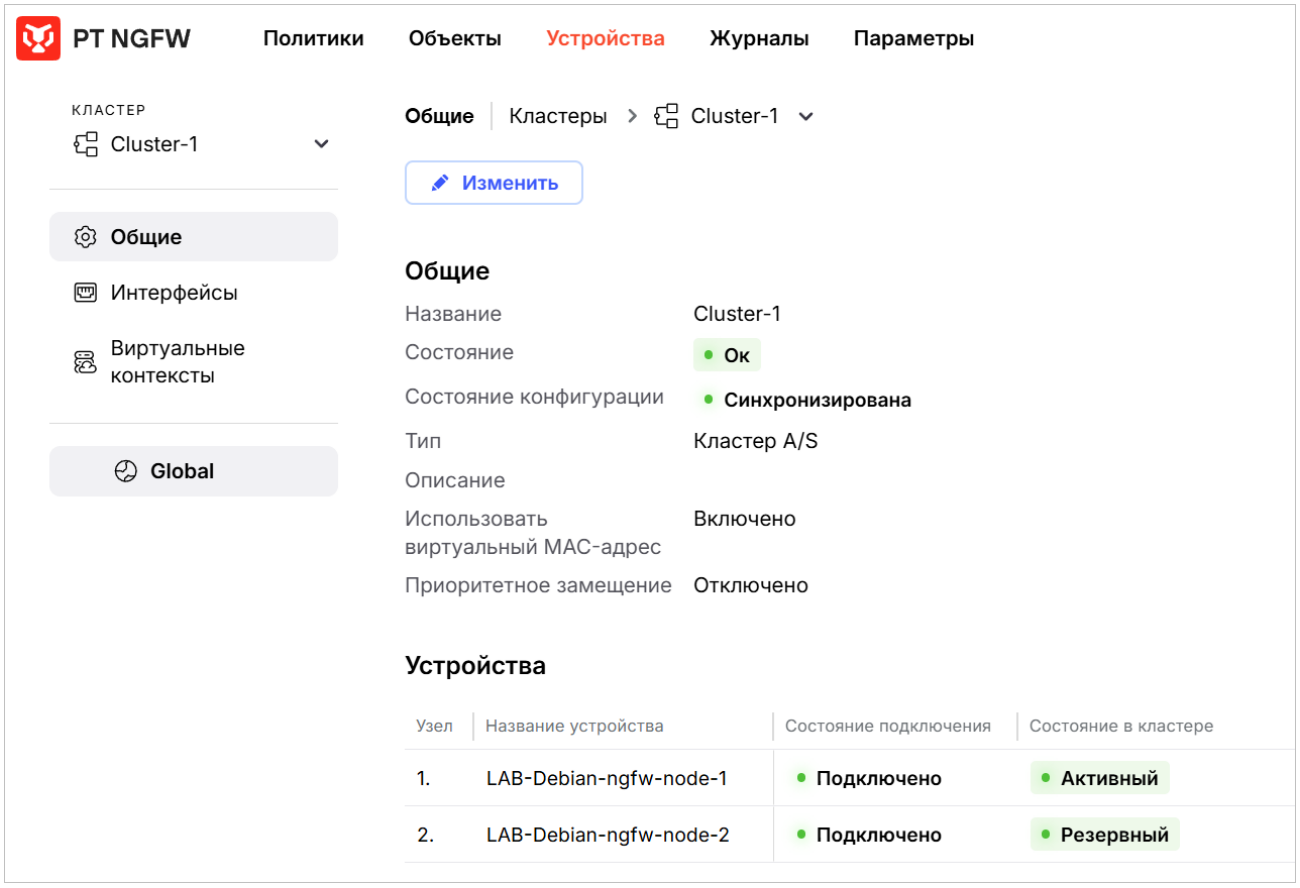


Рисунок 284. Изменение состояния кластера

Пример записей системного журнала

Вывод устройства NGFW1 (активный):

```
ngfw@LAB-Debian-ngfw-node-1:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log | grep
[2025-07-23 16:29:54.406941] [cluster][Cluster][2518] [info] configuring AS cluster
started [state: Active commit_id: 01983788-fc84-75bd-aee6-1988377fedd3]
[2025-07-23 16:29:54.406990] [cluster][Cluster][2518] [info] AS cluster sync link
initialization started
[2025-07-23 16:29:54.408773] [cluster][Cluster][2513] [info] Peer versions: 14.0,15.0
[2025-07-23 16:29:54.408809] [cluster][Cluster][2513] [info] Selected version: 15.0
[2025-07-23 16:29:54.408821] [cluster][Cluster][2513] [info] peer connected
[conn='192.168.250.1:5650'<->'192.168.250.2:5650']
[2025-07-23 16:29:54.418388] [cluster][Cluster][2518] [info] sync link is ready
[state: Active peer_state: Standalone]
[2025-07-23 16:29:54.418416] [cluster][Cluster][2518] [info] configuring device as
'Active'
[2025-07-23 16:29:54.606026] [cluster][Cluster][2518] [info] Configuration has been
successfully applied on peer [commit_id=01983788-fc84-75bd-aee6-1988377fedd3]
[2025-07-23 16:29:54.613033] [cluster][Cluster][2518] [info] configuration has been
applied [state: Active commit_id: 01983788-fc84-75bd-aee6-1988377fedd3]
```

```
[2025-07-23 16:29:54.613107] [cluster][Cluster][2518] [info] send configuration to
standby [commit_id: 01983788-fc84-75bd-aee6-1988377fedd3]
[2025-07-23 16:29:54.871603] [cluster][Cluster][2518] [info] Configuration has been
successfully applied on peer [commit_id=01983788-fc84-75bd-aee6-1988377fedd3]
```

Вывод устройства NGFW2 (добавляется в кластер):

```
ngfw@LAB-Debian-ngfw-node-1:~$ tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log | grep
cluster
[2025-07-23 16:29:54.976699] [cluster][Cluster][43047] [info] initializing AS cluster
started [state: Standalone commit_id: 01983788-fc84-75bd-aee6-1988377fedd3]
[2025-07-23 16:29:54.976723] [cluster][Cluster][43047] [info] AS cluster sync link
initialization started
[2025-07-23 16:29:54.978080] [cluster][Cluster][43041] [info] Peer versions:
14.0,15.0
[2025-07-23 16:29:54.978113] [cluster][Cluster][43041] [info] Selected version: 15.0
[2025-07-23 16:29:54.978125] [cluster][Cluster][43041] [info] peer connected
[conn='192.168.250.2:5650'<->'192.168.250.1:5650']
[2025-07-23 16:29:54.987970] [cluster][Cluster][43047] [info] sync link is ready
[state: Standalone peer_state: Active]
[2025-07-23 16:29:54.988012] [cluster][Cluster][43047] [info] configuring device as
'Standby'
[2025-07-23 16:29:55.172981] [cluster][Cluster][43047] [info] change state [state:
'Standalone' new_state: 'Standby' reason: 'successful configuration']
[2025-07-23 16:29:55.172999] [cluster][Cluster][43047] [info] configuration has been
applied [state: Standby commit_id: 01983788-fc84-75bd-aee6-1988377fedd3]
[2025-07-23 16:29:55.184125] [cluster][Cluster][43047] [info] configuring AS cluster
started [state: Standby commit_id: 01983788-fc84-75bd-aee6-1988377fedd3]
[2025-07-23 16:29:55.184142] [cluster][Cluster][43047] [info] configuring device as
'Standby'
[2025-07-23 16:29:55.440614] [cluster][Cluster][43047] [info] configuration has been
applied [state: Standby commit_id: 01983788-fc84-75bd-aee6-1988377fedd3]
```

30.20. Удаление кластера

Внимание! Удаление кластера, состоящего из двух устройств, не поддерживается. Необходимо сначала удалить одно из устройств, а затем удалить кластер, в котором осталось только одно устройство.

- Чтобы удалить кластер:

1. Удалите одно из устройств кластера (см. раздел 30.18).

   Внимание! После удаления устройства из кластера и применения изменений конфигурация удаленного устройства будет очищена. Это необходимо для предотвращения присутствия в сети двух устройств с одинаковой конфигурацией.

2. После того как в кластере осталось одно устройство, на странице **Устройства** → **Кластеры** в контекстном меню удаляемого кластера выберите **Удалить**.

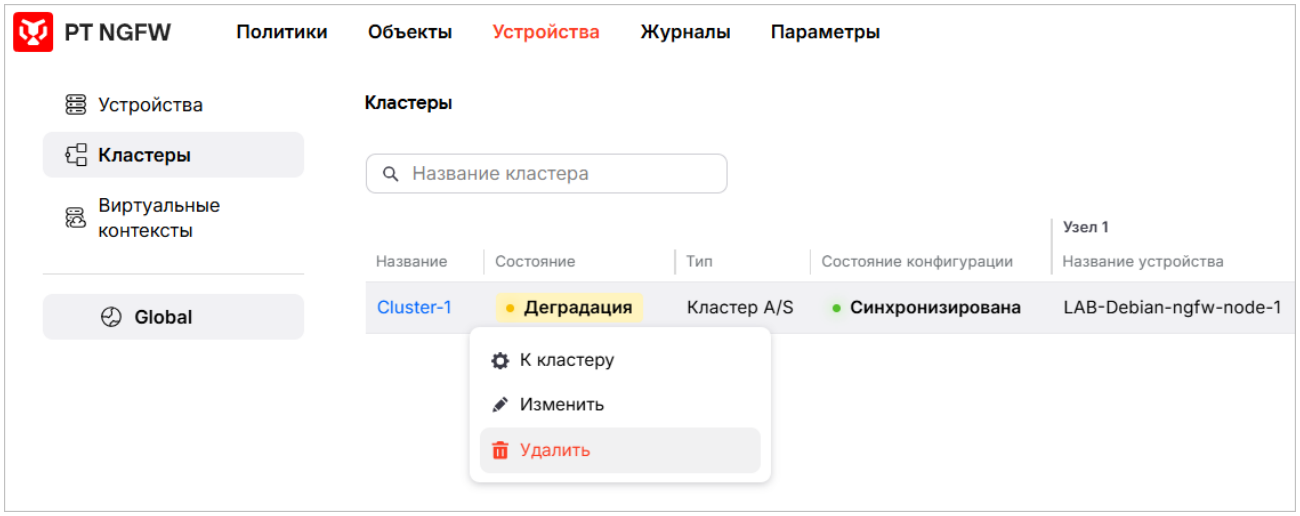


Рисунок 285. Удаление кластера

3. Если вы хотите сохранить конфигурацию кластера на устройстве, которое удаляется из кластера последним, в раскрывающемся списке выберите это устройство.

   Если выбрать **Не сохранять конфигурацию кластера**, конфигурация устройства будет очищена после его выхода из кластера.

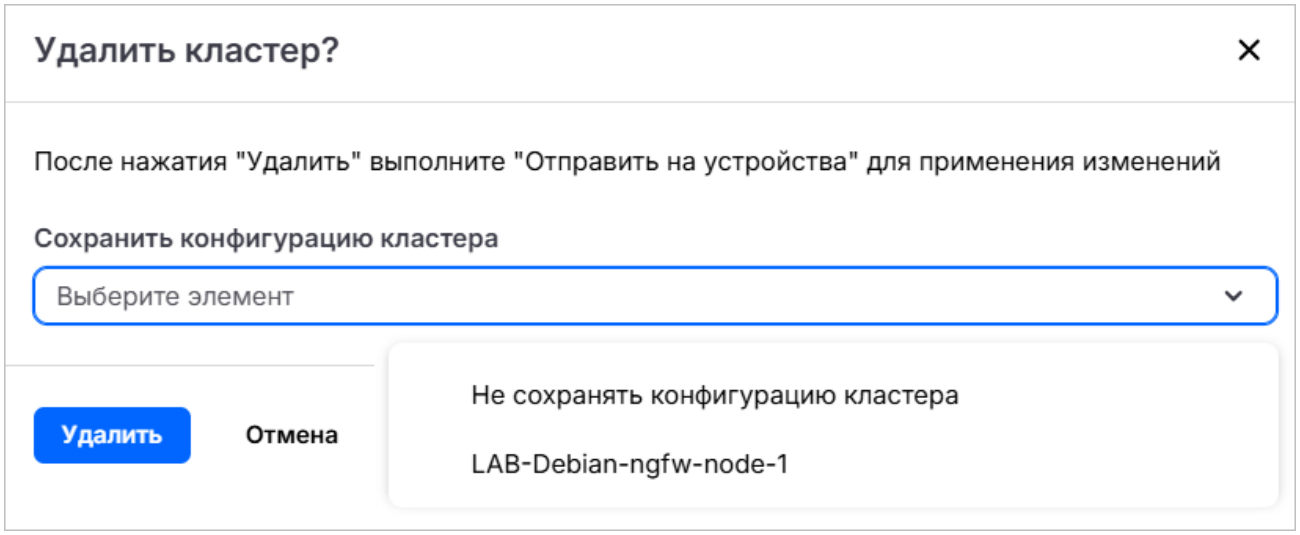


Рисунок 286. Варианты сохранения конфигурации кластера

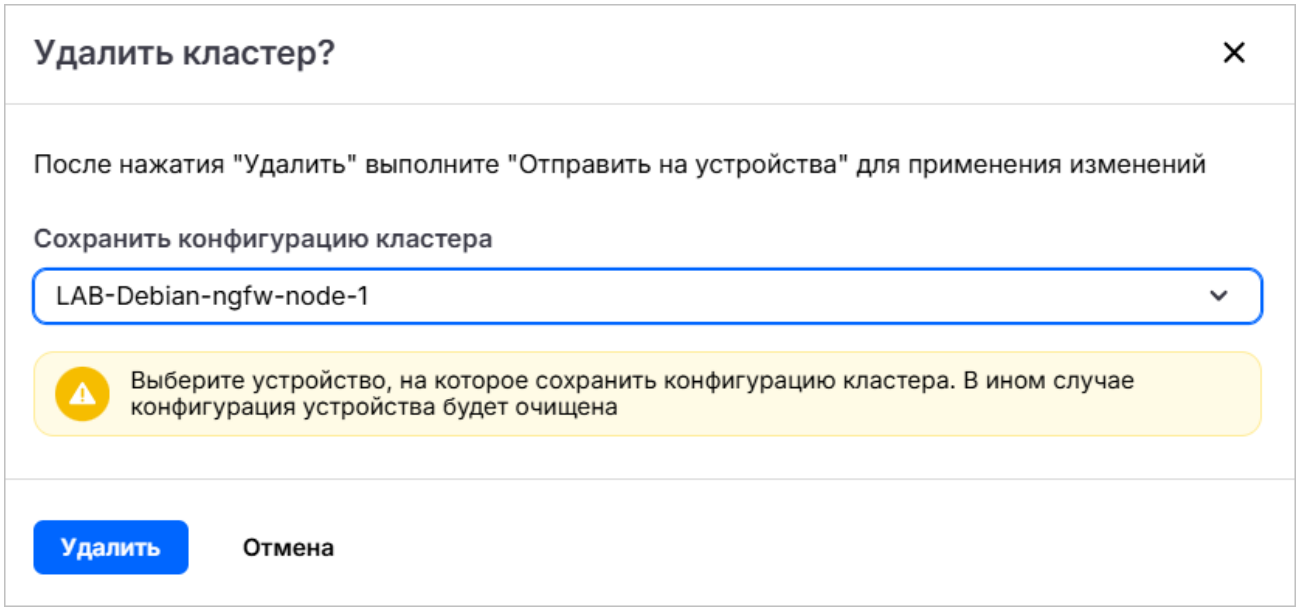


Рисунок 287. Сохранение конфигурации кластера на устройстве

4. Нажмите **Удалить**.
5. Кластер помечается значком , который означает, что он будет удален после применения конфигурации.

   Примечание. На этом этапе вы можете отменить удаление, выбрав соответствующий пункт в контекстном меню кластера.

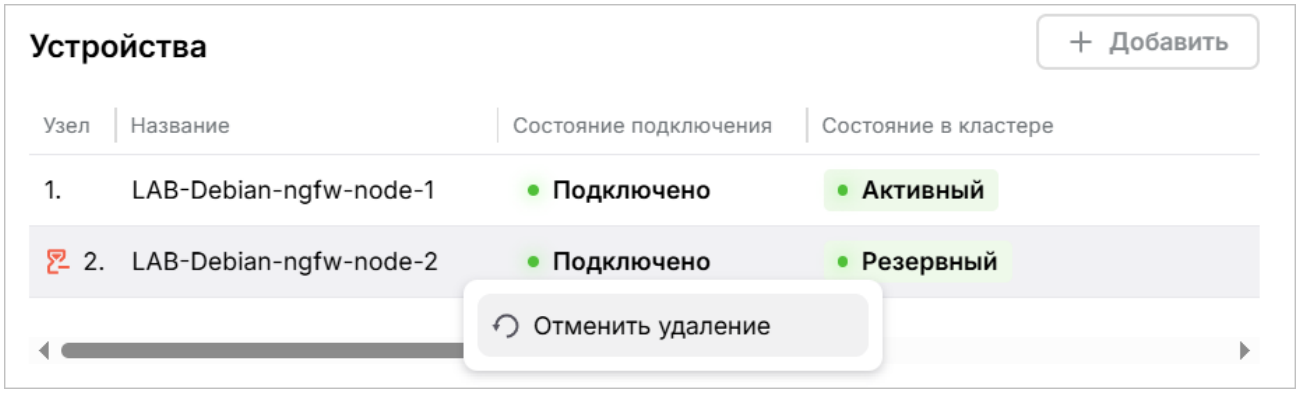


Рисунок 288. Отмена удаления кластера

6. Нажмите **Отправить на устройства**, чтобы применить конфигурацию.

   Вы можете просмотреть результаты удаления кластера в системном журнале.

Пример записей системного журнала

Узел NGFW1 (последний узел кластера) применяет новую конфигурацию и становится отдельным (некластерным) узлом (Standalone):

```
ngfw@LAB-Debian-ngfw-node-1:~$ sudo tail -f /opt/pt-ngfw/ngfw-core/logs/ngfw.log |
grep cluster
[2025-07-23 16:38:49.693507] [cluster][Cluster][2518] [info] configuring AS cluster
started [state: Active commit_id: 01983791-269d-76f0-ad44-1b49404a9e4f]
[2025-07-23 16:38:49.693518] [cluster][Cluster][2518] [info] Active node of AS
cluster has been configured as standalone node
[2025-07-23 16:38:49.693525] [cluster][Cluster][2518] [info] configuring device as
'Standalone'
[2025-07-23 16:38:49.862706] [cluster][Cluster][2518] [info] change state [state:
'Active' new_state: 'Standalone' reason: 'successful configuration']
[2025-07-23 16:38:49.862721] [cluster][Cluster][2518] [info] configuration has been
applied [state: Standalone commit_id: 01983791-269d-76f0-ad44-1b49404a9e4f]
```

31. Кластер системы управления

Резервирование системы управления — важный этап в обеспечении отказоустойчивости PT NGFW. Сбой в работе системы управления не прерывает обработку трафика, однако приводит к потере доступа к администрированию и конфигурированию PT NGFW. Вы можете объединить два узла с развернутой системой управления в отказоустойчивый кластер, сохраняющий работоспособность системы управления при выходе из строя любого из узлов.

Узлы кластера могут работать в активном или пассивном режиме, при этом активный узел обеспечивает работу системы управления, а пассивный работает в режиме ожидания.

Все изменения конфигурации и операции по управлению PT NGFW выполняются на активном узле и затем реплицируются на пассивный. Обратная синхронизация с пассивного узла на активный не предусмотрена. Синхронизация конфигурации выполняется сразу после внесения изменений. Внести изменения или применить политику на пассивном узле невозможно до его назначения активным. При попытке подключения к веб-интерфейсу управления пассивного узла запрос будет перенаправлен на активный узел. Таким образом, все изменения выполняются на активном узле, как если бы администратор подключался непосредственно к нему.

Настройка и диагностика кластера, а также переключение режимов его работы осуществляются вручную в командном интерпретаторе.

Особенности использования кластера системы управления

— Не допускается одновременная работа обоих узлов кластера системы управления в активном режиме — это приведет к рассинхронизации и потере части настроек. Перед переключением кластера переведите активный узел в режим обслуживания.

— Независимо от того, к какому из узлов кластера подключается администратор, работа с системой управления фактически ведется на активном узле. При подключении к пассивному узлу (в том числе по IP-адресу пассивного узла) он принимает запросы администратора и перенаправляет их на активный узел, отображая его данные. Веб-интерфейс пассивного узла при этом остается недоступен. Это гарантирует внесение изменений только на активном узле при любом варианте подключения администратора.

— При нарушении связи между активным и пассивным узлами подключение к системе управления через пассивный узел становится невозможным, а веб-интерфейс доступен только на активном узле. Синхронизация настроек приостанавливается до момента восстановления связи между узлами кластера.

Развертывание кластера системы управления

► Чтобы развернуть кластер системы управления:

1. Выберите два узла с развернутой системой управления PT NGFW либо подготовьте два узла с одинаковыми системными характеристиками и разверните на них систему управления.

Примечание. Версии системы управления на узлах кластера должны совпадать. Если вы используете версию системы управления ниже 1.9.0, то перед развертыванием кластера обновите ее до версии 1.9.0 или выше.

2. Выберите узел, который будет работать в активном режиме, и создайте его резервную копию (см. раздел 41). Это поможет вернуть конфигурацию к исходному состоянию в случае неудачного развертывания кластера.

   Примечание. После создания резервной копии скачайте и сохраните ее локально.

3. Подключитесь к командному интерпретатору активного узла.
4. Откройте конфигурационный файл `msctl.yaml` для редактирования:
   ```
   $ sudo nano /opt/pt-ngfw/ngfw-ms-msctl/config/msctl.yaml
   ```
5. В секции `[remote]` задайте параметры подключения к пассивному узлу:
   - `postgres_address: <Адрес>:<Порт>` — параметры подключения к службе postgresql пассивного узла, где:

     `<Адрес>` — IP-адрес или доменное имя пассивного узла;

     `<Порт>` — номер порта службы postgresql (по умолчанию — 5432);
   - `api_address: <Адрес>:<Порт>` — параметры подключения к API пассивного узла, где:

     `<Адрес>` — IP-адрес или доменное имя пассивного узла;

     `<Порт>` — номер порта API (по умолчанию — 8040);
   - `s3_address: <Адрес>:<Порт>` — параметры подключения к объектному хранилищу пассивного узла, где:

     `<Адрес>` — IP-адрес или доменное имя пассивного узла;

     `<Порт>` — номер порта объектного хранилища (по умолчанию — 8230);
   - `replication_password: <Пароль>` — пароль пользователя репликации;

     Примечание. Пароли пользователя репликации должны совпадать на обоих узлах кластера.
   - `enable_tls: <true | false>` — включить или выключить TLS-шифрование при обмене данными с пассивным узлом.
6. Сохраните изменения **Ctrl+O** и закройте редактор **Ctrl+X**.
7. Примените конфигурацию активного узла:
   ```
   $ sudo msctl setup
   ```
8. Дождитесь завершения операции, после чего убедитесь, что узел запущен в активном режиме:
   ```
   $ sudo msctl status
   PostgreSQL status:
   - Role: Active
   - Health: Ok
   ```

```
MS status:
- Role: Active
- Maintenance mode: disabled
```

9. Подключитесь к командному интерпретатору пассивного узла.
10. Откройте конфигурационный файл msctl.yaml для редактирования:
    ```
    $ sudo nano /opt/pt-ngfw/ngfw-ms-msctl/config/msctl.yaml
    ```
11. В секции `[remote]` задайте параметры подключения к активному узлу:
    - `postgres_address: <Адрес>:<Порт>` — параметры подключения к службе postgresql активного узла, где:

      `<Адрес>` — IP-адрес или доменное имя активного узла;

      `<Порт>` — номер порта службы postgresql (по умолчанию — 5432);
    - `api_address: <Адрес>:<Порт>` — параметры подключения к API активного узла, где:

      `<Адрес>` — IP-адрес или доменное имя активного узла;

      `<Порт>` — номер порта API (по умолчанию — 8040);
    - `s3_address: <Адрес>:<Порт>` — параметры подключения к объектному хранилищу активного узла, где:

      `<Адрес>` — IP-адрес или доменное имя активного узла;

      `<Порт>` — номер порта объектного хранилища (по умолчанию — 8230);
    - `replication_password: <Пароль>` — пароль пользователя репликации;

      Примечание. Пароли пользователя репликации должны совпадать на обоих узлах кластера.
    - `enable_tls: <true | false>` — включить или выключить TLS-шифрование при обмене данными с активным узлом.
12. Сохраните изменения **Ctrl+O** и закройте редактор **Ctrl+X**.
13. Примените конфигурацию пассивного узла:
    ```
    $ sudo msctl setup
    ```
14. Переключите узел в пассивный режим:
    ```
    $ sudo msctl standby
    ```
15. Дождитесь завершения операции, после чего убедитесь, что узел запущен в пассивном режиме:
    ```
    $ sudo msctl status
    PostgreSQL status:
    - Role: Standby
    - Health: Ok
    MS status:
    - Role: Standby
    - Maintenance mode: disabled
    ```

Переключение кластера системы управления

При переключении кластера пассивный узел становится активным и далее обеспечивает работу системы управления, а узел, который был активным, переводится в пассивный режим. Переключение кластера выполняется вручную в случаях неработоспособности активного узла, например при выходе из строя аппаратной платформы. Перед переключением активный узел переводится в режим обслуживания и игнорирует управляющие запросы.

- Чтобы переключить кластер системы управления:

  1. Подключитесь к командному интерпретатору активного (первого) узла.
  2. Переключите активный узел в режим обслуживания:
     ```
     $ sudo msctl maintenance --enable
     ```
  3. Подключитесь к командному интерпретатору пассивного (второго) узла.
  4. Переключите второй узел в активный режим:
     ```
     $ sudo msctl active
     ```
  5. Подключитесь к командному интерпретатору первого узла (который ранее работал в активном режиме).
  6. Переключите первый узел в пассивный режим:
     ```
     $ sudo msctl standby
     ```
  7. Выключите режим обслуживания:
     ```
     $ sudo msctl maintenance --disable
     ```

  В результате второй узел переключится в активный режим и начнет обеспечивать работу системы управления, а первый продолжит работу в пассивном режиме.

Пример настройки кластера системы управления

Рассмотрим пример настройки кластера системы управления, состоящего из двух узлов:

— Node1 — узел с развернутой системой управления и IP-адресом доступа 10.13.18.61.

— Node2 — узел с развернутой системой управления и IP-адресом доступа 10.13.17.14.

В качестве активного узла выбран узел Node1. В этом случае секции `[remote]` в файлах конфигурации должны быть заданы следующим образом:

Таблица 18. Параметры кластера в файле msctl.yaml

Параметры на узле Node1	Параметры на узле Node2
`remote:`	`remote:`
`postgres_address: "10.13.17.14:5432"`	`postgres_address: "10.13.18.61:5432"`
`s3_address: "10.13.17.14:8230"`	`s3_address: "10.13.18.61:8230"`
`api_address: "10.13.17.14:8040"`	`api_address: "10.13.18.61:8040"`

Параметры на узле Node1	Параметры на узле Node2
`replication_password: "P@ssw0rd"` `enable_tls: true`	`replication_password: "P@ssw0rd"` `enable_tls: true`

32. Туннелирование GRE и GRE over IPsec

PT NGFW поддерживает туннелирование трафика посредством GRE и GRE over IPsec.

Протокол GRE (Generic Routing Encapsulation) предназначен для инкапсуляции сетевого трафика и позволяет передавать пакеты разных сетевых протоколов через IP-соединения типа точка-точка. Поддержка туннелей GRE не требует больших накладных расходов, проста в настройке и, в отличие от IPsec Site-to-Site VPN (см. раздел 33), поддерживает многоадресную и широковещательную рассылку.

Протокол GRE не предоставляет встроенных механизмов аутентификации трафика, и не поддерживает шифрование и защиту целостности данных. Поэтому для организации безопасных каналов связи через сети общего пользования применяется комбинация GRE over IPsec (см. раздел 32.2), когда данные, передаваемые через туннель GRE, защищаются средствами IPsec.

В этом разделе

Настройка туннеля GRE (см. раздел 32.1)

Настройка туннеля GRE over IPsec (см. раздел 32.2)

32.1. Настройка туннеля GRE

В процессе настройки туннеля GRE создается логический туннельный интерфейс, который будет использоваться для взаимодействия с удаленным узлом (пиром).

Чтобы добавить и настроить туннель GRE:

1. В главном меню нажмите **Устройства** → **Устройства** и выберите устройство, для которого хотите создать туннель GRE.
2. Если требуется сменить контекст, нажмите **Виртуальные контексты** и выберите контекст.
3. Выполните одно из действий:
   - Нажмите **Интерфейсы** → **Добавить** → **GRE**.
   - Нажмите **GRE** → **Добавить** → **GRE**.

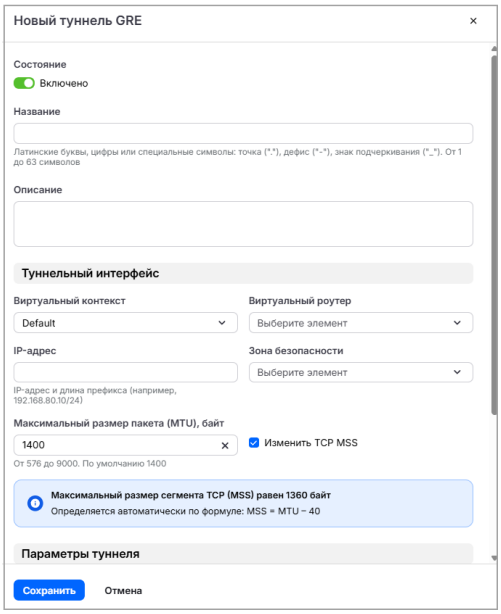


Рисунок 289. Создание туннеля GRE

4. Введите параметры туннельного интерфейса:

   — **Название** — имя туннельного интерфейса.

   — **Описание** — текстовое описание.

   — **Виртуальный контекст** — выберите из списка.

   — **Виртуальный роутер** — выберите из списка.

   — **Зона безопасности** — выберите из списка.

   Примечание. Виртуальный роутер и зону безопасности можно выбрать, только если выбран виртуальный контекст.

   — **IP-адрес** — адрес туннельного интерфейса.

   — **Максимальный размер пакета (MTU)** — значение MTU для туннельного интерфейса в байтах.

   — Если требуется, установите флажок **Изменить TCP MSS**. При этом размер MSS будет определяться по формуле: MSS = MTU – 40.

5. Введите параметры туннеля:

   — **Интерфейс** — выберите из списка.

   Примечание. Интерфейс можно выбрать, только если выбран виртуальный контекст.

   — **Тип адреса пира** — тип адреса удаленного узла: **IP-адрес** или **FQDN**.

   — **Адрес пира** — адрес удаленного узла согласно выбранному типу.

   — **Key ID** — целочисленный идентификатор туннеля. Опциональный параметр, позволяет различать несколько туннелей с совпадающими IP-адресами источника и получателя.

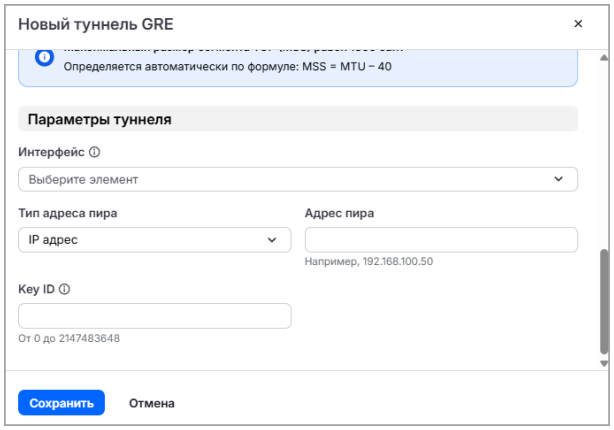


Рисунок 290. Настройка параметров туннеля

6. Нажмите **Сохранить**

32.2. Настройка туннеля GRE over IPsec

Технология GRE over IPsec позволяет сочетать возможности GRE-инкапсуляции и IPsec-шифрования для построения защищенных каналов связи поверх сетей общего пользования. Туннелирование GRE over IPsec обеспечивает передачу multicast пакетов, что требуется, например, для работы протоколов динамической маршрутизации.

- Чтобы создать туннель GRE over IPsec на PT NGFW:

1. В главном меню нажмите **Устройства** → **Устройства** и выберите устройство, для которого хотите добавить туннель GRE over IPsec.
2. Если требуется сменить контекст, нажмите **Виртуальные контексты** и выберите контекст.
3. Выполните одно из действий:
   - Нажмите **Интерфейсы** → **Добавить** → **GRE over IPsec**.
   - Нажмите **GRE** → **Добавить** → **GRE over IPsec**.

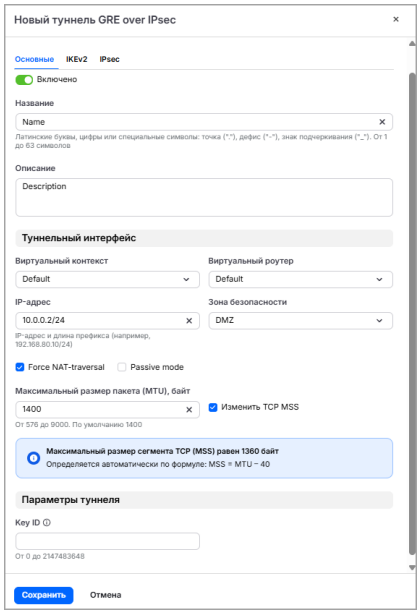


Рисунок 291. Создание туннеля GRE over IPsec

4. На вкладке **Основные** настройте параметры создаваемого туннельного интерфейса:
   - **Название** — имя туннельного интерфейса.
   - **Описание** — текстовое описание.
   - **Виртуальный контекст** — выберите из списка.
   - **Виртуальный роутер** — выберите из списка.
   - **Зона безопасности** — выберите из списка.

     Примечание. Виртуальный роутер и зону безопасности можно выбрать, только если выбран виртуальный контекст.
   - **IP-адрес** — адрес туннельного интерфейса.
   - **Максимальный размер пакета (MTU)** — значение MTU для туннельного интерфейса в байтах.
   - Если требуется, установите флажок **Force NAT-traversal**.

     Примечание. Если параметр включен, VPN-шлюз всегда инкапсулирует IPsec-пакеты в UDP, используя порт 4500, как если бы NAT был обнаружен.
   - Если требуется, установите флажок **Passive mode**. При этом межсетевой экран не будет первым инициировать IPsec-соединение.
   - Если требуется, установите флажок **Изменить TCP MSS**. При этом размер MSS будет определяться по формуле: MSS = MTU – 40.
   - **Key ID** — целочисленный идентификатор туннеля. Опциональный параметр, позволяет различать несколько туннелей с совпадающими IP-адресами источника и получателя.

5. На вкладке **IKEv2** настройте параметры протокола обмена ключами:
   - **Шифрование** — выберите необходимые алгоритмы шифрования.
   - **Аутентификация / PRF** — выберите алгоритмы хэширования.
   - **Обмен ключами / PFS** — выберите алгоритмы обмена ключами.
   - **Key lifetime** — время жизни сессионных ключей в секундах.
   - **Интерфейс** — сетевой интерфейс, который будет использоваться для соединения по протоколу IKEv2.

     Примечание. Интерфейс можно выбрать, только если выбран виртуальный контекст.
   - **Тип локального ID** — выберите из списка.
   - **Локальный ID** — введите в соответствии с выбранным типом.
   - **Pre-shared key** — значение предварительно распределенного ключа.

     Примечание. Рекомендуемая длина ключа — не менее 20 символов.
   - **Тип адреса** — выберите тип адреса пира из списка.
   - **Адрес** — введите адрес пира в соответствии с выбранным типом.
   - **Тип удаленного ID** — выберите тип идентификатора пира из списка
   - **Удаленный ID** — введите идентификатор пира в соответствии с выбранным типом.
   - **Ассиметричные pre-shared keys** — если требуется использование ассиметричных предварительно распределенных ключей, установите этот флажок и введите значение ключа.
   - **Dead Peer Detection (DPD)** — если требуется проверка доступности пира, установите этот флажок и задайте параметры проверки.
   - **DPD Interval —** значение интервала проверки пира (сек)**.**
   - **DPD retry** — количество повторных попыток проверки.

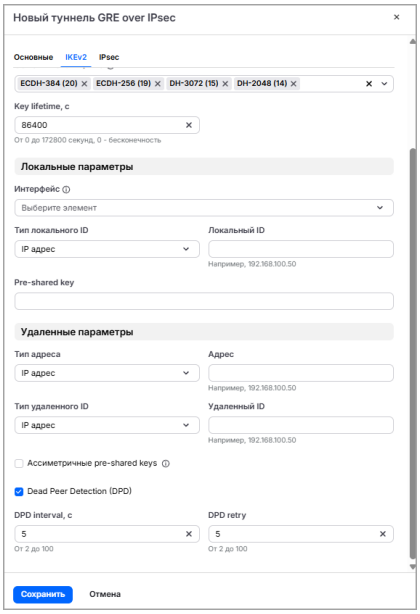


Рисунок 292. Настройка параметров протокола IKEv2

6. На вкладке **IPsec** настройте параметры протокола IPsec:
   - **Шифрование** — выберите необходимые алгоритмы шифрования
   - **Аутентификация** — выберите алгоритмы хэширования.
   - **Key lifetime** — время жизни сессионных ключей (сек).
   - **Key lifesize** — максимальный размер данных, шифруемых одним ключом (кбайт).
   - **Perfect Forward secrecy** — установите флажок если требуется уникальность сессионных ключей.

     Примечание. Эта функция обеспечивает уникальность сессионных ключей: для каждого сеанса связи создается новый, временный ключ, который уничтожается после завершения сессии.
7. Выберите способ защиты GRE-трафика (**Режим IPsec SA**):
   - **Туннельный** — выполняется полная инкапсуляция GRE-трафика.
   - **Транспортный** — шифруется только полезная нагрузка.

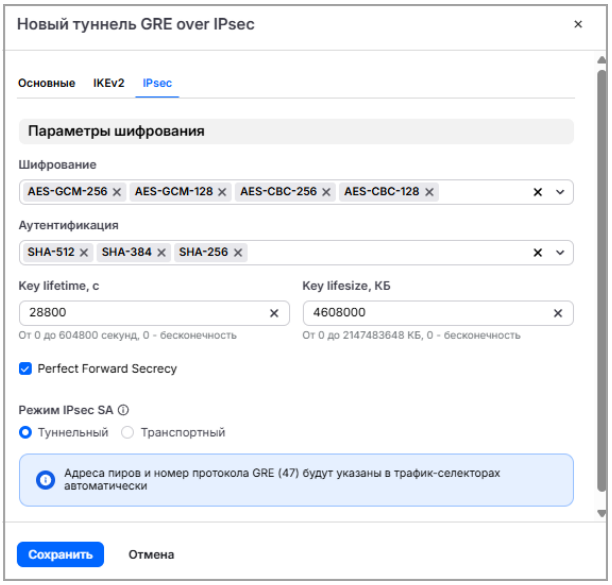


Рисунок 293. Настройка параметров IPsec

8. Нажмите **Сохранить**.

33. IPsec site-to-site VPN

Site-to-site VPN — это тип виртуальной частной сети, предназначенный для объединения двух или более удаленных сетей через защищенный туннель. Он используется для постоянного соединения между офисами, филиалами или дата-центрами организации с помощью IPsec и других VPN-протоколов. Основная задача — обеспечить безопасную маршрутизацию трафика между внутренними подсетями через публичные сети. Такой тип VPN особенно подходит для постоянного и автоматического обмена данными между сетями без участия конечных пользователей.

PT NGFW поддерживает возможность создания соединений site-to-site VPN. После установки туннеля устройства в одной сети получают доступ к ресурсам другой, как если бы они находились в одной локальной сети. Конфигурация site-to-site VPN включает настройку политик безопасности, идентификацию участвующих подсетей и определение параметров шифрования и аутентификации.

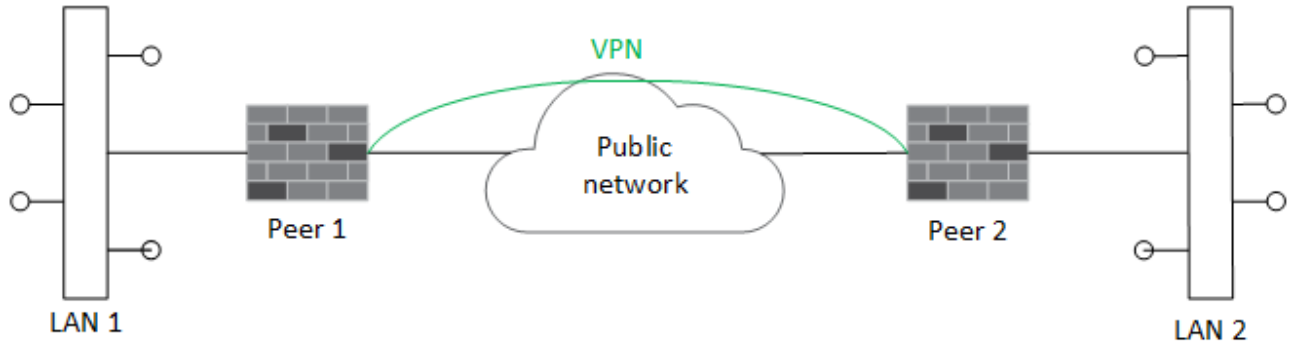


Рисунок 294. Схема соединения site-to-site VPN

В этом разделе

Преимущества Site-to-Site VPN (см. раздел 33.1)

Принцип работы и условия использования (см. раздел 33.2)

Создание Site-to-Site VPN-соединения (см. раздел 33.3)

33.1. Преимущества Site-to-Site VPN

Безопасность. Весь трафик между сетями шифруется, что защищает данные от перехвата и несанкционированного доступа при передаче через интернет.

Интеграция сетей. Обеспечивает единое адресное пространство и внутреннюю маршрутизацию между офисами. Позволяет использовать общие ресурсы (файловые серверы, базы данных, принтеры и т.п.).

Автоматизация. Соединение устанавливается между шлюзами и не требует участия пользователей — VPN работает на уровне сети и активен постоянно.

Масштабируемость. Можно подключать новые офисы или филиалы по той же схеме, используя единые политики безопасности.

Совместимость. Site-to-Site VPN реализован на многих сетевых устройствах и поддерживает стандартные протоколы (в частности — протоколы IPsec).

33.2. Принцип работы и условия использования

Фреймворк IPsec

Работа Site-to-Site VPN на основе фреймворка IPsec обеспечивается двумя протоколами: IKE (служебное взаимодействие между узлами и согласование всех параметров) и ESP (передача данных).

При создании IPsec-соединения автоматически создается туннельный интерфейс, который привязан только к этому соединению. IPsec-соединение и туннельный интерфейс — это составляющие одной сущности VPN. IPsec-соединение хранит в себе информацию о туннеле: протоколы шифрования, ограничения и селекторы трафика.

> **Примечание.** Для работы IPsec-соединения необходимо разрешить IPsec и IKE-трафик, создав соответствующие правила и создать статический маршрут между сетями, которые объединяются IPsec соединением.

Условия соединения по протоколу IKE

Для корректной установки соединения Site-to-Site VPN требуется соблюдение следующих условий:

— Пиры должны пройти взаимную аутентификацию — с использованием общего ключа (pre-shared key) или сертификатов — и обеспечить криптографическую защиту для последующего обмена.

— Пиры должны согласовать между собой:

- используемые криптографические протоколы и механизм генерации сессионных ключей;
- параметры защищаемого трафика (селекторы трафика), обычно представляющие собой пары подсетей, но допускается также указание конкретных портов и протоколов.

Для автоматического выполнения вышеуказанных условий во фреймворке IPSec используется протокол IKE, доступный в настоящий момент в двух версиях — IKEv1 и IKEv2. Версия IKEv1 не поддерживается PT NGFW, так как является устаревшей и не обеспечивает надлежащий уровень безопасности.

Работа IKEv2 через NAT

Для корректной работы протокола IKEv2 через NAT пиры при установке соединения через UDP-порт 500 обмениваются специальными сообщениями, с помощью которых определяется наличие NAT; если он обнаружен, дальнейший обмен информацией осуществляется через UDP-порт 4500.

Установка соседства в IKEv2

Отправка пакетов по протоколу IKEv2 осуществляется через UDP-порт 500 (источника и назначения). Поскольку промежуточные устройства NAT могут подменять порт источника, допускается прием входящих подключений IKEv2 с любого порта. Соседство в IKEv2 устанавливается посредством четырех сообщений (пара IKE_SA_INIT и пара IKE_AUTH).

В IKE_SA_INIT:

— пиры обмениваются наборами поддерживаемых криптографических протоколов (proposals), то есть инициатор перечисляет поддерживаемые им протоколы, а принимающая сторона отвечает, какой именно протокол она выбирает;

— генерируется пара DH-ключей для защиты последующего диалога.

В IKE_AUTH пиры выполняют взаимную аутентификацию и договариваются о наборе защищаемых сетей.

Для изменения набора защищаемых сетей, добавления или замены используемых ключей, а также удаления соседства используются отдельные сообщения.

Security Associations

В результате успешной установки соседства создаются две структуры данных — Security Associations (SA), содержащие полную информацию о соединении:

— IKEv2 SA — один для каждого VPN-соединения «точка — точка»:
  - принадлежность туннельному интерфейсу;
  - статус соединения;
  - IP-адреса пиров (локальный и удаленный);
  - криптоалгоритмы, используемые в обмене IKEv2;
  - время жизни сессии (общее и оставшееся).

— IPSec SA — пара (входящая и исходящая) для каждого туннеля (для пары подсетей):
  - принадлежность туннельному интерфейсу;
  - принадлежность родительскому IKEv2 SA;
  - IP-адреса пиров (локальный и удаленный);
  - согласованная пара селекторов трафика;

- количество переданных (шифрованных и расшифрованных) пакетов;
- MTU туннеля;
- идентификаторы SPI входящих и исходящих туннелей: криптоалгоритмы, используемые для шифрования трафика в туннеле и время жизни сессии (общее и оставшееся).

Алгоритмы шифрования, аутентификации и обмена ключами

PT NGFW поддерживает работу с современными алгоритмами, такими как:

— алгоритмы шифрования: AES-GCM-128/256, AES-CBC-128/256, 3DES, DES;

— алгоритмы аутентификации: SHA-2 (512/384/256), SHA-1, MD5;

— алгоритмы обмена ключами: ECDH-384 (group 20), ECDH-256 (group 19), DH-3072 (group 15), DH-2048 (group 14), DH-1024 (group 2), DH-768 (group 1).

33.3. Создание Site-to-Site VPN-соединения

► Чтобы создать Site-to-Site VPN-соединение:

1. В главном меню выберите **Устройства**.
2. Выберите устройство, для которого хотите добавить Site-to-Site VPN-соединение.
3. Выберите виртуальный контекст, для которого хотите добавить Site-to-Site VPN-соединение.
4. Выберите вкладку **Интерфейсы**.
5. Нажмите **Добавить** → **IPsec-туннель**.

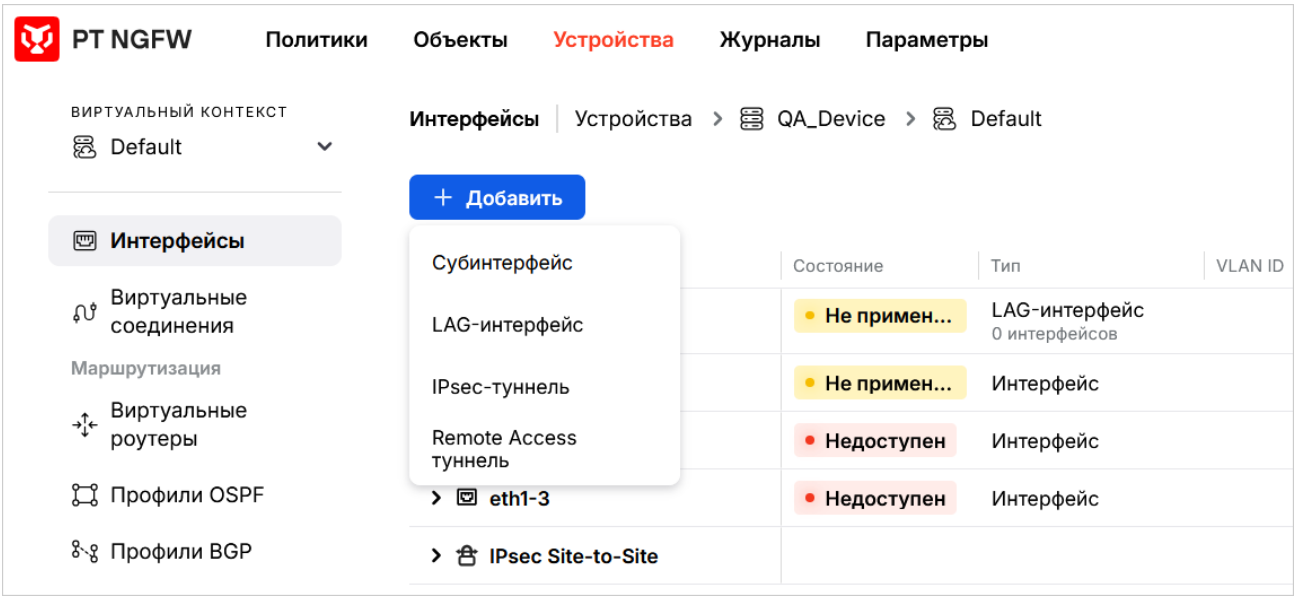


Рисунок 295. Добавление VPN-соединения

Примечание. Вы также можете создать соединение на вкладке **IPsec Site-to-Site**.

6. На вкладке **Основные** настройте параметры туннельного интерфейса:
   - Введите название туннельного интерфейса.

     Примечание. Рекомендуется добавлять описание для упрощения последующей работы.
   - Выберите виртуальный роутер.
   - Выберите зону безопасности.
   - Введите IP-адрес туннельного интерфейса.
   - Если требуется, установите флажок **Force NAT-traversal**.

     Примечание. Если параметр включен, VPN-шлюз всегда инкапсулирует IPsec-пакеты в UDP, используя порт 4500, как если бы NAT был обнаружен.
   - Если требуется, установите флажок **Passive mode**.

     Примечание. Если параметр включен, межсетевой экран не будет первым инициировать IPsec-соединение.
   - Укажите размер MTU для VPN-интерфейса в байтах.

     Примечание. Рекомендованное значение MTU: 1400.
   - Если требуется, установите флажок **Изменить TCP MSS**.

     Примечание. При установленном флажке размер MSS будет определяться по формуле: MSS = MTU – 40.

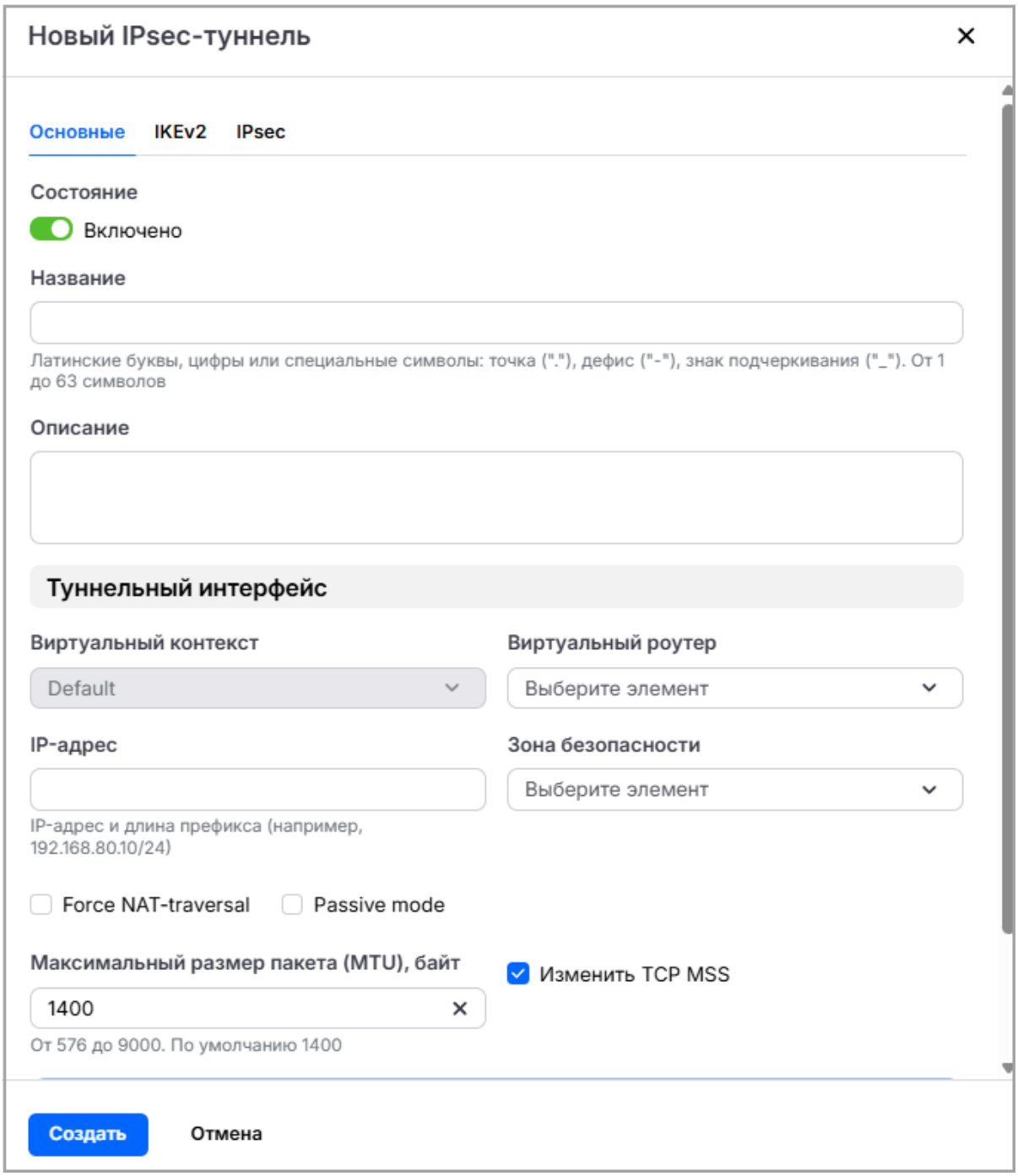


Рисунок 296. Вкладка **Основные**

7. На вкладке **IKEv2** настройте параметры протокола:
   - Выберите необходимые алгоритмы шифрования, аутентификации и обмена ключами.
   - Введите время жизни сессионных ключей в секундах.
   - Выберите интерфейс, который будет использоваться для соединения по протоколу IKEv2.

- Выберите тип локального ID.
- Введите локальный ID.
- Введите значение предварительно распределенного ключа.

  Примечание. Рекомендуемая длина ключа — не менее 20 символов.
- Выберите тип адреса.
- Введите адрес пира.
- Введите тип идентификатора пира.
- Введите идентификатор пира.
- Если требуется использование ассиметричных предварительно распределенных ключей, установите соответствующий флажок и введите значение ключа.
- Если требуется включить проверку доступности пира, установите флажок **Dead Peer Detection (DPD)**.
- Введите значение интервала проверки **DPD Interval (сек)**.
- Введите значение повторных попыток проверки **DPD retry**.

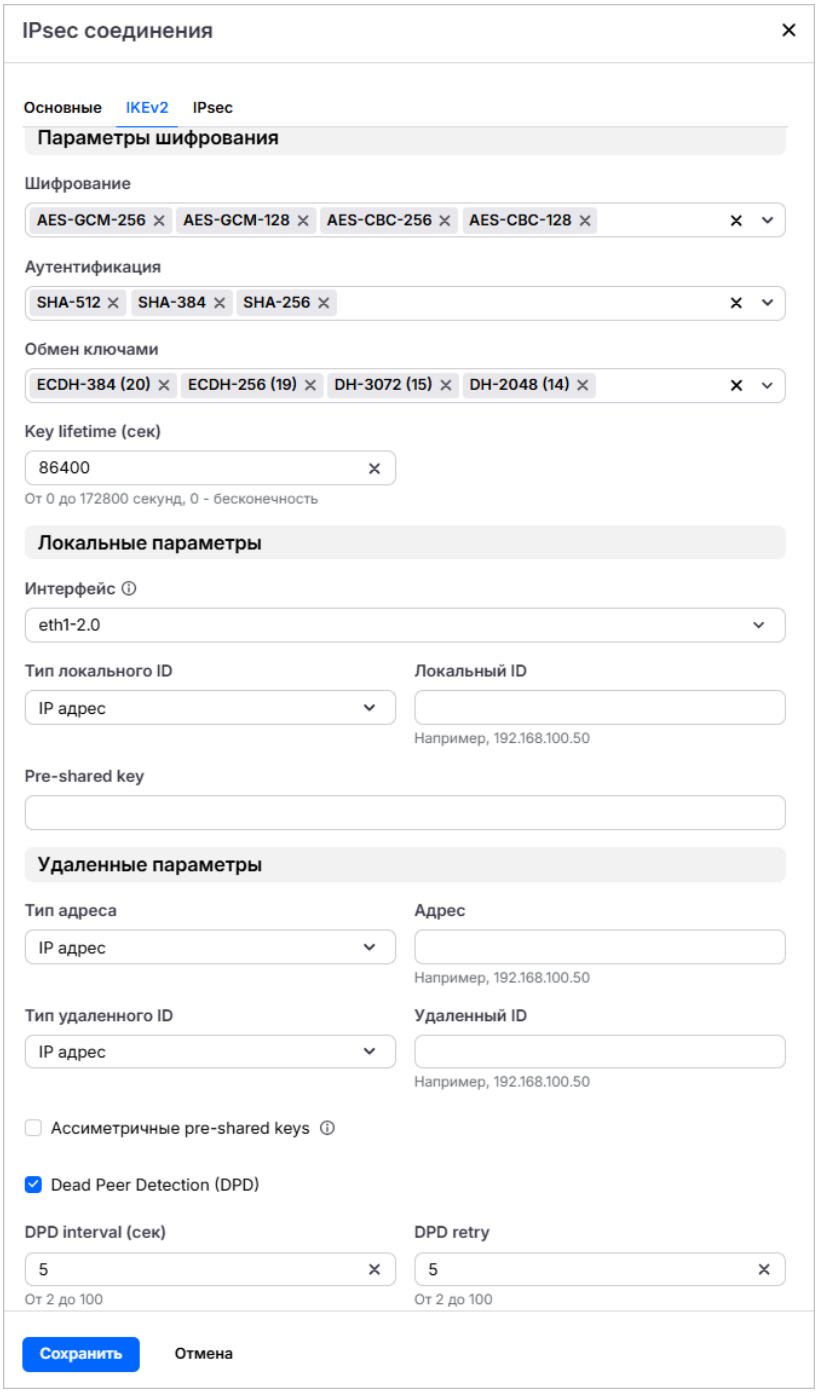


Рисунок 297. Вкладка **IKEv2**

8. На вкладке **IPsec** настройте параметры протокола:
   - Выберите необходимые алгоритмы шифрования, аутентификации и обмена ключами.
   - Введите значение времени жизни сессионных ключей в секундах.
   - Введите в килобайтах значение максимального размера данных, шифруемых одним ключом.

Примечание. При достижении любого из двух пределов происходит повторное установление ключей без разрыва сессии.

- Если требуется, установите флажок **Perfect Forward secrecy**.

  Примечание. Эта функция обеспечивает уникальность сессионных ключей: для каждого сеанса связи создается новый, временный ключ, который уничтожается после завершения сессии.

- Добавьте локальные селекторы трафика.
- Добавьте удаленные селекторы трафика.
- Нажмите **Сохранить**.

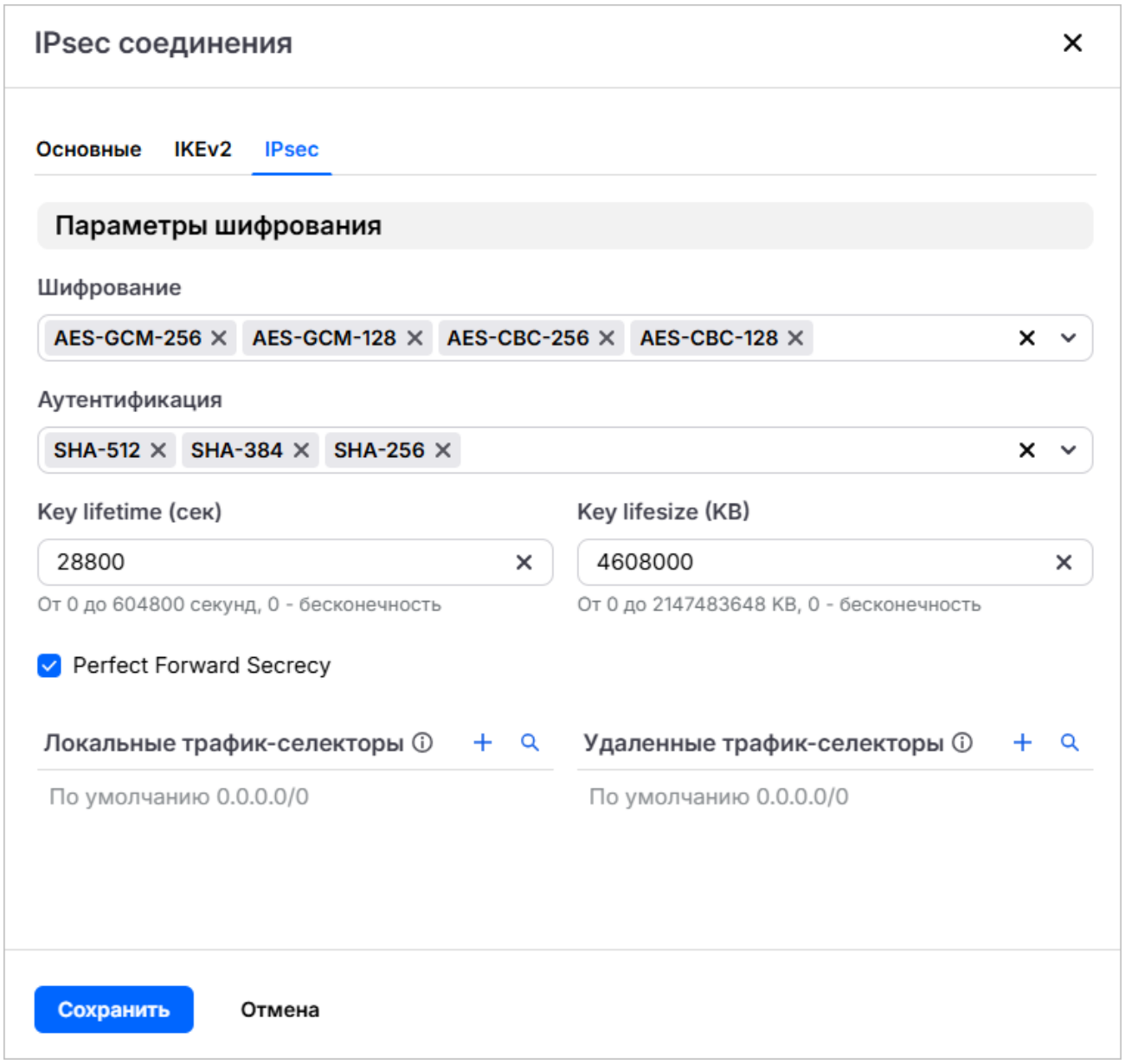


Рисунок 298. Вкладка **IPsec**

34. Remote Access VPN

Remote Access VPN (RA VPN) — это функциональность PT NGFW для организации защищенного доступа рабочих станций пользователей из внешних сетей к корпоративной сети с помощью технологий туннелирования и шифрования на базе фреймворка IPsec с использованием протокола IKEv2. Настройка RA VPN-шлюза (см. раздел 34.1) выполняется в системе управления PT NGFW через создание RA VPN-туннеля, работающего на виртуальном туннельном интерфейсе. В результате создания такого туннеля система управления генерирует JSON-файл конфигурации соединения. Этот файл передается пользователю любым удобным способом, импортируется в приложении PT VPN Agent (см. раздел 34.2), после чего агент может инициировать подключение к VPN-шлюзу. Защищенное соединение устанавливается только после успешной аутентификации пользователя.

В этом разделе

Настройка RA VPN-шлюза (см. раздел 34.1)

PT VPN Agent (см. раздел 34.2)

34.1. Настройка RA VPN-шлюза

В этом разделе приведены инструкции по подготовке и настройке RA VPN-шлюза, включая генерацию сертификатов и добавление VPN-туннеля.

Для корректной работы RA VPN администратору сети необходимо:

- Сгенерировать (см. раздел 34.1.1) сертификат шлюза и закрытый ключ. Сертификат используется в PT VPN Agent для идентификации шлюза (защита от поддельных серверов) и шифрования туннеля. Содержимое сертификата (поля CN и SAN) должно соответствовать адресу шлюза (FQDN или IP), указанному в профиле.
- Настроить в агенте Identity Control интеграцию с RADIUS-сервером (см. раздел 28.4.3). RADIUS-сервер выступает единой точкой аутентификации клиентов, через которую шлюз проверяет учетные данные пользователей.
- Настроить интеграцию с Active Directory (см. раздел 28). Это необходимо для получения системой управления информации о списках пользователей и их принадлежности к группам, что позволит применять политики безопасности по конкретному пользователю или группе AD.

В этом разделе

Генерация сертификатов шлюза (см. раздел 34.1.1)

Создание туннеля RA VPN (см. раздел 34.1.2)

34.1.1. Генерация сертификатов шлюза

PT VPN Agent проверяет сертификат PT NGFW при установке соединения. Подключение возможно только при успешной проверке цепочки доверия.

На стороне клиента должна быть собрана полная цепочка доверия от сертификата PT NGFW до доверенного корневого центра сертификации.

Не имеет значения, как именно формируется цепочка: корневой и промежуточные сертификаты могут быть заранее установлены в системе или переданы шлюзом PT NGFW в процессе IKE-обмена.

Ниже перечислены инструкции по генерации цепочки сертификатов. Примеры основаны на OpenSSL. Инструкции по генерации корневого и промежуточного сертификатов приведены для иллюстрации структуры цепочки: в реальных инфраструктурах они, как правило, уже существуют. При необходимости могут быть сгенерированы промежуточные и даже корневой сертификаты, однако это не является обязательным требованием для корректной работы.

Основное внимание следует уделить параметрам сертификата шлюза (end-entity certificate), так как именно он используется PT NGFW при установке соединения.

Генерация корневого сертификата

Примечание. Генерацию сертификата можно пропустить, если он уже был создан ранее.

- Чтобы сгенерировать корневой сертификат:

  1. Сгенерируйте закрытый ключ:

     ```
     openssl genrsa -out root.key 4096
     ```

  2. Сгенерируйте самоподписанный сертификат:

     ```
     openssl req -x509 -new -nodes -key root.key -sha256 -days 3650 -out root.crt -subj "/
     CN=Example Root CA"
     ```

После выполнения команд будут созданы следующие файлы:

— `root.key` — закрытый ключ корневого сертификата.

— `root.crt` — корневой сертификат.

Генерация промежуточного сертификата

Примечание. Генерацию сертификата можно пропустить, если он уже был создан ранее.

► Чтобы сгенерировать промежуточный сертификат:

1. Сгенерируйте закрытый ключ:
   ```
   openssl genrsa -out int.key 4096
   ```
2. Создайте CSR для промежуточного сертификата:
   ```
   openssl req -new -key int.key -out int.csr -subj "/CN=Example Intermediate CA"
   ```
3. Подпишите промежуточный сертификат корневым CA:
   ```
   openssl x509 -req -in int.csr -CA root.crt -CAkey root.key -CAcreateserial -out int.crt
   -days 1825 -sha256 \
   -extfile <(cat <<EOF
   basicConstraints=critical,CA:TRUE,pathlen:0
   keyUsage=critical,keyCertSign,cRLSign
   subjectKeyIdentifier=hash
   authorityKeyIdentifier=keyid,issuer
   EOF
   )
   ```

После выполнения команд будут созданы следующие файлы:

— `int.key` — закрытый ключ промежуточного сертификата.

— `int.crt` — промежуточный сертификат.

Генерация сертификата шлюза RA VPN

Сертификат шлюза должен отвечать следующим требованиям:

— `basicConstraints=CA:FALSE` — сертификат должен быть конечным, а не сертификатом центра сертификации; значение `CA:FALSE` указывает, что сертификат нельзя использовать для выпуска других сертификатов.

— `keyUsage`:

- `digitalSignature` — требуется для подтверждения подлинности сервера в криптографическом обмене. Обязательный параметр.
- `keyEncipherment` — обычно требуется для совместимости с клиентами.

— `extendedKeyUsage`:

- `serverAuth` — указывает, что сертификат может использоваться для аутентификации сервера. Обязательный параметр.
- `1.3.6.1.5.5.7.3.17` — указывает, что сертификат предназначен для применения в IKE- и IPsec-сценариях. Обязательный параметр.

— `subjectAltName` — должен содержать название DNS и (или) IP-адрес, используемые клиентом при подключении. В примере команды это доменное имя `gateway.example.com` и IP-адрес `10.0.0.1`.

— `CN` — не является основным источником имени сервера при проверке сертификата, но его рекомендуется согласовать со значением в `subjectAltName`.

- Чтобы сгенерировать сертификат шлюза:

  1. Сгенерируйте закрытый ключ:
     ```
     openssl genrsa -out gw.key 2048
     ```
  2. Создайте CSR для промежуточного сертификата:
     ```
     openssl req -new -key gw.key -out gw.csr -subj "/CN=gateway.example.com"
     ```
  3. Подпишите его промежуточным центром сертификации (или корневым, если нет промежуточного):
     ```
     openssl x509 -req -in gw.csr -CA int.crt -CAkey int.key -CAcreateserial -out gw.crt -days
     825 -sha256 \
     -extfile <(cat <<EOF
     basicConstraints=critical,CA:FALSE
     keyUsage=critical,digitalSignature,keyEncipherment
     extendedKeyUsage=serverAuth,1.3.6.1.5.5.7.3.17
     subjectAltName=DNS:gateway.example.com,IP:10.0.0.1
     subjectKeyIdentifier=hash
     authorityKeyIdentifier=keyid,issuer
     EOF
     )
     ```

После выполнения команд будут созданы следующие файлы:

— `gw.key` — закрытый ключ RA VPN шлюза PT NGFW.

— `gw.crt` — сертификат RA VPN шлюза PT NGFW.

Эти файлы теперь можно использовать в конфигурации RA VPN PT NGFW.

Формирование PEM-файла цепочки сертификатов

Для удобства на стороне шлюза RA VPN PT NGFW рекомендуется передавать клиенту не только свой сертификат, но и промежуточные — это упрощает построение цепочки доверия на клиенте.

- Чтобы сформировать PEM-файл цепочки сертификатов,

  введите команду:
  ```
  cat gw.crt int.crt > chain.pem
  ```

  Примечание. В файле важен порядок: от конечного сертификата до корневого. При этом корневой сертификат в цепочку обычно не включается.

  Примечание. На стороне клиента должен быть установлен только корневой сертификат.

После выполнения команды будет создан файл `chain.pem` с цепочкой сертификатов, который шлюз RA VPN на PT NGFW будет передавать клиенту.

34.1.2. Создание туннеля RA VPN

- Чтобы создать туннель удаленного доступа:

  1. На странице **Устройства** → **Виртуальные контексты** выберите виртуальный контекст, внутри которого хотите создать туннель RA VPN.
  2. Выберите вкладку **Удаленный доступ**.
  3. Нажмите **Добавить**.
  4. На вкладке **Основные** настройте следующие параметры:
     - Введите название профиля.
     - Если требуется, введите описание.

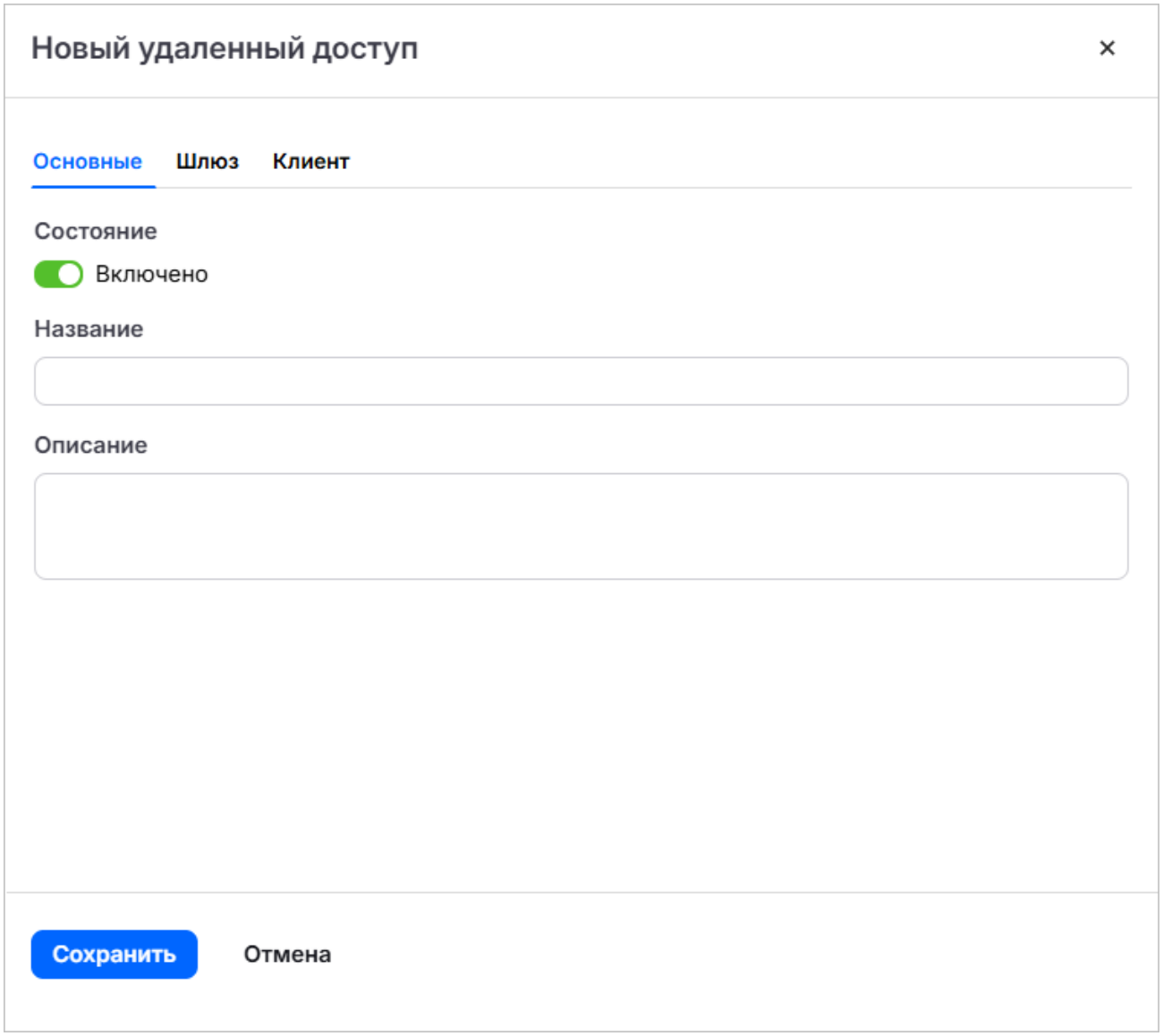


Рисунок 299. Вкладка **Основные**

5. На вкладке **Шлюз** настройте следующие параметры:
   - Выберите интерфейс для удаленного доступа по VPN-соединению.
   - Добавьте сертификат шлюза, выбрав его в списке сертификатов.

     Примечание. Для каждого профиля RA VPN администратору сети необходимо заранее сгенерировать пару «сертификат и закрытый ключ». Вы можете добавлять сертификаты в этот список путем загрузки сгенерированных файлов сертификатов и их закрытых ключей.
   - Выберите виртуальный роутер.
   - Введите внутренний IP-адрес шлюза.

Указанный IP-адрес должен входить в диапазон, заданный на вкладке **Клиент** в блоке **Конфигурация IP**.

- Выберите зону безопасности.
- Укажите размер MTU для VPN-интерфейса в байтах (рекомендованное значение — 1400).
- Если требуется, установите флажок **Корректировка TCP MSS**.

  При установленном флажке размер MSS будет определяться по формуле MSS = MTU – 40.
- Введите значение максимального времени подключения в днях от 1 до 30.

  Примечание. По истечении этого времени соединение разрывается, и пользователю необходимо установить его заново.
- Введите значение периода неактивности в минутах от 5 до 43200.

  Примечание. Если в течение указанного времени через соединение не проходит ни одного пакета, VPN-сессия считается неактивной и автоматически разрывается.

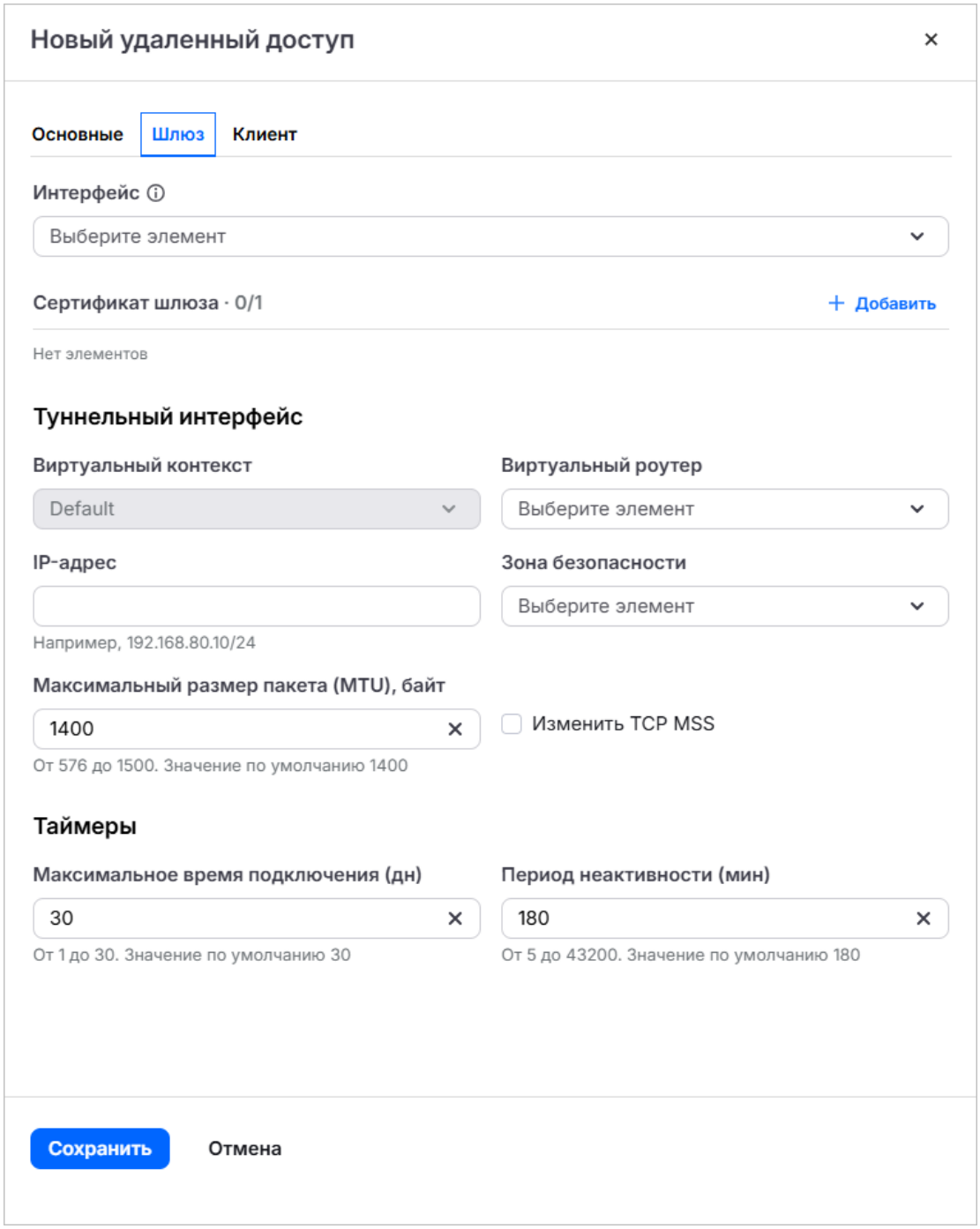


Рисунок 300. Вкладка **Шлюз**

6. На вкладке **Клиент** настройте следующие параметры:
   - Выберите способ подключения к шлюзу: **IP-адрес** или **FQDN**.
   - Введите внешний адрес шлюза.

     Примечание. Адрес должен совпадать с адресом, указанным в сертификате шлюза, который вы добавляли на предыдущем шаге.

- Добавьте доверенный корневой сертификат, выбрав его в списке сертификатов.
- Выберите формат, в котором необходимо задать адреса в IP-пуле: **Подсеть** или **Диапазон**.
- Введите адрес подсети или диапазон IP-адресов.

  Это значение необходимо задать, чтобы система могла выделять из него IP-адреса подключающимся клиентам.

  Внимание! Диапазоны IP-адресов для разных VPN-туннелей не должны пересекаться — это может привести к конфликтам маршрутизации и некорректному назначению адресов пользователям.
- Введите значение таймера удержания аренды в секундах от 1 до 86400.

  Примечание. Это значение определяет, на какое время IP-адрес, выданный клиенту из пула, будет резервироваться за ним после отключения VPN-сессии. По истечении указанного времени арендованный адрес возвращается в пул и может быть использован для новых подключений.
- Если требуется, включите параметр **Раздельное туннелирование**.

  Примечание. Параметр позволяет настроить, какой трафик будет проходить через VPN-туннель, а какой — использовать маршрут по умолчанию.
- Если параметр **Раздельное туннелирование** включен, добавьте необходимые адреса в списки включений (трафик, проходящий через VPN-туннель) и исключений (трафик, проходящий по маршруту по умолчанию).
- В поле **DNS-суффикс** укажите доменное имя вашей сети.

  Примечание. Это значение будет автоматически добавляться к коротким именам ресурсов в пользовательских сетевых запросах.
- В поле **DNS-список** укажите IP-адрес (IP-адреса) внутренних DNS-серверов.

  Примечание. На эти серверы будут направляться все DNS-запросы, относящиеся к домену, указанному в поле **DNS-суффикс.**
- Нажмите **Создать**.

  После успешного создания туннеля RA VPN в списке туннелей в столбце **Agent configuration file** появится ссылка для скачивания файла конфигурации PT VPN Agent. См. подробнее в разделе Добавление нового соединения.

  Внимание! Изменение любых параметров, влияющих на работу IPsec и IKEv2 (алгоритмы шифрования, пулы адресов, сертификаты), в рамках настроенного VPN-туннеля приведет к принудительному разрыву всех активных сессий VPN-агентов. Пользователям PT VPN Agent потребуется установить соединение заново, используя обновленную конфигурацию.

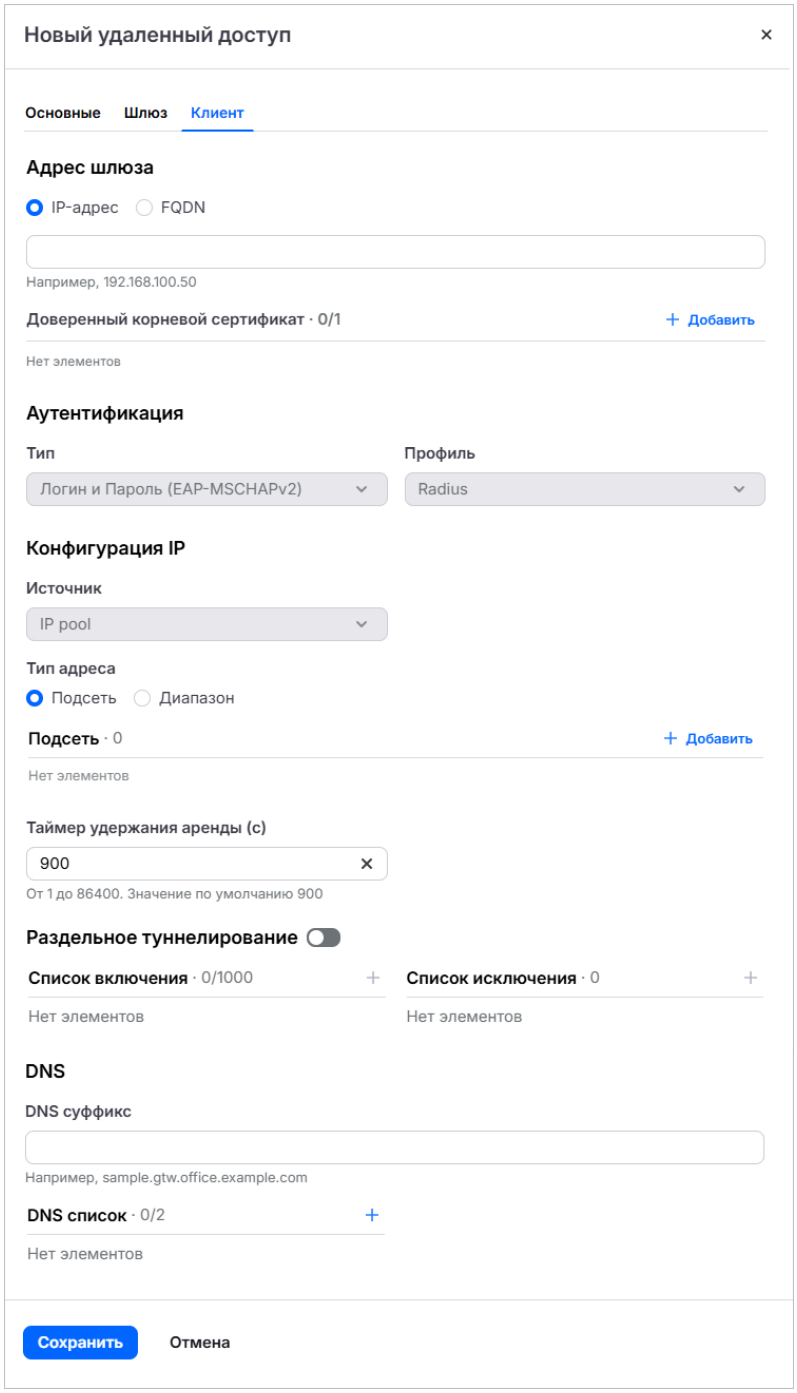


Рисунок 301. Вкладка **Клиент**

34.2. PT VPN Agent

PT VPN Agent — приложение, с помощью которого можно настраивать VPN-соединение и подключаться по нему к корпоративной сети. Агент шифрует трафик и устанавливает защищенный туннель до VPN-сервера. Подключение к серверу настраивается путем импортирования файла конфигурации в формате JSON.

В этом разделе

Аппаратные и программные требования (см. раздел 34.2.1)

Установка PT VPN Agent (см. раздел 34.2.2)

Обновление PT VPN Agent (см. раздел 34.2.3)

Удаление PT VPN Agent (см. раздел 34.2.4)

Интерфейс PT VPN Agent (см. раздел 34.2.5)

Настройка PT VPN Agent (см. раздел 34.2.6)

Просмотр журналов (см. раздел 34.2.7)

34.2.1. Аппаратные и программные требования

Минимальные аппаратные и программные требования для установки и работы PT VPN Agent:

- любой x86_64-совместимый процессор с тактовой частотой 1 ГГц и выше;
- 2 ГБ оперативной памяти;
- 200 МБ на жестком на диске;
- графический процессор с поддержкой OpenGL ES 2.0;
- сетевой адаптер 100 Мбит/с;
- операционные системы Windows 10, Windows 11 и их серверные аналоги, Astra Linux 1.8.2 Desktop SE, Ubuntu Desktop 24.04.3 LTS, Debian 12.10 (gnome).

34.2.2. Установка PT VPN Agent

Установка в Windows

► Чтобы установить PT VPN Agent в ОС Windows:

1. Получите файл установщика PT VPN Agent от администратора сети и запустите его.
2. Ознакомьтесь с условиями лицензионного соглашения.
3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите **Next**, чтобы принять его.
4. Выберите путь установки.
5. Нажмите **Install**.

   После успешной установки появится соответствующее сообщение.
6. Нажмите **Finish**.

   После установки в меню **Пуск** и на рабочем столе появится ярлык PT VPN Agent.

Установка в Linux

- Чтобы установить PT VPN Agent в ОС Linux:

  1. Получите архив с установщиком PT VPN Agent от администратора сети и распакуйте его.
  2. В терминале перейдите в каталог с установщиком и введите команду `sudo ./install.sh`.
  3. Выберите язык.
  4. Выберите **Установка PT VPN Agent**.

     После успешной установки в терминале появится соответствующее сообщение, а в меню приложений появится ярлык PT VPN Agent.

34.2.3. Обновление PT VPN Agent

Обновление в Windows

- Чтобы обновить PT VPN Agent в ОС Windows:

  1. Получите файл установщика новой версии PT VPN Agent от администратора сети и запустите его.
  2. Нажмите **Next**.
  3. Нажмите **Update**.
  4. Ознакомьтесь с условиями лицензионного соглашения и примите его.
  5. Нажмите **Next**.
  6. Нажмите **Install**.

     При успешном обновлении появится соответствующее сообщение.
  7. Нажмите **Finish**.

Обновление в Linux

- Чтобы обновить PT VPN Agent в ОС Linux:

  1. В терминале перейдите в каталог с установщиком и введите команду `sudo ./install.sh`.
  2. Выберите язык.
  3. Выберите **Установка PT VPN Agent**.

4. Выберите **Обновить**.
5. При успешном обновлении в терминале появится соответствующее сообщение.

34.2.4. Удаление PT VPN Agent

Вы можете удалить PT VPN Agent с помощью стандартных средств ОС либо воспользоваться одним из способов ниже.

Удаление в Windows

- Чтобы удалить PT VPN Agent в ОС Windows:

  1. Запустите установщик агента и нажмите **Remove**.

     При успешном удалении появится соответствующее сообщение.
  2. Нажмите **Finish**.

Удаление в Linux

- Чтобы удалить PT VPN Agent в ОС Linux:

  1. В терминале перейдите в каталог с установщиком и введите команду `sudo ./install.sh`.
  2. Выберите язык.
  3. Выберите **Установка PT VPN Agent**.
  4. Выберите **Удалить**.

     При успешном удалении в терминале появится соответствующее сообщение.

34.2.5. Интерфейс PT VPN Agent

В PT VPN Agent все действия выполняются с помощью графического пользовательского интерфейса. При запуске агента его значок появляется в области уведомлений. Он отображается серым при выключенном VPN-соединении и красным — при включенном.

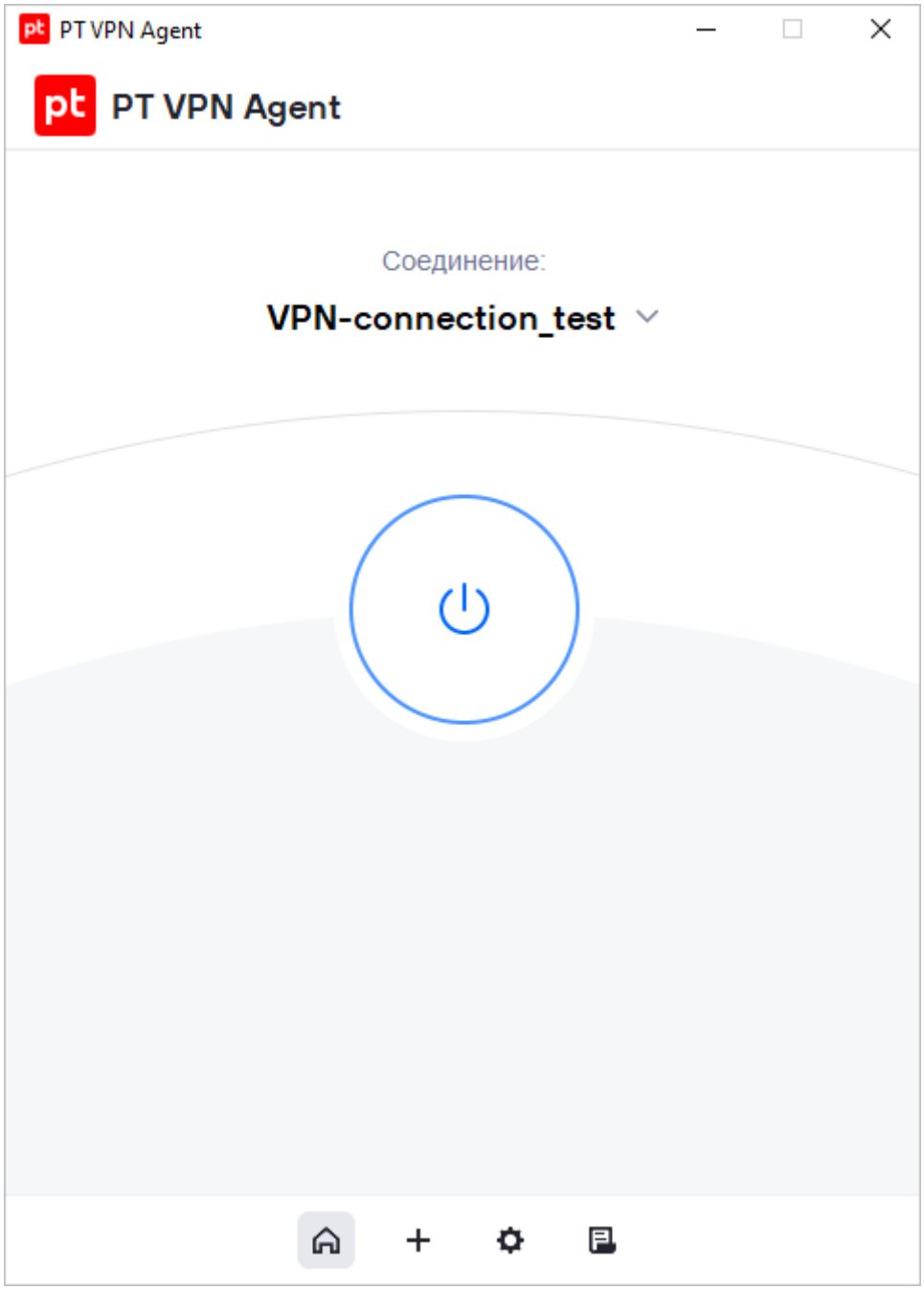


Рисунок 302. Интерфейс PT VPN Agent

В нижней части интерфейса расположено меню, состоящее из следующих кнопок:

— для выбора и переключения между соединениями, их включения и выключения и просмотра их состояния;

— для добавления конфигураций новых соединений;

— при нажатии кнопки вы можете:

- просмотреть список текущих конфигураций, удалить их или добавить новые, а также изменить их некоторые параметры, такие как название соединения, логин и пароль;
- просмотреть контактную информацию службы технической поддержки и информацию о версии приложения;
- настроить такие параметры, как включение соединения при запуске приложения и запуск приложения при входе в ОС;
- сменить тему и язык интерфейса PT VPN Agent.

— для просмотра записей журналов текущих соединений.

34.2.6. Настройка PT VPN Agent

В этом разделе описаны основные операции по настройке VPN-подключений.

Добавление нового соединения

- Чтобы добавить новое соединение:

1. Запустите PT VPN Agent.
2. Нажмите +.
3. Добавьте конфигурационный файл, полученный от администратора сети, одним из способов:
   - Перетащите файл в область загрузки VPN-агента.
   - Нажмите **на диске...** и укажите путь к файлу.
4. Нажмите **Сохранить**.

Изменение параметров соединения

- Чтобы изменить параметры соединения:

1. Нажмите .
2. Нажмите > напротив соединения, параметры которого хотите изменить.
3. Если требуется:
   - Измените имя соединения.
   - Измените имя пользователя.
   - Измените пароль.

- Включите или выключите **Автоматическое переподключение**, если хотите, чтобы VPN-соединение автоматически восстанавливалось при разрыве.

4. Нажмите **Сохранить**.

Удаление соединения

- Чтобы удалить соединение:

1. Нажмите .
2. Нажмите напротив соединения, которое хотите удалить, и подтвердите удаление.

Включение соединения

- Чтобы включить соединение:

1. Нажмите .
2. Выберите нужное соединение.
3. Нажмите .

   При успешном подключении кнопка подключения изменит цвет на зеленый.
4. Введите логин и пароль, полученные от администратора сети.
5. Чтобы не вводить пароль при каждом подключении, установите флажок **Запомнить**.

Примечание. Единовременно может быть подключено только одно VPN-соединение. При подключении нового соединения текущее автоматически отключится.

Выключение соединения

- Чтобы выключить VPN-соединение:

1. Нажмите .
2. Выберите нужное соединение.
3. Нажмите .

   При успешном отключении кнопка подключения станет прозрачной.

Смена языка

- Чтобы сменить язык интерфейса PT VPN Agent:

  1. Нажмите ⚙.
  2. Выберите **Общие**.
  3. Выберите нужный язык.

     Внимание! При смене языка требуется перезапуск приложения. Текущее VPN-соединение будет разорвано.

Смена темы интерфейса

Интерфейс PT VPN Agent доступен в светлой и темной темах, а также вы можете выбрать тему, как в вашей системе.

- Чтобы сменить тему интерфейса PT VPN Agent:

  1. Нажмите ⚙.
  2. Выберите **Общие**.
  3. Выберите нужную тему.

     Внимание! При смене языка требуется перезапуск приложения. Текущее VPN-соединение будет разорвано.

34.2.7. Просмотр журналов

Записи журнала агента фиксируются в самом приложении, а также в файле log.txt.

- Чтобы просмотреть журнал,

  нажмите 📄.

Вы можете:

— Включить параметры **Автопрокрутка** и **Перенос строк**.

— Открыть папку с файлом `log.txt`, нажав 🗀 и просмотреть его содержимое.

— Очистить записи журнала в приложении, нажав 🧹. Записи в файле `log.txt` при этом не удалятся.

35. DHCP relay

В PT NGFW предусмотрена функция DHCP relay, которая применяется в случаях, когда DHCP-сервер и DHCP-клиенты находятся в разных широковещательных доменах. Такая ситуация возникает, например, в сегментированной сети, в которой широковещательные пакеты от клиента не достигают DHCP-серверов напрямую. В этом случае PT NGFW выступает в роли агента DHCP relay, пересылая DHCP-запросы от клиента к серверу и обратно, тем самым обеспечивая корректное получение параметров конфигурации, IP-адресов и других сетевых параметров.

В этом разделе

Обработка DHCP-сообщений при использовании DHCP relay в PT NGFW (см. раздел 35.1)

Настройка DHCP relay (см. раздел 35.2)

35.1. Обработка DHCP-сообщений при использовании DHCP relay в PT NGFW

В процессе работы протокола DHCP клиент и сервер обмениваются сообщениями следующих типов:

- **DHCPDISCOVER** — клиент ищет доступные DHCP-серверы;
- **DHCPOFFER** — сервер предлагает клиенту сетевые параметры, такие как IP-адрес, маску подсети, DNS и другие;
- **DHCPREQUEST / DHCPRENEW** — клиент запрашивает или продлевает аренду IP-адреса;
- **DHCPACK** — сервер подтверждает выдачу IP-адреса клиенту.

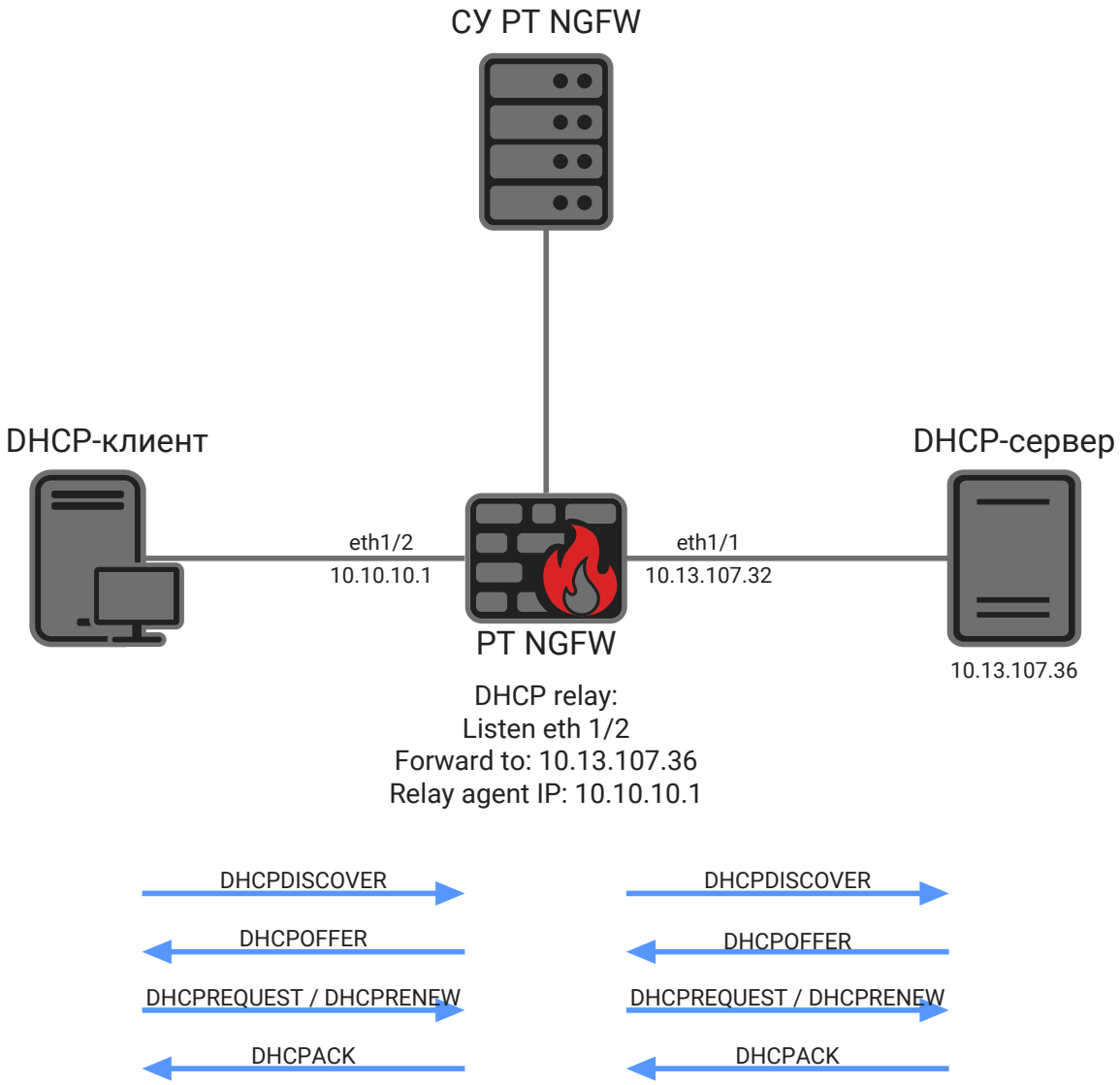


Рисунок 303. Схема DHCP relay

Когда DHCP-клиент отправляет широковещательное (broadcast) сообщение DHCPDISCOVER с целью обнаружения доступных DHCP-серверов, межсетевой экран принимает это сообщение на L3-интерфейсе, на котором настроен агент DHCP relay, и пересылает его однонаправленно (unicast) на указанные DHCP-серверы. При этом межсетевой экран дополнительно устанавливает атрибут Relay Agent IP (IP-адрес L3-интерфейса, на который межсетевой экран получил запрос от клиента). В примере выше Relay Agent IP — 10.10.10.1.

На основании значения Relay Agent IP DHCP-сервер может:

— определить, из какого сетевого сегмента поступил запрос;

— выдать клиенту IP-адрес из соответствующего пула адресов.

Если администратор настроит несколько DHCP-серверов, то DHCP relay перешлет запрос от DHCP-клиента всем настроенным DHCP-серверам.

В зависимости от параметров DHCP-клиента может быть выбран определенный DHCP-сервер, с которым DHCP-клиент взаимодействует дальше:

— DHCP-клиент продолжает работать с DHCP-сервером, который первым прислал сообщение DHCPOFFER;

— DHCP-клиент выбирает DHCP-сервер, с которым взаимодействовал раньше;

— DHCP-клиент может предпочесть адрес в определенном сегменте сети или с определенными опциями (такими как MTU, маршруты) на основании своей конфигурации.

35.2. Настройка DHCP relay

- Чтобы настроить DHCP relay:

1. На странице **Устройства** → **Виртуальные контексты** выберите виртуальный контекст, на котором хотите создать DHCP relay.

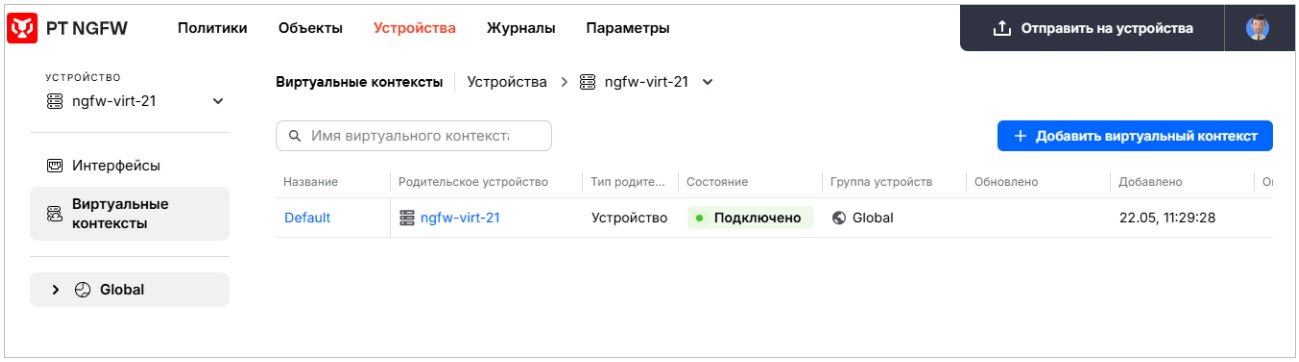


Рисунок 304. Страница **Устройства**

2. В левой части страницы выберите вкладку **DHCP**.
3. На вкладке **DHCP relay** нажмите **Добавить DHCP relay**.

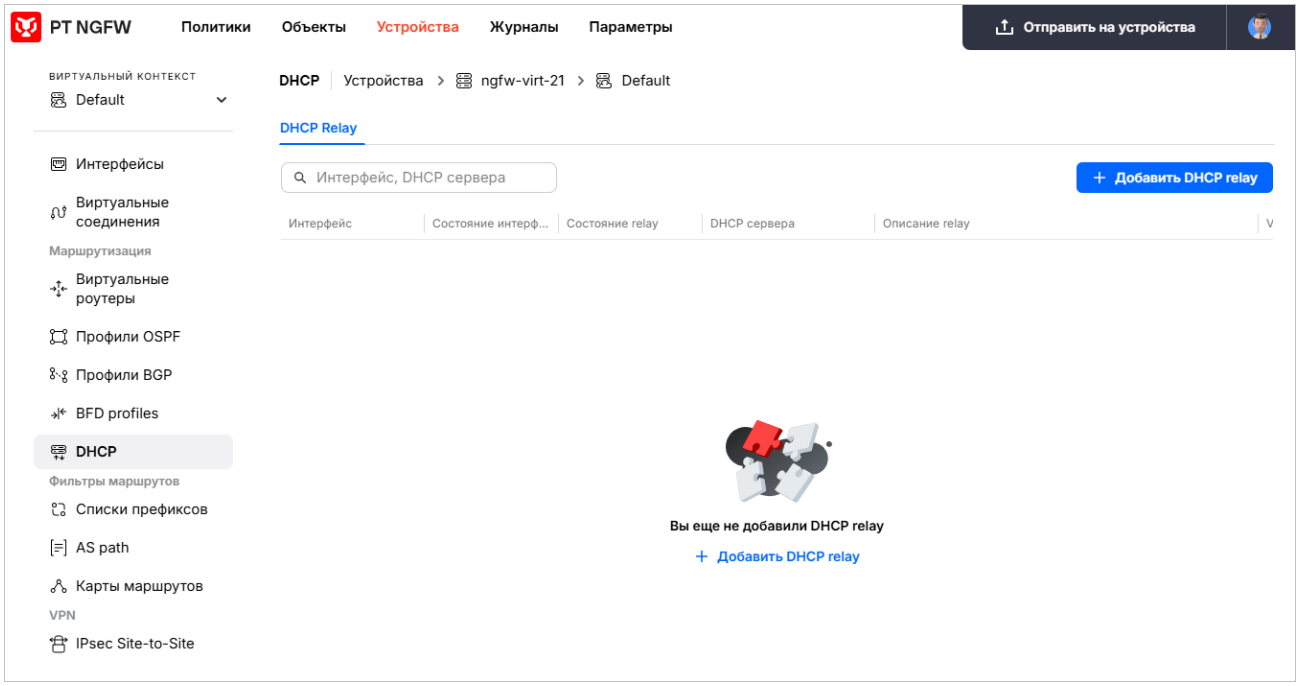


Рисунок 305. Добавление DHCP relay

4. Введите описание relay.
5. Выберите сабинтерфейс, привязанный к виртуальному роутеру и работающий в режиме маршрутизатора, который будет принимать широковещательные DHCP-запросы от клиентов.
6. Добавьте IP-адреса DHCP-серверов, на которые будут пересылаться DHCP-запросы.

   Примечание. Вы можете добавить до восьми DCHP-серверов.
7. Нажмите **Сохранить**.

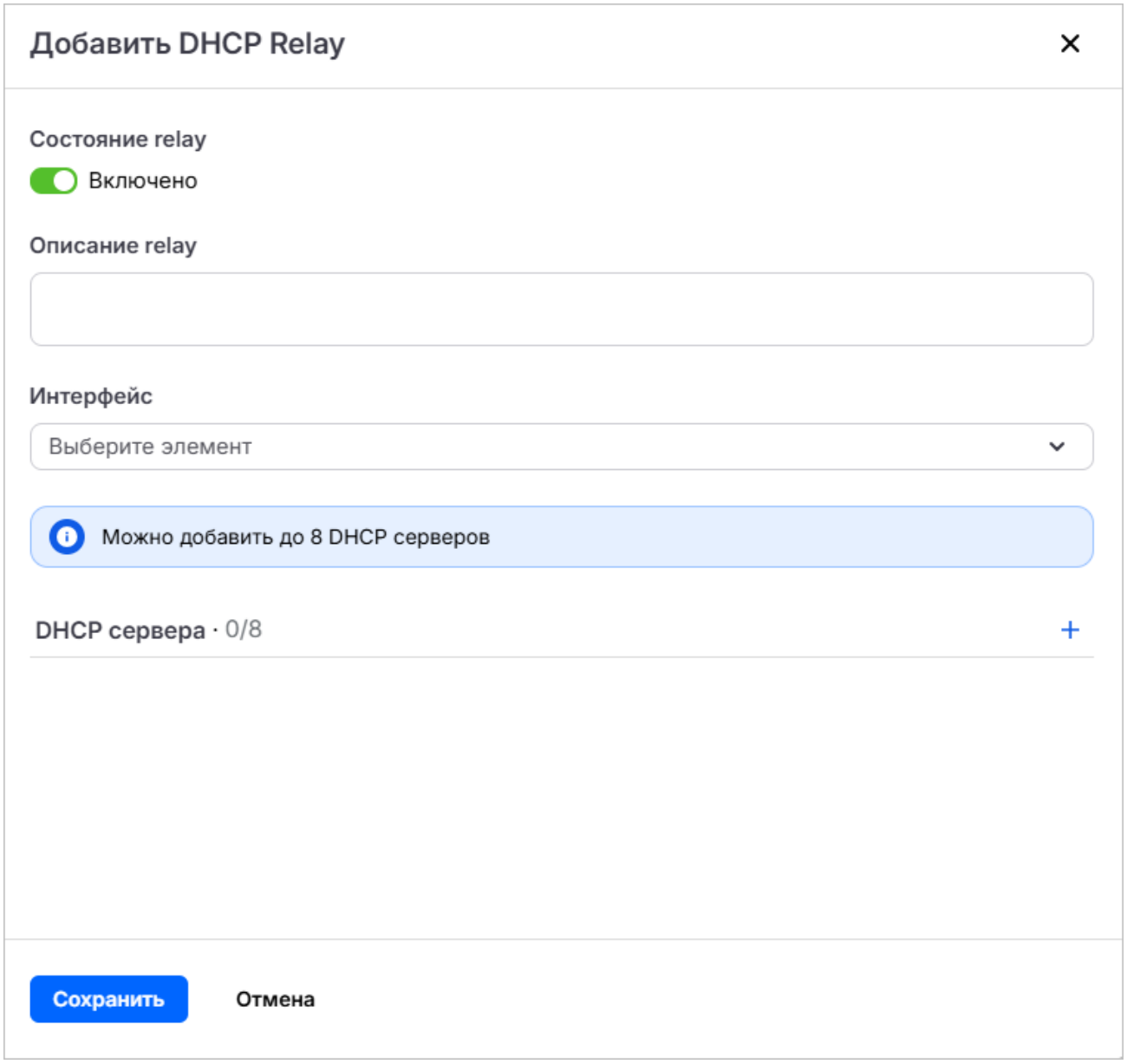


Рисунок 306. Добавление DHCP relay

Примечание. На одном межсетевом экране может быть настроено несколько объектов DHCP relay на разных интерфейсах. Максимальное количество объектов DHCP relay равняется количеству L3-интерфейсов межсетевого экрана. Для каждого объекта DHCP relay можно использовать только один интерфейс в режиме L3.

36. ICAP

ICAP (Internet Content Adaptation Protocol) (RFC 3507) — протокол, позволяющий передать HTTP-сообщения на ICAP-сервер для обработки. ICAP-сервер может выполнить модификацию HTTP-сообщения и вернуть модифицированную версию или ответить, что модификация не требуется (сообщение ICAP с кодом 204 "No content"). Передаваемые сообщения HTTP инкапсулируются в сообщения протокола ICAP.

При передаче HTTP-сообщений ICAP работает в двух режимах:

— Request Modification (ReqMod, «модификация запроса») — PT NGFW пересылает ICAP-серверу HTTP-запросы.

— Response Modification (RespMod, «модификация ответа») — PT NGFW пересылает ICAP-серверу HTTP-ответы.

В примере ниже внутри сообщения ICAP пересылается HTTP-запрос (режим Request Modification). Например, пересылается HTTP-запрос на скачивание файла, запрос на доступ к какому-то веб-ресурсу, POST-запрос или другой HTTP-запрос.

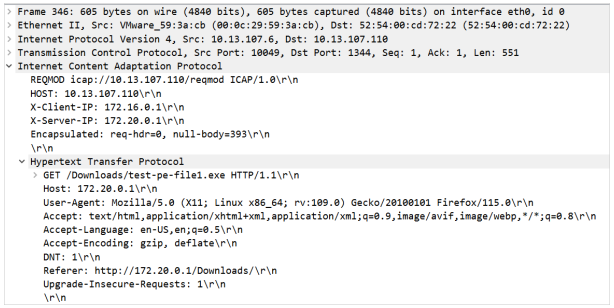


Рисунок 307. Передача HTTP-запроса

В примере ниже внутри сообщения ICAP пересылается HTTP-ответ (режим Response Modification). Например, пересылается HTTP-ответ веб-сервера, в котором сервер передает скачиваемый клиентом файл или веб-страницу со всем ее содержимым, или другой HTTP-ответ.

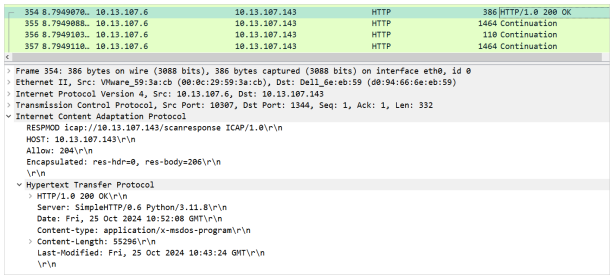


Рисунок 308. Передача HTTP-ответа

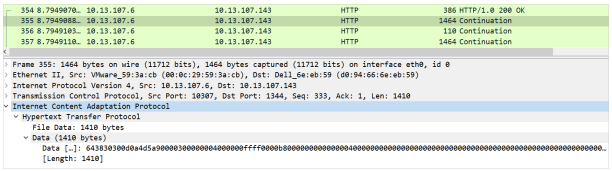


Рисунок 309. Передача HTTP-ответа

В этом разделе

Реализация отправки данных по ICAP в PT NGFW (см. раздел 36.1)

Настройка отправки данных по ICAP (см. раздел 36.2)

36.1. Реализация отправки данных по ICAP в PT NGFW

PT NGFW позволяет отправлять на внешний ICAP-сервер транзитный трафик HTTP-приложений, то есть HTTP-запросы и (или) ответы, и в зависимости от ответа ICAP-сервера блокировать или разрешать его дальнейшую передачу. Блокирование происходит при получении любого ответа ICAP-сервера, отличного от ответа с кодом 204 "No content", и сопровождается отправкой сообщения TCP RST клиенту и серверу. В роли ICAP-сервера может в том числе выступать система класса DLP (data leak prevention) или Sandbox (песочница).

PT NGFW отправляет на ICAP-сервер не весь транзитный трафик, а только тот, который соответствует правилу безопасности, имеющему действие **Разрешить** и в разделе **Профили безопасности** которого указан ICAP-профиль. Трафик только тех HTTP-приложений, которые соответствует этому правилу безопасности, будет отправляться на проверку в ICAP согласно параметрам, настроенным в ICAP-профиле.

В ICAP-профиле указывается, нужно ли отправлять на ICAP-сервер HTTP-запросы (режим Request Modification), и если да, то задается профиль ICAP-сервера, в адрес которого необходимо пересылать HTTP-запросы, а также другие параметры. Для режима Request Modification также возможно указать какие именно типы файлов требуется пересылать (это актуально, например, для POST-запросов).

В ICAP-профиле также указывается, нужно ли отправлять на ICAP-сервер HTTP-ответы (режим Response Modification), и если да, то задается профиль ICAP-сервера, в адрес которого необходимо пересылать HTTP-ответы, а также другие параметры. Для режима Response Modification также возможно указать, какие именно типы файлов требуется пересылать.

В профиле ICAP-сервера указываются параметры отправки сообщений в адрес конкретного ICAP-сервера, тайм-ауты для работы с конкретным сервером и другие параметры.

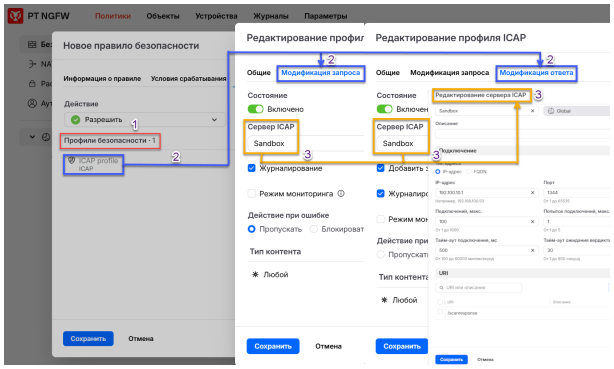


Рисунок 310. Отправка данных по ICAP в PT NGFW

Таким образом, PT NGFW позволяет:

— отправлять на один ICAP-сервер или на разные ICAP-серверы трафик HTTP-приложений, подпадающий только под определенное правило (правила) безопасности, обеспечивая таким образом высокую гранулярность и гибкость обработки трафика, а также оптимизировать загрузку ресурсов ICAP-сервера (серверов);

— отправлять трафик HTTP-приложений, подпадающий под различные правила безопасности, на различные ICAP-серверы, причем используя разные параметры для разных ICAP-серверов, например:

  • отправлять HTTP-запросы клиентов на DLP-сервер и одновременно с этим отправлять HTTP-ответы серверов в Sandbox (это достигается, если в профиле ICAP для ReqMod указать один ICAP-сервер, DLP, и в том же профиле ICAP для RespMod указать другой ICAP-сервер, Sandbox);

  • отправлять трафик HTTP-приложений, подпадающий под различные правила безопасности, на один и тот же ICAP-сервер, при этом используя разные URI (разные параметры ICAP-сервера), например трафик HTTP-приложения «А», подпадающий под правило «А» отправлять на ICAP-сервер для работы ICAP-сервера в режиме Bypass, а трафик HTTP-приложения «Б», подпадающий под правило «Б» — для работы того же ICAP-сервера, но в режиме «Блокировка».

— отправлять на ICAP-сервер (серверы) только определенные типы и (или) категории файлов;

— отправлять данные в режиме **Мониторинг** (**Monitoring mode**), в котором PT NGFW отправляет трафик на проверку ICAP-серверу и пересылает трафик получателю, не дожидаясь вердикта от ICAP-сервера;

— задавать действие (пропускать или блокировать передачу данных HTTP-приложений получателю) в случае недоступности и (или) ошибок при отправке данных ICAP-серверу.

Поддержка ICAP в PT NGFW имеет следующие особенности:

— PT NGFW получает вердикт от ICAP-сервера и блокирует или разрешает пересылку оригинального контента согласно вердикту от ICAP-сервера (за исключением режима **Мониторинг**, **Monitoring mode**).

— PT NGFW не выполняет пересылку адресату модифицированного контента, полученного от ICAP-сервера.

— На ICAP-сервер передаются не оригинальные HTTP-сообщения, а их копии.

— Сессии HTTP, данные которых отправляются на проверку ICAP-серверу (серверам), не синхронизируется между узлами кластера. Это обусловлено архитектурными особенностями работы самого протокола ICAP.

Работа PT NGFW в режиме Request Modification (модификация запроса)

Пример сценария:

1. Клиент пытается выгрузить PDF-файл в облачное хранилище, например в Яндекс Диск.
2. Сессия приложения Яндекс Диск соответствует разрешающему правилу безопасности в PT NGFW. ICAP-профиль является одним из профилей безопасности этого правила.
3. Если PT NGFW определяет приложение по первым пакетам запроса HTTP-транзакции, то он пересылает копию пакетов запроса этой транзакции на ICAP-сервер, указанный в ICAP-профиле, и согласно параметрам, настроенным в профиле.
4. Если пакетов запроса больше одного, то PT NGFW пересылает пакеты запроса веб-серверу назначения, придерживая последний пакет, ожидая вердикта от ICAP-сервера. Если запрос состоит из единственного пакета, то PT NGFW придерживает его в ожидании вердикта и не пересылает серверу.
5. Если ICAP-сервер отвечает вердиктом о необходимости блокировки данных (любое сообщение ICAP, за исключением 204 "No content"), то PT NGFW сбрасывает последний пакет, отправляет пакеты TCP Reset клиенту и серверу, извещая их о необходимости сброса TCP-сессии. Таким образом, на сервере происходит сброс получения файла, сервер удаляет данные полученного частично запроса.
6. Если ICAP-сервер отвечает сообщением ICAP 204 "No content" («Модификация не требуется»), то PT NGFW пропускает последний пакет. Веб-сервер успешно получает полный запрос от клиента.
7. Для следующей HTTP-транзакции в рамках той же сессии выполняются аналогичные действия.

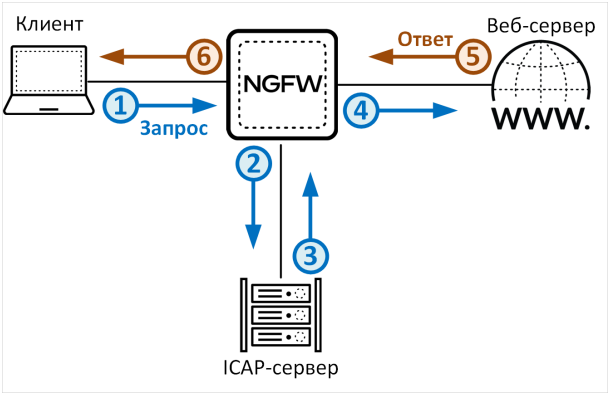


Рисунок 311. Работа в режиме Request Modification

В крайне редких случаях для идентификации HTTP-приложения требуется анализ HTTP-ответа, то есть идентификация приложения выполняется по либо совокупности запроса (запросов) и ответа (ответов), либо только по ответу. Если в правиле безопасности «А» в критериях срабатывания правила в поле **Приложение** указано именно такое приложение и в профиле безопасности указан ICAP-профиль «А», согласно которому требуется пересылка HTTP-запросов на ICAP-сервер, то такая пересылка невозможна, если на момент получения запроса PT NGFW еще не идентифицировал приложение. В таком случае может сработать правило «Б», в котором в критериях срабатывания правила в поле **Приложение** указано приложение, для идентификации которого было достаточно данных HTTP-запроса. Если в таком правиле в профиле безопасности указан ICAP-профиль «Б», согласно которому требуется пересылка HTTP-запросов на ICAP-сервер, то такая пересылка будет выполнена. После получения HTTP-ответа вердикт идентификации приложения будет уточнен и начнет применяться ICAP-профиль, указанный в правиле «А». Учитывая количество таких приложений (~0,1%), их характер и распространенность, вероятность возникновения такой ситуации в production-сети ничтожно мала.

Работа PT NGFW в режиме Response Modification (модификация ответа)

Пример сценария:

1. Клиент пытается скачать исполняемый файл с веб-сайта, например из Яндекс Диск.
2. Сессия приложения Яндекс Диск соответствует разрешающему правилу безопасности в PT NGFW. ICAP-профиль является одним из профилей безопасности этого правила.
3. PT NGFW пересылает копию пакетов ответа HTTP-транзакции на ICAP-сервер, указанный в ICAP-профиле и согласно параметрам, настроенным в профиле.
4. Если пакетов ответа больше одного, то PT NGFW пересылает пакеты ответа веб-серверу назначения, придерживая последний пакет, ожидая вердикта от ICAP-сервера. Если ответ состоит из единственного пакета, то PT NGFW придерживает его в ожидании вердикта и не пересылает клиенту.

5. Если ICAP-сервер отвечает вердиктом о необходимости блокировки данных (любое сообщение ICAP, за исключением 204 "No content"), то PT NGFW сбрасывает последний пакет, отправляет пакеты TCP Reset клиенту и серверу, извещая их о необходимости сброса TCP-сессии. Таким образом, на клиенте происходит сброс скачивания файла, клиент удаляет данные полученного частично файла.
6. Если ICAP-сервер отвечает сообщением ICAP 204 "No content" («Модификация не требуется»), то PT NGFW пропускает последний пакет. Клиент успешно завершает скачивания файла.
7. Для следующей HTTP-транзакции в рамках той же сессии выполняются аналогичные действия.

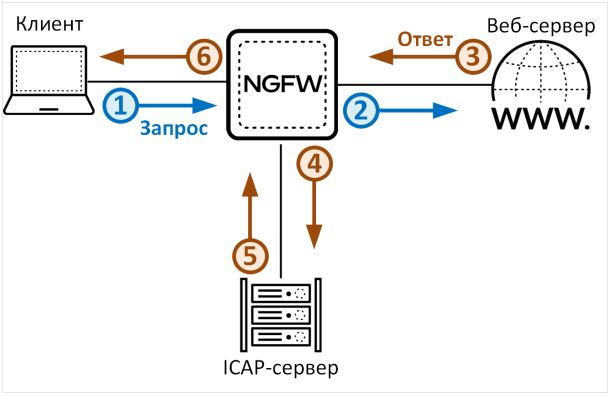


Рисунок 312. Работа в режиме Response Modification

36.2. Настройка отправки данных по ICAP

Поскольку PT NGFW отправляет ICAP-сообщения через интерфейс MGMT, перед выполнением настройки, убедитесь, что между интерфейсом MGMT и ICAP-сервером существует сетевая связность. Если узел PT NGFW и ICAP-сервер находятся в разных подсетях, то в базовой ОС узла PT NGFW может потребоваться создание статического маршрута.

- Чтобы добавить статический маршрут:

  1. Внесите изменения в файл сетевой конфигурации `10-mgmt1.network` базовой ОС, добавив секцию `[Route]` и оставив секции `[Match]` и `[Network]` без изменений.

```
ngfw@pt-ngfw-node:~$ sudo nano /etc/systemd/network/10-mgmt1.network
[Match]
Name=mgmt1
[Network]
Address=10.20.30.40/24
Gateway=10.20.30.1
DNS=10.1.2.3
DNS=10.1.2.4
[Route]
```

```
Destination=<Адрес ICAP-сервера, например 192.168.25.25/32>
Gateway=<Шлюз, через который доступен ICAP-сервер, например 10.20.30.254>
```

Примечание. Шлюз, указанный в секции [Network] является шлюзом по умолчанию. Соответственно, добавление специфичного маршрута к ICAP-серверу в секции [Route] может потребоваться, только если ICAP-сервер недоступен через шлюз по умолчанию.

2. Нажмите Ctrl+O для сохранения изменений, а затем — Ctrl+X для выхода из редактора nano.
3. Перезапустите сервис, чтобы изменения вступили в силу.
   ```
   ngfw@pt-ngfw-node:~$ sudo systemctl restart systemd-networkd
   ```

Первый шаг для настройки ICAP в PT NGFW — в разделе **Объекты** → **ICAP** → **Серверы** добавление одного или нескольких профилей ICAP-серверов, в адрес которых требуется отправлять HTTP-трафик, по одному профилю для каждого ICAP-сервера, который используется в вашей инфраструктуре и на который PT NGFW должен будет отправлять данные. При добавлении профиля ICAP-сервера настраиваются параметры подключения к серверу и указывается один или несколько возможных путей на этом ICAP-сервере.

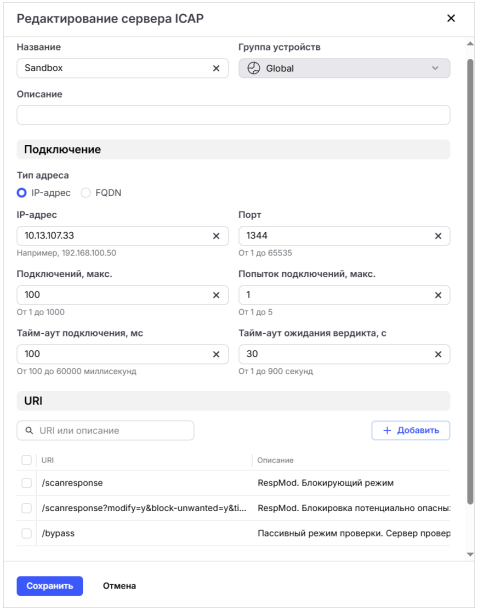


Рисунок 313. Изменение ICAP-сервера

Параметры профиля ICAP-сервера включают:

— **Название** (обязательно) — название ICAP-сервера.

— **Описание** (необязательно) — дополнительная информация о сервере или любые другие сведения на усмотрение администратора.

— **Тип адреса** (IP-адрес или FQDN) (обязательно) — адрес сервера в виде IP или FQDN, который PT NGFW будет использовать для отправки данных на этот ICAP-сервер.

- **Порт** (обязательно) — TCP-порт для подключения PT NGFW к ICAP-серверу. По умолчанию используется порт 1344. Необходимо изменить, если ваш ICAP-сервер использует другой порт для приема подключений.
- **Подключений** (необязательно) — максимальное число одновременно открываемых TCP-соединений к ICAP-серверу. Зависит от используемого ICAP-сервера, от его производительности. Различные ICAP-серверы поддерживают разное число подключений. В каждом соединении может передаваться контент для проверки ICAP-сервером. Диапазон от 1 до 1000. По умолчанию 100.
- **Попыток подключений** (необязательно) — максимальное количество попыток, которое PT NGFW предпринимает, чтобы отправить контент ICAP-серверу. Диапазон от 1 до 5. По умолчанию 1.
- **Тайм-аут подключения** в миллисекундах (необязательно) — тайм-аут на установление TCP-соединения с ICAP-сервером. Диапазон от 100 до 60000. По умолчанию 500 миллисекунд. PT NGFW предпринимает указанное количество попыток подключения и при каждой попытке ожидает тайм-аут подключения. Если PT NGFW исчерпал указанное количество попыток подключения, то ICAP-сервер считается недоступным и к данным HTTP-транзакции, подлежащей проверке, применяется действие, указанное в поле **Действие при ошибке** профиля ICAP.
- **Тайм-аут ожидания вердикта** в секундах (необязательно) — после того как контент (данные запроса или ответа или файл) успешно переданы на проверку ICAP-серверу, PT NGFW ожидает вердикт в течение указанного времени тайм-аута. Если по истечении тайм-аута ожидания вердикта ICAP-сервер не прислал ответ, то он считается недоступным и PT NGFW применяет к данным, отправленным на проверку, действие, указанное в поле **Действие при ошибке** профиля ICAP. Диапазон от 1 до 900 (15 минут). По умолчанию 30 секунд.
- **URI** (обязательно, минимум один) — путь (пути) на ICAP-сервере. Некоторые ICAP-серверы позволяют задавать параметры проверки в виде атрибутов пути. Например, при использовании пути `/scanresponse` ICAP-сервер выполнит полную антивирусную проверку файла, а если использовать путь `/scanresponse?block-unwanted=y&timeout=10`, то дополнительно будет присылать вердикт о необходимости блокировки потенциально опасных файлов и, если в течение 10 секунд не успеет завершить проверку, присылать вердикт о разрешении файла. Конкретные параметры и их значения разнятся для разных ICAP-серверов и для получения их списка и возможных значений вы можете обратиться к документации конкретного ICAP-сервера. В профиле ICAP-сервера возможно задать все пути, необходимые в ваших сетевых сценариях и добавить их описания.

  Внимание! PT NGFW самостоятельно составит полный URI для выполнения запросов к ICAP-серверу, используя параметры, указанные в профиле ICAP-сервера: icap://<адрес сервера>:<порт>/<reqmod-uri | respmod-uri>. Пример: icap://192.168.1.1:1344/scanrequest?modify=y&block-unwanted=y&timeout=100.

Второй шаг — в разделе **Объекты** → **ICAP** → **Профили** необходимо добавить ICAP-профиль, в котором указываются созданные ранее профили ICAP-серверов, включаются и настраиваются режимы (модификации запроса и (или) ответа), указываются отправляемые на проверку файлы и другие параметры. ICAP-профиль привязывается к правилу безопасности, разрешающему трафик, который необходимо передавать на ICAP-сервер или серверы.

Параметры профиля ICAP включают:

— **Название** (обязательно) — название ICAP-профиля.

— **Описание** (необязательно) — дополнительная информация о профиле или любые другие сведения на усмотрение администратора.

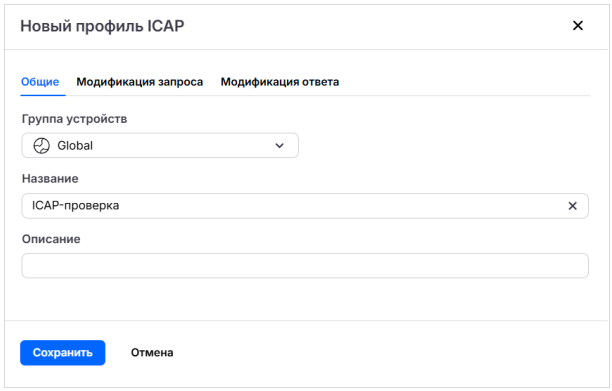


Рисунок 314. Добавление ICAP-профиля

— **Состояние** — включено или отключено. Если режим модификации запроса и (или) ответа отключен, то PT NGFW не отправляет данные запросов и (или) ответов HTTP-приложений на проверку ICAP-серверу. Если режим включен, то используются параметры, заданные на вкладке настройки режима.

— **Сервер ICAP** (обязательно) — выберите ранее созданный профиль ICAP-сервера. Для отправки данных HTTP-запросов и (или) ответов PT NGFW будет использовать параметры из указанного профиля сервера.

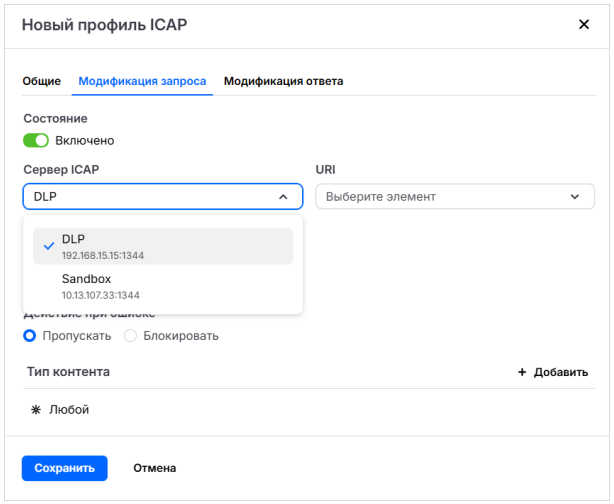


Рисунок 315. Выбор сервера ICAP

— **URI** (обязательно) — выберите один из заданных путей, который PT NGFW будет использовать для выполнения запросов к выбранному ICAP-серверу. В раскрывающемся списке отображаются пути, заданные в выбранном профиле ICAP-сервера.

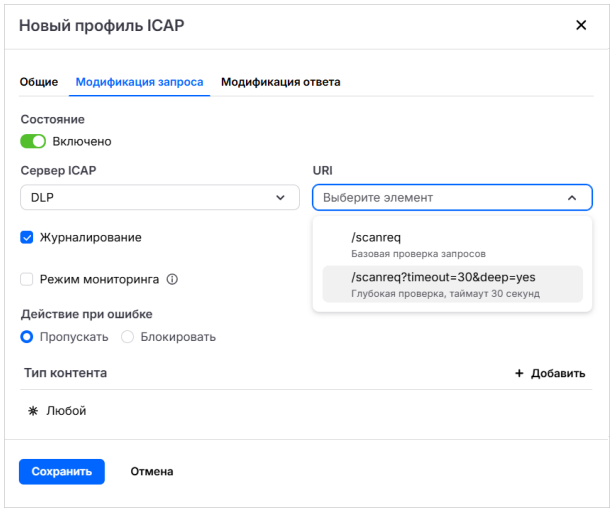


Рисунок 316. Выбор URI

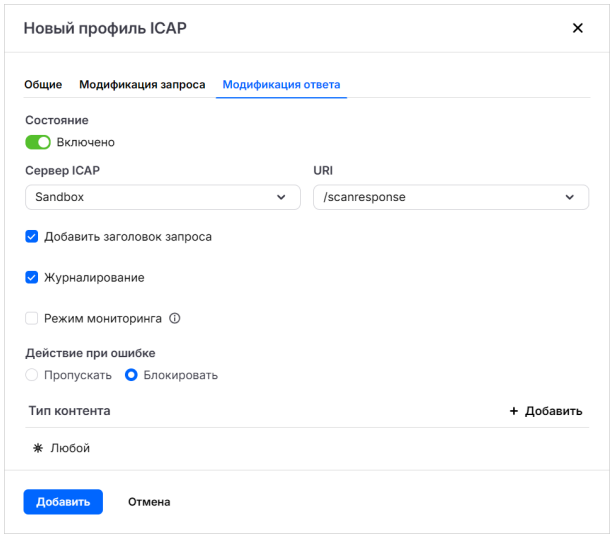


Рисунок 317. Выбор URI

- **Добавить заголовок запроса** (необязательно). Когда опция включена, PT NGFW при пересылке HTTP-ответа веб-сервера добавляет соответствующий HTTP-запрос в ICAP-сообщение, чтобы информировать ICAP-сервер, например песочницу, об исходном запросе, ответ на который пересылается в теле ICAP-сообщения. Таким образом, ICAP-сервер имеет возможность отобразить источник скачанного файла.
- **Журналирование** (необязательно) — если включено для режима, то PT NGFW отправляет события журнала в систему управления. События отображаются в разделе **Журналы** → **ICAP**.
- **Мониторинг** (необязательно) — для каждого из режимов можно включить режим **Мониторинг**, при активации которого PT NGFW будет отправлять HTTP-запросы и (или) ответы указанному ICAP-серверу и передавать эти HTTP-запросы и (или) ответы дальше, не задерживая их и не дожидаясь вердикта ICAP-сервера. В режиме мониторинга трафик всегда пропускается независимо от параметра **Действие при ошибке**.
- **Действие при ошибке** — параметр определяет, какое действие должен выполнить PT NGFW в случае недоступности ICAP-сервера, истечения таймаутов и других ошибок связи с ним. Если выбрано **Пропустить**, то PT NGFW будет пропускать проверяемый контент далее получателю, а если выбрано **Блокировать**, то PT NGFW будет блокировать передачу HTTP-запроса или ответа и отправлять сообщение TCP Reset клиенту и серверу. Например, PT NGFW предпринимает количество попыток подключения, указанных в профиле ICAP-сервера, и при каждой попытке ожидает тайм-аут подключения. Если PT NGFW исчерпал указанное количество попыток подключения, то ICAP-сервер считается недоступным и применяется указанное действие.
- **Тип контента** (необязательно) — позволяет выбрать типы и категории файлов, которые следует отправлять на проверку ICAP-серверу.

Внимание! HTTP-запросы и ответы, которые не содержат данных в теле сообщения, например HTTP-запрос GET или HTTP-ответ сервера, который содержит только заголовки, соответствуют типу файла **Unknown**. Для проверки такого контента фильтр в профиле ICAP должен содержать тип файлов **Unknown** или должен быть выбран тип файлов **Любой** (**Any**).

Внимание! Если в HTTP-сообщении передается содержимое типа multipart, то оно соответствует типу файла **Unknown**. Фильтр в профиле ICAP должен содержать тип файлов **Unknown** или должен быть выбран тип файлов **Любой** (**Any**). Извлечение отдельных файлов из multipart-контента, например извлечение только исполняемого файла или только документа, в настоящее время не поддерживается.

Третий шаг — указание ICAP-профиля в разделе **Политики** → **Безопасность** в правиле безопасности в разделе **Профили безопасности**. Трафик HTTP-приложений, который соответствует этому правилу безопасности, будет отправляться на проверку ICAP-серверу (серверам) в соответствии с указанным ICAP-профилем.

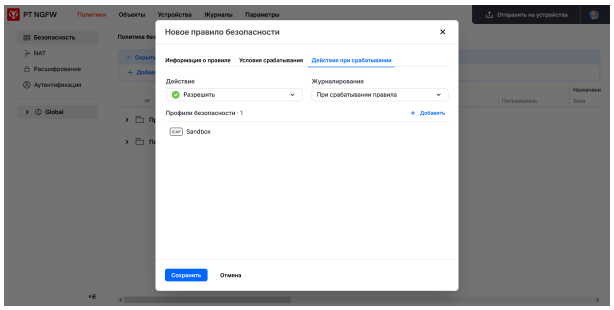


Рисунок 318. Выбор ICAP-профиля в правиле безопасности

Внимание! В одном правиле безопасности может быть указан только один ICAP-профиль.

Изменение профиля ICAP-сервера

- Чтобы изменить профиль ICAP-сервера,

  в разделе **Объекты** → **ICAP** → **Серверы** в контекстном меню профиля выберите **Изменить**.

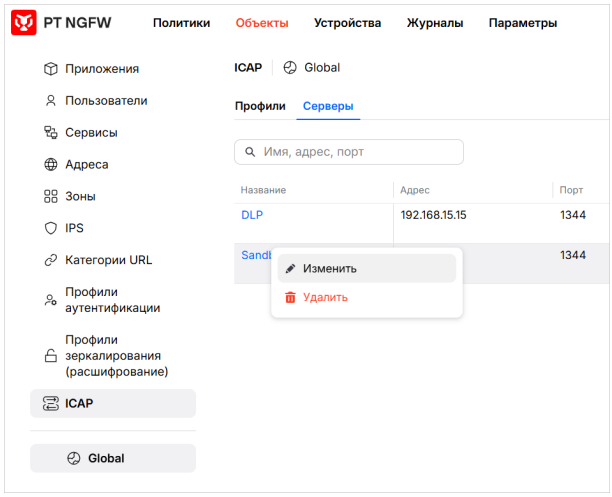


Рисунок 319. Изменение профиля ICAP-сервера

Примечание. Изменение или удаление ICAP-сервера затрагивает только новые сессии. Существующие сессии продолжают работать согласно тем параметрам, которые были актуальны на момент установления этих сессий.

Изменение ICAP-профиля

- Чтобы изменить ICAP-профиль,

  в разделе **Объекты** → **ICAP** → **Профили** в контекстном меню профиля выберите **Изменить**.

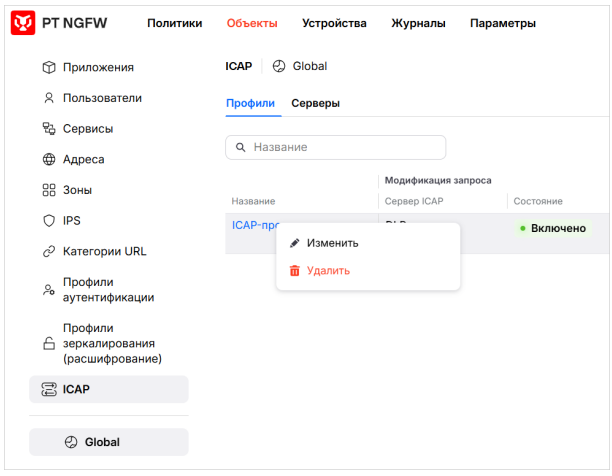


Рисунок 320. Изменение ICAP-профиля

Примечание. Изменение или удаление ICAP-профиля затрагивает только новые сессии. Существующие сессии продолжают работать согласно тем параметрам, которые были актуальны на момент установления этих сессий.

37. Аутентификация пользователей

Примечание. При необходимости получить инструкцию по настройке портала аутентификации нужно обратиться в службу технической поддержки PT NGFW. После настройки портала аутентификации можно добавлять адреса порталов при создании профилей аутентификации, а затем выбирать эти профили при создании правил.

Примечание. В рамках технической поддержки PT NGFW специалисты Positive Technologies не производят первичную или повторную установку и (или) настройку продукта, не решают проблемы с инфраструктурой заказчика или сторонним программным обеспечением, не проводят доработку, модификацию, разработку любого программного обеспечения или иных продуктов по запросам заказчика. Техническая поддержка также не включает обучение специалистов заказчика, объяснение принципов, алгоритмов, методов, лежащих в основе работы PT NGFW. Подробнее см. в разделе «О технической поддержке PT NGFW (см. раздел 49)"».

Используя правило аутентификации, вы можете настроить перенаправление пользователей на портал аутентификации, которая осуществляется в домене Active Directory, связанном с межсетевым экраном. Прохождение пользователями аутентификации позволяет применять к ним правила межсетевого экрана. Проверка трафика правилами аутентификации выполняется до проверки правилами безопасности и только для неаутентифицированных пользователей. Действием правила аутентификации может быть перенаправление или исключение трафика из процесса перенаправления.

При работе с политиками аутентификации необходимо учитывать следующее:

- Трафик, предназначенный для портала аутентификации, проверяется правилами безопасности, поэтому необходимо создать правило безопасности, разрешающее такой трафик.
- Любой трафик, отличный от DNS и подходящий под условия правила аутентификации, сбрасывается (TCP RST).
- При успешной аутентификации пользователь перенаправляется на запрошенный ранее ресурс, а его IP-адрес закрепляется за логином на время, указанное в основном конфигурационном файле устройства.

  Внимание! Перенаправление пользователей выполняется только для DNS-трафика.

Добавление профиля аутентификации

- Чтобы добавить профиль аутентификации:

  1. В главном меню выберите **Объекты**.
  2. Выберите вкладку **Профили аутентификации**.
  3. Нажмите **Добавить**.
  4. Выберите группу устройств.

5. Введите название профиля аутентификации.
6. Если требуется, введите описание профиля аутентификации.

   Примечание. Рекомендуется добавлять описание для упрощения последующей работы с профилем.
7. Выберите адрес портала аутентификации.
8. Нажмите **Добавить**.

Вы можете изменить или удалить профиль аутентификации в его контекстном меню.

38. SNMP-мониторинг

SNMP (Simple Network Management Protocol) — это протокол, который позволяет централизованно собирать информацию о состоянии сетевых устройств. Вы можете использовать SNMP для контроля состояния устройств PT NGFW (межсетевых экранов). Поддерживается SNMP версии 2c (SNMPv2c) и 3 (SNMPv3).

На каждом устройстве PT NGFW может быть запущен SNMP-агент. Он передает данные о различных показателях устройства SNMP-менеджеру (менеджерам) — устройству, с которого выполняется мониторинг. Данные могут передаваться либо как ответы на запросы от SNMP-менеджера (get requests, SNMP polling), либо как оповещения (traps). Ответы всегда передаются на тот UDP-порт, с которого приходят запросы; оповещения — по умолчанию на UDP-порт 162 (возможен выбор другого порта).

Запуск и настройка SNMP-агента выполняются из системы управления. Если устройство находится в кластере, то это выполняется для кластера (одновременно для всех устройств в кластере), а не для отдельного устройства. При этом каждый узел кластера самостоятельно отвечает на запросы и отправляет оповещения.

Функциональность имеет следующие ограничения:

— SNMP-агент получает и отправляет данные только через интерфейсы управления (не через dataplane).

— SNMP-агент поддерживает все типы сообщений, кроме SetRequest и InformRequest.

— SNMP-агент возвращает статистику только по физическим интерфейсам dataplane и интерфейсам Linux.

— Для dataplane-интерфейсов перечень поддерживаемых объектов таблиц ifTable и ifXTable в IF-MIB может отличаться в зависимости от драйвера сетевой карты. Для неподдерживаемых объектов возвращается значение **0**.

Параметры устройства PT NGFW, которые вы можете отслеживать путем отправки запросов, включают:

— общие сведения об устройстве (версия ПО и продукта, состояние узла в кластере и др.);

— используемые ресурсы (загрузка CPU, RAM, объем свободного места на дисках);

— количество соединений (общее и в секунду);

— загрузка физических интерфейсов (количество входящих и исходящих пакетов, пакетов с ошибками).

Информация о работе устройства PT NGFW, которую вы можете получать в виде оповещений, включает сведения о:

— запуске устройства;

— изменении статуса физического интерфейса;

— возникновении ошибки аутентификации SNMP.

В журнале **Аудит** фиксируется изменение параметров SNMP-агента. В системном журнале фиксируются ошибки запросов, отправка оповещений, ошибки аутентификации и другие события.

Для некоторых пользовательских ролей доступ к функциональности частично или полностью ограничен.

Мониторинг PT NGFW по протоколу SNMP осуществляется с использованием OID из проприетарной MIB и стандартных: MIB-II, HOST-RESOURCES-MIB, IF-MIB.

В этом разделе

Настройка и запуск SNMP-агента (см. раздел 38.1)

Поддерживаемые объекты из стандартных MIB (см. раздел 38.2)

Перечень объектов из проприетарной MIB (см. раздел 38.3)

38.1. Настройка и запуск SNMP-агента

Настройка включает настройку общих параметров, параметров SNMPv2c или SNMPv3 и выбор оповещений для отправки.

Настройка и запуск выполняются на странице устройства или кластера на вкладке **SNMP**.

Настройка общих параметров SNMP-агента

- Чтобы настроить общие параметры SNMP-агента:

  1. На вкладке **Общие** нажмите **Изменить**.
  2. Настройте общие параметры SNMP:
     - **Состояние SNMP-агента** — включение (запуск) или отключение SNMP-агента;
     - **Порт SNMP-агента** — порт для прослушивания запросов от SNMP-менеджера (менеджеров);
     - **Расположение** — информация о физическом расположении устройства;

       Примечание. Значения полей **Расположение** и **Контактная информация** можно будет получить, используя соответствующие SNMP-запросы.

     - **Контактная информация**;

       Примечание. При настройке SNMP-агента для кластера расположение и контактная информация указываются отдельно для каждого из узлов кластера.
  3. Нажмите **Сохранить**.

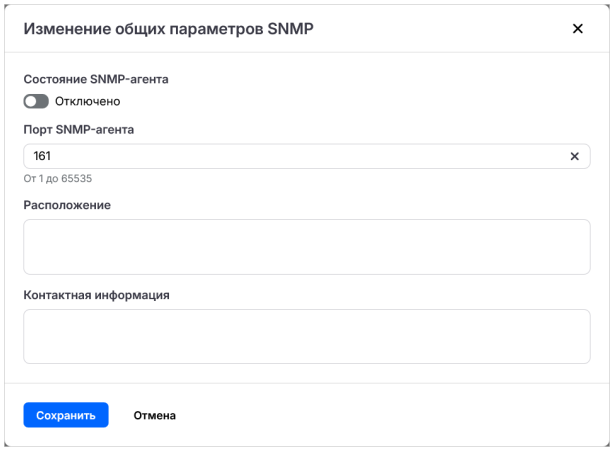


Рисунок 321. Изменение общих параметров SNMP

Настройка параметров SNMPv2c

Настройка заключается в добавлении community (сообщества), в котором, среди прочего, указывается:

— Имя SNMP-сообщества — агент будет обрабатывать запросы и отправлять оповещения с указанием этого имени.

Примечание. Имя SNMP-сообщества содержится в каждом SNMP-сообщении. Фактически это имя логической группы, состоящей из одного или более менеджеров и агентов, и в то же время пароль, предъявление которого делает обмен сообщениями возможным — агент и менеджер отбрасывают сообщение, содержащее имя SNMP-сообщества, неизвестное им.

— IP-адреса, запросы с которых должны обрабатываться, если они содержат указанное имя SNMP-сообщества.

— IP-адреса, на которые должны отправляться оповещения с указанным именем SNMP-сообщества.

Вы можете добавить более одного community.

Внимание! В протоколе SNMPv2c данные передаются в открытом (незашифрованном) виде.

► Чтобы добавить community:

1. Выберите вкладку **SNMP v2c**.
2. Нажмите **Добавить**.
3. Настройте параметры community:
   - **Community** — имя SNMP-сообщества; ;
   - **Обработка запросов** — включение или отключение обработки запросов с указанным именем SNMP-сообщества;

- **Разрешенные SNMP-менеджеры** — IP-адреса или подсети, запросы из которых требуется обрабатывать;
- **Trap-сообщения** — включение или отключение отправки оповещений с указанным именем SNMP-сообщества;
- **Получатели** — IP-адреса, на которые требуется отправлять оповещения;
- **Порт** — порт назначения для отправки оповещений.

4. Нажмите **Сохранить**.

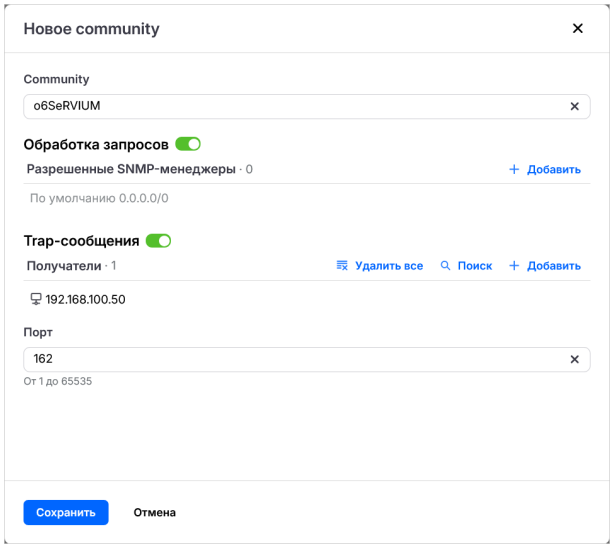


Рисунок 322. Настройка параметров SNMPv2c

Настройка параметров SNMPv3

Настройка заключается в добавлении пользователя. При этом, помимо прочего, указываются:

— Имя SNMP-пользователя — агент будет обрабатывать запросы и отправлять оповещения с указанием этого имени.

Примечание. Имя SNMP-пользователя содержится в каждом SNMP-сообщении. Оно может рассматриваться как пароль, предъявление которого делает обмен сообщениями возможным — агент и менеджер отбрасывают сообщение, содержащее имя SNMP-пользователя, неизвестное им.

— IP-адреса, запросы с которых должны обрабатываться, если они содержат указанное имя SNMP-пользователя.

— IP-адреса, на которые должны отправляться оповещения с указанным именем SNMP-пользователя.

— Уровень безопасности — выбор уровня безопасности, отличного от уровня по умолчанию, позволяет повысить безопасность взаимодействия агента PT NGFW и менеджера при использовании указанного имени SNMP-пользователя.

Возможен выбор одного из трех уровней безопасности:

— **noAuthNoPriv.** Не предусматривает аутентификацию или конфиденциальность. Данные, передаваемые между агентом и менеджером, передаются в незашифрованном виде.

— **authNoPriv.** Предусматривает аутентификацию на основе пароля с хешированием, но не конфиденциальность. Данные передаются по сети в незашифрованном виде.

— **authPriv.** Предусматривает аутентификацию на основе пароля с хешированием и конфиденциальность. За исключением имени пользователя, данные передаются по сети в зашифрованном виде.

Вы можете добавить более одного пользователя.

► Чтобы добавить пользователя:

1. Выберите вкладку **SNMP v3**.
2. Нажмите **Добавить**.
3. Настройте параметры пользователя:
   - **Имя пользователя** — имя SNMP-пользователя;
   - **Уровень безопасности**;
   - **Алгоритм аутентификации** — алгоритм, используемый для создания хеш-суммы;
   - **Пароль аутентификации** — пароль, используемый для создания хеш-суммы;
   - **Алгоритм шифрования** — алгоритм, используемый для шифрования данных;
   - **Пароль шифрования** — пароль, используемый для шифрования данных;
   - **Обработка запросов** — включение или отключение обработки запросов с указанным именем SNMP-пользователя;
   - **Trap-сообщения** — включение или отключение отправки оповещений с указанным именем SNMP-пользователя;
   - **Получатели** — IP-адреса, на которые требуется отправлять оповещения;
   - **Порт** — порт назначения для отправки оповещений.
4. Нажмите **Сохранить**.

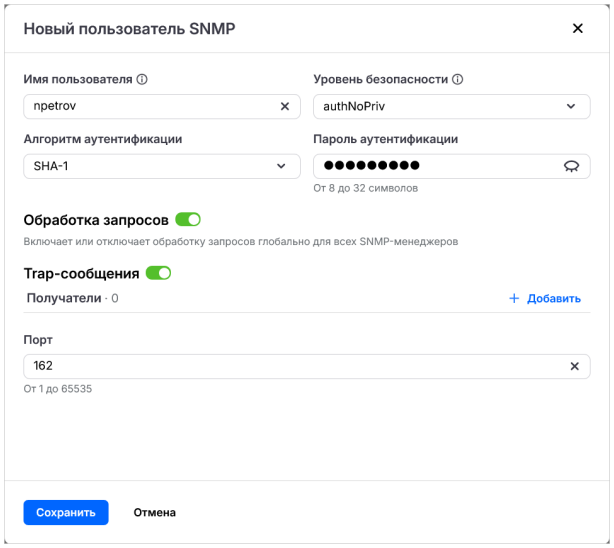


Рисунок 323. Настройка параметров SNMPv3

Включение или отключение оповещений

- Чтобы включить или отключить отправку оповещений определенного типа:

  1. Выберите вкладку **Trap-сообщения**.
  2. Нажмите **Изменить**.
  3. Включите или отключите оповещения.
  4. Нажмите **Сохранить**.

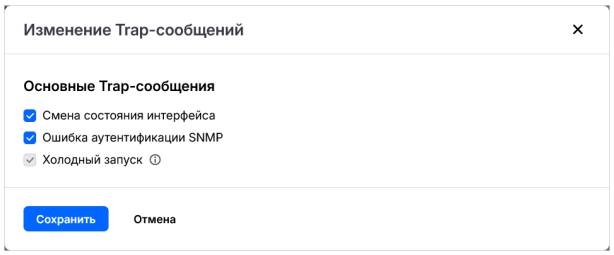


Рисунок 324. Включение или отключение оповещений

38.2. Поддерживаемые объекты из стандартных MIB

Объекты MIB-II

Объекты для запросов:

— **sysObjectID** — OID объекта **ptNgfwMib** из проприетарного MIB. Всегда возвращается значение **1.3.6.1.4.1.50213.1**.

— **sysUpTime** — время, прошедшее с последней реинициализации SNMP-агента.

— **sysContact** — контактная информация, заданная в конфигурации SNMP-агента.

— **sysName** — название устройства, заданное в системе управления.

— **sysLocation** — расположение устройства, заданное в конфигурации SNMP-агента.

— **sysServices** — набор поддерживаемых сервисов.

Объекты для оповещений (traps):

— **linkDown** — переход интерфейса в состояние Down.

— **linkUp** — переход интерфейса в состояние Up.

— **coldStart** — перезагрузка устройства или первый запуск SNMP-агента после получения конфигурации.

— **authenticationFailure** — ошибка аутентификации.

Объекты HOST-RESOURCES-MIB

— **hrDeviceIndex** — индекс устройства.

— **hrDeviceType** — тип устройства (всегда равно **hrDeviceProcessor**).

— **hrDeviceDescr** — описание процессора. Возможные значения: **Management Processor** — для неизолированных ядер Linux, **Control Processor** — для изолированных ядер Linux, **Data Processor** — для ядер обработки трафика.

— **hrDeviceStatus** — статус процессора. Возможные значения: **unknown(1)** — состояние неизвестно, **running(2)** — работает без ошибок, **warning(3)** — работает с ошибками, **down(5)** — недоступен.

— **hrDeviceErrors** — количество зафиксированных ошибок для данного процессора.

— **hrProcessorLoad** — среднее значение загрузки процессора в процентах за последнюю минуту.

— **hrMemorySize** — объем физической памяти.

— **hrStorageIndex** — индекс хранилища.

— **hrStorageType** — тип хранилища. Возможные значения: **hrStorageRam** — для физического RAM, **hrStorageVirtualMemory** — для HugePages, **hrStorageFixedDisk** — для разделов диска.

— **hrStorageDescr** — описание хранилища. Возможные значения: **Physical memory** — для физического RAM, **Heap numa<номер Numa node>** — для HugePages, **System Partition** - для загрузочного(основного) раздела диска, **Configuration Partition** — для раздела диска с конфигурацией, контентом и дистрибутивом обновления, **Logs Partition** — раздел диска с журналами.

— **hrStorageAllocationUnits** — размерность данных в байтах.

— **hrStorageSize** — общий размер хранилища в единицах **hrStorageAllocationUnits**.

— **hrStorageUsed** — занятый размер хранилища в единицах **hrStorageAllocationUnits**.

— **hrStorageAllocationFailures** — количество запросов на хранение, которые не удалось выполнить из-за нехватки места.

— **hrSystemUptime** — количество времени с последней инициализации SNMP-агента.

— **hrSystemDate** — локальная дата и время системы.

— **hrSystemInitialLoadParameters** — строка параметров загрузки ОС.

— **hrSystemNumUsers** — количество пользователей.

— **hrSystemProcesses** — количество процессов, которые загружены в память или выполняются.

Объекты IF-MIB

— **ifNumber** — количество интерфейсов, по которым возвращается статистика.

— **ifIndex** — для интерфейсов ОС Linux — номер интерфейса, для физических интерфейсов dataplane — результат сложения 1000 и номера порта (например, **1001**, если номер порта равен 1).

— **ifDescr** — описание интерфейса.

— **ifType** — тип интерфейса.

— **ifMtu** — максимальный размер пакета в байтах, который можно отправить или получить через этот интерфейс.

— **ifSpeed** — пропускная способность в битах в секунду. Если значение пропускной способности превышает 4294967295, SNMP-агент возвращает значение **4294967295**.

— **ifPhysAddress** — физический адрес интерфейса (MAC-адрес).

— **ifAdminStatus** — состояние интерфейса, заданное администратором. Возможные значения: **up(1)** — включено, **down (2)** — отключено.

— **ifOperStatus** — текущее состояние интерфейса. Возможные значения: **up(1)** — интерфейс активен, **down (2)** — интерфейс неактивен, **unknown (4)** — интерфейс в неизвестном состоянии, **dormant (5)** — интерфейс ожидает внешнего воздействия, **notPresent(6)** — интерфейс отсутствует, **lowerLayerDown (7)** — интерфейс не может передавать пакеты, потому что он работает поверх других интерфейсов, которые недоступны. Для физических интерфейсов dataplane возвращаются только состояния **up(1)** и **down (2)**. Если состояние **ifAdminStatus** изменилось на **up(1)**, то состояние **ifOperStatus** изменится на **up(1)** при отсутствии ошибок на интерфейсе.

— **ifLastChange** — значение **SysUpTime**, когда интерфейс последний раз менял состояние (**ifOperStatus**).

— **ifInOctets** — количество байтов, принятое интерфейсом.

— **ifInUcastPkts** — количество принятых одноадресных пакетов.

- **ifInDiscards** — количество принятых пакетов, которые были отброшены, даже если не было ошибок, препятствующих их доставке.
- **ifInErrors** — количество принятых пакетов с ошибками, препятствующими их доставке.
- **ifInUnknownProtos** — количество принятых пакетов, которые были отброшены из-за неизвестного или неподдерживаемого протокола.
- **ifOutOctets** — количество байтов, отправленных интерфейсом.
- **ifOutUcastPkts** — количество исходящих одноадресных пакетов.
- **ifOutDiscards** — количество исходящих пакетов, которые были отброшены, даже если не было ошибок, препятствующих их доставке.
- **ifOutErrors** — количество исходящих пакетов с ошибками, препятствующими их доставке.
- **ifName** — название интерфейса.
- **ifInMulticastPkts** — количество принятых пакетов многоадресной рассылки.
- **ifInBroadcastPkts** — количество принятых широковещательных пакетов.
- **ifOutMulticastPkts** — количество исходящих пакетов многоадресной рассылки.
- **ifOutBroadcastPkts** — количество исходящих широковещательных пакетов.
- **ifHCInOctets** — назначение аналогично **ifInOctets**. Счетчик большей емкости.
- **ifHCInUcastPkts** — назначение аналогично **ifInUcastPkts**. Счетчик большей емкости.
- **ifHCInMulticastPkts** — назначение аналогично **ifInMulticastPkts**. Счетчик большей емкости.
- **ifHCInBroadcastPkts** — назначение аналогично **ifInBroadcastPkts**. Счетчик большей емкости.
- **ifHCOutOctets** — назначение аналогично **ifOutOctets**. Счетчик большей емкости.
- **ifHCOutUcastPkts** — назначение аналогично **ifOutUcastPkts**. Счетчик большей емкости.
- **ifHCOutMulticastPkts** — назначение аналогично **ifOutMulticastPkts**. Счетчик большей емкости.
- **ifHCOutBroadcastPkts** — назначение аналогично **ifOutBroadcastPkts**. Счетчик большей емкости.
- **ifLinkUpDownTrapEnable** — включена ли отправка trap-сообщений об изменении состояния интерфейса. Возможные значения: **true(1)** — включена, **false(2)** — отключена.
- **ifHighSpeed** — пропускная способность интерфейса в Мбит/с.
- **ifPromiscuousMode** — «неразборчивый» режим. Возможные значения: **true(1)** — принимает все пакеты, **false(2)** — принимает только пакеты, адресованные устройству. Значение не влияет на прием широковещательных и многоадресных пакетов.
- **ifConnectorPresent** — наличие физического разъема у интерфейса. Возможные значения: **true(1)** — физический интерфейс, **false(2)** — логический интерфейс.

38.3. Перечень объектов из проприетарной MIB

Проприетарный MIB-файл может быть загружен по ссылке.

Объекты из проприетарной MIB включают:

- **ptFwProductVersion** — версия продукта.
- **ptFwSoftwareVersion** — версия ПО.
- **ptFwSerialNumber** — серийный номер.
- **ptFwSessionActive** — общее количество активных сессий.
- **ptFwSessionCps** — количество соединений в секунду.
- **ptFwPoolDescr** — описание пула.
- **ptFwPoolUsage** — использование пула в процентах.
- **ptFwHADeviceMode** — режим работы устройства (standalone, active-standby).
- **ptFwHANodeStatus** — состояние узла кластера (**ok**, **warning**, **error**).
- **ptFwHANodeRole** — роль узла кластера (active, standby).
- **ptFwHANodeSuspendMode** — состояние режима ожидания (**enabled**, **disabled**).

39. Работа с журналами

PT NGFW регистрирует события, для которых настроено журналирование, и записывает их в журнал соответствующего типа:

- **Трафик** — информация об IP-пакетах, проходящих через сетевые интерфейсы. Записи в журнале трафика формируются при срабатывании правил безопасности.
- **Расшифрование** — срабатывания правил расшифрования.
- **IPS** — информация о срабатывании правил системы предотвращения вторжений.
- **Антивирус** — события антивируса, например попытки передачи зараженных файлов.
- **Политика аутентификации**. В этом журнале фиксируются срабатывания правил аутентификации.
- **ICAP** — события, связанные с обработкой трафика ICAP-сервером.
- **IPsec** — журнал IPsec-соединений, содержащий данные об установлении и разрыве соединения, а также об ошибках согласования параметров или селекторов трафика.
- **Удаленный доступ** — события изменения состояния соединений VPN.
- **Аудит** — действия пользователей в системе управления: создание виртуальных контекстов, настройка правил межсетевого экрана, работа с учетными записями и пр.
- **Аутентификация** — попытки входа в систему управления и выхода.

Записи журналов содержат детальную информацию о событиях: время срабатывания правила безопасности, адреса источника и назначения и пр. Подробное описание параметров записей в зависимости от типа журнала см. в разделе «Параметры событий, регистрируемых в журналах (см. раздел 39.5)».

Система журналирования использует для регистрации и хранения событий сборщик журналов — сетевой сервис для централизованного хранения журналов от нескольких устройств. Вы можете использовать сборщик журналов, установленный на узле системы управления, либо сборщик, развернутый на внешнем сетевом узле.

Просмотр журналов и настройка взаимодействия PT NGFW со сборщиками журналов осуществляется в системе управления. Для узлов PT NGFW, работающих в одиночном режиме или в кластере, вы можете назначить основной и резервный сборщик журналов, которые будут регистрировать события этих узлов. При этом резервный сборщик будет использоваться при недоступности основного.

В этом разделе

Настройка сборщиков журналов (см. раздел 39.1)

Просмотр журналов (см. раздел 39.2)

Передача журналов по протоколу syslog (см. раздел 39.3)

Работа с системным журналом (см. раздел 39.4)

Параметры событий, регистрируемых в журналах (см. раздел 39.5)

Параметры syslog-сообщений (см. раздел 39.6)

Причины завершения сессий (см. раздел 39.7)

39.1. Настройка сборщиков журналов

В этом разделе описаны шаги по добавлению сборщика журналов и его назначению для устройства.

Добавление сборщика журналов

Чтобы добавить сборщик журналов:

1. В главном меню выберите **Параметры**.
2. Выберите вкладку **Сборщики журналов**.
3. Нажмите **Добавить**.

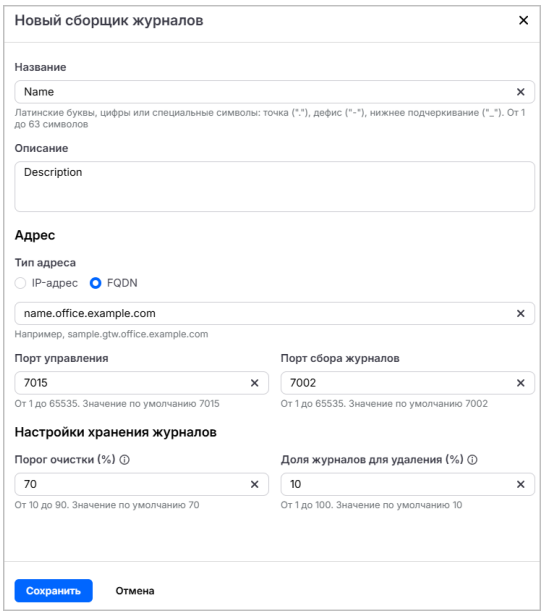


Рисунок 325. Добавление сборщика журналов

4. Введите параметры сборщика журналов:
   - **Название** — имя, под которым сборщик будет отображаться в системе управления;
   - **Описание** — расширенная информация о сборщике;
   - **Тип адреса** — формат адреса сборщика;
   - **Адрес** — IP-адрес или FQDN (в зависимости от выбранного типа) узла, на котором развернут сборщик;

- **Порт управления** — номер порта, по которому осуществляется управление сборщиком;
- **Порт сбора журналов** — номер порта, по которому устройства подключаются к сборщику для передачи журналов;
- **Порог очистки (%)** — степень заполнения, при достижении которой начнется очистка хранилища журналов;
- **Доля журналов для удаления (%)** — процент от общего количества журналов, который будет удален при очистке хранилища.

5. Нажмите **Сохранить**.

Назначение сборщика журналов для устройства

Чтобы назначить сборщик журналов для устройства:

1. В главном меню выберите **Устройства**, затем имя устройства или кластера.
2. Выберите **Журналирование**.

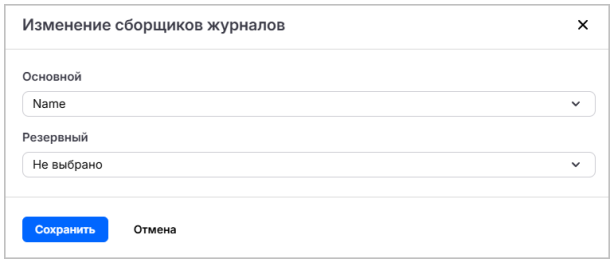


Рисунок 326. Окно выбора сборщиков журналов

3. Выберите основной и резервный сборщики журналов.

Назначенные сборщики журналов будут использоваться для регистрации событий этого устройства, при этом резервный сборщик будет использоваться в случае недоступности основного.

39.2. Просмотр журналов

Записи журналов выводятся в табличном виде в хронологическом порядке с учетом выбранного периода и фильтров. Чтобы просмотреть журналы:

1. В главном меню выберите **Журналы**, затем выберите необходимый тип журнала.

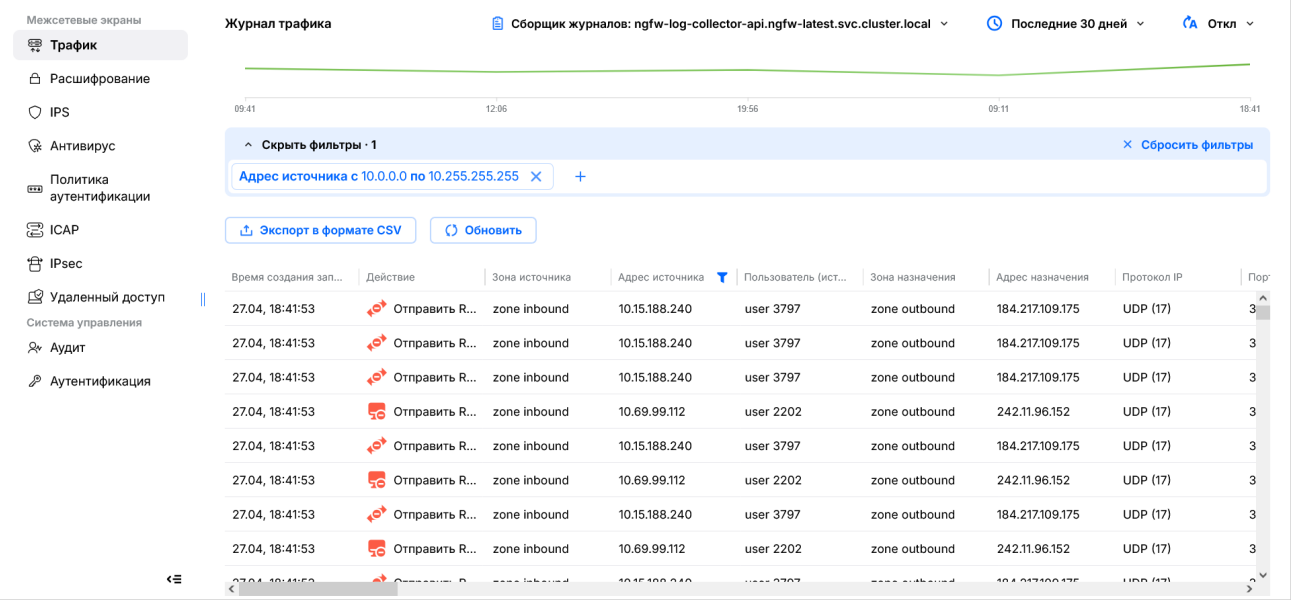


Рисунок 327. Страница **Журналы**

2. Выберите **Сборщик журналов**, записи которого хотите просмотреть.
3. Задайте период времени, за который хотите просмотреть записи.
4. Для поиска нужных записей задайте один или несколько фильтров.

Вы можете экспортировать записи журнала, нажав **Экспорт в формате CSV**. Размер CSV-файла ограничен 500 МБ — при достижении этого размера формирование файла завершается и начинается скачивание.

39.3. Передача журналов по протоколу syslog

Вы можете передавать информацию о журналируемых событиях во внешние системы (например, SIEM) по протоколу syslog. Для использования этой функции необходимо добавить хотя бы один syslog-сервер и настроить правила отправки событий. Параметры syslog-сообщений зависят от типа передаваемых событий, подробнее см. в разделе Параметры syslog-сообщений (см. раздел 39.6).

Добавление syslog-сервера

- Чтобы добавить syslog-сервер:
  1. В главном меню выберите **Параметры**.
  2. Выберите вкладку **Syslog-серверы**.
  3. Нажмите **Добавить**.
  4. Введите название сервера.
  5. Если требуется, введите описание.

6. Укажите IP-адрес сервера или FQDN.
7. Если требуется, укажите порт сервера, отличный от 514.
8. Нажмите **Сохранить**.

Syslog-сервер может быть изменен или удален — в контекстном меню сервера.

Примечание. Удаление сервера возможно, если он не указан ни в одном из правил отправки событий.

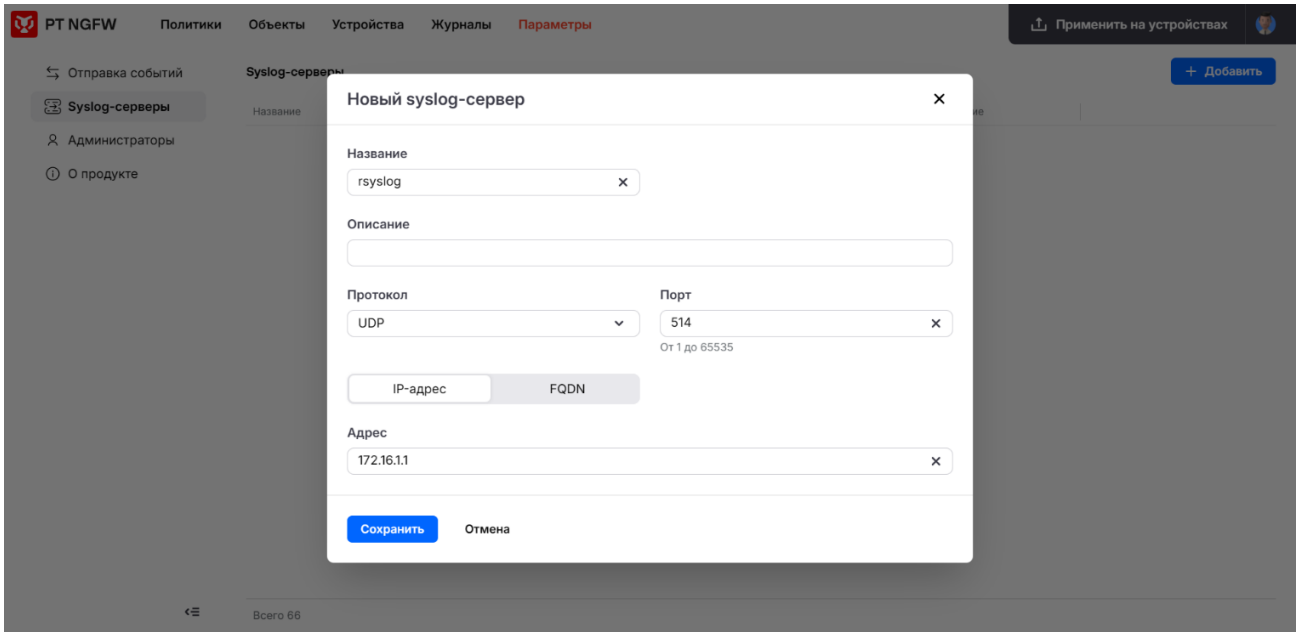


Рисунок 328. Добавление syslog-сервера

Добавление правила отправки событий

- Чтобы добавить правило отправки событий:

1. В главном меню выберите **Параметры**.
2. Нажмите **Добавить**.
3. Введите название правила.
4. Если требуется, введите описание.
5. Выберите типы журналов, к которым относятся события.
6. Нажмите **Добавить** и выберите syslog-серверы, на которые должны приходить сообщения о событиях.
7. Нажмите **Сохранить**.

Правило отправки событий может быть изменено или удалено — в контекстном меню правила.

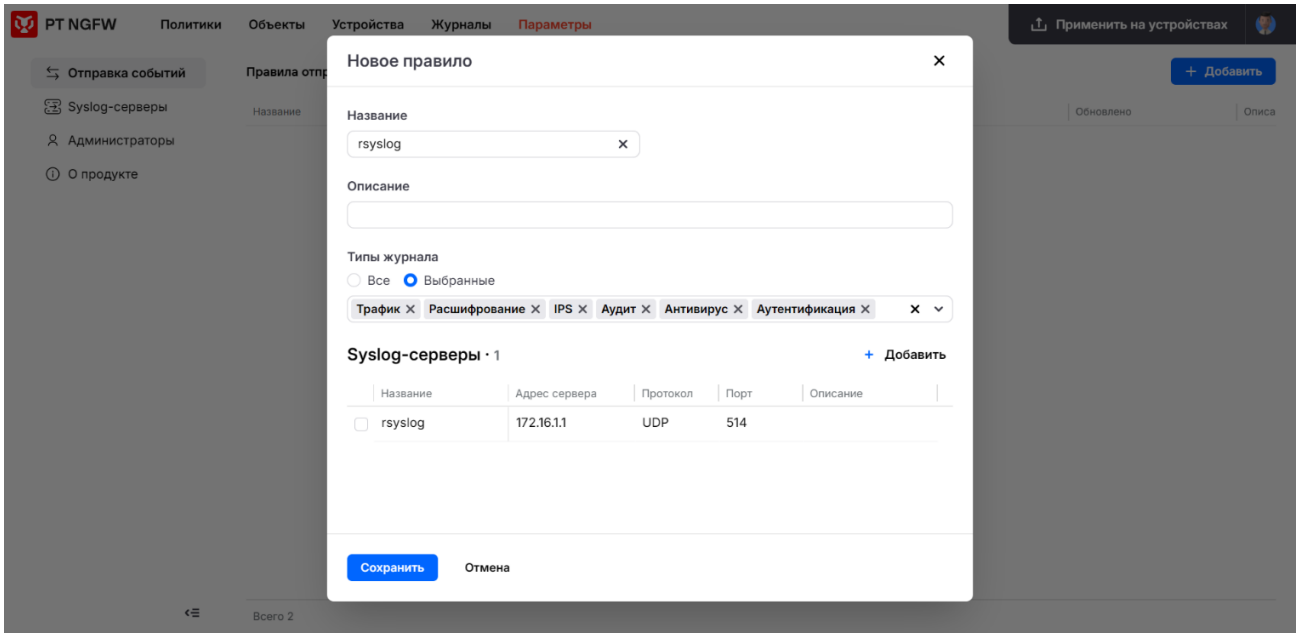


Рисунок 329. Добавление правила отправки событий

39.4. Работа с системным журналом

Службы PT NGFW записывают информацию о событиях, происходящих в процессе их работы, в системные журналы. Эти журналы позволяют контролировать работоспособность PT NGFW, своевременно выявлять и устранять причины сбоев в его работе.

Работа с системными журналами осуществляется с помощью командного интерпретатора. Подробнее см. в разделе Интерфейс командной строки (см. раздел 46).

39.5. Параметры событий, регистрируемых в журналах

Параметры записей журнала трафика

- **Время создания записи** — дата и время создания записи;
- **Действие** — действие, выполненное над трафиком, например разрешение прохождения;
- **Зона источника** — зона безопасности источника трафика;
- **Адрес источника** — IP-адрес источника трафика;
- **Пользователь (источник)** — учетная запись Active Directory источника трафика;
- **Зона назначения** — зона безопасности назначения трафика;
- **Адрес назначения** — IP-адрес назначения трафика;
- **Протокол IP**;
- **Порт назначения** — порт назначения трафика;

— **Приложение** — протокол прикладного уровня или приложение, которые были определены в трафике;

— **Категории URL** — список категорий сервера из запроса клиента;

— **Правило безопасности** — название сработавшего правила безопасности;

— **Причина завершения сессии** — причина завершения сессии, например по тайм-ауту;

Примечание. С полным списком возможных причин завершения сессии можно ознакомиться в разделе «Причины завершения сессий (см. раздел 39.7)».

— **Страна источника** — страна источника трафика;

— **Регион источника** — регион источника трафика;

— **Входящий интерфейс** — физический интерфейс, с которого пакет вошел в межсетевой экран;

— **Страна назначения** — страна назначения трафика;

— **Регион назначения** — регион назначения трафика;

— **Исходящий интерфейс** — физический интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;

— **Название PBR** — название сработавшего правила PBR;

— **Правило NAT** — название правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;

— **Транслированный IP-адрес источника** — IP-адрес источника трафика после трансляции сетевых адресов;

— **Транслированный порт источника** — порт источника трафика после трансляции сетевых адресов;

— **Транслированный IP-адрес назначения** — IP-адрес назначения трафика после трансляции сетевых адресов;

— **Транслированный порт назначения** — порт назначения трафика после трансляции сетевых адресов;

— **Порт источника** — порт источника трафика;

— **Расшифрование** — **Да**, если трафик был расшифрован;

— **Название устройства** — название устройства, на котором была зафиксирована сессия;

— **Модель устройства** — модель устройства, на котором была зафиксирована сессия;

— **Серийный номер устройства** — серийный номер устройства, на котором была зафиксирована сессия;

— **Название виртуального контекста** — название виртуального контекста, на котором была зафиксирована сессия;

— **MAC-адрес источника** — MAC-адрес источника трафика;

- **MAC-адрес назначения** — MAC-адрес назначения трафика;
- **X-Forwarded-For IP** — значение заголовка X-Forwarded-For;
- **Идентификатор сессии** — идентификатор сессии, сгенерированный межсетевым экраном;
- **Длительность сессии (с)** — длительность сессии в секундах;
- **Время начала сессии** — дата и время начала сессии;
- **Время завершения сессии** — дата и время завершения сессии;
- **Первый пакет получен** — дата и время получения первого пакета;
- **Получено байтов** — число байтов, полученных в рамках сессии;
- **Отправлено байтов** — число байтов, отправленных в рамках сессии;
- **Получено пакетов** — число пакетов, полученных в рамках сессии;
- **Отправлено пакетов** — число пакетов, отправленных в рамках сессии;
- **Запись получена** — дата и время получения записи модулем журналирования;
- **Пользователь (назначение)** — учетная запись Active Directory назначения трафика;
- **Идентификатор правила** — идентификатор сработавшего правила безопасности.

Параметры записей журнала расшифрования

- **Время создания записи** — дата и время создания записи;
- **Действие** — действие, выполненное над трафиком;
- **Зона источника** — зона безопасности источника трафика;
- **Адрес источника** — IP-адрес источника трафика;
- **Пользователь (источник)** — учетная запись Active Directory источника трафика;
- **Зона назначения** — зона безопасности назначения трафика;
- **Адрес назначения** — IP-адрес назначения трафика;
- **Протокол IP**;
- **Порт назначения** — порт назначения трафика;
- **Приложение** — протокол прикладного уровня или приложение, которые были определены в трафике;
- **Категории URL** — список категорий сервера из запроса клиента;
- **Правило расшифрования** — название сработавшего правила расшифрования;
- **Описание ошибки** — ошибка расшифрования;
- **Страна источника** — страна источника трафика;

- **Регион источника** — регион источника трафика;
- **Входящий интерфейс** — физический интерфейс, с которого пакет вошел в межсетевой экран;
- **Страна назначения** — страна назначения трафика;
- **Регион назначения** — регион назначения трафика;
- **Исходящий интерфейс** — физический интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;
- **Транслированный IP-адрес источника** — IP-адрес источника трафика после трансляции сетевых адресов;
- **Транслированный IP-адрес назначения** — IP-адрес назначения трафика после трансляции сетевых адресов;
- **Транслированный порт источника** — порт источника трафика после трансляции сетевых адресов;
- **Транслированный порт назначения** — порт назначения трафика после трансляции сетевых адресов;
- **Правило трансляции** — название правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;
- **Идентификатор сессии** — идентификатор сессии, сгенерированный межсетевым экраном;
- **Получено байтов** — число байтов, полученных в рамках сессии;
- **Отправлено пакетов** — число пакетов, отправленных в рамках сессии;
- **Пользователь (назначение)** — учетная запись Active Directory назначения трафика;
- **Получено пакетов** — число пакетов, полученных в рамках сессии;
- **Отправлено пакетов** — число пакетов, отправленных в рамках сессии;
- **Запись получена** — дата и время получения записи модулем журналирования;
- **Идентификатор правила** — идентификатор сработавшего правила расшифрования;
- **Порт источника** — порт источника трафика;
- **Название устройства** — название устройства, на котором была зафиксирована сессия;
- **Модель устройства** — модель устройства, на котором была зафиксирована сессия;
- **Серийный номер устройства** — серийный номер устройства, на котором была зафиксирована сессия;
- **Название виртуального контекста** — название виртуального контекста, на котором была зафиксирована сессия;
- **Сессия клиент-NGFW** — этап образования TLS-соединения между клиентом и межсетевым экраном;

— **Сессия NGFW-сервер** — этап образования TLS-соединения между сервером и межсетевым экраном;

— **Версия TLS** — версия TLS-протокола, используемая в сессии, например TLSv1.3 или TLSv1.2;

— **Алгоритм обмена ключами** — алгоритм обмена ключами, используемый в сессии, например RSA или DHE;

— **Алгоритм шифрования** — алгоритм, используемый для шифрования данных сессии, например AES-128-CBC;

— **Алгоритм хеширования** — алгоритм создания хеша, используемый в сессии, например SHA, SHA-256, SHA-384;

— **Серийный номер сертификата**;

— **Отпечаток сертификата**;

— **Начало действия сертификата**;

— **Конец действия сертификата**;

— **Версия сертификата**;

— **Общее имя субъекта**;

— **Общее имя издателя**;

— **Общее имя корневого сертификата**;

— **Указание имени сервера (SNI)**;

— **Статус корневого сертификата**;

— **Альтернативные имена субъекта сертификата**;

— **Состояние цепочки сертификатов**;

— **MAC-адрес источника** — MAC-адрес источника трафика;

— **MAC-адрес назначения** — MAC-адрес назначения трафика.

Параметры записей журнала IPS

— **Время создания записи** — дата и время создания записи;

— **Действие** — действие, выполненное в отношении сессии;

— **Название угрозы** — название сигнатуры, которой соответствует обнаруженная активность;

— **Уровень опасности** — степень опасности вредоносной активности;

— **CVE** — CVE-идентификатор уязвимости;

— **Имя файла** — имя файла из запроса клиента или ответа сервера;

— **Зона источника** — зона безопасности источника трафика;

- **Адрес источника** — IP-адрес источника трафика;
- **Пользователь (источник)** — учетная запись Active Directory источника трафика;
- **Зона назначения** — зона безопасности назначения трафика;
- **Адрес назначения** — IP-адрес назначения трафика;
- **Протокол IP**;
- **Порт назначения** — порт назначения трафика;
- **Приложение** — протокол прикладного уровня или приложение, которые были определены в трафике;
- **URL** — URL-адрес, к которому происходит обращение;
- **Категории URL** — список категорий сервера из запроса клиента;
- **Правило безопасности** — название сработавшего правила безопасности;
- **Категория угрозы** — категория вредоносной активности;
- **Идент. сигнатуры** — идентификатор сигнатуры;
- **Страна источника** — страна источника трафика;
- **Регион источника** — регион источника трафика;
- **Входящий интерфейс** — физический интерфейс, с которого пакет вошел в межсетевой экран;
- **Страна назначения** — страна назначения трафика;
- **Регион назначения** — регион назначения трафика;
- **Исходящий интерфейс** — физический интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;
- **Транслированный IP-адрес источника** — IP-адрес источника трафика после трансляции сетевых адресов;
- **Транслированный порт источника** — порт источника трафика после трансляции сетевых адресов;
- **Транслированный IP-адрес назначения** — IP-адрес назначения трафика после трансляции сетевых адресов;
- **Транслированный порт назначения** — порт назначения трафика после трансляции сетевых адресов;
- **Порт источника** — порт источника трафика;
- **Название устройства** — название устройства, на котором была зафиксирована сессия;
- **Модель устройства** — модель устройства, на котором была зафиксирована сессия;
- **Серийный номер устройства** — серийный номер устройства, на котором была зафиксирована сессия;

— **Название виртуального контекста** — название виртуального контекста, на котором была зафиксирована сессия;

— **Запись получена** — дата и время получения записи модулем журналирования;

— **Идентификатор сессии** — идентификатор сессии, в которой была обнаружена вредоносная или подозрительная активность;

— **Идентификатор правила** — идентификатор сработавшего правила безопасности;

— **MAC-адрес источника** — MAC-адрес источника трафика;

— **MAC-адрес назначения** — MAC-адрес назначения трафика;

— **X-Forwarded-For IP** — значение заголовка X-Forwarded-For.

Параметры записей журнала антивируса

— **Время создания записи** — дата и время создания записи;

— **Действие** — действие, выполненное в отношении трафика;

— **Идент. ВПО** — идентификатор вредоносного программного обеспечения;

— **Имя файла** — название зараженного файла;

— **Зона источника** — зона безопасности источника трафика;

— **Адрес источника** — IP-адрес источника трафика;

— **Пользователь (источник)** — учетная запись Active Directory источника трафика;

— **Зона назначения** — зона безопасности назначения трафика;

— **Адрес назначения** — IP-адрес назначения трафика;

— **Протокол IP**;

— **Порт назначения** — порт назначения трафика;

— **Приложение** — протокол прикладного уровня или приложение, которые были определены в трафике;

— **URL** — URL-адрес, к которому происходит обращение;

— **URL-категории** — список категорий сервера из запроса клиента;

— **Правило безопасности** — правило, в соответствии с которым была разрешена сессия;

— **Страна источника** — страна источника трафика;

— **Регион источника** — регион источника трафика;

— **Входящий интерфейс** — физический интерфейс, с которого пакет вошел в межсетевой экран;

— **Страна назначения** — страна назначения трафика;

— **Регион назначения** — регион назначения трафика;

- **Исходящий интерфейс** — физический интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;
- **Пользователь (назначение)** — учетная запись Active Directory назначения трафика;
- **Порт источника** — порт источника трафика;
- **Идентификатор сессии** — идентификатор сессии, в которой был обнаружен зараженный файл;
- **Запись получена** — дата и время получения записи модулем журналирования;
- **Название устройства** — название устройства, на котором была зафиксирована сессия;
- **Модель устройства** — модель устройства, на котором была зафиксирована сессия;
- **Серийный номер устройства** — серийный номер устройства, на котором была зафиксирована сессия;
- **Название виртуального контекста** — название виртуального контекста, на котором была зафиксирована сессия;
- **Идентификатор правила** — идентификатор сработавшего правила безопасности;
- **Версия антивируса** — версия антивирусной программы;
- **Хеш-сумма** — контрольная сумма заблокированного файла;
- **Алгоритм хеширования** — алгоритм контрольной суммы (например, SHA-1, SHA-256);
- **Транслированный IP-адрес источника** — IP-адрес источника трафика после трансляции сетевых адресов;
- **Транслированный порт источника** — порт источника трафика после трансляции сетевых адресов;
- **Транслированный IP-адрес назначения** — IP-адрес назначения трафика после трансляции сетевых адресов;
- **Транслированный порт назначения** — порт назначения трафика после трансляции сетевых адресов;
- **MAC-адрес источника** — MAC-адрес источника трафика;
- **MAC-адрес назначения** — MAC-адрес назначения трафика;
- **X-forwarded-For IP** — значение заголовка X-Forwarded-For.

Параметры записей журнала политики аутентификации

- **Время создания записи** — дата и время создания записи;
- **Действие** — действие, выполненное над трафиком;
- **Зона источника** — зона безопасности источника трафика;
- **Адрес источника** — IP-адрес источника трафика;

— **Зона назначения** — зона безопасности назначения трафика;

— **Адрес назначения** — IP-адрес назначения трафика;

— **Протокол IP**;

— **Порт назначения** — порт назначения трафика;

— **Приложение** — протокол прикладного уровня или приложение, которые были определены в трафике;

— **Правило аутентификации** — название сработавшего правила аутентификации;

— **Страна источника** — страна источника трафика;

— **Регион источника** — регион источника трафика;

— **Входящий интерфейс** — физический интерфейс, с которого пакет вошел в межсетевой экран;

— **Страна назначения** — страна назначения трафика;

— **Регион назначения** — регион назначения трафика;

— **Исходящий интерфейс** — физический интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;

— **Название устройства** — название устройства, на котором была зафиксирована сессия;

— **Модель устройства** — модель устройства, на котором была зафиксирована сессия;

— **Серийный номер устройства** — серийный номер устройства, на котором была зафиксирована сессия;

— **Название виртуального контекста** — название виртуального контекста, на котором была зафиксирована сессия;

— **Транслированный IP-адрес источника** — IP-адрес источника трафика после трансляции сетевых адресов;

— **Транслированный IP-адрес назначения** — IP-адрес назначения трафика после трансляции сетевых адресов;

— **Транслированный порт источника** — порт источника трафика после трансляции сетевых адресов;

— **Транслированный порт назначения** — порт назначения трафика после трансляции сетевых адресов;

— **MAC-адрес источника** — MAC-адрес источника трафика;

— **MAC-адрес назначения** — MAC-адрес назначения трафика;

— **Порт источника** — порт источника трафика;

— **Идентификатор сессии** — идентификатор сессии, сгенерированный межсетевым экраном;

— **Запись получена** — дата и время получения записи модулем журналирования;

— **X-Forwarded-For IP** — значение заголовка X-Forwarded-For.

Параметры записей журнала ICAP

— **Время создания записи** — дата и время создания записи.

— **Действие** — действие, выполненное над трафиком:

- **Разрешить** (**Pass**) — HTTP-сообщение было разрешено и передано далее получателю.
- **Разрешить-внимание** (**Pass-warning**). Отображается, когда:

  — Включен режим **Мониторинг**, HTTP-сообщение было разрешено и передано далее получателю, однако от ICAP-сервера поступил вердикт о необходимости блокировки сообщения.

  — Включен режим **Мониторинг**, HTTP-сообщение было разрешено и передано далее получателю, однако не удалось переслать сообщение на проверку ICAP-серверу из-за ошибки. Причина ошибки будет указана в поле **Описание ошибки**.

  — Включен стандартный режим, HTTP-сообщение было разрешено и передано далее получателю, однако не удалось переслать сообщение на проверку ICAP-серверу из-за ошибки и в параметре **Действие при ошибке** ICAP-профиля указано действие **Пропустить**. Причина ошибки будет указана в поле **Описание ошибки**.
- **Блокировать** (**Block**) — межсетевой экран заблокировал передачу контента получателю в результате получения любого ответа ICAP-сервера, отличного от ответа с кодом 204 "No Content", или в связи с ошибкой связи с ICAP-сервером, если в параметре **Действие при ошибке** ICAP-профиля указано действие **Блокировать**.

— **Категория контента** — категория, к которой относится файл из HTTP-сообщения (например, «Архивы» или «Документы»).

— **Тип контента** — тип, к которому относится файл из HTTP-сообщения (например, 7z или pdf).

— **Имя файла** — имя, которое имеет файл из HTTP-сообщения.

— **URI ICAP-сервера** — URI, использованный для передачи HTTP-сообщения на ICAP-сервер.

— **Описание ошибки** — причина, по которой не удалось передать HTTP-сообщение на ICAP-сервер.

— **Зона источника** — зона безопасности источника трафика.

— **Адрес источника** — IP-адрес источника трафика.

— **Пользователь (источник)** — учетная запись Active Directory источника трафика.

— **Зона назначения** — зона безопасности назначения трафика.

— **Адрес назначения** — IP-адрес назначения трафика.

- **Протокол IP** - имя IP-протокола, например, TCP (protocol 6), UDP (protocol 17), ICMP (protocol 1).
- **Порт назначения** — порт назначения трафика.
- **Приложение** — протокол прикладного уровня или приложение, которые были определены в трафике.
- **URL** — URL-адрес, к которому происходит обращение.
- **Категории URL** — список категорий сервера из запроса клиента.
- **Правило безопасности** — название сработавшего правила безопасности.
- **Страна источника** — страна источника трафика.
- **Регион источника** — регион источника трафика.
- **Страна назначения** — страна назначения трафика.
- **Регион назначения** — регион назначения трафика.
- **Входящий интерфейс** — физический интерфейс, с которого пакет вошел в межсетевой экран.
- **Исходящий интерфейс** — физический интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла.
- **Транслированный IP-адрес источника** — IP-адрес источника трафика после трансляции сетевых адресов.
- **Транслированный порт источника** — порт источника трафика после трансляции сетевых адресов.
- **Транслированный IP-адрес назначения** — IP-адрес назначения трафика после трансляции сетевых адресов.
- **Транслированный порт назначения** — порт назначения трафика после трансляции сетевых адресов.
- **Правило трансляции** — NAT-правило, в соответствии с которым была выполнена трансляция.
- **Порт источника** — порт источника трафика.
- **Название устройства** — название устройства, на котором была зафиксирована сессия.
- **Модель устройства** — модель устройства, на котором была зафиксирована сессия.
- **Серийный номер устройства** — серийный номер устройства, на котором была зафиксирована сессия.
- **Название виртуального контекста** — название виртуального контекста, на котором была зафиксирована сессия.
- **X-Forwarded-For IP** — значение HTTP-заголовка X-Forwarded-For.

— **Идентификатор сессии** — идентификатор сессии, сгенерированный межсетевым экраном.

— **MAC-адрес источника** — MAC-адрес источника трафика.

— **MAC-адрес назначения** — MAC-адрес назначения трафика.

— **Запись получена** — дата и время получения записи модулем журналирования.

— **Пользователь (назначение)** — учетная запись Active Directory назначения трафика.

— **Идентификатор правила** — идентификатор сработавшего правила безопасности.

Параметры записей журнала IPsec

В журнале **IPsec** фиксируются изменения состояния IPsec-соединений — успешная установка соединения, разрыв соединения, возникновение ошибки на этапе согласования параметров или на этапе согласования селекторов трафика. Параметры записей журнала **IPsec** включают:

— **Время создания записи** — дата и время создания записи;

— **Название туннеля** — название IPsec-соединения;

— **Название устройства** — название устройства, к которому относится IPsec-соединение;

— **Модель устройства** — модель устройства, к которому относится IPsec-соединение;

— **Серийный номер устройства** — серийный номер устройства, к которому относится IPsec-соединение;

— **Название виртуального контекста** — название виртуального контекста IPsec-соединения;

— **Описание** — описание возникшей ошибки;

— **Событие** — журналируемое событие;

— **Локальный адрес** — локальный IP-адрес;

— **Удаленный адрес** — IP-адрес пира;

— **IKE SA** — набор согласованных параметров IKE:

- **IKEv2 локальный SPI** — идентификатор входящего SA для IKE;
- **IKEv2 удаленный SPI** — идентификатор исходящего SA для IKE;
- **IKEv2 локальный адрес** — локальный адрес для IKE;
- **IKEv2 удаленный адрес** — удаленный адрес для IKE;
- **IKEv2 шифрование** — согласованный алгоритм шифрования для IKE;
- **IKEv2 аутентификация** — согласованный алгоритм аутентификации для IKE;
- **IKEv2 обмен ключами** — согласованный алгоритм обмена ключами для IKE;
- **IKEv2 key lifetime** — ограничение времени жизни ключей для IKE.

— **IPsec SA** — набор согласованных параметров IPsec:
  - **IPsec локальный SPI** — идентификатор входящего SA для IPsec;
  - **IPsec удаленный SPI** — идентификатор исходящего SA для IPsec;
  - **IPsec локальный адрес** — локальный адрес для IPsec;
  - **IPsec удаленный адрес** — удаленный адрес для IPsec;
  - **IPsec шифрование** — согласованный алгоритм для шифрования трафика в туннеле;
  - **IPsec аутентификация** — согласованный алгоритм для аутентификации в туннеле;
  - **IPsec key lifetime** — согласованное ограничение времени жизни сессии;
  - **IPsec key lifesize (kb)** — согласованное ограничение сессии по объему данных;
  - **Локальные трафик-селекторы** — согласованные локальные селекторы трафика;
  - **Удаленные трафик-селекторы** — согласованные удаленные селекторы трафика.
— **Отправленные** — отправленные наборы параметров IKE или IPsec для согласования:
  - **Шифрование** — алгоритм или набор алгоритмов шифрования, отправленный в составе proposal;
  - **Аутентификация** — алгоритм или набор алгоритмов аутентификации, отправленный в составе proposal;
  - **Обмен ключами** — алгоритм или набор алгоритмов обмена ключами, отправленный в составе proposal.
— **Полученные** — полученные наборы параметров IKE или IPsec для согласования:
  - **Шифрование** — алгоритм или набор алгоритмов шифрования, полученный в составе proposal;
  - **Аутентификация** — алгоритм или набор алгоритмов аутентификации, полученный в составе proposal;
  - **Обмен ключами** — алгоритм или набор алгоритмов обмена ключами, полученный в составе proposal;
  - **Псевдослучайное число** — псевдослучайная функция, используемая для генерации сессионных ключей;
  - **ESN** — расширенный порядковый номер IPsec.

— **Отправленные селекторы** — отправленные трафик-селекторы:
  - **Отправленные локальные трафик селекторы** — отправленный набор локальных трафик-селекторов;
  - **Отправленные удаленные трафик селекторы** — отправленный набор удаленных трафик-селекторов.
— **Полученные селекторы** — полученные трафик-селекторы:
  - **Полученные локальные трафик селекторы** — полученный набор локальных трафик-селекторов;
  - **Полученные удаленные трафик селекторы** — полученный набор удаленных трафик-селекторов;
  - **Диапазон портов** — диапазон портов для трафик селектора;
  - **IP-протокол**.

Параметры записей журнала удаленного доступа

Параметры записей журнала удаленного доступа включают:

— **Время создания записи** — дата и время создания записи;

— **Событие** — событие изменения состояния соединения с клиентом;

— **Описание события** — причина разрыва соединения или ошибки установки соединения;

— **Туннель** — название туннеля;

— **Виртуальный контекст** — название виртуального контекста, к которому относится туннель;

— **Устройство** — название устройства, к которому относится туннель;

— **Адрес шлюза** — IP-адрес шлюза, через который фактически установилось соединение с клиентом;

— **Внешний IP-адрес клиента** — публичный IP-адрес источника, устанавливающего соединение;

— **Выделенный адрес** — выданный при установке туннеля клиенту адрес;

— **Страна источника** — страна IP-адреса клиента;

— **Логин** — учетная запись пользователя;

— **Тип аутентификации** — способ аутентификации.

Возможные причины разрыва соединения:

- **Сессия завершена. Превышено максимальное время подключения.** Сессия разорвана шлюзом из-за достижения максимального времени сессии.
- **Сессия завершена. Превышен максимальный период бездействия.** Сессия разорвана шлюзом из-за достижения максимального периода бездействия.
- **VPN шлюз переконфигурирован.** Сессия разорвана шлюзом из-за изменения параметров, которое вынужденно привело к сбросу соединения, или из-за отключения туннеля.
- **Отключение VPN-клиента.** VPN-клиент самостоятельно отключился.
- **Учетная запись отключена.** Отключение пользовательской учетной записи.

Возможные причины ошибки установки соединения:

- **Ошибка в IPsec. Общий сбой.** Внутренняя ошибка в протоколе IPsec.
- **Ошибка в IPsec. Некорректное IKE-сообщение**.
- **Ошибка в IPsec. Не выбраны IKE-параметры**.
- **Ошибка в IPsec. Не выбраны IPsec-параметры**.
- **Ошибка в IPsec. Неверная IKE-версия**.
- **Ошибка в IPsec. Тайм-аут в IKE**.
- **Ошибка аутентификации. Неудача.** Получение от сервера аутентификации неуспеха на ранее отправленный запрос аутентификации.
- **Ошибка аутентификации. Тайм-аут соединения с сервером аутентификации.** Сервер аутентификации не ответил на запрос за отведенное время.
- **Ошибка аутентификации. Нет свободных IP-адресов из IP-пула.** Все доступные адреса из IP-пула выделены для других подключений.
- **Ошибка аутентификации. Неверный сертификат VPN-клиента.** Ошибка клиентского сертификата.
- **Ошибка аутентификации. Ошибка в сертификате шлюза**.

Параметры записей журнала аудита

- **Время создания записи** — дата и время попытки выполнить действие;
- **Идент. администратора** — идентификатор администратора, совершившего попытку;
- **Логин** — логин администратора, совершившего попытку;
- **Адрес источника** — IP-адрес источника запроса (администратора);
- **Действие** — действие, которое попытались выполнить;

— **Результат** — результат попытки выполнить действие;

— **Параметры действия** — параметры действия, которое попытались выполнить.

Параметры записей журнала аутентификации

— **Время создания записи** — дата и время попытки входа или выхода в систему управления;

— **Роль администратора** — роль учетной записи администратора;

— **Идент. администратора** — идентификатор учетной записи администратора;

— **Логин администратора** — логин администратора;

— **Действие** — действие, которое попытались выполнить (вход или выход в систему);

— **Адрес источника** — IP-адрес источника запроса (администратора);

— **Результат** — результат действия (успех или неуспех).

— **Отправленные** — отправленные наборы параметров IKE или IPsec для согласования:

39.6. Параметры syslog-сообщений

Syslog-сообщения типа «Трафик»

— `srcUser` — учетная запись Active Directory источника трафика;

— `dstUser` — учетная запись Active Directory назначения трафика;

— `outIfaceName` — сетевой интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;

— `inIfaceName` — сетевой интерфейс, с которого пакет вошел в межсетевой экран;

— `ipProtocol` — название IP-протокола, например TCP (protocol 6) или UDP (protocol 17);

— `app` — протокол прикладного уровня или приложение, которые были определены в трафике;

— `sessionEndReason` — причина завершения сессии, например по тайм-ауту;

— `srcCountry` — страна источника трафика;

— `dstCountry` — страна назначения трафика;

— `srcRegion` — регион источника трафика;

— `dstRegion` — регион назначения трафика;

— `natRuleName` — название правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;

— `srcZoneName` — зона безопасности источника трафика;

— `srcMacAddr` — MAC-адрес источника трафика;

- `dstMacAddr` — MAC-адрес назначения трафика;
- `dstZoneName` — зона безопасности назначения трафика;
- `url` — URL, к которому происходит обращение;
- `fileName` — имя файла из запроса клиента или ответа сервера;
- `natSrcPort` — порт источника трафика после трансляции сетевых адресов;
- `natDstPort` — порт назначения трафика после трансляции сетевых адресов;
- `sessionId` — идентификатор сессии, сгенерированный межсетевым экраном;
- `srcPort` — порт источника трафика;
- `dstPort` — порт назначения трафика;
- `inIfaceId` — идентификатор входящего интерфейса;
- `outIfaceId` — идентификатор исходящего интерфейса;
- `natRuleId` — идентификатор правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;
- `srcZoneId` — идентификатор зоны безопасности источника трафика;
- `dstZoneId` — идентификатор зоны безопасности назначения трафика;
- `srcAddr` — IP-адрес источника трафика;
- `dstAddr` — IP-адрес назначения трафика;
- `natSrcAddr` — IP-адрес источника трафика после трансляции сетевых адресов;
- `natDstAddr` — IP-адрес назначения трафика после трансляции сетевых адресов;
- `xForwardedFor` — значение HTTP-заголовка X-Forwarded-For;
- `timeGen` — дата и время создания записи;
- `timeArrived` — дата и время получения записи модулем журналирования;
- `sessionEnd` — дата и время завершения сессии;
- `sessionFirstPacketTime` — дата и время получения первого пакета сессии;
- `sessionStart` — дата и время начала сессии;
- `type` — тип syslog-сообщения;
- `contextName` — название виртуального контекста, на котором была зафиксирована сессия;
- `deviceName` — название устройства, на котором была зафиксирована сессия;
- `deviceSerial` — серийный номер устройства, на котором была зафиксирована сессия;
- `deviceModel` — модель устройства, на котором была зафиксирована сессия;
- `securityRuleName` — название сработавшего правила безопасности;

— `pbrRuleName` — название сработавшего правила PBR;

— `action` — действие, выполненное над трафиком, например разрешение прохождения;

— `bytesRecv` — число байтов, полученных в рамках сессии;

— `bytesSent` — число байтов, отправленных в рамках сессии;

— `packetsRecv` — число пакетов, полученных в рамках сессии;

— `packetsSent` — число пакетов, отправленных в рамках сессии;

— `sessionDuration` — длительность сессии в секундах;

— `deviceId` — идентификатор устройства, на котором была зафиксирована сессия;

— `contextId` — идентификатор виртуального контекста, на котором была зафиксирована сессия;

— `securityRuleId` — идентификатор сработавшего правила безопасности;

— `pbrRuleId` — идентификатор сработавшего правила PBR;

— `urlCategoriesId` — идентификаторы категорий URL;

— `urlCategories` — список категорий сервера из запроса клиента;

— `decrypted` — `true`, если трафик был расшифрован.

Syslog-сообщения типа «Расшифрование»

— `srcUser` — учетная запись Active Directory источника трафика;

— `dstUser` — учетная запись Active Directory назначения трафика;

— `outIfaceName` — сетевой интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;

— `inIfaceName` — сетевой интерфейс, с которого пакет вошел в межсетевой экран;

— `ipProtocol` — название IP-протокола, например TCP (protocol 6) или UDP (protocol 17);

— `app` — протокол прикладного уровня или приложение, которые были определены в трафике;

— `srcCountry` — страна источника трафика;

— `dstCountry` — страна назначения трафика;

— `srcRegion` — регион источника трафика;

— `dstRegion` — регион назначения трафика;

— `natRuleName` — название правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;

— `srcZoneName` — зона безопасности источника трафика;

— `srcMacAddr` — MAC-адрес источника трафика;

- `dstMacAddr` — MAC-адрес назначения трафика;
- `dstZoneName` — зона безопасности назначения трафика;
- `url` — URL-адрес, URL, к которому происходит обращение;
- `fileName` — имя файла из запроса клиента или ответа сервера;
- `natSrcPort` — порт источника трафика после трансляции сетевых адресов;
- `natDstPort` — порт назначения трафика после трансляции сетевых адресов;
- `sessionId` — идентификатор сессии, сгенерированный межсетевым экраном;
- `srcPort` — порт источника трафика;
- `dstPort` — порт назначения трафика;
- `inIfaceId` — идентификатор входящего интерфейса;
- `outIfaceId` — идентификатор исходящего интерфейса;
- `natRuleId` — идентификатор правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;
- `srcZoneId` — идентификатор зоны безопасности источника трафика;
- `dstZoneId` — идентификатор зоны безопасности назначения трафика;
- `srcAddr` — IP-адрес источника трафика;
- `dstAddr` — IP-адрес назначения трафика;
- `natSrcAddr` — IP-адрес источника трафика после трансляции сетевых адресов;
- `natDstAddr` — IP-адрес назначения трафика после трансляции сетевых адресов;
- `xForwardedFor` — значение HTTP-заголовка X-Forwarded-For;
- `timeGen` — дата и время создания записи;
- `timeArrived` — дата и время получения записи модулем журналирования;
- `certStart` — начало действия сертификата;
- `certEnd` — дата истечения сертификата;
- `certCn` — общее имя субъекта;
- `certFingerprint` — отпечаток сертификата;
- `certIssuerCn` — общее имя издателя;
- `certRootCn` — общее имя корневого ЦС;
- `certSni` — SNI;
- `contextName` — название виртуального контекста, на котором была зафиксирована сессия;
- `decryptionRule` — название сработавшего правила расшифрования;

— `deviceModel` — модель устройства, на котором была зафиксирована сессия;

— `deviceName` — название устройства, на котором была зафиксирована сессия;

— `deviceSerial` — серийный номер устройства, на котором была зафиксирована сессия;

— `rootCertStatus` — статус корневого сертификата;

— `chainStatus` — состояние цепочки сертификатов;

— `tlsAuthAlg` — алгоритм создания хеша, используемый в сессии, например SHA или SHA-256;

— `tlsEncryption` — алгоритм, используемый для шифрования данных сессии, например AES-128-CBC;

— `tlsHandshakeStageC2f` — этап образования TLS-соединения между клиентом и межсетевым экраном;

— `tlsHandshakeStageF2s` — этап образования TLS-соединения между сервером и межсетевым экраном;

— `tlsKeyExchange` — алгоритм обмена ключами, используемый в сессии, например RSA или DHE;

— `tlsVersion` — версия TLS-протокола, используемая в сессии, например TLS 1.2 или TLS 1.3;

— `tlsParamError` — ошибка расшифрования;

— `certAlternativeNames` — альтернативные имена субъекта сертификата;

— `action` — действие, выполненное над трафиком;

— `type` — тип syslog-сообщения;

— `bytesRecv` — число байтов, полученных в рамках сессии;

— `bytesSent` — число байтов, отправленных в рамках сессии;

— `packetsRecv` — число пакетов, полученных в рамках сессии;

— `packetsSent` — число пакетов, отправленных в рамках сессии;

— `certSerial` — серийный номер сертификата;

— `certVer` — версия сертификата;

— `contextId` — идентификатор виртуального контекста, на котором была зафиксирована сессия;

— `deviceId` — идентификатор устройства, на котором была зафиксирована сессия;

— `decryptionRuleId` — идентификатор сработавшего правила расшифрования;

— `urlCategories` — список категорий сервера из запроса клиента;

— `urlCategoriesId` — идентификаторы категорий URL;

— `decrypted` — `true`, если трафик был расшифрован.

Syslog-сообщения типа «IPS»

— `srcUser` — учетная запись Active Directory источника трафика;

— `dstUser` — учетная запись Active Directory назначения трафика;

— `outIfaceName` — сетевой интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;

— `inIfaceName` — сетевой интерфейс, с которого пакет вошел в межсетевой экран;

— `ipProtocol` — название IP-протокола, например TCP (protocol 6) или UDP (protocol 17);

— `app` — протокол прикладного уровня или приложение, которые были определены в трафике;

— `srcCountry` — страна источника трафика;

— `dstCountry` — страна назначения трафика;

— `srcRegion` — регион источника трафика;

— `dstRegion` — регион назначения трафика;

— `natRuleName` — название правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;

— `srcZoneName` — зона безопасности источника трафика;

— `srcMacAddr` — MAC-адрес источника трафика;

— `dstMacAddr` — MAC-адрес назначения трафика;

— `dstZoneName` — зона безопасности назначения трафика;

— `url` — URL, к которому происходит обращение;

— `fileName` — имя файла из запроса клиента или ответа сервера;

— `natSrcPort` — порт источника трафика после трансляции сетевых адресов;

— `natDstPort` — порт назначения трафика после трансляции сетевых адресов;

— `sessionId` — идентификатор сессии, в которой была обнаружена вредоносная или подозрительная активность;

— `srcPort` — порт источника трафика;

— `dstPort` — порт назначения трафика;

— `inIfaceId` — идентификатор входящего интерфейса;

— `outIfaceId` — идентификатор исходящего интерфейса;

— `natRuleId` — идентификатор правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;

— `srcZoneId` — идентификатор зоны безопасности источника трафика;

— `dstZoneId` — идентификатор зоны безопасности назначения трафика;

— `srcAddr` — IP-адрес источника трафика;

— `dstAddr` — IP-адрес назначения трафика;

— `natSrcAddr` — IP-адрес источника трафика после трансляции сетевых адресов;

— `natDstAddr` — IP-адрес назначения трафика после трансляции сетевых адресов;

— `xForwardedFor` — значение HTTP-заголовка X-Forwarded-For;

— `timeGen` — дата и время создания записи;

— `timeArrived` — дата и время получения записи модулем журналирования;

— `type` — тип syslog-сообщения;

— `contextName` — название виртуального контекста, на котором была зафиксирована сессия;

— `deviceName` — название устройства, на котором была зафиксирована сессия;

— `deviceSerial` — серийный номер устройства, на котором была зафиксирована сессия;

— `deviceModel` — модель устройства, на котором была зафиксирована сессия;

— `securityRuleName` — название сработавшего правила безопасности;

— `cve` — CVE-идентификатор уязвимости;

— `threatCategory` — категория вредоносной активности;

— `threatName` — название сигнатуры, которой соответствует обнаруженная активность;

— `threatSeverity` — степень опасности вредоносной активности;

— `action` — действие, выполненное в отношении сессии;

— `signatureId` — идентификатор сигнатуры;

— `contextId` — идентификатор виртуального контекста, на котором была зафиксирована сессия;

— `deviceId` — идентификатор устройства, на котором была зафиксирована сессия;

— `securityRuleId` — идентификатор сработавшего правила безопасности.

Syslog-сообщения типа «Антивирус»

— `srcUser` — учетная запись Active Directory источника трафика;

— `dstUser` — учетная запись Active Directory назначения трафика;

— `outIfaceName` — сетевой интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;

— `inIfaceName` — сетевой интерфейс, с которого пакет вошел в межсетевой экран;

— `ipProtocol` — название IP-протокола, например TCP (protocol 6) или UDP (protocol 17);

— `app` — протокол прикладного уровня или приложение, которые были определены в трафике;

- `srcCountry` — страна источника трафика;
- `dstCountry` — страна назначения трафика;
- `srcRegion` — регион источника трафика;
- `dstRegion` — регион назначения трафика;
- `natRuleName` — название правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;
- `srcZoneName` — зона безопасности источника трафика;
- `srcMacAddr` — MAC-адрес источника трафика;
- `dstMacAddr` — MAC-адрес назначения трафика;
- `dstZoneName` — зона безопасности назначения трафика;
- `url` — URL-адрес, к которому происходит обращение;
- `fileName` — название зараженного файла;
- `natSrcPort` — порт источника трафика после трансляции сетевых адресов;
- `natDstPort` — порт назначения трафика после трансляции сетевых адресов;
- `sessionId` — идентификатор сессии, в которой был обнаружен зараженный файл;
- `srcPort` — порт источника трафика;
- `dstPort` — порт назначения трафика;
- `inIfaceId` — идентификатор входящего интерфейса;
- `outIfaceId` — идентификатор исходящего интерфейса;
- `natRuleId` — идентификатор правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;
- `srcZoneId` — идентификатор зоны безопасности источника трафика;
- `dstZoneId` — идентификатор зоны безопасности назначения трафика;
- `srcAddr` — IP-адрес источника трафика;
- `dstAddr` — IP-адрес назначения трафика;
- `natSrcAddr` — IP-адрес источника трафика после трансляции сетевых адресов;
- `natDstAddr` — IP-адрес назначения трафика после трансляции сетевых адресов;
- `xForwardedFor` — значение HTTP-заголовка X-Forwarded-For;
- `timeGen` — дата и время создания записи;
- `timeArrived` — дата и время получения записи модулем журналирования;
- `type` — тип syslog-сообщения;

- `action` — действие, выполненное в отношении трафика;
- `malwareId` — идентификатор вредоносного программного обеспечения;
- `contextName` — название виртуального контекста, на котором была зафиксирована сессия;
- `deviceModel` — модель устройства, на котором была зафиксирована сессия;
- `deviceName` — название устройства, на котором была зафиксирована сессия;
- `deviceSerial` — серийный номер устройства, на котором была зафиксирована сессия;
- `securityRuleName` — правило, в соответствии с которым была разрешена сессия;
- `antivirusCheckSum` — контрольная сумма заблокированного файла;
- `antivirusCheckSumAlgorithm` — алгоритм контрольной суммы (например, SHA-1, SHA-256);
- `antivirusVersion` — версия антивирусной программы;
- `threatName` — название вредоносного программного обеспечения;
- `contextId` — идентификатор виртуального контекста, на котором была зафиксирована сессия;
- `deviceId` — идентификатор устройства, на котором была зафиксирована сессия;
- `securityRuleId` — идентификатор сработавшего правила безопасности.

Syslog-сообщения типа «Политика аутентификации»

- `deviceId` — идентификатор устройства, на котором была зафиксирована сессия;
- `deviceName` — название устройства, на котором была зафиксирована сессия;
- `deviceSerial` — серийный номер устройства, на котором была зафиксирована сессия;
- `contextId` — идентификатор виртуального контекста, на котором была зафиксирована сессия;
- `contextName` — название виртуального контекста, на котором была зафиксирована сессия;
- `entryReceived` — дата и время получения записи модулем журналирования;
- `entryGeneration` — дата и время создания записи;
- `srcMacAddr` — MAC-адрес источника трафика;
- `dstMacAddr` — MAC-адрес назначения трафика;
- `srcAddr` — IP-адрес источника трафика;
- `dstAddr` — IP-адрес назначения трафика;
- `xForwardedFor` — значение HTTP-заголовка X-Forwarded-For;
- `srcPort` — порт источника трафика;

- `dstPort` — порт назначения трафика;
- `natSrcAddr` — IP-адрес источника трафика после трансляции сетевых адресов;
- `natDstAddr` — IP-адрес назначения трафика после трансляции сетевых адресов;
- `natSrcPort` — порт источника трафика после трансляции сетевых адресов;
- `natDstPort` — порт назначения трафика после трансляции сетевых адресов;
- `natRuleId` — идентификатор правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;
- `natRule` — название правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов;
- `srcCountry` — страна источника трафика;
- `dstCountry` — страна назначения трафика;
- `srcRegion` — регион источника трафика;
- `dstRegion` — регион назначения трафика;
- `inIfaceId` — идентификатор входящего интерфейса;
- `inIfaceName` — сетевой интерфейс, с которого пакет вошел в межсетевой экран;
- `outIfaceId` — идентификатор исходящего интерфейса;
- `outIfaceName` — сетевой интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла;
- `srcZoneId` — идентификатор зоны безопасности источника трафика;
- `srcZoneName` — зона безопасности источника трафика;
- `dstZoneId` — идентификатор зоны безопасности назначения трафика;
- `dstZoneName` — зона безопасности назначения трафика;
- `ipProtocol` — название IP-протокола, например TCP (protocol 6) или UDP (protocol 17);
- `app` — протокол прикладного уровня или приложение, которые были определены в трафике;
- `sessionId` — идентификатор сессии, сгенерированный межсетевым экраном;
- `action` — действие, выполненное над трафиком;
- `authRuleId` — идентификатор сработавшего правила аутентификации;
- `authRuleName` — название сработавшего правила аутентификации;
- `deviceModel` — модель устройства, на котором была зафиксирована сессия.

Syslog-сообщения типа «ICAP»

— `srcUser` — учетная запись Active Directory источника трафика.

— `dstUser` — учетная запись Active Directory назначения трафика.

— `outIfaceName` — сетевой интерфейс, через который пакет должен быть отправлен, чтобы достичь следующего узла.

— `inIfaceName` — сетевой интерфейс, с которого пакет вошел в межсетевой экран.

— `ipProtocol` — название IP-протокола, например TCP (protocol 6) или UDP (protocol 17).

— `app` — протокол прикладного уровня или приложение, которые были определены в трафике.

— `srcCountry` — страна источника трафика.

— `dstCountry` — страна назначения трафика.

— `srcRegion` — регион источника трафика.

— `dstRegion` — регион назначения трафика.

— `natRuleName` — NAT-правило, в соответствии с которым была выполнена трансляция.

— `srcZoneName` — зона безопасности источника трафика.

— `srcMacAddr` — MAC-адрес источника трафика.

— `dstMacAddr` — MAC-адрес назначения трафика.

— `dstZoneName` — зона безопасности назначения трафика.

— `url` — URL-адрес, к которому происходит обращение.

— `fileName` — имя, которое имеет файл из HTTP-сообщения.

— `natSrcPort` — порт источника трафика после трансляции сетевых адресов.

— `natDstPort` — порт назначения трафика после трансляции сетевых адресов.

— `sessionId` — идентификатор сессии, сгенерированный межсетевым экраном.

— `srcPort` — порт источника трафика.

— `dstPort` — порт назначения трафика.

— `inIfaceId` — идентификатор входящего интерфейса.

— `outIfaceId` — идентификатор исходящего интерфейса.

— `natRuleId` — идентификатор правила NAT, в соответствии с которым была выполнена трансляция сетевых адресов.

— `srcZoneId` — идентификатор зоны безопасности источника трафика.

— `dstZoneId` — идентификатор зоны безопасности назначения трафика.

— `srcAddr` — IP-адрес источника трафика.

— `dstAddr` — IP-адрес назначения трафика.

— `natSrcAddr` — IP-адрес источника трафика после трансляции сетевых адресов.

— `natDstAddr` — IP-адрес назначения трафика после трансляции сетевых адресов.

— `xForwardedFor` — значение HTTP-заголовка X-Forwarded-For.

— `timeGen` — дата и время создания записи.

— `timeArrived` — дата и время получения записи модулем журналирования.

— `contentCategory` — категория, к которой относится файл из HTTP-сообщения (например, «Архивы» или «Документы»).

— `contentType` — тип, к которому относится файл из HTTP-сообщения (например, 7z или pdf).

— `contextName` — название виртуального контекста, на котором была зафиксирована сессия.

— `deviceName` — название устройства, на котором была зафиксирована сессия.

— `deviceModel` — модель устройства, на котором была зафиксирована сессия.

— `deviceSerial` — серийный номер устройства, на котором была зафиксирована сессия.

— `error` — причина, по которой не удалось передать HTTP-сообщение на ICAP-сервер.

— `icapServerURI` — URI, использованный для передачи HTTP-сообщения на ICAP-сервер.

— `securityRuleName` — название сработавшего правила безопасности.

— `action` — действие, выполненное над трафиком:

- `pass` — HTTP-сообщение было разрешено и передано далее получателю.
- `passWarning`. Отображается, когда:

  — Включен режим **Мониторинг**, HTTP-сообщение было разрешено и передано далее получателю, однако от ICAP-сервера поступил вердикт о необходимости блокировки сообщения.

  — Включен режим **Мониторинг**, HTTP-сообщение было разрешено и передано далее получателю, однако не удалось переслать сообщение на проверку ICAP-серверу из-за ошибки. Причина ошибка указана в поле `error`.

  — Включен стандартный режим, HTTP-сообщение было разрешено и передано далее получателю, однако не удалось переслать сообщение на проверку ICAP-серверу из-за ошибки и в параметре **Действие при ошибке** ICAP-профиля указано действие **Пропустить**. Причина ошибка будет указана в поле `error`.
- `block` — межсетевой экран заблокировал передачу контента получателю в результате получения любого ответа ICAP-сервера, отличного от ответа с кодом 204 "No Content", или в связи с ошибкой связи с ICAP-сервером, если в параметре **Действие при ошибке** ICAP-профиля указано действие **Блокировать**.

— `type` — тип syslog-сообщения.

— `contextId` — идентификатор виртуального контекста, на котором была зафиксирована сессия.

— `deviceId` — идентификатор устройства, на котором была зафиксирована сессия.

— `securityRuleId` — идентификатор сработавшего правила безопасности.

— `urlCategories` — список категорий сервера из запроса клиента.

Syslog-сообщения типа «IPsec»

— `deviceId` — идентификатор устройства, к которому относится IPsec-соединение;

— `deviceName` — название устройства, к которому относится IPsec-соединение;

— `deviceSerial` — серийный номер устройства, к которому относится IPsec-соединение;

— `contextId` — идентификатор виртуального контекста IPsec-соединения;

— `contextName` — название виртуального контекста IPsec-соединения;

— `entryReceived` — дата и время получения записи модулем журналирования;

— `entryGeneration` — дата и время создания записи;

— `natSrcAddr` — IP-адрес источника трафика после трансляции сетевых адресов;

— `natDstAddr` — IP-адрес назначения трафика после трансляции сетевых адресов;

— `xForwardedFor` — значение HTTP-заголовка X-Forwarded-For;

— `ipsecId` — идентификатор IPsec-соединения;

— `ipsecName` — название IPsec-соединения;

— `ipsecType` — тип IPsec-соединения;

— `ipsecEvent` — журналируемое событие;

— `ipsecError` — описание возникшей ошибки;

— `ipsecLocalAddr` — локальный IP-адрес;

— `ipsecPeerAddr` — IP-адрес пира;

— `ipsecIkeLocalSpi` — идентификатор входящего SA для IKE;

— `ipsecIkePeerSpi` — идентификатор исходящего SA для IKE;

— `ipsecIkeLocalAddr` — локальный адрес для IKE;

— `ipsecIkePeerAddr` — удаленный адрес для IKE;

— `ipsecIkeKeyLifetime` — ограничение времени жизни ключей для IKE;

— `ipsecIke2Encryption` — согласованный алгоритм шифрования для IKE;

— `ipsecIke2Authentication` — согласованный алгоритм аутентификации для IKE;

- `ipsecIke2KeyExchange` — согласованный алгоритм обмена ключами для IKE;
- `ipsecEspSa` — набор согласованных параметров IPsec:
  - `local_spi` — идентификатор входящего SA для IPsec;
  - `peer_spi` — идентификатор исходящего SA для IPsec;
  - `local_addr` — локальный адрес для IPsec;
  - `peer_addr` — удаленный адрес для IPsec;
  - `enc` — согласованный алгоритм для шифрования трафика в туннеле;
  - `auth` — согласованный алгоритм для аутентификации в туннеле;
  - `key_life_time IPsec key lifetime` — согласованное ограничение времени жизни сессии;
  - `key_life_size_kb IPsec key lifesize (kb)` — согласованное ограничение сессии по объему данных;
  - `local_ts` — согласованные локальные селекторы трафика;
  - `remote_ts` — согласованные удаленные селекторы трафика.
- `ipsecSentProposal` — отправленные наборы параметров IKE или IPsec для согласования:
  - `encryption` — алгоритм или набор алгоритмов шифрования, отправленный в составе proposal;
  - `auth` — алгоритм или набор алгоритмов аутентификации, отправленный в составе proposal;
  - `key_exchange` — алгоритм или набор алгоритмов обмена ключами, отправленный в составе proposal.
- `ipsecReceivedProposal` — полученные наборы параметров IKE или IPsec для согласования:
  - `encryption` — алгоритм или набор алгоритмов шифрования, полученный в составе proposal;
  - `authentication` — алгоритм или набор алгоритмов аутентификации, полученный в составе proposal;
  - `key_exchange` — алгоритм или набор алгоритмов обмена ключами, полученный в составе proposal;
  - `pseudo_random` — псевдослучайная функция, используемая для генерации сессионных ключей;
  - `esn ESN` — расширенный порядковый номер IPsec.
- `ipsecSentLocalSelectors` — отправленный набор локальных трафик-селекторов;
- `ipsecSentRemoteSelectors` — отправленный набор удаленных трафик-селекторов;

— `ipsecReceivedLocalSelectors` — полученный набор локальных трафик-селекторов;

— `ipsecReceivedRemoteSelectors` — полученный набор удаленных трафик-селекторов;

— `deviceModel` — модель устройства, к которому относится IPsec-соединение.

Syslog-сообщения типа «Удаленный доступ»

Сообщения типа «Удаленный доступ» содержат следующие поля:

— `deviceId` — идентификатор устройства, к которому относится туннель;

— `deviceName` — название устройства, к которому относится туннель;

— `deviceSerial` — серийный номер устройства, к которому относится туннель;

— `contextId` — идентификатор виртуального контекста, к которому относится туннель;

— `contextName` — название виртуального контекста, к которому относится туннель;

— `entryReceived` — дата и время получения записи модулем журналирования;

— `entryGeneration` — дата и время создания записи;

— `tunnelName` — название туннеля;

— `raEvent` — событие изменения состояния соединения с клиентом:

- `RA_EVENT_UNSPECIFIED` — внутренняя ошибка;
- `RA_EVENT_CONNECTED` — успешная установка соединения;
- `RA_EVENT_DISCONNECTED` — завершение соединения;
- `RA_EVENT_CONNECTION_FAILED` — ошибка соединения.

— `raEventDescription` — причина разрыва соединения или ошибки установки соединения;

— `raGatewayAddress` — IP-адрес шлюза, через который фактически установилось соединение с клиентом;

— `raPeerAddress` — выданный при установке туннеля клиенту адрес;

— `srcUser` — учетная запись пользователя;

— `srcAddr` — публичный IP-адрес источника, устанавливающего соединение;

— `srcCountry` — страна IP-адреса клиента;

— `authMethod` — способ аутентификации.

Возможные причины разрыва соединения:

— `RA_EVENT_DESCRIPTION_SESSION_MAX_CONNECTION_TIME_EXCEEDED` — сессия разорвана шлюзом из-за достижения максимального времени сессии.

— `RA_EVENT_DESCRIPTION_SESSION_MAX_INACTIVITY_PERIOD_REACHED` — сессия разорвана шлюзом из-за достижения максимального периода бездействия.

— RA_EVENT_DESCRIPTION_GATEWAY_RECONFIGURED — сессия разорвана шлюзом из-за изменения параметров, которое вынуждено привело к сбросу соединения, или из-за отключения туннеля.

— RA_EVENT_DESCRIPTION_CLIENT_LOGOUT — клиент самостоятельно отключился.

— RA_EVENT_DESCRIPTION_USER_ACCOUNT_DISABLED — отключение пользовательской учетной записи.

Возможные причины ошибки установки соединения:

— RA_EVENT_DESCRIPTION_UNSPECIFIED — внутренняя ошибка.

— RA_EVENT_DESCRIPTION_IPSEC_GENERIC_ERROR — внутренняя ошибка в протоколе IPsec.

— RA_EVENT_DESCRIPTION_IPSEC_INCORRECT_IKE_MESSAGE — некорректное IKE-сообщение.

— RA_EVENT_DESCRIPTION_IPSEC_NO_IKE_PROPOSAL_CHOSEN — не выбраны IKE-параметры.

— RA_EVENT_DESCRIPTION_IPSEC_NO_IPSEC_PROPOSAL_CHOSEN — не выбраны IPsec-параметры.

— RA_EVENT_DESCRIPTION_IPSEC_WRONG_IKE_VERSION — неверная IKE версия.

— RA_EVENT_DESCRIPTION_IPSEC_IKE_TIMEOUT — тайм-аут в IKE.

— RA_EVENT_DESCRIPTION_AUTH_UNSUCCESS — получение от сервера аутентификации неуспеха на ранее отправленный запрос аутентификации.

— RA_EVENT_DESCRIPTION_AUTH_SERVER_TIMEOUT — сервер аутентификации не ответил на запрос за отведенное время.

— RA_EVENT_DESCRIPTION_AUTH_NO_AVAILABLE_IP_ADDRESSES — все доступные адреса из IP-пула выделены для других подключений.

— RA_EVENT_DESCRIPTION_AUTH_VPN_CLIENT_CERTIFICATE_ERROR — ошибка клиентского сертификата.

— RA_EVENT_DESCRIPTION_AUTH_GATEWAY_CERTIFICATE_ERROR — ошибка в сертификате шлюза.

Syslog-сообщения типа «Аудит»

— adminId — идентификатор администратора, совершившего попытку;

— adminLogin — логин администратора, совершившего попытку;

— generateTime — дата и время попытки выполнить действие;

— sourceAddress — IP-адрес источника запроса (администратора);

— action — действие, которое попытались выполнить;

— queryArgs — параметры действия, которое попытались выполнить;

— result — результат попытки выполнить действие.

Syslog-сообщения типа «Аутентификация»

— `createdAt` — дата и время попытки входа или выхода в систему управления;

— `login` — логин администратора;

— `adminId` — идентификатор учетной записи администратора;

— `roles` — роль учетной записи администратора;

— `action` — действие, которое попытались выполнить (вход или выход в систему);

— `sourceAddress` — IP-адрес источника запроса (администратора);

— `error` — причина неуспеха.

39.7. Причины завершения сессий

Ниже перечислены возможные причины завершения сессии и дается их пояснение:

— **policyDeny** — сессия запрещена правилом безопасности.

— **tcpRstFromClient** — межсетевой экран получил TCP RST от клиента и закрыл сессию.

— **tcpRstFromServer** — межсетевой экран получил TCP RST от сервера и закрыл сессию.

— **tcpFin** — штатное закрытие TCP-сессии.

— **decryptError** — сессия закрыта из-за ошибок расшифрования.

— **decoderError** — сессия закрыта из-за ошибок парсинга.

— **resourceLimit** — сессия закрыта из-за нехватки ресурсов.

— **agedOut** — сессия закрыта из-за неактивности.

— **ipsBlock** — сессия заблокирована модулем IPS.

— **avBlock** — сессия заблокирована антивирусным модулем.

— **icapExportError** — ошибка отправки данных на ICAP-сервер.

— **icapBlock** — сессия заблокирована согласно вердикту ICAP.

— **fileBlock** — сессия заблокирована модулем анализа файлов.

— **internalError** — внутренняя ошибка— недопустимая операция над потоком в LW-стеке.

— **rerouteError** — для существующей сессии недоступен подходящий маршрут.

— **tcpInitTimeout** — межсетевой экран не получил SYN-ACK после получения TCP SYN.

— **tcpHandshakeTimeout** — в ходе TCP-рукопожатия межсетевой экран получил TCP SYN, затем SYN-ACK, но не получил завершающее ACK.

— **tcpNoKeepalivesFromClient** — нет ответов на keepalive-сообщения от клиента.

— **tcpNoKeepalivesFromServer** — нет ответов на keepalive-сообщения от сервера.

- **tcpRetxExhaustedToClient** — выполняется повторная пересылка данных клиенту (TCP retransmission) и от клиента не приходят подтверждения о получении данных. Межсетевой экран исчерпал все попытки повторной пересылки данных.
- **tcpRetxExhaustedToServer** — выполняется повторная пересылка данных серверу (TCP retransmission) и от сервера не приходят подтверждения о получении данных. Межсетевой экран исчерпал все попытки повторной пересылки данных.
- **tcpPersistExhaustedToClient** — от клиента получено TCP Zero Window. Межсетевой экран отправляет window probe по истечению TCP persist timeout. Клиент не отвечает. Межсетевой экран исчерпал все попытки отправки window probe.
- **tcpPersistExhaustedToServer** — от сервера получено TCP Zero Window. Межсетевой экран отправляет window probe по истечению TCP persist timeout. Сервер не отвечает. Межсетевой экран исчерпал все попытки отправки window probe.
- **tcpHalfClosedClient** — сессия закрыта до завершения ее закрытия сервером. Клиент закрыл свою половину соединения (TCP FIN и TCP ACK), а сервер нет.
- **tcpHalfClosedServer** — сессия закрыта до завершения ее закрытия клиентом. Сервер закрыл свою половину соединения (TCP FIN и TCP ACK), а клиент нет.
- **tcp5TupleReuse** — повторное использование 5-tuple. Межсетевой экран завершил сессию, поскольку после ответа сервера TCP SYN-ACK клиент попытался открыть новое соединение, направив серверу TCP SYN с таким же 5-tuple.
- **noVirtualContext** — виртуальный контекст, в рамках которого создана сессия, был удален.
- **routingModeChanged** — для потока поменялся режим передачи данных (vWire, маршрутизация).
- **noVirtualRouter** — виртуальный маршрутизатор, в рамках которого выполнялась маршрутизация сессии, был удален.
- **noRouteToServer** — не найден маршрут для запроса от клиента к серверу (forward-маршрут).
- **noRouteToClient** — не найден маршрут для ответа от сервера клиенту (backward-маршрут).
- **routeToClientNotApplicable** — маршрут в сторону клиента найден, но он или без интерфейса, или интерфейс не UNICAST.
- **routeToServerNotApplicable** — маршрут в сторону сервера найден, но он или без интерфейса, или интерфейс не UNICAST.
- **broadcastRerouteError** — для широковещательного трафика нет source-интерфейса. Перемаршрутизация broadcast-потоков невозможна.
- **directedBroadcastNoSupport** — маршрутизация directed broadcast не поддерживается.
- **aeDownClientSide** — у агрегированного интерфейса (LACP или статического) в сторону клиента нет рабочих физических интерфейсов или он еще не собрался.

- **aeDownServerSide** — у агрегированного интерфейса (LACP или статического) в сторону сервера нет рабочих физических интерфейсов или он еще не собрался.
- **vwireForwardingError** — не найден оригинальный интерфейс или найден, но идентификатор виртуального контекста сессии не соответствует интерфейсу.
- **noClientMACaddress** — не удалось выяснить MAC-адрес клиента, находящегося в сети, подключенной напрямую (directly connected) к интерфейсу межсетевого экрана.
- **noServerMACaddress** — не удалось выяснить MAC-адрес сервера, находящегося в сети, подключенной напрямую (directly connected) к интерфейсу межсетевого экрана.
- **noGatewayMACtoClient** — не удалось выяснить MAC-адрес шлюза в сторону клиента.
- **noGatewayMACtoServer** — не удалось выяснить MAC-адрес шлюза в сторону сервера.
- **pbrBlock** — сессия заблокирована правилом маршрутизации (PBR).
- **natChanged** — сессия закрыта в связи с изменением правила NAT: обновленные критерии правила (зона безопасности, IP-адрес, порт источника или порт получателя) не соответствуют сессии или изменились параметры трансляции (выходной интерфейс или его адрес, адресный пул, транслированный порт).
- **adminCleared** — сессия удалена администратором.

40. Описание графиков дашборда PT NGFW Lite

Примечание. Описание графиков в этом разделе относится только к дашборду PT NGFW Lite.

Bandwidth Total

График **Bandwidth Total** показывает суммарную пропускную способность межсетевого экрана по всем интерфейсам dataplane.

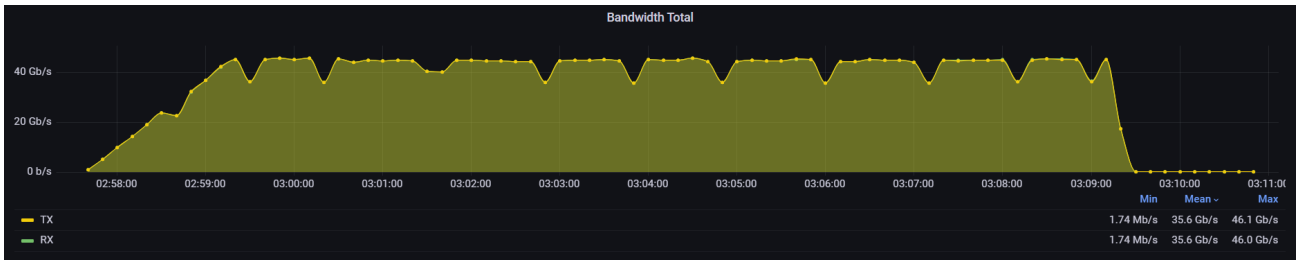


Рисунок 330. График **Bandwidth Total**

Примечание. Значения **RX** (receive) и **TX** (transmit) не обязательно должны совпадать: межсетевой экран может не пропускать часть передаваемого трафика из-за перегрузки, политик фильтрации и других механизмов обработки трафика.

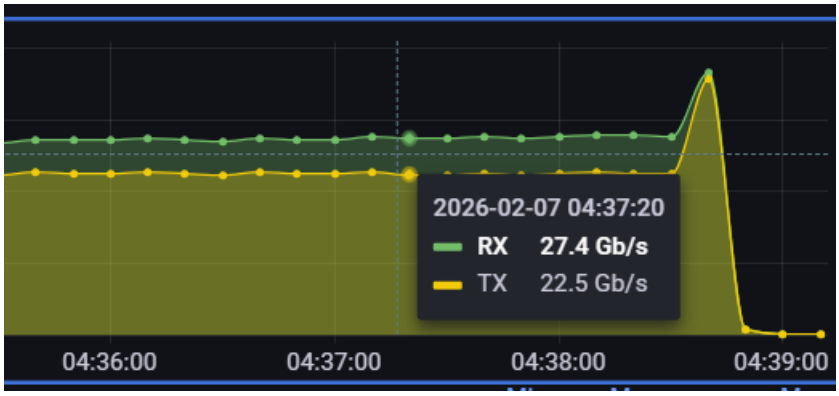


Рисунок 331. Пример несовпадения значений **RX** и **TX**

Bandwidth by interfaces

График **Bandwidth by interfaces** показывает данные по пропускаемому трафику на каждом физическом интерфейсе.

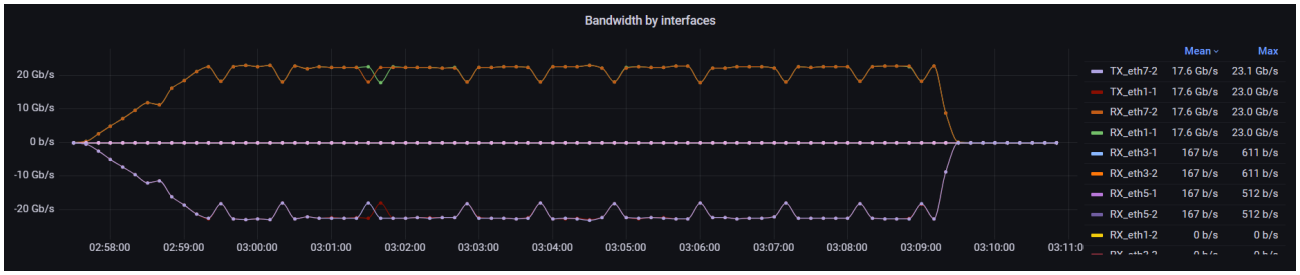


Рисунок 332. График **Bandwidth by interfaces**

Примечание. Отрицательные значения на графике представлены для удобства восприятия: в верхней части графика — RX (положительные), в нижней — TX (отрицательные).

PPS Total

График **PPS Total** демонстрирует агрегированное число пакетов в секунду, передаваемых через межсетевой экран по всем интерфейсам dataplane.



Рисунок 333. График **PPS Total**

Примечание. Значения **RX** (receive) и **TX** (transmit) не обязательно должны совпадать: межсетевой экран может не пропускать часть подаваемого трафика из-за перегрузки, политик фильтрации и других механизмов обработки трафика.

PPS by interfaces

График **PPS by interfaces** показывает число передаваемых пакетов на каждом физическом интерфейсе.

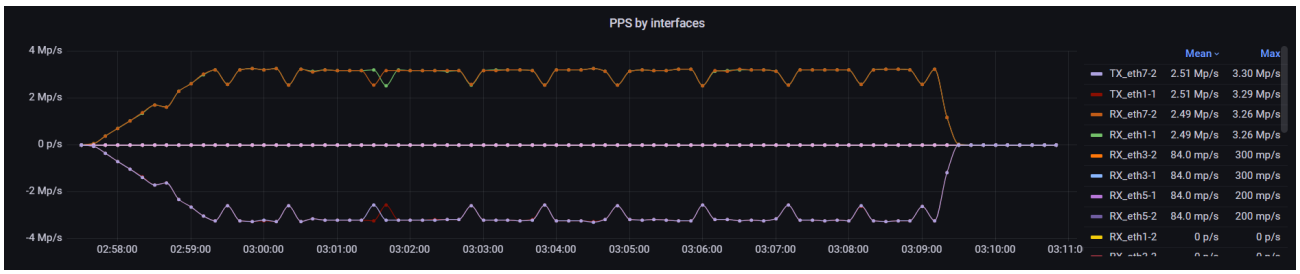


Рисунок 334. График **PPS by interfaces**

Примечание. Отрицательные значения на графике представлены для удобства восприятия: в верхней части графика — RX (положительные), в нижней — TX (отрицательные).

Concurrent connections(ip_alloc_flow_used)

График **Concurrent connections(ip_alloc_flow_used)** отражает текущее число соединений, находящихся в оперативной памяти межсетевого экрана.

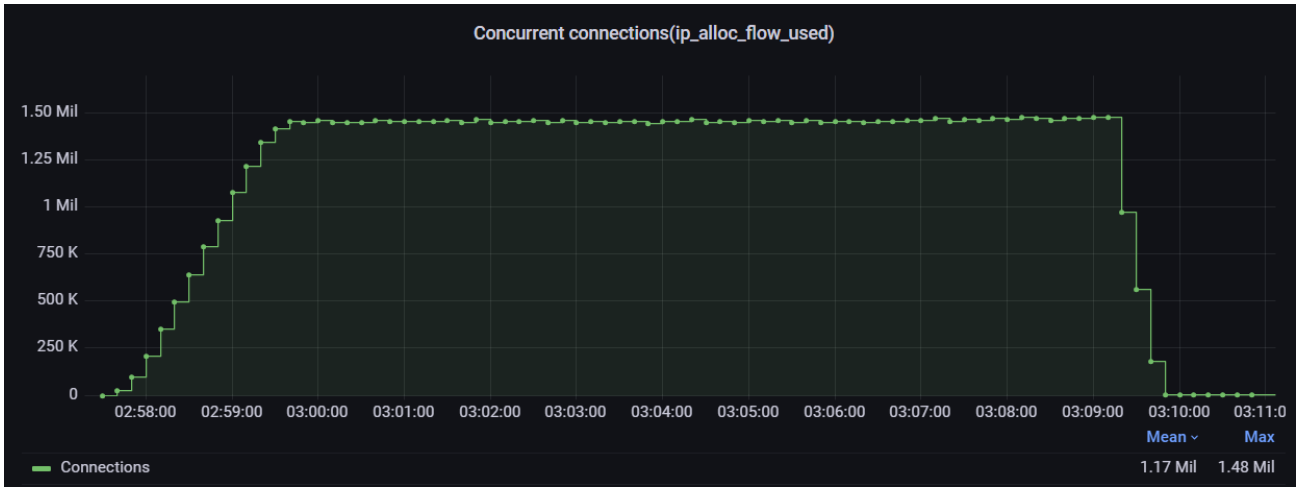


Рисунок 335. График **Concurrent connections(ip_alloc_flow_used)**

Примечание. Рекомендуется не превышать пороговые значения по числу поддерживаемых соединений для межсетевого экрана, приведенные в datasheet. Например, в datasheet указано, что максимальное число соединений для межсетевого экрана — 1,5 млн. На примере графика выше загрузка подсистемы оперативной памяти по этому показателю составляет 99%.

Примечание. Ознакомиться с datasheet на каждую модель PT NGFW вы можете по ссылке.

New Connections/s

График **New Connections/s** отражает количество новых соединений в секунду.

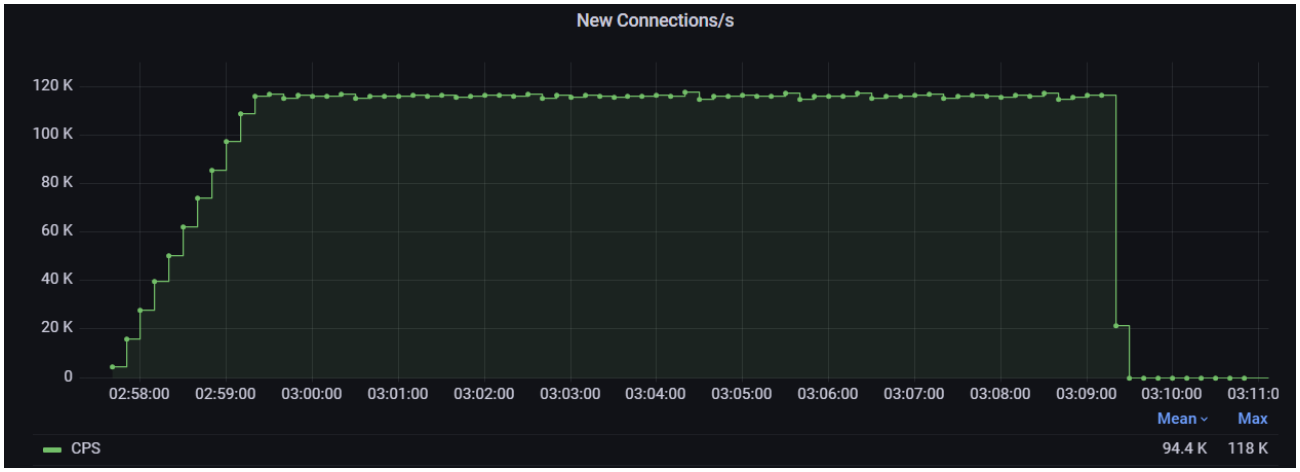


Рисунок 336. График **New Connections/s**

Примечание. Рекомендуется не превышать пороговые значения по темпу установки соединений для межсетевого экрана, приведенные в datasheet. Например, в datasheet указано, что максимальный темп установки соединений для межсетевого экрана — 150 тыс. На примере выше этот показатель составляет 79% от максимального значения.

Links status

График **Links status** отражает состояние физических интерфейсов: 1 — интерфейс активен, 0 — интерфейс не подключен.

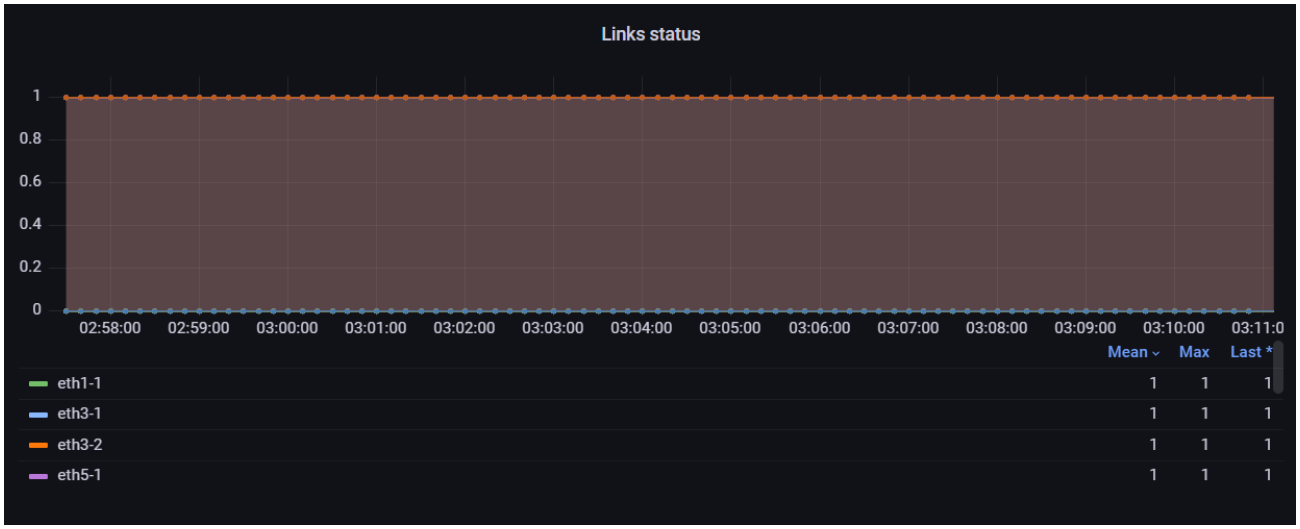


Рисунок 337. График **Links status**

CPU Usage Total (periodic + workload), %

График **CPU Usage Total (periodic + workload), %** отражает усредненное значение нагрузки на ЦП межсетевого экрана.

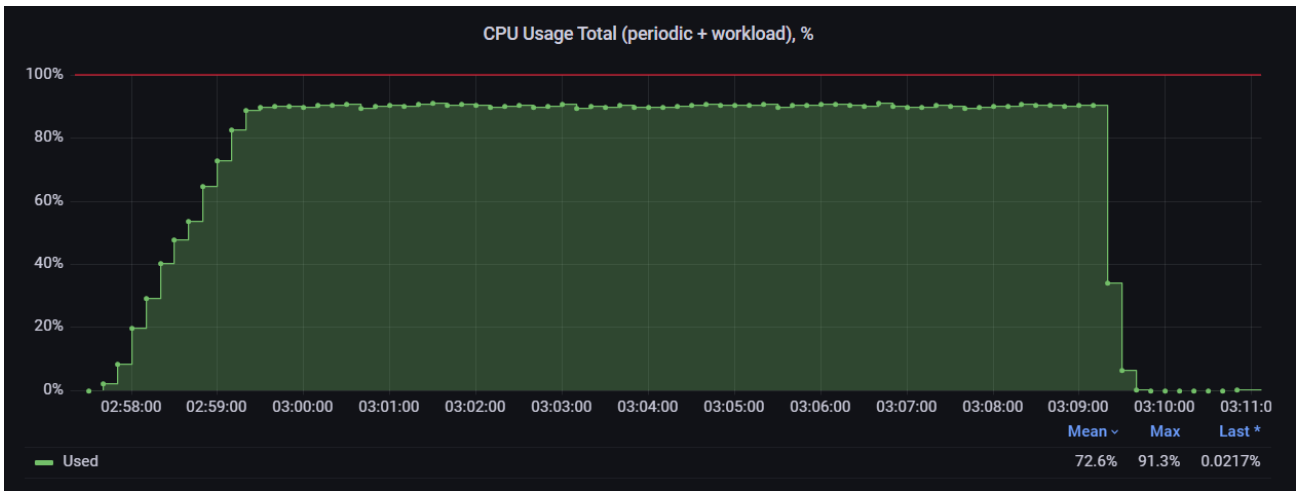


Рисунок 338. График **CPU Usage Total (periodic + workload), %**

Не рекомендуется превышать следующие пороги средней нагрузки на ЦП межсетевого экрана.

Таблица 19. Пороговые значения средней нагрузки на ЦП межсетевого экрана

Модель платформы	1005	1010	1020	1050	2010	2020	2050	3010	3040	3050
Максимальная нагрузка на ЦП, %	95	95	90	90	90	90	90	90	90	90

Примечание. Указанные значения загрузки ЦП являются порогом, при котором межсетевой экран в заметных объемах отбрасывает пакеты из-за перегрузки. Не рекомендуется допускать постоянной нагрузки на указанных пределах; следует оставлять достаточный запас по производительности с учетом перспектив развития сети, места установки межсетевого экрана и других внешних факторов.

CPU work Usage by task, %

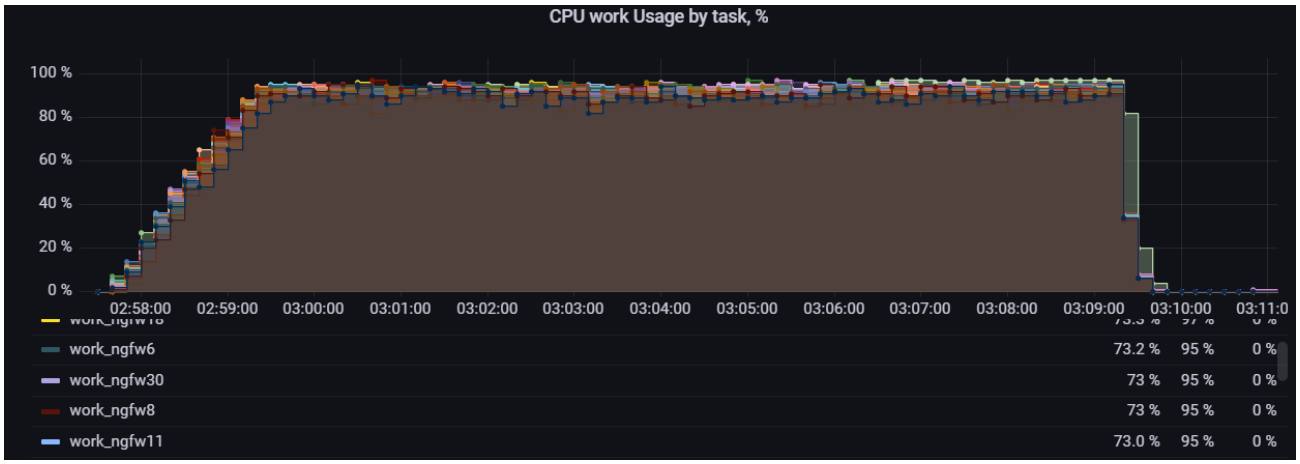


Рисунок 339. График **CPU work Usage by task, %**

Входящая нагрузка распределяется между ядрами, выделенными для обработки трафика dataplane. При возникновении крупных непрерывных потоков данных (elephant flow), проходящих через межсетевой экран, график **CPU Usage Total (periodic + workload), %** может не отражать фактическую загрузку. Пример такого случая изображен на рисунке ниже.

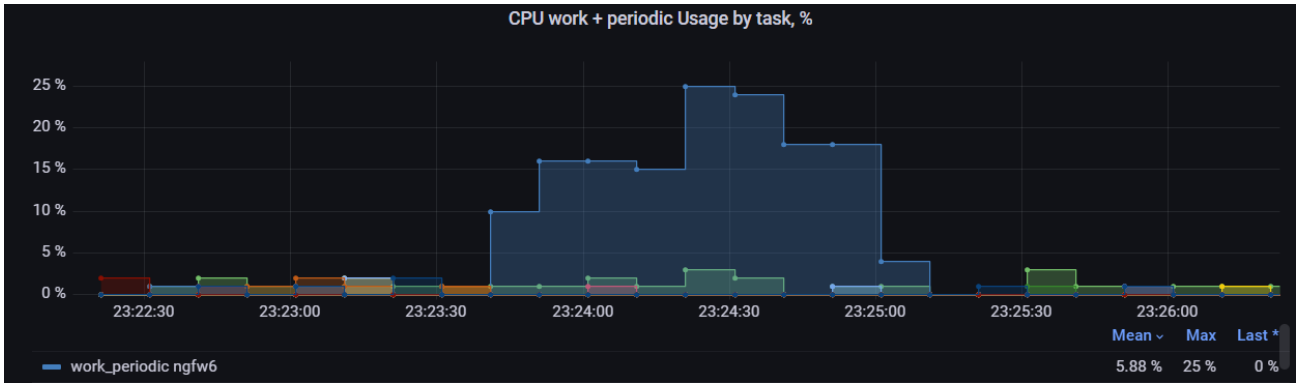


Рисунок 340. Пример elephant flow

На графике выше виден эффект возникновения elephant flow: одно из ядер ЦП заметно загружено, в то время как остальные ядра не заняты полезной нагрузкой. На общем графике нагрузки на ЦП этот же интервал времени выглядит следующим образом:

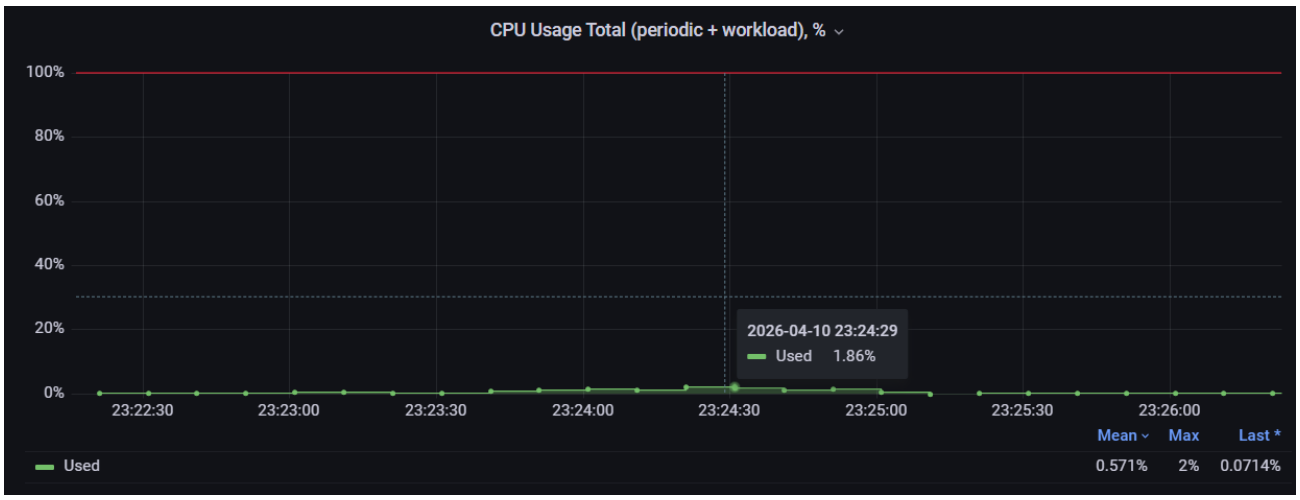


Рисунок 341. График нагрузки на ЦП

Примечание. Для более точного определения нагрузки рекомендуется ориентироваться на график нагрузки по каждому ядру, выделенному для обработки трафика dataplane.

Блок Pools

В блоке **Pools** каждый график отражает нагрузку на пул оперативной памяти, отвечающий за отдельный модуль межсетевого экрана. Граница **limit** показывает пороговое значение для каждого пула.



Рисунок 342. Блок **Pools**

На двухпроцессорных аппаратных платформах показатели использования и лимиты для пулов отображаются отдельно по NUMA-узлу 0 и NUMA-узлу 1. При оценке нагрузки необходимо учитывать оба значения, поскольку они могут различаться.

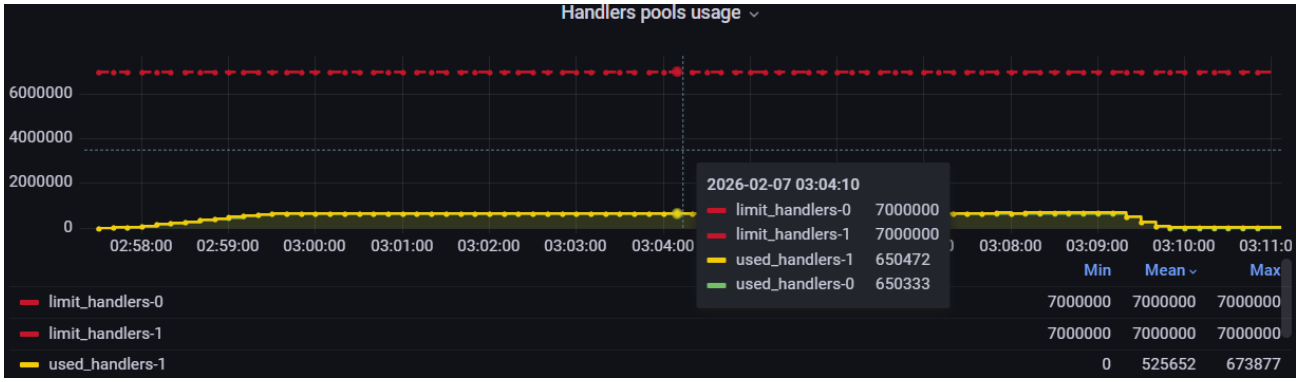


Рисунок 343. График **Handlers pools usage** на двухпроцессорной аппаратной платформе

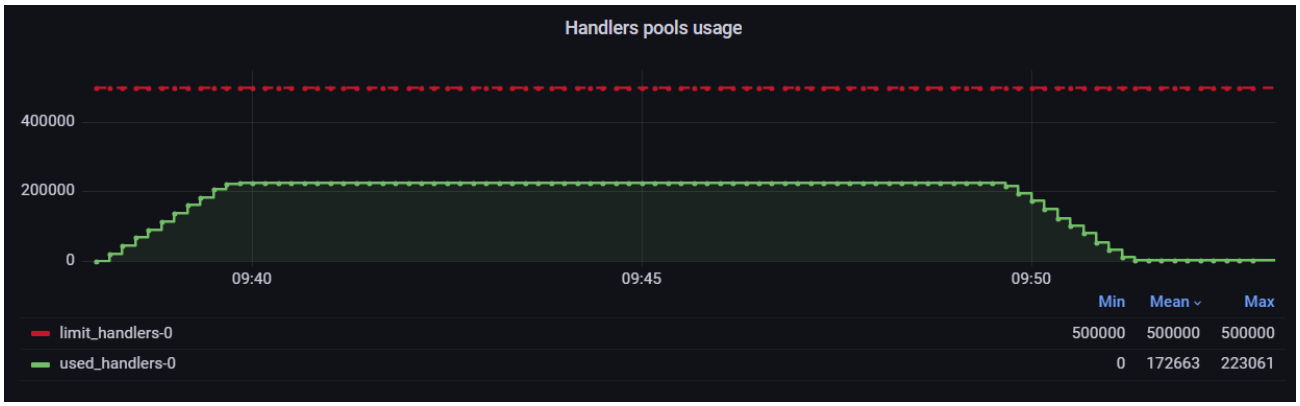


Рисунок 344. Пример, иллюстрирующий ситуацию загруженности пула

Примечание. Показатели на графике не имеют единиц измерения и приведены в условных единицах.

Превышение лимита недопустимо, поскольку после его достижения межсетевой экран начинает отбрасывать часть трафика, проходящего через него.

Назначение пулов оперативной памяти:

— pkt_poolX — выделение памяти под входящие или отправляемые пакеты;

— handlers-X — выделение памяти под контексты обработки L4-потоков;

— msgs_nodeX — выделение памяти под сообщения межмодульного взаимодействия;

— app-dataX — размещение потоков данных прикладного уровня (например, потоков для сообщений HTTP либо расшифрованных потоков TLS);

— transactions-X — выделение памяти под транзакции прикладного уровня;

— files-X — выделение памяти под описатели выделенных файлов из транзакций прикладного уровня;

— file-data-X — размещение потоков данных файлов;

— export-block-X — размещение экспортируемых (отправляемых во внешние получатели, , в ICAP-сервер) потоков данных;

— event_log — выделение памяти для записей журналов;

— url_cache — кеширование результатов URL-категоризации потоков.

Блок L7 protocols classifier

Диаграмма **Total L7 bytes** отражает в процентах распределение трафика по протоколам относительно объемов передаваемых данных.

График **L7 protocols Mbits/s** отражает статистику скорости передачи данных по протоколам через межсетевой экран за указанный период.

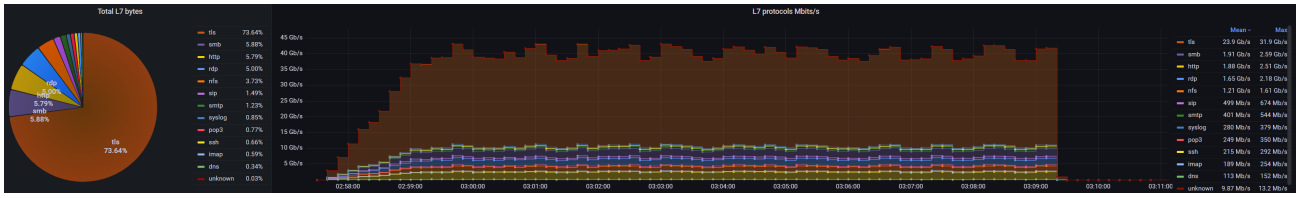


Рисунок 345. Диаграмма **Total L7 bytes** и график **L7 protocols Mbits/s**

Диаграмма **Total connections** отражает в процентах распределение трафика по протоколам относительно установленных сессий.

График **Connections/sec** отражает статистику скорости установки сессий по протоколам.

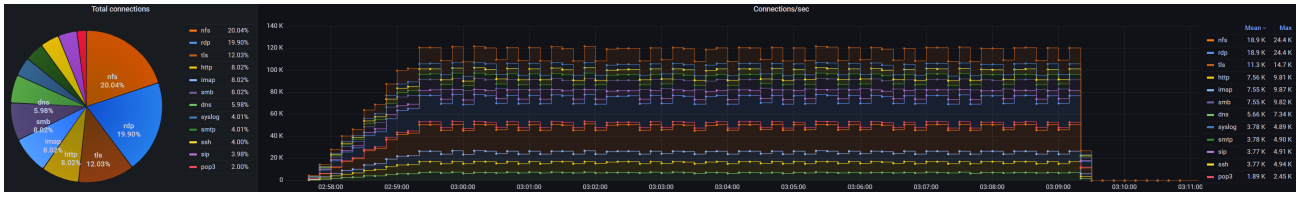


Рисунок 346. Диаграмма **Total connections** и график **Connections/sec**

Диаграмма **Total bytes (Decrypt)** отражает в процентах распределение трафика по протоколам относительно объемов расшифровываемого трафика.

График **L7 protocols Mbits/s (Decrypt)** отражает статистику скорости передачи данных по протоколам, подвергающихся расшифровке, через межсетевой экран за указанный период.



Рисунок 347. Диаграмма **Total bytes (Decrypt)** и график **L7 protocols Mbits/s (Decrypt)**

Блок Security policy stats

В блоке **Security policy stats** показаны следующие графики:

- **Export Mbits/s** — отражает скорость отправки сообщений для журналирования соединений.
- **Export Messages** — отражает число отправляемых сообщений для журналирования соединений.
- **Total rules (for all vctx)** — отражает статистику числа установленных правил на межсетевом экране. Для двухпроцессорных платформ число отображаемых правил в два раза больше, чем фактически установлено, так как график отражает суммарное число правил на NUMA-узле 0 и NUMA-узле 1.
- **Blocked Mbits/s** — отражает статистику по блокируемому трафику.
- **Blocked PPS** — отражает статистику по заблокированным пакетам в секунду.
- **Flows Rate** — отражает статистику по сообщениям о блокировке или разрешению трафика.

Блок Accounting stats

В блоке **Accounting stats** показаны следующие графики:

- **Total user stats** — отражает число добавленных, удаленных, обновленных записей о пользователях, получаемых межсетевым экраном от агента Identity Control.
- **Total storage size** — отражает число и тип хранимых записей, полученных межсетевым экраном от агента Identity Control.

41. Резервное копирование и восстановление

Вы можете создавать, экспортировать и импортировать резервные копии конфигурации системы управления. Такая копия содержит политики, объекты, устройства, группы устройств, параметры отправки событий на syslog-серверы, учетные записи администраторов, включая текущие пароли, и не содержит записи журналов. При создании или импорте резервной копии она сохраняется на устройстве с установленной системой управления. При восстановлении конфигурации текущая конфигурация системы управления заменяется конфигурацией из резервной копии. Восстановление конфигурации может потребоваться, например, в случае некорректной настройки устройства или при смене сервера системы управления.

Функциональность имеет следующие особенности:

— Если на устройстве, на котором происходит восстановление конфигурации, ранее присутствовали записи в журналах, то они не удалятся.

— События создания резервной копии и восстановления фиксируются в журнале **Аудит**.

— Отсутствует возможность автоматического (запланированного) создания резервных копий.

— Восстановление конфигурации, созданной в системе управления более новой версии, чем текущая, не поддерживается.

  Внимание! Если в текущей конфигурации присутствует A/S-кластер, при восстановлении конфигурации из резервной копии, в которой этот A/S-кластер отсутствует, конфигурацию не удастся применить на устройствах кластера. Для применения конфигурации на устройствах кластера потребуется сначала расформировать кластер. Для получения соответствующих инструкций вы можете обратиться в техническую поддержку (см. раздел 49).

Работа с резервными копиями выполняется на странице **Параметры** → **Резервное копирование**.

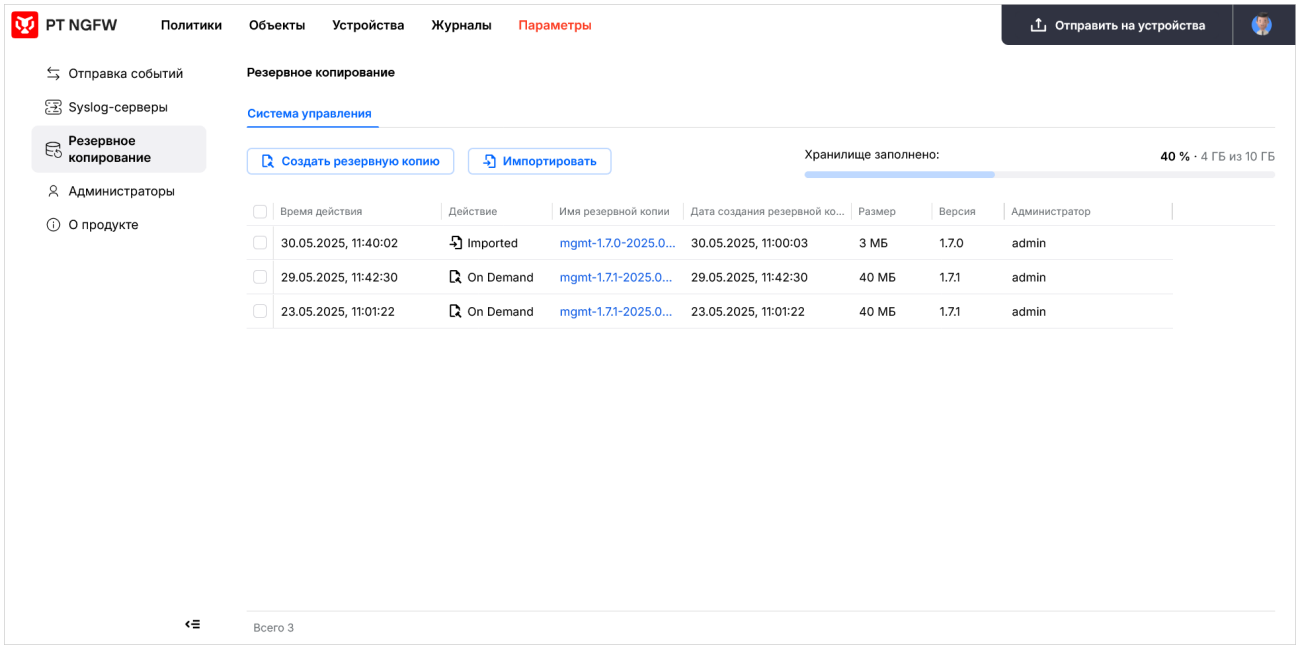


Рисунок 348. Страница **Резервное копирование**

Примечание. На странице **Резервное копирование** в столбце **Время действия** отображается время создания или импорта резервной копии в зависимости от того, была ли копия создана или импортирована.

Создание резервной копии

- Чтобы создать резервную копию,

  нажмите **Создать резервную копию**.

После завершения создания или импорта резервная копия отображается в таблице.

В имени файла резервной копии указывается время создания копии в часовом поясе UTC+0. В столбце **Дата создания резервной копии** учитывается часовой пояс, получаемый от браузера администратора.

Импорт резервной копии

- Чтобы импортировать резервную копию,

  нажмите **Импортировать**.

Экспорт резервной копии

- Чтобы экспортировать резервную копию,

  в контекстном меню копии выберите **Скачать**.

Восстановление конфигурации

- Чтобы восстановить конфигурацию,

  в контекстном меню резервной копии выберите **Восстановить**.

При запуске восстановления текущие сессии администраторов завершаются. Во время восстановления система управления остается недоступной — на странице входа отображается сообщение о выполнении восстановления. Когда восстановление завершено, вы можете войти в систему, используя учетную запись из резервной копии.

Удаление резервной копии

- Чтобы удалить резервную копию,

  в контекстном меню копии выберите **Удалить**.

  Примечание. Вы можете удалить несколько копий сразу, установив флажок напротив каждой из них и нажав **Удалить** на панели инструментов внизу страницы.

42. Предустановленные категории URL

Ниже перечислены категории URL, поставляемые вместе с PT NGFW.

Таблица 20. URL-категории

Класс категории	Название категории на рус.	Название категории на англ.	Описание
Контент для взрослых	Порнография и секс	Adult and Pornography	Порнографические сайты, включая анимацию и рассказы
Контент для взрослых	Сайты для взрослых прочие	Adult Other	Сайты стрип-клубов, секс-шопов, непорнографические сайты с материалами о сексе
Контент для взрослых	Алкоголь и табак	Alcohol and Tobacco	Продажа, продвижение, производство или употребление алкогольной и (или) табачной продукции. Материалы об электронных сигаретах и вейпах
Контент для взрослых	Альтернативные верования	Alternative Beliefs	Нетрадиционные верования, не связанные с мировыми религиями. Сайты с информацией о заклинаниях, проклятиях, магических способностях, гаданиях, колдовстве, сатанизме, сверхъестественных явлениях
Контент для взрослых	Свидания	Dating	Сайты знакомств
Контент для взрослых	Азартные игры	Gambling	Азартные игры, например казино, лотереи, розыгрыши, ставки. Информация об играх и статистика
Контент для взрослых	Нижнее белье и купальники	Lingerie and Swimsuit	Магазины нижнего белья и купальников, использующие изображения полуобнаженных моделей с целью продажи или продвижения таких товаров
Контент для взрослых	Нагота	Nudity	Сайты, не имеющие цели сексуального возбуждения, с изображениями полностью или частично обнаженного человеческого тела

Класс категории	Название категории на рус.	Название категории на англ.	Описание
Контент для взрослых	Оружие	Weapons	Оружие, сайты оружейных магазинов, стрелковых клубов, материалы о военных играх, например о страйкболе
Потребители трафика	Обмен и хранение файлов	File Sharing and Storage	Онлайн-хранилища и сервисы для резервного копирования, в том числе сайты, предоставляющие ссылки на файлы (как правило, бесплатно), и сайты для обмена фотографиями
Потребители трафика	Интернет-телефония	Internet Telephony	Сервисы телефонной связи через интернет
Потребители трафика	Торренты и сети Peer-to-peer	Torrents and Peer-to-peer	Сайты, агрегирующие ссылки BitTorrent, позволяя пользователям обмениваться файлами
Потребители трафика	Скачивание ПО и медиа	Software and Media Downloads	Сайты с программным обеспечением или медиаконтентом, включая изображения, фоновые рисунки, видео, предоставляемым бесплатно или за пожертвование (плату)
Потребители трафика	Стриминговые сервисы и телевидение	Streaming Media and TV	Потоковая передача медиаконтента, в том числе трансляции радио и телевидения через интернет
Общие темы. Бизнес	Бизнес	Business	Коммерческие организации, компании, корпорации, фирмы, ассоциации, отраслевые группы. Категория включает сайты о маркетинге, управлении, экономике, предпринимательстве или ведении бизнеса
Общие темы. Бизнес	Компьютерная безопасность	Computer Security	Материалы по кибер- и информационной безопасности, такие как статьи, новости, рекомендации, лучшие практики. Категория включает сайты, которые продвигают или предлагают услуги безопасности, такие как сервисы аутентификации и управления паролями

Класс категории	Название категории на рус.	Название категории на англ.	Описание
Общие темы. Бизнес	Криптовалюты	Cryptocurrency	Криптовалюты и криптомайнинг, за исключением самих криптомайнеров. Категория включает сайты, управляющие криптовалютными кошельками и реестрами, а также сайты криптовалютных бирж и продавцов
Общие темы. Бизнес	Финансы и банки	Finance and Banking	Банки и другие финансовые организации. Категория включает онлайн-банкинг, кредиты, ипотеку, кредитные карты и сайты страховых компаний. Не включает торговлю и брокерские услуги
Общие темы. Бизнес	Правительственные сайты	Government	Государственные агентства, бюро или другие правительственные организации. Категория включает вооруженные силы, суды, полицейские учреждения, сайты городских органов власти
Общие темы. Бизнес	Поисковые системы	Search Engines	Поисковые службы в интернете, где можно использовать ключевые слова, фразы, изображения для получения информации в любой форме (ссылки, тексты, изображения и т. д.)
Общие темы. Бизнес	Некоммерческие и неправительственные организации	Non-profits and NGOs	Некоммерческие или неправительственные организации, которые занимаются социальной, благотворительной деятельностью, защитой природы, борются с различными формами неравенства. Категория включает некоммерческие и неправительственные организации, продвигающие политические взгляды и мнения по общественным вопросам
Общие темы. Бизнес	Онлайн-конференции	Online Meetings	Сервисы онлайн-встреч, совместного использования экрана и совместной работы через интернет

Класс категории	Название категории на рус.	Название категории на англ.	Описание
Общие темы. Бизнес	Политические организации и взгляды	Political Organizations and Advocacy	Политические партии и группы по интересам, ориентированные на политику, выборы, законодательство, а также сайты, содержащие информацию, точки зрения или кампании, связанные с политическими взглядами. Не включает сайты, связанные с правительством
Общие темы. Бизнес	Наука и технологии	Science and Technology	Сайты, посвященные науке, информационным технологиям, технологиях в целом, с технической информацией и информацией об искусственном интеллекте
Общие темы. Бизнес	Интернет-порталы	Internet Portals	Платформы, агрегирующие различный онлайн-контент и служащие отправной точкой для пользователей при работе в интернете
Общие темы. Бизнес	Переводчики	Translation	Услуги перевода, которые могут включать перевод текста, введенного пользователем, или целых веб-страниц через ввод URL. Кроме того, такие сайты могут помогать пользователям обходить фильтрацию контента, так как переведенный контент отображается под доменом переводчика, а не исходного источника
Общие темы. Бизнес	Сервисы сокращения URL	URL Shortening	Сервисы по сокращению веб-адресов. Делают URL значительно короче, при этом перенаправляя пользователей на целевую страницу
Общие темы. Бизнес	Веб-аналитика	Web Analytics	Аналитика и сбор данных, связанных с посещаемостью, взаимодействием пользователей и их поведением на сайтах
Общие темы. Бизнес	Хостинговые сервисы	Web Hosting	Услуги хостинга, страницы доменов верхнего уровня для онлайн-сообществ. Эти сайты предлагают бесплатные или платные хостинго-

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			вые сервисы. Они также могут включать ресурсы, связанные с веб-разработкой, публикацией контента, продвижением и различными стратегиями для увеличения трафика на веб-сайты
Общие темы. Бизнес	Веб-приложения	Web-based Applications	Веб-приложения, работающие по модели «программное обеспечение как услуга» (SaaS). Примерами таких приложений являются Miro, Figma, Salesforce, Trello, Asana, HubSpot
Общие темы. Бизнес	Офисные веб-приложения	Web-based Office Applications	SaaS-приложения, которые предоставляют услуги, аналогичные традиционным настольным офисным инструментам, включая текстовые редакторы, электронные таблицы и презентации. Примерами таких приложений являются Google Docs, Google Sheets, Microsoft 365, Zoho Docs, Dropbox Paper и подобные сервисы
Общие темы. Бизнес	Генеративный ИИ. Диалоговые инструменты	Generative AI. Conversational Tools	Сервисы искусственного интеллекта для решения широкого спектра задач посредством диалогового интерфейса, таких как генерация текста, ведение диалогов, написание статей, составление резюме, перевод и другие задачи
Общие темы. Бизнес	Генеративный ИИ. Мультимедиа	Generative AI. Multimedia	Сервисы искусственного интеллекта для создания мультимедийного контента, такого как изображения, видео или аудио, а также приложения для преобразования текста в речь, редактирования видео, музыки, звука или изображений
Общие темы. Бизнес	Генеративный ИИ. Код	Generative AI. Code	Сервисы искусственного интеллекта для написания и оптимизации кода. Включают платформы, поддерживающие автодополнение

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			кода в режиме реального времени, обнаружение ошибок и предложения по улучшению кода
Общие темы. Бизнес	Генеративный ИИ. Анализ данных	Generative AI. Data Analysis	Сервисы искусственного интеллекта для бизнеса и аналитики, например платформы для предприятий, автоматизирующие создание контента с учетом SEO, генерацию изображений и хештегов, анализ данных, оптимизацию и управление повторяющимися задачами для повышения эффективности и производительности
Общие темы. Частное	Реклама	Advertising	Онлайн-реклама, медиа, баннеры и промоконтент. Эти сайты часто включают страницы для подписки или отказа от рассылок и рекламы. Они также могут предоставлять рекламную графику, медиафайлы или другие промоматериалы, включая рекламные серверы, которые часто имеют доменные имена с префиксами, такими как «ad.» (например, ad.example.com)
Общие темы. Частное	Культура и искусство	Arts and Culture	Искусство, культура и традиции, обычаи, изобразительное искусство, живопись, музыка и языки. Эта категория также включает учреждения, такие как музеи, библиотеки, и исторические достопримечательности. Сайты категории сосредоточены на демонстрации исторического и культурного наследия конкретных регионов и могут косвенно продвигать туризм и путешествия
Общие темы. Частное	Брокерские и трейдинговые сервисы	Brokerage and Trading	Торговля ценными бумагами и управление инвестициями. Сайты, которые содержат только информацию о поставщиках и покупателях или рекламу, не относятся к

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			этой категории, так как они не обеспечивают возможность реальной торговой деятельности
Общие темы. Частное	Сети доставки данных	Content Delivery Networks	Контент для связанных (партнерских) сайтов. Эти сети занимаются доставкой различных типов данных и медиа для третьих сторон, включая рекламу, файлы, изображения и видео
Общие темы. Частное	Динамический контент	Dynamic Content	Веб-сайты, которые создают контент в реальном времени в ответ на определенные параметры в URL-адресах или дополнительные данные (например, геолокацию) из входящих веб-запросов. Сюда также включаются URL-адреса, которые динамически создаются веб-сервером
Общие темы. Частное	Образование	Education	Школы, образовательные учреждения, неакадемические исследовательские организации, образовательные мероприятия и активности. Платформы, предлагающие информацию о продаже или поставке учебных материалов, учебников, пособий, инструкций и программ обучения, в том числе бесплатных, а также академических журналов и подобных изданий
Общие темы. Частное	Развлечения	Entertainment	Фильмы и видео, радио- и телешоу (не новостные), музыка, программы передач, книги, юмор, комиксы, кинотеатры, художественные галереи, рецензии на развлекательный контент. Категория включает журналы, аниме и юмористические материалы
Общие темы. Частное	Игры	Games	Игры различных видов, например электронные игры, видеоигры, компьютерные игры, ролевые игры, настольные или онлайн-игры,

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			включая платформы по распространению и продаже игр, например Steam, Battle.net. Сайты с псевдонаучными играми, требующими много времени и имеющими минимальную образовательную ценность, также относятся к этой категории
Общие темы. Частное	Здоровье и медицина	Health and Medicine	Личное здоровье, медицинские услуги и процедуры, а также медицинские устройства и лекарства. В эту категорию входят поставщики услуг косметической хирургии, медицинского страхования, клиники и больницы. Она также включает сайты с общей информацией о здоровье, проблемах, традиционных и альтернативных методах лечения, терапии и советы. Кроме того, сюда относятся платформы, связанные с различными медицинскими специальностями, практиками, учреждениями (такими как тренажерные залы и фитнес-центры) и специалистами в области здравоохранения
Общие темы. Частное	Хобби и стиль жизни	Hobby and Lifestyle	Материалы о частной жизни, личных интересах, включая хобби, например, садоводство, коллекционирование и уход за домашними животными, астрология, а также журналы, блоги и сайты, связанные с домом и семьей. Категория также охватывает сайты об активном отдыхе, например рыбалке, охоте и других увлечениях
Общие темы. Частное	Поиск работы и карьера	Job Search and Careers	Поиск работы или найм сотрудников. Сюда входят кадровые агентства и консалтинговые услуги, предлагающие списки вакансий и возможности трудоустройства

Класс категории	Название категории на рус.	Название категории на англ.	Описание
Общие темы. Частное	Доски объявлений и форумы	Message Boards and Forums	Пространства для обсуждений, такие как доски объявлений и форумы, где пользователи могут обмениваться сообщениями и участвовать в беседах
Общие темы. Частное	Музыка	Music	Продажа, распространение или обмен информацией, относящейся к музыке. Категория включает сайты, посвященные музыкальным исполнителям, группам, звукозаписывающим компаниям, мероприятиям, текстам песен и другим аспектам музыкальной индустрии. Стриминговые сервисы для прослушивания музыки не входят в эту категорию
Общие темы. Частное	Новости и СМИ	News and Media	Новостные службы и агентства, включая сайты телеканалов и радиостанций, если их контент не ограничивается исключительно развлекательной тематикой
Общие темы. Частное	Запаркованные домены	Parked Domains	Временные заглушки для доменных имен. Сайты не содержат значимого или полезного контента. На таких сайтах часто размещается минимальный контент или реклама с переходом по ссылкам, что может приносить доход владельцу домена, но обычно не представляет ценности для посетителей. Эта категория также включает домены, которые выставлены на продажу
Общие темы. Частное	Персональные сайты и блоги	Personal Sites and Blogs	Онлайн-платформы, где пользователи делятся своей личной информацией, мыслями и идеями. Эти сайты позволяют пользователям быстро публиковать или обновлять неформальный контент
Общие темы. Частное	Недвижимость	Real Estate	Сайты, предоставляющие информацию об аренде, покупке, продаже или финансировании жилой не-

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			движимости. Эти сайты часто продвигаются сервисами, связанными как с коммерческой, так и с жилой недвижимостью. Они включают списки объектов недвижимости, а также информацию об оценке и брокерских услугах
Общие темы. Частное	Справочная информация	Reference and Research	Личные, профессиональные или информационные ресурсы. К ним относятся онлайн-словари, карты, данные переписей, сборники, библиотечные каталоги, инструменты для генеалогии, тезаурусы, энциклопедии, справочники и стандарты
Общие темы. Частное	Религия	Religion	Мировые религии, такие как буддизм, бахаи, христианство, христианская наука, индуизм, ислам, иудаизм, мормонизм, синтоизм и сикхизм, а также атеизм. Эти сайты также охватывают связанные с ними мероприятия, события и ресурсы, включая информацию о религиозных организациях, лидерах, местах поклонения и религиозных предметах
Общие темы. Частное	Рестораны и кафе	Restaurants and Dining	Рестораны, кафе и гастрономические впечатления. Такие сайты предоставляют информацию о местоположении, отзывы о еде, рецепты, информацию об услугах кейтеринга и др.
Общие темы. Частное	Магазины	Shopping	Продажа широкого ассортимента товаров и услуг, включая электронику, цветы, ювелирные изделия, музыку и многое другое, но исключая недвижимость. Эта категория также включает услуги онлайн-аукционов, таких как eBay, а также маркетплейсы, такие как Ozon, Wildberries, Amazon, AliExpress и другие

Класс категории	Название категории на рус.	Название категории на англ.	Описание
Общие темы. Частное	Социальные сети	Social Networks	Онлайн-платформы, предназначенные для помощи пользователям в создании и поддержании социальных связей с людьми, которые имеют схожие интересы, занятия, хобби и отношения. Эти сайты позволяют пользователям обмениваться сообщениями, фотографиями и участвовать в различных формах общения
Общие темы. Частное	Спорт	Sports	Спорт и спортивные события, информация о спортсменах, тренерах, судьях, командах или организациях, а также результаты, расписания, новости и товары, связанные со спортом. Эта категория включает онлайн-журналы или рассылки, посвящённые спорту, а также сайты, посвящённые фэнтези-спорту и виртуальным спортивным лигам
Общие темы. Частное	Вульгарность и пошлость	Tasteless	Неприемлемый или оскорбительный контент, не всегда насильственный. Категория включает материалы, связанные с испражнениями, функциями организма, окровавленной одеждой, грубым юмором, изображениями ран или крови, экстремальными изменениями тела (такими как разрезы, клеймение или пирсинг гениталий)
Общие темы. Частное	Путешествия	Travel	Путешествия, информация о размещении, видах транспорта (поезда, авиакомпании, круизные лайнеры и т. д.), туристических агентствах, курортных направлениях, достопримечательностях. Сайты содержат советы путешественникам, информацию о специальных предложениях, ценах, путеводителях по направлениям, туризме и

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			связанных услугах, таких как инструменты для бронирования или функции отслеживания цен
Общие темы. Частное	Транспорт	Vehicles	Автомобили и транспортные средства. Категория включает сайты для покупки, продажи или обмена транспортных средств или их запчастей, а также обзоры, модификации и обсуждение автомобилей, мотоциклов, лодок, грузовиков и транспортных средств для отдыха (рекреационных)
Общие темы. Частное	Веб-почта	Web-based Email	Сервисы электронной почты. Предоставляют доступ к почтовому ящику, позволяя пользователям отправлять и получать электронные письма, как правило, предлагая бесплатный или платный публичный доступ к таким услугам
Общие темы. Частное	Веб-чаты и обмен сообщениями	Web Chat and Instant Messaging	Общение в реальном времени через интернет. Категория включает сайты, которые предоставляют услуги веб-чатов или предлагают информацию о чатах на базе протокола HTTP или других протоколов
Потенциально незаконные	Сексуальное насилие над детьми	Child Sexual Abuse	Веб-сайты, которые согласно данным различных организаций размещают или распространяют незаконные изображения несовершеннолетних, насилия над нами. Эти сайты идентифицированы как содержащие незаконный и вредоносный контент, связанный с эксплуатацией детей
Потенциально незаконные	Криптомайнинг	Crypto Mining	Инструменты для майнинга криптовалют и майнинговые пулы. Категория включает сайты, которые позволяют майнерам объединять свои вычислительные мощности в сети. Категория включает сайты,

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			которые размещают вредоносное ПО, рекламное ПО или другое нежелательное программное обеспечение, относящееся к майнингу, в том числе встроенные криптовалютные майнеры, схемы кликджекинга или программы, изменяющие настройки браузера без согласия пользователя
Потенциально незаконные	Дискриминация	Discrimination	Пропаганда расовой сегрегации, принижение или угнетение определенных групп людей или утверждение превосходства одной группы над другими. Эти сайты могут поддерживать нетерпимость, ненависть или дискриминационные взгляды в отношении отдельных лиц или групп на основе этнической принадлежности, религии, убеждений или других признаков
Потенциально незаконные	Экстремизм	Extremism	Радикальные группы или движения, пропагандирующие враждебную антиправительственную или антисоциальную идеологию. Категория включает сайты, демонстрирующие контент, связанный с террористическими актами, которые являются или кажутся незаконными в юрисдикции, где проводится оценка, а также платформы, незаконно поощряющие вербовку людей в террористические организации
Потенциально незаконные	Взлом (хакинг)	Hacking	Незаконная деятельность, связанная с несанкционированным доступом или взломом программ, компьютеров, устройств и сайтов. Категория включает сайты с контентом, который может не представлять прямой угрозы безопасности, но демонстрирует другие формы несанкционированного доступа

Класс категории	Название категории на рус.	Название категории на англ.	Описание
Потенциально незаконные	Нелегальное содержимое	Illegal Content	Информация, методы или руководства по ненасильственным мошенническим или незаконным действиям, таким как аферы, подделка, уклонение от уплаты налогов, мелкие кражи, шантаж и подобные действия
Потенциально незаконные	Наркотики	Illegal Drugs	Употребление, производство и продажа наркотиков, продажа оборудования, связанного с наркотиками. Категория включает сайты с материалами о различных типах наркотических веществ, включая вдыхание клея, злоупотребление рецептурными лекарствами или использование других легальных веществ в запрещенных целях
Потенциально незаконные	Плагиат	Plagiarism	Сайты, распространяющие или продающие академические эссе, проекты и подобные материалы. Эти сайты способствуют мошенничеству, предоставляя материалы, такие как ответы на экзамены или поддельные дипломы
Потенциально незаконные	Насилие	Violence	Шокирующий контент, связанный с жестокостью, смертью, насилием, издевательствами, увечьями или пропагандой насилия и причинения физического вреда, включая самоповреждения
Потенциально незаконные	Сервисы VPN и прокси	VPN and Proxy	Обход ограничений доступа в интернет и анонимный веб-серфинг. Категория включает анонимные прокси-серверы, а также сайты, предоставляющие списки адресов прокси-серверов и другие методы обхода фильтрации или мониторинга URL-адресов
Риск безопасности	Командные центры бот-нетов	Command and Control	Ресурсы, на которых размещаются URL-адреса и домены сетей управления ботами (Command-and-

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			Control). Они используются вредоносным ПО или скомпрометированными системами для скрытой связи с удаленным сервером злоумышленника, что позволяет получать вредоносные инструкции или красть данные
Риск безопасности	Динамические DNS	Dynamic DNS	Сервисы динамических DNS (DDNS) для привязки полного доменного имени (FQDN) к определенному IP-адресу или группе адресов. Эти сервисы часто используются в кибератаках и для работы серверов управления бот-сетями (Command-and-Control)
Риск безопасности	Вредоносные сайты	Malware	Вредоносный контент, например вредоносные исполняемые файлы, скрипты, вирусы, трояны или код. Эта категория также включает сайты, которые способствуют заражению через drive-by-загрузки, эксплойт-киты и т. д.
Риск безопасности	Недавно активировавшиеся домены	Newly Observed Domains	Домены, которые начали работу или были активированы недавно, при этом они могли быть зарегистрированы давно
Риск безопасности	Недавно зарегистрированные домены	Newly Registered Domains	Домены, которые были недавно зарегистрированы. Эти домены могли быть созданы намеренно или с использованием алгоритмов генерации доменов (DGA) и могут быть связаны с вредоносной деятельностью
Риск безопасности	Фишинг	Phishing	Поддельные веб-страницы, созданные для имитации настоящий сайтов компаний. Такие платформы тайно собирают конфиденциальную информацию, такую как учетные данные, номера банковских карт, PIN-коды и другие личные данные (ПДн, PII), исполь-

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			зуя методы социальной инженерии, как с согласия, так и без согласия пользователя. Эта категория также включает мошенничество и scareware (программы, вызывающие ложную тревогу)
Риск безопасности	Частные IP-адреса	Private IP Addresses	IP-адреса, определённые в RFC 1918 — «Выделение адресов для частных интрасетей»
Риск безопасности	Программы-вымогатели	Ransomware	Платформы, которые размещают, распространяют или участвуют во вредоносной деятельности, связанной с программами-вымогателями. Эти кампании обычно угрожают публикацией конфиденциальных данных или блокируют доступ к определенным данным или системам, часто с помощью шифрования, до тех пор, пока не будет выплачен выкуп. Эта категория также включает URL-адреса, распространяющие связанные с этим стилеры, вайперы и лоадеры, способные доставлять полезную нагрузку программ-вымогателей
Риск безопасности	Спам	Spam	Сайты, URL-адреса которых часто встречаются в спам-письмах или нежелательных коммерческих сообщениях. Эти страницы нередко продвигают контент для взрослых, мошеннические товары и другие материалы, которые могут считаться оскорбительными или неприемлемыми
Риск безопасности	Подозрительное содержимое	Suspicious Content	Сомнительный контент, нежелательное ПО (potentially unwanted software, PUA), пиратское ПО (warez) или подозрительные ссылки. Эти сайты нельзя однозначно классифицировать как полностью

Класс категории	Название категории на рус.	Название категории на англ.	Описание
			безопасные или полностью вредоносные, поскольку они демонстрируют неоднозначное поведение
Неизвестные	Недостаточно данных	Insufficient Content	Сайты и онлайн-сервисы, которые отображают тестовые страницы, не содержат значимого контента, предоставляют доступ к API, не предназначенному для взаимодействия с конечным пользователем, или требуют аутентификации, не имеют контента, который позволил бы их классифицировать
Неизвестные	Неизвестно	Unknown	«Неизвестно» означает, что URL-адрес еще не был классифицирован. URL-адрес из запроса будет классифицирован сервисом категоризации как можно скорее

43. Сетевые протоколы, обнаруживаемые PT NGFW

В этом разделе перечислены сетевые протоколы, которые PT NGFW может обнаруживать в трафике.

Таблица 21. Обнаруживаемые сетевые протоколы

Обозначение	Протокол
`1c-enterprise-client`	Набор правил обмена данными между клиентским приложением и сервером 1С для выполнения бизнес-логики, обработки данных и взаимодействия с информационной базой в распределенной клиент-серверной архитектуре системы «1С:Предприятие»
`amqp`	Advanced Message Queuing Protocol (amqp.org)
`assistant-transport`	Протокол для удаленного доступа, управления и администрирования (мойассистент.рф)
`bgp`	Border Gateway Protocol (RFC4271)
`bitcoin`	Протокол Bitcoin (en.bitcoin.it)
`bittorrent`	Протокол BitTorrent (bittorrent.org)
`canon-bjnp`	Протокол обнаружения сервиса LAN, используемый в принтерах и сканерах Canon (canon.com)
`clickhouse`	Протокол системы управления базами данных ClickHouse (clickhouse.com)
`db2-drda`	Db2 Distributed Relational Database Architecture (ibm.com)
`dcerpc`	Distributed Computing Environment / Remote Procedure Call
`dhcp`	Dynamic Host Configuration Protocol (RFC 2131)
`dhcpv6`	Dynamic Host Configuration Protocol for IPv6 (RFC 3315)
`dns`	Domain Name System (RFC 1034)
`drweb`	Протокол продукта Dr.Web Enterprise Security Suite (drweb.ru)
`dtls`	Datagram Transport Layer Security (RFC 6347)
`elasticsearch`	Протокол системы Elasticsearch (elastic.co)
`facebook`	Протокол сети Facebook[5] (developers.facebook.com)
`falcongaze`	Протокол продукта Falcongaze SecureTower Agent (falcongaze.com)

5 Facebook, Instagram и WhatsApp — продукты компании Meta, которая, в соответствии с законодательством Российской Федерации, признана экстремистской организацией и запрещена в России.

Обозначение	Протокол
fb-zero	Протокол сети Facebook Zero[5] (0.facebook.com)
ftp	File Transfer Protocol (RFC 959)
guardant	Протокол продукта Guardant Net (guardant.ru)
http	Hypertext Transfer Protocol
icap	Internet Content Adaptation Protocol (RFC 3507)
imap	Internet Message Access Protocol (RFC 3501)
infowatch	Протокол продукта InfoWatch Device Monitor (infowatch.ru)
isakmp	Internet Security Association and Key Management Protocol (RFC 2408)
jrmi	Java Remote Method Invocation Protocol (oracle.com)
kafka	Протокол платформы Apache Kafka (kafka.apache.org)
kerberos	Протокол аутентификации Kerberos (RFC 4120)
ksn	Протокол сети Kaspersky Security Network (kaspersky.ru/ksn)
ldap	Lightweight Directory Access Protocol (RFC 4510)
llmnr	Link-Local Multicast Name Resolution (RFC 4795)
lotus	Протокол платформы HCL Notes (ранее IBM Notes и Lotus Notes)
mc-nmf	Net.TCP Port Sharing (docs.microsoft.com)
mdns	Multicast DNS (RFC 6762)
memcache	Протокол системы Memcached (memcached.org)
mongodb	Протокол системы управления базами данных MongoDB (docs.mongodb.com)
ms-scom	Протокол программы System Center Operations Manager (docs.microsoft.com)
ms-update	Протокол утилиты Windows Update Delivery Optimization (docs.microsoft.com)
mysql	Протокол системы управления базами данных MySQL (dev.mysql.com)
nat-t	NAT Traversal
nbns	NetBIOS Name Server (RFC 1001)
nfs	Network File System (RFC 1094)
ntp	Network Time Protocol (ntp.org)
openvpn	Протокол технологии OpenVPN (openvpn.net)

Обозначение	Протокол
oracle-tns	Oracle TNS (Transparent Network Substrate, протокол компании Oracle)
p2p-dc	Протокол Direct Connect
pop3	Post Office Protocol 3 (RFC 1081)
postgresql	Протокол системы управления базами данных PostgreSQL (postgresql.org)
pptp	Point-to-Point Tunneling Protocol (RFC 2637)
printer-pjl	Протокол Printer Job Language (hp.com)
printer-ps	Протокол печати PostScript (adobe.com)
quic	UDP-Based Multiplexed and Secure Transport, экспериментальный протокол Google (tools.ietf.org/html/draft-ietf-quic-transport-27)
radius	Remote Authentication Dial In User Service (RFC 2865)
rdp	Remote Desktop Protocol (docs.microsoft.com)
redis	Протокол системы управления базами данных Redis (redis.io)
rexec	Протокол приложения REXEC (ibm.com)
rfb	Remote Framebuffer (RFC 6143)
rlogin	BSD Rlogin (RFC 1282)
rsync	Протокол утилиты rsync (rsync.samba.org)
rtcp	Real-Time Transport Protocol (RFC 3550)
rtsp	Real-Time Streaming Protocol (RFC 7826)
sip	Session Initiation Protocol (RFC 3261)
skinny-voip	Skinny Client Control Protocol (cisco.com)
skype	Протокол программы Skype (skype.com)
smb	Server Message Block (docs.microsoft.com)
smb-mailslot	Server Message Block Mailslot (docs.microsoft.com)
smtp	Simple Mail Transfer Protocol (RFC 5321)
snmp	Simple Network Management Protocol
socks5	SOCKS 5 (RFC 1928)
splunk	Протокол платформы Splunk (splunk.com)
ssdp	Simple Service Discovery Protocol
ssh	Secure Shell (RFC 4251)

Обозначение	Протокол
sstp	Secure Socket Tunneling Protocol — VPN-протокол от Microsoft, который создает защищенные туннели для передачи данных, используя TLS (SSL) (как в HTTPS) через стандартный порт 443
stakhanovets	Протокол DLP-системы компании «Стахановец» (stakhanovets.ru/dlp)
stratum	Протокол майнинга Stratum reference.cash/mining/stratum-protocol)
stun	Session Traversal Utilities for NAT (RFC 3489)
stun-apple	
stun-classic	
syslog	Протокол системного журнала (RFC 5424)
tds	Tabular Data Stream (docs.microsoft.com)
teamviewer	Протокол программы TeamViewer (teamviewer.com)
telnet	Telnet (RFC 854)
tftp	Trivial File Transfer Protocol (RFC 1350)
thrift	Протокол фреймворка Apache Thrift (thrift.apache.org)
tls	Transport Layer Security (RFC 8446)
trueconf	Протокол системы TrueConf (trueconf.ru)
ubiquiti	
umeye-app	Протокол приложения UMEye (umeye.com)
viber	Протокол приложения Viber (viber.com)
vipaks-data	Протокол передачи видео компании «Випакс» (vipaks.ru)
vipnet	Протокол системы ViPNet VPN (infotecs.ru)
vipnet-mftp	
vipnet-sync	
vmware	Протокол компании VMware (vmware.com)
vpn_kontinent	Протокол комплекса шифрования «Континент» (securitycode.ru)
whatsapp	Протокол приложения WhatsApp[5] (whatsapp.com)
wireguard	WireGuard (wireguard.com)
ws-discovery	Web Services Dynamic Discovery (specs.xmlsoap.org)
xmpp	Extensible Messaging and Presence Protocol (xmpp.org)
zabbix	Протокол системы Zabbix (zabbix.com)

Обозначение	Протокол
zmtp	ZeroMQ Message Transport Protocol (zeromq.org)
zmtp_v2	

44. Промышленные протоколы, обнаруживаемые PT NGFW

В таблице ниже перечислены промышленные протоколы, которые PT NGFW может обнаруживать в трафике.

Таблица 22. Обнаруживаемые промышленные протоколы

Протокол	Стандарт, описание
Alpha.Link	Внутренний протокол обмена данными в российской проприетарной платформе автоматизации АСУ ТП «Альфа платформа» от «Атомик Софт»
BACnet	ISO 16484-5, протокол автоматизации управления зданиями
CIP	Спецификации «The CIP Networks Library Volume 1: Common Industrial Protocol (Edition 3.3)» и «The CIP Networks Library Volume 2: EtherNet/IP Adaptation of CIP (Edition 1.4)»
DICOM	National Electrical Manufacturers Association (NEMA). Протокол обработки, хранения, печати и передачи информации в области медицинской визуализации
HART-IP	Промышленный протокол HART-IP (fieldcommgroup.org)
IEC104	IEC 60870-5-104, ГОСТ Р МЭК 60870-5-104-2004
MMS	IEC 61850 MMS, МЭК 61850-8-1
Modbus	MODBUS Application Protocol Specification V1.1b3
MQTT	Упрощенный протокол обмена сообщениями по принципу «издатель — подписчик», используемый в области интернета вещей (IoT) и промышленного интернета вещей (IIoT)
OPC DA	OLE for Process Control Data Access Automation Interface Standard version 2.0
OPC UA	IEC 62541. Платформонезависимый стандарт. Он позволяет системам и устройствам обмениваться данными при помощи клиент-серверной архитектуры или по принципу «издатель — подписчик» в сетях различных типов
S7Comm	Стандарт коммуникационных модулей серий Siemens SIMATIC S7-300/400
S7Comm-Plus	Стандарт коммуникационных модулей серий Siemens SIMATIC S7-1200/1500
UMAS	Расширение протокола Modbus (код функции 90). Протокол используется для сетевого обмена между инженерным ПО компании Unity и контроллерами Modicon компании Schneider Electric

Протокол	Стандарт, описание
Vnet/IP	IEC PAS 62405. Протокол сетевого обмена между оборудованием компании Yokogawa

45. Использование API

В этом разделе приводятся сведения о функциях сервиса API в PT NGFW. Полный список доступных запросов находится по адресу `https://<Адрес системы управления>/apidoc/v2`.

О сервисе API

Взаимодействие между вашим приложением и API продукта происходит по HTTPS. Допустимые методы запросов — GET и POST.

Корневой URL API:

```
https://<Адрес системы управления>/api/v2
```

Например:

```
https://ptngfw.example/api/v2/
```

В ответ на запросы вашего приложения сервис возвращает сообщения в формате JSON.

Авторизация запросов

Запросы к API должны быть авторизованы. Для того чтобы каждый раз не вводить имя пользователя и пароль, вам необходимо использовать токен авторизации. Время жизни токена авторизации — 600 минут.

Метод и URL запроса

POST → `<Корневой URL API>/Login`

Параметры запроса

Отсутствуют.

Тело запроса

В теле запроса должны содержаться параметры `login` и `password` для входа в PT NGFW.

Пример запроса

JSON-структура тела запроса на авторизацию:

```
{
"login": "admin",
"password": "admin"
}
```

Ответ на запрос

В случае успешной авторизации сервис вернет ответ с кодом 200 и токеном авторизации в виде куки для использования в последующих запросах.

В случае неуспешной авторизации сервис вернет сообщение об ошибке.

> **Примечание.** Во всех последующих запросах нужно использовать токен авторизации в заголовке Authorization.

Пример запроса в формате cURL:

```
curl --location 'https://[IP Address]/api/v2/ListLogicalInterfaces' \
--header 'Accept: application/json' \
--header 'Cookie: Authorization=<Токен авторизации>'
--header 'Content-Type:
application/json' \
--data '{
"limit": 10000,
"logicalDeviceId": "01940272-57c6-7b39-8743-b2e4e499e45f"
}'
```

46. Интерфейс командной строки (CLI)

При возникновении сбоев в работе межсетевого экрана для их диагностики может быть использован встроенный интерфейс командной строки (command line interface, или CLI). Он позволяет оперативно проверить сетевую связность, проследить маршруты, проанализировать трафик и оценить текущее состояние системы.

В этом разделе

Вход и работа в CLI (см. раздел 46.1)

Операционные команды (см. раздел 46.2)

46.1. Вход и работа в CLI

Вход в CLI выполняется через выделенный интерфейс управления по протоколу SSH. При подключении необходимо использовать специальный логин, который создается на уровне ОС при ее установке (по умолчанию — `pt-ngfw-core-cli`).

> **Внимание!** По умолчанию у логина `pt-ngfw-core-cli` пустой пароль. Для входа в CLI необходимо сначала сменить пароль на уровне ОС при помощи стандартной утилиты для смены пароля — Passwd.
>
> **Внимание!** При входе в CLI все команды выполняются на уровне устройства с использованием интерфейса управления (MGMT) и не задействуют порты dataplane. Чтобы выполнить команду с портов dataplane (например, `ping` удаленного узла с определенного интерфейса eth1.1), сначала необходимо войти в соответствующий виртуальный контекст (VC).

- Чтобы войти в CLI:

  1. В командной строке введите команду:
     `ssh pt-ngfw-core-cli@<IP-адрес интерфейса управления (MGMT)>`
  2. Введите пароль.

Работа в CLI выполняется на уровне устройства либо на уровне виртуального контекста. Можно переключаться между контекстами и просматривать их список. При входе в CLI пользователь попадает на уровень устройства. Например:

```
pt-ngfw-core-cli@nfgw-msk>
```

В этом примере `pt-ngfw-core-cli` — имя пользователя; `ngfw-msk` — название узла; символ `>` означает, что пользователь находится в операционном режиме. Этот режим используется для просмотра диагностической информации и выполнения различных эксплуатационных команд.

Переход в виртуальный контекст осуществляется при помощи команды `enter <Название виртуального контекста>`. При входе в виртуальный контекст его название будет отображено в приглашении командной строки (в примере ниже — vc). Например:

```
pt-ngfw-core-cli@nfgw-msk> enter context Default
vc: Default
pt-ngfw-core-cli@nfgw-msk>
```

46.2. Операционные команды

В этом разделе описаны операционные команды CLI PT NGFW на уровне устройства и виртуального контекста, их синтаксис и иерархическое представление.

В этом разделе

Синтаксис команд (см. раздел 46.2.1)

Иерархическое представление команд (см. раздел 46.2.2)

Команды на уровне устройства (см. раздел 46.2.3)

Команды на уровне виртуального контекста (см. раздел 46.2.4)

См. также

Зоны безопасности (см. раздел 6.8)

46.2.1. Синтаксис команд

Для описания синтаксиса команд используются условные обозначения, перечисленные ниже.

Таблица 23. Синтаксис команд

Специальные символы	Описание
Угловые скобки `<>`	Содержат текстовую переменную. Например: `show interface <Название интерфейса>`
Фигурные скобки `{}`	Указывают, что параметр обязательный. Например: `show interface {<Название интерфейса>}`
Квадратные скобки `[]`	Указывает, что параметр необязательный. Например: `show session [source address]`

Специальные символы	Описание
Вертикальная черта |	Разделяет альтернативные взаимоисключающие варианты. Например: `clear session {all | id}`
Пробел	Если можно ввести несколько невзаимоисключающих параметров, они разделяются пробелами. Например: `show session [source address] [destination address] [source port] [destination port]`

См. также

Зоны безопасности (см. раздел 6.8)

46.2.2. Иерархическое представление команд

В CLI PT NGFW дерево команд выглядит следующим образом:

```
Device (уровень устройства):
├── exit
├── ping
├── traceroute
├── show
│   ├── version
│   ├── context
│   └── interfaces
└── enter context <Название виртуального контекста>
    Virtual Context (уровень виртуального контекста):
        ├── exit
        ├── ping
        ├── traceroute
        ├── nslookup
        └── show
        │   ├── context
        │   ├── security-rule
        │   ├── session
        │   ├── arp
        │   ├── route
        │   ├── ike
        │   ├── ipsec
        └── packet-capture
            ├── list-all
            ├── session
            └── stopall
```

Примечание. При вводе команд вы можете использовать клавишу Tab для просмотра и автоматического заполнения команд и их аргументов, доступных на текущем уровне.

См. также

Зоны безопасности (см. раздел 6.8)

46.2.3. Команды на уровне устройства

help

Команда выводит на экран список доступных команд. Команда `?` выполняет ту же функцию.

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> ?
Usage:
Hit '<TAB>' to complete arguments or get list of suggestions.

Available commands:
------------------------------------------------------------
Command Description
------------------------------------------------------------
enter enter virtual context
show command show with operational parameters
exit exit CLI session
ping send ICMP ECHO_REQUEST packets to network hosts
traceroute print the route packets trace to network host
Total: 5
```

ping

Проверяет доступность узла. Используется для проверки базовой сетевой связности.

```
ping [source-address <IP-адрес>] [count <Количество пакетов>] [TTL <Время жизни пакета>]
```

Доступные параметры:

- `source-address` — в качестве адреса по умолчанию будет использоваться IP-адрес интерфейса управления (MGMT).
- `count` — количество пакетов. После передачи заданного количества пакетов останавливает выполнение команды `ping`. Диапазон от 1 до 2 000 000 000.
- `ttl` — время жизни пакета IP. Диапазон от 1 до 255.

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> ping 8.8.8.8 count 5
/usr/bin/ping: socket: Address family not supported by protocol
```

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=105 time=21.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=105 time=20.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=105 time=21.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=105 time=20.8 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=105 time=18.3 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 18.257/20.504/21.389/1.139 ms
pt-ngfw-core-cli@pt-ngfw-cli>
```

traceroute

Отслеживает маршрут до удаленного узла, отображая каждый промежуточный узел на пути. Позволяет выявить, на каком участке теряется трафик.

```
traceroute [source-address <IP-адрес>] [TTL <Время жизни пакета>]
```

Доступные параметры:

- `source-address` — в качестве адреса по умолчанию будет использоваться IP-адрес интерфейса управления (MGMT).
- `ttl` — время жизни пакета IP. Диапазон от 1 до 255.

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
1 10.13.107.1 0.944 ms 0.941 ms 0.940 ms
2 188.246.191.161 1.366 ms 1.369 ms 1.368 ms
3 * * *
4 195.94.230.5 2.092 ms 2.129 ms 2.165 ms
5 195.94.233.65 2.806 ms 2.921 ms 2.923 ms
6 * * *
7 195.94.226.198 2.378 ms 2.452 ms 2.469 ms
8 195.94.226.29 1.966 ms 1.972 ms 2.011 ms
9 195.208.209.7 3.502 ms 3.505 ms 3.391 ms
10 * * *
11 1.1.1.1 2.491 ms 2.464 ms 2.505 ms
pt-ngfw-core-cli@pt-ngfw-cli>
```

show context

Позволяет просмотреть список всех созданных виртуальных контекстов.

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> show context
Virtual contexts:
```

```
------------------------------------------------------------
UUID Name
------------------------------------------------------------
{0196e869-1d72-7534-ab4b-a8d0d7ce1e97} Default
{01972feb-e377-7ce3-8363-5f12f984be84} test-virtual-context
Total: 2
pt-ngfw-core-cli@pt-ngfw-cli>
```

enter context <Название виртуального контекста>

Вход в виртуальный контекст (переключение между контекстами).

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> enter context Default
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli>
```

exit

При использовании команды на уровне устройства текущая SSH-сессия завершится.

show interface

Позволяет просмотреть данные об интерфейсах PT NGFW: текущее состояние, статистику и параметры.

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> show interface

Physical interfaces:
------------------------------------------------------------------------------------------
-
Interface Speed Duplex Admin state Link state Mac address MTU
------------------------------------------------------------------------------------------
-
eth1 auto auto n/a up 00:50:56:94:57:b6 1500
eth2 auto auto n/a up 00:50:56:94:5f:9e 1500
eth3 auto auto n/a up 00:50:56:94:32:2a 1500
eth4 auto auto n/a up 00:50:56:94:46:c5 1500
eth5 auto auto n/a up 00:50:56:94:72:22 1500
eth6 auto auto n/a up 00:50:56:94:da:77 1500

Total physical interfaces: 6
Total LAG interfaces: 0

Logical interfaces:
```

```
-------------------------------------------------------------------------------
-------------------------
Interface VLAN ID Mode Virtual Context VR / VWire Zone Admin State Address
-------------------------------------------------------------------------------
-------------------------
eth2.0 Routing Default Default Trusted n/a 10.10.10.1/24
3.3.3.3/32
4.4.4.4/32
eth1.0 Routing Default Default Untrusted n/a 10.13.107.32/24

Total logical interfaces: 2
pt-ngfw-core-cli@pt-ngfw-cli>
```

show version

Позволяет просмотреть текущую версию программного обеспечения и сведения об аппаратной платформе PT NGFW.

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> show version
Model: pt-ngfw-virt
Serial number: pt-ngfw-virt
Product version: 1.7.0
Core version: 3.0.0(12310)
NGFW protocol version: 3.0.15
Acco protocol version: 1.0.0
Compiler: gcc 10.2.1
DPDK version: 21.11.9-2ptngfw
Profile: x86_gcc_generic
Commit: 0c9cc61c5afd005641205d2238fd3ceba4f1613e
Date: 2025-05-20T18:18:53+03:00
pt-ngfw-core-cli@pt-ngfw-cli>
```

См. также

Зоны безопасности (см. раздел 6.8)

46.2.4. Команды на уровне виртуального контекста

help

Команда выводит на экран список доступных команд. Команда `?` выполняет ту же функцию.

Пример вывода:

```
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli> help
Usage:
```

```
Hit '<TAB>' to complete arguments or get list of suggestions.

Available commands:
------------------------------------------------------------
Command Description
------------------------------------------------------------
exit exit virtual context
show command show with operational parameters
ping send ICMP ECHO_REQUEST packets to network hosts
traceroute print the route packets trace to network host
nslookup query Internet name servers
clear
Total: 6
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli>
```

exit

Выход из виртуального контекста на уровень устройства.

Пример вывода:

```
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli> exit
pt-ngfw-core-cli@pt-ngfw-cli>
```

show session

Просмотр всех активных сессий, проходящих через межсетевой экран. Поддерживает фильтрацию по следующим параметрам:

- `source-address <Адрес источника>`;
- `destination-address <Адрес назначения>`;
- `source-port <Номер порта источника>`;
- `destination-port <Номер порта назначения>`;
- `source-zone <Зона безопасности источника>`;
- `destination-zone <Зона безопасности назначения>`;
- `application <Название приложения>`;
- `ip-protocol <Номер IP-протокола от 1 до 255>`;
- `security-rule <Название правила безопасности>`;
- `NAT-applied yes|no` — показывает, применена ли политика NAT к сессии.

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> show session
Displaying sessions for context: "Default"
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Session ID Security Rule Name State Application IP Protocol Src Address [Src Port]
Src Zone (NAT Src Address [Src Port]) Packets/Bytes
Dst Address [Dst Port] Dst Zone (NAT Dst Address [Dst Port])
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
00029323506390986983 Allow any ACTIVE mdns 17 10.10.10.13 [5353] Trusted 1/149
224.0.0.251 [5353] Local
00029323506390986982 Allow any ACTIVE dns 17 10.10.10.13 [56905] Trusted
(10.13.107.32 [41375]) 7/448
10.0.52.101 [53] Untrusted (10.0.52.101 [53])
00029323506390986981 Allow any ACTIVE dns 17 10.10.10.13 [33499] Trusted
(10.13.107.32 [38670]) 9/468
10.0.52.101 [53] Untrusted (10.0.52.101 [53])
00029323506390986980 Allow any ACTIVE dns 17 10.10.10.13 [58472] Trusted
(10.13.107.32 [10592]) 19/836
10.0.52.101 [53] Untrusted (10.0.52.101 [53])
00029323506390986979 Allow any ACTIVE dns 17 10.10.10.13 [41417] Trusted
(10.13.107.32 [59488]) 19/950
10.0.52.101 [53] Untrusted (10.0.52.101 [53])
00029323506390986978 Allow any ACTIVE dns 17 10.10.10.13 [45900] Trusted
(10.13.107.32 [27730]) 21/672
10.0.52.101 [53] Untrusted (10.0.52.101 [53])
00029323506390986977 Allow any ACTIVE dns 17 10.10.10.13 [37780] Trusted
(10.13.107.32 [40154]) 21/672
.............
Total: 42
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli>
```

show security-rule

Просмотр информации о правилах безопасности виртуального контекста.

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> show security-rule
1 ekutumin
2 Allow any
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli>
```

ping

Проверяет доступность узла. Используется для проверки базовой сетевой связности.

Внимание! Команда `ping` на уровне виртуального контекста использует интерфейсы dataplane PT NGFW, в связи с чем для обеспечения работоспособности этой команды необходимо наличие разрешающих правил безопасности и NAT. В качестве зоны источника и (или) зоны назначения вы можете использовать зону Local (см. раздел «Зоны безопасности (см. раздел 6.8)»).

```
ping [source-address <IP-адрес>] [count <Количество пакетов>] [TTL <Время жизни пакета>] [virtual-router <Название виртуального роутера>]
```

Доступные параметры:

- `source-address` — IP-адрес одного из настроенных интерфейсов межсетевого экрана уровня L3. Без указания параметра `source address` по умолчанию будет использоваться IP-адрес исходящего интерфейса, который определяется на основе текущей таблицы маршрутизации. Если указанный IP-адрес не соответствует ни одному интерфейсу, система выдаст ошибку.
- `virtual-router` — название виртуального роутера.
- `count` — количество пакетов. После передачи заданного количества пакетов останавливает выполнение команды `ping`. Диапазон от 1 до 2 000 000 000.
- `ttl` — время жизни пакета IP. Диапазон от 1 до 255.

Пример вывода:

```
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli> ping 8.8.8.8 source-address 10.10.10.1
/usr/bin/ping: socket: Address family not supported by protocol
PING 8.8.8.8 (8.8.8.8) from 10.10.10.1 vctx0-vrf0: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=105 time=27.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=105 time=18.6 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 18.608/23.230/27.853/4.622 ms
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli> ping 8.8.8.8
/usr/bin/ping: socket: Address family not supported by protocol
/usr/bin/ping: Warning: source address might be selected on device other than: vctx0-vrf0
PING 8.8.8.8 (8.8.8.8) from 10.13.107.32 vctx0-vrf0: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=9 ttl=105 time=18.7 ms
^C
--- 8.8.8.8 ping statistics ---
9 packets transmitted, 1 received, 88.8889% packet loss, time 8181ms
rtt min/avg/max/mdev = 18.739/18.739/18.739/0.000 ms
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli>
```

show arp

Команда `show arp` используется для вывода таблицы, содержащей ARP-записи (IP-адреса в сопоставлении с MAC-адресами) в рамках виртуального контекста, в котором находится пользователь. Команда имеет необязательный параметр `interface <Название интерфейса>`, при использовании которого выводятся ARP-записи, относящиеся только к указанному интерфейсу.

Пример вывода (без параметра `interface`):

```
vc: Default
pt-ngfw-core-cli@ngfw> show arp
Displaying ARP table for context: "Default"
maximum of entries supported: unlimited
default timeout : 1200 seconds
total ARP entries in table : 3
------------------------------------------------------------------------------
interface ip-address mac-address status virtual-router
------------------------------------------------------------------------------
eth1-1.0 10.13.107.2 00:00:00:00:00:00 incomplete Default
eth1-2.0 10.10.10.250 0E:00:5E:00:00:0C complete Default
eth1-2.0 10.10.10.11 00:50:56:94:3D:00 complete Default
vc: Default
pt-ngfw-core-cli@ngfw>
```

Пример вывода (с параметром `interface`):

```
vc: Default
pt-ngfw-core-cli@ngfw> show arp interface eth1-1.0
Displaying ARP table for context: "Default"
maximum of entries supported: unlimited
default timeout : 1200 seconds
total ARP entries in table : 1
------------------------------------------------------------------------------
interface ip-address mac-address status virtual-router
------------------------------------------------------------------------------
eth1-1.0 10.13.107.2 00:00:00:00:00:00 incomplete Default
vc: Default
pt-ngfw-core-cli@ngfw>
```

show route

Команда `show route` используется для вывода таблицы маршрутизации PT NGFW. Она позволяет просмотреть активные маршруты, через которые осуществляется передача данных в сети.

Доступные параметры:

— `bgp` — вывод RIB-таблицы по протоколу BGP;

— `ospf` — вывод RIB-таблицы по протоколу OSPF;

— `static` — вывод RIB-таблицы для статических маршрутов;

— `connected` — вывод RIB-таблицы для связанных маршрутов;

— `virtual-router <Название виртуального роутера>` — вывод RIB-таблицы по указанному виртуальному роутеру.

Пример вывода:

```
vc: Default
pt-ngfw-core-cli@ngfw> show route
Codes: K - kernel route, C - connected, L - local, S - static,
       R - RIP, O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric, t - Table-Direct,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

VRF vctx0-vrf0:
S>* 0.0.0.0/0 [1/0] via 10.13.107.1, eth1-1, weight 1, 22:34:35
  *                 via 10.13.107.2, eth1-1, weight 1, 22:34:35
  *                 via 10.13.107.107, eth1-1, weight 1, 22:34:35
C>* 10.10.10.0/24 is directly connected, eth1-2, 22:34:35
L>* 10.10.10.1/32 is directly connected, eth1-2, 22:34:35
C>* 10.13.107.0/24 is directly connected, eth1-1, 22:34:35
L>* 10.13.107.39/32 is directly connected, eth1-1, 22:34:35

VRF vctx0-vrf1:
C>* 5.5.5.0/24 is directly connected, eth1-3, 22:34:35
L>* 5.5.5.5/32 is directly connected, eth1-3, 22:34:35
C>* 7.7.7.0/24 is directly connected, eth1-6, 22:34:35
L>* 7.7.7.7/32 is directly connected, eth1-6, 22:34:35
```

Примечание. В настоящий момент в выводе команды `show route` отображаются внутренние названия VRF. Применять фильтры необходимо используя исходные названия VRF, заданные в системе управления, список которых можно просмотреть в подсказке к параметру `virtual-router` с помощью клавиши Tab или введя `?`. Например:

```
vc: Default
pt-ngfw-core-cli@ngfw> show route virtual-router ?
Default
VRF-2
```

traceroute

Отслеживает маршрут до удаленного узла, отображая каждый промежуточный узел на пути. Позволяет выявить, на каком участке теряется трафик.

> **Внимание!** Команда `traceroute` на уровне виртуального контекста использует интерфейсы dataplane PT NGFW, в связи с чем для обеспечения работоспособности этой команды необходимо наличие разрешающих правил безопасности и NAT. В качестве зоны источника и (или) зоны назначения вы можете использовать зону Local (см. раздел «Зоны безопасности (см. раздел 6.8)»).

```
traceroute [source-address <IP-адрес>] [TTL <Время жизни пакета>] [virtual-router
<Название виртуального роутера>]
```

Доступные параметры:

- `source-address` — IP-адрес одного из настроенных интерфейсов межсетевого экрана уровня L3. Без указания параметра `source address` по умолчанию будет использоваться IP-адрес исходящего интерфейса, который определяется на основе текущей таблицы маршрутизации. Если указанный IP-адрес не соответствует ни одному интерфейсу, система выдаст ошибку.
- `virtual-router` — название виртуального роутера.
- `ttl` — время жизни пакета IP. Диапазон от 1 до 255.

Пример вывода:

```
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli> traceroute 1.1.1.1
traceroute to 1.1.1.1 (1.1.1.1), 30 hops max, 60 byte packets
1 10.13.107.1 0.846 ms 0.833 ms 0.829 ms
2 188.246.191.161 1.115 ms 1.114 ms 1.112 ms
3 85.249.7.73 1.645 ms 1.644 ms *
4 195.94.230.5 1.637 ms 1.634 ms 1.630 ms
5 195.94.233.65 2.660 ms 2.658 ms 2.919 ms
6 * * *
7 195.94.226.198 2.910 ms 2.687 ms 2.682 ms
8 195.94.226.29 16.686 ms 16.200 ms 16.194 ms
9 195.208.209.7 13.149 ms 13.149 ms 13.647 ms
10 172.68.8.49 3.351 ms 3.607 ms 3.350 ms
11 1.1.1.1 3.341 ms 3.340 ms 3.337 ms
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli>
```

nslookup

Запрос к DNS-серверу и получение информации о доменном имени или IP-адресе. В качестве DNS-сервера на уровне виртуального контекста используется сервер, указанный в файле конфигурации `/opt/pt-ngfw/ngfw-core/etc/config/pt-ngfw.conf` в секции `dns_resolver`.

Пример вывода:

```
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli> nslookup ya.ru
Name: ya.ru
Addresses:
77.88.44.242
5.255.255.242
77.88.55.242
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli>
```

clear session

Сброс сессий, проходящих через межсетевой экран.

Доступные параметры:

— `id` — сброс сессии по уникальному идентификатору сессии (см. show session (см. раздел 46.2.4)).

— `all` — сброс всех установленных сессий.

Пример вывода:

```
pt-ngfw-core-cli@pt-ngfw-cli> show session destination-port 5000
Displaying sessions for context: "Default"
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Session ID Security Rule Name State Application IP Protocol Src Address [Src Port]
Src Zone (NAT Src Address [Src Port]) Packets/Bytes
Dst Address [Dst Port] Dst Zone (NAT Dst Address [Dst Port])
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
0002934094863899039 8 Allow any ACTIVE unknown 6 10.10.10.13 [54848] Trusted
(10.13.107.32 [14013]) 39/5875
54.39.129.129 [5000] Untrusted (54.39.129.129 [5000])
Total: 1
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli> clear session id 00029340948638990398
Total sessions cleared: 1
vc: Default
pt-ngfw-core-cli@pt-ngfw-cli>
```

packet-capture

Команда используется для захвата трафика, проходящего через межсетевой экран. Основные возможности:

— Администратор может указать параметры для фильтрации захватываемого трафика, такие как название интерфейса, источник, назначение, протокол, направление трафика. Параметры фильтрации могут быть указаны в произвольном порядке.

— Каждый фильтр задается с помощью отдельного вызова команды с указанием сессии, для которой он применяется. В сессии захвата трафика можно задать от 1 до 4 фильтров. Если в сессии не задано ни одного фильтра, будет выполняться захват всего трафика в текущем виртуальном контексте.

— Продолжительность работы сессии захвата трафика ограничена по времени: при запуске команды указывается время, по истечении которого захват трафика останавливается (максимум — 7 дней).

— Результаты захвата могут записываться в файл (несколько файлов) в формате PCAPNG. Файлы с результатами захвата сохраняются на межсетевом экране в каталоге `/opt/pt-ngfw/ngfw-core/<Название каталога хранения журналов>/PCAP/<Название виртуального контекста, в котором запущена команда захвата трафика>/<Название файла>`. Например: `/opt/pt-ngfw/ngfw-core/logs/PCAP/Default/pcap1`.

— Сессию можно принудительно остановить с помощью команды `stop` (`stop-all`).

— Объем отдельного файла для записи ограничен заданным значением. При отключенной ротации достижение этого размера приводит к завершению сессии захвата трафика. Максимально возможный размер файла — 2048 МБ.

— При включенной ротации создаются файлы с постфиксами (например, `<Название файла-1>.pcapng`, `<Название файла-2>.pcapng` и так далее). При достижении предельного размера файла запись продолжается в следующий файл. При достижении заданного количества файлов (от 2 до 10) запись в файл с наименьшим постфиксом возобновляется, его содержимое перезаписывается, а ротация продолжается по кругу.

Доступные параметры:

— `help|?` — просмотр справки по команде;

— `session <Номер сессии от 1 до 5>}` — выбор сессии packet-capture для настройки и старта (остановки). Используется с одной из следующих опций:

  • `filter <Номер фильтра от 1 до 4>` — настройка фильтров, доступны следующие опции фильтров:

    • `[interface <Название интерфейса>]` — название интерфейса, на котором выполняется захват трафика;

    • `[source-address <Адрес источника>]` — адрес источника;

    • `[destination-address <Адрес назначения>]` — адрес назначения;

    • `[source-port <Порт источника>]` — порт источника;

- [destination-port <Порт назначения>] — порт назначения;
- [protocol {ID протокола от 1 до 255}] — ID протокола от 1 до 255. Подробнее см. https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
- [direction <send | receive | send+receive>] — выбор направления трафика (исходящий, входящий или оба направления);

- clear-filter <Номер фильтра от 1 до 4> — сброс настройки фильтров;
- clear-filter-all — сброс настройки всех фильтров сессии;
- start — запуск сессии захвата трафика. Может быть использована со следующими опциями:
  - [count <Число>] — ограничение количества захватываемых пакетов;
  - [filename <file_name>] — сохранение данных о захватываемом трафике в файл, используется с опциями {filesize <Максимальный размер файла в МБ>}, {duration <Длительность захвата в формате 0-7d 0-24H 0-60m 0-60s>} и [filerotation <Количество файлов для ротации от 2 до 10>];

    Примечание. Опции file_name и filesize являются обязательными.
- stop — остановка сессии захвата трафика;
- list — просмотр параметров сессии;

— stop-all — остановка всех сессий захвата трафика в текущем виртуальном контексте;

— list-all — просмотр параметров всех сессий захвата трафика в текущем виртуальном контексте;

Примеры использования packet-capture:

1. Захват 1000 пакетов с узла 10.10.10.10 на интерфейсе eth1-1.0 с портом назначения 443 с записью в файл размером до 200 МБ и длительностью 8 часов:
```
packet-capture session 1 filter 1 interface eth1-1.0 source-address
10.10.10.10 destination-port 443
packet-capture session 1 start count 1000 filename web-10-10-10-10 filesize
200 duration 8h
```
2. Захват всего входящего и исходящего трафика на интерфейсе eth1-1.0 с записью в файлы по 500 МБ, ротацией до четырёх файлов и длительностью один день (24 часа):
```
packet-capture session 2 filter 1 interface eth1-1.0 direction send+receive
packet-capture session 2 start filename dmz-eth1 filesize 500 filerotation 4
duration 1d
```
3. Захват трафика между узлами 10.10.10.10 и 20.20.20.20 по порту 3389 в обоих направлениях, с ограничением по длительности 15 минут и максимальным размером файла 300 МБ:
```
packet-capture session 3 filter 1 source-address 10.10.10.10 destination-
address 20.20.20.20 destination-port 3389
packet-capture session 3 filter 2 source-address 20.20.20.20 destination-
address 10.10.10.10 source-port 3389
packet-capture session 3 start filename s3 duration 15m filesize 300
```

show ike sa

Просмотр текущих IKE SA (Internet Key Exchange Security Association).

Синтаксис:

```
show ike sa [local-address {<IP-address> | <FQDN>}] [peer-address {<IP-address>
| <FQDN>}] [tunnel {<tunnel-name>}]
```

Доступные параметры:

- `local-address {<IP-адрес> | <FQDN>}` — IP-адрес или FQDN локального межсетевого экрана, с которого было установлено IKE-соединение с удаленной стороной.
- `peer-address {<IP-адрес> | <FQDN>}` — IP-адрес или FQDN удаленного пира.
- `tunnel {<Название туннеля>}` — название IPSec соединения (туннеля).

При вызове команды без параметров отображаются все текущие IKE SA в виде краткой таблицы. При указании параметров вывод фильтруется по заданным значениям; параметры могут использоваться по отдельности или в различных комбинациях.

Примеры вывода:

```
vc: Default
pt-ngfw-core-cli@ngfw> show ike sa local-address 10.13.107.32
------------------------------------------------------------------------------
-------------
tunnel local address peer address status initiator
------------------------------------------------------------------------------
-------------
{019bc6df-97e3-7e29-a480-db124b14a2aa} 10.13.107.32 10.13.107.143 CONNECTED true


vc: Default
pt-ngfw-core-cli@ngfw> show ike sa peer-address 10.13.107.143
------------------------------------------------------------------------------
-------------
tunnel local address peer address status initiator
------------------------------------------------------------------------------
-------------
{019bc6df-97e3-7e29-a480-db124b14a2aa} 10.13.107.32 10.13.107.143 CONNECTED true


vc: Default
pt-ngfw-core-cli@ngfw> show ike sa tunnel "IPSec Tunnel with 3rd party NGFW"
------------------------------------------------------------------------------
-------------
tunnel local address peer address status initiator
------------------------------------------------------------------------------
-------------
{019bc6df-97e3-7e29-a480-db124b14a2aa} 10.13.107.32 10.13.107.143 CONNECTED true
```

show ipsec sa

Просмотр текущих IPSec SA (IPSec Security Association).

Синтаксис:

```
show ipsec sa [local-address {<IP-address> | <FQDN>}] [peer-address {<IP-address> | <FQDN>}] [tunnel {<tunnel-name>}]
```

Доступные параметры:

- `local-address {<IP-адрес> | <FQDN>}` — IP-адрес или FQDN локального межсетевого экрана, с которого было установлено IKE-соединение с удаленной стороной.
- `peer-address {<IP-адрес> | <FQDN>}` — IP-адрес или FQDN удаленного пира.
- `tunnel {<Название туннеля>}` — название IPSec соединения (туннеля).

При вызове команды без параметров отображаются все текущие IPSec SA в виде краткой таблицы. При указании параметров вывод фильтруется по заданным значениям; параметры могут использоваться по отдельности или в различных комбинациях.

Примеры вывода:

```
vc: Default
pt-ngfw-core-cli@ngfw> show ipsec sa local-address 10.13.107.32
-------------------------------------------------------------------------------------------
-----------
spi encryption authentication life (sec/bytes) local address peer address
-------------------------------------------------------------------------------------------
-----------
0xbf37e4c1 AES_CBC128 SHA512_256 26860/0 10.13.107.32 10.13.107.143


vc: Default
pt-ngfw-core-cli@ngfw> show ipsec sa peer-address 10.13.107.143
-------------------------------------------------------------------------------------------
-----------
spi encryption authentication life (sec/bytes) local address peer address
-------------------------------------------------------------------------------------------
-----------
0xbf37e4c1 AES_CBC128 SHA512_256 26876/0 10.13.107.32 10.13.107.143


vc: Default
pt-ngfw-core-cli@ngfw> show ipsec sa tunnel "IPSec Tunnel with 3rd party NGFW"
-------------------------------------------------------------------------------------------
-----------
spi encryption authentication life (sec/bytes) local address peer address
-------------------------------------------------------------------------------------------
-----------
0xbf37e4c1 AES_CBC128 SHA512_256 28465/0 10.13.107.32 10.13.107.143
```

clear ike sa

Команда используется для принудительного удаления IKE SA.

Синтаксис:

```
clear ike sa [{all} | {peer-address {<IP-address> | <FQDN>}} | tunnel {<tunnel-name>}]
```

Доступные параметры:

— `all` — удаление всех IKE SA.

— `peer-address {<IP-адрес> | <FQDN>}` — удаление IKE SA, связанных с указанным пиром.

— `tunnel {<название туннеля>}` — удаление IKE SA, относящихся к указанному IPSec туннелю.

Администратор может удалить либо все IKE SA (с опцией `all`), либо выборочно по одному из параметров `peer-address` или `tunnel`. При удалении IKE SA в адрес удаленного пира отправляется сообщение DELETE с запросом на удаление соответствующей SA.

clear ipsec sa

Команда используется для принудительного удаления IPSec SA.

Синтаксис:

```
clear ipsec sa [{all} | {peer-address {<IP-address> | <FQDN>}} | tunnel {<tunnel-name>}]
```

Доступные параметры:

— `all` — удаление всех IPSec SA.

— `peer-address {<IP-address> | <FQDN>}` — удаление IPSec SA, связанных с указанным удаленным пиром.

— `tunnel {<tunnel-name>}` — удаление IPSec SA, относящихся к указанному IPSec туннелю.

Администратор может удалить либо все IPSec SA (с опцией `all`), либо выборочно по одному из параметров `peer-address` или `tunnel`. При удалении IPSec SA в адрес удаленного пира отправляется сообщение DELETE с запросом на удаление соответствующей SA.

47. Получение телеметрии

Вы можете получить телеметрию межсетевого экрана, обратившись к локальному HTTPS-сервису, возвращающему данные телеметрии в формате JSON. Телеметрия доступна по адресу https://server-address/stats, где server-address — IP-адрес MGMT-интерфейса межсетевого экрана.

Взаимодействие с HTTPS-сервисом осуществляется с использованием взаимной TLS-аутентификации (mTLS). Это означает, что запрос клиента должен содержать клиентский сертификат и приватный ключ от этого сертификата.

> **Примечание.** Вы можете использовать либо предустановленные сертификаты (находятся по пути `/opt/pt-ngfw/ngfw-tools/certs/`), либо собственные.

Пример curl-запроса

```
curl -k --cert client.crt --key client.key https://server-address/stats
```

В примере выше `--cert client.crt` означает клиентский сертификат, `--key client.key` — ключ к клиентскому сертификату, `-k` — отключение проверки доверия к сертификату сервера, что может потребоваться при использовании самоподписанных сертификатов.

Пример curl-запроса для быстрой проверки: `curl -k --cert client.crt --key client.key https://localhost/stats | head`.

Пример curl-запроса с использованием jq: `curl -k --cert client.crt --key client.key https://localhost/stats | jq`.

Типовые проблемы и диагностика

- **TLS handshake failed.** Наиболее частая причина проблемы — неверный сертификат или закрытый ключ или отсутствие клиентского сертификата.
- **Ошибка 404.** Убедитесь, что указан корректный URL.
- **Нет доступа к файлу закрытого ключа.** Проверьте права доступа файла закрытого ключа и пользователя, от которого запускается обращение.

48. Часто используемые команды

В разделе приведены команды, часто используемые в терминале межсетевого экрана. Для доступа к терминалу необходимо подключиться к межсетевому экрану по протоколу SSH.

Команды настройки маршрутизации FRR

— Отображение сводки информации о протоколе BGP на всех виртуальных роутерах межсетевого экрана. Вывод команды включает общее количество BGP-соседей, количество активных маршрутов, количество принятых префиксов и другие сводные данные о состоянии протокола BGP на различных виртуальных роутерах:
```
sudo vtysh -c 'show ip bgp vrf all summary'
```

— Отображение информации об IP-маршрутах всех виртуальных роутеров межсетевого экрана. Вывод команды включает информацию о прямых подключениях, статических и динамических маршрутах, которые могут быть размещены на различных виртуальных роутерах:
```
sudo vtysh -c 'show ip route vrf all'
```

— Отображение информации о состоянии протокола BGP на всех виртуальных роутерах межсетевого экрана. Вывод команды включает информацию о BGP-соседях, принятых и отправленных маршрутах, атрибутах маршрутов и других связанных с BGP данных для каждого виртуального роутера:
```
sudo vtysh -c 'show ip bgp vrf all'
```

— Отображение информации о соседях OSPF на всех виртуальных роутерах межсетевого экрана:
```
sudo vtysh -c 'show ip ospf vrf all neighbor'
```

— Отображение информации о состоянии OSPF на всех виртуальных роутерах межсетевого экрана:
```
sudo vtysh -c 'show ip ospf vrf all'
```

— Отображение информации о текущей конфигурации межсетевого экрана:
```
sudo vtysh -c 'show run'
```

— Отображение информации о созданных списках префиксов:
```
sudo vtysh -c 'show ip prefix-list'
```

— Запуск командной оболочки FRR в интерактивном режиме:
```
sudo vtysh
```

Внимание. Работа с FRR в интерактивном режиме может вызывать перебои в работе динамической маршрутизации, поэтому используйте его только в случае необходимости.

Команды просмотра информации об устройстве и настройках сети

— Просмотр версии межсетевого экрана:

```
/opt/pt-ngfw/ngfw-core/bin/pt-ngfw --version
```

— Просмотр информации о состоянии интерфейсов:
```
cat /opt/pt-ngfw/ngfw-core/stats/debug.info
```

— Просмотр состояния сетевых интерфейсов в dataplane:
```
grep link_status /opt/pt-ngfw/ngfw-core/stats/ngfw.stat
```

Пример вывода команды:
```
/drm/devices/eth1-1/link_status: 1
/drm/devices/eth1-2/link_status: 0
```

Состояние `1` — интерфейс включен, `0` — отключен.

— Просмотр адресов интерфейсов dataplane межсетевого экрана:
```
sudo ip netns exec ngfwns ip -br a
```

— Просмотр таблицы маршрутов межсетевого экрана:
```
sudo ip netns exec ngfwns ip r s t 0
```

— Просмотр таблицы ARP для интерфейсов dataplane:
```
sudo ip netns exec ngfwns ip neigh
```

Команды, выполняемые в пространстве имен ngfwns

— Вызов командной оболочки Bash в сетевом пространстве имен `ngfwns`. Необходимо для последующего выполнения команд в контексте этого пространства имен:
```
sudo ip netns exec ngfwns bash
```

— Просмотр сетевых интерфейсов и их IP-адресов:
```
ip a
```

— Просмотр трафика, предназначенного только для межсетевого экрана (транзитный трафик, проходящий через межсетевой экран, не отображается):
```
tcpdump -i vdeth1-4
```

— Запуск трассировки маршрута:
```
traceroute -i vdeth1-4 8.8.8.8
```

— Проверка доступности узла:
```
ping -I vdeth1-4 8.8.8.8
```

49. О технической поддержке PT NGFW

В рамках технической поддержки Positive Technologies Next Generation Firewall специалисты Positive Technologies:

— не производят первичную или повторную установку и (или) настройку продукта;

— не решают проблемы с инфраструктурой заказчика или сторонним программным обеспечением;

— не проводят доработку, модификацию, разработку любого программного обеспечения или иных продуктов по запросам заказчика;

— не предоставляют информацию о сроках выхода новых версий программного обеспечения;

— не обучают специалистов заказчика принципам, алгоритмам и методам, лежащим в основе работы PT NGFW.

Техническая поддержка PT NGFW вида Advanced включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления ПО PT NGFW выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта.

Positive Technologies не производит установку обновлений продукта в рамках технической поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

> **Примечание.** Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Консультации по работе и настройке продукта

Вы можете обратиться в техническую поддержку с вопросами, возникающими в процессе эксплуатации PT NGFW. Для этого необходимо максимально подробно описать возникшую проблему. Специалисты Positive Technologies изучат ваш вопрос и текущие конфигурационные

параметры продукта, ответят на вопросы, связанные с использованием продукта, и по возможности предоставят рекомендации по настройке необходимых параметров PT NGFW. Для получения услуги продукт должен быть внедрен и находиться в промышленной эксплуатации.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо доработок. Если Positive Technologies принимает решение о доработке продукта, то способы и сроки ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются на портале технической поддержки.

Портал технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к порталу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения гарантийной поддержки необходимо оставить заявку на портале технической поддержки и предоставить следующие данные:

- номер лицензии на использование продукта;
- серийные номера PT NGFW;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Техническая поддержка оказывается удаленно, онлайн.

Услуги по технической поддержке PT NGFW оказываются в отношении поддерживаемых версий ПО PT NGFW и аппаратных платформ PT NGFW. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном сайте Positive Technologies.

Специалист технической поддержки вправе в ответ на заявку запросить дополнительную информацию. Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по инициативе заказчика при условии предоставления запрошенной ранее информации. Positive Technologies не берет на себя обязательств по оказанию услуг технической поддержки в случае отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

В соответствии с уровнем значимости и графиком обслуживания по заявке определяется время реакции на заявку и осуществляется ее обработка.

Время первичной реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время первичной реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 24. Время реакции и приоритизация заявок

Уровень значимости заявки	Критерии значимости заявки	График обслуживания	Время первичной реакции на заявку
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие	Круглосуточно	До 1 часа

Уровень значимости заявки	Критерии значимости заявки	График обслуживания	Время первичной реакции на заявку
	критически значимое влияние на бизнес заказчика		
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	Круглосуточно	До 2 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта, либо не оказывающие значительного влияния на бизнес заказчика	По рабочим дням с 9:00 до 18:00 UTC+3	До 4 рабочих часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	По рабочим дням с 9:00 до 18:00 UTC+3	До 6 рабочих часов

Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Для оперативного рассмотрения заявок с уровнями значимости «Критический» и «Высокий» специалисты заказчика должны быть готовы круглосуточно предоставлять данные, которые требуются специалистам технической поддержки Positive Technologies для диагностики и устранения заявленного сбоя.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

— о ходе диагностики по заявленной проблеме и ее результатах;

— планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление (с учетом релизного цикла ПО PT NGFW, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект ПО PT NGFW, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления ПО PT NGFW;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как функциональность, неподдерживаемая PT NGFW;
- для продукта, поставляемого в виде программно-аппаратного комплекса (ПАК PT NGFW), предоставлено оборудование или компоненты ПАК PT NGFW взамен вышедших из строя (подробно — в разделе «Условия замены оборудования ПАК PT NGFW»).

Условия замены оборудования ПАК PT NGFW

Если работоспособность аппаратных компонентов ПАК PT NGFW ограничена или нарушена, Positive Technologies производит упреждающую (до получения неисправных деталей от заказчика) замену оборудования, входящего в состав ПАК PT NGFW или его компонентов в рамках сертификата на техническую поддержку уровня Advanced NCD. Positive Technologies переходит к процессу замены неисправного оборудования (компонентов) после того, как специалисты технической поддержки в рамках обработки заявки подтвердят наличие неисправности аппаратных компонентов ПАК PT NGFW. Полный перечень условий замены оборудования приведен в тексте сертификата технической поддержки Advanced NCD.

Замена оборудования и компонентов осуществляется на следующих условиях:

- Доставка оборудования осуществляется в пределах Российской Федерации.
- Если Positive Technologies принимает решение о необходимости замены оборудования до 15:00 UTC+3 текущего дня, то по г. Москве доставка осуществляется не позднее календарного дня, следующего за днем принятия решения о замене. За пределы г. Москвы отправка оборудования осуществляется курьерской службой не позднее календарного дня, следующего за днем принятия решения о замене (срок доставки оговаривается отдельно).
- Если Positive Technologies принимает решение о необходимости замены оборудования после 15:00 UTC+3 текущего дня, то по г. Москве доставка осуществляется не позднее двух календарных дней с даты принятия решения о замене. За пределы г. Москвы отправка оборудования осуществляется курьерской службой не позднее двух календарных дней с даты принятия решения о замене (срок доставки оговаривается отдельно).

— Точный адрес доставки заказчик указывает в заявке. Адрес может быть изменен по согласованию с Positive Technologies.

— По запросу заказчика доставка может быть перенесена на более поздний срок. В этом случае специалисты Positive Technologies согласовывают с заказчиком новые сроки и указывают их в заявке.

— Positive Technologies оставляет за собой право предоставлять заказчику отдельные компоненты взамен вышедших из строя (без замены оборудования целиком). К таким компонентам в зависимости от конкретной модели ПАК PT NGFW могут относиться блоки питания, вентиляторные модули, жесткие диски, сетевые карты и т. д.

— Передаваемое заказчику оборудование (компоненты) сопровождается необходимыми документами, подписанными со стороны Positive Technologies и по форме Positive Technologies.

— В дату и по адресу доставки заказчик обязан провести приемку переданных устройств, подписать и передать Positive Technologies необходимые документы.

— Заказчик должен вернуть неисправное оборудование: не позднее 10 рабочих дней после получения замены подготовить и упаковать неисправное оборудование (в максимально полной комплектации, включая упаковку) и все необходимые документы, оставить заявку на портале и согласовать дату, время и адрес встречи с представителями Positive Technologies.

— Транспортировка оборудования и компонентов осуществляется силами и за счет Positive Technologies. При несоблюдении условий возврата оборудования или отказе от его возврата Positive Technologies вправе потребовать от заказчика полного возмещения убытков, причиненных в связи с этим.

— Positive Technologies оставляет за собой право отказать в замене неисправного оборудования (компонентов) или произвести замену за отдельную плату, например в следующих случаях:

  - при несоблюдении условий эксплуатации, хранения;
  - при наличии следов неосторожного использования, постороннего вмешательства или несанкционированного ремонта;
  - в случае, если неисправности в оборудовании (компонентах) возникли до начала действия обязательств Positive Technologies по замене;
  - в случае, если заводская маркировка или серийный номер повреждены, неразборчивы, имеют следы переклеивания или отсутствуют.

В случае реализации услуги по ремонту или замене оборудования (компонентов) сертификат Advanced NCD продолжает действовать в отношении оборудования (компонентов), предоставленного заказчику в рамках соответствующего ремонта (замены) на указанных в нем условиях.



positive technologies

Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.