ФАКЕЛ

ДОКУМЕНТАЦИЯ ПРОДУКТА

РУКОВОДСТВО АДМИНИСТРАТОРА

Маршрутизатор «Факел»

ВЕРСИЯ ДОКУМЕНТАЦИИ

2.1

ООО «ИТ Роут» fakel.io

Оглавление

1 Быстрый старт **1**

1.1 Введение . . . 2
1.2 Установка ПО Факел . . . 3
1.2.1 Установка ПО Факел на аппаратную платформу . . . 3
1.2.2 Установка **ПО Факел** на виртуальную платформу . . . 5
1.3 Подключение к устройству . . . 7
1.3.1 Доступ по SSH . . . 7
1.4 Командная строка . . . 8
1.4.1 Режимы работы командной строки . . . 8
1.4.2 Применение и сохранение конфигурации . . . 8
1.5 Учетные записи . . . 9
1.6 Сетевые интерфейсы и маршрутизация . . . 10
1.7 Правила фильтрации (Firewall) . . . 11
1.8 Правила трансляции (NAT) . . . 13
1.9 DNS, NTP и DHCP сервисы . . . 14

2 Руководство Администратора **16**

2.1 Командная строка . . . 17
2.1.1 Режим Администрирования . . . 18
2.1.2 Режим Конфигурирования . . . 20
2.1.2.1 Работа в режиме Конфигурирования . . . 20
2.1.2.2 Доступ к командам режима Администрирования через режим Конфигурирования . . . 22
2.2 Сетевые интерфейсы . . . 39
2.2.1 Интерфейс Ethernet . . . 40
2.2.1.1 Обзор . . . 40
2.2.1.2 Пример настройки . . . 41
2.2.1.3 Список команд . . . 41
2.2.2 Агрегированный интерфейс . . . 100
2.2.2.1 Обзор . . . 100
2.2.2.2 Пример настройки . . . 100
2.2.2.3 Список команд . . . 100
2.2.3 Интерфейс сетевого моста . . . 141
2.2.3.1 Обзор . . . 141
2.2.3.2 Пример настройки . . . 141
2.2.3.3 Список команд . . . 142

2.2.4 Интерфейс Loopback . . . 185
2.2.4.1 Обзор . . . 185
2.2.5 Интерфейс Dummy . . . 191
2.2.5.1 Обзор . . . 191
2.2.6 Интерфейс L2TPv3 . . . 198
2.2.6.1 Обзор . . . 198
2.2.6.2 Пример настройки . . . 199
2.2.6.3 Список команд . . . 199
2.2.7 Интерфейс туннеля . . . 215
2.2.7.1 Обзор . . . 215
2.2.7.2 Пример настройки . . . 216
2.2.7.3 Список команд . . . 216
2.2.8 Интерфейс WireGuard . . . 247
2.2.8.1 Обзор . . . 247
2.2.8.2 Пример настройки . . . 248
2.2.8.3 Список команд . . . 249
2.2.9 OpenVPN . . . 269
2.2.9.1 Описание . . . 269
2.2.9.2 Настройка . . . 270
2.2.10 PPoE интерфейс . . . 278
2.2.10.1 Описание . . . 278
2.2.10.2 Настройка . . . 280
2.2.10.3 Список команд . . . 281
2.2.11 VTI интерфейс . . . 285
2.2.11.1 Список команд . . . 285
2.3 Маршрутизация . . . 286
2.3.1 Статические маршруты . . . 287
2.3.1.1 Описание . . . 287
2.3.1.2 Список команд . . . 287
2.3.2 Динамическая маршрутизация . . . 290
2.3.2.1 OSPF . . . 291
2.3.2.2 BGP . . . 310
2.3.2.3 IS-IS . . . 333
2.3.2.4 RIP . . . 339
2.3.2.5 Групповая рассылка . . . 344
2.3.2.6 BFD . . . 350
2.3.3 Политика маршрутизации . . . 353
2.3.3.1 Описание . . . 353
2.3.3.2 Настройка . . . 353
2.3.3.3 Список команд . . . 354
2.3.4 MPLS . . . 358
2.3.4.1 Описание . . . 358
2.3.4.2 Настройка . . . 359
2.3.4.3 Список команд . . . 359
2.3.5 Виртуальная маршрутизация . . . 363
2.3.5.1 Описание . . . 363
2.3.5.2 Настройка . . . 363

2.3.5.3 Список команд . . . 365
2.4 Защищенные коммуникации . . . 371
2.4.1 Стек протоколов IPsec . . . 372
2.4.1.1 Описание . . . 372
2.4.1.2 Настройка . . . 372
2.4.1.3 Список команд . . . 375
2.4.2 Сервер L2TP . . . 377
2.4.2.1 Описание . . . 377
2.4.2.2 Настройка . . . 377
2.4.2.3 Список команд . . . 379
2.4.3 Сервер OpenConnect . . . 383
2.4.3.1 Описание . . . 383
2.4.3.2 Настройка . . . 383
2.4.3.3 Список команд . . . 384
2.4.4 Сервер PPTP . . . 385
2.4.4.1 Описание . . . 385
2.4.4.2 Настройка . . . 385
2.4.4.3 Список команд . . . 386
2.4.5 Ключевая схема RSA . . . 387
2.4.5.1 Описание . . . 387
2.4.5.2 Настройка . . . 387
2.4.5.3 Список команд . . . 388
2.4.6 Сервер SSTP . . . 390
2.4.6.1 Описание . . . 390
2.4.6.2 Настройка . . . 390
2.4.6.3 Список команд . . . 393
2.4.7 DMVPN . . . 397
2.4.7.1 Описание . . . 397
2.4.7.2 Настройка . . . 398
2.4.7.3 Список команд . . . 401
2.4.8 Site-to-Site VPN . . . 404
2.4.8.1 Описание . . . 404
2.4.8.2 Настройка . . . 406
2.4.8.3 Список команд . . . 413
2.5 Контроль трафика . . . 415
2.5.1 Межсетевой экран . . . 416
2.5.1.1 Обзор . . . 416
2.5.1.2 Пример настройки . . . 416
2.5.1.3 Список команд . . . 417
2.5.2 Преобразование сетевых адресов (NAT) . . . 584
2.5.2.1 Обзор . . . 584
2.6 Приоритизация трафика (QoS) . . . 634
2.6.1 Общие принципы работы . . . 635
2.6.1.1 Единицы измерения . . . 635
2.6.1.2 Классы . . . 636
2.6.1.3 Действие над трафиком . . . 638
2.6.1.4 Встраивание политики . . . 639

2.6.2 Создание политики обработки трафика . . . 640
2.6.2.1 Политика Drop Tail . . . 641
2.6.2.2 Политика Fair Queue . . . 642
2.6.2.3 Политика FQ-CoDel . . . 644
2.6.2.4 Политика Limiter . . . 646
2.6.2.5 Политика Network Emulator . . . 648
2.6.2.6 Политика Priority Queue . . . 649
2.6.2.7 Политика Random Detect . . . 651
2.6.2.8 Политика Rate Control . . . 654
2.6.2.9 Политика Round Robin . . . 655
2.6.2.10 Политика Shaper . . . 657
2.6.3 Применение политики . . . 660
2.6.4 Обработка входящего трафика . . . 661
2.7 Отказоустойчивость . . . 662
2.7.1 VRRP . . . 663
2.7.1.1 Описание . . . 663
2.7.1.2 Настройка . . . 664
2.7.1.3 Список команд . . . 667
2.7.2 Балансировка WAN-каналов . . . 671
2.7.2.1 Описание . . . 671
2.7.2.2 Настройка . . . 676
2.7.2.3 Список команд . . . 676
2.8 Сервисы . . . 680
2.8.1 Сервисные механизмы . . . 681
2.8.1.1 Удаленное управление по протоколу SSH . . . 682
2.8.1.2 Протокол SNMP . . . 693
2.8.1.3 Протокол ARP . . . 699
2.8.1.4 Широковещательная ретрансляция UDP . . . 700
2.8.1.5 Отслеживание соединений . . . 702
2.8.1.6 Консольный сервер . . . 707
2.8.1.7 Ретранслятор DHCP . . . 710
2.8.1.8 DHCP сервер . . . 713
2.8.1.9 Перенаправляющий DNS сервер . . . 726
2.8.1.10 Динамический DNS . . . 730
2.8.2 Системные механизмы . . . 733
2.8.2.1 Системный DNS . . . 734
2.8.2.2 Протокол сетевого времени . . . 735
2.8.2.3 Информация об устройстве . . . 737
2.8.2.4 Управление пользователями . . . 739
2.9 Встроенные контейнеры . . . 743
2.9.1 Конфигурирование . . . 743
2.9.2 Команды эксплуатационного режима . . . 745
2.9.3 Пример конфигурации . . . 746
2.10 Эксплуатация . . . 748
2.10.1 Управление лицензиями ПО Факел . . . 749
2.10.1.1 Общие сведения . . . 749
2.10.2 Общие сведения . . . 750

2.10.2.1 Аппаратное обеспечение . . . 750
2.10.2.2 Версия ПО Факел . . . 751
2.10.3 Параметры загрузки . . . 753
2.10.3.1 Произвольный файл конфигурации . . . 753
2.10.3.2 Отключение шагов загрузки . . . 753
2.10.4 Восстановление пароля . . . 754
2.10.5 Дисковый массив . . . 755
2.10.5.1 Варианты установки . . . 755
2.10.5.2 Конфигурирование . . . 755
2.10.5.3 Эксплуатация . . . 757

3 История изменений ПО 759
3.1 Версия 2.1 . . . 759
3.1.1 Версия 2.1.0 от 27 января 2026 г. . . . 759
3.1.1.1 Исправленные ошибки . . . 759
3.1.1.2 Новые функции и улучшения . . . 759
3.1.1.3 Известные проблемы . . . 759
3.2 Версия 2.0 . . . 760
3.2.1 Версия 2.0.0 от 27 сентября 2024 г. . . . 760
3.2.1.1 Новые функции и улучшения . . . 760
3.2.1.2 Известные проблемы . . . 760
3.3 Версия 1.2 . . . 761
3.3.1 Версия 1.2.0 от 11 августа 2025 г. . . . 761
3.3.1.1 Исправленные ошибки . . . 761
3.3.1.2 Новые функции и улучшения . . . 761
3.4 Версия 1.1 . . . 761
3.4.1 Версия 1.1.1 от 02 ноября 2024 г. . . . 762
3.4.1.1 Исправленные ошибки . . . 762
3.4.1.2 Новые функции и улучшения . . . 762
3.4.1.3 Известные проблемы . . . 762
3.4.2 Версия 1.1.2 от 12 ноября 2024 г. . . . 762
3.4.2.1 Исправленные ошибки . . . 762
3.4.3 Версия 1.1.3 от 29 мая 2025 г. . . . 762
3.4.3.1 Исправленные ошибки . . . 762

Алфавитный указатель 763

Быстрый старт

Быстрый старт описывает минимальные настройки для ввода в эксплуатацию маршрутизатора **Факел**.

1.1 Введение

Данный раздел представляет собой краткое руководство по вводу в эксплуатацию маршрутизатора **Факел**. Краткое руководство описывает действия, которые необходимо выполнить с новым устройством, для настройки его базового функционала. Настройка устройства будет выполнена в соответствии со схемой, представленной ниже:

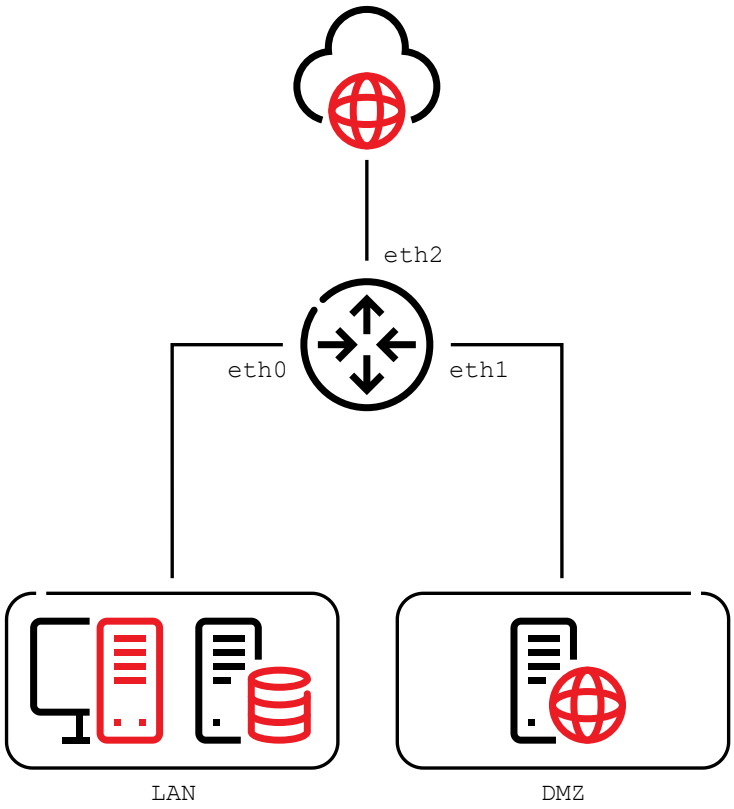


Рисунок 1.1. Пример базовой конфигурации

1.2 Установка ПО Факел

ПО Факел поддерживает установку на аппаратные платформы или на виртуальные машины. Для установки **ПО Факел** используется ISO-образ, который представляет собой образ для установки операционной системы в режиме реального времени (live install image).

1.2.1 Установка ПО Факел на аппаратную платформу

Для установки **ПО Факел** на аппаратную платформу выполните следующие действия:

1. Подготовьте установочный USB-носитель с ISO-образом **ПО Факел**. Чтобы подготовить образ **ПО Факел**, можно использовать приложение **Rufus** (или аналогичные ему) для Windows систем или использовать утилиту **dd**, если вы предпочитаете использовать Linux системы.

2. Подключите USB-носитель с установочным образом в один из доступных USB-портов на аппаратной платформе. Аппаратная платформа во время подключения установочного USB-носителя должна быть выключена.

3. Подключите консольный кабель к консольному порту аппаратной платформы и к компьютеру, с которого будет осуществляться подключение к аппаратной платформе.

4. **Для подключения к аппаратной платформе через консольный порт:**

   - Если вы используете ОС Windows для подключения по консольному кабелю, используйте утилиту **PuTTy**. Запустите **Диспетчер устройств** и определите, какой номер COM-порта нужно использовать для подключения к аппаратной платформе. После этого запустите приложение **PuTTy**, выберите тип подключения *Serial*. В поле *Последовательная линия* введите номер COM-порта, а в поле *Скорость* установите значение 115200.
   - Если вы используете ОС Linux для подключения по консольному кабелю, используйте утилиту **minicom**. Запустите приложение терминала. В приложении терминала выполните команду:

   ```
   minicom -D /dev/ttyUSB0 -b 115200
   ```

5. Включите аппаратную платформу.

6. В процессе загрузки аппаратной платформы дождитесь, когда появится сообщение:

   ```
   - Press ESC for boot menu
   ```

   Нажмите на клавишу ESC.

7. Выберите номер пункта из загрузочного меню, который отвечает за загрузку системы с USB-носителя, и нажмите на клавишу ENTER.

8. Дождитесь загрузки **ПО Факел**.

9. Авторизуйтесь в системе. Для авторизации используйте имя пользователя `fakel` и пароль `fakel`.

10. После успешной авторизации в системе, в командной строке выполните команду:

    ```
    install image
    ```

11. Подтвердите запуск процесса установки ОС. Когда в консоли появится сообщение с предложением продолжить установку:

- `Would you like to continue? (Yes/No) [Yes]:`

  Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

12. Выберете автоматический способ разметки жесткого диска. Когда в консоли появится сообщение с выбором способа настройки разделов жестокого диска:

    - `Partition (Auto/Parted/Skip) [Auto]:`

    Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

13. Выберите устройство, на которое будет установлена ОС. Когда в консоли появится сообщение с выбором устройства на которое будет установлена ОС, введите имя устройства:

    - `Install the image on? [sda]:`

    Нажмите на клавишу ENTER.

14. Когда в консоли появится сообщение о том, что установка ОС удалит все текущие данные с устройства:

    - `This will destroy all data on /dev/sda. Continue? (Yes/No) [No]:`

    Ведите `Yes` и нажмите на клавишу ENTER.

15. Укажите размер *root* раздела. Когда в консоли появится сообщение о том, сколько места нужно выделить под *root* раздел:

    - `How big of a root partition should I create? (2000MB - 55021MB) [55021]MB:`

    Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

16. Укажите имя для образа, который будет установлен. Когда в консоли появится сообщение с предложением указать имя для устанавливаемого образа:

    - `What would you like to name this image? [1.0.0-224]:`

    Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

17. Выберите, какой файл будет использован для загрузки конфигурации ОС. Когда в консоли появится сообщение с предложением выбрать путь к файлу с конфигурацией ОС:

    - `Which one should I copy to sda? [/opt/vyatta/etc/config/config.boot]:`

    Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

18. Установите пароль для учетной записи *fakel*.

19. Выберите устройство, на которое будет установлен *boot* раздел. Когда в консоли появится сообщение с предложением выбрать устройство для установки *boot* раздела:

    - `Which drive should GRUB modify the boot partition on? [sda]:`

    Введите имя устройства и нажмите на клавишу ENTER.

20. После завершения процесса установки перезагрузите аппаратную платформу. Извлеките USB-носитель с установочным образом. В командной строке **ПО Факел** выполните команду:

    ```
    reboot
    ```

21. Дождитесь успешной загрузки ОС и авторизуйтесь в системе.

1.2.2 Установка ПО Факел на виртуальную платформу

ПО Факел поддерживает среды виртуализации, основанные на технологии Linux KVM.

Для установки **ПО Факел** на виртуальную платформу выполните следующие действия:

1. Добавьте файл ISO-образа **ПО Факел** в хранилище образов на сервере виртуализации.
2. **Создайте виртуальную машину на сервере виртуализации со следующими параметрами (в данном примере представлены минимальные характеристики для создания виртуальной машины для установки ПО Факел):**
    - CPU: 2 ядра
    - RAM: 2 Гб
    - Hard Disk: 10 ГБ
    - Network Interfaces: 2 шт.
    - Disc Image File: ISO-образ **ПО Факел**
3. Откройте консоль подготовленной виртуальной машины и включите виртуальную машину.
4. Дождитесь загрузки **ПО Факел** на виртуальной машине.
5. Авторизуйтесь в системе. Для авторизации используйте имя пользователя `fakel` и пароль `fakel`.
6. После успешной авторизации в системе, в командной строке выполните команду:

```
install image
```

7. Подтвердите запуск процесса установки ОС. Когда в консоли появится сообщение с предложением продолжить установку:

```
- Would you like to continue? (Yes/No) [Yes]:
```

   Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

8. Выберете автоматический способ разметки жесткого диска. Когда в консоли появится сообщение с выбором способа настройки разделов жестокого диска:

```
- Partition (Auto/Parted/Skip) [Auto]:
```

   Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

9. Выберите устройство, на которое будет установлена ОС. Когда в консоли появится сообщение с выбором устройства на которое будет установлена ОС введите имя устройства:

```
- Install the image on? [sda]:
```

   Нажмите на клавишу ENTER.

10. Когда в консоли появится сообщение о том, что установка ОС удалит все текущие данные с устройства:

```
- This will destroy all data on /dev/sda. Continue? (Yes/No) [No]:
```

    Ведите `Yes` и нажмите на клавишу ENTER.

11. Укажите размер *root* раздела. Когда в консоли появится сообщение о том, сколько места нужно выделить под *root* раздел:

```
- How big of a root partition should I create? (2000MB - 55021MB) [55021]MB:
```

Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

12. Укажите имя для образа, который будет установлен. Когда в консоли появится сообщение с предложением указать имя для устанавливаемого образа:

```
- What would you like to name this image? [1.0.0-224]:
```

Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

13. Выберите, какой файл будет использован для загрузки конфигурации. Когда в консоли появится сообщение с предложением выбрать путь к файлу с конфигурацией:

```
- Which one should I copy to sda? [/opt/vyatta/etc/config/config.boot]:
```

Нажмите на клавишу ENTER (будет выбрано значение по умолчанию).

14. Установите пароль для учетной записи *fakel*.

15. Выберите устройство, на которое будет установлен *boot* раздел. Когда в консоли появится сообщение с предложением выбрать устройство для установки *boot* раздела:

```
- Which drive should GRUB modify the boot partition on? [sda]:
```

Введите имя устройства и нажмите на клавишу ENTER.

16. После завершения процесса установки перезагрузите аппаратную платформу. В командной строке **ПО Факел** выполните команду:

```
reboot
```

17. Дождитесь успешной загрузки **ПО Факел** и авторизуйтесь в системе.

1.3 Подключение к устройству

При первом запуске устройства на выбор можно использовать два типа подключения:

- Подключение к интерфейсу командной строки через консольный порт. Консольный порт устройства работает на скорости 115200;
- Подключение к интерфейсу командной строки по SSH через сетевой порт управления. По умолчанию в качестве сетевого порта управления настроен порт *eth0*.

Для подключения к устройству укажите ip адрес *192.168.150.1/24*, который настроен на порту *eth0*. После подключения к устройству открывается интерфейс командной строки в режиме Администрирования.

1.3.1 Доступ по SSH

Для настройки удаленного доступа к устройству по протоколу SSH выполните следующую команду:

```
set service ssh port '22'
```

Для настройки метода аутентификации по ключам выполните следующие команды.:

```
set system login user fakel authentication public-keys new_user@description type
 ssh-rsa
set system login user fakel authentication public-keys new_user@description key
 contents_of_id_rsa.pub
```

Для получения подробной информации о возможности ограничения доступа по протоколу SSH обратитесь к разделу *Удаленное управление по протоколу SSH* (страница 682).

1.4 Командная строка

1.4.1 Режимы работы командной строки

Интерфейс командной строки операционной системы по умолчанию запускается в режиме Администрирования. Символ $ указывает на то, что интерфейс командной строки работает в режиме Администрирования.

Для внесения изменений в настройки операционной системы переведите интерфейс командной строки в режим конфигурирования. Символ # указывает на то, что интерфейс командной строки работает в режиме Конфигурирования. Для перехода в режим конфигурирования, введите команду `configure`:

```
fakel@fakel:~$ configure
[edit]
fakel@fakel#
```

Для выхода из режима Конфигурирования и перехода в режим администрирования введите команду `exit`:

```
fakel@fakel# exit
exit
fakel@fakel:~$
```

Для получения подробной информации о работе с командной строкой обратитесь к разделу *Командная строка* (страница 17).

1.4.2 Применение и сохранение конфигурации

После внесения изменений, выполненных в режиме Конфигурирования, необходимо применить эти изменения. Чтобы применить внесенные изменения, выполните команду `commit`.

Чтобы сохранить внесённые изменения, используйте команду `save`.

Если вы хотите отменить внесённые изменения, выполните команду `exit discard`. Однако команда `exit discard` может отменить изменения только в том случае, если команда `save` не была выполнена. После применения команды `exit discard` интерфейс командной строки перейдет в режим администрирования.

Чтобы отменить сохранённые изменения, используйте команду `rollback`. Команда `rollback` выполняет откат до предыдущих версий конфигураций.

Для получения подробной информации о работе с настройкой устройства, обратитесь к разделу *Работа с конфигурацией системы* (страница 24).

1.5 Учетные записи

При первом подключении к устройству используется учетная запись пользователя с именем `fakel` и паролем `fakel`. После аутентификации с использованием учетной записи пользователя `fakel` выполните смену пароля.

Для этого выполните следующую команду:

```
set system login user fakel authentication plaintext-password text_password
```

Чтобы создать нового пользователя `new_user`, выполните следующую команду:

```
set system login user new_user authentication plaintext-password text_password
```

Для получения подробной информации о управлении учетными записями обратитесь к разделу *Управление пользователями* (страница 739).

1.6 Сетевые интерфейсы и маршрутизация

Роль внешнего WAN интерфейса будет выполнять сетевой интерфейс *eth2*. Сетевые параметры этот интерфейс будет получать динамически по средствам протокола DHCP.

Для настройки IP адреса на интерфейсе *eth2* выполните следующие команды:

```
set interfaces ethernet eth2 address dhcp
set ethernet eth0 description 'WAN'
```

В роли внутреннего LAN интерфейса выступает сетевой интерфейс *eth0*, а интерфейс *eth1* в роли DMZ интерфейс. Сетевые параметры для этих интерфейсов будут настроены статически.

Для настройки IP адреса на интерфейсах *eth0* и *eth1* выполните следующие команды:

```
set interfaces ethernet eth1 address '172.16.100.1/24'
set interfaces ethernet eth1 description 'LAN'
set interfaces ethernet eth1 address '10.150.0.1/24'
set interfaces ethernet eth1 description 'DMZ'
```

После настройки сетевых интерфейсов укажите статический маршрут в сторону шлюза по умолчанию.

Для настройки статического маршрута выполните следующую команду:

```
set protocols static route 0.0.0.0/0 next-hop 87.156.23.1
```

Для получения подробной информации о настройке сетевых интерфейсов обратитесь к разделу *Сетевые интерфейсы* (страница 39).

1.7 Правила фильтрации (Firewall)

Для фильтрации входящего и исходящего трафика настройте правила межсетевого экрана. Фильтрация трафика выполняется в зависимости от направления, по которому этот трафик проходит через сетевой интерфейс

- **local** - трафик, который приходит непосредственно на адрес сетевого интерфейса
- **in** - трафик, входящий на сетевой интерфейс
- **out** - трафик, исходящий с сетевого интерфейса

Для настройки фильтрации трафика создайте набор правил и примените его к сетевому интерфейсу.

Для настройки правил фильтрации трафика выполните следующие команды:

```
# Создание группы объектов для правил межсетевого экрана
set firewall group network-group LAN-NET description 'LAN network'
set firewall group network-group LAN-NET network '172.16.100.0/24'
set firewall group network-group DMZ-NET description 'DMZ network'
set firewall group network-group DMZ-NET network '10.150.0.0/24'

# Настройка работы межсетевого экрана в режиме контроля состояния сессий
set firewall receive-redirects 'disable'
set firewall send-redirects 'disable'

# Создание набора правил для фильтрации входящего трафика на внешний интерфейс
set firewall name WAN-IN default-action 'drop'

# Создание набора правил для фильтрации локального трафика на внешнем интерфейсе
set firewall name WAN-LOCAL default-action 'drop'

# Создание набора правил для фильтрации исходящего с внешнего интерфейса трафика
set firewall name WAN-OUT default-action 'drop'
set firewall name WAN-OUT rule 10 action 'accept'
set firewall name WAN-OUT rule 10 source group network-group LAN-NET
set firewall name WAN-OUT rule 10 destination address 0.0.0.0/24
set firewall name WAN-OUT rule 10 description 'Allow LAB-NET to Internet'
set firewall name WAN-OUT rule 20 action 'accept'
set firewall name WAN-OUT rule 20 source group network-group DMZ-NET
set firewall name WAN-OUT rule 20 destination address 0.0.0.0/24
set firewall name WAN-OUT rule 20 destination port 'https, http'
set firewall name WAN-OUT rule 20 protocol 'tcp'
set firewall name WAN-OUT rule 20 description 'Allow DMZ-NET to Internet'

# Применение набора правил к сетевому интерфейсу
set interfaces ethernet eth2 firewall in name 'WAN-IN'
set interfaces ethernet eth2 firewall local name 'WAN-LOCAL'
set interfaces ethernet eth2 firewall out name 'WAN-OUT'
```

Для получения подробной информации о настройке правил фильтрации обратитесь к разделу *Межсе-*

тевой экран (страница 416).

1.8 Правила трансляции (NAT)

Чтобы предоставить доступ из внутренних сетей LAN и DMZ к ресурсам из внешней сети WAN, настройте правила трансляции адреса источника **SNAT**. Правила трансляции адресов будут заменять адрес источника из локальной сети *172.16.100.0/24* или сети DMZ *10.150.0.0/24* на адрес, настроенный на внешнем интерфейсе *eth2* по типу MASQUERADE.

Для настройки правил трансляции адресов выполните следующие команды:

```
# Настройка правил трансляции для источника из локальной сети
set nat source rule 10 description ”LAN to WAN translation”
set nat source rule 10 source address '172.16.100.0/24'
set nat source rule 10 outbound-interface 'eth2'
set nat source rule 10 translation address masquerade

# Настройка правил трансляции для источника из сети DMZ
set nat source rule 20 description ”DMZ to WAN translation”
set nat source rule 20 source address '10.150.0.0/24'
set nat source rule 20 outbound-interface 'eth2'
set nat source rule 20 translation address masquerade
```

Чтобы предоставить доступ из внешней сети WAN к веб серверу из сети DMZ настройте правила трансляции адреса назначения **DNAT**. Правила трансляции адресов будут заменять адрес внешнего интерфейса *87.156.23.78* на адрес веб сервера *10.150.0.78* при обращении к адресу внешнего интерфейса из сети WAN по протоколу HTTPS.

Для настройки правил трансляции адресов выполните следующие команды:

```
set nat destination rule 10 description ”Port Forward: 443 to 10.150.0.78”
set nat destination rule 10 destination address '87.156.23.78'
set nat destination rule 10 destination port '443'
set nat destination rule 10 inbound-interface 'eth2'
set nat destination rule 10 protocol 'tcp'
set nat destination rule 10 translation address '10.150.0.78'
set nat destination rule 10 translation options address-mapping 'persistent'
```

Для получения подробной информации о настройке правил трансляции обратитесь к разделу *Преобразование сетевых адресов (NAT)* (страница 584).

1.9 DNS, NTP и DHCP сервисы

Устройство может выступать в качестве шлюза по умолчанию, DNS, DHCP и NTP сервера локальной сети.

DNS сервер будет отвечать на запросы от хостов из подсети *172.16.100.0/24*. В качестве адреса DNS сервера будет настроен адрес *172.16.100.1*.

Для настройки функционала DNS сервера выполните следующие команды:

```
set service dns forwarding listen-address '172.16.100.1'
set service dns forwarding allow-from '172.16.100.0/24'
set service dns forwarding cache-size '0'
```

DHCP сервер будет выдавать адреса хостам из подсети *172.16.100.0/24* начиная с адреса *172.16.100.9* и заканчивая адресом *172.16.100.254*. В качестве DNS сервера и шлюза по умолчания для хостов из подсети *172.16.100.0/24* будет указан адрес *172.16.100.1*. Имя домена для хостов из подсети *172.16.100.0/24* будет *fakel.net*.

Для настройки функционала DHCP сервера выполните следующие команды:

```
set service dhcp-server shared-network-name LAN subnet 172.16.100.0/24
set service dhcp-server shared-network-name LAN subnet 172.16.100.0/24 default-
  router '172.16.100.1'
set service dhcp-server shared-network-name LAN subnet 172.16.100.0/24 name-server
  '172.16.100.1'
set service dhcp-server shared-network-name LAN subnet 172.16.100.0/24 domain-name
  'fakel.net'
set service dhcp-server shared-network-name LAN subnet 172.16.100.0/24 lease '86400
  '
set service dhcp-server shared-network-name LAN subnet 172.16.100.0/24 range 0
  start 172.16.100.9
set service dhcp-server shared-network-name LAN subnet 172.16.100.0/24 range 0 stop
  '172.16.100.254'
```

NTP сервер будет отвечать на запросы клиентов из подсетей *172.16.100.0/24* и *10.150.0.0/24*.

Для настройки NTP сервера выполните следующие команды:

```
set system ntp allow-clients address '172.16.100.0/24'
set system ntp allow-clients address '10.150.0.0/24'
set system ntp listen-address '172.16.100.1'
set system ntp listen-address '10.150.0.1'
```

Для настройки сервисов NTP и DNS на самом устройстве выполните следующие команды:

```
set system name-server 1.1.1.1
set system ntp server 172.16.100.10
```

После выполнения всех действий, описанных в данной главе, вы получите решение на базе **ПО Факел** в базовой конфигурации и обладающее достаточной степенью защищенности. Теперь вы можете присту-

пить к дальнейшему ознакомлению с функциональными возможностями **ПО Факел**.

2

Руководство Администратора

Руководство Администратора описывает действия администратора при конфигурации и эксплуатации **ПО Факел**.

2.1 Командная строка

ПО Факел допускает использование интерфейса CLI (Command Line Interface) в двух режимах:

- *Режим Администрирования* (страница 18)
- *Режим Конфигурирования* (страница 20)

2.1.1 Режим Администрирования

Режим Администрирования позволяет использовать команды управления питанием устройства, получать информацию о текущем статусе операционной системы в целом и сервисов в ее составе в частности, а также выполнять диагностические команды по типу `traceroute` или `ping`.

Интерфейс CLI предоставляет возможность получения справки по всем поддерживаемым командам посредством ввода символа ?. Клавиша TAB может быть использована для автозаполнения строки с командами, а также для проверки введенной команды, в случае ввода конфликтующих или неизвестных значений. При вводе в командной строке значения sh и последующем нажатии клавиши TAB операционная система предложит вариант команды show. Повторное нажатие клавиши TAB приведет к выводу на экран всех возможных дополнительных команд и параметров, соответствующих команде show.

Пример работы команды show:

```
fakel@fakel:~$ sh[tab]
set   show
```

```
fakel@fakel:~$ show [tab]
Possible completions:
    arp             Show Address Resolution Protocol (ARP) information
    bridge          Show bridging information
    cluster         Show clustering information
    configuration   Show running configuration
    conntrack       Show conntrack entries in the conntrack table
    conntrack-sync  Show connection syncing information
    date            Show system date and time
    dhcp            Show Dynamic Host Configuration Protocol (DHCP) information
    dhcpv6          Show status related to DHCPv6
    disk            Show status of disk device
    dns             Show Domain Name Server (DNS) information
    file            Show files for a particular image
    firewall        Show firewall information
    flow-accounting Show flow accounting statistics
    hardware        Show system hardware details
    history         show command history
    host            Show host information
    incoming        Show ethernet input-policy information
: q
```

Вы можете пролистывать выводимую на экран информацию вверх с помощью сочетания клавиш `Shift+PageUp` и вниз с помощью сочетания клавиш `Shift+PageDown`.

Когда вывод данных в командной строке в ответ на заданную команду содержит количество строк, превышающее буфер отображаемой на экране информации, выводимая информация будет разделена на части, о чем будет свидетельствовать отображение на экране символа `:`.

При просмотра вывода данных с разделенной информацией доступны следующие действия:

- Использование клавиши q для прекращения вывода.

- Использование клавиши SPACE для перехода к следующей странице.
- Использование клавиши b для перехода к предыдущей странице.
- Использование клавиши ⏎ для перемещения выводимой на экран информации на одну строчку вниз.
- Использование клавиш ⇧ и ⇩ для перемещения выводимой информации на одну строчку вверх и на одну строчку вниз соответственно.
- Использование клавиш ⇦ и ⇨ для перемещения выводимой информации влево и вправо соответственно, в случае если вывод данных в строке содержит количество символов, превышающее буфер отображаемой на экране информации по горизонтали.

2.1.2 Режим Конфигурирования

Режим Конфигурирования позволяет использовать команды, приводящие к изменению в конфигурации операционной системы.

Для перевода операционной системы из режима Администрирования в режим Конфигурирования используйте команду:

- `configure`

```
fakel@fakel:~$ configure
[edit]
fakel@fakel#
```

Подсказка

Обозначение текущего режима при запросе ввода в командной строке поменяется с символа $ (режим Администрирования) на символ # (режим Конфигурирования).

Для перевода устройства под управлением операционной системы обратно в режим Администрирования используйте команду:

- `exit`

```
fakel@fakel# exit
exit
fakel@fakel:~$
```

2.1.2.1 Работа в режиме Конфигурирования

Все команды, выполняемые в режиме Конфигурирования, связаны с определенным уровнем иерархической структуры, который определяется администратором в процессе ввода команд. В режиме Конфигурирования можно производить изменения в настройках операционной системы с самого верхнего уровня иерархической структуры, но в таком случае цепочка команд при их ручном вводе получится достаточно длинной. Изменение уровня иерархической структуры сократит длину используемых команд и упростит настройку конфигурации операционной системы.

Для изменения текущего уровня иерархической структуры используйте команду:

- `edit`

```
fakel@fakel# edit interfaces ethernet eth0
[edit interfaces ethernet eth0]
fakel@fakel#
```

Пример выше демонстрирует работу команды `edit`. После ввода команды `edit interfaces ethernet eth0` операционная система переходит на уровень иерархической структуры конфигурации, связанный с цепочкой команд `interfaces ethernet eth0`. Все команды, будут выполняться в отношение данного уровня.

Для возвращения на самый верхний уровень иерархической структуры используйте команды:

- `top`
- `exit`

Для перемещения на один уровень иерархической структуры вверх используйте команду:

- `up`

Для вывода на экран рабочей конфигурации используйте команду:

- `show`

Команда `show`, введенная в режиме Конфигурирования, приведет к отображению рабочей конфигурации с обозначением ее строк символами:

- `+` - добавленные строки
- `>` - измененные строки
- `-` - удаленные строки

Пример работы команды show:

```
fakel@fakel# show interfaces
        ethernet eth0 {
        description MY_OLD_DESCRIPTION
        disable
        hw-id 00:53:dd:44:3b:03
    }
    loopback lo {
    }
    [edit]
    fakel@fakel# set interfaces ethernet eth0 address dhcp
    [edit]
    fakel@fakel# set interfaces ethernet eth0 description MY_NEW_DESCRIPTION
    [edit]
    fakel@fakel# delete interfaces ethernet eth0 disable
    [edit]
    fakel@fakel# show interfaces
    ethernet eth0 {
    +   address dhcp
    >   description MY_NEW_DESCRIPTION
    -   disable
    hw-id 00:53:dd:44:3b:03
    }
    loopback lo {
    }
```

Пример выше демонстрирует работу команды `show interfaces`, которая выводит информацию о рабочей конфигурации сетевых интерфейсов до и после внесения изменений в настройки интерфейса *eth0*.

Для вывода информации обо всех выполненных командах `set` используется набор команд:

- `show | commands`

Пример работы команды show | commands:

```
fakel@fakel# show interfaces ethernet eth0 | commands

    set address dhcp
    set hw-id 00:53:ad:44:3b:03
```

Пример выше демонстрирует работу команды `show interfaces ethernet eth0 | commands`, которая выводит информации о выполненных командах для интерфейса *eth0*.

В режиме Конфигурирования вывод команды show зависит от текущего активного уровня иерархической структуры. Команда show выводит информацию о настройках конфигурации, которая относится к текущему активному уровню иерархической структуры.

```
[edit interfaces ethernet eth0]
fakel@fakel# show
address dhcp
hw-id 00:53:ad:44:3b:03
```

Пример выше демонстрирует вывод команды show, когда система находится на иерархическом уровне, который отвечает за настройку интерфейса eth0.

Для выхода из режима Конфигурирования используйте команду:

- `exit`

Во время выполнения команды `exit` операционная система должна находится на самом верхнем уровне иерархической структуры. Использование данной команды на любой другом уровне приведет к перемещению на самый верхний уровень иерархической структуры.

```
[edit interfaces ethernet eth0]
fakel@fakel# exit
[edit]
fakel@fakeel# exit
fakel@fakel:~$
```

Пример выше демонстрирует работу команды `exit`. После первого ввода команды `exit` система переходит на самый верхний иерархический уровень. Повторный ввод команды `exit` переводит систему в режим Администрирования

2.1.2.2 Доступ к командам режима Администрирования через режим Конфигурирования

Когда операционная система находится в режиме Конфигурирования, команды режима Администрирования не доступны для использования напрямую. Все команды режима Администрирования можно использовать в составе набора команд:

- `run [command]`

Где параметр command это команда из режима Администрирования.

При использовании набора команд `run [command]` автозаполнение строки с командами при помощи клавиши TAB и получение справки посредством ввода символа ? доступны для использования.

Пример работы команды run:

```
[edit]
fakel@fakel# run show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                     S/L  Description
---------        ----------                     ---  -----------
eth0             0.0.0.0/0                      u/u
```

Пример выше демонстрирует работу команды `run show interfaces`, которая выводит информации о сетевых интерфейсах.

Для получения дополнительной информации о возможностях режима Конфигурирования обратитесь к главе *Работа с конфигурацией системы* (страница 24).

Работа с конфигурацией системы

Операционная система использует унифицированный формат файла для описания всех параметров своей конфигурации:

/config/config.boot.

Это обеспечивает легкую работу с конфигурацией системы в части создания шаблонов, резервного копирования и восстановления. Операционная система может быть перенесена на другое устройство с сохранением текущих настроек посредством создания копий определенных конфигурационных файлов.

Типы конфигурации системы

В контексте операционной системы существует три основных типа конфигурации:

- **Активная конфигурация** - конфигурация системы, которая загружена и используется в настоящий момент. Любое изменение конфигурации должно быть применено для включения в активную конфигурацию.
- **Рабочая конфигурация** - конфигурация системы, которая подвергается изменениям в режиме Конфигурирования. Изменения, внесенные в рабочую конфигурацию не вступят в силу до их применения с помощью команды `commit`, после ввода которой конфигурация становится активной.
- **Хранимая конфигурация** - конфигурация, записанная в файл с помощью команды `save`. Такой подход позволяет безопасно хранить конфигурацию для последующего использования. В системе может храниться несколько файлов с конфигурацией. Конфигурация по умолчанию или загруженная конфигурация хранится в файле */config/config.boot*.

Просмотр активной конфигурации системы

В операционной системе информацию об активной конфигурации системы можно получить различными способами:

- Вывод информацию в виде иерархически упорядоченных секций и параметров в их составе
- Вывод полного списка всех команд, с помощью которых была сформирована активная конфигурация
- Вывод информации в формате JSON[1]
- Вывод информации в формате JSON[2] иерархического вида (секции и параметры упорядочены по вложенности)

Для получения информации об активной конфигурации системы в виде иерархически упорядоченных секций и параметров в их составе используйте команду:

- `show configuration`

Пример работы команды show configuration:

```
fakel@fakel:~$ show configuration
    interfaces {
```

(продолжается на следующей странице)

[1] https://www.json.org
[2] https://www.json.org

(продолжение с предыдущей страницы)

```
    ethernet eth0 {
        address dhcp
        hw-id 00:53:00:00:aa:01
    }
    loopback lo {
    }
}
service {
    ssh {
        port 22
    }
}
system {
    config-management {
        commit-revisions 20
    }
    console {
        device ttyS0 {
            speed 9600
        }
    }
    login {
        user fakel {
            authentication {
                encrypted-password ****************
            }
            level admin
        }
    }
    ntp {
        server 0.pool.ntp.org {
        }
        server 1.pool.ntp.org {
        }
        server 2.pool.ntp.org {
        }
    }
    syslog {
        global {
            facility all {
                level notice
            }
            facility protocols {
                level debug
            }
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
        }
    }
}
```

Для вывода полного списка всех команд, с помощью которых была сформирована активная конфигурация, используйте команду:

- `show configuration commands`

Пример работы команды show configuration commands:

```
fakel@fakel:~$ show configuration commands
    set interfaces ethernet eth0 address 'dhcp'
    set interfaces ethernet eth0 hw-id '00:53:dd:44:3b:0f'
    set interfaces loopback 'lo'
    set service ssh port '22'
    set system config-management commit-revisions '20'
    set system console device ttyS0 speed '9600'
    set system login user fakel authentication encrypted-password '$6$Vt68...QzF0'
    set system login user fakel level 'admin'
    set system ntp server '0.pool.ntp.org'
    set system ntp server '1.pool.ntp.org'
    set system ntp server '2.pool.ntp.org'
    set system syslog global facility all level 'notice'
    set system syslog global facility protocols level 'debug'
```

Подсказка

Используйте набор команд `show configuration commands | strip-private` в случае, если вы хотите скрыть конфиденциальную информацию, содержащуюся в конфигурации при ее отображении. Это может понадобиться в случае, если вы захотите передать или опубликовать снимок конфигурации кому-либо.

Для просмотра активной конфигурации в формате JSON[3], используйте команду:

- `show configuration json`

Пример работы команды show configuration json:

```
fakel@fakel:~$ show configuration json

{"interfaces": {"ethernet": {"eth0": {"address": ["192.0.2.11/24",
  "192.0.2.35/24"], "hw-id": "52:54:00:48:a0:c6"}, "eth1": {"address":
  ["203.0.113.1/24"], "hw-id": "52:54:00:fc:50:0b"}}, "loopback": {"lo": {}}},
  "protocols": {"static": {"route": {"0.0.0.0/0": {"next-hop": {"192.0.2.254": {}}}}
  }}, "service": {"ssh": {"disable-host-validation": {}}}, "system": {
```

(продолжается на следующей странице)

[3] https://www.json.org

(продолжение с предыдущей страницы)

```
"config-management": {"commit-revisions": "100"}, "console": {"device": {"ttyS0":
{"speed": "115200"}}}, "host-name": "r11-fakel", "login": {"user": {"fakel": {
"authentication": {"encrypted-password": "$6$Vt68...F0", "plaintext-password": "",
"public-keys": {"fakel@fakel": {"key": "AAAAxxx=", "type": "ssh-rsa"}}}}}},
"name-server": ["203.0.113.254"], "ntp": {"server": {"time1.fakel.net": {},
"time2.fakel.net": {}, "time3.fakel.net": {}}}, "syslog": {"global": {"facility":
{"all": {"level": "info"}, "protocols": {"level": "debug"}}}}, "time-zone":
"America/New_York"}}
```

Для просмотра активной конфигурации в формате JSON[4] иерархического вида (секции и параметры упорядочены по вложенности), используйте команду:

- `show configuration json pretty``.

Пример работы команды show configuration json pretty:

```
fakel@fakel:~$ show configuration json pretty
{
    "interfaces": {
        "ethernet": {
            "eth0": {
                "address": [
                    "192.0.2.11/24",
                    "192.0.2.35/24"
                ],
                "hw-id": "52:54:00:48:a0:c6"
            },
            "eth1": {
                "address": [
                    "203.0.113.1/24"
                ],
                "hw-id": "52:54:00:fc:50:0b"
            }
        },
        "loopback": {
            "lo": {}
        }
    },
    "protocols": {
        "static": {
            "route": {
                "0.0.0.0/0": {
                    "next-hop": {
                        "192.0.2.254": {}
                    }
```

(продолжается на следующей странице)

[4] https://www.json.org

(продолжение с предыдущей страницы)

```
            }
        }
    }
},
"service": {
    "ssh": {
        "disable-host-validation": {}
    }
},
"system": {
    "config-management": {
        "commit-revisions": "100"
    },
    "console": {
        "device": {
            "ttyS0": {
                "speed": "115200"
            }
        }
    },
    "host-name": "r11-fakel",
    "login": {
        "user": {
            "fakel": {
                "authentication": {
                    "encrypted-password": "$6$Vt68...F0",
                    "plaintext-password": "",
                    "public-keys": {
                        "fakel@fakel": {
                            "key": "AAAAxxx=",
                            "type": "ssh-rsa"
                        }
                    }
                }
            }
        }
    },
    "name-server": [
        "203.0.113.254"
    ],
    "ntp": {
        "server": {
            "time1.fakel.net": {},
            "time2.fakel.net": {},
            "time3.fakel.net": {}
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
            }
        },
        "syslog": {
            "global": {
                "facility": {
                    "all": {
                        "level": "info"
                    },
                    "protocols": {
                        "level": "debug"
                    }
                }
            }
        },
        "time-zone": "Asia/Novosibirsk"
    }
}
```

Представленные выше сценарии использования команды `show` работают когда операционная система находится в режиме Администрирования. В режиме Конфигурирования данные сценарии не работают, однако есть способ получить доступ к командам режима Администрирования когда операционная система находится в режиме Конфигурирования.

Подробная информации об использовании команд режима Администрирования из режима Конфигурирования представлена в разделе *Доступ к командам режима Администрирования через режим Конфигурирования* (страница 22).

Редактирование рабочей конфигурации

Для редактирования рабочей конфигурации операционной системы используются команды `set` и `delete`. Команды `set` и `delete` работают, когда операционная система находится в режиме Конфигурирования.

Чтобы установить значение существующего параметра в конфигурации или добавить новый параметр, используется команда:

- `set`

Команда `set` имеет иерархическую структуру. Выполняемые команды выстраиваются в последовательную цепочку, например `set interface ethernet eth0 address 192.0.2.100/24`. При этом вся введенная информация, являющаяся избыточной для данного уровня, удаляется из введенной цепочки команд.

Команды относятся к уровню, на котором они выполняются:

- **Операционная система находится на самом верхнем уровне иерархической структур**

```
fakel@fakel# set interface ethernet eth0 address 192.0.2.100/24
[edit]
```

Пример выше демонстрирует работу команды `set interface ethernet eth0 address 192.0.2.100/24`, которая выполняет настройку адреса для сетевого интерфейса *eth0* когда операционная система находится на самом верхнем уровне иерархической структуры.

- **Операционная система находится на уровне иерархической структуры, который отвечает за конфигурацию сетевого интерфейса eth0**

```
fakel@fakel# set address 203.0.113.6/24
[edit interfaces ethernet eth0]
```

Пример выше демонстрирует работу команды `set address 192.0.2.100/24`, которая выполняет настройку адреса для сетевого интерфейса *eth0* когда операционная система находится на уровне иерархической структуры, который отвечает за конфигурацию сетевого интерфейса *eth0*.

Обе команды, представленные в примерах выше, идентичны, но выполняются на разных уровнях иерархической структуры.

Чтобы удалить запись из конфигурации, используйте команду:

- `delete`

Выполнение команды `delete` также приводит к удалению всех нижестоящих уровней в иерархической структуре. При удаление записи элемента конфигурации его настройки переводятся к значению по умолчанию.

```
fakel@fakel# delete address 192.0.2.100/24
```

Пример выше демонстрирует работу команды `delete address 192.0.2.100/24`, которая удаляет IP адрес сетевого интерфейса *eth0*:

Чтобы применить изменения, которые были внесены в конфигурацию системы используйте команду:

- `commit`

Чтобы сохранить изменения, которые были внесены в конфигурацию системы используйте команду:

- `save`

Использование команды `save` без дополнительных параметров сохраняет конфигурацию системы в хранилище по умолчанию.

```
fakel@fakel# save
Saving configuration to '/config/config.boot'...
Done
```

По умолчанию конфигурация системы храниться в файле, расположенном по следующему пути:

/config/config.boot

Если необходимо разместить конфигурационный файл в другом месте, в качества хранилища можно указать локальный путь или адреса SCP, FTP и TFTP серверов.

```
fakel@fakel# save tftp://192.168.0.100/fakel.config.boot
Saving configuration to 'tftp://192.168.0.100/fakel-test.config.boot'...
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
########################################################################## 100.0%
Done
```

Пример выше демонстрирует работу команды `save tftp://192.168.0.100/fakel.config.boot`, которая сохраняет конфигурацию системы в файл *fakel.config.boot* на tftp сервере *192.168.0.100*.

Для выхода из режима Конфигурирования без применения внесенных изменений в конфигурации системы используйте команду:

- `exit discard`

```
fakel@fakel# exit discard
exit
fakel@fakel:~$
```

Команда `exit discard`, сбрасывает все изменения, внесенные в рабочую конфигурацию.

Подсказка

При использовании команды `exit` для выхода из режима Конфигурирования без применения внесенных изменений, операционная система выдает сообщение с ошибкой.

Чтобы временно применить изменения, которые были внесены в конфигурацию, и установить период времени в минутах, необходимый для проверки корректности полученной конфигурации используйте команду:

- `commit-confirm`

Команда `confirm` должна быть выполнена в течение заданного периода времени для окончательного применения конфигурации. В противном случае операционная система автоматически выполнит перезагрузку и возврат к конфигурации предыдущей версии конфигурации. По умолчанию используется период времени длительностью в 10 минут.

Пример работы команды commit-confirm:

Нужно настроить межсетевой экран и проверить, что внесенные в конфигурацию изменения, не заблокируют доступ к операционной системе для администратора. Для этого используйте команду `commit-confirm`. Если после применения, внесенных изменений доступ к межсетевому экрану не заблокирован, используйте команду `confirm`, чтобы подтвердить примененные изменения. В случае потери доступа к межсетевому экрану после использования команды `commit-confirm`, будет выполнена перезагрузка и возврат к конфигурации предыдущей версии.

```
fakel@fakel# set interfaces ethernet eth0 firewall local name FromWorld
fakel@fakel# commit-confirm
commit confirm will be automatically reboot in 10 minutes unless confirmed
Proceed? [confirm]y
[edit]
fakel@fakel# confirm
[edit]
```

Команда `commit-confirm` временно применяет изменения внесенные в конфигурацию системе в результате ввода команды `set interfaces ethernet eth0 firewall local name FromWorld`. Если в течении 10 минут не будет выполнена команда `confirm`, в результате перезагрузки устройства будет выполнен возврат к предыдущей версии конфигурации системы.

Чтобы скопировать определенный элемент конфигурации используйте команду:

- `copy`

С помощью команды `copy` можно копировать целые ветви иерархической структуры конфигурации.

Пример работы команды copy:

Для межсетевого экрана нужно создать набор правил *FromWorld* с одним правилом фильтрации, разрешающим трафик из определенной подсети и добавить в этот набор похожее правило, но уже для другой подсети. Для этого нужно перейти на соответствующий уровень иерархической структуры конфигурации - `firewall name FromWorld`, а затем использовать набор команд `copy rule 10 to rule 20` для создания нового правила через копирование данных из уже существующего, после чего модифицировать правило с номером 20 необходимым образом.

```
# Просмотр рабочей конфигурации набора правил FromWorld
   fakel@fakel# show firewall name FromWorld
       default-action drop
       rule 10 {
           action accept
           source {
               address 203.0.113.0/24
           }
       }
   [edit]

# Переход на иерархический уровень FromWorld
   fakel@fakel# edit firewall name FromWorld
   [edit firewall name FromWorld]

# Копирование параметров
   fakel@fakel# copy rule 10 to rule 20
   [edit firewall name FromWorld]

# Изменение параметров ip адреса
   fakel@fakel# set rule 20 source address 198.51.100.0/24
   [edit firewall name FromWorld]

# Применение внесенных изменений
   fakel@fakel# commit
   [edit firewall name FromWorld]
```

Чтобы переименовать определенный элемент конфигурации используйте команду:

- `rename`

С помощью команды `rename` можно переименовывать ветви иерархической структуры конфигурации.

```
fakel@fakel# rename rule 10 to rule 5
[edit firewall name FromWorld]
fakel@fakel# commit
[edit firewall name FromWorld]
```

Пример выше демонстрирует работу команды `rename rule 10 to rule 5`, которая переименовывает 10-е правило межсетевого экрана.

Для просмотра внесенных изменений в рабочую конфигурацию используйте команду:

- `show`

```
fakel@fakel# show
    default-action drop
    +rule 5 {
        action accept
        source {
            address 203.0.113.0/24
        }
    }
    rule 20 {
        action accept
        source {
            address 198.51.100.0/24
        }
    }
```

Пример выше демонстрирует работу команды `show` на уровне иерархической структуры, который отвечает за настройку набора привил межсетевого экрана *FromWorld*.

Чтобы добавить текстовый комментарий (аннотацию) к выбранной секции конфигурации <*config node*> используйте команду:

- `comment <config node> "comment text"`

В иерархической структуре конфигурации комментарий добавляется до выбранной секции. При выводе на экран комментарий заключается в рамки, обозначаемые разделителями `/*` (начало комментария) и `*/` (конец комментария). Добавление комментариев требует использования команды `commit`, как и любые другие изменения, вносимые в конфигурацию. Для удаления существующего комментария из текущей конфигурации используйте ту же команду, но укажите пустую строку (`""`) в качестве параметра.

```
fakel@fakel# comment firewall all-ping "Comment example"
fakel@fakel# commit
fakel@fakel# show
    firewall {
        /* Comment example */
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
        all-ping enable
        broadcast-ping disable
        ...
    }
```

Пример выше демонстрирует работу команды `comment firewall all-ping "Comment example"`, которая добавляет комментарий к секции *firewall*.

Примечание

Важно отметить, что комментарий добавляется до выбранной секции конфигурации, то есть при использовании команды `show <section>` он не будет отображаться. Например, если добавить комментарий для к секции `firewall`, а затем использовать набор команд `show firewall`, то на экран будет выведено содержимое данной секции, но не комментарий.

Управление версиями конфигурации

Операционная система содержит встроенную систему учета версий конфигурации. Эта система автоматически сохраняет копию каждой предыдущей примененной конфигурации - версию конфигурации. Версии конфигурации хранятся локально и используются для отката, однако они также могут быть размещены на внешнем (удаленном) хранилище с целью организации архива резервных копий.

Локальное хранение версий конфигурации

Версии конфигурации автоматически сохраняются на диске устройства. Можно просмотреть список всех версий, выполнить сравнение версий и откат в к любой версии в случае возникновения проблем с функционированием операционной системы.

Для просмотра списка всех версий конфигурации, размещенных локально на диске устройства используйте команду:

- `show system commit`

Пример работы команды show system commit:

```
fakel@fakel:~$ show system commit
0   2015-03-30 08:53:03 by fakel via cli
1   2015-03-30 08:52:20 by fakel via cli
2   2015-03-26 21:26:01 by root via boot-config-loader
3   2015-03-26 20:43:18 by root via boot-config-loader
4   2015-03-25 11:06:14 by root via boot-config-loader
5   2015-03-25 01:04:28 by root via boot-config-loader
6   2015-03-25 00:16:47 by fakel via cli
7   2015-03-24 23:43:45 by root via boot-config-loader
```

Чтобы установить ограничение на количество версий конфигурации, сохраняемых локально на диске устройства используйте команду:

- `set system config-management commit-revisions <N>`

Значение параметра *N* может быть в диапазоне от 0 до 65535. Когда количество версий конфигурации превышает заданное значение, старые версии удаляются. Значение параметра *N* по умолчанию подразумевает хранение до 100 версий конфигурации локально.

Сравнение версий конфигурации

Операционная система позволяет сравнивать различные версии конфигурации.

Для вывода на экран списка отличий между выбранными версиями конфигурации используйте команду:

- `compare <saved | N> <M>`

```
fakel@fakel# compare [tab]
Possible completions:
    <Enter> Compare working & active configurations
    saved   Compare working & saved configurations
    <N>     Compare working with revision N
    <N> <M> Compare revision N with M
    Revisions:
        0    2013-12-17 20:01:37 root by boot-config-loader
        1    2013-12-13 15:59:31 root by boot-config-loader
        2    2013-12-12 21:56:22 fakel by cli
        3    2013-12-12 21:55:11 fakel by cli
        4    2013-12-12 21:27:54 fakel by cli
        5    2013-12-12 21:23:29 fakel by cli
        6    2013-12-12 21:13:59 root by boot-config-loader
        7    2013-12-12 16:25:19 fakel by cli
        8    2013-12-12 15:44:36 fakel by cli
        9    2013-12-12 15:42:07 root by boot-config-loader
        10   2013-12-12 15:42:06 root by init
```

Команда `compare` позволяет выполнять следующие действия:

- Сравнивать различные типы конфигураций
- Сравнивать различные версии конфигурации с помощью команды `compare N M`, где параметры *N* и *M* - идентификаторы версий

При выводе на экран результатов сравнения двух версий символом + обозначаются добавленные в конфигурацию *N* элементы по сравнению с конфигурацией *M*, а символом - обозначаются удаленные из конфигурации элементы соответственно.

Пример работы команды compare:

```
fakel@fakel# compare 0 6
[edit interfaces]
+   dummy dum1 {
+       address 10.189.0.1/31
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
+   }
[edit interfaces ethernet eth0]
+   vif 99 {
+       address 10.199.0.1/31
+   }
-   vif 900 {
-       address 192.0.2.4/24
-   }
```

Пример выше демонстрирует работу команды `compare 0 6`, которая сравнивает *0* и *6* версии конфигурации операционной системы.

Для вывода на экран результатов сравнения двух версий примененной конфигурации используйте команду:

```
# run show system commit diff <number>
```

По умолчанию на экран выводятся результаты сравнения с активной конфигурацией.

Пример работы команды run show system commit diff <number>:

```
fakel@fakel# run show system commit diff 4
[edit system]
+   ipv4 {
+       disable-forwarding
+   }
```

Пример выше демонстрирует работу команды `run show system commit diff 4`, которая выводит результат сравнения версии активной конфигурации с конфигурацией *4*.

Откат изменений конфигурации

Для отката изменений конфигурации к версии, указанной в параметре *N* используйте команду:

```
# rollback <N>
```

Пример работы команды rollback <N>:

```
fakel@fakel# compare 1
[edit system]
>   host-name fakel-1
[edit]
fakel@fakel# rollback 1
Proceed with reboot? [confirm][y]
Broadcast message from root@fakel-1 (pts/0) (Tue Dec 17 21:07:45 2013):
The system is going down for reboot NOW!
```

Ввод команды `rollback` приведет к применению указанной версии конфигурации и перезагрузке системы.

Использование внешнего хранилища версий конфигурации

Операционная система позволяет загружать версию конфигурации на внешнее (удаленное) хранилище после каждого использования команды `commit`. Для сохранения версии конфигурации на внешнее хранилище нужно указать его адрес.

В качестве такого хранилища могут быть использованы TFTP, FTP, SCP и SFTP серверы:

- `scp://<user>:<passwd>@<host>:/<dir>`
- `sftp://<user>:<passwd>@<host>/<dir>`
- `ftp://<user>:<passwd>@<host>/<dir>`
- `tftp://<host>/<dir>`

Таким образом каждый раз, когда конфигурация успешно применяется, файл *config.boot* копируется по указанному адресу. При этом копии задается новое имя *config.boot-hostname.YYYYMMDD_HHMMSS*. Копирование может выполняться по нескольким адресам одновременно.

Для того, чтобы задать адрес внешнего (удаленного) хранилище в формате URI (Uniform Resource Identifier) используйте команду:

- `set system config-management commit-archive location <URI>`

Примечание

Количество версий конфигурации, хранимых локально на диске устройства, которое может задать администратор с помощью команды `set system config-management commit-revisions <N>` не распространяется на внешнее (удаленное) хранилище.

Операционная система не позволяет установить с внешним (удаленным) хранилищем защищенное (SSL/TLS) соединение, так как невозможно подтвердить легитимность данного хоста. Однако есть обходное решение данной проблемы через добавление отпечатка SSH ключа хоста в файл `~/.ssh/known_hosts`:

```
fakel@fakel# ssh-keyscan <host> >> ~/.ssh/known_hosts
```

Сохранение и загрузка конфигурации вручную

Команды `save` и `load` используются для управления файлами конфигурации вручную.

Чтобы сохранить файл конфигурации используйте команду:

- `save`

Чтобы загрузить конфигурацию из файла используйте команду:

- `load`

Команда `load <URI>` используется для загрузки конфигурации, которая в итоге заменит активную конфигурацию. Для данной команды необходимо определить расположение файла в виде пути до него. В качестве расположения можно указать локальный путь или адреса SCP, SFTP, FTP, HTTP, HTTPS и TFTP серверов:

```
fakel@fakel# load

    Possible completions:
        <Enter>                                 Load from system config file
        <file>                                  Load from file on local machine
        scp://<user>:<passwd>@<host>:/<file>    Load from file on remote machine
        sftp://<user>:<passwd>@<host>/<file>    Load from file on remote machine
        ftp://<user>:<passwd>@<host>/<file>     Load from file on remote machine
        http://<host>/<file>                    Load from file on remote machine
        https://<host>/<file>                   Load from file on remote machine
        tftp://<host>/<file>                    Load from file on remote machine
```

Восстановление конфигурации по умолчанию

Если требуется сбросить рабочую конфигурацию до состояния по умолчанию используется команда `load /opt/fakel/etc/config.boot.default`. При этом операционная система запросит подтверждение данного действия. Для подтверждения действия используется команду `commit`. После подтверждения действия операционная система будет использовать конфигурацию по умолчанию.

Примечание

В процессе сброса конфигурации до состояния по умолчанию удаленное подключение к устройству будет сброшено. Поэтому перед выполнением сброса рекомендуется создать копию конфигурации, внести в нее изменения для обеспечения сетевой связности, а потом загрузить измененную конфигурацию.

2.2 Сетевые интерфейсы

2.2.1 Интерфейс Ethernet

2.2.1.1 Обзор

Ethernet — технология передачи данных между устройствами при помощи кабеля. Включает в себя протокол обмена информацией, физический порт, кабель и чип на плате устройства. Ethernet работает на двух нижних уровнях модели OSI: физическом и канальном. Ethernet-соединения могут отличаться скоростью передачи данных, типом соединительного кабеля, топологией, максимальным расстоянием между двумя устройствами без ретрансляции. Ethernet часто используют в связке с другими сетевыми технологиями.

Интерфейс Ethernet — физический порт на маршрутизаторе Факел. Все модели маршрутизаторов Факел поддерживают следующие технологии и протоколы:

- DHCP/DHCPv6;
- EAP over LAN;
- EVPN;
- VLAN (802.1q);
- QinQ (802.1ad);
- VRF;
- множественную адресацию (multihoming);
- аппаратную разгрузку (gro, gso, lro, rps, sg, tso);
- зеркалирование портов (SPAN).

Характеристики интерфейса Ethernet зависят от модели маршрутизатора Факел.

Интерфейсы Ethernet	Модель маршрутизатора Факел		
	M100	M500	M1000
1000BASE-T (RJ-45)	4	4	8
1000BASE-X SFP	1	—	—
10GBASE-R/1000BASE-X	—	4	8

Вне зависимости от настроек и конфигурации, интерфейсы Ethernet работают по одному и тому же принципу. Перед тем как отправить пакет с данными, устройство инкапсулирует информацию в кадр. Затем чип устройства преобразует кадр в аналоговый сигнал для передачи по кабелю на MAC-адрес принимающего интерфейса. Получатель считывает поступивший сигнал, декапсулирует в кадр, проверяет контрольную сумму и обрабатывает.

При изготовлении каждому устройству с интерфейсом Ethernet присваивается индивидуальный MAC-адрес. Такой уникальный идентификатор помогает устройствам опознать друг друга в сети Ethernet. Но чтобы к устройству можно было обратиться с более высокого сетевого уровня, необходимо задействовать дополнительные протоколы, например ARP. После этого устройства смогут общаться друг с другом через протоколы сетевого уровня семейства TCP/IP.

При обмене кадрами на высоких скоростях возможны ошибки, потери данных, искажения значений контрольных сумм. В таких случаях данные отбрасываются и устройство-получатель сигнализирует об

ошибке. Администратор ПО Факел может влиять на процесс обмена данными через настройку интерфейса Ethernet.

2.2.1.2 Пример настройки

Шаг	Команда	Описание
1	set interfaces ethernet eth0 address 192.168.1.1/24	Назначает IP-адрес 192.168.1/24 интерфейсу Ethernet
2	set interfaces ethernet eth0 vrf 300 description RED	Добавляет описание RED VRF-экземпляру под номером 300 на интерфейсе Ethernet
3	set interfaces ethernet eth0 vif 400 vrf RED	Включает VLAN-интерфейс под номером 400 на VRF-экземпляре с описанием RED
4	set interfaces ethernet eth0 vif 400 address dhcp	Включает протокол DHCP для автоматического назначения IP-адреса VLAN-интерфейсу под номером 400

2.2.1.3 Список команд

Режим «Конфигурирование»

interfaces ethernet <interface> address <address | dhcp | dhcpv6>

Описание:

Устанавливает, каким способом IP-адрес будет назначен интерфейсу Ethernet.

Синтаксис:

- set interfaces ethernet <interface> address <address | dhcp | dhcpv6>
- delete interfaces ethernet <interface> address <address | dhcp | dhcpv6>
- show interfaces ethernet <interface> address

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <address> — IP-адрес, который администратор вручную назначает интерфейсу Ethernet. Может быть указан несколько раз;
- <dhcp> — DHCPv4-сервер автоматически назначит IPv4-адрес интерфейсу Ethernet на конкретном сегменте сети;

Режим: «Конфигурирование».

Примечание

Если вы используете протокол DHCP для получения IPv4-адреса и вам требуется дополнительная настройка, используйте указатели начала и конца данных. Эти файлы расположены в директории:

- /config/scripts/dhcp-client/pre-hooks.d/
- /config/scripts/dhcp-client/post-hooks.d/

---

interfaces ethernet <interface> description <description>

Описание:

Добавляет описание для интерфейса Ethernet.

Синтаксис:

- set interfaces ethernet `<interface>` description `<description>`
- delete interfaces ethernet `<interface>` description `<description>`
- show interfaces ethernet `<interface>` description

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<description>` — описание для интерфейса Ethernet.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к интерфейсу Ethernet по указанному описанию.

---

interfaces ethernet <interface> disable

Описание:

Выключает интерфейс Ethernet. Интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces ethernet `<interface>` disable
- delete interfaces ethernet `<interface>` disable
- show interfaces ethernet `<interface>`

Аргументы:

- <interface> — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> disable-flow-control

Описание:

Останавливает передачу данных в сети Ethernet на стороне отправителя, пока принимающая сторона не получит все пакеты. Используйте эту команду, чтобы предотвратить потерю пакетов при большом скоплении трафика.

Синтаксис:

- set interfaces ethernet <interface> disable-flow-control
- delete interfaces ethernet <interface> disable-flow-control
- show interfaces ethernet <interface>

Аргументы:

- <interface> — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> disable-link-detect

Описание:

Прекращает отслеживать состояние физического соединения на интерфейсе Ethernet. Если соединение по Ethernet-кабелю пропадет, система проигнорирует это событие для интерфейса Ethernet. По умолчанию состояние физического соединения отслеживается.

Синтаксис:

- set interfaces ethernet <interface> disable-link-detect
- delete interfaces ethernet <interface> disable-link-detect
- show interfaces ethernet <interface>

Аргументы:

- <interface> — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> mac <xx:xx:xx:xx:xx:xx>

Описание:

Назначает интерфейсу Ethernet пользовательский MAC-адрес.

Синтаксис:

- set interfaces ethernet <interface> mac <xx:xx:xx:xx:xx:xx>
- delete interfaces ethernet <interface> mac <xx:xx:xx:xx:xx:xx>
- show interfaces ethernet <interface> mac

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <xx:xx:xx:xx:xx:xx> — MAC-адрес.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на интерфейсе Ethernet.

Синтаксис:

- set interfaces ethernet <interface> mtu <mtu>
- delete interfaces ethernet <interface> mtu <mtu>
- show interfaces ethernet <interface> mtu

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <mtu> — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>

Описание:

Устанавливает на интерфейсе Ethernet конкретное значение для максимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces ethernet <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>
- delete interfaces ethernet <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>
- show interfaces ethernet <interface> ip adjust-mss

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <mss> — конкретное значение для максимального размера сегмента на протоколе TCP. Диапазон значений: от 536 до 65535;
- <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces ethernet <interface> ip arp-cache-timeout <sec>

Описание:

Задает временной интервал между записями в ARP-кэш на интерфейсе Ethernet. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Синтаксис:

- set interfaces ethernet <interface> ip arp-cache-timeout sec
- delete interfaces ethernet <interface> ip arp-cache-timeout sec
- show interfaces ethernet <interface> ip arp-cache-timeout

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <sec> — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ip disable-arp-filter

Описание:

Выключает фильтрацию по протоколу ARP на интерфейсе Ethernet. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами.

Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set interfaces ethernet `<interface>` ip disable-arp-filter
- delete interfaces ethernet `<interface>` ip disable-arp-filter
- show interfaces ethernet `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с интерфейса Ethernet на любой другой интерфейс. После выполнения команды интерфейс Ethernet перейдет в режим хоста.

Синтаксис:

- set interfaces ethernet `<interface>` ip disable-forwarding
- delete interfaces ethernet `<interface>` ip disable-forwarding
- show interfaces ethernet `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ip enable-directed-broadcast

Описание:

Включает направленную широковещательную переадресацию на интерфейсе Ethernet. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на подсеть назначения.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces ethernet `<interface>` ip enable-directed-broadcast
- delete interfaces ethernet `<interface>` ip enable-directed-broadcast
- show interfaces ethernet `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице интерфейса Ethernet для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица все равно будет обновлена, даже если команда не была выполнена.

Синтаксис:

- set interfaces ethernet `<interface>` ip enable-arp-accept
- delete interfaces ethernet `<interface>` ip enable-arp-accept
- show interfaces ethernet `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ip enable-arp-announce

Описание:

Ограничивает на интерфейсе Ethernet анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. ПО Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса интерфейс Ethernet проверяет все целевые подсети. По умолчанию ПО Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces ethernet <interface> ip enable-arp-announce
- delete interfaces ethernet <interface> ip enable-arp-announce
- show interfaces ethernet <interface> ip

Аргументы:

- <interface> — имя интерфейса Ethernet.

Режим: «Конфигурирование».

Примечание

Если вы выполнили команду, то при отправке ARP-запросов не используйте адреса вне подсети назначения.

---

interfaces ethernet <interface> ip enable-arp-ignore

Описание

Указывает интерфейсу Ethernet отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию интерфейс Ethernet отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе. Независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces ethernet <interface> ip enable-arp-ignore
- delete interfaces ethernet <interface> ip enable-arp-ignore
- show interfaces ethernet <interface> ip

Аргументы:

- <interface> — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ip enable-proxy-arp

Описание:

Включает прокси-сервер на интерфейсе Ethernet для маршрутизации ARP-запросов. Интерфейс Ethernet сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces ethernet `<interface>` ip enable-proxy-arp
- delete interfaces ethernet `<interface>` ip enable-proxy-arp
- show interfaces ethernet `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ip proxy-arp-pvlan

Описание:

Создает на интерфейсе Ethernet частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом напрямую, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces ethernet `<interface>` ip proxy-arp-pvlan
- delete interfaces ethernet `<interface>` ip proxy-arp-pvlan
- show interfaces ethernet `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Конфигурирование».

Подсказка

Вы можете использовать эту команду без предварительного выполнения команды `interfaces ethernet <interface> ip enable-proxy-arp`.

---

interfaces ethernet <interface> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces ethernet `<interface>` redirect `<destination>`
- delete interfaces ethernet `<interface>` redirect `<destination>`
- show interfaces ethernet `<interface>` redirect

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<destination>` — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ip source-validation [<strict> | <loose> | <disable>]

Описание:

Включает на интерфейсе Ethernet различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces ethernet `<interface>` ip source-validation `<strict | loose | disable>`
- delete interfaces ethernet `<interface>` ip source-validation `<strict | loose | disable>`
- show interfaces ethernet `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<strict>` — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;

- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vrf <vrf>

Описание:

Размещает интерфейс Ethernet на указанном VRF-экземпляре.

Синтаксис:

- set interfaces ethernet <interface> vrf <vrf>
- delete interfaces ethernet <interface> vrf <vrf>
- show interfaces ethernet <interface> vrf

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> dhcp-options client-id <description>

Описание:

Присваивает идентификатор клиента интерфейсу Ethernet. Интерфейс Ethernet будет отображать свой идентификатор при запросе IP-адреса у DHCP-сервера.

Синтаксис:

- set interfaces ethernet <interface> dhcp-options client-id <description>
- delete interfaces ethernet <interface> dhcp-options client-id <description>
- show interfaces ethernet <interface> dhcp-options client-id

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <description> — идентификатор клиента. Формат: произвольный.

Режим: «Конфигурирование».

Примечание

Более подробная информация содержится в документе RFC 2131. Отмечается, что клиент может специально ограничить свое обнаружение только посредством идентификатора (опция client identifier). В этом случае клиенту необходимо будет использовать один и тот же идентификатор во всех последующих сообщениях ICMPv6, а серверу придется использовать точно такой же идентификатор для поиска клиента.

---

interfaces ethernet <interface> dhcp-options host-name <hostname>

Описание:

Присваивает имя хоста DHCP-серверу на интерфейсе Ethernet. Созданное имя заменит имя хоста по умолчанию. Когда клиент будет запрашивать IP-адрес у интерфейса Ethernet, ему отобразится присвоенное имя хоста.

Синтаксис:

- set interfaces ethernet <interface> dhcp-options host-name <hostname>
- delete interfaces ethernet <interface> dhcp-options host-name <hostname>
- show interfaces ethernet <interface> dhcp-options host-name

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <hostname> — имя хоста.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> dhcp-options vendor-class-id <vendor-id>

Описание:

Присваивает идентификатор поставщика оборудования интерфейсу Ethernet. Если маршрутизатору Факел назначить идентификатор поставщика оборудования, то DHCP-сервер выдаст IP-адрес по тем правилам, которые применяются к соответствующему поставщику оборудования.

Синтаксис:

- set interfaces ethernet <interface> dhcp-options vendor-class-id <vendor-id>
- delete interfaces ethernet <interface> dhcp-options vendor-class-id <vendor-id>
- show interfaces ethernet <interface> dhcp-options vendor-class-id

Аргументы:

- <interface> — имя интерфейса Ethernet;

- `vendor-id` — идентификатор поставщика оборудования.Будет передан DHCP-серверу как строка с бинарными данными. Формат: произвольный.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> dhcp-options no-default-route

Описание:

Запрещает интерфейсу Ethernet запрашивать у DHCP-сервера шлюз по умолчанию. Интерфейс будет запрашивать только IP-адрес.

Синтаксис:

- set interfaces ethernet `<interface>` dhcp-options no-default-route
- delete interfaces ethernet `<interface>` dhcp-options no-default-route
- show interfaces ethernet `<interface>` dhcp-options

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> dhcp-options default-route-distance <distance>

Описание:

Задает на интерфейсе Ethernet приоритет до шлюза по умолчанию.

Синтаксис:

- set interfaces ethernet `<interface>` dhcp-options default-route-distance `<distance>`
- delete interfaces ethernet `<interface>` dhcp-options default-route-distance `<distance>`
- show interfaces ethernet `<interface>` dhcp-options default-route-distance

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<distance>` — приоритет до шлюза по умолчанию. Диапазон значений: от 1 до 255. Чем ниже значение, тем выше приоритет.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> dhcp-options reject <address>

Описание:

Указывает интерфейсу Ethernet не присваивать себе временно полученный IP-адрес от DHCP-сервера, а дождаться, когда DHCP-сервер назначит корректный IP-адрес.

Синтаксис:

- set interfaces ethernet `<interface>` dhcp-options reject `<address>`
- delete interfaces ethernet `<interface>` dhcp-options reject `<address>`
- show interfaces ethernet `<interface>` dhcp-options reject

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<address>`— IP-адрес, который будет проигнорирован интерфейсом. Можно задать несколько значений или указать диапазон IP-адресов. Пример: 192.168.100.0/24.

Режим: «Конфигурирование».

Совет

Используйте эту команду, если маршрутизатор присваивает себе при старте неправильный IP-адрес.

---

interfaces ethernet <interface> dhcp-options user-class <string>

Описание:

Добавляет пользовательское описание для DHCP-клиента на интерфейсе Ethernet. Обычно используется для обозначения группы пользователей.

Синтаксис:

- set interfaces ethernet `<interface>` dhcp-options user-class `<string>`
- delete interfaces ethernet `<interface>` dhcp-options user-class `<string>`
- interfaces ethernet `<interface>` dhcp-options user-class

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<string>` — пользовательское описание DHCP-клиента.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> dhcpv6-options duid <duid>

Описание:

Присваивает уникальный идентификатор DUID DHCP-клиенту на интерфейсе Ethernet. DUID необходим, чтобы получить IP-адрес от DHCPv6-сервера. Сервер сравнивает идентификатор DUID клиента со своей базой данных и в ответ выдает нужные настройки (IP-адрес, срок аренды, параметры DNS-серверов и т.д.).

DUID состоит из двухбитного поля типа DUID и поля с изменяемой частью длиной до 128 байт. Длина идентификатора зависит от его типа. Основные типы DUID: LLT (Link-Layer Address + Time) и UUID (Universally Unique Identifier).

DUID может быть создан вручную или сгенерирован автоматически сторонними средствами.

Более подробная информация содержится в документе RFC 3315.

Синтаксис:

- set interfaces ethernet `<interface>` dhcpv6-options duid `<duid>`
- delete interfaces ethernet `<interface>` dhcpv6-options duid `<duid>`
- show interfaces ethernet `<interface>` dhcpv6-options duid

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<duid>` — идентификатор DUID. Формат: зависит от типа DUID.

Режим: «Конфигурирование».

Совет

DUID типа LLT легче сгенерировать вручную нежели DUID типа UUID. Для этого необходимо перевести MAC-адрес устройства в шестнадцатеричный формат и добавить метку времени также в шестнадцатеричном формате.

---

interfaces ethernet <interface> duplex <auto | full | half>

Описание:

Настраивает работу дуплексного режима на интерфейсе Ethernet.

Синтаксис:

- set interfaces ethernet `<interface>` duplex `<auto | full | half>`
- delete interfaces ethernet `<interface>` duplex `<auto | full | half>`
- show interfaces ethernet `<interface>` duplex

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <auto> — дуплексный режим будет выбираться автоматически. Значение по умолчанию;
- <full> — интерфейс Ethernet будет работать в режиме полного дуплекса. Маршрутизатор сможет одновременно принимать и отправлять данные;
- <half> — интерфейс Ethernet будет работать в режиме полудуплекса. Маршрутизатор не сможет одновременно принимать и отправлять данные.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> speed <auto | 10 | 100 | 1000 | 2500 | 5000 | 10000 | 25000 | 40000 | 50000 | 100000>

Описание:

Устанавливает скорость обмена данными на интерфейсе Ethernet.

Синтаксис:

- set interfaces ethernet <interface> speed <auto | 10 | 100 | 1000 | 2500 | 5000 | 10000 | 25000 | 40000 | 50000 | 100000>
- delete interfaces ethernet <interface> speed <auto | 10 | 100 | 1000 | 2500 | 5000 | 10000 | 25000 | 40000 | 50000 | 100000>
- show interfaces ethernet <interface> speed

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <auto> — скорость обмена данными устанавливается автоматически. Значение по умолчанию;
- <10> — скорость в 10 Мбит/с;
- <100> — скорость в 100 Мбит/с;
- <1000> — скорость в 1 Гбит/с;
- <2500> — скорость в 2,5 Гбит/с;
- <5000> — скорость в 5 Гбит/с;
- <10000> — скорость в 10 Гбит/с;
- <25000> — скорость в 25 Гбит/с;
- <40000> — скорость в 40 Гбит/с;
- <50000> — скорость в 50 Гбит/с;
- <100000> — скорость в 100 Гбит/с.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> ring-buffer tx <value>

Описание:

Устанавливает размер кольцевого буфера при отправке данных с интерфейса Ethernet.

Синтаксис:

- set interfaces ethernet `<interface>` ring-buffer tx `<value>`
- delete interfaces ethernet `<interface>` ring-buffer tx `<value>`
- show interfaces ethernet `<interface>` ring-buffer tx

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<value>` — размер кольцевого буфера. Диапазон значений: от 80 до 16384.

Совет

Чтобы получить список значений, которые поддерживает интерфейс Ethernet, выполните команду: `ethtool -g <interface>`

---

interfaces ethernet <interface> offload <gro | gso | hw-tc-offload | lro | rfs | rps | sg | tso>

Описание

Включает различные механизмы аппаратной разгрузки ЦП на интерфейсе Ethernet.

Синтаксис:

- set interfaces ethernet <interface> offload `<interface> offload <gro | gso | hw-tc-offload | lro | rfs | rps | sg | tso>`
- delete interfaces ethernet `<interface> offload <gro | gso | hw-tc-offload | lro | rfs | rps | sg | tso>`
- show interfaces ethernet `<interface>` offload

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<gro>` — механизм Generic Receive Offload. Программная реализация аппаратной разгрузки. Снижает количество пакетов на сетевом стеке за счет объединения относительно похожих пакетов;
- `<lro>` — механизм Large Receive Offload. Объединяет несколько входящих пакетов из одного потока в общий буфер перед тем, как передать их выше по сетевому стеку. Уменьшает количество пакетов, которые необходимо обработать;
- `<gso>`— механизм Generic Segmentation Offload для увеличения пропускной способности. Программный аналог TSO. Данные одного пакета распределяются между остальными пакетами. Под-

держивает следующие типы пакетов IPv4: TCP, UDP, VXLAN, GRE TCP. Как правило, настраивается в паре с GRO;

- <hw-tc-offload> — механизм Hardware Traffic Control Flow Offload. Перенаправляет пакеты непосредственно на сетевое оборудование для ускорения обработки трафика;
- <rfs> — механизм Receive Flow Steering. Перенаправляет обработку пакетов из ядра на центральный процессор, где запущен поток приложения, которому адресованы пакеты. Повышает скорость обращения к кэшу данных;
- <rps> — механизм Receive Packet Steering. Программная реализация технологии Receive Side Scaling (RSS). Генерирует для входящих данных хэш, чтобы определить, какой CPU должен их обработать. Затем данные помещаются во входящую очередь этого процессора в ожидании последующей обработки;
- <sg> — механизм Scatter-Gather. Увеличивает скорость обработки сетевого трафика в маршрутизаторах за счет параллельной и одновременной обработки нескольких пакетов данных или запросов;
- <tso> — механизм TCP Segmentation Offloading.Сегментирует пакеты с помощью сетевой карты, а затем добавляет заголовки протоколов TCP, IP и канального уровня передачи данных к каждому сегменту.

Режим: «Конфигурирование».

Примечание

Чтобы использовать механизмы аппаратной разгрузки TSO или LRO на виртуальной сетевой картой VMXNET3, необходимо сначала включить механизм SG.

---

interfaces ethernet <interface> eapol ca-certificate <name>

Описание:

Присваивает сертификату на интерфейсе Ethernet имя записи в концепции SSL CA PKI для аутентификации устройств извне.

При подключении новых устройств интерфейс Ethernet будет сверять их сертификаты с сертификатом от центра сертификации. Если сертификат устройства будет признан действительным, устройство получит доступ к маршрутизатору.

Если устройство предоставит сертификат промежуточного центра сертификации, то все родительские центры сертификации в инфраструктуре PKI будут автоматически задействованы при проверке сертификата. Такой метод обеспечивает функционирование всей цепочки доверия. К родительским центрам сертификации относятся корневой центр сертификации или другие дополнительные промежуточные центры сертификации.

Синтаксис:

- set interfaces ethernet <interface> eapol ca-certificate <name>
- delete interfaces ethernet <interface> eapol ca-certificate <name>
- show interfaces ethernet <interface> eapol ca-certificate

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <name> — имя записи в концепции SSL CA PKI.

Режим: «Конфигурирование».

Примечание

По умолчанию при аутентификации по протоколу EAPoL в качестве идентификатора ПО Факел использует MAC-адрес.

---

interfaces ethernet <interface> eapol certificate <name>

Описание:

Присваивает имя для пары из открытого и закрытого ключей с сертификатами x509. Клиент будет использовать ключи, чтобы получить доступ к системе, защищенной по стандарту безопасности 802.1x. Все сертификаты, выданные родительскими центрами сертификации (такими как промежуточный центр сертификации и корневой центр сертификации), будут отправлены клиентом на сервер аутентификации как часть доверительного рукопожатия EAP-TLS.

Синтаксис:

- set interfaces ethernet <interface> eapol certificate <name>
- delete interfaces ethernet <interface> eapol certificate <name>
- show interfaces ethernet <interface> eapol certificate

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <name> — имя записи в концепции SSL CA PKI.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> evpn uplink

Описание:

Следит за состоянием связи с вышестоящим устройством. Если произойдет обрыв на физической сети, то маршрутизатор на стороне провайдера потеряет доступ к VxLAN и виртуальной сети. В таком случае,

чтобы предотвратить потерю пакетов, маршрутизатор на стороне провайдера остановит связь между сервером и остальным сегментом Ethernet.

Синтаксис:

- set interfaces ethernet `<interface>` evpn uplink
- delete interfaces ethernet `<interface>` evpn uplink
- show interfaces ethernet `<interface>` evpn

Аргументы:

- `<interface>` — имя интерфейса Ethernet

Режим: «Конфигурирование».

Режим «Администрирование»

interfaces ethernet

Описание:

Отображает краткую информацию о статусе всех интерфейсов Ethernet.

Синтаксис:

- show interfaces ethernet

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces ethernet <interface>

Описание:

Отображает детальную информацию о статусе конкретного интерфейса Ethernet.

Синтаксис:

- show interfaces ethernet `<interface>`

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces ethernet <interface> physical

Описание:

Отображает детальную информацию об аппаратных возможностях и статусе конкретного интерфейса Ethernet.

Синтаксис:

- show interfaces ethernet `<interface>` physical

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces ethernet <interface> physical offload

Описание:

Отображает детальную информацию о доступных способах аппаратной разгрузки сетевой карты и об их статусе.

Синтаксис:

- show interfaces ethernet `<interface>` physical offload

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces ethernet <interface> transceiver

Описание:

Отображает информацию о подключаемых приемо-передающих модулях, таких как SFP+, QSFP и др.

Синтаксис:

- show interfaces ethernet `<interface>` transceiver

Аргументы:

- `<interface>` — имя интерфейса Ethernet.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

VLAN-интерфейс

Обзор

Маршрутизатор Факел поддерживает стандарт инкапсуляции данных IEEE 802.1q, что позволяет создавать виртуальные VLAN-интерфейсы на базе физического интерфейса Ethernet. В ПО Факел такие виртуальные субинтерфейсы обозначаются термином *vif*.

Список команд

Режим «Конфигурирование»

interfaces ethernet <interface> vif <vlan-id>

Описание:

Создает на интерфейсе Ethernet новый виртуальный VLAN-интерфейс. На одном физическом интерфейсе может быть создано несколько виртуальных интерфейсов.

Синтаксис:

- set interfaces ethernet `<interface>` vif `<vlan-id>`
- delete interfaces ethernet `<interface>` vif `<vlan-id>`
- show interfaces ethernet `<interface>` vif

Аргументы:

- `<interfaces>` — имя интерфейса Ethernet;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Примечание
VLAN-интерфейс может принимать лишь пакеты с метками типа 802.1q.

---

interfaces ethernet <interface> vif <vlan-id> address <address | dhcp | dhcpv6>

Описание:

Устанавливает, каким способом IP-адрес будет назначен VLAN-интерфейсу.

Синтаксис: * set interfaces ethernet <interface> vif <vlan-id> address <address | dhcp | dhcpv6> * delete interfaces ethernet <interface> vif <vlan-id> address <address | dhcp | dhcpv6> * show interfaces ethernet <interface> vif <vlan-id> address

Аргументы: * <interface> — имя интерфейса Ethernet; * <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094; * <address> — IP-адрес, который администратор вручную назначает интерфейсу Ethernet. Может быть указан несколько раз как адрес; * <dhcp> — DHCPv4-сервер автоматически назначит IPv4-адрес интерфейсу Ethernet на конкретном сегменте сети; .. * <dhcpv6> — DHCPv6-сервер автоматически назначит IPv6-адрес интерфейсу Ethernet на конкретном сегменте сети.

Режим: «Конфигурирование».

Примечание

Если вы используете протокол DHCP для получения IPv4-адреса и вам требуется дополнительная настройка, используйте указатели начала и конца данных. Эти файлы расположены в директории:

- /config/scripts/dhcp-client/pre-hooks.d/
- /config/scripts/dhcp-client/post-hooks.d/

---

interfaces ethernet <interface> vif <vlan-id> description <description>

Описание:

Добавляет описание для VLAN-интерфейса.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> description <description>
- delete interfaces ethernet <interface> vif <vlan-id> description <description>
- show interfaces ethernet <interface> vif <vlan-id> description

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <description> — описание VLAN-интерфейса.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к VLAN-интерфейсу по указанному описанию.

---

interfaces ethernet <interface> vif <vlan-id> disable

Описание:

Выключает VLAN-интерфейс. VLAN-интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> disable
- delete interfaces ethernet <interface> vif <vlan-id> disable
- show interfaces ethernet <interface> vif <vlan-id>

Аргументы: * <interface> — имя интерфейса Ethernet; * <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> disable-link-detect

Описание:

Прекращает отслеживать состояние физического соединения на VLAN-интерфейсе. Если соединение по Ethernet-кабелю пропадет, система проигнорирует это событие для VLAN-интерфейса. По умолчанию состояние физического соединения отслеживается.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> disable-link-detect
- delete interfaces ethernet <interface> vif <vlan-id> disable-link-detect
- show interfaces ethernet <interface> vif <vlan-id>

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>

Описание:

Назначает пользовательский MAC-адрес для VLAN-интерфейса.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>

- delete interfaces ethernet <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>
- show interfaces ethernet <interface> vif <vlan-id> mac

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <xx:xx:xx:xx:xx:xx> — MAC-адрес.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на VLAN-интерфейсе.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> mtu <mtu>
- delete interfaces ethernet <interface> vif <vlan-id> mtu <mtu>
- show interfaces ethernet <interface> vif <vlan-id> mtu

Аргументы: <interface> — имя интерфейса Ethernet; <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094; <mtu> — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>

Описание:

Устанавливает на VLAN-интерфейсе конкретное значение для максимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>
- delete interfaces ethernet <interface> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>

- show interfaces ethernet <interface> vif <vlan-id> ip adjust-mss

Аргументы: * <interface> — имя интерфейса Ethernet; * <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094; * <mss> — конкретное значение для максимального размера сегмента на протоколе TCP; * <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces ethernet <interface> vif <vlan-id> ip arp-cache-timeout <sec>

Описание:

Задает временной интервал между записями в ARP-кэш на VLAN-интерфейсе. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip arp-cache-timeout <sec>
- delete interfaces ethernet <interface> vif <vlan-id> ip arp-cache-timeout <sec>
- show interfaces ethernet <interface> vif <vlan-id> ip arp-cache-timeout

Аргументы:

- <interface> — имя интерфейса Ethernet.
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <sec> — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip disable-arp-filter

Описание: | Выключает фильтрацию по протоколу ARP на VLAN-интерфейсе. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами. | Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный

интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set ethernet <interface> vif <vlan-id> ip disable-arp-filter
- delete ethernet <interface> vif <vlan-id> ip disable-arp-filter
- show ethernet <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с VLAN-интерфейса на любой другой интерфейс. После выполнения команды VLAN-интерфейс перейдет в режим хоста.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip disable-forwarding
- delete interfaces ethernet <interface> vif <vlan-id> ip disable-forwarding
- show interfaces ethernet <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip enable-directed-broadcast

Описание:

Включает на VLAN-интерфейсе различные режимы направленной широковещательной переадресации. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на подсеть назначения.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip enable-directed-broadcast

- delete interfaces ethernet <interface> vif <vlan-id> ip enable-directed-broadcast
- show interfaces ethernet <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице VLAN-интерфейса для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица будет обновлена даже если команда не была выполнена.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip enable-arp-accept
- delete interfaces ethernet <interface> vif <vlan-id> ip enable-arp-accept
- show interfaces ethernet <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip enable-arp-announce

Описание:

Ограничивает на VLAN-интерфейсе анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. ПО Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса VLAN-интерфейс проверяет все целевые подсети. По умолчанию ПО Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip enable-arp-announce
- delete interfaces ethernet <interface> vif <vlan-id> ip enable-arp-announce

- show interfaces ethernet <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Совет

Если вы выполнили команду, то при отправке ARP-запросов не используйте адреса вне подсети назначения.

---

interfaces ethernet <interface> vif <vlan-id> ip enable-arp-ignore

Описание

Указывает VLAN-интерфейсу отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию VLAN-интерфейс отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе, независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip enable-arp-ignore
- delete interfaces ethernet <interface> vif <vlan-id> ip enable-arp-ignore
- show interfaces ethernet <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip enable-proxy-arp

Описание:

Включает прокси-сервер на VLAN-интерфейсе для маршрутизации ARP-запросов. VLAN-интерфейс сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip enable-proxy-arp
- delete interfaces ethernet <interface> vif <vlan-id> ip enable-proxy-arp
- show interfaces ethernet <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip proxy-arp-pvlan

Описание:

Создает на VLAN-интерфейсе частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip proxy-arp-pvlan
- delete interfaces ethernet <interface> vif <vlan-id> ip proxy-arp-pvlan
- show interfaces ethernet <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Подсказка

Вы можете использовать эту команду без предварительного выполнения команды `interfaces ethernet <interface> ip enable-proxy-arp`.

---

interfaces ethernet <interface> vif <vlan-id> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> redirect <destination>
- delete interfaces ethernet <interface> vif <vlan-id> redirect <destination>
- show interfaces ethernet <interface> vif <vlan-id> redirect

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <destination> — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip source-validation <strict | loose | disable>

Описание:

Включает на VLAN-интерфейсе различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip source-validation <strict | loose | disable>
- delete interfaces ethernet <interface> vif <vlan-id> ip source-validation <strict | loose | disable>
- show interfaces ethernet <interface> vif <vlan-id> ip source-validation

Аргументы:

- <interface> — имя интерфейса Ethernet.
- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> vrf <vrf>

Описание:

Размещает VLAN-интерфейс на указанном VRF-экземпляре.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> vrf <vrf>
- delete interfaces ethernet <interface> vif <vlan-id> vrf <vrf>
- show interfaces ethernet <interface> vif <vlan-id> vrf

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> dhcp-options client-id <description>

Описание:

Присваивает идентификатор клиента VLAN-интерфейсу. VLAN-интерфейс будет отображать свой идентификатор при запросе IP-адреса у DHCPv6-сервера.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> dhcp-options client-id <description>
- delete interfaces ethernet <interface> vif <vlan-id> dhcp-options client-id <description>
- show interfaces ethernet <interface> vif <vlan-id> dhcp-options client-id

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <description> — идентификатор клиента. Формат: произвольный.

Режим: «Конфигурирование».

Примечание

Более подробная информация содержится в документе RFC 2131. Отмечается, что клиент может специально ограничить свое обнаружение только посредством идентификатора (опция -client identifier-). В этом случае клиенту необходимо будет использовать один и тот же идентификатор во всех последующих сообщениях ICMPv6, а серверу придется использовать точно такой же идентификатор для нахождения клиента.

interfaces ethernet <interface> vif <vlan-id> dhcp-options host-name <hostname>

Описание:

Присваивает имя хоста DHCPv6-серверу на VLAN-интерфейсе. Созданное имя заменит имя хоста по умолчанию. Когда клиент будет запрашивать IP-адрес у VLAN-интерфейса, ему отобразится присвоенное имя хоста.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> dhcp-options host-name <hostname>
- delete interfaces ethernet <interface> vif <vlan-id> dhcp-options host-name <hostname>
- show interfaces ethernet <interface> vif <vlan-id> dhcp-options host-name

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <hostname> — имя хоста.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> dhcp-options vendor-class-id <vendor-id>

Описание:

Присваивает идентификатор поставщика оборудования VLAN-интерфейсу. Если маршрутизатору Факел назначить идентификатор поставщика оборудования, то DHCP-сервер выдаст IP-адрес по тем правилам, которые применяются к соответствующему поставщику оборудования.

Синтаксис:

- set ethernet <interface> vif <vlan-id> dhcp-options vendor-class-id <vendor-id>
- delete ethernet <interface> vif <vlan-id> dhcp-options vendor-class-id <vendor-id>
- show ethernet <interface> vif <vlan-id> dhcp-options vendor-class-id

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <vendor-id> — идентификатор поставщика оборудования. Формат: произвольный. Будет передан DHCP-серверу как строка с бинарными данными.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> dhcp-options no-default-route

Описание:

Запрещает VLAN-интерфейсу запрашивать у DHCP-сервера шлюз по умолчанию. Интерфейс будет запрашивать только IP-адрес.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> dhcp-options no-default-route
- delete interfaces ethernet <interface> vif <vlan-id> dhcp-options no-default-route
- show interfaces ethernet <interface> vif <vlan-id> dhcp-options

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> dhcp-options default-route-distance <distance>

Описание:

Задает на VLAN-интерфейсе приоритет до шлюза по умолчанию.

Синтаксис:

- set ethernet <interface> vif <vlan-id> dhcp-options default-route-distance <distance>
- delete ethernet <interface> vif <vlan-id> dhcp-options default-route-distance <distance>
- show ethernet <interface> vif <vlan-id> dhcp-options default-route-distance

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <distance> — приоритет до шлюза по умолчанию. Диапазон значений: от 1 до 255. Чем ниже значение, тем выше приоритет.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> dhcp-options reject <address>

Описание:

Указывает VLAN-интерфейсу не присваивать себе временно полученный IP-адрес от DHCP-сервера, а дождаться, когда DHCP-сервер назначит корректный IP-адрес.

Синтаксис:

- set ethernet <interface> vif <vlan-id> dhcp-options reject <address>
- delete ethernet <interface> vif <vlan-id> dhcp-options reject <address>
- show ethernet <interface> vif <vlan-id> dhcp-options reject

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <address>— IP-адрес, который будет проигнорирован интерфейсом. Можно задать несколько значений или указать диапазон IP-адресов. Пример: 192.168.100.0/24.

Режим: «Конфигурирование».

Совет

Используйте эту команду, если маршрутизатор присваивает себе при старте неправильный IP-адрес.

---

interfaces ethernet <interface> vif <vlan-id> dhcp-options user-class <string>

Описание:

Добавляет пользовательское описание для DHCP-клиента на VLAN-интерфейсе. Обычно используется для обозначения группы пользователей.

Синтаксис:

- set ethernet <interface> vif <vlan-id> dhcp-options user-class <string>
- delete ethernet <interface> vif <vlan-id> dhcp-options user-class <string>
- show ethernet <interface> vif <vlan-id> dhcp-options user-class

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <string> — пользовательское описание DHCP-клиента.

Режим: «Конфигурирование».

Режим «Администрирование»

interfaces ethernet <interface> vif <vlan-id> brief

Описание:

Отображает краткую информацию о конкретном VLAN-интерфейсе.

Синтаксис:

- show interfaces ethernet <interface> vif <vlan-id> brief

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces ethernet <interface> vif <vlan-id>

Описание:

Отображает детальную информацию о конкретном VLAN-интерфейсе.

Синтаксис:

- show interfaces ethernet <interface> vif <vlan-id>

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Интерфейс Q-in-Q

Обзор

Маршрутизатор Факел поддерживает стандарт двойной инкапсуляции данных IEEE 802.ad, что позволяет создавать виртуальные интерфейсы Q-in-Q на базе физического интерфейса Ethernet. Технология Q-in-Q инкапсулирует две метки стандарта 802.1q в один кадр данных. Таким образом удается построить сети более крупного масштаба в соответствии с топологией Metro Ethernet.

В ПО Факел *vif-s* и *vif-c* — метки поля EtherType в кадре Ethernet. Метка vif-s располагается ближе к заголовку Ethernet и называется меткой сети провайдера, ее значение EtherType: 0x88a8. Метка vif-c находится ближе к части кадра с полезными данными и называется меткой сети клиента, ее значение EtherType: 0x8100. Трафик на VLAN-интерфейсе с метками vif-c является внутренним по отношению к трафику с меткой vif-s на другом VLAN-интерфейсе. Соответственно, трафик с меткой vif-s является внешним по отношению к трафику с меткой vif-c.

Список команд

Режим «Конфигурирование»

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> address <address | dhcp | dhcpv6>

Описание:

Устанавливает способ назначения IP-адреса интерфейсу Q-in-Q.

Синтаксис:

- set ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` address `<address | dhcp | dhcpv6>`
- delete ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` address `<address | dhcp | dhcpv6>`
- show ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` address

Аргументы: * `<interface>` — имя интерфейса Ethernet; * `<vlan-id>` — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094; * `<address>` — IP-адрес, который администратор присваивает интерфейсу Ethernet. Может быть указан несколько раз как адрес; * `dhcp` — DHCPv4-сервер автоматически назначит IPv4-адрес интерфейсу Q-in-Q на конкретном сегменте сети; .. * `dhcpv6` — DHCPv6-сервер автоматически назначит IPv6-адрес интерфейсу Q-in-Q на конкретном сегменте сети.

Режим: «Конфигурирование».

Примечание

Если вы используете протокол DHCP для получения IPv4-адреса и вам требуется дополнительная настройка, используйте указатели начала и конца данных. Эти файлы расположены в директории:

- /config/scripts/dhcp-client/pre-hooks.d/
- /config/scripts/dhcp-client/post-hooks.d/

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> description <description>

Описание:

Добавляет описание для интерфейса Q-in-Q.

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` description `<description>`
- delete interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` description `<description>`
- show interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` description

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `vland-id` — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- `description` — описание интерфейса Q-in-Q.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к VLAN-интерфейсу по указанному описанию.

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> disable

Описание:

Выключает интерфейс Q-in-Q. Интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` disable
- delete interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` disable

- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id>

Аргументы:

- <interface> — имя интерфейса Ethernet;
- vland-id — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> disable-link-detect

Описание:

Прекращает отслеживать состояние физического соединения на интерфейсе Q-in-Q. Если соединение по Ethernet-кабелю пропадет, система проигнорирует это событие для интерфейса Q-in-Q. По умолчанию состояние физического соединения отслеживается.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> disable-link-detect
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> disable-link-detect
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id>

Аргументы:

- <interface> — имя интерфейса Ethernet;
- vland-id — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> mac <xx:xx:xx:xx:xx:xx>

Описание:

Назначает пользовательский MAC-адрес интерфейсу Q-in-Q.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> mac <xx:xx:xx:xx:xx:xx>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> mac <xx:xx:xx:xx:xx:xx>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> mac

Аргументы:

- <interface> — имя интерфейса Ethernet;

- `vland-id` — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- `<xx:xx:xx:xx:xx:xx>` — MAC-адрес.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на интерфейсе Q-in-Q.

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` mtu `<mtu>`
- delete interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` mtu `<mtu>`
- show interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` mtu

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `vland-id` — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- `<mtu>` — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>

Описание:

Устанавливает на интерфейсе Q-in-Q конкретное значение для ммаксимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` ip adjust-mss `<mss | clamp-mss-to-pmtu>`
- delete interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` ip adjust-mss `<mss | clamp-mss-to-pmtu>`

- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip adjust-mss

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <mss> — конкретное значение для максимального размера сегмента на протоколе TCP;
- <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip arp-cache-timeout <sec>

Описание:

Задает временной интервал между записями в ARP-кэш на интерфейсе Q-in-Q. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip arp-cache-timeout <sec>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip arp-cache-timeout <sec>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip arp-cache-timeout

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <sec> — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip disable-arp-filter

Описание:

Выключает фильтрацию по протоколу ARP на интерфейсе Q-in-Q. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами.

Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip disable-arp-filter
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip disable-arp-filter
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с интерфейса Q-in-Q на любой другой интерфейс. После выполнения команды интерфейс Q-in-Q перейдет в режим хоста.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip disable-forwarding
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip disable-forwarding
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif <vlan-id> ip enable-directed-broadcast

Описание:

Включает направленную широковещательную переадресацию на интерфейсе Q-in-Q. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на подсеть назначения.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces ethernet <interface> vif <vlan-id> ip enable-directed-broadcast
- delete interfaces ethernet <interface> vif <vlan-id> ip enable-directed-broadcast
- show interfaces ethernet <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице интерфейса Q-in-Q для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица все равно будет обновлена, даже если команда не была выполнена.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip enable-arp-accept
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip enable-arp-accept
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip enable-arp-announce

Описание:

Ограничивает на интерфейсе Q-in-Q анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. ПО Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса интерфейс Q-in-Q проверяет все целевые подсети. По умолчанию ПО Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` ip enable-arp-announce
- delete interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` ip enable-arp-announce
- show ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` ip

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<vlan-id>` — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

Совет

Если вы выполнили команду, то при отправке ARP-запросов не используйте адреса вне подсети назначения.

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip enable-arp-ignore

Описание

Указывает интерфейсу Q-in-Q отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию интерфейс Q-in-Q отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе, независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` ip enable-arp-ignore
- delete set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` ip enable-arp-ignore
- show set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip enable-proxy-arp

Описание:

Включает прокси-сервер на интерфейсе Q-in-Q для маршрутизации ARP-запросов. Интерфейс Q-in-Q сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip enable-proxy-arp
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip enable-proxy-arp
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip proxy-arp-pvlan

Описание:

Создает на интерфейсе Q-in-Q частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip proxy-arp-pvlan
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip proxy-arp-pvlan
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<vlan-id>` — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

Подсказка

Вы можете использовать эту команду без предварительного выполнения команды `interfaces ethernet <interface> ip enable-proxy-arp`.

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` redirect `<destination>`
- delete interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` redirect `<destination>`
- show interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` redirect

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<vlan-id>` — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- `<destination>` — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip source-validation <strict | loose | disable>

Описание:

Включает на интерфейсе Q-in-Q различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` ip source-validation `<strict | loose | disable>`

- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip source-validation <strict | loose | disable>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ip source-validation

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отвергнут. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отвергнут;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

Описание:

Включает на интерфейсе Q-in-Q механизм получения IPv6-адреса другими устройствами через автоматическую настройку адресов без сохранения состояния (SLAAC).
Хост-устройства с поддержкой связи по протоколу IPv6 могут автоматически производить свою настройку при подключении к сети IPv6 при обмене сообщениями ICMPv6 по протоколу обнаружения соседей.

При первичном подключении хост-устройство отправляет многоадресную рассылку с запросом параметров у маршрутизатора. Роутер отвечает на запрос и высылает объявление, которое содержит параметры конфигурации сетевого уровня. Узнав эти параметры, хост-устройство сможет подключиться к маршрутизатору.

Более подробная информация содержится в документе RFC 4862.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 address autoconf
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 address autoconf
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 address

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

Примечание

Команда автоматически выключает перенаправление IPv6-трафика на интерфейсе Q-in-Q.

Описание:

Запускает преобразование EUI-64 на интерфейсе Q-in-Q. После этого хост-устройство сгенерирует себе уникальный 64-битный IPv6-адрес на основе своего MAC-адреса.

Более подробная информация содержится в документах RFC 4291.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 address eui64 <prefix>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 address eui64 <prefix>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 address eui64

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <prefix> — префикс IPv6-адреса. Будет добавлен к основной части IPv6-адреса при запуске преобразования EUI-64.

Режим: «Конфигурирование».

Описание:

Запрещает назначать IPv6-адрес интерфейсу Q-in-Q для связи между локальными устройствами.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 address no-default-link-local
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 address no-default-link-local
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 address

Аргументы:

- <interface> — имя интерфейса Ethernet;

- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

Описание:

Выключает переадресацию пакетов по протоколу IPv6 с интерфейса Q-in-Q на любой другой интерфейс. После выполнения команды интерфейс Q-in-Q перейдет в режим хоста.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 disable-forwarding
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 disable-forwarding
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

Описание:

Устанавливает на интерфейсе Q-in-Q конкретное значение для максимального размера сегмента при передаче IPv6-пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 adjust-mss

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

Подсказка

Максимальный размера сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

Описание:

Настраивает работу механизма обнаружения дубликатов IPv6-адресов на интерфейсе Q-in-Q.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 accept-dad <1-3>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 accept-dad <1-3>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 accept-dad

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <0> — выключает механизм по обнаружению дубликатов IPv6-адресов.
- <1> — включает механизм по обнаружению дубликатов IPv6-адресов. Значение по умолчанию;
- <2> — включает механизм по обнаружению дубликатов IPv6- и MAC-адресов в сегменте локальной сети. Если будут найдены два устройства с одинаковыми MAC-адресами и использующие одинаковые IPv6-адреса на одном сегменте сети, передача данных по протоколу IPv6 будет остановлена для избежания конфликтов.

Режим: «Конфигурирование».

Описание:

Задает, сколько сообщений типа «опрос соседа» интерфейс Q-in-Q отправит по сети для обнаружения дубликатов IPv6-адресов.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 dup-addr-detect-transmits <n>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 dup-addr-detect-transmits <n>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> ipv6 dup-addr-detect-transmits

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <n> — количество сообщений типа «опрос соседа», рассылаемых по сети.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> vrf <vrf>

Описание:

Размещает интерфейс Q-in-Q на указанном VRF-экземпляре.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> vrf <vrf>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> vrf <vrf>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> vrf

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options client-id <description>

Описание:

Присваивает интерфейсу Q-in-Q идентификатор клиента. Интерфейс Q-in-Q будет отображать свой идентификатор при запросе IP-адреса у DHCPv6-сервера.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options client-id <description>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options client-id <description>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options client-id

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <description> — идентификатор клиента. Формат: произвольный.

Режим: «Конфигурирование».

Примечание

Подробно принцип работы описан в документе RFC 2131. В частности, отмечается, что клиент может специально ограничить свое обнаружение только посредством идентификатора (опция -client identifier-). В этом случае клиенту необходимо будет использовать один и тот же идентификатор во всех последующих сообщениях ICMPv6, а серверу придется использовать точно такой же идентификатор для нахождения клиента.

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options host-name <hostname>

Описание:

Присваивает имя хоста DHCPv6-серверу на интерфейсе Q-in-Q. Созданное имя заменит имя хоста по умолчанию. Когда клиент будет запрашивать IP-адрес у интерфейса Q-in-Q, ему отобразится присвоенное имя хоста.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options host-name <hostname>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options host-name <hostname>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options host-name

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <hostname> — имя хоста.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options vendor-class-id <vendor-id>

Описание:

Присваивает идентификатор поставщика оборудования интерфейсу Q-in-Q. Если маршрутизатору Факел назначить идентификатор поставщика оборудования, то DHCPv6-сервер выдаст IP-адрес по тем правилам, которые применяются к соответствующему поставщику оборудования.

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` dhcp-options vendor-class-id `<vendor-id>`
- delete interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` dhcp-options vendor-class-id `<vendor-id>`
- show interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` dhcp-options vendor-class-id

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<vlan-id>` — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- `vendor-id` — идентификатор поставщика оборудования. Формат: произвольный. Будет передан DHCP-серверу как строка с бинарными данными.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options no-default-route

Описание:

Запрещает интерфейсу Q-in-Q запрашивать у DHCP-сервера шлюз по умолчанию. Интерфейс будет запрашивать только IP-адрес.

Синтаксис:

- set interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` dhcp-options no-default-route
- delete interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` dhcp-options no-default-route
- show interfaces ethernet `<interface>` vif-s `<vlan-id>` vif-c `<vlan-id>` dhcp-options

Аргументы:

- `<interface>` — имя интерфейса Ethernet;

- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options default-route-distance <distance>

Описание:

Задает на интерфейсе Q-in-Q приоритет до шлюза по умолчанию.

Синтаксис:

- set interfaces ethernet <interface> vif-s <*vlan-id*> vif-c <vlan-id> dhcp-options default-route-distance <distance>
- delete interfaces ethernet <interface> vif-s <*vlan-id*> vif-c <vlan-id> dhcp-options default-route-distance <distance>
- show interfaces ethernet <interface> vif-s <*vlan-id*> vif-c <vlan-id> dhcp-options default-route-distance

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <distance> — приоритет до шлюза по умолчанию. Диапазон значений: от 1 до 255. Чем ниже значение, тем выше приоритет.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options reject <address>

Описание:

Указывает интерфейсу Q-in-Q не присваивать себе временно полученный IP-адрес от DHCP-сервера, а дождаться, когда DHCP-сервер назначит корректный IP-адрес.

Синтаксис:

- set interfaces ethernet <interface> vif-s :code:`<vlan-id> vif-c <vlan-id> dhcp-options reject <address>
- delete interfaces ethernet <interface> vif-s :code:`<vlan-id> vif-c <vlan-id> dhcp-options reject <address>
- show interfaces ethernet <interface> vif-s :code:`<vlan-id> vif-c <vlan-id> dhcp-options reject

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <address>— IP-адрес, который будет проигнорирован интерфейсом. Можно задать несколько значений или указать диапазон IP-адресов. Пример: 192.168.100.0/24.

Режим: «Конфигурирование».

Совет

Используйте эту команду, если маршрутизатор присваивает себе при старте неправильный IP-адрес.

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options user-class <string>

Описание:

Добавляет пользовательское описание для DHCP-клиента на интерфейсе Q-in-Q. Обычно используется для обозначения группы пользователей.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options user-class <string>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options user-class <string>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcp-options user-class

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <string> — пользовательское описание DHCP-клиента.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcpv6-options duid <duid>

Описание:

Присваивает уникальный идентификатор DUID DHCP-клиенту на интерфейсе Q-in-Q. DUID необходим, чтобы получить IP-адрес от DHCPv6-сервера. Сервер сравнивает идентификатор DUID клиента со своей базой данных и в ответ выдает нужные настройки (IP-адрес, срок аренды, параметры DNS-серверов и т.д.).

DUID состоит из двухбитного поля типа DUID и поля с изменяемой частью длиной до 128 байт. Длина идентификатора зависит от его типа. Основные типы DUID: LLT (Link-Layer Address + Time) и UUID (Universally Unique Identifier).

DUID может быть создан вручную или сгенерирован автоматически сторонними средствами.

Более подробная информация содержится в документе RFC 3315.

Синтаксис:

- set interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcpv6-options duid <duid>
- delete interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcpv6-options duid <duid>
- show interfaces ethernet <interface> vif-s <vlan-id> vif-c <vlan-id> dhcpv6-options duid

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса на интерфейсе Q-in-Q. Диапазон значений: от 0 до 4094;
- <duid> — идентификатор DUID. Формат: зависит от типа DUID.

Режим: «Конфигурирование».

Совет

DUID типа LLT легче сгенерировать вручную нежели DUID типа UUID. Для этого необходимо перевести MAC-адрес устройства в шестнадцатеричный формат и добавить метку времени также в шестнадцатеричном формате.

Режим «Администрирование»

interfaces ethernet <interface> vif <vlan-id> brief

Описание:

Отображает краткую информацию только о трафике с меткой сети провайдера на интерфейсе Q-in-Q.

Синтаксис:

- show interfaces ethernet <interface> vif <vlan-id> brief

Аргументы:

- <interface> — имя интерфейса Ethernet;

- <vlan-id> — идентификатор VLAN-интерфейса, который обрабатывает трафик с меткой сети провайдера. Диапазон значений: от 0 до 4094.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces ethernet <interface> vif <vlan-id>

Описание:

Отображает детальную информацию только о трафике с меткой сети провайдера на интерфейсе Q-in-Q.

Синтаксис:

- show interfaces ethernet <interface> vif <vlan-id> brief

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <vlan-id> — идентификатор VLAN-интерфейса, который обрабатывает трафик с меткой сети провайдера. Диапазон значений: от 0 до 4094.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Зеркалирование интерфейса Ethernet

Обзор

Зеркалирование дублирует входящий или исходящий трафик с физического интерфейса Ethernet на физический или виртуальный *SPAN-интерфейс*. К SPAN-интерфейсу может быть подключено специальное анализирующее оборудование или ПО: система контроля поведения, система обнаружения вторжения, сборщик трафика. Технология зеркалирования анализирует трафик изолировано от порта с исходным трафиком и не оказывает влияния на передаваемые данные или быстродействие системы.

Для каждого направления трафика существует своя настройка: *mirror ingress* для входящего трафика и *mirror egress* для исходящего. SPAN-интерфейсы должны быть настроены отдельно для трафика с различным направлением.

Список команд

Режим «Конфигурирование»

interfaces ethernet <interface> mirror ingress <monitor-interface>

Описание:
Дублирует входящий трафик с порта интерфейса Ethernet на порт SPAN-интерфейса.

Синтаксис:

- set interfaces ethernet `<interface>` mirror ingress `<monitor-interface>`
- delete interfaces ethernet `<interface>` mirror ingress `<monitor-interface>`
- show interfaces ethernet `<interface>` mirror ingress

Аргументы:

- `<interface>` — имя интерфейса Ethernet;
- `<monitor-interface>` — имя SPAN-интерфейса.

Режим: «Конфигурирование».

---

interfaces ethernet <interface> mirror egress <monitor-interface>

Описание:
Дублирует исходящий трафик с порта интерфейса Ethernet на порт SPAN-интерфейса.

Синтаксис:

- set interfaces ethernet <interface> mirror egress <monitor-interface>
- delete interfaces ethernet <interface> mirror egress <monitor-interface>
- show interfaces ethernet <interface> mirror egress

Аргументы:

- <interface> — имя интерфейса Ethernet;
- <monitor-interface> — имя SPAN-интерфейса.

Режим: «Конфигурирование».

2.2.2 Агрегированный интерфейс

2.2.2.1 Обзор

Технология агрегирования каналов объединяет несколько независимых *физических сетевых интерфейсов* в один *логический агрегированный интерфейс*. Один агрегированный интерфейс может объединять до 8 физических интерфейсов.

По умолчанию маршрутизатор Факел агрегирует каналы по протоколу IEEE 802.3ad. Режимы агрегирования влияют на поведение и производительность агрегированного интерфейса. Всего доступно 7 режимов агрегирования.

При правильной настройке агрегирование каналов способно дать ряд преимуществ:

1. Увеличивается пропускная способность канала связи.
2. Нагрузка распределяется между несколькими физическими интерфейсами.
3. Обеспечивается горячее резервирование каналов. Если один из физических интерфейсов выйдет из строя, трафик без потери связи будет перенаправлен на рабочие порты.
4. Отслеживается состояние каналов связи.

Администратор маршрутизатора Факел может создавать на агрегированном интерфейсе VLAN-интерфейсы, зеркалировать трафик, настраивать множественную адресацию и выполнять ряд других операций.

2.2.2.2 Пример настройки

Шаг	Команда	Описание
1	set interfaces bonding `bond1` member interface `eth6`	Добавляет физический сетевой интерфейс `eth6` в состав агрегированного интерфейса `bond1`
2	set interfaces bonding `bond1` address `dhcp`	DHCP-сервер назначит IP-адрес агрегированному интерфейсу автоматически
3	set interfaces bonding `bond1` mode `round-robin`	Включает на агрегированном интерфейсе режим циклического алгоритма. Пакеты будут распределяться по порядку от первого доступного физического интерфейса к следующему

2.2.2.3 Список команд

Режим «Конфигурирование»

interfaces bonding <interface> member interface <member>

Описание:

Добавляет физический сетевой интерфейс в состав агрегированного интерфейса.

Синтаксис:

- set interfaces bonding `<interface>` member interface `<member>`
- delete interfaces bonding `<interface>` member interface `<member>`
- show interfaces bonding `<interface>` member interface

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<member>` — имя физического интерфейса Ethernet, который будет добавлен в состав агрегированного интерфейса. Интерфейсы добавляются по очереди.

Режим: «Конфигурирование».

Примечание

Одновременно в составе агрегированного интерфейса могут работать лишь 8 физических интерфейсов.

---

interfaces bonding <interface> mode <802.3ad | active-backup | broadcast | round-robin | transmit-load-balance | adaptive-load-balance | xor-hash>

Описание:

Включает различные режимы объединения физических интерфейсов в агрегированный интерфейс.

Синтаксис:

- set interfaces bonding `<interface>` mode `<802.3ad | active-backup | broadcast | round-robin | transmit-load-balance | adaptive-load-balance | xor-hash>`
- delete interfaces bonding `<interface>` mode `<802.3ad | active-backup | broadcast | round-robin | transmit-load-balance | adaptive-load-balance | xor-hash>`
- show interfaces bonding `<interface>` mode

Аргументы:

- `<interface>` — имя агрегированного интерфейса;

- <802.3ad> — режим динамической агрегации по протоколу IEEE 802.3ad. Объединяет каналы в группы с одинаковой скоростью и дуплексным режимом. Задействует все физические интерфейсы на активном агрегированном интерфейсе. Значение по умолчанию.

Выбор физического интерфейса, который будет отправлять трафик, зависит от алгоритма генерации хеша. По умолчанию используется алгоритм исключающего ИЛИ. Администратор ПО Факел может включить другой алгоритм командой `set interfaces bonding <interface> hash-policy <policy>`.

Не все алгоритмы генерации хеша совместимы со стандартом 802.3ad. Стандарт стремится не допускать изменений в порядке передачи пакетов (как описано в секции 43.2.4 стандарта 802.3ad);

- `active-backup` — режим горячего резервирования. В этом режиме на агрегированном интерфейсе активен только один физический интерфейс. Этот интерфейс будет считаться основным. Другой физический интерфейс в составе агрегированного интерфейса будет считаться резервным и начнет работать только в том случае, если основной интерфейс выйдет из строя.

Внешние узлы сети видят только MAC-адрес агрегированного интерфейса. Агрегированный интерфейс, в свою очередь, назначает себе MAC-адрес первого активного физического интерфейса, который он включил в свой состав. Это делается для того, чтобы не вводить коммутатор в заблуждение. При выходе из строя основного интерфейса, резервный интерфейс станет основным и продолжит работать под MAC-адресом агрегированного интерфейса.

После выхода из строя основного интерфейса агрегированный интерфейс отправит один и более gratuitous ARP-запросов с только что включившегося в работу резервного интерфейса. Один gratuitous ARP-запрос адресуется агрегированному интерфейсу и каждому VLAN-интерфейсу, созданному на его основе. Gratuitous ARP-запросы, адресованные VLAN-интерфейсам, помечаются соответствующим идентификатором VLAN-интерфейса. В каждом случае интерфейс-получатель должен иметь хотя бы один назначенный IP-адрес.

Настроить поведение устройства в режиме горячего резервирования можно с помощью команды `set interfaces bonding <interface> primary <interface>`.

Режим обеспечивает отказоустойчивость;

- `broadcast` — режим широковещательной рассылки. Рассылает пакеты широким вещанием на все физический интерфейсы в составе агрегированного интерфейса.

Режим обеспечивает отказоустойчивость;

- `round-robin` — режим циклического алгоритма. Передает пакеты по порядку от первого доступного физического интерфейса к следующему.

Режим обеспечивает отказоустойчивость и распределение нагрузки;

- `transmit-load-balance` — режим адаптивного распределения передаваемой нагрузки. Распределяет исходящий трафик между физическими интерфейсами в зависимости от их скорости передачи данных.

Только один активный физический интерфейс принимает весь входящий трафик. Затем драйвер агрегирования распределяет поступившие пакеты данных между физическими интерфейсами в зависимости от их скорости передачи данных. Выбранные физические интерфейсы отправят ARP-ответы одноранговым узлам сети со своих MAC-адресов.

Если один из физических интерфейсов выйдет из строя, другой физический интерфейс перехватит MAC-адрес выбывшего интерфейса и продолжит работу.

В этом режиме агрегированный интерфейс может работать без коммутатора;

- `adaptive-load-balance` — режим адаптивного распределения принимаемой и передаваемой нагрузки. Распределяет входящий и исходящий IPv4-трафик между физическими интерфейсами в зависимости от их скорости обработки данных и в обоих случаях заменяет MAC-адрес агрегированного интерфейса уникальным MAC-адресом одного из выбранных физических интерфейсов. Таким образом режим распределяет нагрузку между физическими интерфейсами и предотвращает перегрузку маршрутизатора.

Принимаемая нагрузка распределяется между физическими интерфейсами поочередно в режиме циклического алгоритма. При этом чем выше скорость обработки данных у конкретного физического интерфейса, тем выше его приоритет в очереди.

Передаваемая нагрузка также распределяется. Драйвер агрегирования перехватывает ARP-ответы на выходе с агрегированного интерфейса и заменяет MAC-адрес агрегированного интерфейса уникальным MAC-адресом выбранного физического интерфейса. При этом драйвер агрегирования копирует и сохраняет информацию об IP-адресе назначения из ARP-ответа. Когда ARP-ответ приходит уже обратно от одноранговогo узла сети, драйвер агрегирования вспоминает его MAC-адрес и выбирает физический интерфейс, который отправит ARP-ответ.

Процесс обмена ARP-сообщениями имеет и свою проблемную сторону. При каждой широковещательной рассылке ARP-запроса агрегированный интерфейс использует свой MAC-адрес. Одноранговые узлы сети запоминают MAC-адрес агрегированного интерфейса вместо адреса физического интерфейса. В этой ситуации вся нагрузка переходит на активный физический интерфейс. Чтобы решить эту проблему, драйвер агрегирования отправляет обновления в виде ARP-ответов с MAC-адресами выбранных физических интерфейсов на MAC-адреса всех одноранговых узлов сети. Теперь одноранговые узлы сети будут обращаться не к одному MAC-адресу, а к MAC-адресам соответствующих физических интерфейсов.

Трафик перераспределяется и тогда, когда новый физический интерфейс добавляется в агрегированный интерфейс или когда неактивный физический интерфейс вновь включается в работу.

Если в сети присутствует коммутатор, то для стабильной работы сети необходимо также правильно настроить время задержки перед тем, как физический интерфейс станет активным (updelay). Значение updelay должно быть выше или равняться задержке у коммутатора на передачу пакетов по новому MAC-адресу (forwarding delay). Теперь коммутатор будет обновлять ARP-таблицу вовремя и не заблокирует входящие пакеты.

В этом режиме агрегированный интерфейс может работать без коммутатора;

- `xor-hash` — алгоритм генерации хеша с использованием операции исключающего ИЛИ. По умолчанию используется упрощенная операция [(MAC-адрес источника ИЛИ MAC-адрес назначения ИЛИ идентификатор типа пакета) модуль числа физических интерфейсов]. Альтернативные алгоритмы генерации хеша могут быть выбраны с помощью аргумента `hash-policy`, описанного ниже.

Режим обеспечивает отказоустойчивость и распределение нагрузки.

Примечание

К середине 2000-х годов большинство производителей перешли на выпуск сетевых устройств с поддержкой стандарта IEEE 802.3ad, что в принципе должно обеспечивать возможность совместной работы устройств различных марок. Однако на практике некоторые сочетания могут оказаться неработоспособными, поэтому в своих спецификациях производители зачастую специально уточняют

возможность совместной работы тех или иных устройств.

Режим: «Конфигурирование».

---

interfaces bonding <interface> min-links <0-16>

Описание:

Задает минимальное количество активных соединений, которое должно быть установлено перед тем как агрегированный интерфейс объявит о готовности к работе. В некоторых ситуациях службы более высокого уровня (такие как кластеризация) перед переключением на другой интерфейс требуют, чтобы было активно минимальное число соединений с низкой пропускной способностью.

Применимо только к режиму динамической агрегации по протоколу IEEE 802.3ad.

Агрегированный интерфейс будет считаться готовым к работе в режиме динамической агрегации по протоколу IEEE 802.3ad, когда на агрегированном интерфейсе будет активно хотя бы одно соединение.

Синтаксис:

- set interfaces bonding `<interface>` min-links `<0-16>`
- delete interfaces bonding `<interface>` min-links `<0-16>`
- show interfaces bonding `<interface>` min-links

Аргументы:

- `interface` — имя агрегированного интерфейса;
- `0-16` — минимальное количество активных соединений, которое должно быть установлено перед тем, как агрегированный интерфейс объявит о готовности к работе. Поскольку агрегированный интерфейс не может работать без хотя бы одного активного соединения, значение равное 0 или 1 будет иметь одинаковый эффект. Значение по умолчанию: 0.

Режим: «Конфигурирование».

---

interfaces bonding <interface> lacp-rate <slow|fast>

Описание:

Устанавливает интенсивность, с которой одноранговый узел сети будет передавать LACDPU-пакеты в режиме динамической агрегации по протоколу IEEE 802.3ad.

Синтаксис:

- set interfaces bonding `<interface>` lacp-rate `<slow|fast>`
- delete interfaces bonding `<interface>` lacp-rate `<slow|fast>`
- show interfaces bonding `<interface>` lacp-rate

Аргументы:

- `interface` — имя агрегированного интерфейса;
- `slow` — низкая интенсивность. Одноранговый узел сети соединения будет передавать LACDPU-пакеты каждые 30 секунд. Значение по умолчанию;
- `fast` — высокая интенсивность. Одноранговый узел сети будет передавать LACDPU-пакеты каждую секунду.

Режим: «Конфигурирование».

---

interfaces bonding <interface> system-mac <mac address>

Описание:

Назначает системный MAC-адрес агрегированному интерфейсу в режиме динамической агрегации по протоколу IEEE 802.3ad.

Синтаксис:

- set interfaces bonding `<interface>` system-mac `<mac address>`
- delete interfaces bonding `<interface>` system-mac `<mac address>`
- show interfaces bonding `<interface>` system-mac

Аргументы:

- `interface` — имя агрегированного интерфейса;
- `mac address` — системный MAC-адрес для агрегированного интерфейса. Формат: шестибайтный из шестнадцатиричных чисел. Допустимо использование случайно сгенерированного MAC-адреса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> hash-policy <layer2 | layer2+3 | layer3+4 | encap2+3 | encap3+4>

Описание:

Включает на агрегированном интерфейсе различные алгоритмы генерации хеша для распределения передаваемой нагрузки между физическими интерфейсами. Значение сгенерированного хеша будет определять, на какой физический интерфейс поступит трафик. Разные режимы используют информацию с разных уровней модели OSI.

Синтаксис:

- set interfaces bonding `<interface>` hash-policy `<layer2 | layer2+3 | layer3+4 | encap2+3 | encap3+4>`
- delete interfaces bonding `<interface>` hash-policy `<layer2 | layer2+3 | layer3+4 | encap2+3 | encap3+4>`

- show interfaces bonding <interface> hash-policy

Аргументы:

- <interface> — имя агрегированного интерфейса;
- layer2 — алгоритм использует информацию с канального уровня модели OSI. Применяет операцию исключающего ИЛИ к MAC-адресу и полю EtherType, чтобы сгенерировать хеш. Весь трафик, адресованный конкретному одноранговому узлу сети, будет отправлен с соответствующего физического интерфейса, специально выделенного для маршрутизации этого трафика. Значение по умолчанию.

Алгоритм совместим с протоколом IEEE 802.3ad.

Хеш = MAC-адрес источника ИЛИ MAC-адрес назначения ИЛИ поле идентификатора типа пакета. Число физических интерфейсов = хеш модуля числа физических интерфейсов;

- layer2+3 — алгоритм использует информацию с канального и сетевого уровня модели OSI. Применяет операцию исключающего ИЛИ к MAC- и IP-адресам источника и назначения, чтобы сгенерировать хеш.

Хеш = исходный MAC-адрес ИЛИ MAC-адрес назначения ИЛИ идентификатор типа пакета Хеш = хеш ИЛИ IP-адрес источника ИЛИ IP-адрес назначения Хеш = хеш ИЛИ (хеш от сдвига вправо на 16 бит) Хеш = хеш ИЛИ (хеш от сдвига вправо на 8 бит) Затем хеш делится на общее число физических интерфейсов и используется остаток от этого деления.

Алгоритм адресует весь трафик на одноранговый узел сети, с которым физический интерфейс установил связь. Для трафика, маршрутизируемого не по протоколу IP, формула такая же как для алгоритма layer2, т.е.:

Хеш = MAC-адрес источника ИЛИ MAC-адрес назначения ИЛИ поле идентификатора типа пакета. Число физических интерфейсов = хеш модуля числа физических интерфейсов.

Алгоритм layer2+3 призван предоставить более сбалансированное распределение трафика, нежели layer2. Некоторые окружения требуют наличия шлюза на сетевом уровне модели OSI для того, чтобы трафик достиг назначения.

Алгоритм совместим с протоколом IEEE 802.3ad;

- layer3+4 — алгоритм использует информацию с сетевого и транспортного уровня модели OSI. Трафик, исходящий с агрегированного интерфейса и адресованный одному одноранговому узлу сети, будет распределен между несколькими физическим интерфейсам. Однако трафик в рамках одного установленного соединения не будет распределяться между несколькими физическими интерфейсами.

Алгоритм генерации хеша для нефрагментированных TCP- и UDP-пакетов: Хеш = порт источника, порт назначения (как указано в заголовке пакета данными) Хеш = хеш ИЛИ IP-адрес источника ИЛИ IP-адрес назначения Хеш = хеш ИЛИ (хеш от сдвига вправо на 16 бит) Хеш = хеш ИЛИ (хеш от сдвига вправо на 8 бит) Затем хеш делится на общее число физических интерфейсов и используется остаток от этого деления.

Для фрагментированных TCP- или UDP-пакетов и для всего остального трафика информация о портах источника и назначения опускается. Для трафика, маршрутизируемого не по протоколу IP, алгоритм генерации хеша такой же как и для layer2;

Этот алгоритм лишь частично совместим с протоколом IEEE 802.3ad. Если в одном TCP- или UDP-соединении участвуют одновременно фрагментированные и нефрагментированные пакеты данных,

трафик будет распределен между двумя физическими интерфейсами. Это может привести к нарушению порядка доставки трафика. Большинство типов трафика не соответствуют этому критерию, поскольку протокол TCP редко фрагментирует трафик, а большинство UDP-трафика не участвует в продолжительном обмене данными между двумя конечными точками. Другие типы реализации протокола 802.3ad могут как допускать, так и не допускать эту несовместимость.

- `encap2+3` — алгоритм работает схоже с алгоритмом `layer2+3`, однако для генерации хеша в дополнение использует информацию от инкапсулированных заголовков на канальном и сетевом уровнях модели OSI. К примеру, если включено туннелирование с инкапсуляцией, алгоритм может выбрать внутренние заголовки вместо внешних.

Используйте этот алгоритм, если на агрегированном интерфейсе задействовано туннелирование типа 6to4, GRE, GRE6, IPIP, IPIP6, PPPoE или PPTP;

- `encap3+4` — алгоритм работает схоже с алгоритмом `layer3+4`, однако для генерации хеша также использует информацию от инкапсулированных заголовков на сетевом и транспортном уровнях модели OSI. К примеру, если включено туннелирование с инкапсуляцией, алгоритм может выбрать внутренние заголовки вместо внешних.

Используйте этот алгоритм, если на агрегированном интерфейсе задействовано туннелирование типа 6to4, GRE, GRE6, IPIP, IPIP6, PPPoE или PPTP;

Режим: «Конфигурирование».

---

interfaces bonding <interface> primary <interface>

Описание:

Отдает приоритет одному из физических интерфейсов в составе агрегированного интерфейса. Приоритетный физический интерфейс будет всегда активен при доступности. Другие физические интерфейсы будут задействованы только в случае отсутствия связи с приоритетным физическим интерфейсом.

Работает только в режимах `active-backup`, `transmit-load-balance`, `adaptive-load-balance`.

Синтаксис:

- set interfaces bonding `<interface>` primary `<interface>`
- delete interfaces bonding `<interface>` primary `<interface>`
- show interfaces bonding `<interface>` primary

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<interface>` — физический интерфейс, которому будет отдан приоритет.

Режим: «Конфигурирование».

Совет

Используйте приоритетность, когда пропускная способность одного физического интерфейса выше другого.

---

interfaces bonding <interface> arp-monitor interval <time>

Описание:

Отслеживает состояние физических интерфейсов на канале связи через указанный интервал времени. Для работы необходимо указать IP-адреса назначения через `set interfaces bonding <interface> arp-monitor target <address>`. Агрегированный интерфейс отправит на указанный IP-адрес назначения икусственный ARP-запрос. Если физический интерфейс ответит на искусственный ARP-ответ с указанного IP-адреса, то агрегированный интерфейс будет знать, что данный физический интерфейс активен и готов обрабатывать трафик. Точные критерии недавней активности зависят от режима агрегирования и от характера активности физического интерфейса.

Отслеживание состояния связи через ARP-запросы может работать некорректно в EtherChannel-совместимых режимах распределения нагрузки. К таким режимам относятся циклический алгоритм и алгоритм генерации хеша через исключающее ИЛИ. В этих случаях только один физический интерфейс получит все ARP-ответы от узлов сети. Это может привести к выходу из строя остальных физических интерфейсов. Чтобы устранить эту проблему, необходимо настроить коммутатор так, чтобы пакеты распределялись равномерно между всеми физическими интерфейсами.

Синтаксис:

- set interfaces bonding `<interface>` arp-monitor interval `<time>`
- delete interfaces bonding `<interface>` arp-monitor interval `<time>`
- show interfaces bonding `<interface>` arp-monitor interval

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<time>` — временной интервал, через который ARP-сообщения будут отправляться на физический интерфейс для отслеживания состояния канала связи. При значении в 0 секунд отслеживание состояния связи через ARP-запросы не работает. Значение по умолчанию: 0 секунд.

Режим: «Конфигурирование».

---

interfaces bonding <interface> arp-monitor target <address>

Описание:

Задает IP-адреса назначения, которые будут участвовать в проверке состояния канала связи. IP-адреса назначения должны находиться в той же сети, что и агрегированный интерфейс.

Агрегированный интерфейс отправит на указанный IP-адрес назначения икусственный ARP-запрос. Если физический интерфейс ответит на последующий искусственный ARP-ответ с указанного IP-адреса,

то агрегированный интерфейс будет знать, что данный физический интерфейс активен и готов обрабатывать трафик.

Команда будет выполнена, если `arp-monitor interval <time>` больше 0.

Синтаксис:

- set bonding `<interface>` arp-monitor target `<address>`
- delete bonding `<interface>` arp-monitor target `<address>`
- show bonding `<interface>` arp-monitor target

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `address` — IP-адреса устройств, которым будут отправлены ARP-запросы для проверки состояния физических интерфейсов. Можно указать несколько IP-адресов. Однако для выполнения команды необходимо указать хотя бы один IP-адрес. Максимально допустимое число IP-адресов: 16. Значение по умолчанию: IP-адрес не задан.

Режим: «Конфигурирование».

---

interfaces bonding <interface> address <address | dhcp | dhcpv6>

Описание:

Устанавливает, каким способом IP-адрес будет назначен агрегированному интерфейсу.

Синтаксис:

- set interfaces bonding `<interface>` address `<address | dhcp | dhcpv6>`
- delete interfaces bonding `<interface>` address `<address | dhcp | dhcpv6>`
- show interfaces bonding `<interface>` address

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<address>` — IP-адрес, который администратор вручную назначает агрегированному интерфейсу. Может быть указан несколько раз как адрес IPv4 или адрес IPv6;
- <dhcp> — DHCPv4-сервер автоматически назначит IPv4-адрес агрегированному интерфейсу на конкретном сегменте сети;

Режим: «Конфигурирование».

Примечание

Если вы используете протокол DHCP для получения IPv4-адреса и вам требуется дополнительная настройка, используйте указатели начала и конца данных. Эти файлы расположены в директории:

- /config/scripts/dhcp-client/pre-hooks.d/
- /config/scripts/dhcp-client/post-hooks.d/

interfaces bonding <interface> description <description>

Описание:

Добавляет описание для агрегированного интерфейса.

Синтаксис:

- set interfaces bonding `<interface>` description `<description>`
- delete interfaces bonding `<interface>` description `<description>`
- show interfaces bonding `<interface>` description

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<description>` — описание для агрегированного интерфейса.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к агрегированному интерфейсу по указанному описанию.

interfaces bonding <interface> disable

Описание:

Выключает агрегированный интерфейс. Интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces bonding `<interface>` disable
- delete interfaces bonding `<interface>` disable
- show interfaces bonding `<interface>`

Аргументы:

- `<interface>` — имя агрегированного интерфейса.

Режим: «Конфигурирование».

interfaces bonding <interface> disable-flow-control

Описание:

Останавливает передачу данных в сети Ethernet на стороне отправителя, пока принимающая сторона не получит все пакеты. Используйте эту команду, чтобы предотвратить потерю пакетов при большом скоплении трафика.

Синтаксис:

- set interfaces bonding `<interface>` disable-flow-control
- delete interfaces bonding `<interface>` disable-flow-control
- show interfaces bonding `<interface>`

Аргументы:

- `<interface>` — имя агрегированного интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> disable-link-detect

Описание:

Прекращает отслеживать состояние физического соединения между физическими интерфейсами и агрегированным интерфейсом. Если физический интерфейс выйдет из строя или с ним пропадет связь, система проигнорирует это событие для агрегированного интерфейса. По умолчанию состояние физического соединения отслеживается.

Синтаксис:

- set interfaces bonding `<interface>` disable-link-detect
- delete interfaces bonding `<interface>` disable-link-detect
- show interfaces bonding `<interface>`

Аргументы:

- `<interface>` — имя агрегированного интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> mac <xx:xx:xx:xx:xx:xx>

Описание:

Назначает пользовательский MAC-адрес для агрегированного интерфейса.

Синтаксис:

- set interfaces bonding <interface> mac <xx:xx:xx:xx:xx:xx>
- delete interfaces bonding <interface> mac <xx:xx:xx:xx:xx:xx>
- show interfaces bonding <interface> mac

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <xx:xx:xx:xx:xx:xx> — MAC-адрес.

Режим: «Конфигурирование».

---

interfaces bonding <interface> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на агрегированном интерфейсе.

Синтаксис:

- set interfaces bonding <interface> mtu <mtu>
- delete interfaces bonding <interface> mtu <mtu>
- show interfaces bonding <interface> mtu

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <mtu> — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces bonding <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>

Описание:

Устанавливает на агрегированном интерфейсе конкретное значение для максимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces bonding <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>

- delete interfaces bonding <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>
- show interfaces bonding <interface> ip adjust-mss

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <mss> — конкретное значение для максимального размера сегмента на протоколе TCP. Диапазон значений: от 536 до 65535;
- <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces bonding <interface> ip arp-cache-timeout <sec>

Описание:

Задает временной интервал между записями в ARP-кэш на агрегированном интерфейсе. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Синтаксис:

- set interfaces bonding <interface> ip arp-cache-timeout sec
- delete interfaces bonding <interface> ip arp-cache-timeout sec
- show interfaces bonding <interface> ip arp-cache-timeout

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <sec> — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces bonding <interface> ip disable-arp-filter

Описание:

Выключает фильтрацию по протоколу ARP на агрегированном интерфейсе. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы

будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами.

Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set interfaces bonding `<interface>` ip disable-arp-filter
- delete interfaces bonding `<interface>` ip disable-arp-filter
- show interfaces bonding `<interface>` ip

Аргументы:

- `<interface>` — имя агрегированного интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с агрегированного интерфейса на любой другой интерфейс. После выполнения команды интерфейс перейдет в режим хоста.

Синтаксис:

- set interfaces bonding `<interface>` ip disable-forwarding
- delete interfaces bonding `<interface>` ip disable-forwarding
- show interfaces bonding `<interface>` ip

Аргументы:

- `<interface>` — имя агрегированного интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> ip enable-directed-broadcast

Описание:

Включает направленную широковещательную переадресацию на агрегированном интерфейсе. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на целевую подсеть.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces bonding <interface> ip enable-directed-broadcast
- delete interfaces bonding <interface> ip enable-directed-broadcast
- show interfaces bonding <interface> ip

Аргументы:

- <interface> — имя агрегированного интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице агрегированного интерфейса для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица все равно будет обновлена, даже если команда не была выполнена.

Синтаксис:

- set interfaces bonding <interface> ip enable-arp-accept
- delete interfaces bonding <interface> ip enable-arp-accept
- show interfaces bonding <interface> ip

Аргументы:

- <interface> — имя агрегированного интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> ip enable-arp-announce

Описание:

Ограничивает на агрегированном интерфейсе анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. Маршрутизатор Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса агрегированный интерфейс проверяет все целевые подсети. По умолчанию маршрутизатор Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces bonding <interface> ip enable-arp-announce
- delete interfaces bonding <interface> ip enable-arp-announce
- show interfaces bonding <interface> ip

Аргументы:

- <interface> — имя агрегированного интерфейса.

Режим: «Конфигурирование».

Примечание

Если вы выполнили команду, то при отправке ARP-запросов не используйте адреса вне подсети назначения.

---

interfaces bonding <interface> ip enable-arp-ignore

Описание

Указывает агрегированному интерфейсу отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию агрегированный интерфейс отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе. Независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces bonding <interface> ip enable-arp-ignore
- delete interfaces bonding <interface> ip enable-arp-ignore
- show interfaces bonding <interface> ip

Аргументы:

- <interface> — имя агрегированного интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> ip enable-proxy-arp

Описание:

Включает прокси-сервер на агрегированном интерфейсе для маршрутизации ARP-запросов. Агрегированный интерфейс сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces bonding <interface> ip enable-proxy-arp
- delete interfaces bonding <interface> ip enable-proxy-arp
- show interfaces bonding <interface> ip

Аргументы:

- <interface> — имя агрегированного интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> ip proxy-arp-pvlan

Описание:

Создает на агрегированном интерфейсе частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом напрямую, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces bonding <interface> ip proxy-arp-pvlan
- delete interfaces bonding <interface> ip proxy-arp-pvlan
- show interfaces bonding <interface> ip

Аргументы:

- <interface> — имя агрегированного интерфейса.

Режим: «Конфигурирование».

Подсказка

Вы можете использовать эту команду без предварительного выполнения команды `interfaces bonding <interface> ip enable-proxy-arp`.

---

interfaces bonding <interface> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces bonding <interface> redirect <destination>
- delete interfaces bonding <interface> redirect <destination>
- show interfaces bonding <interface> redirect

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <destination> — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces bonding <interface> ip source-validation <strict | loose | disable>

Описание:

Включает на агрегированном интерфейсе различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces bonding <interface> ip source-validation <strict | loose | disable>
- delete interfaces bonding <interface> ip source-validation <strict | loose | disable>
- show interfaces bonding <interface> ip

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vrf <vrf>

Описание:

Размещает агрегированный интерфейс на указанном VRF-экземпляре.

Синтаксис:

- set interfaces bonding <interface> vrf <vrf>
- delete interfaces bonding <interface> vrf <vrf>
- show interfaces bonding <interface> vrf

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

---

interfaces bonding <interface> dhcp-options client-id <description>

Описание:

Присваивает идентификатор клиента агрегированному интерфейсу. Агрегированный интерфейс будет отображать свой идентификатор при запросе IP-адреса у DHCP-сервера.

Синтаксис:

- set interfaces bonding <interface> dhcp-options client-id <description>
- delete interfaces bonding <interface> dhcp-options client-id <description>
- show interfaces bonding <interface> dhcp-options client-id

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <description> — идентификатор клиента. Формат: произвольный.

Режим: «Конфигурирование».

Примечание

Более подробная информация содержится в документе RFC 2131. Отмечается, что клиент может специально ограничить свое обнаружение только посредством идентификатора (опция client identifier). В этом случае клиенту необходимо будет использовать один и тот же идентификатор во всех последующих сообщениях ICMPv6, а серверу придется использовать точно такой же идентификатор для поиска клиента.

---

interfaces bonding <interface> dhcp-options host-name <hostname>

Описание:

Присваивает имя хоста DHCP-серверу на агрегированном интерфейсе. Созданное имя заменит имя хоста по умолчанию. Когда клиент будет запрашивать IP-адрес у агрегированного интерфейса, ему отобразится присвоенное имя хоста.

Синтаксис:

- set interfaces bonding <interface> dhcp-options host-name <hostname>
- delete interfaces bonding <interface> dhcp-options host-name <hostname>
- show interfaces bonding <interface> dhcp-options host-name

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <hostname> — имя хоста.

Режим: «Конфигурирование».

---

interfaces bonding <interface> dhcp-options vendor-class-id <vendor-id>

Описание:

Присваивает идентификатор поставщика оборудования агрегированному интерфейсу. Если маршрутизатору Факел назначить идентификатор поставщика оборудования, то DHCP-сервер выдаст IP-адрес по тем правилам, которые применяются к соответствующему поставщику оборудования.

Синтаксис:

- set interfaces bonding <interface> dhcp-options vendor-class-id <vendor-id>
- delete interfaces bonding <interface> dhcp-options vendor-class-id <vendor-id>
- show interfaces bonding <interface> dhcp-options vendor-class-id

Аргументы:

- <interface> — имя агрегированного интерфейса;
- vendor-id — идентификатор поставщика оборудования.Будет передан DHCP-серверу как строка с бинарными данными. Формат: произвольный.

Режим: «Конфигурирование».

---

interfaces bonding <interface> dhcp-options no-default-route

Описание:

Запрещает агрегированному интерфейсу запрашивать у DHCP-сервера шлюз по умолчанию. Интерфейс будет запрашивать только IP-адрес.

Синтаксис:

- set interfaces bonding <interface> dhcp-options no-default-route
- delete interfaces bonding <interface> dhcp-options no-default-route
- show interfaces bonding <interface> dhcp-options

Аргументы:

- <interface> — имя агрегированного интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> dhcp-options default-route-distance <distance>

Описание:

Задает на агрегированном интерфейсе пользовательское значение, которое будет означать приоритет до шлюза по умолчанию.

Синтаксис:

- set interfaces bonding <interface> dhcp-options default-route-distance <distance>
- delete interfaces bonding <interface> dhcp-options default-route-distance <distance>
- show interfaces bonding <interface> dhcp-options default-route-distance

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <distance> — значение, которое означает приоритет до шлюза по умолчанию. Диапазон значений: от 1 до 255.

Режим: «Конфигурирование».

---

interfaces bonding <interface> dhcp-options reject <address>

Описание:

Указывает агрегированному интерфейсу не присваивать себе временно полученный IP-адрес от DHCP-сервера, а дождаться, когда DHCP-сервер назначит корректный IP-адрес.

Синтаксис:

- set interfaces bonding <interface> dhcp-options reject <address>
- delete interfaces bonding <interface> dhcp-options reject <address>
- show interfaces bonding <interface> dhcp-options reject

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <address>— IP-адрес, который будет проигнорирован интерфейсом. Можно задать несколько значений или указать диапазон IP-адресов. Пример: 192.168.100.0/24.

Режим: «Конфигурирование».

Совет

Используйте эту команду, если маршрутизатор присваивает себе при старте неправильный IP-адрес.

---

interfaces bonding <interface> dhcp-options user-class <string>

Описание:

Добавляет пользовательское описание для DHCP-клиента на агрегированном интерфейсе. Обычно используется для обозначения группы пользователей.

Синтаксис:

- set interfaces bonding <interface> dhcp-options user-class <string>
- delete interfaces bonding <interface> dhcp-options user-class <string>
- interfaces bonding <interface> dhcp-options user-class

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <string> — пользовательское описание DHCP-клиента.

Режим: «Конфигурирование».

---

interfaces bonding <interface> dhcpv6-options duid <duid>

Описание:

Присваивает уникальный идентификатор DUID DHCP-клиенту на агрегированном интерфейсе. DUID необходим, чтобы получить IP-адрес от DHCPv6-сервера. Сервер сравнивает идентификатор DUID клиента со своей базой данных и в ответ выдает нужные настройки (IP-адрес, срок аренды, параметры DNS-серверов и т.д.).

DUID состоит из двухбитного поля типа DUID и поля с изменяемой частью длиной до 128 байт. Длина идентификатора зависит от его типа. Основные типы DUID: LLT (Link-Layer Address + Time) и UUID (Universally Unique Identifier).

DUID может быть создан вручную или сгенерирован автоматически сторонними средствами.

Более подробная информация содержится в документе RFC 3315.

Синтаксис:

- set interfaces bonding <interface> dhcpv6-options duid <duid>
- delete interfaces bonding <interface> dhcpv6-options duid <duid>
- show interfaces bonding <interface> dhcpv6-options duid

Аргументы: * `<interface>` — имя агрегированного интерфейса; * `<duid>` — идентификатор DUID. Формат: зависит от типа DUID.

Режим: «Конфигурирование».

Совет

DUID типа LLT легче сгенерировать вручную нежели DUID типа UUID. Для этого необходимо перевести MAC-адрес устройства в шестнадцатеричный формат и добавить метку времени также в шестнадцатеричном формате.

Множественная адресация EVPN

Технология множественной адресации EVPN со всеми активными соединениями применяется для распределения нагрузки и создания резерва мощности. Множественная адресация EVPN создает виртуальную сеть между разными сегментами Ethernet. В такой конфигурации агрегированный интерфейс будет выступать в роли маршрутизатора на стороне провайдера. Маршрутизаторы на стороне клиента подключаются к двум и более маршрутизаторам на стороне провайдера и каналы связи между одним клиентом и разными провайдерами агрегируются. Такая группа соединений обозначается как сегмент сети Ethernet.

Сегмент сети Ethernet настраивается через указание системного MAC-адреса и локального дискриминатора или полного идентификатора сегмента Ethernet (ESINAME) на агрегированном интерфейсе в роли маршрутизатора на стороне провайдера.

Маршруты 1-го типа (Type-1 EAD-per-ES and EAD-per-EVI) используются для объявления локальных сегментов Ethernet и для поиска удаленных сегментов Ethernet в сети. Маршруты 2-го типа (Type-2/MAC-IP) при объявлении отображают идентификатор назначения сегмента Ethernet. Это позволяет устройствам на разных сегментах Ethernet синхронизировать свои MAC- и IP-адреса. Устройства будут беспрепятственно общаться друг с другом на втором уровне модели OSI, вне зависимости от их физического нахождения.

Более подробная информация содержится в документах RFC 7432 и 8365.

В случае множественной адресации EVPN каждый маршрутизатор на стороне провайдера имеет уникальный адрес точки VTEP, для которого требуется новый компонент уровня данных — MAC-ECMP. Запись MAC/FDB ссылается на список, в котором показано, какая точка VTEP соответствует какому маршрутизатору на стороне провайдера.

---

interfaces bonding <interface> evpn es-id <1-16777215|10-byte ID>

Описание:

Присваивает агрегированному интерфейсу уникальный идентификатор сегмента Ethernet.

Идентификатор служит для разграничения сегментов Ethernet, корректной маршрутизации пакетов и назначения распределителя BUM-трафика.

Синтаксис:

- set interfaces bonding <interface> evpn es-id <1-16777215|10-byte ID>
- delete interfaces bonding <interface> evpn es-id <1-16777215|10-byte ID>
- show interfaces bonding <interface> evpn es-id

Аргументы: * <1-16777215> — числовой идентификатор сегмента Ethernet. Диапазон значений: от 1 до 16777215; * 10-byte ID — 10-битный идентификатор сегмента Ethernet нулевого типа (ESINAME). Формат: произвольное шестнадцатеричное число. Пример: 00:01:02:03:04:05:06:07:08:09.

Режим: «Конфигурирование».

---

interfaces bonding <interface> evpn es-sys-mac <xx:xx:xx:xx:xx:xx>

Описание:

Генерирует для агрегированного интерфейса уникальный идентификатор сегмента Ethernet на основе произвольно заданного MAC-адреса и автоматически сгенерированного локального дискриминатора. Сгенерированный идентификатор будет являться 10-битным идентификатором 3-го типа.

Идентификатор служит для разграничения сегментов Ethernet, корректной маршрутизации пакетов и назначения распределителя BUM-трафика.

Синтаксис:

- set interfaces bonding <interface> evpn es-sys-mac <xx:xx:xx:xx:xx:xx>
- delete interfaces bonding <interface> evpn es-sys-mac <xx:xx:xx:xx:xx:xx>
- show interfaces bonding <interface> evpn es-sys-mac

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <xx:xx:xx:xx:xx:xx> — системный MAC-адрес агрегированного интерфейса в сети Ethernet VPN. Числа задаются произвольно в формате MAC-адреса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> evpn es-df-pref <1-65535>

Описание:

Присваивает агрегированному интерфейсу приоритет при распределении BUM-трафика. Указанный агрегированный интерфейс будет назначен распределителем BUM-трафика. Чем больше заданное значение, тем выше приоритет перед остальными маршрутизаторами в сети.

Технология EVPN создает виртуальную сеть между разными сегментами Ethernet. В такой конфигурации агрегированный интерфейс будет выступать в роли маршрутизатора на стороне провайдера. Все маршрутизаторы на стороне провайдера будут получать BUM-трафик через интернет. Однако только

назначенный распределитель BUM-трафика сможет отправить декапсулированные пакеты на сегменты Ethernet. При этом маршрутизаторы на стороне провайдера, которые не являются назначенными распределителями BUM-трафика, будут отбрасывать входящие пакеты.

Для назначения распределителя BUM-трафика используются маршруты расширенного 4-го типа (Type-4 ESR). В основе работы этого механизма лежит принцип, указанный в проекте документа IETF (draft-ietf-bess-evpn-pref-df).

Если маршрутизаторы на стороне провайдера получат через виртуальную сеть исходящий трафик от участников сегмента Ethernet, то они не будут перенаправлять такой трафик во внешнюю сеть интернет. Этот механизм называется расширенной фильтрацией типа «local bias» по принципу расщепления горизонта.

Распределитель BUM-трафика назначается отдельно на каждом сегменте Ethernet.

Синтаксис:

- set interfaces bonding <interface> evpn es-df-pref <1-65535>
- delete interfaces bonding <interface> evpn es-df-pref <1-65535>
- show interfaces bonding <interface> evpn es-df-pref

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <1-65535> — приоритет, согласно которому будет выбран назначенный распределитель BUM-трафика из числа агрегированных интерфейсов на стороне провайдера. Диапазон значений: от 1 до 65535. Чем выше значение, тем выше приоритет.

Режим: «Конфигурирование».

---

interfaces bonding <interface> evpn uplink

Описание:

Следит за состоянием связи с вышестоящим устройством. Если произойдет обрыв на физической сети, то маршрутизатор на стороне провайдера потеряет доступ к VxLAN и виртуальной сети. В таком случае, чтобы предотвратить потерю пакетов, маршрутизатор на стороне провайдера остановит связь между сервером и остальным сегментом Ethernet.

Синтаксис:

- set interfaces bonding <interface> evpn uplink
- delete interfaces bonding <interface> evpn uplink
- show interfaces bonding <interface> evpn

Аргументы:

- <interface> — имя агрегированного интерфейса.

Режим: «Конфигурирование».

Режим «Администрирование»

show interfaces bonding

Описание:

Отображает краткую информацию о статусе всех агрегированных интерфейсов.

Синтаксис:

- show interfaces bonding

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show interfaces bonding <interface>

Описание:

Отображает детальную информацию о статусе конкретного агрегированного интерфейса.

Синтаксис:

- show interfaces bonding `<interface>`

Аргументы:

- `<interface>` — имя агрегированного интерфейса.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show interfaces bonding <interface> detail

Описание:

Отображает детальную информацию о статусе физических соединений на агрегированном интерфейсе.

Синтаксис:

- show interfaces bonding `<interface>`

Аргументы:

- `<interface>` — имя агрегированного интерфейса.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

VLAN-интерфейс на агрегированном интерфейсе

Обзор

Маршрутизатор Факел поддерживает стандарт инкапсуляции данных IEEE 802.1q, что позволяет создавать виртуальные VLAN-интерфейсы на базе агрегированного интерфейса. В ПО Факел виртуальные субинтерфейсы обозначаются термином *vif*.

Список команд

Режим «Конфигурирование»

interfaces bonding <interface> vif <vlan-id>

Описание:

Создает на агрегированном интерфейсе новый виртуальный VLAN-интерфейс. На одном физическом интерфейсе может быть создано несколько виртуальных интерфейсов.

Синтаксис:

- set interfaces bonding `<interface>` vif `<vlan-id>`
- delete interfaces bonding `<interface>` vif `<vlan-id>`
- show interfaces bonding `<interface>` vif

Аргументы:

- `<interfaces>` — имя агрегированного интерфейса;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Примечание
VLAN-интерфейс может принимать лишь пакеты с метками типа 802.1q.

---

interfaces bonding <interface> vif <vlan-id> address <address | dhcp | dhcpv6>

Описание:

Устанавливает, каким способом IP-адрес будет назначен VLAN-интерфейсу.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> address <address | dhcp | dhcpv6>
- delete interfaces bonding <interface> vif <vlan-id> address <address | dhcp | dhcpv6>
- show interfaces bonding <interface> vif <vlan-id> address

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <address> — IP-адрес, который администратор вручную назначает VLAN-интерфейсу. Может быть указан несколько раз как адрес IPv4 или адрес IPv6;
- <dhcp> — DHCPv4-сервер автоматически назначит IPv4-адрес VLAN-интерфейсу на конкретном сегменте сети;

Режим: «Конфигурирование».

Примечание

Если вы используете протокол DHCP для получения IPv4-адреса и вам требуется дополнительная настройка, используйте указатели начала и конца данных. Эти файлы расположены в директории:

- /config/scripts/dhcp-client/pre-hooks.d/
- /config/scripts/dhcp-client/post-hooks.d/

---

interfaces bonding <interface> vif <vlan-id> description <description>

Описание:

Добавляет описание для VLAN-интерфейса.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> description <description>
- delete interfaces bonding <interface> vif <vlan-id> description <description>
- show interfaces bonding <interface> vif <vlan-id> description

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <description> — описание VLAN-интерфейса.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к VLAN-интерфейсу по указанному описанию.

---

interfaces bonding <interface> vif <vlan-id> disable

Описание:

Выключает VLAN-интерфейс. VLAN-интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces bonding `<interface>` vif `<vlan-id>` disable
- delete interfaces bonding `<interface>` vif `<vlan-id>` disable
- show interfaces bonding `<interface>` vif `<vlan-id>`

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> disable-link-detect

Описание:

Прекращает отслеживать состояние физического соединения на интерфейсе. По умолчанию состояние физического соединения отслеживается.

Синтаксис:

- set interfaces bonding `<interface>` vif `<vlan-id>` disable-link-detect
- delete interfaces bonding `<interface>` vif `<vlan-id>` disable-link-detect
- show interfaces bonding `<interface>` vif `<vlan-id>`

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>

Описание:

Назначает пользовательский MAC-адрес для VLAN-интерфейса.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>
- delete interfaces bonding <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>
- show interfaces bonding <interface> vif <vlan-id> mac

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <xx:xx:xx:xx:xx:xx> — MAC-адрес.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на VLAN-интерфейсе.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> mtu <mtu>
- delete interfaces bonding <interface> vif <vlan-id> mtu <mtu>
- show interfaces bonding <interface> vif <vlan-id> mtu

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <mtu> — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>

Описание:

Устанавливает на VLAN-интерфейсе конкретное значение для максимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>
- delete interfaces bonding <interface> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>
- show interfaces bonding <interface> vif <vlan-id> ip adjust-mss

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <mss> — конкретное значение для максимального размера сегмента на протоколе TCP;
- <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces bonding <interface> vif <vlan-id> ip arp-cache-timeout <sec>

Описание:

Задает временной интервал между записями в ARP-кэш на VLAN-интерфейсе. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> ip arp-cache-timeout <sec>
- delete interfaces bonding <interface> vif <vlan-id> ip arp-cache-timeout <sec>
- show interfaces bonding <interface> vif <vlan-id> ip arp-cache-timeout

Аргументы:

- <interface> — имя агрегированного интерфейса.
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;

- <sec> — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> ip disable-arp-filter

Описание:

Выключает фильтрацию по протоколу ARP на VLAN-интерфейсе. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами.

Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set bonding <interface> vif <vlan-id> ip disable-arp-filter
- delete bonding <interface> vif <vlan-id> ip disable-arp-filter
- show bonding <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с VLAN-интерфейса на любой другой интерфейс. После выполнения команды VLAN-интерфейс перейдет в режим хоста.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> ip disable-forwarding
- delete interfaces bonding <interface> vif <vlan-id> ip disable-forwarding
- show interfaces bonding <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя агрегированного интерфейса;

- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> ip enable-directed-broadcast

Описание:

Включает на VLAN-интерфейсе различные режимы направленной широковещательной переадресации. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на целевую подсеть.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> ip enable-directed-broadcast
- delete interfaces bonding <interface> vif <vlan-id> ip enable-directed-broadcast
- show interfaces bonding <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице VLAN-интерфейса для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица будет обновлена даже если команда не была выполнена.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> ip enable-arp-accept
- delete interfaces bonding <interface> vif <vlan-id> ip enable-arp-accept
- show interfaces bonding <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> ip enable-arp-announce

Описание:

Ограничивает на VLAN-интерфейсе анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. ПО Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса VLAN-интерфейс проверяет все целевые подсети. По умолчанию ПО Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces bonding `<interface>` vif `<vlan-id>` ip enable-arp-announce
- delete interfaces bonding `<interface>` vif `<vlan-id>` ip enable-arp-announce
- show interfaces bonding `<interface>` vif `<vlan-id>` ip

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Совет

Если вы выполнили команду, то при отправке ARP-запросов не используйте адреса вне подсети назначения.

---

interfaces bonding <interface> vif <vlan-id> ip enable-arp-ignore

Описание

Указывает VLAN-интерфейсу отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию VLAN-интерфейс отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе, независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces bonding `<interface>` vif `<vlan-id>` ip enable-arp-ignore
- delete interfaces bonding `<interface>` vif `<vlan-id>` ip enable-arp-ignore
- show interfaces bonding `<interface>` vif `<vlan-id>` ip

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> ip enable-proxy-arp

Описание:

Включает прокси-сервер на VLAN-интерфейсе для маршрутизации ARP-запросов. VLAN-интерфейс сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> ip enable-proxy-arp
- delete interfaces bonding <interface> vif <vlan-id> ip enable-proxy-arp
- show interfaces bonding <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> ip proxy-arp-pvlan

Описание:

Создает на VLAN-интерфейсе частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> ip proxy-arp-pvlan
- delete interfaces bonding <interface> vif <vlan-id> ip proxy-arp-pvlan
- show interfaces bonding <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Подсказка

Вы можете использовать эту команду без предварительного выполнения команды interfaces bonding <interface> ip enable-proxy-arp.

---

interfaces bonding <interface> vif <vlan-id> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> redirect <destination>
- delete interfaces bonding <interface> vif <vlan-id> redirect <destination>
- show interfaces bonding <interface> vif <vlan-id> redirect

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <destination> — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> ip source-validation <strict | loose | disable>

Описание:

Включает на VLAN-интерфейсе различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> ip source-validation <strict | loose | disable>
- delete interfaces bonding <interface> vif <vlan-id> ip source-validation <strict | loose | disable>
- show interfaces bonding <interface> vif <vlan-id> ip source-validation

Аргументы:

- <interface> — имя агрегированного интерфейса.
- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

---

interfaces bonding <interface> vif <vlan-id> vrf <vrf>

Описание:

Размещает VLAN-интерфейс на указанном VRF-экземпляре.

Синтаксис:

- set interfaces bonding <interface> vif <vlan-id> vrf <vrf>
- delete interfaces bonding <interface> vif <vlan-id> vrf <vrf>
- show interfaces bonding <interface> vif <vlan-id> vrf

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

Режим «Администрирование»

interfaces bonding <interface> vif <vlan-id> brief

Описание:

Отображает краткую информацию о конкретном VLAN-интерфейсе.

Синтаксис:

- show interfaces bonding <interface> vif <vlan-id> brief

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces bonding <interface> vif <vlan-id>

Описание:

Отображает детальную информацию о конкретном VLAN-интерфейсе.

Синтаксис:

- show interfaces bonding <interface> vif <vlan-id>

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Зеркалирование агрегированного интерфейса

Обзор

Зеркалирование дублирует входящий или исходящий трафик с агрегированного интерфейса на физический или виртуальный *SPAN-интерфейс*. К SPAN-интерфейсу может быть подключено специальное анализирующее оборудование или ПО: система контроля поведения, система обнаружения вторжения, сборщик трафика. Технология зеркалирования анализирует трафик изолировано от порта с исходным трафиком и не оказывает влияния на передаваемые данные или быстродействие системы.

Для каждого направления трафика существует своя настройка: *mirror ingress* для входящего трафика и *mirror egress* для исходящего. SPAN-интерфейсы должны быть настроены отдельно для трафика с различным направлением.

Список команд

Режим «Конфигурирование»

interfaces bonding <interface> mirror ingress <monitor-interface>

Описание:
Дублирует входящий трафик с порта агрегированного интерфейса на порт SPAN-интерфейса.

Синтаксис:

- set interfaces bonding `<interface>` mirror ingress `<monitor-interface>`
- delete interfaces bonding `<interface>` mirror ingress `<monitor-interface>`
- show interfaces bonding `<interface>` mirror ingress

Аргументы:

- `<interface>` — имя агрегированного интерфейса;
- `<monitor-interface>` — имя SPAN-интерфейса.

Режим: «Конфигурирование».

---

interfaces bonding <interface> mirror egress <monitor-interface>

Описание:
Дублирует исходящий трафик с порта агрегированного интерфейса на порт SPAN-интерфейса.

Синтаксис:

- set interfaces bonding <interface> mirror egress <monitor-interface>
- delete interfaces bonding <interface> mirror egress <monitor-interface>
- show interfaces bonding <interface> mirror egress

Аргументы:

- <interface> — имя агрегированного интерфейса;
- <monitor-interface> — имя SPAN-интерфейса.

Режим: «Конфигурирование».

2.2.3 Интерфейс сетевого моста

2.2.3.1 Обзор

Логический интерфейс сетевого моста соединяет независимые друг от друга физические или виртуальные интерфейсы, а также целые сегменты Ethernet.

Интерфейс сетевого моста маршрутизирует данные между интерфейсами на канальном уровне модели OSI. Поэтому данные пересылаются прозрачно, без препятствий и вне зависимости от протокола их передачи. Интерфейсы на двух сегментах не знают, что между ними проложен сетевой мост и думают, что соединены друг с другом напрямую.

При поступлении трафика интерфейс сетевого моста анализирует заголовок пакета данных. Если MAC-адрес назначения указывает на интерфейс в составе интерфейса сетевого моста, то пакет будет передан в сегмент назначения. Если же MAC-адрес принадлежит интерфейсу в другом сегменте Ethernet, то пакет будет отброшен. На протяжении всей сессии интерфейс сетевого моста продолжит пассивно наблюдать за трафиком и будет поддерживать и обновлять свою таблицу коммутации для корректного распределения трафика. Однако все же не исключено возникновение петель в маршрутах движения трафика. Чтобы решить эту проблему, на маршрутизаторе Факел включена поддержка протокола STP.

Протокол STP, также известный как протокол остовного дерева, — это сетевой протокол, который строит логическую топологию сетей Ethernet без петель и предотвращает появление широковещательного шторма.

После включения протокола STP узлы в сети начинают обмениваться друг с другом своими MAC-адресами и служебной информацией. Каждому порту на интерфейсе назначается уникальный идентификатор. Затем протокол определяет корневой мост, корневой порт, назначенный порт. Если в сегменте Ethernet существуют несколько интерфейсов сетевого моста, то также будет выбран назначенный мост. Остальные узлы в сети выбирают наикратчайший путь до корневого моста. Другие сетевые порты блокируются, чтобы предотвратить возникновение петель.

Если изменится строение сети или статус участников, протокол STP произведет конвергенцию, то есть перестроит маршрут движения трафика с учетом изменений.

Протокол STP также позволяет включать в структуру сети резервные каналы, чтобы избежать отказа всего интерфейса при выходе из строя основного канала.

> **Важно**
>
> В ПО Факел протокол STP по умолчанию выключен.

2.2.3.2 Пример настройки

Шаг	Команда	Описание
1	set interfaces bridge `br1` address `dhcp`	DHCPv6-сервер автоматически назначит IPv4-адрес интерфейсу сетевого моста
2	set interfaces bridge `br1` member interface member `eth3.40`	Добавляет сетевой интерфейс `eth3.40` в состав интерфейса сетевого моста `br1`
3	set interfaces bridge `br1` stp	Включает протокол STP на интерфейсе сетевого моста

2.2.3.3 Список команд

Режим «Конфигурирование»

interfaces bridge <interface> member interface <member>

Описание:

Добавляет сетевой интерфейс в состав интерфейса сетевого моста. Поддерживаются следующие типы интерфейсов:

- интерфейс Ethernet,
- агрегированный интерфейс,
- интерфейс L2TPv3,
- интерфейс OpenVPN,
- VXLAN-интерфейс,
- интерфейсы WLAN и WIFI,
- интерфейс туннеля,
- интерфейс GENEVE.

Синтаксис:

- set interfaces bridge `<interface>` member interface `<member>`
- delete interfaces bridge `<interface>` member interface `<member>`
- show interfaces bridge `<interface>` member interface

Аргументы:

- `<interface>` — имя интерфейса сетевого моста;
- `<member>` — имя интерфейса, который будет добавлен в состав агрегированного интерфейса. Интерфейсы добавляются по очереди.

Режим: «Конфигурирование».

---

interfaces bridge <interface> member interface <member> priority <priority>

Описание:

Задает приоритет для интерфейса в составе интерфейса сетевого моста при использовании протокола STP. Если на сегменте Ethernet включено несколько интерфейсов сетевого моста, то по умолчанию приоритет будет отдан устройству с наименьшим MAC-адресом. Такое устройство может обладать слабой производительностью, что приведет к неравномерному распределению нагрузки. Чтобы

избежать подобного сценария, необходимо для корректной маршрутизации установить приоритетность в соответствии с производительностью машин. Чем ниже значение, тем выше приоритет.

Синтаксис:

- set interfaces bridge <interface> member interface <member> priority <priority>
- delete interfaces bridge <interface> member interface <member> priority <priority>
- show interfaces bridge <interface> member interface <member> priority

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <member> — имя сетевого интерфейса, который будет добавлен в состав агрегированного интерфейса. Интерфейсы добавляются по очереди;
- <priority> — приоритет интерфейса. Чем ниже значение, тем выше приоритет. Диапазон значений: от 0 до 63.

Режим: «Конфигурирование».

---

interfaces bridge <interface> member interface <member> cost <cost>

Описание:

Задает стоимость порта на интерфейсах в составе интерфейса сетевого моста при использовании протокола STP. В сети с несколькими интерфейсами трафик движется к корневому порту через серию назначенных портов. Установка стоимости порта позволяет оптимизировать маршрут в зависимости от пропускной способности порта, загруженности линии и других показателей. Низкая стоимость порта означает, что трафик на сегменте Ethernet будет маршрутизироваться именно через этот порт. Все стоимости в итоге суммируются. Маршрут с суммарной наименьшей стоимостью будет приоритетным.

Синтаксис:

- set interfaces bridge <interface> member interface <member> cost <cost>
- delete interfaces bridge <interface> member interface <member> cost <cost>
- show interfaces bridge <interface> member interface <member> cost

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <member> — имя сетевого интерфейса, который будет добавлен в состав агрегированного интерфейса. Интерфейсы добавляются по очереди;
- <cost> — стоимость порта. Диапазон значений: от 1 до 65535.

Режим: «Конфигурирование».

---

interfaces bridge <interface> aging <time>

Описание:

Задает временной интервал, после которого MAC-адрес интерфейса сетевого моста будет считаться устаревшим и будет стерт из таблицы коммутации. Однако если интерфейс сетевого моста получит пакет с данными, то таймер будет сброшен и отсчет начнется заново.

Синтаксис:

- set interfaces bridge <interface> aging <time>
- delete interfaces bridge <interface> aging <time>
- show interfaces bridge <interface> aging

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <member> — имя сетевого интерфейса, который будет добавлен в состав агрегированного интерфейса. Интерфейсы добавляются по очереди;
- <time> — временной интервал, после которого MAC-адрес интерфейса сетевого моста будет считаться устаревшим и будет стерт из таблицы коммутации. Значение сбросится, если интерфейс сетевого моста получит пакет с данными. Формат: секунды. Диапазон значений: от 10 до 1000000. Значение по умолчанию: 300 секунд.

Режим: «Конфигурирование».

---

interfaces bridge <interface> max-age <time>

Описание:

Задает временной интервал, после которого которого MAC-адрес интерфейса сетевого моста будет считаться устаревшим и будет стерт из таблицы коммутации. Даже если интерфейс сетевого моста получит пакет с данными, то таймер не будет сброшен и по окончании отсчета MAC-адрес будет удален.

Синтаксис:

- set interfaces bridge <interface> max-age <time>
- delete interfaces bridge <interface> max-age <time>
- show interfaces bridge <interface> max-age

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <member> — имя сетевого интерфейса, который будет добавлен в состав агрегированного интерфейса. Интерфейсы добавляются по очереди;
- <time> — временной интервал, после которого MAC-адрес интерфейса сетевого моста будет считаться устаревшим и будет стерт из таблицы коммутации. Формат: секунды. Диапазон значений: от 1 до 40. Значение по умолчанию: 20 секунд.

Режим: «Конфигурирование».

---

interfaces bridge <interface> igmp querier

Описание:

Включает механизм регулирования потоков многоадресного трафика по протоколам IGMP и MLD. Интерфейс сетевого моста будет посылать IGMP-запросы на интерфейсы в составе интерфейса сетевого моста, чтобы определить, кто из них заинтересован в получении трафика.

Синтаксис:

- set interfaces bridge `<interface>` igmp querier
- delete interfaces bridge `<interface>` igmp querier
- show interfaces bridge `<interface>`

Аргументы:

- `<interface>` — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> igmp snooping

Описание:

Включает отслеживание трафика по протоколам IGMP и MLD. Только заинтересованные устройства в составе группы получат трафик с портов в составе интерфейса сетевого моста. Предотвращает широковещательную рассылку и снижает нагрузку на сеть. Однако требует затрат со стороны маршрутизатора.

Синтаксис:

- set interfaces bridge `<interface>` igmp snooping
- delete interfaces bridge `<interface>` igmp snooping
- show interfaces bridge `<interface>`

Аргументы:

- `<interface>` — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> stp

Описание:

Включает протокол STP на интерфейсе сетевого моста. По умолчанию протокол STP выключен.

Синтаксис:

- set interfaces bridge <interface> stp
- delete interfaces bridge <interface> stp
- show interfaces bridge <interface>

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> forwarding-delay <delay>

Описание:

Задает временную задержку, после которой интерфейс сетевого моста начнет маршрутизировать трафик по протоколу STP на новый MAC-адрес.

Когда в сети появляется новый интерфейс сетевого моста, он сразу приступает к маршрутизации данных, что может привести к бесконтрольной рассылке пакетов. Временная задержка даст интерфейсу сетевого моста время, чтобы собрать информацию об узлах сети и распределить пакеты корректно.

Синтаксис:

- set interfaces bridge <interface> forwarding-delay <delay>
- delete interfaces bridge <interface> forwarding-delay <delay>
- show interfaces bridge <interface>

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <delay> — временная задержка, после которой интерфейс сетевого моста начнет маршрутизировать трафик по протоколу STP на новый MAC-адрес. Формат: секунды. Диапазон значений: от 0 до 200. Значение по умолчанию: 15 секунд.

Режим: «Конфигурирование».

---

interfaces bridge <interface> hello-time <interval>

Описание:

Задает интервал, через который корневой и назначенный мост будут обмениваться служебными hello-сообщениями. Такие сообщения содержат в себе идентификатор моста, информацию о статусе моста, стоимость маршрута до корневого моста. Таким образом, поддерживается актуальная конфигурация сети.

Синтаксис:

- set interfaces bridge <interface> hello-time <interval>
- delete interfaces bridge <interface> hello-time <interval>
- show interfaces bridge <interface> hello-time

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <interval> — интервал, через который корневой и назначенный мост будут обмениваться служебными hello-сообщениями. Формат: секунды. Диапазон значений: от 1 до 10. Значение по умолчанию: 2 секунды.

Режим: «Конфигурирование».

---

interfaces bridge <interface> address <address | dhcp | dhcpv6>

Описание:

Устанавливает, каким способом IP-адрес будет назначен интерфейсу сетевого моста.

Синтаксис:

- set interfaces bridge <interface> address <address | dhcp | dhcpv6>
- delete interfaces bridge <interface> address <address | dhcp | dhcpv6>
- show interfaces bridge <interface> address

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <address> — IP-адрес, который администратор вручную назначает интерфейсу интерфейсу сетевого моста. Может быть указан несколько раз как адрес IPv4 или адрес IPv6;
- <dhcp> — DHCPv4-сервер автоматически назначит IPv4-адрес интерфейсу сетевого моста на конкретном сегменте сети;

Режим: «Конфигурирование».

Примечание

Если вы используете протокол DHCP для получения IPv4-адреса и вам требуется дополнительная настройка, используйте указатели начала и конца данных. Эти файлы расположены в директории:

- /config/scripts/dhcp-client/pre-hooks.d/
- /config/scripts/dhcp-client/post-hooks.d/

---

interfaces bridge <interface> description <description>

Описание:

Добавляет описание для интерфейса сетевого моста.

Синтаксис:

- set interfaces bridge <interface> description <description>
- delete interfaces bridge <interface> description <description>
- show interfaces bridge <interface> description

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <description> — описание для интерфейса сетевого моста.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к интерфейсу сетевого моста по указанному описанию.

---

interfaces bridge <interface> disable

Описание:

Выключает интерфейс сетевого моста. Интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces bridge <interface> disable
- delete interfaces bridge <interface> disable
- show interfaces bridge <interface>

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> disable-flow-control

Описание:

Останавливает передачу данных в сети Ethernet на стороне отправителя, пока принимающая сторона не получит все пакеты. Используйте эту команду, чтобы предотвратить потерю пакетов при большом скоплении трафика.

Синтаксис:

- set interfaces bridge <interface> disable-flow-control
- delete interfaces bridge <interface> disable-flow-control
- show interfaces bridge <interface>

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> mac <xx:xx:xx:xx:xx:xx>

Описание:

Назначает пользовательский MAC-адрес для интерфейса сетевого моста.

Синтаксис:

- set interfaces bridge <interface> mac <xx:xx:xx:xx:xx:xx>
- delete interfaces bridge <interface> mac <xx:xx:xx:xx:xx:xx>
- show interfaces bridge <interface> mac

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <xx:xx:xx:xx:xx:xx> — MAC-адрес.

Режим: «Конфигурирование».

---

interfaces bridge <interface> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на интерфейсе сетевого моста.

Синтаксис:

- set interfaces ethernet <interface> mtu <mtu>
- delete interfaces ethernet <interface> mtu <mtu>
- show interfaces ethernet <interface> mtu

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <mtu> — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces bridge <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>

Описание:

Устанавливает на интерфейсе сетевого моста конкретное значение для максимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces bridge <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>
- delete interfaces bridge <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>
- show interfaces bridge <interface> ip adjust-mss

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <mss> — конкретное значение для максимального размера сегмента на протоколе TCP. Диапазон значений: от 536 до 65535;
- <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

> **Подсказка**
>
> Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces ethernet <interface> ip arp-cache-timeout <sec>

Описание:

Задает временной интервал между записями в ARP-кэш на интерфейсе сетевого моста. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Синтаксис:

- set interfaces bridge <interface> ip arp-cache-timeout sec
- delete interfaces bridge <interface> ip arp-cache-timeout sec
- show interfaces bridge <interface> ip arp-cache-timeout

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <sec> — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces bridge <interface> ip disable-arp-filter

Описание:

Выключает фильтрацию по протоколу ARP на интерфейсе сетевого моста. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами.

Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set interfaces bridge <interface> ip disable-arp-filter
- delete interfaces bridge <interface> ip disable-arp-filter
- show interfaces bridge <interface> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с интерфейса сетевого моста на любой другой интерфейс. После выполнения команды интерфейс сетевого моста перейдет в режим хоста.

Синтаксис:

- set interfaces bridge <interface> ip disable-forwarding
- delete interfaces bridge <interface> ip disable-forwarding
- show interfaces bridge <interface> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> ip enable-directed-broadcast

Описание:

Включает направленную широковещательную переадресацию на интерфейсе сетевого моста. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на подсеть назначения.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces bridge <interface> ip enable-directed-broadcast
- delete interfaces bridge <interface> ip enable-directed-broadcast
- show interfaces bridge <interface> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице интерфейса сетевого моста для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица все равно будет обновлена, даже если команда не была выполнена.

Синтаксис:

- set interfaces ethernet <interface> ip enable-arp-accept
- delete interfaces ethernet <interface> ip enable-arp-accept
- show interfaces ethernet <interface> ip

Аргументы:

- <interface> — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces bridge <interface> ip enable-arp-announce

Описание:

Ограничивает на интерфейсе сетевого моста анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. ПО Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса интерфейс сетевого моста проверяет все целевые подсети. По умолчанию ПО Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces bridge <interface> ip enable-arp-announce
- delete interfaces bridge <interface> ip enable-arp-announce
- show interfaces bridge <interface> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

Примечание

Если вы выполнили команду, то при отправке ARP-запросов не используйте адреса вне подсети назначения.

---

interfaces bridge <interface> ip enable-arp-ignore

Описание

Указывает интерфейсу сетевого моста отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию интерфейс сетевого моста отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе. Независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces bridge <interface> ip enable-arp-ignore
- delete interfaces bridge <interface> ip enable-arp-ignore
- show interfaces bridge <interface> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> ip enable-proxy-arp

Описание:

Включает прокси-сервер на интерфейсе сетевого моста для маршрутизации ARP-запросов. Интерфейс сетевого моста сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces bridge <interface> ip enable-proxy-arp
- delete interfaces bridge <interface> ip enable-proxy-arp
- show interfaces bridge <interface> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> ip proxy-arp-pvlan

Описание:

Создает на интерфейсе сетевого моста частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом напрямую, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces bridge <interface> ip proxy-arp-pvlan
- delete interfaces bridge <interface> ip proxy-arp-pvlan
- show interfaces bridge <interface> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

Подсказка

Вы можете использовать эту команду без предварительного выполнения команды interfaces bridge <interface> ip enable-proxy-arp.

---

interfaces bridge <interface> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces bridge <interface> redirect <destination>
- delete interfaces bridge <interface> redirect <destination>
- show interfaces bridge <interface> redirect

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <destination> — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces bridge <interface> ip source-validation <strict | loose | disable>

Описание:

Включает на интерфейсе сетевого моста различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces bridge <interface> ip source-validation <strict | loose | disable>
- delete interfaces bridge <interface> ip source-validation <strict | loose | disable>

- show interfaces bridge <interface> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vrf <vrf>

Описание:

Размещает интерфейс сетевого моста на указанном VRF-экземпляре.

Синтаксис:

- set interfaces bridge <interface> vrf <vrf>
- delete interfaces bridge <interface> vrf <vrf>
- show interfaces bridge <interface> vrf

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

---

interfaces bridge <interface> dhcp-options client-id <description>

Описание:

Присваивает идентификатор клиента интерфейсу сетевого моста. Интерфейс сетевого моста будет отображать свой идентификатор при запросе IP-адреса у DHCP-сервера.

Синтаксис:

- set interfaces bridge <interface> dhcp-options client-id <description>

- delete interfaces bridge <interface> dhcp-options client-id <description>
- show interfaces bridge <interface> dhcp-options client-id

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <description> — идентификатор клиента. Формат: произвольный.

Режим: «Конфигурирование».

Примечание

Более подробная информация содержится в документе RFC 2131. Отмечается, что клиент может специально ограничить свое обнаружение только посредством идентификатора (опция client identifier). В этом случае клиенту необходимо будет использовать один и тот же идентификатор во всех последующих сообщениях ICMPv6, а серверу придется использовать точно такой же идентификатор для поиска клиента.

---

interfaces bridge <interface> dhcp-options client-id <description>

Описание:

Присваивает идентификатор клиента интерфейсу сетевого моста. Интерфейс сетевого моста будет отображать свой идентификатор при запросе IP-адреса у DHCP-сервера.

Синтаксис:

- set interfaces bridge <interface> dhcp-options client-id <description>
- delete interfaces bridge <interface> dhcp-options client-id <description>
- show interfaces bridge <interface> dhcp-options client-id

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <description> — идентификатор клиента. Формат: произвольный.

Режим: «Конфигурирование».

Примечание

Более подробная информация содержится в документе RFC 2131. Отмечается, что клиент может специально ограничить свое обнаружение только посредством идентификатора (опция client identifier). В этом случае клиенту необходимо будет использовать один и тот же идентификатор во всех последующих сообщениях ICMPv6, а серверу придется использовать точно такой же идентификатор для поиска клиента.

---

interfaces bridge <interface> dhcp-options host-name <hostname>

Описание:

Присваивает имя хоста DHCP-серверу на интерфейсе сетевого моста. Созданное имя заменит имя хоста по умолчанию. Когда клиент будет запрашивать IP-адрес у интерфейса сетевого моста, ему отобразится присвоенное имя хоста.

Синтаксис:

- set interfaces bridge <interface> dhcp-options host-name <hostname>
- delete interfaces bridge <interface> dhcp-options host-name <hostname>
- show interfaces bridge <interface> dhcp-options host-name

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <hostname> — имя хоста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> dhcp-options vendor-class-id <vendor-id>

Описание:

Присваивает идентификатор поставщика оборудования интерфейсу сетевого моста. Если маршрутизатору Факел назначить идентификатор поставщика оборудования, то DHCP-сервер выдаст IP-адрес по тем правилам, которые применяются к соответствующему поставщику оборудования.

Синтаксис:

- set interfaces bridge <interface> dhcp-options vendor-class-id <vendor-id>
- delete interfaces bridge <interface> dhcp-options vendor-class-id <vendor-id>
- show interfaces bridge <interface> dhcp-options vendor-class-id

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- vendor-id — идентификатор поставщика оборудования.Будет передан DHCP-серверу как строка с бинарными данными. Формат: произвольный.

Режим: «Конфигурирование».

---

interfaces bridge <interface> dhcp-options no-default-route

Описание:

Запрещает интерфейсу сетевого моста запрашивать у DHCP-сервера шлюз по умолчанию. Интерфейс будет запрашивать только IP-адрес.

Синтаксис:

- set interfaces bridge <interface> dhcp-options no-default-route
- delete interfaces bridge <interface> dhcp-options no-default-route
- show interfaces bridge <interface> dhcp-options

Аргументы:

- <interface> — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> dhcp-options default-route-distance <distance>

Описание:

Задает на интерфейсе сетевого моста приоритет до шлюза по умолчанию.

Синтаксис:

- set interfaces bridge <interface> dhcp-options default-route-distance <distance>
- delete interfaces bridge <interface> dhcp-options default-route-distance <distance>
- show interfaces bridge <interface> dhcp-options default-route-distance

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <distance> — приоритет до шлюза по умолчанию. Диапазон значений: от 1 до 255. Чем ниже значение, тем выше приоритет.

Режим: «Конфигурирование».

---

interfaces bridge <interface> dhcp-options reject <address>

Описание:

Указывает интерфейсу сетевого моста не присваивать себе временно полученный IP-адрес от DHCP-сервера, а дождаться, когда DHCP-сервер назначит корректный IP-адрес.

Синтаксис:

- set interfaces bridge <interface> dhcp-options reject <address>
- delete interfaces bridge <interface> dhcp-options reject <address>
- show interfaces bridge <interface> dhcp-options reject

Аргументы:

- <interface> — имя интерфейса сетевого моста;

- <address>— IP-адрес, который будет проигнорирован интерфейсом. Можно задать несколько значений или указать диапазон IP-адресов. Пример: 192.168.100.0/24.

Режим: «Конфигурирование».

Совет

Используйте эту команду, если маршрутизатор присваивает себе при старте неправильный IP-адрес.

---

interfaces bridge <interface> dhcp-options user-class <string>

Описание:

Добавляет пользовательское описание для DHCP-клиента на интерфейсе сетевого моста. Обычно используется для обозначения группы пользователей.

Синтаксис:

- set interfaces bridge <interface> dhcp-options user-class <string>
- delete interfaces bridge <interface> dhcp-options user-class <string>
- interfaces bridge <interface> dhcp-options user-class

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <string> — пользовательское описание DHCP-клиента.

Режим: «Конфигурирование».

---

interfaces bridge <interface> dhcpv6-options duid <duid>

Описание:

Присваивает уникальный идентификатор DUID DHCP-клиенту на интерфейсе сетевого моста. DUID необходим, чтобы получить IP-адрес от DHCPv6-сервера. Сервер сравнивает идентификатор DUID клиента со своей базой данных и в ответ выдает нужные настройки (IP-адрес, срок аренды, параметры DNS-серверов и т.д.).

DUID состоит из двухбитного поля типа DUID и поля с изменяемой частью длиной до 128 байт. Длина идентификатора зависит от его типа. Основные типы DUID: LLT (Link-Layer Address + Time) и UUID (Universally Unique Identifier).

DUID может быть создан вручную или сгенерирован автоматически сторонними средствами.

Более подробная информация содержится в документе RFC 3315.

Синтаксис:

- set interfaces bridge <interface> dhcpv6-options duid <duid>

- delete interfaces bridge <interface> dhcpv6-options duid <duid>
- show interfaces bridge <interface> dhcpv6-options duid

Аргументы: * <interface> — имя интерфейса сетевого моста; * <duid> — идентификатор DUID. Формат: зависит от типа DUID.

Режим: «Конфигурирование».

Совет

DUID типа LLT легче сгенерировать вручную нежели DUID типа UUID. Для этого необходимо перевести MAC-адрес устройства в шестнадцатеричный формат и добавить метку времени также в шестнадцатеричном формате.

Режим «Администрирование»

bridge

Описание:

Отображает информацию о созданных интерфейсах сетевого моста.

Синтаксис:

- show bridge

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

bridge <name> fdb

Описание:

Отображает детальную информацию о конкретном VLAN-интерфейсе.

Синтаксис:

- show bridge <name> fdb

Аргументы:

- <name> — имя интерфейса сетевого моста;

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

bridge <name> mdb

Описание:

Отображает таблицу с участниками многоадресной группы. Обновляется автоматически при включенном отслеживании по протоколам IGMP и MLD.

Синтаксис:

- show bridge <name> fdb

Аргументы:

- <name> — имя интерфейса сетевого моста;

Режим: «Администрирование».

Уровень привилегий: «Администратор».

VLAN-интерфейс на интерфейсе сетевого моста

Обзор

Маршрутизатор Факел поддерживает стандарт инкапсуляции данных IEEE 802.1q, что позволяет создавать виртуальные VLAN-интерфейсы на базе интерфейса сетевого моста. В ПО Факел такие виртуальные субинтерфейсы обозначаются термином *vif*.

По умолчанию все пакеты без VLAN-метки будут относиться к VLAN-интерфейсу 1. Физический интерфейс также получит идентификатор VLAN 1, поскольку логический интерфейс сетевого моста создается на базе физического интерфейса. Таким образом, из-за настроек по умолчанию не удастся создать vif с идентификатором 1.

Список команд

Режим «Конфигурирование»

interfaces bridge <interface> enable-vlan

Описание:

Включает поддержку VLAN на интерфейсе сетевого моста.

Синтаксис:

- set interfaces bridge `<interface>` enable-vlan
- delete interfaces bridge `<interface>` enable-vlan
- show interfaces bridge `<interface>`

Аргументы:

- `<interfaces>` — имя интерфейса сетевого моста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> protocol <802.1ad|802.1q>

Описание:

Устанавливает, какие метки будут использоваться для инкапсуляции поля EtherType в кадрах. Для поля EtherType 0x8100 используется метка 802.1q, а для поля EtherType 0x88a8 — метка 802.1ad.

Синтаксис:

- set interfaces bridge `<interface>` protocol `<802.1ad|802.1q>`

- delete interfaces bridge <interface> protocol <802.1ad|802.1q>
- show interfaces bridge <interface> protocol

Аргументы:

- <interfaces> — имя интерфейса сетевого моста;
- <802.1ad> — метка стандарта 802.1ad;
- <802.1q> — метка стандарта 802.1q. Значение по умолчанию.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id>

Описание:

Создает на интерфейсе сетевого моста новый виртуальный VLAN-интерфейс. На одном интерфейсе сетевого моста может быть создано несколько виртуальных интерфейсов.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id>
- delete interfaces bridge <interface> vif <vlan-id>
- show interfaces bridge <interface> vif

Аргументы:

- <interfaces> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Примечание
VLAN-интерфейс может принимать лишь пакеты с метками типа 802.1q.

---

interfaces bridge <interface> vif <vlan-id> address <address | dhcp | dhcpv6>

Описание:

Устанавливает, каким способом IP-адрес будет назначен VLAN-интерфейсу.

Синтаксис: * set interfaces bridge <interface> vif <vlan-id> address <address | dhcp | dhcpv6> * delete interfaces bridge <interface> vif <vlan-id> address <address | dhcp | dhcpv6> * show interfaces bridge <interface> vif <vlan-id> address

Аргументы: * <interface> — имя интерфейса сетевого моста; * <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094; * <address> — IP-адрес, который администратор вручную назначает интерфейсу сетевого моста. Может быть указан несколько раз как адрес IPv4 или адрес

IPv6; * <dhcp> — DHCPv4-сервер автоматически назначит IPv4-адрес интерфейсу сетевого моста на конкретном сегменте сети; .. * <dhcpv6> — DHCPv6-сервер автоматически назначит IPv6-адрес интерфейсу сетевого моста на конкретном сегменте сети.

Режим: «Конфигурирование».

Примечание

Если вы используете протокол DHCP для получения IPv4-адреса и вам требуется дополнительная настройка, используйте указатели начала и конца данных. Эти файлы расположены в директории:

- /config/scripts/dhcp-client/pre-hooks.d/
- /config/scripts/dhcp-client/post-hooks.d/

---

interfaces bridge <interface> vif <vlan-id> description <description>

Описание:

Добавляет описание для VLAN-интерфейса.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> description <description>
- delete interfaces bridge <interface> vif <vlan-id> description <description>
- show interfaces bridge <interface> vif <vlan-id> description

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <description> — описание VLAN-интерфейса.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к VLAN-интерфейсу по указанному описанию.

---

interfaces bridge <interface> vif <vlan-id> disable

Описание:

Выключает VLAN-интерфейс. VLAN-интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> disable
- delete interfaces bridge <interface> vif <vlan-id> disable
- show interfaces bridge <interface> vif <vlan-id>

Аргументы: * <interface> — имя интерфейса сетевого моста; * <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> disable-link-detect

Описание:

Прекращает отслеживать состояние физического соединения на интерфейсе. По умолчанию состояние физического соединения отслеживается.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> disable-link-detect
- delete interfaces bridge <interface> vif <vlan-id> disable-link-detect
- show interfaces bridge <interface> vif <vlan-id>

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>

Описание:

Назначает пользовательский MAC-адрес для VLAN-интерфейса.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>
- delete interfaces bridge <interface> vif <vlan-id> mac <xx:xx:xx:xx:xx:xx>
- show interfaces bridge <interface> vif <vlan-id> mac

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <xx:xx:xx:xx:xx:xx> — MAC-адрес.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на VLAN-интерфейсе.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> mtu <mtu>
- delete interfaces bridge <interface> vif <vlan-id> mtu <mtu>
- show interfaces bridge <interface> vif <vlan-id> mtu

Аргументы: <interface> — имя интерфейса сетевого моста; <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094; <mtu> — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>

Описание:

Устанавливает на VLAN-интерфейсе конкретное значение для максимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>
- delete interfaces bridge <interface> vif <vlan-id> ip adjust-mss <mss | clamp-mss-to-pmtu>
- show interfaces bridge <interface> vif <vlan-id> ip adjust-mss

Аргументы: * <interface> — имя интерфейса сетевого моста; * <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094; * <mss> — конкретное значение для максимального размера сегмента на протоколе TCP; * <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces bridge <interface> vif <vlan-id> ip arp-cache-timeout <sec>

Описание:

Задает временной интервал между записями в ARP-кэш на VLAN-интерфейсе. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ip arp-cache-timeout <sec>
- delete interfaces bridge <interface> vif <vlan-id> ip arp-cache-timeout <sec>
- show interfaces bridge <interface> vif <vlan-id> ip arp-cache-timeout

Аргументы:

- <interface> — имя интерфейса сетевого моста.
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <sec> — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> ip disable-arp-filter

Описание: | Выключает фильтрацию по протоколу ARP на VLAN-интерфейсе. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами. | Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set bridge <interface> vif <vlan-id> ip disable-arp-filter
- delete bridge <interface> vif <vlan-id> ip disable-arp-filter
- show bridge <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с VLAN-интерфейса на любой другой интерфейс. После выполнения команды VLAN-интерфейс перейдет в режим хоста.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ip disable-forwarding
- delete interfaces bridge <interface> vif <vlan-id> ip disable-forwarding
- show interfaces bridge <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> ip enable-directed-broadcast

Описание:

Включает на VLAN-интерфейсе различные режимы направленной широковещательной переадресации. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на подсеть назначения.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ip enable-directed-broadcast
- delete interfaces bridge <interface> vif <vlan-id> ip enable-directed-broadcast
- show interfaces bridge <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице VLAN-интерфейса для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица будет обновлена даже если команда не была выполнена.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ip enable-arp-accept
- delete interfaces bridge <interface> vif <vlan-id> ip enable-arp-accept
- show interfaces bridge <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> ip enable-arp-announce

Описание:

Ограничивает на VLAN-интерфейсе анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. ПО Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса VLAN-интерфейс проверяет все целевые подсети. По умолчанию ПО Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ip enable-arp-announce
- delete interfaces bridge <interface> vif <vlan-id> ip enable-arp-announce
- show interfaces bridge <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Совет

Если вы выполнили команду, то при отправке ARP-запросов не используйте адреса вне подсети назначения.

---

interfaces bridge <interface> vif <vlan-id> ip enable-arp-ignore

Описание

Указывает VLAN-интерфейсу отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию VLAN-интерфейс отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе, независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces bridge `<interface>` vif `<vlan-id>` ip enable-arp-ignore
- delete interfaces bridge `<interface>` vif `<vlan-id>` ip enable-arp-ignore
- show interfaces bridge `<interface>` vif `<vlan-id>` ip

Аргументы:

- `<interface>` — имя интерфейса сетевого моста;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> ip enable-proxy-arp

Описание:

Включает прокси-сервер на VLAN-интерфейсе для маршрутизации ARP-запросов. VLAN-интерфейс сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces bridge `<interface>` vif `<vlan-id>` ip enable-proxy-arp
- delete interfaces bridge `<interface>` vif `<vlan-id>` ip enable-proxy-arp
- show interfaces bridge `<interface>` vif `<vlan-id>` ip

Аргументы:

- `<interface>` — имя интерфейса сетевого моста;

- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> ip proxy-arp-pvlan

Описание:

Создает на VLAN-интерфейсе частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ip proxy-arp-pvlan
- delete interfaces bridge <interface> vif <vlan-id> ip proxy-arp-pvlan
- show interfaces bridge <interface> vif <vlan-id> ip

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Подсказка

Вы можете использовать эту команду без предварительного выполнения команды `interfaces bridge <interface> ip enable-proxy-arp`.

---

interfaces bridge <interface> vif <vlan-id> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> redirect <destination>
- delete interfaces bridge <interface> vif <vlan-id> redirect <destination>
- show interfaces bridge <interface> vif <vlan-id> redirect

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <destination> — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> ip source-validation <strict | loose | disable>

Описание:

Включает на VLAN-интерфейсе различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ip source-validation <strict | loose | disable>
- delete interfaces bridge <interface> vif <vlan-id> ip source-validation <strict | loose | disable>
- show interfaces bridge <interface> vif <vlan-id> ip source-validation

Аргументы:

- <interface> — имя интерфейса сетевого моста.
- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

Описание:

Включает на VLAN-интерфейсе механизм получения IPv6-адреса другими устройствами через автоматическую настройку адресов без сохранения состояния (SLAAC).
Хост-устройства с поддержкой связи по протоколу IPv6 могут автоматически производить свою настройку при подключении к сети IPv6 при обмене сообщениями ICMPv6 по протоколу обнаружения соседей.

При первичном подключении хост-устройство отправляет многоадресную рассылку с запросом параметров у маршрутизатора. Роутер отвечает на запрос и высылает объявление,

которое содержит параметры конфигурации сетевого уровня. Узнав эти параметры, хост-устройство сможет подключиться к маршрутизатору.

Более подробная информация содержится в документе RFC 4862.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ipv6 address autoconf
- delete interfaces bridge <interface> vif <vlan-id> ipv6 address autoconf
- show interfaces bridge <interface> vif <vlan-id> ipv6 address

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Примечание

Команда автоматически выключает перенаправление IPv6-трафика на VLAN-интерфейсе.

Описание:

Запускает преобразование EUI-64 на VLAN-интерфейсе. После этого хост-устройство сгенерирует себе уникальный 64-битный IPv6-адрес на основе своего MAC-адреса.

Более подробная информация содержится в документе RFC 4291.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ipv6 address eui64 <prefix>
- delete interfaces bridge <interface> vif <vlan-id> ipv6 address eui64 <prefix>
- show interfaces bridge <interface> vif <vlan-id> ipv6 address eui64

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <prefix> — префикс IPv6-адреса. Будет добавлен к основной части IPv6-адреса при запуске преобразования EUI-64.

Режим: «Конфигурирование».

Описание:

Запрещает назначать IPv6-адрес VLAN-интерфейсу для связи между локальными устройствами.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ipv6 address no-default-link-local
- delete interfaces bridge <interface> vif <vlan-id> ipv6 address no-default-link-local
- show interfaces bridge <interface> vif <vlan-id> ipv6 address

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Описание:

Выключает переадресацию пакетов по протоколу IPv6 с VLAN-интерфейса на любой другой интерфейс. После выполнения команды VLAN-интерфейс перейдет в режим хоста.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ipv6 disable-forwarding
- delete interfaces bridge <interface> vif <vlan-id> ipv6 disable-forwarding
- show interfaces bridge <interface> vif <vlan-id> ipv6

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

Описание:

Устанавливает на VLAN-интерфейсе конкретное значение для максимального размера сегмента при передаче IPv6-пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ipv6 adjust-mss <mss | clamp-mss-to-pmtu>

- delete interfaces bridge <interface> vif <vlan-id> ipv6 adjust-mss <mss | clamp-mss-to-pmtu>
- show interfaces bridge <interface> vif <vlan-id> ipv6 adjust-mss

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <mss> — конкретное значение для максимального размера сегмента на протоколе TCP. Диапазон значений: от 536 до 65535;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

Описание:

Настраивает работу механизма обнаружения дубликатов IPv6-адресов на VLAN-интерфейсе.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ipv6 accept-dad <1-3>
- delete interfaces bridge <interface> vif <vlan-id> ipv6 accept-dad <1-3>
- show interfaces bridge <interface> vif <vlan-id> ipv6 accept-dad

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <0> — выключает механизм по обнаружению дубликатов IPv6-адресов;
- <1> — включает механизм по обнаружению дубликатов IPv6-адресов. Значение по умолчанию;
- <2> — включает механизм по обнаружению дубликатов IPv6- и MAC-адресов в сегменте локальной сети. Если будут найдены два устройства с одинаковыми MAC- и IPv6-адресами на одном сегменте сети, передача данных по протоколу IPv6 будет остановлена для избежания конфликтов.

Режим: «Конфигурирование».

Описание:

Задает, сколько сообщений типа «опрос соседа» VLAN-интерфейс отправит по сети для обнаружения дубликатов IPv6-адресов.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> ipv6 dup-addr-detect-transmits <n>
- delete interfaces bridge <interface> vif <vlan-id> ipv6 dup-addr-detect-transmits <n>
- show interfaces bridge <interface> vif <vlan-id> ipv6 dup-addr-detect-transmits

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <n> — количество сообщений типа «опрос соседа», рассылаемых по сети.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> vrf <vrf>

Описание:

Размещает VLAN-интерфейс на указанном VRF-экземпляре.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> vrf <vrf>
- delete interfaces bridge <interface> vif <vlan-id> vrf <vrf>
- show interfaces bridge <interface> vif <vlan-id> vrf

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> dhcp-options client-id <description>

Описание:

Присваивает идентификатор клиента VLAN-интерфейсу. VLAN-интерфейс будет отображать свой идентификатор при запросе IP-адреса у DHCP-сервера.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> dhcp-options client-id <description>
- delete interfaces bridge <interface> vif <vlan-id> dhcp-options client-id <description>
- show interfaces bridge <interface> vif <vlan-id> dhcp-options client-id

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <description> — идентификатор клиента. Формат: произвольный.

Режим: «Конфигурирование».

Примечание

Более подробная информация содержится в документе RFC 2131. Отмечается, что клиент может специально ограничить свое обнаружение только посредством идентификатора (опция -client identifier-). В этом случае клиенту необходимо будет использовать один и тот же идентификатор во всех последующих сообщениях ICMPv6, а серверу придется использовать точно такой же идентификатор для нахождения клиента.

---

interfaces bridge <interface> vif <vlan-id> dhcp-options host-name <hostname>

Описание:

Присваивает имя хоста DHCPv6-серверу на VLAN-интерфейсе. Созданное имя заменит имя хоста по умолчанию. Когда клиент будет запрашивать IP-адрес у VLAN-интерфейса, ему отобразится присвоенное имя хоста.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> dhcp-options host-name <hostname>
- delete interfaces bridge <interface> vif <vlan-id> dhcp-options host-name <hostname>
- show interfaces bridge <interface> vif <vlan-id> dhcp-options host-name

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <hostname> — имя хоста.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> dhcp-options vendor-class-id <vendor-id>

Описание:

Присваивает идентификатор поставщика оборудования VLAN-интерфейсу. Если маршрутизатору Факел назначить идентификатор поставщика оборудования, то DHCP-сервер выдаст IP-адрес по тем правилам, которые применяются к соответствующему поставщику оборудования.

Синтаксис:

- set bridge <interface> vif <vlan-id> dhcp-options vendor-class-id <vendor-id>
- delete bridge <interface> vif <vlan-id> dhcp-options vendor-class-id <vendor-id>
- show bridge <interface> vif <vlan-id> dhcp-options vendor-class-id

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <vendor-id> — идентификатор поставщика оборудования. Формат: произвольный. Будет передан DHCP-серверу как строка с бинарными данными.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> dhcp-options no-default-route

Описание:

Запрещает VLAN-интерфейсу запрашивать у DHCP-сервера шлюз по умолчанию. Интерфейс будет запрашивать только IP-адрес.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> dhcp-options no-default-route
- delete interfaces bridge <interface> vif <vlan-id> dhcp-options no-default-route
- show interfaces bridge <interface> vif <vlan-id> dhcp-options

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> dhcp-options default-route-distance <distance>

Описание:

Задает на VLAN-интерфейсе приоритет до шлюза по умолчанию.

Синтаксис:

- set bridge <interface> vif <vlan-id> dhcp-options default-route-distance <distance>
- delete bridge <interface> vif <vlan-id> dhcp-options default-route-distance <distance>
- show bridge <interface> vif <vlan-id> dhcp-options default-route-distance

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <distance> — приоритет до шлюза по умолчанию. Диапазон значений: от 1 до 255. Чем ниже значение, тем выше приоритет.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> dhcp-options reject <address>

Описание:

Указывает VLAN-интерфейсу не присваивать себе временно полученный IP-адрес от DHCP-сервера, а дождаться, когда DHCP-сервер назначит корректный IP-адрес.

Синтаксис:

- set bridge <interface> vif <vlan-id> dhcp-options reject <address>
- delete bridge <interface> vif <vlan-id> dhcp-options reject <address>
- show bridge <interface> vif <vlan-id> dhcp-options reject

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <address>— IP-адрес, который будет проигнорирован интерфейсом. Можно задать несколько значений или указать диапазон IP-адресов. Пример: 192.168.100.0/24.

Режим: «Конфигурирование».

> **Совет**
>
> Используйте эту команду, если маршрутизатор присваивает себе при старте неправильный IP-адрес.

---

interfaces bridge <interface> vif <vlan-id> dhcp-options user-class <string>

Описание:

Добавляет пользовательское описание для DHCP-клиента на VLAN-интерфейсе. Обычно используется для обозначения группы пользователей.

Синтаксис:

- set bridge <interface> vif <vlan-id> dhcp-options user-class <string>
- delete bridge <interface> vif <vlan-id> dhcp-options user-class <string>
- show bridge <interface> vif <vlan-id> dhcp-options user-class

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <string> — пользовательское описание DHCP-клиента.

Режим: «Конфигурирование».

---

interfaces bridge <interface> vif <vlan-id> dhcpv6-options duid <duid>

Описание:

Присваивает уникальный идентификатор DUID DHCP-клиенту на VLAN-интерфейсе. DUID необходим, чтобы получить IP-адрес от DHCPv6-сервера. Сервер сравнивает идентификатор DUID клиента со своей базой данных и в ответ выдает нужные настройки (IP-адрес, срок аренды, параметры DNS-серверов и т.д.).

DUID состоит из двухбитного поля типа DUID и поля с изменяемой частью длиной до 128 байт. Длина идентификатора зависит от его типа. Основные типы DUID: LLT (Link-Layer Address + Time) и UUID (Universally Unique Identifier).

DUID может быть создан вручную или сгенерирован автоматически сторонними средствами.

Более подробная информация содержится в документе RFC 3315.

Синтаксис:

- set interfaces bridge <interface> vif <vlan-id> dhcpv6-options duid <duid>
- delete interfaces bridge <interface> vif <vlan-id> dhcpv6-options duid <duid>
- show interfaces bridge <interface> vif <vlan-id> dhcpv6-options duid

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094;
- <duid> — идентификатор DUID. Формат: зависит от типа DUID.

Режим: «Конфигурирование».

Совет

DUID типа LLT легче сгенерировать вручную нежели DUID типа UUID. Для этого необходимо перевести MAC-адрес устройства в шестнадцатеричный формат и добавить метку времени также в шестнадцатеричном формате.

Режим «Администрирование»

interfaces bridge <interface> vif <vlan-id> brief

Описание:

Отображает краткую информацию о конкретном VLAN-интерфейсе.

Синтаксис:

- show interfaces bridge <interface> vif <vlan-id> brief

Аргументы:

- `<interface>` — имя интерфейса сетевого моста;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces bridge <interface> vif <vlan-id>

Описание:

Отображает детальную информацию о конкретном VLAN-интерфейсе.

Синтаксис:

- show interfaces bridge <interface> vif <vlan-id>

Аргументы:

- `<interface>` — имя интерфейса сетевого моста;
- `<vlan-id>` — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4094.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Зеркалирование интерфейса сетевого моста

Обзор

Зеркалирование дублирует входящий или исходящий трафик с интерфейса сетевого моста на физический или виртуальный *SPAN-интерфейс*. К SPAN-интерфейсу может быть подключено специальное анализирующее оборудование или ПО: система контроля поведения, система обнаружения вторжения, сборщик трафика. Технология зеркалирования анализирует трафик изолировано от порта с исходным трафиком и не оказывает влияния на передаваемые данные или быстродействие системы.

Для каждого направления трафика существует своя настройка: *mirror ingress* для входящего трафика и *mirror egress* для исходящего. SPAN-интерфейсы должны быть настроены отдельно для трафика с различным направлением.

Список команд

Режим «Конфигурирование»

interfaces bridge <interface> mirror ingress <monitor-interface>

Описание:

Дублирует входящий трафик с порта интерфейса сетевого моста на порт SPAN-интерфейса.

Синтаксис:

- set interfaces bridge `<interface>` mirror ingress `<monitor-interface>`
- delete interfaces bridge `<interface>` mirror ingress `<monitor-interface>`
- show interfaces bridge `<interface>` mirror ingress

Аргументы:

- `<interface>` — имя интерфейса сетевого моста;
- `<monitor-interface>` — имя SPAN-интерфейса.

Режим: «Конфигурирование».

---

interfaces bridge <interface> mirror egress <monitor-interface>

Описание:

Дублирует исходящий трафик с порта агрегированного интерфейса на порт SPAN-интерфейса.

Синтаксис:

- set interfaces bridge <interface> mirror egress <monitor-interface>
- delete interfaces bridge <interface> mirror egress <monitor-interface>
- show interfaces bridge <interface> mirror egress

Аргументы:

- <interface> — имя интерфейса сетевого моста;
- <monitor-interface> — имя SPAN-интерфейса.

Режим: «Конфигурирование».

2.2.4 Интерфейс Loopback

2.2.4.1 Обзор

Интерфейс Loopback — это логический сетевой интерфейс с виртуальным портом на маршрутизаторе Факел. Интерфейс эмулирует поведение физического порта и работает на сетевом уровне модели OSI. Интерфейс Loopback по умолчанию обладает собственным локальным IP-адресом 127.0.0.1/8. Чтобы интерфейс мог общаться со внешними узлами сети, назначьте ему любой другой внешний IP-адрес.

Интерфейс Loopback всегда активен во время работы маршрутизатора, его нельзя выключить. Одновременно может работать только один интерфейс Loopback. Поскольку интерфейс Loopback не привязан к физическому порту, его нельзя подключить к другому устройству или добавить в агрегированный интерфейс.

Интерфейс Loopback подходит для сценариев маршрутизации трафика, где требуется постоянный доступ к конечной точке. Например, для поддержания связи по iBGP. Также интерфейс Loopback может быть использован для тестирования на маршрутизаторе локальных служб и приложений, которым не нужен выход во внешнюю сеть.

Совет

Если для вашей задачи одного интерфейса Loopback недостаточно, то вы можете создать несколько интерфейсов Dummy со схожим набором функций.

Список команд

Режим «Конфигурирование»

interfaces loopback <interface> address <address>

Описание:

Назначает интерфейсу Loopback IP-адрес.

Синтаксис:

- set interfaces loopback `<interface>` address `<address>`
- delete interfaces loopback `<interface>` address `<address>`
- show interfaces loopback `<interface>` address

Аргументы:

- <interface> — имя интерфейса Loopback;
- **<address> — IP-адрес, который администратор вручную назначает интерфейсу Loopback. Может быть указан несколько раз как адрес.**
  Значение по умолчанию: 127.0.0.1/8.

Режим: «Конфигурирование».

---

interfaces loopback <interface> description <description>

Описание:

Добавляет описание для интерфейса Loopback.

Синтаксис:

- set interfaces loopback <interface> description <description>
- delete interfaces loopback <interface> description <description>
- show interfaces loopback <interface> description

Аргументы:

- <interface> — имя интерфейса Loopback;
- <description> — описание для интерфейса Loopback.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к интерфейсу Loopback по указанному описанию.

---

interfaces loopback <interface> ip source-validation <strict | loose | disable>

Описание:

Включает на интерфейсе Loopback различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces loopback <interface> ip source-validation <strict | loose | disable>
- delete interfaces loopback <interface> ip source-validation <strict | loose | disable>
- show interfaces loopback <interface> ip

Аргументы:

- <interface> — имя интерфейса Loopback;

- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

---

interfaces loopback <interface> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces loopback <interface> redirect <destination>
- delete interfaces loopback <interface> redirect <destination>
- show interfaces loopback <interface> redirect

Аргументы:

- <interface> — имя интерфейса Loopback;
- <destination> — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

Режим «Администрирование»

interfaces loopback

Описание:

Отображает краткую информацию о статусе интерфейса Loopback.

Синтаксис:

- show interfaces loopback

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces loopback lo

Описание:

Отображает детальную информацию о статусе интерфейса Loopback.

Синтаксис:

- show interfaces loopback lo

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Зеркалирование интерфейса Loopback

Обзор

Зеркалирование дублирует входящий или исходящий трафик с логического интерфейса Loopback на физический или виртуальный *SPAN-интерфейс*. К SPAN-интерфейсу может быть подключено специальное анализирующее оборудование или ПО: система контроля поведения, система обнаружения вторжения, сборщик трафика. Технология зеркалирования анализирует трафик изолировано от порта с исходным трафиком и не оказывает влияния на передаваемые данные или быстродействие системы.

Для каждого направления трафика существует своя настройка: *mirror ingress* для входящего трафика и *mirror egress* для исходящего. SPAN-интерфейсы должны быть настроены отдельно для трафика с различным направлением.

Список команд

Режим «Конфигурирование»

interfaces loopback <interface> mirror ingress <monitor-interface>

Описание:
Дублирует входящий трафик с порта интерфейса Loopback на порт SPAN-интерфейса.

Синтаксис:

- set interfaces loopback `<interface>` mirror ingress `<monitor-interface>`
- delete interfaces loopback `<interface>` mirror ingress `<monitor-interface>`
- show interfaces loopback `<interface>` mirror ingress

Аргументы:

- `<interface>` — имя интерфейса Loopback;
- `<monitor-interface>` — имя SPAN-интерфейса.

Режим: «Конфигурирование».

---

interfaces loopback <interface> mirror egress <monitor-interface>

Описание:
Дублирует исходящий трафик с порта интерфейса Loopback на порт SPAN-интерфейса.

Синтаксис:

- set interfaces loopback <interface> mirror egress <monitor-interface>
- delete interfaces loopback <interface> mirror egress <monitor-interface>
- show interfaces loopback <interface> mirror egress

Аргументы:

- <interface> — имя интерфейса Loopback;
- <monitor-interface> — имя SPAN-интерфейса.

Режим: «Конфигурирование».

2.2.5 Интерфейс Dummy

2.2.5.1 Обзор

Интерфейс Dummy — это логический сетевой интерфейс с виртуальным портом на маршрутизаторе Факел. Так же, как и Loopback, интерфейс Dummy работает на сетевом уровне модели OSI и не привязан к физическому порту. Его нельзя подключить к другому устройству или добавить в агрегированный интерфейс. Интерфейс поддерживает те же функции, что и интерфейс Loopback и всегда активен во время работы маршрутизатора.

Главное отличие Dummy от Loopback в том, что одновременно могут работать несколько интерфейсов Dummy.

Ряд дополнительных особенностей интерфейса Dummy:

- может быть создан на VRF-экземпляре;
- можно установить максимальный размер передаваемого пакета;
- интерфейс можно выключить.

Как и Loopback, чаще всего интерфейс Dummy используется для тестирования приложений, служб и для обеспечения постоянного доступа к маршрутизатору.

Список команд

Режим «Конфигурирование»

interfaces dummy <interface> address <address>

Описание:

Назначает интерфейсу Dummy IP-адрес.

Синтаксис:

- set interfaces dummy `<interface>` address `<address>`
- delete interfaces dummy `<interface>` address `<address>`
- show interfaces dummy `<interface>` address

Аргументы:

- `<interface>` — имя интерфейса Dummy;
- **`<address>` — IP-адрес, который администратор вручную назначает интерфейсу Dummy.**
  Может быть указан несколько раз.

Режим: «Конфигурирование».

---

interfaces dummy <interface> description <description>

Описание:

Добавляет описание для интерфейса Dummy.

Синтаксис:

- set interfaces dummy `<interface>` description `<description>`
- delete interfaces dummy `<interface>` description `<description>`
- show interfaces dummy `<interface>` description

Аргументы:

- `<interface>` — имя интерфейса Dummy;
- `<description>` — описание для интерфейса Dummy.

Режим: «Конфигурирование».

> **Примечание**
>
> Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к интерфейсу Dummy по указанному описанию.

---

interfaces dummy <interface> disable

Описание:

Выключает интерфейс Dummy. Интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces dummy `<interface>` disable
- delete interfaces dummy `<interface>` disable
- show interfaces dummy `<interface>`

Аргументы:

- `<interface>` — имя интерфейса Dummy.

Режим: «Конфигурирование».

---

interfaces dummy <interface> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с интерфейса Dummy на любой другой интерфейс. После выполнения команды интерфейс Dummy перейдет в режим хоста.

Синтаксис:

- set interfaces dummy <interface> ip disable-forwarding
- delete interfaces dummy <interface> ip disable-forwarding
- show interfaces dummy <interface> ip

Аргументы:

- <interface> — имя интерфейса Dummy.

Режим: «Конфигурирование».

---

interfaces dummy <interface> ip source-validation <strict | loose | disable>

Описание:

Включает на интерфейсе Dummy различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces dummy <interface> ip source-validation <strict | loose | disable>
- delete interfaces dummy <interface> ip source-validation <strict | loose | disable>
- show interfaces dummy <interface> ip

Аргументы:

- <interface> — имя интерфейса Dummy;
- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

---

interfaces dummy <interface> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на интерфейсе Dummy.

Синтаксис:

- set interfaces dummy <interface> mtu <mtu>
- delete interfaces dummy <interface> mtu <mtu>
- show interfaces dummy <interface> mtu

Аргументы:

- <interface> — имя интерфейса Dummy;
- <mtu> — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces dummy <interface> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces dummy <interface> redirect <destination>
- delete interfaces dummy <interface> redirect <destination>
- show interfaces dummy <interface> redirect

Аргументы:

- <interface> — имя интерфейса Dummy;
- <destination> — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces dummy <interface> vrf <vrf>

Описание:

Размещает интерфейс Dummy на указанном VRF-экземпляре.

Синтаксис:

- set interfaces dummy <interface> vrf <vrf>
- delete interfaces dummy <interface> vrf <vrf>

- show interfaces dummy <interface> vrf

Аргументы:

- <interface> — имя интерфейса Dummy;
- <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

Режим «Администрирование»

interfaces dummy

Описание:

Отображает краткую информацию о статусе интерфейса Dummy.

Синтаксис:

- show interfaces dummy

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces dummy lo

Описание:

Отображает детальную информацию о статусе интерфейса Dummy.

Синтаксис:

- show interfaces dummy lo

Уровень привилегий: «Администратор».

Зеркалирование интерфейса Dummy

Обзор

Зеркалирование дублирует входящий или исходящий трафик с логического интерфейса Dummy на физический или виртуальный *SPAN-интерфейс*. К SPAN-интерфейсу может быть подключено специальное анализирующее оборудование или ПО: система контроля поведения, система обнаружения вторжения, сборщик трафика. Технология зеркалирования анализирует трафик изолировано от порта с исходным трафиком и не оказывает влияния на передаваемые данные или быстродействие системы.

Для каждого направления трафика существует своя настройка: *mirror ingress* для входящего трафика и *mirror egress* для исходящего. SPAN-интерфейсы должны быть настроены отдельно для трафика с различным направлением.

Список команд

Режим «Конфигурирование»

interfaces dummy <interface> mirror ingress <monitor-interface>

Описание:
Дублирует входящий трафик с порта интерфейса Dummy на порт SPAN-интерфейса.

Синтаксис:

- set interfaces dummy `<interface>` mirror ingress `<monitor-interface>`
- delete interfaces dummy `<interface>` mirror ingress `<monitor-interface>`
- show interfaces dummy `<interface>` mirror ingress

Аргументы:

- `<interface>` — имя интерфейса Dummy;
- `<monitor-interface>` — имя SPAN-интерфейса.

Режим: «Конфигурирование».

---

interfaces dummy <interface> mirror egress <monitor-interface>

Описание:
Дублирует исходящий трафик с порта интерфейса Dummy на порт SPAN-интерфейса.

Синтаксис:

- set interfaces dummy <interface> mirror egress <monitor-interface>
- delete interfaces dummy <interface> mirror egress <monitor-interface>
- show interfaces dummy <interface> mirror egress

Аргументы:

- <interface> — имя интерфейса Dummy;
- <monitor-interface> — имя SPAN-интерфейса.

Режим: «Конфигурирование».

2.2.6 Интерфейс L2TPv3

2.2.6.1 Обзор

Интерфейс L2TPv3 — логический интерфейс на маршрутизаторе Факел, работающий по протоколу L2TPv3. Используется для связи участников в локальных сетях через общую сеть посредством L2TPv3-туннеля. Протокол функционирует на сетевом уровне модели OSI, но инкапсулирует данные канального уровня.

Основные принципы работы: мультиплексирование и инкапсуляция IP-пакетов. Туннель прокладывается между двумя пограничными маршрутизаторами, которые выступают в роли посредников для устройств в локальных сетях. Для работы туннеля на обоих маршрутизаторах должны быть настроены интерфейсы L2TPv3. Маршрутизаторы будут видны устройствам в локальной сети и будут отвечать за инкапсуляцию, декапсуляцию и маршрутизацию данных между локальными устройствами.

Таким образом, устройства в изолированных локальных сетях общаются через пограничные маршрутизаторы так, как если бы они принадлежали к одной физической сети. При этом данные маршрутизируются прозрачно, вне зависимости от протокола их передачи.

Порядок работы интерфейса L2TPv3:

1. Устройство в локальной сети передает на интерфейс L2TPv3 маршрутизатора «А» пакеты канального уровня, которые нужно доставить до получателя в удаленной локальной сети.
2. Маршрутизатор «А» на одном конце туннеля инкапсулирует пакет с данными в заголовок L2TPv3 и доставляет до интерфейса L2TPv3 маршрутизатора «Б» на другом конце туннеля.
3. Маршрутизатор «Б» декапсулирует пакет, снимает заголовок L2TPv3 и передает данные адресату в удаленной локальной сети.

Чтобы L2TPv3-туннель начал работать, необходимо соответствующим образом настроить оба интерфейса L2TPv3 на двух пограничных маршрутизаторах:

- задать интерфейсу L2TPv3 локальный IP-адрес. Указанный адрес будет виден устройствам в локальной сети;
- задать IP-адрес источника и IP-адрес назначения. Интерфейсы L2TPv3 на пограничных маршрутизаторах с двух концов туннеля будут использовать эти адреса для связи друг с другом;
- задать номер UDP-порта источника и номер UDP-порта назначения. Интерфейсы L2TPv3 на пограничных маршрутизаторах с двух концов туннеля будут использовать эти номера портов для связи друг с другом;
- назначить идентификаторы сессии для маршрутизатора «А» и маршрутизатора «Б»;
- назначить идентификаторы туннеля для маршрутизатора «А» и маршрутизатора «Б»;
- установить метод инкапсуляции данных (UDP или IP).

Более подробная информация о протоколе L2TPv3 содержится в документе RFC 3931.

Примечание

По умолчанию данные по протоколу L2TPv3 передаются незащищенными. Для шифрования канала связи рекомендуем подключить стек протоколов IPsec.

2.2.6.2 Пример настройки

Шаг	Настройка маршрутизатора «А»	Настройка маршрутизатора «Б»	Описание
1	set interfaces l2tpv3 l2tpeth100 address 20.1.1.1/30	set interfaces l2tpv3 l2tpeth100 address 20.1.1.2/30	Задает интерфейсу L2TPv3 локальный IP-адрес
2	set interfaces l2tpv3 l2tpeth100 destination-port 9000	set interfaces l2tpv3 l2tpeth100 destination-port 9001	Задает интерфейсу L2TPv3 номер UDP-порта назначения
3	set interfaces l2tpv3 l2tpeth100 encapsulation udp	set interfaces l2tpv3 l2tpeth100 encapsulation udp	Устанавливает метод инкапсуляции данных в туннеле L2TPv3
4	set interfaces l2tpv3 l2tpeth100 peer-session-id 30	set interfaces l2tpv3 l2tpeth100 peer-session-id 50	Задает уникальный идентификатор сессии на стороне получателя
5	set interfaces l2tpv3 l2tpeth100 peer-tunnel-id 64	set interfaces l2tpv3 l2tpeth100 peer-tunnel-id 157	Задает уникальный идентификатор туннеля на стороне получателя
6	set interfaces l2tpv3 l2tpeth100 remote 76.39.201.2	set interfaces l2tpv3 l2tpeth100 remote 98.16.47.2	Задает интерфейсу L2TPv3 IP-адрес назначения
7	set interfaces l2tpv3 l2tpeth100 session-id 50	set interfaces l2tpv3 l2tpeth100 session-id 30	Задает уникальный идентификатор сессии на стороне отправителя
8	set interfaces l2tpv3 l2tpeth100 source-address 98.16.47.2	set interfaces l2tpv3 l2tpeth100 source-address 76.39.201.2	Задает интерфейсу L2TPv3 IP-адрес источника
9	set interfaces l2tpv3 l2tpeth100 source-port 9001	set interfaces l2tpv3 l2tpeth100 source-port 9000	Задает интерфейсу L2TPv3 номер UDP-порта источника
10	set interfaces l2tpv3 l2tpeth100 tunnel-id 157	set interfaces l2tpv3 l2tpeth100 tunnel-id 64	Задает уникальный идентификатор туннеля на стороне отправителя

2.2.6.3 Список команд

Режим «Конфигурирование»

interfaces l2tpv3 <interface> address <address>

Описание:

Задает интерфейсу L2TPv3 локальный IP-адрес.

Синтаксис:

- set interfaces l2tpv3 <interface> address <address>
- delete interfaces l2tpv3 <interface> address <address>
- show interfaces l2tpv3 <interface> address

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <address> — локальный IP-адрес, который администратор вручную назначает интерфейсу L2TPv3. Может быть указан несколько раз как адрес.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> description <description>

Описание:

Добавляет описание для интерфейса L2TPv3.

Синтаксис:

- set interfaces l2tpv3 <interface> description <description>
- delete interfaces l2tpv3 <interface> description <description>
- show interfaces l2tpv3 <interface> description

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <description> — описание для интерфейса L2TPv3.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к интерфейсу L2TPv3 по указанному описанию.

---

interfaces l2tpv3 <interface> destination-port <port>

Описание:

Задает интерфейсу L2TPv3 номер UDP-порта назначения.

Синтаксис:

- set l2tpv3 <interface> destination-port <port>
- delete l2tpv3 <interface> destination-port <port>
- show l2tpv3 <interface> destination-port

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <port> — номер UDP-порта назначения. Диапазон значений: от 1 до 65535. Значение по умолчанию: 500.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> disable

Описание:

Выключает интерфейс L2TPv3. Интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces l2tpv3 <interface> disable
- delete interfaces l2tpv3 <interface> disable
- show interfaces l2tpv3 <interface>

Аргументы:

- <interface> — имя интерфейса L2TPv3.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на интерфейсе L2TPv3.

Синтаксис:

- set interfaces l2tpv3 <interface> mtu <mtu>
- delete interfaces l2tpv3 <interface> mtu <mtu>

- show interfaces l2tpv3 <interface> mtu

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <mtu> — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>

Описание:

Устанавливает на интерфейсе L2TPv3 конкретное значение для максимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces l2tpv3 <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>
- delete interfaces l2tpv3 <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>
- show interfaces l2tpv3 <interface> ip adjust-mss

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <mss> — конкретное значение для максимального размера сегмента на протоколе TCP. Диапазон значений: от 536 до 65535;
- <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces l2tpv3 <interface> ip arp-cache-timeout <sec>

Описание:

Задает временной интервал между записями в ARP-кэш на интерфейсе L2TPv3. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Синтаксис:

- set interfaces l2tpv3 `<interface>` ip arp-cache-timeout `sec`
- delete interfaces l2tpv3 `<interface>` ip arp-cache-timeout `sec`
- show interfaces l2tpv3 `<interface>` ip arp-cache-timeout

Аргументы:

- `<interface>` — имя интерфейса L2TPv3;
- `<sec>` — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> ip disable-arp-filter

Описание:

Выключает фильтрацию по протоколу ARP на интерфейсе L2TPv3. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами.

Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set interfaces l2tpv3 `<interface>` ip disable-arp-filter
- delete interfaces l2tpv3 `<interface>` ip disable-arp-filter
- show interfaces l2tpv3 `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса L2TPv3.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с интерфейса L2TPv3 на любой другой интерфейс. После выполнения команды интерфейс L2TPv3 перейдет в режим хоста.

Синтаксис:

- set interfaces l2tpv3 `<interface>` ip disable-forwarding
- delete interfaces l2tpv3 `<interface>` ip disable-forwarding
- show interfaces l2tpv3 `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса L2TPv3.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> ip enable-directed-broadcast

Описание:

Включает направленную широковещательную переадресацию на интерфейсе L2TPv3. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на подсеть назначения.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces l2tpv3 `<interface>` ip enable-directed-broadcast
- delete interfaces l2tpv3 `<interface>` ip enable-directed-broadcast
- show interfaces l2tpv3 `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса L2TPv3.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице интерфейса L2TPv3 для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица все равно будет обновлена, даже если команда не была выполнена.

Синтаксис:

- set interfaces l2tpv3 `<interface>` ip enable-arp-accept
- delete interfaces l2tpv3 `<interface>` ip enable-arp-accept
- show interfaces l2tpv3 `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса L2TPv3.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> ip enable-arp-announce

Описание:

Ограничивает на интерфейсе L2TPv3 анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. ПО Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса интерфейс L2TPv3 проверяет все подсети назначения. По умолчанию ПО Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces l2tpv3 `<interface>` ip enable-arp-announce
- delete interfaces l2tpv3 `<interface>` ip enable-arp-announce
- show interfaces l2tpv3 `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса L2TPv3.

Режим: «Конфигурирование».

Примечание

Если вы выполнили команду, то при отправке ARP-запросов не используйте адреса вне подсети назначения.

---

interfaces l2tpv3 <interface> ip enable-arp-ignore

Описание

Указывает интерфейсу L2TPv3 отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию интерфейс L2TPv3 отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе. Независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces l2tpv3 <interface> ip enable-arp-ignore
- delete interfaces l2tpv3 <interface> ip enable-arp-ignore
- show interfaces l2tpv3 <interface> ip

Аргументы:

- <interface> — имя интерфейса L2TPv3.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> ip enable-proxy-arp

Описание:

Включает прокси-сервер на интерфейсе L2TPv3 для маршрутизации ARP-запросов. Интерфейс L2TPv3 сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces l2tpv3 <interface> ip enable-proxy-arp
- delete interfaces l2tpv3 <interface> ip enable-proxy-arp
- show interfaces l2tpv3 <interface> ip

Аргументы:

- <interface> — имя интерфейса L2TPv3.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> ip proxy-arp-pvlan

Описание:

Создает на интерфейсе L2TPv3 частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом напрямую, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces l2tpv3 <interface> ip proxy-arp-pvlan
- delete interfaces l2tpv3 <interface> ip proxy-arp-pvlan
- show interfaces l2tpv3 <interface> ip

Аргументы:

- <interface> — имя интерфейса L2TPv3.

Режим: «Конфигурирование».

Подсказка

Вы можете использовать эту команду без предварительного выполнения команды interfaces l2tpv3 <interface> ip enable-proxy-arp.

---

interfaces l2tpv3 <interface> ip source-validation <strict | loose | disable>

Описание:

Включает на интерфейсе L2TPv3 различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces l2tpv3 <interface> ip source-validation <strict | loose | disable>
- delete interfaces l2tpv3 <interface> ip source-validation <strict | loose | disable>
- show interfaces l2tpv3 <interface> ip

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> encapsulation <udp | ip>

Описание:

Устанавливает метод инкапсуляции данных в туннеле L2TPv3. Данные будут инкапсулированы в соответствии с протоколом UDP или IP.

Синтаксис:

- set interfaces l2tpv3 <interface> encapsulation <udp | ip>
- delete interfaces l2tpv3 <interface> encapsulation <udp | ip>
- show interfaces l2tpv3 <interface> encapsulation

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <udp | ip> — метод инкапсуляции данных в туннеле L2TPv3. Доступные протоколы: UDP или IP. Значение по умолчанию: UDP.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> source-address <address>

Описание:

Задает интерфейсу L2TPv3 IP-адрес источника.

Синтаксис:

- set interfaces l2tpv3 <interface> source-address <address>
- delete interfaces l2tpv3 <interface> source-address <address>
- show interfaces l2tpv3 <interface> source-address

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <address> — IP-адрес источника. Может быть указан как адрес IPv4 или адрес IPv6.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> remote <address>

Описание:

Задает интерфейсу L2TPv3 IP-адрес назначения.

Синтаксис:

- set interfaces l2tpv3 <interface> remote <address>

- delete interfaces l2tpv3 <interface> remote <address>
- show interfaces l2tpv3 <interface> remote

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <address> — IP-адрес назначения другого интерфейса L2TPv3. Может быть указан как адрес IPv4 или адрес IPv6.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> session-id <id>

Описание:

Задает интерфейсу L2TPv3 уникальный идентификатор сессии для интерфейса L2TPv3 на стороне отправителя. Значение идентификатора должно соответствовать значению *<peer-session-id>* у получателя.

Синтаксис:

- set interfaces l2tpv3 <interface> session-id <id>
- delete interfaces l2tpv3 <interface> session-id <id>
- show interfaces l2tpv3 <interface> session-id

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <id> — уникальный идентификатор сессии интерфейса L2TPv3 на стороне отправителя. Формат: 32-битное целое число. Диапазон значений: 1 — 429496729.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> peer-session-id <id>

Описание:

Задает интерфейсу L2TPv3 уникальный идентификатор сессии для интерфейса L2TPv3 на стороне получателя. Значение идентификатора должно соответствовать значению *<session-id>* у отправителя.

Синтаксис:

- set interfaces l2tpv3 <interface> peer-session-id <id>
- delete interfaces l2tpv3 <interface> peer-session-id <id>
- show interfaces l2tpv3 <interface> peer-session-id

Аргументы:

- <interface> — имя интерфейса L2TPv3;

- <id> — уникальный идентификатор сессии интерфейса L2TPv3 на стороне получателя. Формат: 32-битное целое число. Диапазон значений: 1 — 429496729.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> tunnel-id <id>

Описание:

Задает уникальный идентификатор туннеля L2TPv3 со стороны отправителя.

Синтаксис:

- set interfaces l2tpv3 <interface> tunnel-id <id>
- delete interfaces l2tpv3 <interface> tunnel-id <id>
- show interfaces l2tpv3 <interface> tunnel-id

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <id> — уникальный идентификатор туннеля L2TPv3 со стороны отправителя. Формат: 32-битное целое число. Диапазон значений: 1 — 429496729.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> peer-tunnel-id <id>

Описание:

Задает уникальный идентификатор туннеля L2TPv3 на стороне получателя.

Синтаксис:

- set interfaces l2tpv3 <interface> peer-tunnel-id <id>
- delete interfaces l2tpv3 <interface> peer-tunnel-id <id>
- show interfaces l2tpv3 <interface> peer-tunnel-id

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <id> — уникальный идентификатор туннеля L2TPv3 со стороны отправителя. Формат: 32-битное целое число. Диапазон значений: 1 — 429496729.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> source-port <port>

Описание:

Задает номер UDP-порта источника.

Синтаксис:

- set interfaces l2tp*v3 <interface> source-port <port>
- delete interfaces l2tpv3 <interface> source-port <port>
- show interfaces l2tpv3 <interface> source-port

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <port> — номер UDP-порта источника. Диапазон значений: от 1 до 65535. Значение по умолчанию: 5000.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> vrf <vrf>

Описание:

Размещает интерфейс L2TPv3 на указанном VRF-экземпляре.

Синтаксис:

- set interfaces l2tpv3 <interface> vrf <vrf>
- delete interfaces l2tpv3 <interface> vrf <vrf>
- show interfaces l2tpv3 <interface> vrf

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

Режим «Администрирование»

interfaces l2tpv3

Описание:

Отображает краткую информацию о статусе интерфейса L2TPv3.

Синтаксис:

- show interfaces l2tpv3

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces l2tpv3 detail

Описание:

Отображает детальную информацию о статусе интерфейса L2TPv3.

Синтаксис:

- show interfaces l2tpv3 detail

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Зеркалирование интерфейса L2TPv3

Обзор

Зеркалирование дублирует входящий или исходящий трафик с логического интерфейса L2TPv3 на физический или виртуальный *SPAN-интерфейс*. К SPAN-интерфейсу может быть подключено специальное анализирующее оборудование или ПО: система контроля поведения, система обнаружения вторжения, сборщик трафика. Технология зеркалирования анализирует трафик изолировано от порта с исходным трафиком и не оказывает влияния на передаваемые данные или быстродействие системы.

Для каждого направления трафика существует своя настройка: *mirror ingress* для входящего трафика и *mirror egress* для исходящего. SPAN-интерфейсы должны быть настроены отдельно для трафика с различным направлением.

Список команд

Режим «Конфигурирование»

interfaces l2tpv3 <interface> mirror ingress <monitor-interface>

Описание:
Дублирует входящий трафик с порта интерфейса L2TPv3 на порт SPAN-интерфейса.

Синтаксис:

- set interfaces l2tpv3 `<interface>` mirror ingress `<monitor-interface>`
- delete interfaces l2tpv3 `<interface>` mirror ingress `<monitor-interface>`
- show interfaces l2tpv3 `<interface>` mirror ingress

Аргументы:

- `<interface>` — имя интерфейса L2TPv3;
- `<monitor-interface>` — имя SPAN-интерфейса.

Режим: «Конфигурирование».

---

interfaces l2tpv3 <interface> mirror egress <monitor-interface>

Описание:
Дублирует исходящий трафик с порта интерфейса L2TPv3 на порт SPAN-интерфейса.

Синтаксис:

- set interfaces l2tpv3 <interface> mirror egress <monitor-interface>
- delete interfaces l2tpv3 <interface> mirror egress <monitor-interface>
- show interfaces l2tpv3 <interface> mirror egress

Аргументы:

- <interface> — имя интерфейса L2TPv3;
- <monitor-interface> — имя SPAN-интерфейса.

Режим: «Конфигурирование».

2.2.7 Интерфейс туннеля

2.2.7.1 Обзор

Технология туннелирования соединяет участников локальных сетей через общую сеть с помощью виртуального туннеля.

Туннельное соединение устанавливается между пограничными маршрутизаторами, которые имеют доступ к локальной и общей сети. Для корректной работы туннеля на каждом пограничном маршрутизаторе должен быть настроен интерфейс туннеля. После настройки маршрутизаторы станут видны локальным устройствам и будут выступать в роли посредников: инкапсулировать, декапсулировать и доставлять данные до локальных устройств через общую сеть. В процессе инкапсуляции ко *внутреннему* заголовку пакета исходной сети добавляется *внешний* заголовок общей сети. Таким образом, данные маршрутизируются прозрачно, вне зависимости от их исходного протокола.

Интерфейс туннеля — логический интерфейс на маршрутизаторе Факел.

Порядок работы интерфейса туннеля:

1. Устройство в локальной сети передает на интерфейс туннеля маршрутизатора «А» данные, которые нужно доставить до получателя в удаленной локальной сети.
2. Маршрутизатор «А» на одном конце туннеля инкапсулирует внутренний заголовок исходного пакета с данными во внешний заголовок выбранного протокола и доставляет пакет до интерфейса туннеля маршрутизатора «Б» на другом конце туннеля.
3. Маршрутизатор «Б» декапсулирует пакет, снимает внешний заголовок и передает данные адресату в удаленной локальной сети.

Протоколы туннелирования функционируют на сетевом уровне, но отличаются методами инкапсуляции исходных пакетов. Одни протоколы инкапсулируют данные сетевого уровня, другие — канального. Это позволяет производить более точную настройку в соответствии с требованиями и конфигурацией сети.

Интерфейс туннеля на маршрутизаторе Факел поддерживает следующие протоколы:

- IPv4 поверх IPv4 (IPIP),
- Simple Internet Transition (SIT),
- Generic Routing Encapsulation (GRE),
- Generic Routing Encapsulation Terminal Access Point (GRETAP),

Каждый тип протокола включается отдельной командой `set interfaces tunnel <interface> encapsulation <protocol>`.

2.2.7.2 Пример настройки

Шаг	Настройка маршрутизатора «А»	Настройка маршрутизатора «Б»	Описание
1	set interfaces tunnel tun1 encapsulation sit	set interfaces tunnel tun1 encapsulation sit	Включает протокол инкапсуляции SIT на интерфейсе туннеля
2	set interfaces tunnel tun1 source-address 192.0.2.10	set interfaces tunnel tun1 source-address 192.0.2.20	Задает IP-адреса источника на интерфейсе туннеля
3	set interfaces tunnel tun1 remote 192.0.2.20	set interfaces tunnel tun1 remote 129.0.2.10	Задает IP-адрес назначения на интерфейсе туннеля
4	set interfaces tunnel tun1 parameters ip key 14	set interfaces tunnel tun1 parameters ip key 14	Присваивает интерфейсу туннеля ключ для идентификации созданного туннеля
5	set interfaces tunnel tun1 mtu 1400	set interfaces tunnel tun1 mtu 1400	Устанавливает максимальный размер передаваемого пакета на интерфейсе туннеля

2.2.7.3 Список команд

Режим «Конфигурирование»

interfaces tunnel <interface> address <address>

Описание:

Задает интерфейсу туннеля локальный IP-адрес.

Синтаксис:

- set interfaces tunnel <interface> address <address>
- delete interfaces tunnel <interface> address <address>
- show interfaces tunnel <interface> address

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — локальный IP-адрес, который администратор вручную назначает интерфейсу туннеля. Может быть указан несколько раз как адрес IPv4 или адрес IPv6.

Режим: «Конфигурирование».

interfaces tunnel <interface> description <description>

Описание:

Добавляет описание для интерфейса туннеля.

Синтаксис:

- set interfaces tunnel `<interface>` description `<description>`
- delete interfaces tunnel `<interface>` description `<description>`
- show interfaces tunnel `<interface>` description

Аргументы:

- `<interface>` — имя интерфейса туннеля;
- `<description>` — описание для интерфейса туннеля.

Режим: «Конфигурирование».

Примечание

Инструменты мониторинга, работающие на основе протокола SNMP, также могут обращаться к интерфейсу туннеля по указанному описанию.

---

interfaces tunnel <interface> disable

Описание:

Выключает интерфейс туннеля. Интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces tunnel `<interface>` disable
- delete interfaces tunnel `<interface>` disable
- show interfaces tunnel `<interface>`

Аргументы:

- `<interface>` — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> disable-link-detect

Описание:

Прекращает отслеживать состояние физического соединения на интерфейсе туннеля. Если соединение по Ethernet-кабелю пропадет, система проигнорирует это событие для интерфейса туннеля. По умолчанию состояние физического соединения отслеживается.

Синтаксис:

- set interfaces tunnel <interface> disable-link-detect
- delete interfaces tunnel <interface> disable-link-detect
- show interfaces tunnel <interface>

Аргументы:

- <interface> — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> enable-multicast

Описание:

Включает на интерфейсе туннеля режим многоадресной рассылки.

Синтаксис:

- set interfaces tunnel <interface> enable-multicast
- delete interfaces tunnel <interface> enable-multicast
- show interfaces tunnel <interface>

Аргументы:

- <interface> — имя интерфейса Ethernet.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces tunnel <interface> redirect <destination>
- delete interfaces tunnel <interface> redirect <destination>
- show interfaces tunnel <interface> redirect

Аргументы:

- <interface> — имя интерфейса туннеля;
- <destination> — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> remote <address>

Описание:

Задает интерфейсу туннеля IP-адрес назначения.

Синтаксис:

- set interfaces tunnel <interface> remote <address>
- delete interfaces tunnel <interface> remote <address>
- show interfaces tunnel <interface> remote

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — IP-адрес назначения другого интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> source-address <address>

Описание:

Задает интерфейсу туннеля IP-адрес источника.

Синтаксис:

- set interfaces tunnel <interface> source-address <address>
- delete interfaces tunnel <interface> source-address <address>
- show interfaces tunnel <interface> source-address

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — IP-адрес источника.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> source-interface <source-interface>

Описание:

Выбирает интерфейс, с которого маршрутизатор Факел будет отправлять данные по туннелю.

Синтаксис:

- set interfaces tunnel <interface> source-interface <source-interface>
- delete interfaces tunnel <interface> source-interface <source-interface>

- show interfaces tunnel <interface> source-interface <source-interface>

Аргументы:

- <interface> — имя интерфейса туннеля;
- <source-interface> — имя интерфейса туннеля, с которого маршрутизатор Факел будет отправлять данные по туннелю.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на интерфейсе туннеля.

Синтаксис:

- set interfaces tunnel <interface> mtu <mtu>
- delete interfaces tunnel <interface> mtu <mtu>
- show interfaces tunnel <interface> mtu

Аргументы:

- <interface> — имя интерфейса туннеля;
- <mtu> — максимальный размер передаваемого пакета. Формат: байты.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> vrf <vrf>

Описание:

Размещает интерфейс туннеля на указанном VRF-экземпляре.

Синтаксис:

- set interfaces tunnel <interface> vrf <vrf>
- delete interfaces tunnel <interface> vrf <vrf>
- show interfaces tunnel <interface> vrf

Аргументы:

- <interface> — имя интерфейса туннеля;
- <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> parameters erspan direction <ingress | egress>

Описание:

Выбирает направление трафика на интерфейсе туннеля, которое будет зеркалироваться технологией ERSPAN.

Синтаксис:

- set interfaces tunnel `<interface>` parameters erspan direction `<ingress | egress>`
- delete interfaces tunnel `<interface>` parameters erspan direction `<ingress | egress>`
- show interfaces tunnel `<interface>` parameters erspan direction

Аргументы:

- `interface` — имя интерфейса туннеля;
- `ingress` — входящий трафик;
- `egress` — исходящий трафик.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> parameters erspan hw-id <hw-id>

Описание:

Присваивает интерфейсу туннеля аппаратный идентификатор на время сессии ERSPAN. Помогает различать устройства в туннеле при ERSPAN-зеркалировании.

Синтаксис:

- set interfaces tunnel `<interface>` parameters erspan hw-id `<hw-id>`
- delete interfaces tunnel `<interface>` parameters erspan hw-id `<hw-id>`
- show interfaces tunnel `<interface>` parameters erspan hw-id

Аргументы:

- `<interface>` — имя интерфейса туннеля;
- `<hw-id>` — аппаратный идентификатор. Диапазон значений: 0-1048575.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> parameters erspan index <index>

Описание:

Присваивает интерфейсу туннеля индекс сессии ERSPAN. Это уникальный идентификатор, который связывает источник и приемник зеркалированного трафика. Помогает удалённому анализатору определить, к какой сессии зеркалирования относятся получаемые пакеты.

Синтаксис:

- set interfaces tunnel <interface> parameters erspan index <index>
- delete interfaces tunnel <interface> parameters erspan index <index>
- show interfaces tunnel <interface> parameters erspan index

Аргументы:

- <interface> — имя интерфейса туннеля;
- <index>— индекс сессии ERSPAN. Диапазон значений: от 0 до 63.

Режим: «Конфигурирование».

Примечание

Для работы индекса сессии ERSPAN необходима аппаратная поддержка. Может не функционировать на устройствах других производителей.

---

interfaces tunnel <interface> parameters erspan version <1 | 2>

Описание:

Выбирает версию технологии ERSPAN.

Синтаксис:

- set interfaces tunnel <interface> parameters erspan version <1 | 2>
- delete interfaces tunnel <interface> parameters erspan version <1 | 2>
- show interfaces tunnel <interface> parameters erspan version

Аргументы:

- <interface> — имя интерфейса туннеля;
- <1> — версия ERSPAN Type II. Значение по умолчанию;
- <2> — версия ERSPAN Type III.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> parameters ip key <key>

Описание:

Присваивает интерфейсу туннеля ключ для идентификации созданного туннеля.

Синтаксис:

- set interfaces tunnel <interface> parameters ip key <key>

- delete interfaces tunnel <interface> parameters ip key <key>
- show interfaces tunnel <interface> parameters ip key

Аргументы:

- <interface> — имя интерфейса туннеля;
- <key> — ключ для идентификации созданного туннеля. Диапазон значений: от 0 до 4294967295.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> parameters ip ignore-df

Описание:

Указывает интерфейсу туннеля игнорировать требование бита DF «не фрагментировать IP-пакеты». IP-пакеты, передаваемые по туннелю, будут фрагментироваться, если их размер превысит максимально допустимый размера передаваемого пакета.

Синтаксис:

- set interfaces tunnel <interface> parameters ip ignore-df
- delete interfaces tunnel <interface> parameters ip ignore-df
- show interfaces tunnel <interface> parameters ip

Аргументы:

- <interface> — имя интерфейса туннеля

Режим: «Конфигурирование».

---

interfaces tunnel <interface> parameters ip no-pmtu-discovery

Описание:

Отключает для интерфейса туннеля вычисление максимально допустимого размера передаваемого пакета на маршруте.

Синтаксис:

- set interfaces tunnel <interface> parameters ip no-pmtu-discovery
- delete interfaces tunnel <interface> parameters ip no-pmtu-discovery
- show interfaces tunnel <interface> parameters ip

Аргументы:

- <interface> — имя интерфейса туннеля

Режим: «Конфигурирование».

---

interfaces tunnel <interface> parameters ip tos <tos>

Описание:

Задает значение ToS в IP-заголовке трафика, который будет передаваться по интерфейсу туннеля. Используется для различения трафика по признакам приоритетности или иным заданным параметрам. Маршрутизатор Факел будет обрабатывать пакеты, исходя из заданных значений.

Синтаксис:

- set interfaces tunnel `<interface>` parameters ip tos `<tos>`
- delete interfaces tunnel `<interface>` parameters ip tos `<tos>`
- show interfaces tunnel `<interface>` parameters ip tos

Аргументы:

- `<interface>` — имя интерфейса туннеля
- `<tos>` — значение ToS. Диапазон значений: от 0 до 99.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> parameters ip ttl <ttl>

Описание:

Задает на интерфейсе туннеля время жизни IP-пакета. После того как IP-пакет пройдет один маршрутизатор, его время жизни сократится на одно значение.

Синтаксис:

- set interfaces tunnel `<interface>` parameters ip ttl `<ttl>`
- delete interfaces tunnel `<interface>` parameters ip ttl `<ttl>`
- show interfaces tunnel `<interface>` parameters ip ttl

Аргументы:

- `<interface>` — имя интерфейса туннеля;
- `<ttl>` — время жизни IP-пакета. Формат: количество пройденных маршрутизаторов. Диапазон значений: от 1 до 255. Число `0` копирует значение из IP-заголовка.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>

Описание:

Устанавливает на интерфейсе туннеля конкретное значение для максимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Синтаксис:

- set interfaces tunnel <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>
- delete interfaces tunnel <interface> ip adjust-mss <mss | clamp-mss-to-pmtu>
- show interfaces tunnel <interface> ip adjust-mss

Аргументы:

- <interface> — имя интерфейса туннеля;
- <mss> — конкретное значение для максимального размера сегмента на протоколе TCP. Диапазон значений: от 536 до 65535;
- <clamp-mss-to-pmtu> — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces tunnel <interface> ip arp-cache-timeout

Описание:

Задает временной интервал между записями в ARP-кэш на интерфейсе туннеля. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Синтаксис:

- set interfaces tunnel <interface> ip arp-cache-timeout sec
- delete interfaces tunnel <interface> ip arp-cache-timeout sec
- show interfaces tunnel <interface> ip arp-cache-timeout

Аргументы:

- <interface> — имя интерфейса туннеля;
- <sec> — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> ip disable-arp-filter

Описание:

Выключает фильтрацию по протоколу ARP на интерфейсе туннеля. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами.

Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set interfaces tunnel <interface> ip disable-arp-filter
- delete interfaces tunnel <interface> ip disable-arp-filter
- show interfaces tunnel <interface> ip

Аргументы:

- <interface> — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IPv4 с интерфейса туннеля на любой другой интерфейс. После выполнения команды интерфейс туннеля перейдет в режим хоста.

Синтаксис:

- set interfaces tunnel <interface> ip disable-forwarding
- delete interfaces tunnel <interface> ip disable-forwarding
- show interfaces tunnel <interface> ip

Аргументы:

- <interface> — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> ip enable-directed-broadcast

Описание:

Включает направленную широковещательную переадресацию на интерфейсе туннеля. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на подсеть назначения.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces tunnel `<interface>` ip enable-directed-broadcast
- delete interfaces tunnel `<interface>` ip enable-directed-broadcast
- show interfaces tunnel `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице интерфейса туннеля для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица все равно будет обновлена, даже если команда не была выполнена.

Синтаксис:

- set interfaces tunnel `<interface>` ip enable-arp-accept
- delete interfaces tunnel `<interface>` ip enable-arp-accept
- show interfaces tunnel `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> ip enable-arp-announce

Описание:

Ограничивает на интерфейсе туннеля анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. ПО Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса интерфейс туннеля проверяет все подсети назначения. По умолчанию ПО Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces tunnel `<interface>` ip enable-arp-announce
- delete interfaces tunnel `<interface>` ip enable-arp-announce
- show interfaces tunnel `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса туннеля.

Режим: «Конфигурирование».

Примечание

Если вы выполнили команду, то при отправке ARP-запросов не используйте адреса вне подсети назначения.

---

interfaces tunnel <interface> ip enable-arp-ignore

Описание

Указывает интерфейсу туннеля отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию интерфейс туннеля отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе. Независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces tunnel `<interface>` ip enable-arp-ignore
- delete interfaces tunnel `<interface>` ip enable-arp-ignore
- show interfaces tunnel `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> ip enable-proxy-arp

Описание:

Включает прокси-сервер на интерфейсе туннеля для маршрутизации ARP-запросов. Интерфейс туннеля сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces tunnel `<interface>` ip enable-proxy-arp
- delete interfaces tunnel `<interface>` ip enable-proxy-arp
- show interfaces tunnel `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> ip proxy-arp-pvlan

Описание:

Создает на интерфейсе туннеля частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом напрямую, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces tunnel `<interface>` ip proxy-arp-pvlan
- delete interfaces tunnel `<interface>` ip proxy-arp-pvlan
- show interfaces tunnel `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса туннеля.

Режим: «Конфигурирование».

Подсказка

Вы можете использовать эту команду без предварительного выполнения команды `interfaces tunnel <interface> ip enable-proxy-arp`.

---

interfaces tunnel <interface> ip source-validation <strict | loose | disable>

Описание:

Включает на интерфейсе туннеля различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces tunnel `<interface>` ip source-validation `<strict | loose | disable>`
- delete interfaces tunnel `<interface>` ip source-validation `<strict | loose | disable>`
- show interfaces tunnel `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса туннеля;
- `<strict>` — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- `<loose>` — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- `<disable>` — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

Режим «Администрирование»

interfaces tunnel

Описание:

Отображает краткую информацию о статусе интерфейса туннеля.

Синтаксис:

- show interfaces tunnel

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

interfaces tunnel detail

Описание:

Отображает детальную информацию о статусе интерфейса туннеля.

Синтаксис:

- show interfaces tunnel detail

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Протокол SIT

Обзор

Протокол туннелирования SIT работает на сетевом уровне модели OSI и поддерживает несколько опций инкапсуляции. SIT может работать по схемам: IPv6-in-IPv4, IPv4-in-IPv4, MPLS-in-IPv4, ANY-in-IPv4. Режим ANY поддерживает IPv4-in-IPv4 и IPv6-in-IPv4. Помимо этого, SIT поддерживает протокол адресации внутри инфраструктуры ISATAP.

Строение пакета при инкапсуляции по протоколу SIT:



В отличие от IP6IP6 SIT обладает более сложной структурой заголовка, которая помимо служебных данных канального уровня включает в себя MAC-адреса локальных устройств, которые подключены к маршрутизатору. Это позволяет протоколу SIT связывать несколько сетей IPv6. Однако усложненная структура заголовка SIT увеличивает нагрузку на маршрутизатор: требуется больше ресурсов и времени на обработку данных.

При настройке протокола важно обратить внимание на ряд особенностей:

1. Большинство межсетевых экранов и систем защиты настроены на анализ трафика, который проходит через стандартные транспортные протоколы (TCP или UDP), так как они содержат понятные заголовки (порты, флаги, номера сессий и т.д.). SIT упаковывает данные прямо в IP-пакет, без использования TCP/UDP. Поэтому некоторые фаерволы могут не знать, как обрабатывать такой трафик и просто блокируют его. При инкапсуляции по протоколу SIT в поле IP-заголовка добавляется номер протокола — «4»;
2. Не поддерживает multicast-вещание;
3. Чувствителен к максимально допустимому размеру передаваемого пакета, поскольку инкапсуляция дополнительного IP-заголовка увеличивает общий размер пакета;
4. Не шифрует обрабатываемый трафик. Для защиты канала связи используйте протоколы шифрования, например IPsec;
5. Не способен фрагментировать пакеты, что вместе с неправильно установленным максимально допустимым размером передаваемого пакета может привести к отбрасыванию пакетов.

Пример настройки

Шаг	Настройка маршрутизатора «А»	Настройка маршрутизатора «Б»	Описание
1	set interfaces tunnel tun1 encapsulation sit	set interfaces tunnel tun1 encapsulation sit	Включает протокол инкапсуляции SIT на интерфейсе туннеля
2	set interfaces tunnel tun1 source-address 192.0.2.10	set interfaces tunnel tun1 source-address 192.0.2.20	Задает IP-адреса источника на интерфейсе туннеля
3	set interfaces tunnel tun1 remote 192.0.2.20	set interfaces tunnel tun1 remote 129.0.2.10	Задает IP-адрес назначения на интерфейсе туннеля
4	set interfaces tunnel tun1 address 2001:db8:bb::1/64	set interfaces tunnel tun1 address 2001:db8:bb::2/64	Задает локальный IP-адрес на интерфейсе туннеля

Список команд

Режим «Конфигурирование»

interfaces tunnel <interface> encapsulation sit

Описание:

Включает протокол туннелирования SIT на интерфейсе туннеля.

Синтаксис:

- set interfaces tunnel <interface> encapsulation sit
- delete interfaces tunnel <interface> encapsulation sit
- show interfaces tunnel <interface> encapsulation

Аргументы:

- <interface> — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> address <address>

Описание:

Задает интерфейсу туннеля локальный IP-адрес.

Синтаксис:

- set interfaces tunnel <interface> address <address>
- delete interfaces tunnel <interface> address <address>
- show interfaces tunnel <interface> address

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — локальный IP-адрес, который администратор вручную назначает интерфейсу туннеля. Может быть указан несколько раз как адрес IPv4 или адрес IPv6.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> source-address <address>

Описание:

Задает интерфейсу туннеля IP-адрес источника.

Синтаксис:

- set interfaces tunnel <interface> source-address <address>
- delete interfaces tunnel <interface> source-address <address>
- show interfaces tunnel <interface> source-address

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — IP-адрес источника. Может быть указан как адрес IPv4 или адрес IPv6.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> remote <address>

Описание:

Задает интерфейсу туннеля IP-адрес назначения.

Синтаксис:

- set interfaces tunnel <interface> remote <address>
- delete interfaces tunnel <interface> remote <address>
- show interfaces tunnel <interface> remote

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — IP-адрес назначения другого интерфейса туннеля. Может быть указан как адрес IPv4 или адрес IPv6.

Режим: «Конфигурирование».

Примечание

Полный список команд для настройки туннельного интерфейса представлен в разделе *Интерфейс туннеля* (страница 215).

Протоколы GRE

Обзор

Протоколы туннелирования GRE (Generic Routing Encapsulation) работают на сетевом уровне модели OSI и в зависимости от своего типа инкапсулируют данные канального или сетевого уровня в IPv4- или IPv6-пакеты.

Маршрутизатор Факел поддерживает следующие протоколы: GRE, .. IP6GRE, GRETAP. .. , IP6GRETAP. Инкапсуляция происходит по схемам: IPv4-in-IPv4, .. IPv6-in-IPv4, IPv4-in-IPv6, IPv6-in-IPv6, Ethernet-in-IPv4. .. , Ethernet-in-IPv6. При инкапсуляции между внутренним заголовком исходного пакета и перед внешним заголовком добавляется дополнительный GRE-заголовок. Протокол GRETAP и его разновидность IP6GRETAP поддерживают псевдопроводную технологию.

По сравнению с другими протоколами туннелирования GRE обладает рядом преимуществ:

- инкапсулирует одновременно данные с несколькими протоколами вне зависимости от их типа;
- работает с multicast-трафиком;
- поддерживает multicast-вещание для формирования соседних связей;
- поддерживает туннельные ключи, что позволяет создавать несколько туннелей с одинаковыми интерфейсами источника и назначения. Туннельный ключ — уникальный идентификатор, который помогает отличать один туннель от другого.

Однако в работе GRE есть также и ряд особенностей:

- Размер GRE-заголовка составляет 4 байта, а размер внешнего IP-заголовка — 20 байт. Из-за этого размер всего инкапсулированного пакета увеличивается на 24 байта, что может приводить к ранней фрагментации из-за выхода размера пакета за пределы максимально допустимого размера передаваемого пакета;
- Большинство межсетевых экранов и систем защиты настроены на анализ трафика, который проходит через стандартные транспортные протоколы (TCP или UDP), так как они содержат понятные заголовки (порты, флаги, номера сессий и т.д.). GRE упаковывает данные прямо в IP-пакет, без использования TCP/UDP. Поэтому некоторые фаерволы могут не знать, как обрабатывать такой трафик и просто блокируют его. При инкапсуляции по протоколу GRE в поле IP-заголовка добавляется номер протокола — «47»;
- По умолчанию протокол туннелирования GRE не шифрует передаваемые данные. Чтобы защитить передачу данных по туннелю, используйте протоколы шифрования типа IPsec.

Более подробная информация содержится в документах RFC 2784.

GRE

Протокол туннелирования GRE инкапсулирует пакеты различных протоколов сетевого уровня в IP-пакеты.

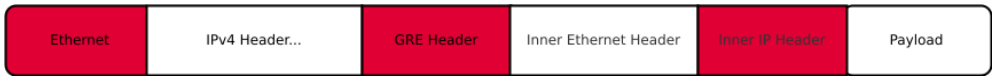
Заголовок пакета при инкапсуляции по протоколу GRE выглядит следующим образом:



GRETAP

Протокол GRETAP инкапсулирует пакеты различных протоколов канального уровня в IPv4-пакеты. Работает по схеме Ethernet-in-IPv4. Поддерживает псевдопроводную технологию.

Структура пакета при инкапсуляции по протоколу GRETAP:



Пример настройки

Шаг	Настройка маршрутизатора «А»	Настройка маршрутизатора «Б»	Описание
1	set interfaces tunnel `tun1` encapsulation `gre`	set interfaces tunnel `tun1` encapsulation `gre`	Включает протокол инкапсуляции GRE на интерфейсе туннеля
2	set interfaces tunnel `tun1` source-address `198.51.100.2`	set interfaces tunnel `tun1` source-address `203.0.113.10`	Задает IP-адреса источника на интерфейсе туннеля
3	set interfaces tunnel `tun1` remote `203.0.113.10`	set interfaces tunnel `tun1` remote `198.51.100.2`	Задает IP-адрес назначения на интерфейсе туннеля
4	set interfaces tunnel `tun1` address `10.0.0.1/30`	set interfaces tunnel `tun1` address `10.0.0.2/30`	Задает локальный IP-адрес на интерфейсе туннеля

Список команд

Режим «Конфигурирование»

interfaces tunnel <interface> encapsulation gre

Описание:

Включает протокол туннелирования GRE на интерфейсе туннеля.

Синтаксис:

- set interfaces tunnel `<interface>` encapsulation gre
- delete interfaces tunnel `<interface>` encapsulation gre

- show interfaces tunnel <interface> encapsulation

Аргументы:

- <interface> — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> encapsulation ip6gre

Описание:

Включает протокол туннелирования IP6GRE на интерфейсе туннеля.

Синтаксис:

- set interfaces tunnel <interface> encapsulation ip6gre
- delete interfaces tunnel <interface> encapsulation ip6gre
- show interfaces tunnel <interface> encapsulation

Аргументы:

- <interface> — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> encapsulation gretap

Описание:

Включает протокол туннелирования GRETAP на интерфейсе туннеля.

Синтаксис:

- set interfaces tunnel <interface> encapsulation gretap
- delete interfaces tunnel <interface> encapsulation gretap
- show interfaces tunnel <interface> encapsulation

Аргументы:

- <interface> — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> encapsulation ip6gretap

Описание:

Включает протокол туннелирования IP6RETAP на интерфейсе туннеля.

Синтаксис:

- set interfaces tunnel <interface> encapsulation ip6gretap
- delete interfaces tunnel <interface> encapsulation ip6gretap
- show interfaces tunnel <interface> encapsulation

Аргументы:

- <interface> — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> address <address>

Описание:

Задает интерфейсу туннеля локальный IP-адрес.

Синтаксис:

- set interfaces tunnel <interface> address <address>
- delete interfaces tunnel <interface> address <address>
- show interfaces tunnel <interface> address

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — локальный IP-адрес, который администратор вручную назначает интерфейсу туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> source-address <address>

Описание:

Задает интерфейсу туннеля IP-адрес источника.

Синтаксис:

- set interfaces tunnel <interface> source-address <address>
- delete interfaces tunnel <interface> source-address <address>
- show interfaces tunnel <interface> source-address

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — IP-адрес источника.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> remote <address>

Описание:

Задает интерфейсу туннеля IP-адрес назначения.

Синтаксис:

- set interfaces tunnel <interface> remote <address>
- delete interfaces tunnel <interface> remote <address>
- show interfaces tunnel <interface> remote

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — IP-адрес назначения другого интерфейса туннеля. Может быть указан как адрес IPv4 или адрес IPv6.

Режим: «Конфигурирование».

Примечание

Полный список команд для настройки туннельного интерфейса представлен в разделе *Интерфейс туннеля* (страница 215).

Зеркалирование интерфейса туннеля

Обзор

Зеркалирование дублирует входящий или исходящий трафик с логического интерфейса туннеля на физический или виртуальный *SPAN-интерфейс*. К SPAN-интерфейсу может быть подключено специальное анализирующее оборудование или ПО: система контроля поведения, система обнаружения вторжения, сборщик трафика. Технология зеркалирования анализирует трафик изолировано от порта с исходным трафиком и не оказывает влияния на передаваемые данные или быстродействие системы.

Для каждого направления трафика существует своя настройка: *mirror ingress* для входящего трафика и *mirror egress* для исходящего. SPAN-интерфейсы должны быть настроены отдельно для трафика с различным направлением.

Список команд

Режим «Конфигурирование»

interfaces tunnel <interface> mirror ingress <monitor-interface>

Описание:

Дублирует входящий трафик с порта интерфейса туннеля на порт SPAN-интерфейса.

Синтаксис:

- set interfaces tunnel `<interface>` mirror ingress `<monitor-interface>`
- delete interfaces tunnel `<interface>` mirror ingress `<monitor-interface>`
- show interfaces tunnel `<interface>` mirror ingress

Аргументы:

- `<interface>` — имя интерфейса туннеля;
- `<monitor-interface>` — имя SPAN-интерфейса.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> mirror egress <monitor-interface>

Описание:

Дублирует исходящий трафик с порта интерфейса туннеля на порт SPAN-интерфейса.

Синтаксис:

- set interfaces tunnel <interface> mirror egress <monitor-interface>
- delete interfaces tunnel <interface> mirror egress <monitor-interface>
- show interfaces tunnel <interface> mirror egress

Аргументы:

- <interface> — имя интерфейса туннеля;
- <monitor-interface> — имя SPAN-интерфейса.

Режим: «Конфигурирование».

Протокол IPIP

Обзор

Протокол туннелирования IPIP работает на сетевом уровне модели OSI и инкапсулирует исходный IPv4- или MPLS-пакет в дополнительный IPv4-заголовок по схемам: IPv4-in-IPv4, MPLS-in-IPv4.

Структура пакета при инкапсуляции по протоколу IPIP:



При настройке протокола важно обратить внимание на ряд особенностей:

1. Большинство межсетевых экранов и систем защиты настроены на анализ трафика, который проходит через стандартные транспортные протоколы (TCP или UDP), так как они содержат понятные заголовки (порты, флаги, номера сессий и т.д.). SIT упаковывает данные прямо в IP-пакет, без использования TCP/UDP. Поэтому некоторые фаерволы могут не знать, как обрабатывать такой трафик и просто блокируют его. При инкапсуляции по протоколу SIT в поле IP-заголовка добавляется номер протокола — «41»;
2. Не поддерживает multicast-вещание;
3. Чувствителен к максимально допустимому размеру передаваемого пакета, поскольку инкапсуляция дополнительного IP-заголовка увеличивает общий размер пакета;
4. Не шифрует обрабатываемый трафик. Для защиты канала связи используйте протоколы шифрования, например IPsec;
5. Не способен фрагментировать пакеты, что вместе с неправильно установленным максимально допустимым размером передаваемого пакета может привести к отбрасыванию пакетов.

Более подробная информация содержится в документе RFC 2003.

Внимание

При загрузке модуля IPIP или при включении протокола IPIP на интерфейсе туннеля, ядро системы Факел по умолчанию создает интерфейс tun0 с атрибутами local = any и remote = any.

Когда на интерфейс поступают IPIP-пакеты, ядро системы направляет данные на интерфейс, чьи атрибуты local и remote соответствуют IP-адресам отправителя и получателя. Однако если этого не произойдет, то ядро перенаправит входящие IPIP-пакеты на интерфейс tun0, как на устройство по умолчанию.

Пример настройки

Шаг	Настройка маршрутизатора «А»	Настройка маршрутизатора «Б»	Описание
1	set interfaces tunnel tun1 encapsulation ipip	set interfaces tunnel tun1 encapsulation ipip	Включает протокол инкапсуляции IPIP на интерфейсе туннеля
2	set interfaces tunnel tun1 source-address 192.0.2.10	set interfaces tunnel tun1 source-address 203.0.113.20	Задает IP-адреса источника на интерфейсе туннеля
3	set interfaces tunnel tun1 remote 203.0.113.20	set interfaces tunnel tun1 remote 192.0.2.10	Задает IP-адрес назначения на интерфейсе туннеля
4	set interfaces tunnel tun1 address 192.168.100.200/24	set interfaces tunnel tun1 address 10.16.200.200/24	Задает локальный IP-адрес на интерфейсе туннеля

Список команд

Режим «Конфигурирование»

interfaces tunnel <interface> encapsulation ipip

Описание:

Включает протокол туннелирования IPIP на интерфейсе туннеля.

Синтаксис:

- set interfaces tunnel <interface> encapsulation ipip
- delete interfaces tunnel <interface> encapsulation ipip
- show interfaces tunnel <interface> encapsulation

Аргументы:

- <interface> — имя интерфейса туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> address <address>

Описание:

Задает интерфейсу туннеля локальный IP-адрес.

Синтаксис:

- set interfaces tunnel <interface> address <address>
- delete interfaces tunnel <interface> address <address>
- show interfaces tunnel <interface> address

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — локальный IP-адрес, который администратор вручную назначает интерфейсу туннеля.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> source-address <address>

Описание:

Задает интерфейсу туннеля IP-адрес источника.

Синтаксис:

- set interfaces tunnel <interface> source-address <address>
- delete interfaces tunnel <interface> source-address <address>
- show interfaces tunnel <interface> source-address

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — IP-адрес источника.

Режим: «Конфигурирование».

---

interfaces tunnel <interface> remote <address>

Описание:

Задает интерфейсу туннеля IP-адрес назначения.

Синтаксис:

- set interfaces tunnel <interface> remote <address>
- delete interfaces tunnel <interface> remote <address>
- show interfaces tunnel <interface> remote

Аргументы:

- <interface> — имя интерфейса туннеля;
- <address> — IP-адрес назначения другого интерфейса туннеля.

Режим: «Конфигурирование».

Примечание

Полный список команд для настройки интерфейса туннеля находится в разделе *Интерфейс туннеля* (страница 215).

2.2.8 Интерфейс WireGuard

2.2.8.1 Обзор

WireGuard — коммуникационный протокол с открытым исходным кодом для создания защищенных VPN-туннелей. Протокол работает на интерфейсе WireGuard, который в свою очередь создается на пограничном маршрутизаторе. Интерфейс выполняет роль шлюза: маршрутизирует, шифрует и расшифровывает трафик между удаленными узлами внутри защищенной частной сети.

WireGuard обладает рядом отличительных особенностей:

- Современная криптография: Noise protocol framework, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF и т.д.;
- Компактный читаемый код, который проще исследовать на уязвимости;
- Высокая производительность, так как протокол работает на третьем уровне модели OSI.

Порядок настройкиы соединения WireGuard

1. Создать интерфейсы WireGuard на пограничных маршрутизаторах.
2. Настроить сетевые параметры на интерфейсах обоих маршрутизаторов.

Чтобы маршрутизаторы могли обнаружить друг друга, убедитесь, что на устройствах заданы корректные IP-адреса, порты и маски подсети.

Когда соединение инициирует одноранговый узел сети, настраивать порт прослушивания не обязательно.

Когда интерфейс WireGuard выступает в роли сервера, к которому будут подключаться другие узлы сети, то необходимо указать порт подключения вручную. Если система перезагрузится или сетевой порт будет назначаться динамически, то удаленные устройства не смогут найти маршрутизатор по номеру порта и потеряют с ним связь.

3. Сгенерировать пару из открытого и закрытого ключей для каждого участника соединения и обменяться открытыми ключами.

Перед сеансом связи одноранговые узлы генерируют пару из открытого и закрытого ключей. После этого устройства обмениваются открытыми ключами. С помощью открытого ключа получателя отправитель шифрует данные, чтобы безопасно передать содержимое через общую сеть. Получатель принимает данные и расшифровывает их с помощью своего закрытого ключа. В обратную сторону метод шифрования работает зеркально.

Совет

Чтобы дополнительно защитить трафик, вы можете подключить симметричное шифрование поверх асимметричного. В этом случае для аутентификации участников генерируется одинаковый общий закрытый ключ (preshared key). Поскольку ключ не открытый, а закрытый, обеспечьте его безопасное распространение.

4. Добавить разрешения для межсетевого экрана.

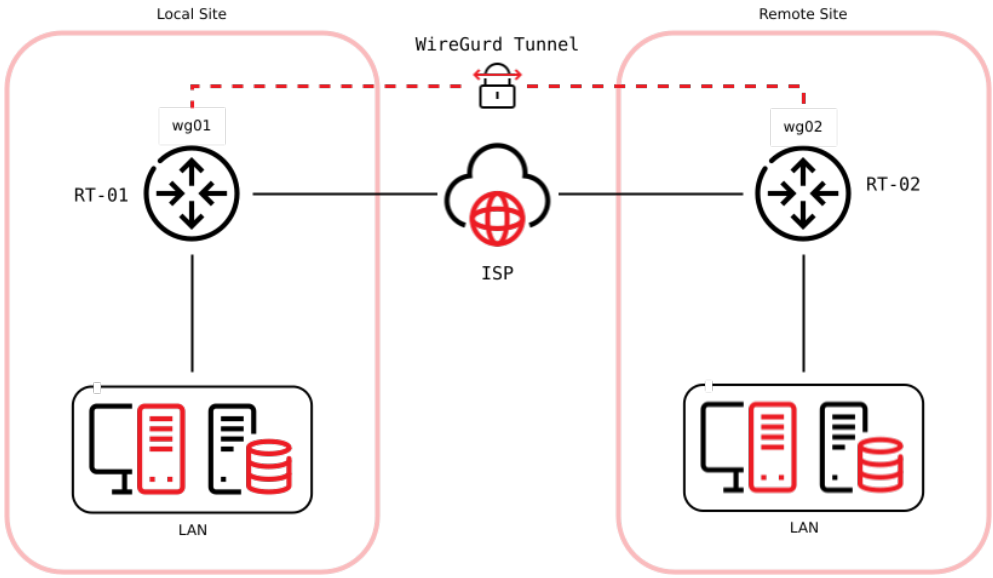
Чтобы туннель WireGuard работал корректно, настройте МСЭ на всех узлах-участниках: разрешите входящий UDP-трафик на порт WireGuard (по умолчанию: 51820), разрешите входящие и производные соединения.

Удаленное подключение

С помощью WireGuard можно не только создать защищенный туннель между двумя узлами сети, но и предоставить безопасный удаленный доступ. В этом случае будет реализована топология сети «звезда».

2.2.8.2 Пример настройки

Шаг	Интерфейс WireGuard 01	Интерфейс WireGuard 02	Описание
1	generate pki wireguard key-pair	generate pki wireguard key-pair	Генерирует пару из открытого и закрытого ключей
2	set interfaces wireguard wg01 private-key KP01	set interfaces wireguard wg02 private-key KP02	Сохраняет закрытый ключ в системе и ассоциирует его с указанным интерфейсом WireGuard
3	set interfaces wireguard wg01 address 10.1.0.1/30	set interfaces wireguard wg02 address 10.1.0.2/30	Назначает интерфейсу WireGuard IPv4-адрес с префиксом подсети
4	set interfaces wireguard wg01 description VPN-to-wg02	set interfaces wireguard wg02 description VPN-to-wg01	Добавляет описание для интерфейса WireGuard
5	set interfaces wireguard wg01 peer to-RT-02 allowed-ips 192.168.2.0/24	set interfaces wireguard wg02 peer to-RT-01 allowed-ips 192.168.1.0/24	Указывает IP-адрес или диапазон IP-адресов одноранговогo узла, через которые интерфейс WireGuard будет поддерживать двустороннюю связь
6	set interfaces wireguard wg01 peer to-RT-02 address 192.0.2.1	set interfaces wireguard wg02 peer to-RT-01 address 192.0.2.2	Указывает IPv4-адрес одноранговогo узла сети
7	set interfaces wireguard wg01 peer to-RT-02 port 51820	set interfaces wireguard wg02 peer to-RT-01 port 51820	Указывает порт для входящий соединений на одноранговом узле
8	set interfaces wireguard wg01 peer to-RT-02 pubkey XMrlPykaxhdAAiSjhtPlvi30N	set interfaces wireguard wg02 peer to-RT-01 public-key EKY0dxRrSD98QHjfHOK13mZ5P3	Ассоциирует открытый ключ с одноранговым узлом сети
9	set interfaces wireguard wg01 port 51820	set interfaces wireguard wg02 port 51820	Указывает порт для входящих соединений на интерфейсе WireGuard
10	set protocols static interface-route 192.168.2.0/24 next-hop-interface wg01	set protocols static route 192.168.1.0/24 interface wg01	Устанавливает в сеть 192.168.2.0/24 статическую маршрутизацию при прохождении трафика через интерфейс WireGuard



2.2.8.3 Список команд

Режим «Конфигурирование»

interfaces wireguard <interface> address [<x.x.x.x/x> | <h:h:h:h:h:h:h:h/x>]

Описание:

Назначает интерфейсу WireGuard диапазон IP-адресов с префиксом подсети.

Синтаксис:

- set interfaces wireguard `<interface>` address `[<x.x.x.x/x> | <h:h:h:h:h:h:h:h/x>]`
- delete interfaces wireguard `<interface>` address `[<x.x.x.x/x> | <h:h:h:h:h:h:h:h/x>]`
- show interfaces wireguard `<interface>` address

Аргументы:

- `<interface>` — имя интерфейса WireGuard;
- `<x.x.x.x/x>` — диапазон IPv4-адресов с префиксом подсети;

Режим: «Конфигурирование».

interfaces wireguard <interface> description <text>

Описание:

Добавляет описание для интерфейса WireGuard.

Синтаксис:

- set interfaces wireguard <interface> description <text>
- delete interfaces wireguard <interface> description <text>
- show interfaces wireguard <interface> description

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <text> — описание для интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> disable

Описание:

Выключает интерфейс WireGuard. Интерфейсу будет присвоен статус A/D (выключен администратором).

Синтаксис:

- set interfaces wireguard <interface> disable
- delete interfaces wireguard <interface> disable
- show interfaces wireguard <interface>

Аргументы:

- <interface> — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> fwmark <number>

Описание:

Присваивает интерфейсу WireGuard метку соединения fwmark.

Синтаксис:

- set interfaces wireguard <interface> fwmark <number>
- delete interfaces wireguard <interface> fwmark <number>
- show interfaces wireguard <interface> fwmark

Аргументы:

- `<interface>` — имя интерфейса WireGuard;
- `<number>` — числовая метка fwmark.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip adjust-mss [<mss> | <clamp-mss-to-pmtu>]

Описание:

Устанавливает на интерфейсе WireGuard конкретное значение для максимального размера сегмента при передаче пакетов по протоколу TCP или рассчитывает значение автоматически, динамически подстраиваясь под допустимый максимальный размер передаваемого пакета на маршруте.

Конкретным значением администратор ПО Факел задает порог и ограничивает отправку пакетов, размер которых будет превышать заданное значение.

Максимальный размер сегмента — это опциональное поле в заголовке TCP-пакета с установленным флагом SYN. Если автоматическое обнаружение максимального размера передаваемого пакета на маршруте работает некорректно, установите конкретный размер сегмента вручную.

Аргументы:

- `<interface>` — имя интерфейса WireGuard;
- `<mss>` — конкретное значение для максимального размера сегмента на протоколе TCP. Диапазон значений: от 536 до 65535;
- `<clamp-mss-to-pmtu>` — максимальный размер сегмента будет задан автоматически.

Режим: «Конфигурирование».

Подсказка

Максимальный размер сегмента = максимальный размер передаваемого пакета - 20 (заголовок протокола IP) - 20 (заголовок протокола TCP) = 1452 байта при максимальном размере передаваемого пакета в 1492 байт.

---

interfaces wireguard <interface> ip arp-cache-timeout <sec>

Описание:

Задает временной интервал между записями в ARP-кэш на интерфейсе WireGuard. ARP-кэш хранит информацию о связях между IP- и MAC-адресами. Кэш продолжит хранить данные, если от протокола верхнего уровня будет получен соответствующий сигнал. Если сигнал получен не будет, данные будут стерты.

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <sec> — интервал между записью данных в ARP-кэш. Формат: секунды. Диапазон значений: от 1 до 86400. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip disable-arp-filter

Описание:

Выключает фильтрацию по протоколу ARP на интерфейсе WireGuard. ПО Факел сможет отвечать на ARP-запросы IP-адресами с других интерфейсов. Это позволит контролировать, какие интерфейсы будут отвечать на ARP-запросы. Применяется в сложных сетевых конфигурациях, где необходимо строго разделять трафик между интерфейсами.

Если фильтрация через протокол ARP включена (по умолчанию), то на одной подсети смогут существовать несколько сетевых интерфейсов. При этом конкретный интерфейс ответит на ARP-запрос тогда, когда ядро системы примет решение маршрутизировать пакеты через этот интерфейс. Это позволяет настраивать на уровне ядра, какой сетевой интерфейс будет отвечать на ARP-запрос. Однако для этого необходимо использовать маршрутизацию от источника.

Синтаксис:

- set interfaces wireguard <interface> ip disable-arp-filter
- delete interfaces wireguard <interface> ip disable-arp-filter
- show interfaces wireguard <interface> ip

Аргументы:

- <interface> — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip disable-forwarding

Описание:

Выключает переадресацию пакетов по протоколу IP с интерфейса WireGuard на любой другой интерфейс. После выполнения команды интерфейс WireGuard перейдет в режим хоста.

Синтаксис:

- set interfaces wireguard <interface> ip disable-forwarding
- delete interfaces wireguard <interface> ip disable-forwarding
- show interfaces wireguard <interface> ip

Аргументы:

- <interface> — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip enable-arp-accept

Описание:

Создает новые записи в ARP-таблице интерфейса WireGuard для gratuitous ARP-кадров, если им не присвоены соответствующие IP-адреса.

Автоматически обновляет ARP-таблицу при появлении gratuitous ARP-кадров типа «запрос», «ответ».

Если ARP-таблица уже содержит IP-адрес, соответствующий gratuitous ARP-кадру, то таблица все равно будет обновлена, даже если команда не была выполнена.

Синтаксис:

- set interfaces wireguard `<interface>` ip enable-arp-accept
- delete interfaces wireguard `<interface>` ip enable-arp-accept
- show interfaces wireguard `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip enable-arp-announce

Описание:

Ограничивает на интерфейсе WireGuard анонсирование локального IP-адреса источника при отправке IP-пакетов через ARP-запрос. ПО Факел будет использовать в исходящих ARP-запросах только те IP-адреса источника, которые соответствуют локальным IP-адресам в подсети цели.

При генерации ARP-запроса интерфейс WireGuard проверяет все целевые подсети. По умолчанию ПО Факел при отправке ARP-запросов использует любой локальный IP-адрес, настроенный на любом интерфейсе.

Синтаксис:

- set interfaces wireguard `<interface>` ip enable-arp-announce
- delete interfaces wireguard `<interface>` ip enable-arp-announce
- show interfaces wireguard `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip enable-arp-ignore

Описание

Указывает интерфейсу WireGuard отвечать на ARP-запросы только в том случае, если целевой IP-адрес — локальный адрес на принимающем интерфейсе, который получил ARP-запрос.

По умолчанию интерфейс WireGuard отвечает на ARP-запросы даже в том случае, если целевой IP-адрес — локальный IP-адрес назначения на любом интерфейсе. Независимо от того, какой интерфейс получил запрос.

Синтаксис:

- set interfaces wireguard `<interface>` ip enable-arp-ignore
- delete interfaces wireguard `<interface>` ip enable-arp-ignore
- show interfaces wireguard `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip enable-directed-broadcast

Описание:

Включает направленную широковещательную переадресацию на интерфейсе WireGuard. Если IP-адрес интерфейса получит пакет через широковещательную рассылку, то маршрутизатор Факел переадресует его на подсеть назначения.

Более подробная информация содержится в документах RFC 1812 и 2644.

Синтаксис:

- set interfaces wireguard `<interface>` ip enable-directed-broadcast
- delete interfaces wireguard `<interface>` ip enable-directed-broadcast
- show interfaces wireguard `<interface>` ip

Аргументы:

- `<interface>` — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip enable-proxy-arp

Описание:

Включает прокси-сервер на интерфейсе WireGuard для маршрутизации ARP-запросов. Интерфейс WireGuard сможет отвечать со своих MAC-адресов на ARP-запросы со стороны IP-адресов назначения, если IP-адреса назначения будут находиться на других интерфейсах маршрутизатора. В дальнейшем ПО Факел будет перенаправлять пакеты на IP-адреса назначения через прокси-сервер.

Синтаксис:

- set interfaces wireguard <interface> ip enable-proxy-arp
- delete interfaces wireguard <interface> ip enable-proxy-arp
- show interfaces wireguard <interface> ip

Аргументы:

- <interface> — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip proxy-arp-pvlan

Описание:

Создает на интерфейсе WireGuard частную сеть VLAN и включает на ней прокси-сервер для маршрутизации ARP-запросов. Устройства на разных портах смогут отвечать на ARP-запросы вышестоящего маршрутизатора и получат возможность обмениваться данными. Фактически интерфейс выступает в роли коммутатора, когда отдельные порты не могут общаться друг с другом напрямую, но могут поддерживать связь через вышестоящий маршрутизатор посредством маршрутизации ARP-запросов через прокси-сервер.

Более подробная информация содержится в документе RFC 3069.

Синтаксис:

- set interfaces wireguard <interface> ip proxy-arp-pvlan
- delete interfaces wireguard <interface> ip proxy-arp-pvlan
- show interfaces wireguard <interface> ip

Аргументы:

- <interface> — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> ip source-validation [<strict> | <loose> | <disable>]

Описание:

Включает на интерфейсе WireGuard различные режимы проверки источника запроса по обратному пути.

Более подробная информация содержится в документе RFC 3704.

Синтаксис:

- set interfaces wireguard <interface> ip source-validation [<strict | loose | disable>]
- delete interfaces wireguard <interface> ip source-validation [<strict | loose | disable>]
- show interfaces wireguard <interface> ip

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <strict> — строгий режим. Применяется для предотвращения подмены IP-адреса при DDos-атаках. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника не соответствует записи в таблице FIB, пакет не пройдет проверку и будет отброшен. В этом режиме некоторые полезные пакеты могут быть отклонены, если сеть имеет сложную конфигурацию;
- <loose> — нестрогий режим. Применяется в случае ассиметричной маршрутизации или другой сложной конфигурации сети. Каждый входящий пакет проверяется по таблице FIB. Если IP-адрес источника недоступен ни через какой интерфейс, то пакет не пройдет проверку и будет отброшен;
- <disable> — проверка источника по обратному пути выключена.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> mirror ingress <monitor-interface>

Описание:

Дублирует входящий трафик с порта интерфейса WireGuard на порт SPAN-интерфейса.

Синтаксис:

- set interfaces wireguard <interface> mirror ingress <monitor-interface>
- delete interfaces wireguard <interface> mirror ingress <monitor-interface>
- show interfaces wireguard <interface> mirror ingress

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <monitor-interface> — имя SPAN-интерфейса.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> mirror egress <monitor-interface>

Описание:

Дублирует исходящий трафик с порта интерфейса WireGuard на порт SPAN-интерфейса.

Синтаксис:

- set interfaces wireguard <interface> mirror egress <monitor-interface>
- delete interfaces wireguard <interface> mirror egress <monitor-interface>
- show interfaces wireguard <interface> mirror egress

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <monitor-interface> — имя SPAN-интерфейса.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> mtu <mtu>

Описание:

Устанавливает максимальный размер передаваемого пакета на интерфейсе WireGuard.

Синтаксис:

- set interfaces wireguard <interface> mtu <mtu>
- delete interfaces wireguard <interface> mtu <mtu>
- show interfaces wireguard <interface> mtu

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <mtu> — максимальный размер передаваемого пакета. Формат: байты. Диапазон значений: от 68 до 16000.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> peer <peer>

Описание:

Ассоциирует интерфейс WireGuard с одноранговым узлом с определенным именем.

Синтаксис:

- set interfaces wireguard <interface> peer <peer>

- delete interfaces wireguard <interface> peer <peer>
- show interfaces wireguard <interface> peer

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <peer> — имя одноранговго узла.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> peer <peer> address [<x.x.x.x> | <h:h:h:h:h:h:h:h>]

Описание:

Указывает IP-адрес одноранговго узла, с которым интерфейс WireGuard будет устанавливать связь.

Синтаксис:

- set interfaces wireguard <interface> peer <peer> address [<x.x.x.x> | <h:h:h:h:h:h:h:h>]
- delete interfaces wireguard <interface> peer <peer> address [<x.x.x.x> | <h:h:h:h:h:h:h:h>]
- show interfaces wireguard <interface> peer <peer> address

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <peer> — имя одноранговго узла;
- <x.x.x.x> — IPv4-адрес одноранговго узла;

Режим: «Конфигурирование».

---

interfaces wireguard <interface> peer <peer> allowed-ips <address>

Описание:

Указывает IP-адрес или диапазон IP-адресов одноранговго узла, через которые интерфейс WireGuard будет поддерживать двустороннюю связь.

Синтаксис:

- set interfaces wireguard <interface> peer <peer> allowed-ips <address>
- delete interfaces wireguard <interface> peer <peer> allowed-ips <address>
- show interfaces wireguard <interface> peer <peer> allowed-ips

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <peer> — имя одноранговго узла;

- <address>— IP-адреса, через которые интерфейс WireGuard будет поддерживать двустороннюю связь. Формат: IPv4, CIDR, диапазон IP-адресов. Перечислить значения можно через запятую.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> peer <peer> description <description>

Описание:

Добавляет описание для одноранговой узла, с которым интерфейс WireGuard будет устанавливать связь.

Синтаксис:

- set interfaces wireguard <interface> peer <peer> description <description>
- delete interfaces wireguard <interface> peer <peer> description <description>
- show interfaces wireguard <interface> peer <peer> description

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <peer> — имя одноранговой узла;
- <description> — описание для одноранговой узла.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> peer <peer> disable

Описание:

Отключает связь интерфейса WireGuard с указанным одноранговым узлом.

Синтаксис:

- set interfaces wireguard <interface> peer <peer> disable
- delete interfaces wireguard <interface> peer <peer> disable
- show interfaces wireguard <interface> peer <peer>

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <peer> — имя одноранговой узла.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> peer <peer> persistent-keepalive <sec>

Описание:

Задает интервал отправки keepalive-сообщений со стороны одноранговового узла, с которым интерфейс WireGuard будет устанавливать связь.

Синтаксис:

set interfaces wireguard <interface> peer <peer> persistent-keepalive <sec> delete interfaces wireguard <interface> peer <peer> persistent-keepalive <sec> show interfaces wireguard <interface> peer <peer> persistent-keepalive

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <peer> — имя одноранговового узла.
- <sec> — интервал отправки keepalive-сообщений со стороны одноранговового узла. Диапазон значений: от 1 до 65535. Формат: секунды.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> peer <peer> port <port>

Описание:

Указывает порт для входящий соединений на одноранговом узле, с которым интерфейс WireGuard будет устанавливать связь.

Синтаксис:

- set interfaces wireguard <interface> peer <peer> port <port>
- delete interfaces wireguard <interface> peer <peer> port <port>
- show interfaces wireguard <interface> peer <peer> port

Аргументы:

- port — Диапазон значений: от 1 до 65535.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> <peer> preshared-key <key>

Описание:

Ассоциирует общий секретный ключ с одноранговым узлом сети, с которым интерфейс WireGuard будет устанавливать связь.

Синтаксис:

- set interfaces wireguard <interface> <peer> preshared-key <key>
- delete interfaces wireguard <interface> <peer> preshared-key <key>
- show interfaces wireguard <interface> <peer> preshared-key

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <peer> — имя одноранговго узла;
- <key> — общий секретный ключ.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> peer <peer> public-key <key>

Описание:

Ассоциирует открытый ключ с одноранговым узлом сети, с которым интерфейс WireGuard будет устанавливать связь.

Синтаксис:

- set interfaces wireguard <interface> peer public-key <key>
- delete interfaces wireguard <interface> peer <peer> public-key <key>
- show interfaces wireguard <interface> peer <peer> public-key

Аргументы:

<interface> — интерфейс WireGuard; <peer> — одноранговый узел; <key> — открытый ключ.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> per-client-thread

Описание:

Обрабатывает трафик от каждого клиента в отдельной очереди.

Синтаксис:

- set interfaces wireguard per-client-thread
- delete interfaces wireguard <interface> per-client-thread
- show interfaces wireguard <interface>

Аргументы:

- <interface> — имя интерфейса WireGuard.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> port <port>

Описание:

Указывает порт для входящих соединений на интерфейсе WireGuard.

Синтаксис:

- set interfaces wireguard <interface> port <port>
- delete interfaces wireguard <interface> port <port>
- show interfaces wireguard <interface> port

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <port> — порт для входящий соединений на интерфейсе WireGuard. Диапазон значений: от 1 до 65535.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> private-key <key>

Описание:

Сохраняет закрытый ключ в системе и ассоциирует его с указанным интерфейсом WireGuard.

Синтаксис:

- set interfaces wireguard <interface> private-key <key>
- delete interfaces wireguard <interface> private-key <key>
- show interfaces wireguard <interface> private-key

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <key> — закрытый ключ.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> redirect <destination>

Описание:

Перенаправляет трафик на другой интерфейс маршрутизатора Факел.

Синтаксис:

- set interfaces wireguard <interface> redirect <destination>

- delete interfaces wireguard <interface> redirect <destination>
- show interfaces wireguard <interface> redirect

Аргументы:

- <interface> — имя интерфейса WireGuard;
- <destination> — имя интерфейса, на который будет перенаправлен трафик.

Режим: «Конфигурирование».

---

interfaces wireguard <interface> vrf <vrf>

Описание:

Размещает интерфейс WireGuard на указанном VRF-экземпляре.

Синтаксис: * set interfaces wireguard <interface> vrf <vrf> * delete interfaces wireguard <interface> vrf <vrf> * show interfaces wireguard <interface> vrf

Аргументы: * <interface> — имя интерфейса WireGuard; * <vrf> — имя VRF-экземпляра.

Режим: «Конфигурирование».

Режим «Администрирование»

generate pki wireguard key-pair

Описание:

Генерирует на интерфейсе WireGuard пару из открытого и закрытого ключей. Отображает ключи в консоли, но не сохраняет в системе.

Синтаксис:

generate pki wireguard key-pair

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

generate pki wireguard key-pair install interface <interface>

Описание:

Генерирует на интерфейсе WireGuard пару из открытого и закрытого ключей, ассоциирует с указанным интерфейсом WireGuard. Отображает ключи в консоли, но не сохраняет ключи в системе, а создает команду для ввода в режиме конфигурирования.

Синтаксис:

generate pki wireguard key-pair install interface <interface>

Аргументы:

- <interface> — имя интерфейса WireGuard.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

generate pki wireguard preshared-key

Описание:

Генерирует на интерфейсе WireGuard общий секретный ключ. Отображает ключ в консоли, но не сохраняет в системе.

Синтаксис:

generate pki wireguard preshared-key

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Внимание

Поскольку ключ не открытый, а закрытый, обеспечьте его безопасное распространение.

---

generate pki wireguard preshared-key install interface <interface> peer <peer>

Описание:

Генерирует на интерфейсе WireGuard общий секретный ключ, ассоциирует с одноранговым узлом на указанном интерфейсе. Отображает ключ в консоли, но не сохраняет ключ в системе, а создает команду для ввода в режиме конфигурирования.

Внимание

Поскольку ключ не открытый, а закрытый, обеспечьте его безопасное распространение.

Синтаксис:

generate pki wireguard preshared-key install interface <interface> peer <peer>

Аргументы:

<interface> — интерфейс WireGuard; <peer> — одноранговый узел;

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

generate wireguard client-config <name> interface <interface> server <ip|fqdn> address <client-ip>

Описание:

Генерирует конфигурацию для клиента, который будет подключаться к интерфейсу WireGuard (серверу). Автоматически встраивает в конфигурацию открытый ключ интерфейса WireGuard. Также создает набор команд для ввода в консоль в режиме конфигурирования. Дополнительно выводит конфигурацию на экран в виде QR-кода.

При выполнении команды система запросит IP-адрес или полное доменное имя (FQDN) сервера, к которому будет подключаться клиент. Также система-сервер предложит назначить клиенту виртуальный IPv4- и/или IPv6-адрес для связи внутри подсети туннеля WireGuard.

Синтаксис:

- set generate wireguard client-config <name> interface <interface> server <ip | fqdn> address <client-ip>
- delete generate wireguard client-config <name> interface <interface> server <ip | fqdn> address <client-ip>
- show generate wireguard client-config <name> interface <interface> server <ip | fqdn> address

Аргументы:

- <name> — имя конфигурации для клиента;
- <interface> — имя интерфейса WireGuard;
- <ip> — IP-адрес WireGuard-сервера;
- <fqdn> — полное доменное имя WireGuard-сервера;
- <client-ip> — виртуальный IP-адрес, который WireGuard-сервер назначит клиенту.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show interfaces wireguard wg10

Описание:

Отображает краткую информацию о статусе интерфейса WireGuard.

Синтаксис:

show interfaces wireguard wg10

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show interfaces wireguard <interface> allowed-ips

Описание:

Отображает IP-адреса, через которые интерфейс WireGuard поддерживает двустороннюю связь с другим одноранговым узлом.

Синтаксис:

show interfaces wireguard <interface> allowed-ips

Аргументы:

- `<interface>` — имя интерфейса WireGuard.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show interfaces wireguard <interface> endpoints

Описание:

Отображает информацию о конечных точка, с которыми интерфейс WireGuard установил связь.

Синтаксис:

show interfaces wireguard <interface> endpoints

Аргументы:

- `<interface>` — имя интерфейса WireGuard.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show interfaces wireguard <interface> peers

Описание:

Отображает идентификаторы одноранговых узлов, с которыми интерфейс WireGuard установил связь.

Синтаксис:

show interfaces wireguard <interface> peers

Аргументы:

- `<interface>` — имя интерфейса WireGuard.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show interfaces wireguard <interface> public-key

Описание:

Отображает открытый ключ, ассоциированный с указанным интерфейсом WireGuard.

Синтаксис:

show interfaces wireguard <interface> public-key

Аргументы:

- `<interface>` — имя интерфейса WireGuard.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show interfaces wireguard <interface> summary

Описание:

Отображает сводную информацию о текущей конфигурации и об устройстве.

Синтаксис:

show interfaces wireguard `<interface>` summary

Аргументы:

- `<interface>` — имя интерфейса WireGuard.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

generate pki key-pair file <filename>

Описание:

Генерирует пару из открытого и закрытого ключей, сохраняет их в файл. Сгенерированные ключи не будут привязаны к какому-либо интерфейсу.

Синтаксис:

generate pki key-pair file `<filename>`

Аргументы:

- `<filename>` — имя файла, в который будет сохранена пара ключей.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

generate pki key-pair install

Описание:

Генерирует пару из открытого и закрытого ключей. Отображает ключи в консоли, но не сохраняет ключи в системе. Также предлагает сгенерировать команду для ввода в режиме конфигурирования. Сгенерированные ключи не будут привязаны к какому-либо интерфейсу.

Команды, которые будут сгенерированы для ввода в режиме конфигурирования:

set pki key-pair <key-name> public key <key>
set pki key-pair <key-name> private key <key>

Синтаксис:

generate pki key-pair install

Режим: «Администрирование».

Уровень привилегий: «Администратор».

2.2.9 OpenVPN

2.2.9.1 Описание

OpenVPN — реализация технологии виртуальной частной сети, которая имеет открытый исходный код с целью формирования зашифрованных каналов по схеме «точка-точка» и «сервер-клиент» между различными компьютерными устройствами.

OpenVPN работает на большом количестве платформ: Windows, macOS, iOS, Android, Linux, FreeBSD, OpenBSD, NetBSD и даже Solaris.

Безопасность OpenVPN обеспечивается с помощью шифрования и аутентификации посредством библиотеки OpenSSL, 256-битных ключей шифрования и шифров высокого уровня.

Общие технические характеристики:

- Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку OpenSSL. Для достижения более высокого уровня безопасности соединения OpenVPN может использовать шифры AES, Camellia, 3DES, CAST-128 или Blowfish.
- Хотя OpenVPN не поддерживает L2TP, IPSec и PPTP, в нём используется собственный протокол на базе TLS и SSL.
- OpenVPN позволяет усовершенствовать процедуру авторизации и аутентификации за счёт привлечения сторонних плагинов и скриптов.
- Клиенты могут подключаться к серверам за пределами сервера OpenVPN, так как он поддерживает настройку частной подсети.
- Чтобы защитить пользователей от переполнения буфера в реализациях TLS/SSL, DoS-атак, сканирования портов и наводнения портов, OpenVPN использует tls-auth для верификации подписи HMAC. Структура OpenVPN позволяет сбросить привилегии при необходимости, а также использовать изоляцию chroot для CRL.
- OpenVPN работает в пространстве пользователя, а не ядра.

OpenVPN предлагает пользователю несколько видов аутентификации:

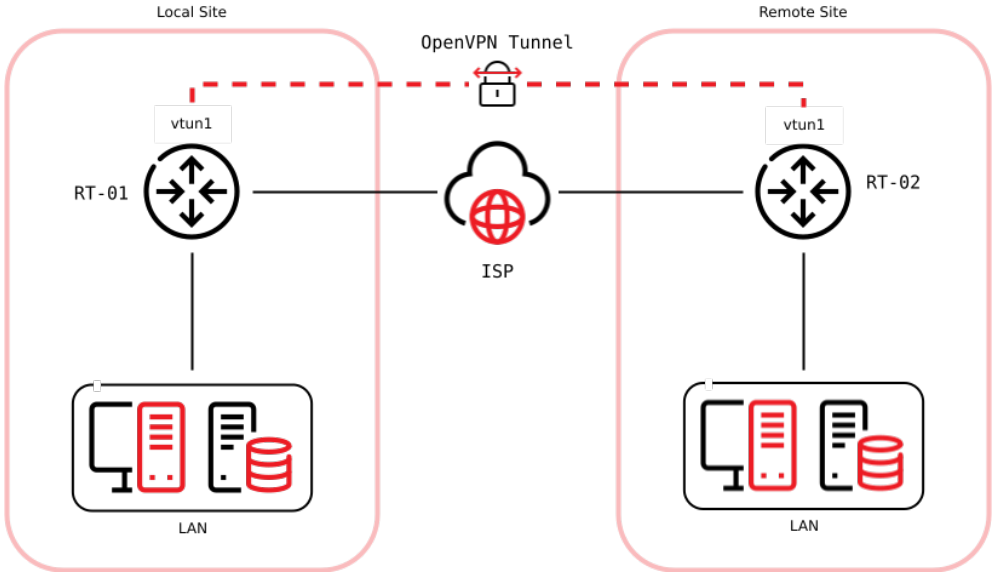
- Предустановленный ключ — самый простой метод.
- Аутентификация по сертификатам x.509 — наиболее гибкий в настройках метод.
- С помощью логина и пароля — может использоваться без создания клиентского сертификата (серверный сертификат всё равно нужен).

Для передачи трафика внутри туннеля OpenVPN использует транспортные протоколы TCP и UDP. В общем случае предпочтительным является использование протокола UDP. Через туннель проходит трафик сетевого уровня и выше, если используется TUN-соединение. OpenVPN для клиента выступает протоколом канального или даже физического уровня, а это значит, что надежность передачи данных может обеспечиваться вышестоящими уровнями, если это необходимо. Именно поэтому протокол UDP по своей концепции наиболее близок к OpenVPN, так как он, как и протоколы канального и физического уровней, не обеспечивает надежности соединения, передавая эту задачу более высоким уровням. Если настроить OpenVPN туннель на работу по протоколу TCP, сервер будет получать TCP сегменты OpenVPN, которые содержат другие TCP сегменты от клиента. В результате в цепи получается двойная проверка на целостность информации, что совершенно не имеет смысла, так как надежность не повышается, а скорости соединения снижается.

2.2.9.2 Настройка

Пример настройки

Пример настройки OpenVPN туннеля между двумя площадками.



Режим site-to-site поддерживает режим аутентификации с использованием сертификатов x.509, но не требует его и также может работать с статическими ключами pre-shared-key (PSK), что во многих случаях проще. Настроим туннель OpenVPN между сайтами, используя 2048-битный PSK.

Сначала на локальном шлюзе генерирует ключ с помощью о `generate openvpn key <имя_файла>`. Это приведет к созданию ключа с указанным именем в директории /config/auth/. После генерации нужно будет скопировать этот ключ на удаленный маршрутизатор. В нашем примере мы использовали имя файла openvpn-1.key, на который будем ссылаться ниже.

- Публичный IP-адрес локальной стороны VPN будет 198.51.100.10.
-
- Публичный IP-адрес удаленной стороны VPN будет 203.0.113.11.
-
- Туннель будет использовать 10.255.1.1 для локального IP-адреса и 10.255.1.2 для удаленного.
-
- Локальный сайт будет иметь подсеть 10.0.0.0/16.
-
- Удаленный сайт будет иметь подсеть 10.1.0.0/16.
-
- Статическая маршрутизация или другие протоколы динамической маршрутизации могут быть использованы через интерфейс vtun.
-
- OpenVPN позволяет использовать TCP или UDP. UDP обеспечивает наименьшую задержку, в то время как TCP лучше работает для соединений с потерями; в целом UDP предпочтительнее, когда это возможно.

-
- Официальный порт для OpenVPN - 1194, который мы оставляем для клиентских VPN; мы будем использовать 1195 для VPN между сайтами.
-
- Директива persistent-tunnel позволит нам настраивать атрибуты, связанные с туннелем, такие как политика межсетевого экрана, как это делается на любом обычном сетевом интерфейсе.
- Если IP-адрес удаленного маршрутизатора известен, его можно настроить с помощью директивы remote-host; если неизвестен, ее можно опустить. Мы будем использовать динамический IP для нашего удаленного маршрутизатора.

Конфигурация локального маршрутизатора

```
set interfaces openvpn vtun1 mode site-to-site
set interfaces openvpn vtun1 protocol udp
set interfaces openvpn vtun1 persistent-tunnel
set interfaces openvpn vtun1 remote-host '203.0.113.11'
set interfaces openvpn vtun1 local-port '1195'
set interfaces openvpn vtun1 remote-port '1195'
set interfaces openvpn vtun1 shared-secret-key-file '/config/auth/openvpn-1.key'
set interfaces openvpn vtun1 local-address '10.255.1.1'
set interfaces openvpn vtun1 remote-address '10.255.1.2'
```

Конфигурация удаленного маршрутизатора

```
set interfaces openvpn vtun1 mode site-to-site
set interfaces openvpn vtun1 protocol udp
set interfaces openvpn vtun1 persistent-tunnel
set interfaces openvpn vtun1 remote-host '198.51.100.10'
set interfaces openvpn vtun1 local-port '1195'
set interfaces openvpn vtun1 remote-port '1195'
set interfaces openvpn vtun1 shared-secret-key-file '/config/auth/openvpn-1.key'
set interfaces openvpn vtun1 local-address '10.255.1.2'
set interfaces openvpn vtun1 remote-address '10.255.1.1'
```

Конфигурация межсетевого экрана

Необходимо создать исключение в межсетевом экране, чтобы разрешить прохождение трафика OpenVPN через WAN-интерфейс.

```
set firewall name OUTSIDE_LOCAL rule 10 action accept
set firewall name OUTSIDE_LOCAL rule 10 description 'Allow established/related'
set firewall name OUTSIDE_LOCAL rule 10 state established enable
set firewall name OUTSIDE_LOCAL rule 10 state related enable
set firewall name OUTSIDE_LOCAL rule 20 action accept
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set firewall name OUTSIDE_LOCAL rule 20 description OpenVPN_IN
set firewall name OUTSIDE_LOCAL rule 20 destination port 1195
set firewall name OUTSIDE_LOCAL rule 20 log enable
set firewall name OUTSIDE_LOCAL rule 20 protocol udp
set firewall name OUTSIDE_LOCAL rule 20 source
```

Также необходимо убедиться, что группа правил межсетевого экрана OUTISDE_LOCAL применяется к интерфейсу WAN и направлению (локальный).

```
set interfaces ethernet eth0 firewall local name 'OUTSIDE-LOCAL'
```

Настройка маршрутизации

Статические маршруты могут быть настроены с учетом интерфейса туннеля. Локальный маршрутизатор будет использовать сеть 10.0.0.0/16, а удаленный - 10.1.0.0/16:

локальный маршрутизатор:

```
set protocols static interface-route 10.1.0.0/16 next-hop-interface vtun1
```

Удаленный маршрутизатор:

```
set protocols static interface-route 10.0.0.0/16 next-hop-interface vtun1
```

В приведенных выше конфигурациях по умолчанию используется 256-битный AES в режиме GCM для шифрования (если обе стороны поддерживают NCP) и SHA-1 для аутентификации HMAC. SHA-1 считается слабым, но доступны и другие алгоритмы хэширования, а также алгоритмы шифрования:

Для шифрования:

```
fakel@fakel# set int open vtun0 encryption ncp-ciphers
Possible completions:
  des           DES algorithm
  3des          DES algorithm with triple encryption
  aes128        AES algorithm with 128-bit key CBC
  aes128gcm     AES algorithm with 128-bit key GCM
  aes192        AES algorithm with 192-bit key CBC
  aes192gcm     AES algorithm with 192-bit key GCM
  aes256        AES algorithm with 256-bit key CBC
  aes256gcm     AES algorithm with 256-bit key GCM
```

Для хэширования:

```
fakel@fakel# set interfaces openvpn vtun1 hash
Possible completions:
  md5           MD5 algorithm
  sha1          SHA-1 algorithm
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  sha256       SHA-256 algorithm
  sha512       SHA-512 algorithm
```

Если вы измените стандартные алгоритмы шифрования и хэширования, убедитесь, что на локальном и удаленном концах установлены одинаковые конфигурации, иначе туннель не заработает.

Политика межсетевого экрана также может быть применена к интерфейсу туннеля для локального, входящего и исходящего направлений и функционирует идентично интерфейсам ethernet.

Если используется несколько туннелей, OpenVPN должен иметь способ различать разные туннели, кроме предварительного совместного ключа. Это может быть либо ссылка на IP-адрес, либо номер порта. Один из вариантов - выделение публичного IP-адреса для каждого туннеля. Другой вариант - присвоить каждому туннелю номер порта.

Статус OpenVPN можно проверить с помощью команды `show openvpn operational`. Полный список опций см. во встроенной справке.

Сервер OpenVPN

Многоклиентский сервер - самый популярный режим OpenVPN на маршрутизаторах. Он всегда использует аутентификацию x.509 и поэтому требует настройки PKI. Обратитесь к разделу Генерация сертификатов и ключей X.509, чтобы сгенерировать сертификат ЦС, сертификат и ключ сервера, список отзыва сертификатов, файл параметров обмена ключами Диффи-Хеллмана. Для настройки сервера клиентские сертификаты и ключи не нужны.

В этом примере используется сценарий, в которой каждый клиент является маршрутизатором, имеющим собственную подсеть, поскольку более простые настройки являются ее подмножествами.

Предположим, вы хотите использовать сеть 10.23.1.0/24 для конечных точек клиентского туннеля, а все клиентские подсети принадлежат 10.23.0.0/20. Всем клиентам необходим доступ к сети 192.168.0.0/16.

Сначала нам нужно указать основные настройки. По умолчанию используется протокол 1194/UDP. Рекомендуется использовать опцию `persistent-tunnel`, она предотвращает закрытие TUN/TAP-устройства при сбросе соединения или перезагрузке демона.

Примечание

Использование **openvpn-опции -reneg-sec** может быть сложным. Эта опция используется для пересогласования канала передачи данных через <n> секунд. При использовании как на сервере, так и на клиенте, меньшее значение будет инициировать пересогласование. Если вы установите значение 0 на одной стороне соединения (чтобы отключить его), выбранное значение на другой стороне будет определять, когда произойдет пересогласование.

```
set interfaces openvpn vtun10 mode server
set interfaces openvpn vtun10 local-port 1194
set interfaces openvpn vtun10 persistent-tunnel
set interfaces openvpn vtun10 protocol udp
```

Затем нам нужно указать местоположение криптографических материалов. В примере будем использовать */config/auth/openvpn*.

```
set interfaces openvpn vtun10 tls ca-cert-file /config/auth/openvpn/ca.crt
set interfaces openvpn vtun10 tls cert-file /config/auth/openvpn/server.crt
set interfaces openvpn vtun10 tls key-file /config/auth/openvpn/server.key
set interfaces openvpn vtun10 tls crl-file /config/auth/openvpn/crl.pem
set interfaces openvpn vtun10 tls dh-file /config/auth/openvpn/dh2048.pem
```

Теперь нам нужно указать сетевые настройки сервера. Во всех случаях нам нужно указать подсеть для конечных точек клиентского туннеля. Поскольку мы хотим, чтобы клиенты получали доступ к определенной сети за внешним маршрутизатором, мы будем использовать опцию `push-route` для установки этого маршрута на клиентах.

```
set interfaces openvpn vtun10 server push-route 192.168.0.0/16
set interfaces openvpn vtun10 server subnet 10.23.1.0/24
```

Поскольку речь идет о штаб-квартире и филиалах, мы хотим, чтобы все клиенты имели фиксированные адреса и направляли трафик в определенные подсети через них. Для этого нам нужна настройка для каждого клиента.

Примечание

Клиенты идентифицируются по полю CN в их сертификатах x.509, в данном примере CN - `client0`:

```
set interfaces openvpn vtun10 server client client0 ip 10.23.1.10
set interfaces openvpn vtun10 server client client0 subnet 10.23.2.0/25
```

OpenVPN не будет автоматически создавать маршруты в ядре для клиентских подсетей при подключении и будет использовать ассоциацию клиент-подсеть только внутри сети, поэтому нам нужно создать маршрут к сети 10.23.0.0/20 самостоятельно:

```

```

set protocols static interface-route 10.23.0.0/20 next-hop-interface vtun10

Генерация сертификата и ключей X.509

OpenVPN поставляется с набором скриптов под названием Easy-RSA, которые могут генерировать соответствующие файлы, необходимые для настройки OpenVPN с использованием сертификатов X.509. Easy-RSA устанавливается по умолчанию.

Скопируйте скрипты Easy-RSA в новый каталог, чтобы изменить значения.

```
cp -r /usr/share/easy-rsa/ /config/my-easy-rsa-config
cd /config/my-easy-rsa-config
```

Чтобы обеспечить последовательное использование значений при генерации, задайте значения по умолчанию, которые будут использоваться скриптами генерации. Переименуйте имя файла vars.example в vars

```
mv vars.example vars
```

Ниже приведен экземпляр файла после редактирования. Вы также можете изменить другие значения в файле по своему усмотрению, хотя для большинства случаев значения по умолчанию ,должны быть в самый раз (не оставляйте ни один из этих параметров пустым).

```
set_var EASYRSA_DN      "ru"
set_var EASYRSA_REQ_COUNTRY     "RU"
set_var EASYRSA_REQ_PROVINCE    "Moscow"
set_var EASYRSA_REQ_CITY        "Moscow"
set_var EASYRSA_REQ_ORG "IT Route LLC"
set_var EASYRSA_REQ_EMAIL       "pki@it-route.ru"
set_var EASYRSA_REQ_OU          "VPN"
set_var EASYRSA_KEY_SIZE        2048
```

Опция `init-pki` создаст новый каталог или удалит все ранее созданные сертификаты, хранящиеся в этом каталоге. Термин «центральный» используется для обозначения сервера, а «филиал» - для клиента.

Примечание

Запомните «Ключевую фразу CA», введенную в команде build-ca,
поскольку она будет запрошена при подписании сертификата сервера/клиента.

fakel@fakel:/config/my-easy-rsa-config$./easyrsa init-pki fakel@fakel:/config/my-easy-rsa-config$./easyrsa build-ca fakel@fakel:/config/my-easy-rsa-config$./easyrsa gen-req central nopass fakel@fakel:/config/my-easy-rsa-config$./easyrsa sign-req server central fakel@fakel:/config/my-easy-rsa-config$./easyrsa gen-dh fakel@fakel:/config/my-easy-rsa-config$./easyrsa build-client-full branch1 nopass

Чтобы создать список отзыва сертификатов для любого клиента, выполните следующие команды:

```
fakel@fakel:/config/my-easy-rsa-config$./easyrsa revoke client1
fakel@fakel:/config/my-easy-rsa-config$ ./easyrsa gen-crl
```

Скопируйте файлы в /config/auth/openvpn/, чтобы использовать их при создании туннеля OpenVPN

```
fakel@fakel:/config/my-easy-rsa-config$ sudo mkdir /config/auth/openvpn
fakel@fakel:/config/my-easy-rsa-config$ sudo cp pki/ca.crt /config/auth/openvpn
fakel@fakel:/config/my-easy-rsa-config$ sudo cp pki/dh.pem  /config/auth/openvpn
fakel@fakel:/config/my-easy-rsa-config$ sudo cp pki/private/central.key /
  config/auth/openvpn
fakel@fakel:/config/my-easy-rsa-config$ sudo cp pki/issued/central.crt  /
  config/auth/openvpn
fakel@fakel:/config/my-easy-rsa-config$ sudo cp pki/crl.pem /config/auth/openvpn
```

Кроме того, каждому клиенту нужна копия ca.crt и собственные файлы клиентских ключей и сертификатов. Эти файлы являются открытым текстом, поэтому их можно скопировать либо вручную, либо с по-

мощью инструмента удаленной передачи файлов, например scp. Какой бы метод вы ни использовали, файлы должны оказаться в нужном месте на каждом маршрутизаторе. Например, на маршрутизаторе филиала 1 могут быть следующие файлы:

```
fakel@fakel:$ ls /config/auth/openvpn
ca.crt branch1.crt branch1.key
```

Клиент OpenVPN

ПО Факел может выступать не только в качестве сервера для нескольких клиентов. Вы также можете настроить любой интерфейс в качестве клиента OpenVPN, подключающегося к серверу OpenVPN или любому другому серверу OpenVPN.

В следующем примере один маршрутизатор выступает в качестве OpenVPN-сервера, а другой маршрутизатор - в качестве OpenVPN-клиента. Сервер также передает статический IP-адрес клиента клиенту OpenVPN. Помните, что клиенты идентифицируются с помощью атрибута CN в сертификате SSL.

Сервер OpenVPN

```
set interfaces openvpn vtun10 encryption cipher 'aes256'
set interfaces openvpn vtun10 hash 'sha512'
set interfaces openvpn vtun10 local-host '10.11.2.1'
set interfaces openvpn vtun10 local-port '1194'
set interfaces openvpn vtun10 mode 'server'
set interfaces openvpn vtun10 persistent-tunnel
set interfaces openvpn vtun10 protocol 'udp'
set interfaces openvpn vtun10 server client client1 ip '10.10.0.10'
set interfaces openvpn vtun10 server domain-name 'example.org'
set interfaces openvpn vtun10 server max-connections '250'
set interfaces openvpn vtun10 server name-server '172.16.254.30'
set interfaces openvpn vtun10 server subnet '10.10.0.0/24'
set interfaces openvpn vtun10 server topology 'subnet'
set interfaces openvpn vtun10 tls ca-cert-file '/config/auth/ca.crt'
set interfaces openvpn vtun10 tls cert-file '/config/auth/server.crt'
set interfaces openvpn vtun10 tls dh-file '/config/auth/dh.pem'
set interfaces openvpn vtun10 tls key-file '/config/auth/server.key'
set interfaces openvpn vtun10 use-lzo-compression
```

Клиент OpenVPN

```
set interfaces openvpn vtun10 encryption cipher 'aes256'
set interfaces openvpn vtun10 hash 'sha512'
set interfaces openvpn vtun10 mode 'client'
set interfaces openvpn vtun10 persistent-tunnel
set interfaces openvpn vtun10 protocol 'udp'
set interfaces openvpn vtun10 remote-host '10.11.2.1'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set interfaces openvpn vtun10 remote-port '1194'
set interfaces openvpn vtun10 tls ca-cert-file '/config/auth/ca.crt'
set interfaces openvpn vtun10 tls cert-file '/config/auth/client1.crt'
set interfaces openvpn vtun10 tls key-file '/config/auth/client1.key'
set interfaces openvpn vtun10 use-lzo-compression
```

2.2.10 PPoE интерфейс

2.2.10.1 Описание

PPPoE (Point-to-Point Protocol over Ethernet) - это сетевой протокол, используемый для установки соединений типа точка-точка между двумя узлами в сети Ethernet. PPPoE обеспечивает механизм аутентификации пользователей, управления сеансами и маршрутизации данных через Ethernet-сеть.

Протокол PPPoE добавляет кадры PPP поверх Ethernet кадров. Каждый кадр PPPoE состоит из заголовка PPPoE и полезной нагрузки PPP. Заголовок PPPoE содержит информацию, необходимую для управления и маршрутизации кадров PPP, а также метаданные для управления сеансом PPPoE.

Основные характеристики протокола PPPoE

Основные характеристики протокола PPPoE включают:

- **Аутентификация и безопасность:** PPPoE обеспечивает механизм аутентификации для контроля доступа к сети. Это позволяет провайдерам услуг Интернета обеспечить безопасный доступ для своих клиентов, требуя аутентификации с помощью уникальных учетных данных.
- **Масштабируемость и гибкость:** PPPoE позволяет обслуживать большое количество пользователей и предоставлять различные уровни услуг, включая широкополосный доступ к Интернету и специализированные сетевые сервисы.
- **Управление сеансами:** Протокол предоставляет механизм управления сеансами, позволяющий установить, поддерживать и завершать соединение по запросу клиента или провайдера услуг.
- **Динамическое присвоение IP-адресов:** PPPoE поддерживает динамическое присвоение IP-адресов клиентам при установлении сеанса. Это позволяет оптимизировать использование адресного пространства и облегчить администрирование сети.
- **Поддержка различных типов сетей:** PPPoE может использоваться в различных типах сетей, включая Ethernet, Wi-Fi и другие технологии передачи данных. Это делает его универсальным средством подключения к Интернету для различных устройств и сетевых конфигураций.
- **Ретрансляция данных:** Протокол включает в себя механизмы ретрансляции данных, который обеспечивает надежную передачу информации в случае возникновения ошибок или потерь пакетов в сети.
- **Поддержка шифрования и защиты данных:** PPPoE может использовать различные методы шифрования и защиты данных для обеспечения конфиденциальности и целостности передаваемой информации, что делает его подходящим для использования в безопасных сетевых средах.

Принцип работы PPPoE

Процесс работы протокола PPPoE может быть разбит на несколько этапов:

- **Инициализация:** Клиентский узел (обычно маршрутизатор или компьютер) инициирует соединение с сервером PPPoE (например, у поставщика услуг интернета).
- **Отправка запроса на соединение (PADI):** Клиент отправляет широковещательное сообщение PADI (PPPoE Active Discovery Initiation), чтобы найти доступные серверы PPPoE.
- **Ответ сервера (PADO):** Сервер, получивший запрос, отправляет сообщение PADO (PPPoE Active Discovery Offer) с предложением соединения клиенту.

- **Запрос на подключение (PADR):** Клиент выбирает сервер из предложенных и отправляет запрос на подключение PADR (PPPoE Active Discovery Request).
- **Подтверждение (PADS):** Сервер, получив запрос на подключение, отправляет подтверждение PADS (PPPoE Active Discovery Session-confirmation) клиенту.
- **Аутентификация:** Происходит обмен данными для аутентификации клиента. Это может включать в себя ввод имени пользователя и пароля.
- **Установление сеанса PPP:** После успешной аутентификации устанавливается сеанс протокола PPP (Point-to-Point Protocol) между клиентом и сервером.
- **Передача данных:** После установления сеанса PPP между клиентом и сервером начинается передача данных. Это может включать передачу IP-пакетов и других сетевых данных.
- **Мониторинг сеанса:** Во время сеанса обе стороны могут отслеживать его состояние, проверяя статус подключения и обмен сетевыми пакетами.
- **Завершение сеанса:** По окончании использования клиент может завершить сеанс, отправив соответствующий запрос серверу PPPoE.
- **Завершение соединения:** После завершения сеанса сервер освобождает ресурсы, занятые для этой сессии, и закрывает соединение.
- **Обработка ошибок и ретрансляция данных:** В случае возникновения ошибок или потерь пакетов в сети, PPPoE может осуществлять ретрансляцию (повторную отправку) пакетов для гарантированной доставки информации.

Этот процесс обеспечивает эффективное и безопасное управление соединением между клиентом и сервером PPPoE, обеспечивая надежный доступ к Интернету и другим сетевым ресурсам.

Сценарии использования

Протокол PPPoE используется в различных сценариях и сетевых средах. Вот несколько примеров его применения:

Домашние сети

PPPoE часто используется в домашних сетях для подключения к Интернету через DSL (Digital Subscriber Line), где сигнал передается по телефонной линии, или через другие технологии, такие как Ethernet.

Корпоративные сети

В корпоративных сетях PPPoE может быть использован для управления доступом сотрудников к корпоративному интернету или внутренним ресурсам, обеспечивая аутентификацию и контроль доступа.

Провайдеры услуг Интернета

ISP (Internet service provider) используют PPPoE для управления и предоставления доступа к интернет-соединениям своим клиентам. Он позволяет провайдерам контролировать и отслеживать подключения, а также предоставлять услуги аутентификации и маршрутизации.

Общественные сети доступа к Интернету

В общественных местах, таких как кафе, аэропорты или гостиницы, PPPoE может быть использован для предоставления доступа к сети Интернет через общедоступные точки доступа Wi-Fi или проводные сети.

Индустриальные и специализированные сети

PPPoE может использоваться в различных промышленных и специализированных сетях, где требуется управление доступом, аутентификация пользователей и обмен данными посредством Ethernet.

Таким образом, PPPoE широко применяется в различных сетевых средах, где необходимо управление доступом, безопасность и эффективная передача данных через Ethernet.

2.2.10.2 Настройка

Пример настройки

Пример настройки PPPoE соединения между провайдером и устройством на базе **ПО Факел**.

Параметры для настройки PPPoE:

- Сетевой интерфейс вашего устройства на базе **ПО Факел** подключен к сетевому оборудованию провайдера.
- Для связи с провайдером не требуется настройка VLAN для сетевого интерфейса устройства на базе **ПО Факел** .
- Для настройки необходимо получить учетные данные PPPoE от вашего DSL провайдера.
- Максимальный размер MTU, который можно использовать в DSL, составляет 1492 байта. Если вы переходите от провайдера, использующего DHCP, например, кабельного, то имейте в виду, что для работы в рамках этого ограничения может потребоваться корректировка размера MTU, например, для VPN-каналов.
- Если для параметра `default-route` установлено значение `auto`, то **ПО Факел** добавит в таблицу маршрутизации шлюз по умолчанию, полученный от DSL-провайдера только в том случае, если у вас нет других WAN подключений. Если вы хотите использовать двойное WAN соединение, измените значение параметра `default-route` на `force`. Можно также установить статический интерфейс маршрут и задать для параметра `default-route` значение `none`.
- Если опция `name-server` установлена в значение `none`, то **ПО Факел** будет игнорировать серверы имен, которые присылает вам провайдер, и будет использовать те, которые вы настроили статически.

Список команд для настройки протокола PPPoE:

```
set interfaces pppoe pppoe0 default-route 'auto'
set interfaces pppoe pppoe0 mtu 1492
set interfaces pppoe pppoe0 authentication user 'userid'
set interfaces pppoe pppoe0 authentication password 'secret'
set interfaces pppoe pppoe0 source-interface 'eth0'
```

В приведенную выше конфигурацию также следует добавить настройку межсетевого экрана для работы на интерфейсе PPPoE. Для этого нужно назначить политики межсетевого экрана для всех направлений

трафика на интерфейс pppoe0.

Список команд для настройки работы межсетевого экрана на интерфейсе PPPoE:

```
set interfaces pppoe pppoe0 firewall in name NET-IN
set interfaces pppoe pppoe0 firewall local name NET-LOCAL
set interfaces pppoe pppoe0 firewall out name NET-OUT
```

Примечание

Политики межсетевого экрана настраиваются индивидуально, в зависимости от типа трафика, который присутствует в вашей сети. Подробное описание настройки правил межсетевого экрана представлено в разделе *Межсетевой экран* (страница 416).

PPPoE соединение через VLAN интерфейс

Некоторые современные провайдеры требуют построения PPPoE соединения через VLAN интерфейс. Операционная система может легко создать PPPoE сессию через VLAN-интерфейс. В следующей конфигурации PPPoE-соединение будет осуществляться через VLAN7.

Список команд для настройки построения PPPoE соединение через VLAN интерфейс:

```
set interfaces pppoe pppoe0 default-route 'auto'
set interfaces pppoe pppoe0 mtu 1492
set interfaces pppoe pppoe0 authentication user 'userid'
set interfaces pppoe pppoe0 authentication password 'secret'
set interfaces pppoe pppoe0 source-interface 'eth0.7'
```

2.2.10.3 Список команд

Основные настройки

- `set interfaces pppoe <interface> description <description>`

  Задает псевдоним <description> для сетевого интерфейса <interface>. Например псевдоним может использоваться командой show interfaces или средствами мониторинга на базе SNMP.

- `set interfaces pppoe <interface> disable`

  Отключает сетевой интерфейс <interface>. После отключения интерфейс будет переведен в состояние административного отключения (A/D).

- `set interfaces pppoe <interface> vrf <vrf>`

  Размещает сетевой интерфейс <interface> в указанном экземпляре VRF <vrf>.

Настройка параметров PPPoE

- `set interfaces pppoe <interface> access-concentrator <name>`

  Определяет сервер доступа <name> для PPPoE соединения через сетевой интерфейс <interface>.

- `set interfaces pppoe <interface> authentication user <username>`

Устанавливает имя пользователя для аутентификации с удаленной конечной точкой для PPPoE соединения через сетевой интерфейс <interface>.

- `set interfaces pppoe <interface> authentication password <password>`

  Устанавливает пароль для аутентификации с удаленной конечной точкой для PPPoE соединения через сетевой интерфейс <interface>.

- `set interfaces pppoe <interface> connect-on-demand`

  Активирует режим `dial-on-demand` для PPPoE интерфейса <interface>.

- `set interfaces pppoe <interface> default-route [auto | force | none]`

  Определяет значение параметра `default-route`, который отвечает за автоматическое добавление маршрута по умолчанию для PPPoE интерфейса <interface>.

  - `default`: Маршрут по умолчанию к удаленной конечной точке добавляется автоматически при появлении соединения.
  - `auto`: Маршрут по умолчанию добавляется, если в системе не существует другого маршрута по умолчанию (из любого источника).
  - `force`: Маршрут по умолчанию добавляется после удаления всех существующих маршрутов по умолчанию.
  - `none`: Маршрут по умолчанию не устанавливается.

Примечание

Маршрут по умолчанию добавляется только в том случае, если в системе не существует другого маршрута по умолчанию.

- `set interfaces pppoe <interface> mru <mru>`

  Устанавливает размер MRU <mru> для PPPoE интерфейса <interface>. Значение MRU должно находиться в диапазоне от 128 до 16384. По умолчанию используется значение 1492 байта.

- `set interfaces pppoe <interface> idle-timeout <time>`

  Устанавливает интервал ожидания <time> для PPPoE интерфейса <interface>. При установке соединения по запросу канал активируется только при отправке трафика и отключается, если канал простаивает в течение указанного интервала.

  Если этот параметр не задан или равен 0, то соединение по запросу будет оставаться включенным всегда.

- `set interfaces pppoe <interface> local-address <address>`

  Задает адрес локального устройства <address> для сеанса PPPoE через PPPoE интерфейс <interface>. Если адрес локального устройства не задан, то он будет согласован в процессе инициализации PPPoE сессии.

- `set interfaces pppoe <interface> mtu <mtu>`

  Устанавливает размер MTU для PPPoE интерфейса <interface>.

- `set interfaces pppoe <interface> no-peer-dns`

Отключает использование внешних DNS серверов. При активации данного параметра используется только локальный DNS сервер.

- `set interfaces pppoe <interface> remote-address <address>`

  Устанавливает адрес удаленного устройства <address> для сеанса PPPoE через PPPoE интерфейс <interface>. Если адрес удаленного устройства не задан, то он будет согласован в процессе инициализации PPPoE сессии.

- `set interfaces pppoe <interface> service-name <name>`

  Задает имя сервиса <name>, по которому локальный интерфейс PPPoE может выбирать сервера доступа для подключения.

- `set interfaces pppoe <interface> source-interface <source-interface>`

  Определяет физический интерфейс <source-interface> для привязки PPPoE соединения к этому физическому интерфейсу. Каждое PPPoE соединение должно быть установлено через физический интерфейс.

Мониторинг и эксплуатация

- `show interfaces pppoe <interface>`

  Выводит на экран подробную информацию об указанном интерфейсе PPPoE <interface>.

  Пример работы команды show interfaces pppoe <interface>:

```
fakel@fakel:~$ show interfaces pppoe pppoe0
pppoe0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1492 qdisc pfifo_fast state
  UNKNOWN group default qlen 3
    link/ppp
    inet 192.0.2.1 peer 192.0.2.255/32 scope global pppoe0
    valid_lft forever preferred_lft forever

    RX:  bytes    packets     errors    dropped    overrun      mcast
    7002658233    5064967          0          0          0          0
    TX:  bytes    packets     errors    dropped    carrier collisions
    533822843    1620173          0          0          0          0
```

- `show interfaces pppoe <interface> queue`

  Выводит на экран информацию об очередях для указанного интерфейса PPPoE <interface>.

  Пример работы команды show interfaces pppoe <interface> queue:

```
fakel@fakel:~$ show interfaces pppoe pppoe0 queue
qdisc pfifo_fast 0: root refcnt 2 bands 3 priomap  1 2 2 2 1 2 0 0 1 1 1 1 1 1 1 1
Sent 534625359 bytes 1626761 pkt (dropped 62, overlimits 0 requeues 0)
backlog 0b 0p requeues 0
```

- `disconnect interface <interface>`

  Отключает указанный интерфейс PPPoE <interface>.

- `connect interface <interface>`

  Включает указанный интерфейс PPPoE `<interface>`.

2.2.11 VTI интерфейс

VTI (Virtual Tunnel Interface) - это виртуальный интерфейс туннеля, который используется для установки виртуальных частных сетей VPN (virtual private network) на основе IPsec (Internet Protocol Security). Он обеспечивает абстракцию уровня интерфейса для настройки и управления IPsec-туннелями между устройствами.

VTI интерфейсы позволяют передавать зашифрованный трафик между сетевыми устройствами через общедоступные или ненадежные сети, обеспечивая тем самым конфиденциальность, целостность и аутентификацию данных. Они также облегчают настройку и управление IPsec-туннелями, предоставляя единый интерфейс для управления VPN соединениями.

В целом, VTI туннели работают почти так же как туннели IPIP или SIT. Исключением является то, что они задействуют `fwmark` и формирование/разбор данных IPsec.

Предупреждение

При настройке Site-to Site IPsec туннеля с использованием VTI интерфейсов, обязательно отключите автоматическую установку маршрута.

```
set vpn ipsec options disable-route-autoinstall
```

2.2.11.1 Список команд

Основные настройки

- `set interfaces vti <interface> address <address>`

  Задает адрес `<address>` для сетевого интерфейса `<interface>`. .. Адрес может быть указан несколько раз как IPv4 и/или IPv6 адрес, например, 192.0.2.1/24 и/или 2001:db8::1/64

- `set interfaces vti <interface> description <text>`

  Задает псевдоним `<description>` для сетевого интерфейса `<interface>`. Например псевдоним может использоваться командой show interfaces или средствами мониторинга на базе SNMP.

- `set interfaces vti <interface> disable`

  Отключает сетевой интерфейс `<interface>`. После отключения интерфейс будет переведен в состояние административного отключения (A/D).

- `set interfaces vti <interface> mtu <68-9000>`

  Устанавливает размер MTU `<mtu>` для сетевого интерфейса `<interface>`.

- `set interfaces vti <interface> redirect <text>`

  Устанавливает интерфейс `<text>` для пересылки входящих на VTI интерфейс `<interface>` пакетов.

2.3 Маршрутизация

В **ПО Факел** маршрутизация обеспечивается следующими механизмами:

- *Статические маршруты* (страница 287)
- *OSPF* (страница 291)
- *IS-IS* (страница 333)
- *RIP* (страница 339)
- *Групповая рассылка* (страница 344)
- *MPLS* (страница 358)
- *Политика маршрутизации* (страница 353)
- *Виртуальная маршрутизация* (страница 363)

2.3.1 Статические маршруты

2.3.1.1 Описание

Статические маршруты представляет собой маршруты, заданные вручную, которые по большей части не обновляются автоматически на основании информации о топологии сети, полученной **ПО Факел** по результатам работы других протоколов маршрутизации. Однако если в канале возникает сбой, система удалит соответствующие маршруты, включая статические маршруты из таблицы RIB (Routing Information Base), которые используются данным интерфейсом для обеспечения достижимости следующего узла. В основном статические маршруты используются для обеспечения связности в относительно простых топологиях сети или для того, чтобы переопределить результаты работы протоколов динамической маршрутизации при небольшом количестве маршрутов. Список всех маршрутов, вне зависимости от того, заданы ли они вручную или определены динамически в результате работы протоколов динамической маршрутизации, хранится в таблице RIB. Одноадресные (unicast) маршруты используются непосредственно для определения содержимого таблицы FIB (Forwarding Information Base), используемой при принятии решения о перенаправлении одноадресных (unicast) пакетов.

2.3.1.2 Список команд

Основные настройки

- `set protocols static route <subnet> next-hop <address>`

  Создает статический маршрут IPv4 до подсети `<subnet>`, которая доступна через узел с адресом `<address>`.

- `set protocols static route <subnet> next-hop <address> disable`

  Выключает активный статический маршрут IPv4 до подсети `<subnet>`, которая доступна через узел с адресом `<address>`.

- `set protocols static route <subnet> next-hop <address> distance <distance>`

  Задает административную дистанцию `<distance>` для статического маршрута IPv4 до подсети `<subnet>`, которая доступна через узел с адресом `<address>`.

- `set protocols static route6 <subnet> next-hop <address>`

  Создает статический маршрут IPv6 до подсети `<subnet>`, которая доступна через узел с адресом `<address>`.

- `set protocols static route6 <subnet> next-hop <address> disable`

  Выключает активный статический маршрут IPv6 до подсети `<subnet>`, которая доступна через узел с адресом `<address>`.

- `set protocols static route6 <subnet> next-hop <address> distance <distance>`

  Задает административную дистанцию `<distance>` для статического маршрута IPv6 до подсети `<subnet>`, которая доступна через узел с адресом `<address>`.

Примечание

Для маршрута можно задать административную дистанцию (1 - 255, по умолчанию - 1). Маршруты с наименьшей административной дистанцией обрабатываются в приоритете по отношению к маршрутам с наибольшей административной дистанцией. Маршруты с административной дистанцией 255 фактический определяются **ПО Факел** как отключенные и не устанавливаются в ядро.

Настройка маршрутов на основе интерфейсов

- `set protocols static interface-route <subnet> next-hop-interface <interface>`

  Создает статический маршрут IPv4 на основе интерфейса до подсети <subnet>, которая доступна через интерфейс с именем <interface>.

- `set protocols static interface-route <subnet> next-hop-interface <interface> disable`

  Выключает активный статический маршрут IPv4 на основе интерфейса до подсети <subnet>, которая доступна через интерфейс с именем <interface>.

- `set protocols static interface-route <subnet> next-hop-interface <interface> distance <distance>`

  Задает административную дистанцию <distance> для статического маршрута IPv4 на основе интерфейса до подсети <subnet>, которая доступна через интерфейс с именем <interface>.

- `set protocols static interface-route6 <subnet> next-hop-interface <interface>`

  Создает статический маршрут IPv6 на основе интерфейса до подсети <subnet>, которая доступна через интерфейс с именем <interface>.

- `set protocols static interface-route6 <subnet> next-hop-interface <interface> disable`

  Выключает активный статический маршрут IPv6 на основе интерфейса до подсети <subnet>, которая доступна через интерфейс с именем <interface>.

- `set protocols static interface-route6 <subnet> next-hop-interface <interface> distance <distance>`

  Задает административную дистанцию <distance> для статического маршрута IPv6 на основе интерфейса до подсети <subnet>, которая доступна через интерфейс с именем <interface>.

Примечание

Для маршрута можно задать административную дистанцию (1 - 255, по умолчанию - 1). Маршруты с наименьшей административной дистанцией обрабатываются в приоритете по отношению к маршрутам с наибольшей административной дистанцией. Маршруты с административной дистанцией 255 фактический определяются **ПО Факел** как отключенные и не устанавливаются в ядро.

Настройка тупиковых маршрутов

Примечание

Тупиковые (black hole) маршруты используются **ПО Факел** для отбрасывания подошедших пакетов без каких-либо уведомлений об этом их отправителя. Использование тупиковых маршрутов предотвращает утечку данных о подсетях через внешние интерфейсы, но при этом не блокирует к ним доступ из локальной сети посредством точечных маршрутов.

- `set protocols static route <subnet> blackhole`

  Создает тупиковый (black hole) маршрут IPv4 до подсети <subnet>.

- `set protocols static route <subnet> blackhole distance <distance>`

  Задает административную дистанцию `<distance>` для тупикового (black hole) маршрута IPv4 до подсети `<subnet>`.

- `set protocols static route6 <subnet> blackhole`

  Создает тупиковый (black hole) маршрут IPv6 до подсети `<subnet>`.

- `set protocols static route6 <subnet> blackhole distance <distance>`

  Задает административную дистанцию `<distance>` для тупикового (black hole) маршрута IPv6 до подсети `<subnet>`.

Примечание

Для маршрута можно задать административную дистанцию (1 - 255, по умолчанию - 1). Маршруты с наименьшей административной дистанцией обрабатываются в приоритете по отношению к маршрутам с наибольшей административной дистанцией. Маршруты с административной дистанцией 255 фактический определяются **ПО Факел** как отключенные и не устанавливаются в ядро.

2.3.2 Динамическая маршрутизация

В **ПО Факел** динамическая маршрутизация обеспечивается следующими протоколами:

2.3.2.1 OSPF

Описание

Протокол OSPF (Open Shortest Path First) является протоколом с контролем состояния соединения из категории IGP (Interior Gateway Protocol) протоколов для маршрутизации внутри локальной сети, оперирующий внутри отдельной автономной системы. В настоящий момент в спецификации **RFC 2328**[5] определен протокол OSPF версии 2 (OSPFv2) для работы в сетях на базе протокола IPv4, а в спецификации **RFC 5340**[6] - протокол OSPF версии 3 (OSPFv3) для работы в сетях на базе протокола IPv6. Протокол OSPF поддерживает использование модели адресации CIDR (Classless Inter-Domain Routing).

- *OSPFv2* (страница 292)
- *OSPFv3* (страница 305)

[5] https://datatracker.ietf.org/doc/html/rfc2328.html
[6] https://datatracker.ietf.org/doc/html/rfc5340.html

OSPFv2

Описание

OSPFv2 - протокол контроля состояния соединений, который широко применяется в сетях. Как и в любом другом протокол контроля состояния соединений, маршрутизаторы в OSPFv2 строят топологию всей сети вообще. Каждый маршрутизатор хранит копию базы знаний по топологии всей сети и запускает свой собственный алгоритм поиска кратчайшего пути по этой базе. База носит название Link State Database или LSDB. Представляет она из себя описание состояния каналов сети. Протокол OSPFv2 работает поверх протокола IPv4.

Настройка

Пример настройки

Пример типичной настройки с использованием двух узлов, перераспределением loopback-адреса и отправкой узлом 1 маршрута по умолчанию:

Список команд для настройки первого узла:

```
set interfaces loopback lo address 10.1.1.1/32
set protocols ospf area 0 network 192.168.0.0/24
set protocols ospf default-information originate always
set protocols ospf default-information originate metric 10
set protocols ospf default-information originate metric-type 2
set protocols ospf log-adjacency-changes
set protocols ospf parameters router-id 10.1.1.1
set protocols ospf redistribute connected metric-type 2
set protocols ospf redistribute connected route-map CONNECT
set policy route-map CONNECT rule 10 action permit
set policy route-map CONNECT rule 10 match interface lo
```

Список команд для настройки второго узла:

```
set interfaces loopback lo address 10.2.2.2/32
set protocols ospf area 0 network 192.168.0.0/24
set protocols ospf log-adjacency-changes
set protocols ospf parameters router-id 10.2.2.2
set protocols ospf redistribute connected metric-type 2
set protocols ospf redistribute connected route-map CONNECT
set policy route-map CONNECT rule 10 action permit
set policy route-map CONNECT rule 10 match interface lo
```

Список команд

Основные настройки

ПО Факел не располагает специальной командой для запуска процесса OSPF. Процесс запускается автоматически при настройке протокола OSPF на интерфейсах.

- `set protocols ospf area <number> network <x.x.x.x/x>`

  Активирует протокол OSPF на определенном интерфейсе в случае, если его адрес находится в указанном диапазоне адресов `<x.x.x.x/x>`, после чего маршрутизатор может обмениваться информацией о топологии сети с другими устройствами, которые также являются участниками OSPF процесса и доступны через этот интерфейс. Номер области `<number>` может быть указан целым числом в диапазоне от 0 до 4294967295 или числом с точкой в формате, похожем на IP адрес.

- `set protocols ospf auto-cost reference-bandwidth <number>`

  Задает значение полосы пропускания `<number>` в Мбит/сек для расчета веса каналов. Полоса пропускания указывается числом в диапазоне от 1 до 4294967. Значение полосы пропускания по умолчанию - 100, что соответствует весу 1. Значения меньше 100 будут также соответствовать весу 1 путем округления.

- `set protocols ospf parameters router-id <rid>`

  Задает идентификатор маршрутизатора `<rid>` для процесса OSPF. В качестве идентификатора может быть указан IP адрес или произвольным 32-разрядным числом, но идентификатор должен быть указан обязательно. Вместе с тем идентификатор для данного маршрутизатора должен быть уникальным в рамках всего OSPF домена. В противном случае возможно возникновение ошибок в работе процесса OSPF.

Дополнительные настройки

- `set protocols ospf default-information originate [always] [metric <number>] [metric-type <1|2>] [route-map <name>]`

  Распространяет сообщение *AS-External* (`type-5`), содержащее маршрут по умолчанию, во все внешние маршрутизируемые области с указанием определенного значения и типа метрики. Если указан параметр `always`, сообщение распространяется всегда, даже если маршрут по умолчанию отсутствует в таблице маршрутизации. Параметр `route-map` позволяет указать карту маршрутов, при совпадении с которой будет распространяться сообщение с маршрутом по умолчанию.

- `set protocols ospf distance global <distance>`

  Изменяет значение административной дистанции глобально для всего процесса OSPF в диапазоне от 1 до 255.

- `set protocols ospf distance ospf <external|inter-area|intra-area> <distance>`

  Изменяет значение административной дистанции для определенных маршрутов: внешних маршрутов (`external`), маршрутов между областями (`inter-area`), маршрутов внутри области (`intra-area`). Значение административной дистанции задается в диапазоне от 1 до 255.

Примечание

Routes with a distance of 255 are effectively disabled and not installed into the kernel.

- `set protocols ospf log-adjacency-changes [detail]`

  Регистрирует изменения в состоянии смежности. С дополнительным аргументом `detail` отображаются все изменения в состоянии смежности. Без аргумента `detail` показываются только изменения в полную или регрессию.

- `set protocols ospf max-metric router-lsa <administrative|on-shutdown <seconds>|on-startup <seconds>>`

  Включает поддержку **RFC 3137**[7], когда процесс OSPF описывает свои транзитные каналы в своем LSA как имеющие бесконечное расстояние, чтобы другие маршрутизаторы не вычисляли транзитные пути через маршрутизатор, сохраняя при этом возможность доступа к сетям через маршрутизатор. Эта поддержка может быть включена административно (и неограниченно) с помощью команды `administrative`. Она также может быть включена условно. Условное включение max-metric router-lsas может осуществляться на период в несколько секунд после запуска с помощью команды `on-startup <seconds>` и/или на период в несколько секунд до выключения с помощью команды `on-shutdown <seconds>`. Диапазон времени составляет от 5 до 86400.

- `set protocols ospf parameters abr-type <cisco|ibm|shortcut|standard>`

  Определяет модель ABR. Маршрутизатор OSPF поддерживает четыре модели ABR:

  - `cisco` – маршрутизатор будет считаться ABR, если он имеет несколько настроенных связей с сетями в разных областях, одна из которых является магистральной. Причем связь с магистральной областью должна быть активной (рабочей).
  - `ibm` – идентична модели «cisco», но в этом случае канал магистральной зоны может быть не активен.
  - `standard` – маршрутизатор имеет несколько активных связей с различными областями.
  - `shortcut` – идентична «стандартной», но в этой модели маршрутизатору разрешено использовать топологию связанных областей без привлечения магистральной области для межобластных соединений.

Примечание

Подробную информацию о различиях моделей `cisco` и `ibm` можно найти в **RFC 3509**[8]. Модель `shortcut` позволяет ABR создавать маршруты между областями, основываясь на топологии областей, подключенных к данному маршрутизатору, но не используя магистральную область в случае, если не магистральный маршрут будет дешевле. Более подробная информация о модели `shortcut` приведена в файле ospf-shortcut-abr-02.txt.

- `set protocols ospf parameters rfc1583-compatibility`

  Включает поддержку **RFC 1583**[9].

- `set protocols ospf passive-interface <interface>`

  Определяет интерфейс `<interface>` как пассивный. Пассивный интерфейс рекламирует свой адрес, но не выполняет протокол OSPF (смежности не формируются и пакеты hello не генерируются).

- `set protocols ospf passive-interface default`

  Определяет все интерфейсы как пассивные по умолчанию. Поскольку данная команда изменяет логику конфигурации на пассивную по умолчанию, поэтому интерфейсы, на которых

[7] https://datatracker.ietf.org/doc/html/rfc3137.html
[8] https://datatracker.ietf.org/doc/html/rfc3509.html
[9] https://datatracker.ietf.org/doc/html/rfc1583.html

ожидается наличие смежных маршрутизаторов, должны быть настроены с помощью команды `passive-interface-exclude`.

- `set protocols ospf passive-interface-exclude <interface>`

  Исключает интерфейс из пассивного состояния. Данная команда используется, если была настроена команда `passive-interface default`.

- `set protocols ospf refresh timers <seconds>`

  Маршрутизатор автоматически обновляет информацию о состоянии связей со своими соседями. Обновляется только та устаревшая информация, возраст которой превысил определенный порог. Данный параметр изменяет пороговое значение, которое по умолчанию составляет 1800 секунд (полчаса). Значение применяется ко всему маршрутизатору OSPF. Диапазон значений таймера составляет от 10 до 1800.

- `set protocols ospf timers throttle spf <delay|initial-holdtime|max-holdtime> <seconds>`

  Задает начальную задержку, начальное время задержки и максимальное время задержки между моментом расчета SPF и событием, вызвавшим расчет. Время задается в миллисекундах и должно находиться в диапазоне от 0 до 600000 миллисекунд. `delay` задает начальную задержку расписания SPF в миллисекундах. Значение по умолчанию равно 200 мс. `initial-holdtime` задает минимальное время удержания между двумя последовательными вычислениями SPF. Значение по умолчанию равно 1000 мс. `max-holdtime` задает максимальное время ожидания между двумя последовательными SPF-расчетами. Значение по умолчанию равно 10000 мс.

Настройки областей

- `set protocols ospf area <number> area-type stub`

  Определяет область <number> как Stub Area. То есть область, в которой ни один маршрутизатор не прокладывает внешние для OSPF маршруты, и, следовательно, все внешние маршруты проходят через ABR. Следовательно, ABR для такой области не нужно передавать в нее AS-External LSAs (тип-5) или ASBR-Summary LSAs (тип-4). Они должны передавать в такую область только Network-Summary (тип-3) LSA вместе с резюме маршрута по умолчанию.

- `set protocols ospf area <number> area-type stub no-summary`

  Определяет область как Totally Stub Area. В дополнение к ограничениям области stub этот тип области не позволяет ABR инжектировать Network-Summary (тип-3) LSA в указанную область stub. Разрешен только суммарный маршрут по умолчанию.

- `set protocols ospf area <number> area-type stub default-cost <number>`

  Устанавливает стоимость LSA по умолчанию, анонсируемых в stubby-областях. Диапазон стоимости составляет от 0 до 16777215.

- `set protocols ospf area <number> area-type nssa`

  Определяет область как Not So Stubby Area. Информация о внешней маршрутизации импортируется в NSSA в виде LSA типа 7. LSA типа 7 аналогичны LSA типа 5 AS-external, за исключением того, что они могут быть переданы только в NSSA. Для дальнейшего распространения внешней информации NSSA LSA Type-7 должен быть транслирован в Type-5 AS-external-LSA на NSSA ABR.

- `set protocols ospf area <number> area-type nssa no-summary`

  Определяет область как NSSA Totally Stub Area. ABR для такой области не должны передавать в

нее LSA Network-Summary (тип-3) (кроме суммарного маршрута по умолчанию), ASBR-Summary LSA (тип-4) и AS-External LSA (тип-5). Однако LSA типа-7, преобразованные в тип-5 на ABR NSSA, разрешены.

- `set protocols ospf area <number> area-type nssa default-cost <number>`

  Устанавливает стоимость по умолчанию для LSA, анонсируемых в области NSSA. Диапазон стоимости составляет от 0 до 16777215.

- `set protocols ospf area <number> area-type nssa translate <always|candidate|never>`

  Указывает, будет ли данный пограничный маршрутизатор NSSA безусловно транслировать LSA типа 7 в LSA типа 5. Если роль - Always, LSA типа 7 транслируются в LSA типа 5 независимо от состояния транслятора других пограничных маршрутизаторов NSSA. Если роль - Candidate, то этот маршрутизатор участвует в выборах транслятора, чтобы определить, будет ли он выполнять обязанности транслятора. Когда роль равна Never, этот маршрутизатор никогда не будет транслировать LSA типа 7 в LSA типа 5.

- `set protocols ospf area <number> authentication plaintext-password`

  Определяет, что для данной области должна использоваться аутентификация с помощью простого пароля. Пароль также должен быть настроен для каждого интерфейса.

- `set protocols ospf area <number> authentication md5`

  Указывает, что пакеты OSPF должны осуществлять аутентификацию с помощью MD5 HMAC в пределах заданной области. Ключевой материал также должен быть сконфигурирован на основе каждого интерфейса.

- `set protocols ospf area <number> range <A.B.C.D/M> [cost <number>]`

  Суммирует пути из указанной зоны в один summary-LSA (Type-3), анонсированный в другие зоны. Эта команда может быть использована только в ABR, и суммировать можно ТОЛЬКО маршрутные-LSA (тип-1) и сетевые-LSA (тип-2) (т.е. LSA с областью действия). AS-external-LSA (Type-5) не могут быть суммированы - их область видимости - AS. Необязательный аргумент `cost` задает метрику агрегированного соединения. Диапазон значений метрики - от 0 до 16777215.

- `set protocols ospf area <number> range <A.B.C.D/M> not-advertise`

  Фильтрует внутриобластные пути - т.е. внутриобластные пути из этого диапазона не рекламируются в другие области. Эта команда имеет смысл только в ABR.

- `set protocols ospf area <number> range <A.B.C.D/M> substitute <E.F.G.H/M>`

  Анонсирует в магистральную область один summary-LSA типа 3 с информацией о маршрутизации <E.F.G.H/M> , если определенная область содержит хотя бы одну внутриобластную сеть (т.е. описанную с помощью router-LSA или network-LSA) из диапазона <A.B.C.D/M>. Данная команда имеет смысл только в ABR.

- `set protocols ospf area <number> shortcut <default|disable|enable>`

  Сокращает маршруты (не магистральные) для межрайонных маршрутов. Для сокращения маршрутов существует три режима:

  - `default` – эта область будет использоваться для короткого замыкания только в том случае, если ABR не имеет связи с магистральной областью или эта связь была потеряна..
  - `enable` – область будет использоваться для сокращения пути каждый раз, когда проходящий через нее маршрут будет дешевле.

- `disable` – эта область никогда не используется ABR для сокращения маршрутов.

- `set protocols ospf area <number> virtual-link <A.B.C.D>`

  Обеспечивает когерентность магистральной области за счет создания виртуальных каналов связи.

  В общем случае протокол OSPF требует, чтобы магистральная область (область 0) была целостной и полностью связанной. Т.е. любой маршрутизатор магистральной области должен иметь маршрут к любому другому маршрутизатору магистральной области. Более того, каждый ABR должен иметь связь с магистральной областью. Однако не всегда возможно иметь физическую связь с магистральной областью. В этом случае между двумя ABR (один из которых имеет связь с магистральной областью) в области (не stub area) организуется виртуальная связь.

  - `<number>` – идентификатор области, через которую проходит виртуальный канал связи.
  - `<A.B.C.D>` – ABR router-id, с которым устанавливается виртуальная связь. Виртуальная связь должна быть настроена на обоих маршрутизаторах.

  Формально виртуальный канал выглядит как сеть «точка-точка», соединяющая два ABR из одной области, один из которых физически подключен к магистральной области. Эта виртуальная сеть считается принадлежащей магистральной области.

Настройки интерфейсов

- `set interfaces <inttype> <interface> ip ospf authentication plaintext-password <text>`

  Устанавливает ключ аутентификации OSPF в виде простого пароля. После установки все пакеты OSPF будут аутентифицированы. Длина ключа может составлять до 8 символов.

  Аутентификация с помощью простого текстового пароля небезопасна и отменена в пользу аутентификации с помощью MD5 HMAC.

- `set interfaces <inttype> <interface> ip ospf authentication md5 key-id <id> md5-key <text>`

  Указывает, что на данном интерфейсе должна использоваться аутентификация MD5 HMAC. Она устанавливает ключ аутентификации OSPF в виде криптографического пароля. Key-id определяет секретный ключ, используемый для создания дайджеста сообщения. Этот идентификатор является частью протокола и должен быть одинаковым для всех маршрутизаторов на линии. Ключ может иметь длину до 16 символов (более длинные строки будут усечены) и ассоциируется с заданным key-id.

- `set interfaces <inttype> <interface> ip ospf bandwidth <number>`

  Задает пропускную способность интерфейса для расчета стоимости, где пропускная способность может быть в диапазоне от 1 до 100000, указана в Мбит/с.

- `set interfaces <inttype> <interface> ip ospf cost <number>`

  Устанавливает стоимость соединения для указанного интерфейса. Значение стоимости устанавливается в поле метрики маршрутизатора-LSA и используется для расчета SPF. Диапазон значений стоимости составляет от 1 до 65535.

- `set interfaces <inttype> <interface> ip ospf dead-interval <number>`

  Задает количество секунд для значения таймера Dead Interval маршрутизатора, используемого

для таймера ожидания и таймера бездействия. Это значение должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети. Значение по умолчанию составляет 40 секунд. Диапазон интервалов составляет от 1 до 65535.

- `set interfaces <inttype> <interface> ip ospf hello-interval <number>`

  Устанавливает количество секунд для значения таймера Hello Interval. При установке этого значения пакет Hello будет отправляться на указанный интерфейс каждые несколько секунд по таймеру. Это значение должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети. Значение по умолчанию составляет 10 секунд. Диапазон значений интервала составляет от 1 до 65535.

- `set interfaces <inttype> <interface> ip ospf mtu-ignore`

  Отключает проверку значения MTU в пакетах OSPF DBD. Таким образом, использование этой команды позволяет OSPF-связке достичь состояния FULL, даже если между двумя OSPF-маршрутизаторами имеется несоответствие MTU интерфейса.

- `set interfaces <inttype> <interface> ip ospf network <type>`

  Указывает тип распределения для сети, подключенной к данному интерфейсу:

  - `broadcast` – распределение широковещательных IP-адресов.
  - `non-broadcast` – распределение адресов в топологии сетей NBMA.
  - `point-to-multipoint` – распределение адресов в сетях «точка-многоточечное соединение.
  - `point-to-point` – распределение адресов в сетях «точка-точка.

- `set interfaces <inttype> <interface> ip ospf priority <number>`

  Устанавливает целочисленное значение Router Priority. Маршрутизатор с наивысшим приоритетом будет иметь больше шансов стать назначенным маршрутизатором. Если установить значение 0, то маршрутизатор не будет иметь права стать назначенным маршрутизатором. Значение по умолчанию равно 1. Диапазон интервалов от 0 до 255.

- `set interfaces <inttype> <interface> ip ospf retransmit-interval <number>`

  Задает количество секунд для значения таймера RxmtInterval. Это значение используется при повторной передаче пакетов Database Description и Link State Request, если подтверждение не было получено. Значение по умолчанию равно 5 секундам. Диапазон интервалов составляет от 3 до 65535.

- `set interfaces <inttype> <interface> ip ospf transmit-delay <number>`

  Задает количество секунд для значения InfTransDelay. Она позволяет установить и настроить для каждого интерфейса интервал задержки перед началом процесса синхронизации базы данных маршрутизатора со всеми соседями. Значение по умолчанию составляет 1 секунду. Диапазон значений интервала составляет от 3 до 65535.

Настройка соседства вручную

Обычно устройства маршрутизации OSPF обнаруживают своих соседей динамически, прослушивая широковещательные или многоадресные пакеты hello в сети. Поскольку сеть NBMA не поддерживает широковещание (или многоадресную рассылку), устройство не может обнаружить своих соседей динамически, поэтому все соседи должны быть настроены статически.

- `set protocols ospf neighbor <A.B.C.D>`

  Задает IP-адрес <A.B.C.D> соседнего устройства.

- `set protocols ospf neighbor <A.B.C.D> poll-interval <seconds>`

  Устанавливает продолжительность времени <seconds>, в течение которого устройство маршрутизации посылает пакеты hello с интерфейса до установления смежности с соседом. Диапазон значений составляет от 1 до 65535 секунд. Значение по умолчанию - 60 секунд.

- `set protocols ospf neighbor <A.B.C.D> priority <number>`

  Задает значение приоритета маршрутизатора для соседа, связанного с указанным IP-адресом. По умолчанию это значение равно 0. Это ключевое слово не применяется к интерфейсам типа «точка-многоточечное соединение».

Настройка редистрибуции

- `set protocols ospf redistribute <route source>`

  Перераспределяет информацию о маршрутизации из заданного источника маршрута в процесс OSPF. Для источника маршрута доступно пять режимов: bgp, connected, kernel, rip, static.

- `set protocols ospf default-metric <number>`

  Задает значение метрики по умолчанию для перераспределенных маршрутов. Диапазон значений метрики составляет от 0 до 16777214.

- `set protocols ospf redistribute <route source> metric <number>`

  Задает метрику для перераспределенных маршрутов из заданного источника маршрута. Для источника маршрута доступно пять режимов: bgp, connected, kernel, rip, static. Диапазон значений метрики составляет от 1 до 16777214.

- `set protocols ospf redistribute <route source> metric-type <1|2>`

  Задает тип метрики для перераспределенных маршрутов. Разница между двумя типами метрик заключается в том, что метрика типа 1 - это метрика, которая «соизмерима» с внутренними связями OSPF. При расчете метрики до внешнего пункта назначения полная метрика пути вычисляется как сумма метрик пути маршрутизатора, который рекламировал эту связь, плюс метрика связи. Таким образом, будет выбран маршрут с наименьшей суммарной метрикой. Если внешняя связь рекламируется с метрикой типа 2, то выбирается путь через маршрутизатор, рекламировавший эту связь с наименьшей метрикой, несмотря на то, что внутренний путь к этому маршрутизатору длиннее (с большей стоимостью). Однако если два маршрутизатора рекламируют внешнюю связь и с метрикой типа 2, то предпочтение отдается пути, проходящему через маршрутизатор с более коротким внутренним путем. Если два разных маршрутизатора рекламируют два канала к одному и тому же внешнему пункту назначения, но с разным типом метрики, то предпочтение отдается маршрутизатору с метрикой типа 1. Если тип метрики не определен, то маршрутизатор будет считать, что эти внешние ссылки по умолчанию имеют метрику типа 2.

- `set protocols ospf redistribute <route source> route-map <name>`

  Устанавливает route map <name> для фильтрации перераспределенных маршрутов из заданного источника маршрута. Для источника маршрута доступно пять режимов: bgp, connected, kernel, rip, static.

Мониторинг состояния

- `show ip ospf neighbor`

  Выводит информацию о состояние соседей.

  Пример работы команды show ip ospf neighbor:

```
fakel@fakel:~$ show ip ospf neighbor

Neighbor ID   Pri   State         Dead Time Address   Interface        RXmtL
  RqstL   DBsmL
10.0.13.1     1     Full/DR       38.365s 10.0.13.1   eth0:10.0.13.3   0       0
     0
10.0.23.2     1     Full/Backup   39.175s 10.0.23.2   eth1:10.0.23.3   0       0
     0
```

- `show ip ospf neighbor detail`

  Выводит информацию о соседях в подробном виде.

  Пример работы команды show ip ospf neighbor detail:

```
fakel@fakel:~$ show ip ospf neighbor detail

Neighbor 10.0.13.1, interface address 10.0.13.1
   In the area 0.0.0.0 via interface eth0
   Neighbor priority is 1, State is Full, 5 state changes
   Most recent state change statistics:
      Progressive change 11m55s ago
   DR is 10.0.13.1, BDR is 10.0.13.3
   Options 2 *|-|-|-|-|-|E|-
   Dead timer due in 34.854s
   Database Summary List 0
   Link State Request List 0
   Link State Retransmission List 0
   Thread Inactivity Timer on
   Thread Database Description Retransmision off
   Thread Link State Request Retransmission on
   Thread Link State Update Retransmission on

Neighbor 10.0.23.2, interface address 10.0.23.2
   In the area 0.0.0.1 via interface eth1
   Neighbor priority is 1, State is Full, 4 state changes
   Most recent state change statistics:
      Progressive change 41.193s ago
   DR is 10.0.23.3, BDR is 10.0.23.2
   Options 2 *|-|-|-|-|-|E|-
   Dead timer due in 35.661s
   Database Summary List 0
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
   Link State Request List 0
   Link State Retransmission List 0
   Thread Inactivity Timer on
   Thread Database Description Retransmision off
   Thread Link State Request Retransmission on
   Thread Link State Update Retransmission on
```

- `show ip ospf neighbor <A.B.C.D>`

  Выводит в подробном виде информацию для конкретного соседа `<A.B.C.D>`.

- `show ip ospf neighbor <interface>`

  Выводит в подробном виде информацию для соседа на указанном интерфейсе `<interface>`.

- `show ip ospf interface [<interface>]`

  Выводит информацию о состоянии и конфигурации OSPF указанного интерфейса `<interface>` или всех интерфейсов, если интерфейс не указан.

  Пример работы команды show ip ospf interface:

```
fakel@fakel:~$ show ip ospf interface

eth0 is up
   ifindex 2, MTU 1500 bytes, BW 4294967295 Mbit <UP,BROADCAST,RUNNING,MULTICAST>
   Internet Address 10.0.13.3/24, Broadcast 10.0.13.255, Area 0.0.0.0
   MTU mismatch detection: enabled
   Router ID 10.0.23.3, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State Backup, Priority 1
   Backup Designated Router (ID) 10.0.23.3, Interface Address 10.0.13.3
   Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
   Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
      Hello due in 4.470s
   Neighbor Count is 1, Adjacent neighbor count is 1
eth1 is up
   ifindex 3, MTU 1500 bytes, BW 4294967295 Mbit <UP,BROADCAST,RUNNING,MULTICAST>
   Internet Address 10.0.23.3/24, Broadcast 10.0.23.255, Area 0.0.0.1
   MTU mismatch detection: enabled
   Router ID 10.0.23.3, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State DR, Priority 1
   Backup Designated Router (ID) 10.0.23.2, Interface Address 10.0.23.2
   Saved Network-LSA sequence number 0x80000002
   Multicast group memberships: OSPFAllRouters OSPFDesignatedRouters
   Timer intervals configured, Hello 10s, Dead 40s, Wait 40s, Retransmit 5
      Hello due in 4.563s
   Neighbor Count is 1, Adjacent neighbor count is 1
```

- `show ip ospf route`

  Выводит таблицу маршрутизации OSPF, определенную по последнему расчету SPF.

Пример работы команды show ip ospf route:

```
fakel@fakel:~$ show ip ospf route

============ OSPF network routing table ============
N IA 10.0.12.0/24          [3] area: 0.0.0.0
                           via 10.0.13.3, eth0
N    10.0.13.0/24          [1] area: 0.0.0.0
                           directly attached to eth0
N IA 10.0.23.0/24          [2] area: 0.0.0.0
                           via 10.0.13.3, eth0
N    10.0.34.0/24          [2] area: 0.0.0.0
                           via 10.0.13.3, eth0
============ OSPF router routing table =============
R    10.0.23.3             [1] area: 0.0.0.0, ABR
                           via 10.0.13.3, eth0
R    10.0.34.4             [2] area: 0.0.0.0, ASBR
                           via 10.0.13.3, eth0
============ OSPF external routing table ===========
N E2 172.16.0.0/24         [2/20] tag: 0
                           via 10.0.13.3, eth0

Таблица состоит из следующих данных:

*  ``OSPF network routing table`` – содержит список полученных маршрутов для всех
  доступных сетей (или агрегированных диапазонов областей) системы OSPF. Флаг ”IA”
  означает, что пункт назначения маршрута находится в области, к которой
  маршрутизатор не подключен, т.е. это межобластной путь. В квадратных скобках
  указывается суммарная метрика для всех связей, через которые лежит путь к данной
  сети. Префикс ”via” определяет маршрутизатор-шлюз, т.е. первый маршрутизатор на
  пути к месту назначения (следующий хоп)

*  ``OSPF router routing table`` – включает список приобретенных маршрутов ко всем
  доступным ABR и ASBR.

*  ``OSPF external routing table`` – включает список приобретенных маршрутов,
  которые являются внешними по отношению к процессу OSPF. Флаг ”E” указывает на тип
  метрики внешнего соединения (E1 - метрика типа 1, E2 - метрика типа 2). Метрика
  внешнего канала выводится в формате ”<метрика маршрутизатора, рекламирующего
  канал>/<метрика канала>”..
```

- `show ip ospf border-routers`

  Выводит таблицу путей к маршрутизаторам границы области и границы автономной системы.

- `show ip ospf database`

  Выводит сводную таблицу с содержимым базы данных (LSA).

  Пример работы команды show ip ospf database:

```
fakel@fakel:~$ show ip ospf database

OSPF Router with ID (10.0.13.1)

                Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.0.13.1       10.0.13.1        984 0x80000005 0xd915 1
10.0.23.3       10.0.23.3       1186 0x80000008 0xfe62 2
10.0.34.4       10.0.34.4       1063 0x80000004 0x4e3f 1

                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.0.13.1       10.0.13.1        994 0x80000003 0x30bb
10.0.34.4       10.0.34.4       1188 0x80000001 0x9411

                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
10.0.12.0       10.0.23.3       1608 0x80000001 0x6ab6 10.0.12.0/24
10.0.23.0       10.0.23.3        981 0x80000003 0xe232 10.0.23.0/24

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route
172.16.0.0      10.0.34.4       1063 0x80000001 0xc40d E2 172.16.0.0/24 [0x0]
```

- `show ip ospf database <type> [A.B.C.D] [adv-router <A.B.C.D>|self-originate]`

  Выводит содержимое базы данных для определенного типа анонсируемых соединений.

  Тип может быть следующим: `asbr-summary`, `external`, `network`, `nssa-external`, `opaque-area`, `opaque-as`, `opaque-link`, `router`, `ummary`.

  Пример работы команды show ip ospf database <type> [A.B.C.D] [adv-router <A.B.C.D>|self-originate]:

```
fakel@fakel:~$ show ip ospf database summary 10.0.13.1

OSPF Router with ID (10.0.13.1)

   Router Link States (Area 0.0.0.0)

   LS age: 1213
   Options: 0x2  : *|-|-|-|-|-|E|-
   LS Flags: 0x3
   Flags: 0x0
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
  LS Type: router-LSA
  Link State ID: 10.0.13.1
  Advertising Router: 10.0.13.1
  LS Seq Number: 80000009
  Checksum: 0xd119
  Length: 36

  Number of Links: 1

  Link connected to: a Transit Network
  (Link ID) Designated Router address: 10.0.13.1
  (Link Data) Router Interface address: 10.0.13.1
  Number of TOS metrics: 0
  TOS 0 Metric: 1
```

- `show ip ospf database max-age`

  Выводит информацию об LSA в списке MaxAge.

OSPFv3

Описание

Для работы в сетях IPv6 разработан бесклассовый протокол маршрутизации по состоянию канала OSPFv3, большинство параметров которого аналогичны протоколу OSPFv2, работающему в сетях IPv4. Оба протокола работают на основе алгоритма SPF. При обмене маршрутной информацией рассылаются те же типы пакетов, что и в версии протокол OSPFv6. Рассылка маршрутной информации в OSPFv3 производится с использованием группового адреса FF02::5 или FF02::6 и маршрутизаторов DR и BDR. Кроме того, для рассылки внутри локального канала используются индивидуальные локальные адреса источника и назначения. OSPFv3 использует аутентификацию IPv6 по протоколу IPSec.

Настройка

Пример настройки

Пример типичной конфигурация OSPFv3 с использованием двух узлов.

Список команд для настройки первого узла:

```
set protocols ospfv3 area 0.0.0.0 interface eth1
set protocols ospfv3 area 0.0.0.0 range 2001:db8:1::/64
set protocols ospfv3 parameters router-id 192.168.1.1
set protocols ospfv3 redistribute connected
```

Список команд для настройки второго узла:

```
set protocols ospfv3 area 0.0.0.0 interface eth1
set protocols ospfv3 area 0.0.0.0 range 2001:db8:2::/64
set protocols ospfv3 parameters router-id 192.168.2.1
set protocols ospfv3 redistribute connected
```

Чтобы получить информацию о редистрибуции маршрутов, используйте команду `show ipv6 ospfv3 redistribute`.

Примечание

Чтобы перераспределить маршруты IPv6 через OSPFv3 на канале интерфейса WireGuard, настройте вручную адреса link-local на интерфейсах WireGuard

Пример настройки OSPFv3 для интерфейсов WireGuard

Список команд для настройки первого узла:

```
set interfaces wireguard wg01 address 'fe80::216:3eff:fe51:fd8c/64'
set interfaces wireguard wg01 address '192.168.0.1/24'
set interfaces wireguard wg01 peer ospf02 allowed-ips '::/0'
set interfaces wireguard wg01 peer ospf02 allowed-ips '0.0.0.0/0'
set interfaces wireguard wg01 peer ospf02 endpoint '10.1.1.101:12345'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set interfaces wireguard wg01 peer ospf02 pubkey 'ie3...='
set interfaces wireguard wg01 port '12345'
set protocols ospfv3 parameters router-id 192.168.1.1
set protocols ospfv3 area 0.0.0.0 interface 'wg01'
set protocols ospfv3 area 0.0.0.0 interface 'lo'
```

Список команд для настройки второго узла:

```
set interfaces wireguard wg01 address 'fe80::216:3eff:fe0a:7ada/64'
set interfaces wireguard wg01 address '192.168.0.2/24'
set interfaces wireguard wg01 peer ospf01 allowed-ips '::/0'
set interfaces wireguard wg01 peer ospf01 allowed-ips '0.0.0.0/0'
set interfaces wireguard wg01 peer ospf01 endpoint '10.1.1.100:12345'
set interfaces wireguard wg01 peer ospf01 pubkey 'NHI...='
set interfaces wireguard wg01 port '12345'
set protocols ospfv3 parameters router-id 192.168.1.2
set protocols ospfv3 area 0.0.0.0 interface 'wg01'
set protocols ospfv3 area 0.0.0.0 interface 'lo'
```

Для проверки состояния между соседствующими узлами, используйте команду `show ipv6 ospfv3 neighbor`.

Пример вывода информации о состоянии соседствующих узлов:

```
fakel@ospf01:~$ show ipv6 ospfv3 neighbor
Neighbor ID     Pri    DeadTime    State/IfState         Duration I/F[State]
192.168.0.2       1    00:00:37     Full/PointToPoint    00:18:03
  wg01[PointToPoint]

fakel@ospf02# run show ipv6 ospfv3 neighbor
Neighbor ID     Pri    DeadTime    State/IfState         Duration I/F[State]
192.168.0.1       1    00:00:39     Full/PointToPoint    00:19:44
  wg01[PointToPoint]
```

Список команд

Основные настройки

Процесс OSPFv3 запускается при настройке первого интерфейса с поддержкой ospf.

- `set protocols ospfv3 area <number> interface <interface>`

  Активирует протокол OSPFv3 на определенном интерфейс `<interface>`. Номер области `<number>` может быть указан в десятичной системе счисления в диапазоне от 0 до 4294967295. Или он может быть указан в десятичной системе счисления, аналогично ip-адресу.

- `set protocols ospfv3 parameters router-id <rid>`

  Задает идентификатор маршрутизатора `<rid>` процесса OSPFv3. Идентификатор маршрутизатора может быть IP-адресом маршрутизатора, но не обязательно - это может быть любое про-

извольное 32-битное число. Однако он ДОЛЖЕН быть уникальным в пределах всего домена OSPFv3 для динамика OSPFv3 - если несколько динамиков OSPFv3 будут сконфигурированы с одним и тем же router-ID, произойдут плохие вещи!

Дополнительные настройки

- `set protocols ospfv3 distance global <distance>`

  Изменяет глобальное значение расстояния `<distance>` в протоколе OSPFv3. Диапазон расстояний составляет от 1 до 255.

- `set protocols ospfv3 distance ospfv3 <external|inter-area|intra-area> <distance>`

  Изменяет значение расстояния `<distance>` в протоколе OSPFv3. Аргументами являются значения расстояния для внешних маршрутов `<external>`, маршрутов, распространяемых между зонами `<inter-area>` и маршрутов, распространяемых внутри одной зоны `<intra-area>` соответственно. Диапазон значений расстояния составляет от 1 до 255.

Настройки областей

- `set protocols ospfv3 area <number> range <prefix>`

  Суммирует маршруты, распространяемые внутри одной зоны в один маршрут, распространяемый между зонами с префиксным типом LSA Type-3, анонсированный в другие зоны. Данная команда может быть использована только в ABR.

- `set protocols ospfv3 area <number> range <prefix> not-advertise`

  Фильтрует внутриобластные пути - т.е. внутриобластные пути из этого диапазона не рекламируются в другие области. Эта команда имеет смысл только в ABR.

Настройки интерфейсов

- `set interfaces <inttype> <interface> ipv6 ospfv3 cost <number>`

  Устанавливает стоимость соединения `<number>` для указанного интерфейса `<interface>`. Значение стоимости устанавливается в поле метрики маршрутизатора-LSA и используется для расчета SPF. Диапазон значений стоимости составляет от 1 до 65535.

- `set interfaces <inttype> <interface> ipv6 ospfv3 dead-interval <number>`

  Задайте количество секунд для значения таймера Dead Interval маршрутизатора, используемого для таймера ожидания и таймера бездействия. Это значение должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети. Значение по умолчанию составляет 40 секунд. Диапазон интервалов составляет от 1 до 65535.

- `set interfaces <inttype> <interface> ipv6 ospfv3 hello-interval <number>`

  Установка количества секунд для значения таймера Hello Interval `<number>`. При установке этого значения пакет Hello будет отправляться на указанный интерфейс каждые несколько секунд по таймеру. Это значение должно быть одинаковым для всех маршрутизаторов, подключенных к общей сети. Значение по умолчанию составляет 10 секунд. Диапазон значений интервала составляет от 1 до 65535.

- `set interfaces <inttype> <interface> ipv6 ospfv3 mtu-ignore`

  Отключает проверку значения MTU в пакетах OSPF DBD. Таким образом, использование

этой команды позволяет OSPF-связке достичь состояния FULL, даже если между двумя OSPF-маршрутизаторами имеется несоответствие MTU интерфейса.

- `set interfaces <inttype> <interface> ipv6 ospfv3 network <type>`

  Определяет тип распределения для сети `<type>`, подключенной к определенному интерфейсу `<inttype>`:

  - `broadcast` – распределение широковещательных IP-адресов.
  - `point-to-point` – распределение адресов в сетях «точка-точка.

- `set interfaces <inttype> <interface> ipv6 ospfv3 priority <number>`

  Задает целочисленное значение Router Priority `<number>`. Маршрутизатор с наивысшим приоритетом будет иметь больше шансов стать назначенным маршрутизатором. Если установить значение 0, то маршрутизатор не будет иметь права стать назначенным маршрутизатором. Значение по умолчанию равно 1. Диапазон интервалов от 0 до 255.

- `set interfaces <inttype> <interface> ipv6 ospfv3 passive`

  Определяет интерфейс `<interface>` как пассивный. Пассивный интерфейс рекламирует свой адрес, но не выполняет протокол OSPF (смежности не формируются и пакеты hello не генерируются).

- `set interfaces <inttype> <interface> ipv6 ospfv3 retransmit-interval <number>`

  Задает количество секунд для значения таймера RxmtInterval `<number>`. Это значение используется при повторной передаче пакетов Database Description и Link State Request, если подтверждение не было получено. Значение по умолчанию равно 5 секундам. Диапазон интервалов составляет от 3 до 65535.

- `set interfaces <inttype> <interface> ipv6 ospfv3 transmit-delay <number>`

  Задает количество секунд для значения InfTransDelay `<number>`. Позволяет установить и настроить для каждого интерфейса интервал задержки перед началом процесса синхронизации базы данных маршрутизатора со всеми соседями. Значение по умолчанию составляет 1 секунду. Диапазон значений интервала составляет от 3 до 65535.

Настройка редистрибуции

- `set protocols ospfv3 redistribute <route source>`

  Перераспределяет информацию о маршрутизации из заданного источника маршрута в процесс OSPF. Для источника маршрута доступно пять режимов: bgp, connected, kernel, rip, static.

- `set protocols ospf redistribute <route source> route-map <name>`

  Устанавливает route map `<name>` для фильтрации перераспределенных маршрутов из заданного источника маршрута `<route source>`. Для источника маршрута доступно пять режимов: bgp, connected, kernel, rip, static.

Мониторинг состояния

- `show ipv6 ospfv3 neighbor`

  Выводит информацию о состоянии соседей.

- `show ipv6 ospfv3 neighbor detail`

  Выводит информацию о соседях в подробном виде.

- `show ipv6 ospfv3 neighbor <A.B.C.D>`

  Выводит в подробном виде информацию для конкретного соседа `<A.B.C.D>`.

- `show ipv6 ospfv3 neighbor <interface>`

  Выводит в подробном виде информацию для соседа на указанном интерфейсе `<interface>`.

- `show ipv6 ospfv3 interface [prefix]|[<interface> [prefix]]`

  Выводит информацию о состоянии и настройках OSPF для указанного интерфейса `<interface>` или для всех интерфейсов, если конкретный интерфейс не указан. С аргументом `prefix` эта команда также выводит информацию о префиксах.

- `show ipv6 ospfv3 route`

  Выводит таблицу маршрутизации OSPF, определенную по последнему расчету SPF.

- `show ipv6 ospfv3 border-routers`

  Выводит таблицу путей к маршрутизаторам, граничащим с областью и автономной системой.

- `show ipv6 ospfv3 database`

  Выводит на экран сводную таблицу с содержимым базы данных (LSA).

- `show ipv6 ospfv3 database <type> [A.B.C.D] [adv-router <A.B.C.D>|self-originate]`

  Выводит содержимое базы данных для определенного типа рекламы каналов.

- `show ipv6 ospfv3 redistribute`

  Выводит информацию о редистрибуции маршрутов в OSPFv3

2.3.2.2 BGP

Описание

BGP (Border Gateway Protocol) — это основной протокол динамической маршрутизации, который используется в Интернете.

Маршрутизаторы, использующие протокол BGP (Border Gateway Protocol), обмениваются информацией о доступности сетей. Вместе с информацией о сетях передаются различные атрибуты этих сетей, с помощью которых BGP выбирает лучший маршрут и настраиваются политики маршрутизации.

ПО Факел использует для реализации протокола BGP механизм FRR (Free Range Routing).

Примечание

В **ПО Факел** нет специальной команды для запуска процесса, реализующего протокол BGP. Процесс запускается при настройке первого BGP соседа.

Концептуальные понятия

Автономные системы

Из спецификации **RFC 1930**[10] следует, что автономная система (далее - АС) представляет собой связанную группу из одного или нескольких IP префиксов, управляемую одним или несколькими провайдерами, которая имеет единую и четко определенную политику маршрутизации.

Каждая АС имеет связанный с ней идентификационный номер, обозначаемый как ASN (Autonomous System Number). Это двухбайтовое значение от 1 до 65535. Номера АС с 64512 по 65535 определяются как частные номера АС. Частные номера АС не должны анонсироваться в глобальной сети Интернет. Диапазон двухбайтовых номеров АС исчерпан. Четырехбайтные номера АС определены в спецификации **RFC 6793**[11] и предоставляют собой пул из 4294967296 номеров.

ASN является одним из основных элементов протокола BGP. Протокол BGP является протоколом дистанционно-векторной маршрутизации, а механизм *AS-Path* обеспечивает метрику для дистанционно-векторной маршрутизации, а также обнаружение петель в протоколе BGP.

Семейства адресов

Мультипротокольное расширение позволяют протоколу BGP передавать информацию о маршрутизации для нескольких протоколов сетевого уровня. Протокол BGP поддерживает идентификатор AFI (Address Family Identifier) для семейства адресов протоколов IP.

Выбор маршрутов

Процесс выбора маршрута, используемый в реализации протокола BGP механизмом FRR, использует следующие критерии принятия решения, начиная с верхней части списка и двигаясь к нижней до тех пор, пока один из критериев не будет определен как подходящий.

1. **Проверка веса маршрутов**

[10] https://datatracker.ietf.org/doc/html/rfc1930.html
[11] https://datatracker.ietf.org/doc/html/rfc6793.html

Выбор в пользу маршрутов с большим локальным весом.

2. **Проверка локальных предпочтений**

Выбор в пользу маршрутов с большими локальными предпочтениями.

3. **Проверка локальных маршрутов**

Выбор в пользу локальных маршрутов (статических, агрегированных, перераспределенных) вместо полученных.

4. **Проверка длины пути до АС**

Выбор в пользу меньшего числа пересылок на пути до АС.

5. **Проверка источника**

Выбор в пользу маршрута с наименьшего типом источника. То есть предпочтение отдается маршрутам IGP, а не EGP и неполным маршрутам.

6. **Проверка атрибута MED**

Если маршруты с атрибутом MED (Multi Exit Discriminator) были получены из одной и той же АС, предпочтение отдается маршруту с наименьшим значением атрибута MED.

7. **Проверка внешних источников маршрутов**

Выбор в пользу маршрута, полученного от внешнего eBGP соседа, вместо маршрутов, полученных от других типов соседей.

8. **Проверка IGP стоимости**

Выбор в пользу маршрута с меньшей IGP стоимостью.

9. **Проверка множественных путей**

Если включено использование множественных путей, то проверяется, можно ли считать равными маршруты, еще не различающиеся по предпочтениям. Если установлено значение параметра `bgp bestpath as-path multipath-relax`, то все такие маршруты считаются равными, в противном случае равными считаются маршруты, полученные через iBGP с одинаковыми *AS-Path*, или маршруты, полученные от соседей eBGP в той же АС.

10. **Проверка уже выбранного внешнего маршрута**

Если оба маршрута получены от eBGP соседей, то предпочтение отдается тому маршруту, который уже выбран. Необходимо учесть, что эта проверка не применяется, если настроен параметр `bgp bestpath compare-routerid`. Эта проверка может предотвратить некоторые случаи колебаний.

11. **Проверка параметра идентификатора маршрутизатора**

Предпочтение отдается маршруту с наименьшим идентификатором *router-ID*. Если маршрут имеет атрибут *ORIGINATOR_ID*, полученный через механизм отражения маршрутов iBGP, то используется идентификатор данного маршрутизатора, в противном случае используется идентификатор *router-ID* соседа, от которого был получен маршрут.

12. **Проверка длины списка кластеризации**

Используется маршрут с наименьшей длиной списка кластеризации. Список кластеризации определяет путь отражения маршрута в iBGP.

13. **Проверка адреса соседа**

Предпочтение отдается маршруту, полученному от соседа с более высоким адресом транспортного уровня, в качестве критерия при прочих равных результатах.

Настройка

Пример настройки

Для протокола IPv4

Пример простой конфигурации eBGP между двумя устройствами.

Узел 1:

```
set protocols bgp 65534 neighbor 192.168.0.2 ebgp-multihop '2'
set protocols bgp 65534 neighbor 192.168.0.2 remote-as '65535'
set protocols bgp 65534 neighbor 192.168.0.2 update-source '192.168.0.1'
set protocols bgp 65534 address-family ipv4-unicast network '172.16.0.0/16'
set protocols bgp 65534 parameters router-id '192.168.0.1'
```

Узел 2:

```
set protocols bgp 65535 neighbor 192.168.0.1 ebgp-multihop '2'
set protocols bgp 65535 neighbor 192.168.0.1 remote-as '65534'
set protocols bgp 65535 neighbor 192.168.0.1 update-source '192.168.0.2'
set protocols bgp 65535 address-family ipv4-unicast network '172.17.0.0/16'
set protocols bgp 65535 parameters router-id '192.168.0.2'
```

По умолчанию префикс, объявленный в операторе `network` не обязательно должен существовать в таблице маршрутизации, однако для предотвращения возникновения петель маршрутизации его обычно добавляют. Наиболее правильный способ сделать это - создать статический маршрут.

Узел 1:

```
set protocols static route 172.16.0.0/16 blackhole distance '254'
```

Узел 2:

```
set protocols static route 172.17.0.0/16 blackhole distance '254'
```

Фильтрация маршрутов

К маршрутам может быть применен фильтр с помощью карты маршрутов (route-map):

Узел 1:

```
set policy prefix-list AS65535-IN rule 10 action 'permit'
set policy prefix-list AS65535-IN rule 10 prefix '172.16.0.0/16'
set policy prefix-list AS65535-OUT rule 10 action 'deny'
set policy prefix-list AS65535-OUT rule 10 prefix '172.16.0.0/16'
set policy prefix-list6 AS65535-IN rule 10 action 'permit'
set policy prefix-list6 AS65535-OUT rule 10 action 'deny'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set policy route-map AS65535-IN rule 10 action 'permit'
set policy route-map AS65535-IN rule 10 match ip address prefix-list 'AS65535-IN'
set policy route-map AS65535-IN rule 20 action 'deny'
set policy route-map AS65535-OUT rule 10 action 'deny'
set policy route-map AS65535-OUT rule 10 match ip address prefix-list 'AS65535-OUT'
set policy route-map AS65535-OUT rule 20 action 'permit'
set protocols bgp 65534 neighbor 2001:db8::2 address-family ipv4-unicast route-map
 export 'AS65535-OUT'
set protocols bgp 65534 neighbor 2001:db8::2 address-family ipv4-unicast route-map
 import 'AS65535-IN'
```

Узел 2:

```
set policy prefix-list AS65534-IN rule 10 action 'permit'
set policy prefix-list AS65534-IN rule 10 prefix '172.17.0.0/16'
set policy prefix-list AS65534-OUT rule 10 action 'deny'
set policy prefix-list AS65534-OUT rule 10 prefix '172.17.0.0/16'
set policy prefix-list6 AS65534-IN rule 10 action 'permit'
set policy prefix-list6 AS65534-OUT rule 10 action 'deny'
set policy route-map AS65534-IN rule 10 action 'permit'
set policy route-map AS65534-IN rule 10 match ip address prefix-list 'AS65534-IN'
set policy route-map AS65534-IN rule 20 action 'deny'
set policy route-map AS65534-OUT rule 10 action 'deny'
set policy route-map AS65534-OUT rule 10 match ip address prefix-list 'AS65534-OUT'
set policy route-map AS65534-OUT rule 20 action 'permit'
set protocols bgp 65535 neighbor 2001:db8::1 address-family ipv4-unicast route-map
 export 'AS65534-OUT'
set protocols bgp 65535 neighbor 2001:db8::1 address-family ipv4-unicast route-map
 import 'AS65534-IN'
```

Можно также расширить данный пример запретом локальных соединений и многоадресной рассылки в правиле с номеров 20 с действием `action deny`.

Список команд

Настройка BGP соседства

Определение BGP соседей

`# set protocols bgp <asn> neighbor <address|interface> remote-as <nasn>`

Данная команда позволяет создать нового соседа, для которого значение параметра `remote-as` равно <nasn>. Адрес соседа может быть IP-адресом или интерфейсом, который будет использоваться для соединения. Команда применима как для отдельного соседа, так и для группы соседей.

`# set protocols bgp <asn> neighbor <address|interface> remote-as internal`

При выполнении данной команды создание соседа происходит так же, как и при указании ASN, за исключением того, что если ASN соседа отличается от собственного, указанного в команде

protocols bgp <asn>, то в соединении будет отказано.

```
# set protocols bgp <asn> neighbor <address|interface> remote-as external
```

При выполнении данной команды создание соседа происходит так же, как и при указании ASN, за исключением того, что если ASN соседа совпадает с собственным, указанным в команде protocols bgp <asn>, то в соединении будет отказано.

```
# set protocols bgp <asn> neighbor <address|interface> shutdown
```

Данная команда позволяет отключить соседа или группу соседей. Для повторной активации соседа необходимо использовать контекст delete для данной команды.

```
# set protocols bgp <asn> neighbor <address|interface> description <text>
```

Данная команда позволяет задать описание для соседа или группы соседей.

```
# set protocols bgp <asn> neighbor <address|interface> update-source
<address|interface>
```

Данная команда позволяет указать адрес отправителя, который будет использоваться для BGP сессии с этим соседом. Адрес может быть указан как IPv4 адрес или как имя интерфейса.

Согласование возможностей BGP соседства

```
# set protocols bgp <asn> neighbor <address|interface> capability dynamic
```

Данная команда позволяет динамически обновлять список доступных функций через установленную BGP сессию.

```
# set protocols bgp <asn> neighbor <address|interface> capability extended-nexthop
```

Данная команда позволяет разрешить для протокола BGP согласование функции extended-nexthop со своим соседом.

```
# set protocols bgp <asn> neighbor <address|interface>
disable-capability-negotiation
```

Данная команда запрещает отправку соседу сообщения *Capability Negotiation* в качестве необязательного параметра сообщения для установления соседства. Команда действует только в случае, если для соседа задана конфигурация, отличная от одноадресной конфигурации IPv4.

Если удаленный сосед не имеет возможности согласования функций, то он не будет посылать список таковых. В этом случае протокол BGP выполнит настройку соседа в соответствии с заданными функциями.

В некоторых случаях может потребоваться использования большего числа функций, чем было согласовано между соседями, даже если удаленный сосед передает определенный список функций. В этом случае, если сосед сконфигурирован с помощью параметра override-capability, то **ПО Факел** игнорирует полученный список функций, а затем заменяет согласованные функции сконфигурированными.

Также необходимо иметь в виду, что данная функция принципиально лишает возможности использовать широко распространенные функции протокола BGP, такие как: использование ненумерованных интерфейсов, поддержка имен хостов, использование четырехбайтных номеров AC, задание нескольких путей для одного и того же префикса, обновление маршрутов, фильтрация маршрутной информации, динамический список функций, плавный перезапуск.

```
# set protocols bgp <asn> neighbor <address|interface> override-capability
```

Данная команда позволяет переопределить результат согласования функций с помощью локальной конфигурации. В этом случае список функций удаленного соседа игнорируется.

```
# set protocols bgp <asn> neighbor <address|interface> strict-capability-match
```

Данная команда принуждает к строгому сравнению списка доступных функций удаленного и локального соседей. Если списка функций отличается, формируется ошибка *Unsupported Capability*, а затем происходит сброс соединения.

Можно также запретить отправку параметра *Capability Negotiation* в сообщении для установления соседства, если удаленный сосед не поддерживается возможности согласования функций. Для отключения необходимо использовать команду `disable-capability-negotiation`.

Настройка параметров для BGP соседей

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> allowas-in number <number>
```

Данная команда принимает входящие маршруты с путем до АС, содержащим номер АС с тем же значением и АС данной системы. Такой подход используется в случаях, когда необходимо использовать один и тот же номер АС для разных сегментов, соединить которые напрямую не представляется возможным.

Параметр `number` (1-10) позволяет настроить количество допустимых повторений системного номера АС в пути до АС.

Допустимо использование данной команды только для отдельных eBGP соседей и не допустимо для групп соседей.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> as-override
```

Данная команда переопределяет номер АС маршрутизатора-источника локальным номером АС.

Обычно такая конфигурация применяется на оконечном оборудовании провайдера (Provider Edge) для замены входящего номера АС клиента таким образом, чтобы оконечное клиентское оборудование (Customer Edge) могло использовать тот же номер АС. Это позволяет клиенту сети провайдера использовать один и тот же номер АС во всех сегментах.

Допустимо использование данной команды только для отдельных eBGP соседей.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> attribute-unchanged <as-path|med|next-hop>
```

Данная команда задает список атрибутов, которые должны быть неизменными при анонсах соседу или группе соседей.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> maximum-prefix <number>
```

Данная команда задает максимальное количество префиксов, которое можно получить от определенного соседа. Если это количество будет превышено, то BGP сессия будет сброшена. Диапазон значений составляет от 1 до 4294967295.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> nexthop-self
```

Данная команда принуждает BGP соседа, являющегося источником анонсов, сообщать о себе как о следующем узле для анонсируемого в адрес своего соседа маршрута.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> remove-private-as
```

Данная команда удаляет частные номера ASN для маршрутов, которые анонсируются сконфигурированному соседу. Ее использование приводит к удалению только частных номеров ASN для маршрутов, анонсируемых eBGP соседям.

Если параметр *AS-Path* содержит только частные номера ASN для маршрута, то все эти номера удаляются.

Если параметр *AS-Path* содержит частные номера ASN наряду с публичными номерами ASN, то считается, что так задумано, и частные номера ASN не удаляются.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> soft-reconfiguration inbound
```

Внесение изменений в политики BGP требуют сброса соответствующих сессий. Сброс оказывает негативное влияние на работу сети. Плавная внесение изменений в конфигурацию позволяет генерировать входящие обновления обновления от соседа, изменять и активировать политики BGP без сброса сессий.

Данная команда определяет, что обновления маршрутов, полученные от определенного соседа, будут сохраняться без изменений вне зависимости от политики входящих соединений. Если включено плавное изменение конфигурации входящих маршрутов, то сохраненные обновления обрабатываются новой конфигурацией политики для создания новых входящих обновлений.

Примечание

Для хранения обновлений маршрутов используется оперативная память. Если включить плавное внесение изменений в конфигурацию входящих маршрутов для нескольких соседей, объем используемой памяти может значительно возрасти.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> weight <number>
```

Данная команда задает значение веса по умолчанию для маршрутов соседа. Диапазон значений составляет от 1 до 65535.

```
# set protocols bgp <asn> neighbor <address|interface> advertisement-interval
<seconds>
```

Данная команда задает минимальный интервал между анонсами маршрутов для соседа. Значение интервала составляет от 0 до 600 секунд, по умолчанию интервал между анонсами равен 0.

```
# set protocols bgp <asn> neighbor <address|interface> disable-connected-check
```

Данная команда позволяет соединять между собой напрямую подключенных eBGP соседей с использованием Loopback адресов и без корректировка времени жизни (TTL), по умолчанию значение которого равно 1.

```
# set protocols bgp <asn> neighbor <address|interface> disable-send-community
<extended|standard>
```

Данная команда определяет, что атрибут *Community* не должен передаваться в обновлениях маршрутов, адресованных соседу. По умолчанию атрибут *Community* передается.

```
# set protocols bgp <asn> neighbor <address|interface> ebgp-multihop <number>
```

Данная команда позволяет устанавливать соединения с eBGP соседями, даже если они находятся на удалении в несколько пересылок между узлами сети. Если сосед не имеет прямого соединения и данная команда не используется, соединение не будет установлено. Диапазон количества пересылок между узлами сети составляет от 1 до 255. Эта команда является взаимоисключающей по отношению к команде `ttl-security hops`.

```
# set protocols bgp <asn> neighbor <address|interface> local-as <asn> [no-prepend]
[replace-as]
```

Данная команда позволяет указать альтернативную AC для данного BGP процесса при взаимодействии с указанным соседом или группой соседей. Без дополнительных атрибутов AC, указанная в параметре `local-as`, добавляется к входящему значению *AS-Path* при получении обновлений маршрутов от соседа и к исходящему значению *AS-Path* (после обработки локальной AC) при передаче локальных маршрутов соседу.

Если указан атрибут `no-prepend`, то заданное значение параметра `local-as` не добавляется к входящему значению *AS-Path*.

Если указан атрибут `replace-as`, то при передаче обновлений локальных маршрутов соседу к значению *AS-Path* добавляется только заданное значение параметра `local-as`.

Примечание

Данная команда применима только для eBGP соседей.

```
# set protocols bgp <asn> neighbor <address|interface> passive
```

Данная команда настраивает узел в качестве источника BGP анонсов таким образом, чтобы он принимал только входящие соединения, но не инициировал исходящие соединения с соседом или группой соседей.

```
# set protocols bgp <asn> neighbor <address|interface> password <text>
```

Данная команда задает пароль для TCP сокета, кодированный алгоритмом MD5 и используемый для соединения с удаленным соседом.

```
# set protocols bgp <asn> neighbor <address|interface> ttl-security hops <number>
```

Данная команда реализует механизм безопасности GTSM (Generalized TTL Security Mechanism) согласно спецификации **RFC 5082**[12]. С помощью этой команды статус соседей разрешается присваивать только узлам, находящимся на расстоянии заданного числа пересылок между узлами. Диапазон числа пересылок между узлами составляет от 1 до 254. Команда является взаимоисключающей по отношению к команде `ebgp-multihop`.

[12] https://datatracker.ietf.org/doc/html/rfc5082.html

Настройка группы BGP соседей

Группы соседей используются для улучшения масштабирования за счет объединения общих параметров и информации об обновлениях для всех участников группы. Это означает, что маршруты, созданные участником группы, будут отправляться обратно в адрес источника с атрибутом *Originator Identifier*, значение которого указывает на соседа-источника маршрутной информации. Соседи, не связанные ни с одной группой, воспринимаются как принадлежащие к группе соседей по умолчанию, и будут использовать общие обновления.

```
# set protocols bgp <asn> peer-group <name>
```

Данная команда определяет новую группу соседей. Для группы можно указать те же параметры, что я для отдельных соседей.

Примечание

Если изменения применяются к IP адресу отдельного соседа, они переопределяют изменения, внесенные для группы соседей, в которую входит данный IP адрес.

```
# set protocols bgp <asn> neighbor <address|interface> peer-group <name>
```

Данная команда связывает конкретную группу соседей с заданным именем.

Настройка анонсов BGP

```
# set protocols bgp <asn> address-family <ipv4-unicast|ipv6-unicast> network
<prefix>
```

Данная команда используется для анонсирования сетей IPv4 или IPv6.

Примечание

По умолчанию префикс BGP анонсируется, даже если он отсутствует в таблице маршрутизации.

```
# set protocols bgp <asn> parameters network-import-check
```

Данная конфигурация позволяет изменить поведение оператора `network`. При такой настройке базовая сеть должна существовать в таблице маршрутизации.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> default-originate [route-map <name>]
```

По умолчанию **ПО Факел** не анонсирует маршрут по умолчанию (0.0.0.0/0), даже если он есть в таблице маршрутизации. Данную команду следует использовать в случае, если необходимо анонсировать маршрут по умолчанию. При использовании дополнительного аргумента `route-map`, можно передать маршрут по умолчанию заданному соседу только в том случае, если выполняются условия заданной аргументом `route-map` карты маршрутов.

Настройка агрегации маршрутов

```
# set protocols bgp <asn> address-family <ipv4-unicast|ipv6-unicast>
aggregate-address <prefix>
```

Данная команда задает агрегированный адрес. Маршрутизатор также будет анонсировать более длинные префиксы внутри агрегированного адреса.

```
# set protocols bgp <asn> address-family <ipv4-unicast|ipv6-unicast>
aggregate-address <prefix> as-set
```

Данная команда задает агрегированный адрес с математическим набором AC. Команда суммирует атрибуты *AS-Path* для всех отдельных маршрутов.

```
# set protocols bgp <asn> address-family <ipv4-unicast|ipv6-unicast>
aggregate-address <prefix> summary-only
```

Данная команда задает агрегированный адрес и обеспечивает подавление более длинных префиксов внутри агрегированного адреса перед отправкой обновлений BGP соседям.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> unsuppress-map <name>
```

Данная команда применяет определенную карту маршрутов для выборочного исключения префиксов, подавленных в процессе суммирования.

Настройка редистрибуции

```
# set protocols bgp <asn> address-family <ipv4-unicast|ipv6-unicast> redistribute
<route source>
```

Данная команда осуществляет редистрибуцию маршрутной информации от заданного источника в процесс BGP. Для источника маршрута доступны следующие режимы: `connected`, `kernel`, `ospf`, `rip`, `static`, `table`.

```
# set protocols bgp <asn> address-family <ipv4-unicast|ipv6-unicast> redistribute
<route source> metric <number>
```

Данная команда задает метрику MED для маршрутов, подлежащих редистрибуции. Диапазон значений метрики составляет от 0 до 4294967295. Для источника маршрутной информации доступны следующие режимы: `connected`, `kernel`, `ospf`, `rip`, `static`, `table`.

```
# set protocols bgp <asn> address-family <ipv4-unicast|ipv6-unicast> redistribute
<route source> route-map <name>
```

Данная команда позволяет использовать определенную карту маршрутов для фильтрации маршрутов, подлежащих редистрибуции. Для источника маршрутной информации доступны следующие режимы: `connected`, `kernel`, `ospf`, `rip`, `static`, `table`.

Базовые настройки

Общие параметры

```
# set protocols bgp <asn> parameters router-id <id>
```

Данная команда задает идентификатор маршрутизатора *router-ID*. Если идентификатор не указан, то в качестве него будет использоваться IP адрес интерфейса с наибольшим значением.

```
# set protocols bgp <asn> address-family <ipv4-unicast|ipv6-unicast> maximum-paths
<ebgp|ibgp> <number>
```

Данная команда определяет максимальное количество параллельных маршрутов, которое может поддерживаться процессом BGP. Для того, чтобы процесс BGP использовал второй путь, необходимо, чтобы совпадали следующие атрибуты: вес, локальные предпочтения, путь до AC (номер AC и длина пути), код источника маршрутной информации, атрибут MED, метрика IGP. Кроме того, адрес следующего узла для каждого пути должен быть разным.

```
# set protocols bgp <asn> parameters default no-ipv4-unicast
```

Данная команда позволяет отключить по умолчанию установление соседства по протоколу IPv4.

```
# set protocols bgp <asn> parameters log-neighbor-changes
```

Данная команда позволяет активирует запись в журнал события, которые связаны изменения статуса соседей (доступен / не доступен) и причины сброса.

```
# set protocols bgp <asn> parameters no-client-to-client-reflection
```

Данная команда отключает отражение маршрутов между клиентами. По умолчанию клиенты не должны быть объединены в полносвязную сеть, и маршруты от определенного клиента отражаются всем остальным. Если клиенты все же объединены в полносвязную сеть, отражение маршрутов не требуется. В этом случае необходимо использовать команду `no-client-to-client-reflection`, чтобы отключить отражение маршрутов между клиентами.

```
# set protocols bgp <asn> parameters no-fast-external-failover
```

Данная команда отключает немедленный сброс сессий при отказе канала связи с соседом.

Административная дистанция

```
# set protocols bgp <asn> parameters distance global <external|internal|local>
<distance>
```

Данная команда изменяет значение административной дистанции в BGP. В качестве аргументов указываются значения административной дистанции для внешних, внутренних и локальных

маршрутов соответственно. Диапазон значений административной дистанции составляет от 1 до 255.

`# set protocols bgp <asn> parameters distance prefix <subnet> distance <distance>`

Данная команда задает административную дистанцию для определенного маршрута. Диапазон значений административной дистанции составляет от 1 до 255.

Примечание

Маршруты с административной дистанцией 255 фактически отключены и не используются модулями ядра при принятии решений о маршрутизации трафика.

Настройка таймеров

`# set protocols bgp <asn> timers holdtime <seconds>`

Данная команда задает время удержания маршрутов в секундах. Диапазон значений такого таймера составляет от 4 до 65535. По умолчанию используется значение 180 секунд. Если установить значение 0, то **ПО Факел** не будет удерживать маршруты.

`# set protocols bgp <asn> timers keepalive <seconds>`

Данная команда задает время жизни маршрутов в секундах. Диапазон значений такого таймера составляет от 4 до 65535. По умолчанию используется значение 60 секунд.

Настройка BGP Route Dampening

Когда маршрут выходит из строя, отправляется обновление маршрут с указанием на то, чтобы изъять его из таблиц маршрутизации. Когда маршрут восстанавливается, об изменении его доступности также сообщается. Поэтому маршрут, который постоянно выходит из строя и восстанавливается, требует значительного объема сетевого трафика для обновлении информации о его состоянии

Гашение маршрутов, описание которого представлено в **RFC 2439**[13], позволяет выявлять маршруты, которые регулярно выходят из строя и восстанавливается. Если гашение маршрутов выключено, то нестабильный маршрут накапливает штрафы при каждом выходе из строя и восстановлении. Если сумма штрафов превышает определенное пороговое значение, маршрут больше не анонсируется. Данное поведение называется подавлением маршрутов. Маршруты, которые были подавлены, могут снова попасть в таблицу маршрутизации только тогда, когда сумма штрафов становится меньше порогового значения

При каждом выходе из строя маршруту начисляется штраф в размере 1000. Когда сумма штрафом достигают порогового значения `suppress-value`, маршрутизатор прекращает анонсировать данный маршрут

После применения штрафа к маршруту, его значение уменьшается ровно вдвое каждый раз по истечении заданного параметром `half-life-time` времени. Когда сумма штрафом становится меньше порогового значения `reuse-value`, маршрут перестает подавляться и снова добавляется в таблицу маршрутизации

Маршруты не остаются подавленными бесконечно. Параметр `maximum-suppress-time` определяет

[13] https://datatracker.ietf.org/doc/html/rfc2439.html

время, в течение которого маршрут может оставаться подавленным, прежде чем произойдет его повторное анонсирование.

`# set protocols bgp <asn> parameters dampening half-life <minutes>`

Данная команда определяет время в минутах, по истечении которого примененный штраф уменьшается вдвое. Диапазон значений составляет от 10 до 45 минут.

`# set protocols bgp <asn> parameters dampening re-use <seconds>`

Данная команда определяет накопленную сумму штрафа, при которой маршрут повторно анонсрируется. Диапазон значений составляет от 1 до 20000.

`# set protocols bgp <asn> parameters dampening start-suppress-time <seconds>`

Данная команда определяет накопленную сумму штрафов, при которой маршрут подавляется. Диапазон значений составляет от 1 до 20000.

`# set protocols bgp <asn> parameters dampening max-suppress-time <seconds>`

Данная команда определяет максимальное время в минутах, в течение которого маршрут может оставаться подавленным, прежде чем произойдет его повторное анонсирование. Диапазон значений составляет от 1 до 255 минут.

Настройка выбора маршрутов

`# set protocols bgp <asn> parameters always-compare-med`

Данная команда позволяет сравнивать значения атрибута MED маршрутов, даже если они были полученных из разных соседних AC. Использование данной опции делает порядок предпочтения маршрутов более определенным и должно исключить возможные колебания, вызванные MED.

`# set protocols bgp <asn> parameters bestpath as-path confed`

Данная команда определяет, что длина наборов и последовательностей разделенных путей (confederation path) должна учитываться в процессе принятия решения протоколом BGP о выборе оптимального пути.

`# set protocols bgp <asn> parameters bestpath as-path multipath-relax`

Данная команда предписывает в процессе принятия протоколом BGP решений о выборе оптимального пути рассмотрение путей одинаковой длины *AS-Path* в качестве кандидатов на расчет множественности путей. Без использования этой команды при расчете соответствующих этой концепции маршрутов требуется совпадение всего значения *AS-Path*.

`# set protocols bgp <asn> parameters bestpath as-path ignore`

Данная команда предписывает игнорирование длины *AS-Path* при выборе маршрута.

`# set protocols bgp <asn> parameters bestpath compare-routerid`

При сравнении маршрутов необходимо убедиться, что если они равны по большинству метрик, включая локальные предпочтения, длину пути до AC, стоимость IGP, значение атрибута MED, равенство в конечном счете определяется по идентификатору маршрутизатора *router-ID*.

Если данная опция включена, то проверка уже выбранных маршрутов, при которой предпочтение отдается уже выбранным маршрутам eBGP, пропускается.

Если маршрут имеет атрибут *ORIGINATOR_ID* в результате отражения, то будет использоваться значение атрибута *ORIGINATOR_ID*. В противном случае будет использоваться идентификатор маршрутизатора того соседа, от которого был получен маршрут.

Преимуществом такого подхода является то, что выбор маршрута на данном этапе будет более детерминированным. Недостатком является то, что из-за такой проверки один или несколько маршрутизаторов или один маршрутизатор с наименьшим идентификатором могут перетянуть весь трафик на другие равные пути. Это может увеличить вероятность возникновения колебаний MED или IGP, если не были приняты другие меры для их предотвращения. Точное поведение будет зависеть от топологии iBGP и процесса отражения маршрутов.

`# set protocols bgp <asn> parameters bestpath med confed`

Данная команда определяет, что протокол BGP учитывает атрибут MED при сравнении маршрутов, источниками которых являются разные дочерние AC в пределах области разделения, к которой принадлежит данный источник анонсов по протоколу BGP. Состоянием по умолчанию является состояние, при котором атрибут MED не учитывается.

`# set protocols bgp <asn> parameters bestpath med missing-as-worst`

Данная команда определяет, что маршрут с атрибутом MED всегда считается маршрутом с самым высоким приоритетом, чем без него, определяя для отсутствующего атрибута MED фактически значение бесконечности. Состоянием по умолчанию является состояние, при котором атрибут MED не учитывается.

`# set protocols bgp <asn> parameters default local-pref <local-pref value>`

Данная команда задает значение локального предпочтения по умолчанию. Диапазон значений локального предпочтения составляет от 0 до 4294967295.

`# set protocols bgp <asn> parameters deterministic-med`

Данная команда позволяет сравнивать различные значения атрибута MED, анонсируемые соседями в одной AC, при выборе маршрутов. Когда эта команда включена, маршруты из одной AC группируются вместе, сравниваются лучшие записи из каждой группы.

`# set protocols bgp <asn> address-family ipv4-unicast network <prefix> backdoor`

Данная команда предписывает маршрутизатору предпочтение маршрут с указанным префиксом, полученным путем использования протокола IGP по через backdoor соединение, вместо маршрута к тому же префиксу, полученному путем использования протокола eBGP.

Настройка фильтрации маршрутов

Для контроля и модификации маршрутной информации, которой обмениваются соседи, можно использовать карту маршрутов, список заданных фильтров и префиксов, список дистрибуции.

Для входящих обновлений предпочтение отдается следующим образом:

- карта маршрутов (`route-map`);
- список заданных фильтров (`filter-list`);
- список заданных префиксов, список дистрибуции (`prefix-list`, `distribute-list`).

Для исходящих обновлений предпочтение отдается следующим образом:

- список заданных префиксов, список дистрибуции (`prefix-list`, `distribute-list`);
- список заданных фильтров (`filter-list`);
- карта маршрутов (`route-map`).

Примечание

Атрибуты `prefix-list` и `distribute-list` являются взаимоисключающими, и только одна команда (`distribute-list` или `prefix-list`) может быть применена к каждому входящему или исходящему направлению для конкретного соседа.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> distribute-list <export|import> <number>
```

Данная команда применяет фильтры списка доступа с именем <number> к указанному соседу BGP для ограничения информации о маршрутизации, которую протокол BGP получает и/или анонсирует. Аргументы `export` и `import` задают направление применения списка доступа.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> prefix-list <export|import> <name>
```

Данная команда применяет фильтры из списка `prfefix-list`, заданные в <name>, к указанному соседу BGP для ограничения маршрутной информации, которую протокол BGP получает и/или анонсирует. Аргументы `export` и `import` задают направление применения списка префиксов.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> route-map <export|import> <name>
```

Данная команда применяет карту маршрутов с именем <name> к указанному соседу BGP для управления и модификации маршрутной информации, которой обмениваются между собой соседи. Аргументы `export` и `import` задают направление применения карты маршрутов.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> filter-list <export|import> <name>
```

Данная команда применяет к определенному соседу BGP фильтры списка доступа к значениям *AS-Path*, указанным в <name>, для ограничения информации о маршрутизации, которую протокол BGP получает и/или анонсирует. Аргументы `export` и `import` задают направление, в котором применяется список доступа к *AS-Path*.

```
# set protocols bgp <asn> neighbor <address|interface> address-family
<ipv4-unicast|ipv6-unicast> capability orf <receive|send>
```

Данная команда включает возможность фильтрации маршрутной информации ORF (Outbound Route Filtering), описание которой представлено в спецификации **RFC 5291**[14], на локальном маршрутизаторе и включает анонсирование возможности ORF для указанного BGP соседа. Ключ `receive` настраивает маршрутизатор на анонсирование возможности приема ORF. Ключ end настраивает маршрутизатор на анонсирование возможности передачи ORF. Чтобы анонсировать фильтр отправителя, необходимо создать список IP префиксов для указанного BGP соседа, применяемый при входящей сортировке.

Настройка масштабирования BGP

Маршрутизаторы BGP, соединенные между собой в рамках одной и той же AC, принадлежат к внутренней сессии BGP или iBGP. Чтобы предотвратить зацикливание таблицы маршрутизации, узел являющийся источником анонсов, не анонсирует маршруты, обнаружение в процессе работы iBGP, другим узлам

[14] https://datatracker.ietf.org/doc/html/rfc5291.html

iBGP - подход называется разделением горизонта (Split Horizon). Таким образом для работы iBGP требуется полносвязная сеть соседей. Для больших сетей это практически невыполнимо.

Существует два способа, позволяющих смягчить требование протокола BGP к полносвязности сети соседей:

- Использование отражения маршрутов;
- Использование разделения АС.

Настройка BGP Route Reflector

Внедрение узлов, выполняющих функцию отражения маршрутов, устраняет необходимость в организации полносвязной сети соседей. При настройке таких узлов необходимо указать маршрутизатору, является ли другой маршрутизатора iBGP клиентом или нет. Клиент представляет собой iBGP маршрутизатор на который узел будет отражать маршруты. Маршрутизатор не являющийся клиентом - обычный iBGP сосед. Описание механизма отражения маршрутов представлено в спецификации **RFC 4456**[15] и дополнено в спецификации **RFC 7606**[16].

`# set protocols bgp <asn> neighbor <address> address-family <ipv4-unicast|ipv6-unicast> route-reflector-client`

Данная команда определяет указанного соседа как клиента для отражения маршрутов.

`# set protocols bgp <asn> parameters cluster-id <id>`

Данная команда задает идентификатор кластера, который формирует совокупность узлов, отражающих маршруты, и их клиентов, и используется узлами, отражающими маршруты, для предотвращения петель в коммуникациях. По умолчанию идентификатор кластера равен значению параметра *router-id* для протокола BGP, но может быть установлен в произвольное 32-битное значение.

Настройка механизма разделения АС

Механизм разделения в протоколе BGP подразумевает деление АС на подсистемы для уменьшения количества необходимых iBGP соединений. В пределах одной подсистемы по-прежнему требуется наличие полносвязной iBGP сети, но между подсистемами используется подобие eBGP, функционирующее как iBGP (таким образом определяется область разделения). Описание механизма представлено в спецификации **RFC 5065**[17].

`# set protocols bgp <subasn> parameters confederation identifier <asn>`

Данная команда задает идентификатор области разделения в протоколе BGP. Параметр `<asn>` - номер АС, которая включает в себя несколько подсистем (область разделения). Параметр `<subasn>` - номер подсистемы в рамках АС, заданной параметром `<asn>`.

`# set protocols bgp <subasn> parameters confederation confederation peers <nsubasn>`

Данная команда устанавливает другие области разделения `<nsubasn>` в качестве подчиненных АС, идентификатор которой указан в команде `confederation identifier <asn>`.

[15] https://datatracker.ietf.org/doc/html/rfc4456.html
[16] https://datatracker.ietf.org/doc/html/rfc7606.html
[17] https://datatracker.ietf.org/doc/html/rfc5065.html

Мониторинг и эксплуатация

`$ show <ip|ipv6> bgp`

Выводит на экран все записи в таблице маршрутизации BGP.

```
BGP table version is 10, local router ID is 10.0.35.3, vrf id 0
Default local pref 100, local AS 65000
Status codes: s suppressed, d damped, h history, * valid, > best, = multipath,
              i internal, r RIB-failure, S Stale, R Removed
Nexthop codes: @NNN nexthop's vrf id, < announce-nh-self
Origin codes:  i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 198.51.100.0/24  10.0.34.4                0             0 65004 i
*> 203.0.113.0/24   10.0.35.5                0             0 65005 i

Displayed  2 routes and 2 total paths
```

`$ show <ip|ipv6> bgp <address|prefix>`

Выводит на экран информацию о конкретной записи в таблице маршрутизации BGP.

```
BGP routing table entry for 198.51.100.0/24
Paths: (1 available, best #1, table default)
  Advertised to non peer-group peers:
  10.0.13.1 10.0.23.2 10.0.34.4 10.0.35.5
  65004
    10.0.34.4 from 10.0.34.4 (10.0.34.4)
      Origin IGP, metric 0, valid, external, best (First path received)
      Last update: Wed Jan  6 12:18:53 2021
```

`$ show ip bgp cidr-only`

Выводит на экран список маршрутов с бесклассовой междоменной маршрутизацией (CIDR).

`$ show <ip|ipv6> bgp community <value>`

Выводит на экран список маршрутов, принадлежащие указанным сообществам BGP. Допустимые значения: номер сообщества в диапазоне от 1 до 4294967200, AA:NN (AA - 2-байтовый номер AC, NN - 2-байтовый номер сообщества), `no-export`, `local-as` или `no-advertise`.

`$ show <ip|ipv6> bgp community-list <name>`

Выводит на экран список маршрутов, разрешенные списком сообществ BGP.

`$ show ip bgp dampened-paths`

Выводит на экран список dampened маршруты BGP.

`$ show ip bgp flap-statistics`

Выводит на экран информацию о нестабильных (flapping) маршрутах BGP.

`$ show ip bgp filter-list <name>`

Выводит на экран список маршрутов BGP, разрешенные указанным списком доступа *AS-Path*.

`$ show <ip|ipv6> bgp neighbors <address> advertised-routes`

Выводит на экран список маршрутов BGP, анонсируемых соседу <address>.

`$ show <ip|ipv6> bgp neighbors <address> received-routes`

Выводит на экран список маршрутов BGP, полученных от указанного сосед <address>, до применения политики входящих соединений.

`$ show <ip|ipv6> bgp neighbors <address> routes`

Выводит на экран список маршрутов BGP, которые были получены от указанного соседа <address> после применения фильтрации.

`$ show <ip|ipv6> bgp neighbors <address> dampened-routes`

Выводит на экран dampened маршруты, полученные от BGP соседа <address>.

`$ show <ip|ipv6> bgp regexp <text>`

Выводит на экран список маршрутов BGP, для которых значение AS-Path соответствует заданному регулярному выражению <text>.

`$ show <ip|ipv6> bgp summary`

Выводит на экран состояние всех BGP соединений.

Пример работы команды show <ip|ipv6> bgp summary:

```
fakel@fakel:~$ show <ip|ipv6> bgp summary
IPv4 Unicast Summary:
BGP router identifier 10.0.35.3, local AS number 65000 vrf-id 0
BGP table version 11
RIB entries 5, using 920 bytes of memory
Peers 4, using 82 KiB of memory

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down
  State/PfxRcd
10.0.13.1       4      65000     148     159        0    0    0 02:16:01
  0
10.0.23.2       4      65000     136     143        0    0    0 02:13:21
  0
10.0.34.4       4      65004     161     163        0    0    0 02:16:01
  1
10.0.35.5       4      65005     162     166        0    0    0 02:16:01
  1

Total number of neighbors 4
```

`$ reset <ip|ipv6> bgp <address> [soft [in|out]]`

Сбрасывает BGP соединения с указанным соседом <address>. С аргументом soft эта команда инициирует плавный сброс. Если не используются опции in или out, то запускается как входящее, так и исходящее плавное изменение в настройках конфигурации маршрутов.

`$ reset ip bgp all`

Сбрасывает все BGP соединения на маршрутизаторе.

$ `reset ip bgp dampening`

Сбрасывает информацию о dampened соединения на маршрутизаторе.

$ `reset ip bgp external`

Сбрасывает все внешние BGP соседства для маршрутизатора.

$ `reset ip bgp peer-group <name> [soft [in|out]]`

Сбрасывает BGP соединения с указанной группой соседей. С аргументом `soft` эта команда инициирует плавный сброс. Если не используются опции `in` или `out`, то запускается как входящее, так и исходящее плавное изменение в настройках конфигурации маршрутов.

Инфраструктура RPKI

Описание

Инфраструктура RPKI (Resource Public Key Infrastructure) использует механизмы PKI (Public Key Infrastructure) для обеспечения безопасности процессов маршрутизации. Основная задача инфраструктуры - подтверждение соответствия анонсов маршрутов BGP корректному номеру автономной системы - ASN, которое используется маршрутизатором с поддержкой протокола BGP для валидации каждого маршрута с помощью механизма ROA (Route Origin Authorization). Описание инфраструктуры представлено в спецификации **RFC 6480**[18].

Устройство под управлением **ПО Факел**, которое также является маршрутизатором с поддержкой протокола BGP, способно получать ROA информацию из надежного источника RPKI, который зачастую обозначается как сервер, который выполняет валидацию RPKI, по протоколу RTR (RPKI to Router).

Существуют несколько видов реализации инфраструктура RPKI с открытым исходным кодом:

- Routinator[19] от NLnet Labs, написанный на языке Rust
- GoRTR[20] и OctoRPKI[21] от CloudFlare, написанные на языке Go
- Validator[22] от RIPE NCC, написанный на языке Java

Описание протокола RTR представлено в спецификации **RFC 8210**[23].

Совет

При первом знакомстве с возможностями инфраструктуры RPKI рекомендуется обратиться к руководству, подготовленному NLnet Labs[24], которое позволит быстро получить наиболее важную для понимания информацию. Данное руководство затрагивает практически все аспекты, начиная с самого понятия RPKI, заканчивая вариантами его развертывания в инфраструктуре. Также руководство содержит подробное описание всех возможностей эксплуатации инфраструктуры RPKI.

Ключевые возможности

Текущая реализация RPKI обладает следующими ключевыми возможностями.

- Маршрутизатор с поддержкой протокола BGP может подключаться к одному или нескольким кэш-серверам RPKI для получения надежных префиксов, чтобы установить их соответствие с автономными системами. Может быть обеспечена отказоустойчивость путем конфигурирования различных сокетов сервера со своим приоритетом.
- Если в течение предварительно заданного тайм-аута не удается установить соединение с кэш-сервером RPKI, маршрутизатор будет обрабатывать префиксы без установления соответствия с автономными системами. При этом маршрутизатор и далее будет пытаться установить соединение с кэш-сервером RPKI в фоновом режиме.

[18] https://datatracker.ietf.org/doc/html/rfc6480.html
[19] https://www.nlnetlabs.nl/projects/rpki/routinator/
[20] https://github.com/cloudflare/gortr
[21] https://github.com/cloudflare/cfrpki#octorpki
[22] https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/tools-and-resources
[23] https://datatracker.ietf.org/doc/html/rfc8210.html
[24] https://rpki.readthedocs.io/en/latest/

- По умолчанию использование инфраструктуры RPKI не влияет на выбор наилучшего пути, а именно: ненадежные маршруты по-прежнему будут рассматриваться в данном процессе. Однако маршрутизатор может быть сконфигурирован таким образом, чтобы игнорировать ненадежные префиксы.
- Карты маршрутов могут быть сконфигурированы таким образом, чтобы соответствовать определенному состоянию в рамках валидации RPKI. Это позволяет создавать локальные политики управления маршрутами BGP, основанные на установлении соответствия между префиксами и автономными системами.
- Обновления, получаемые от кэш-серверов RPKI, применяются сразу, приводя также к обновлению соответствующим образом результатов обнаружения наилучшего пути (для этого необходимо активировать опцию «мягкого» обновления).

Импортированные префиксы в результате валидации могут принимать значения:

- *valid* - префикс и номер ASN соответствуют существующей конфигурации ROA. Это означает, что анонс маршрутов является доверенным.
- *invalid* - префикс или его длина, а также номер ASN не соответствуют существующей конфигурации ROA. Это означает, что имеет место либо попытка взлома системы, либо как минимум некорректная ее конфигурация, что приводит к получению недоверенных анонсов маршрутов.
- *notfound* - отсутствует какая-либо конфигурация ROA, которая покрывает данный префикс. К сожалению данная ситуация характерна для почти 80% префиксов IPv4, анонс которых выполняется в зоне DFZ (default-free zone).

Примечание

Если существует потребность в назначении сети глобальных адресов, необходимо обязательно убедиться в том, что префиксы имеют соответствующую конфигурацию ROA, чтобы избежать присвоения им значения notfound при использовании инфраструктуры RPKI. Для большинства номеров ASN это означает необходимость публикации конфигураций ROA в реестре RIR (Regional Internet Registry) (RIPE NCC, APNIC, ARIN, LACNIC, AFRINIC), которая также возникает при планировании анонсов в зоне DFZ. Зачастую большие сети имеют собственные удостоверяющие центры RPKI и серверы для публикации конфигураций ROA, вместо того, чтобы публиковать их в реестре RIR, но данный вопрос находится за рамкам документации на **ПО Факел**. Для более глубокого погружения в данный вопрос рекомендуется ознакомиться со статьей о продукте Krill[25].

Настройка

Алгоритм настройки

Для настройки протокола RPKI на маршрутизаторе нужно настроить ip адрес для подключения к кэш-серверу RPKI, указать приоритет в случае подключения к нескольким кэш-серверам и задать временной интервал для обновления локального кэша RPKI.

[25] https://www.nlnetlabs.nl/projects/rpki/krill/

Пример настройки

Пример, в котором в качестве кэш-сервера RPKI используется решение Routinator[26] с адресом *192.0.2.1*. В данном примере рассматривается построение карт маршрутов на основе описанных выше состояний префиксов. Создается карта маршрутов для получения маршрутов, обнаруженных при импорте. Такой классификатор подразумевает отбрасывание префиксов с состоянием *invalid* и установку более высокого приоритета для префиксов с состоянием *valid* по сравнению с состоянием *notfound*.

Настройка кэш-сервера RPKI:

```
set protocols rpki cache 192.0.2.1 port '3323'
set protocols rpki cache 192.0.2.1 preference '1'
```

Настройка карты маршрутов:

```
set policy route-map ROUTES-IN rule 10 action 'permit'
set policy route-map ROUTES-IN rule 10 match rpki 'valid'
set policy route-map ROUTES-IN rule 10 set local-preference '300'
set policy route-map ROUTES-IN rule 20 action 'permit'
set policy route-map ROUTES-IN rule 20 match rpki 'notfound'
set policy route-map ROUTES-IN rule 20 set local-preference '125'
set policy route-map ROUTES-IN rule 30 action 'deny'
set policy route-map ROUTES-IN rule 30 match rpki 'invalid'
```

После того, как маршрутизатор настроен отбрасывать префиксы с состоянием *invalid*, можно убедиться в корректности его работы путем использования экспериментальной веб-утилиты RPKI Test[27] от NLnet Labs.

Список команд

Основные настройки

- `set protocols rpki polling-period <1-86400>`

  Задает временной интервал для обновления локального кэша RPKI. Значение временного интервала задается в секундах. По умолчанию значение временного интервала равно 300 секунд.

- `set protocols rpki cache <address> port <port>`

  Задает адрес (IPv4, IPv6 или FQDN) <*address*> и номер порта <*port*> для подключения к кэш-серверу RPKI.

- `set protocols rpki cache <address> preference <preference>`

  Задает приоритет <*preference*> для подключения, к кэш-серверу RPKI <*address*>.

Примечание

Выполнение команды *set protocols rpki cache <address> preference <preference>* является обязательным условие в случае подключения к нескольким кэш-серверам RPKI.

[26] https://www.nlnetlabs.nl/projects/rpki/routinator/
[27] https://rpkitest.nlnetlabs.net/

Настройка доступа по SSH

Подключение к кэш-серверу RPKI может осуществляться не только с использованием стека протоколов HTTP/TLS для защиты коммуникаций, но и с использованием протокола SSH.

- `generate ssh client-key /config/auth/id_rsa_rpki`

  Создает ключевую пару для SSH клиента. После того, как ключевая пара для SSH клиента будет создана, можно переходить к настройке самого подключения.

- `set protocols rpki cache <address> ssh username <user>`

  Задает имя пользователя <*user*> для подключения к кэш-серверу <*address*> по протоколу SSH.

- `set protocols rpki cache <address> ssh known-hosts-file <filepath>`

  Задает путь к файлу <*filepath*>, содержащему известные хосты для подключения по SSH к кэш-серверу RPKI <*address*>.

- `set protocols rpki cache <address> ssh private-key-file <filepath>`

  Задает путь к файлу <*filepath*>, который содержит закрытый ключ устройства для подключения к кэш-серверу RPKI <*address*>.

- `set protocols rpki cache <address> ssh public-key-file <filepath>`

  Задает путь к файлу <*filepath*>, который содержит открытый ключ устройства для подключения к кэш-серверу RPKI <*address*>.

Примечание

При подключении к кэш-серверу по протоколу SSH настройка значений параметров *known-hosts-file*, *private-key-file* и *public-key-file* является обязательным.

2.3.2.3 IS-IS

Описание

Протокол IS-IS (Intermediate System to Intermediate System) является протоколом с контролем состояния соединения из категории IGP протоколов для маршрутизации внутри локальной сети. Данный протокол описан в стандарте ISO/IEC 10589:2002[28] и спецификациях **RFC 1195**[29] и **RFC 5308**[30]. Как и протокол OSPF, протокол IS-IS использует алгоритм Дейкстры для сбора данных о топологии сети и определения по этим данным кратчайшего пути до пункта назначения. Маршрутизаторы обмениваются друг с другом информацией о соседствующих узлах. Протокол IS-IS функционирует на канальном (L2) уровне. Адреса, используемые протоколом IS-IS, называются NETs (Network Entity Titles), и могут быть длиной от 8 до 20 байт, но обычно - 10 байт.

Настройка

Алгоритм настройки

1. Перейти в режим Конфигурирования устройства:

```
configure
```

2. Указать NET адрес маршрутизатора:

```
set protocols isis net <network-entity-title>
```

3. Активировать протокол IS-IS на сетевом интерфейсе:

```
set protocols isis interface <interface>
```

4. Установить уровень работы маршрутизатора:

```
set protocols isis level <level-1|level-1-2|level-2>
```

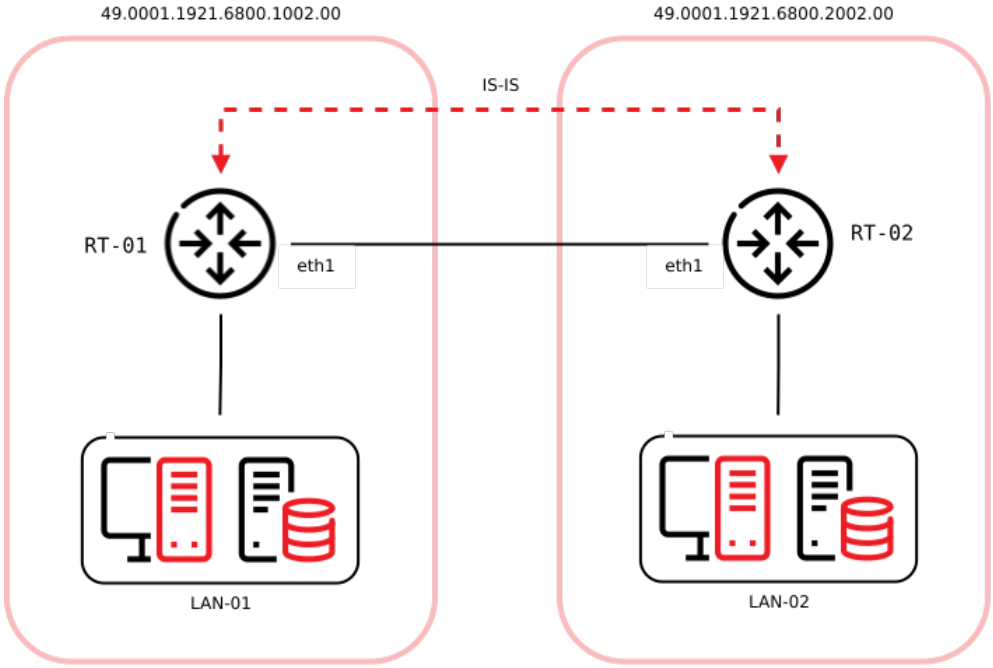
5. Установить уровень работы сетевого интерфейса:

```
set protocols isis interface <interface> circuit-type
  <level-1|level-1-2|level-2-only>
```

Пример настройки

Пример простой конфигурации протокола IS-IS с редистрибуцией маршрутов до непосредственно подключенных (`connected`) к интерфейсам подсетей.

[28] https://www.iso.org/standard/30932.html
[29] https://datatracker.ietf.org/doc/html/rfc1195.html
[30] https://datatracker.ietf.org/doc/html/rfc5308.html



Узел 1:

```
set interfaces dummy dum0 address '203.0.113.1/24'
set interfaces ethernet eth1 address '192.0.2.1/24'
set policy prefix-list EXPORT-ISIS rule 10 action 'permit'
set policy prefix-list EXPORT-ISIS rule 10 prefix '203.0.113.0/24'
set policy route-map EXPORT-ISIS rule 10 action 'permit'
set policy route-map EXPORT-ISIS rule 10 match ip address prefix-list 'EXPORT-ISIS'
set protocols isis interface eth1
set protocols isis net '49.0001.1921.6800.1002.00'
set protocols isis redistribute ipv4 connected level-2 route-map 'EXPORT-ISIS'
```

Узел 2:

```
set interfaces ethernet eth1 address '192.0.2.2/24'
set protocols isis interface eth1
set protocols isis net '49.0001.1921.6800.2002.00'
```

После конфигурирования необходимо убедиться в регистрации маршрутов на **Узле 2**.

```
fakel@F-2:~$ show ip route isis
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

203.0.113.0/24 [115/10] via 192.0.2.1, eth1, 00:03:42
```

Список команд

Основные настройки

- `set protocols isis net <network-entity-title>``

  Задает значение идентификатор NET в стандартном (ISO) формате.

- `set protocols isis interface <interface>`

  Активирует протокола IS-IS на выбранном интерфейсе. Для экземпляра IS-IS необходимо использовать то же имя, что и при настройке процесса IS-IS.

- `set protocols isis dynamic-hostname`

  Активирует механизм DHEM (Dynamic Hostname Exchange Mechanism) динамического сопоставления имени хоста. Описание механизма DHEM представлено в спецификации **RFC 2763**[31].

- `set protocols isis level <level-1|level-1-2|level-2>`

  Устанавливает уровень, на котором будет работать маршрутизатор.

- `set protocols isis lsp-mtu <size>`

  Задает максимальный размер структуры LSP (Label Switched Path) в байтах в диапазоне 128 - 4352.

- `set protocols isis metric-style <narrow|transition|wide>`

  Задает тип метрики, который будет использоваться в работе протокола IS-IS.

  - *narrow* - принимает и генерирует TLV (Type, Length, Value) старого типа;
  - *transition* - принимает и генерирует TLV нового и старого типов;
  - *wide* - принимает и генерирует TLV нового типа.

- `set protocols isis purge-originator`

  Активирует идентификацию инициатора очистки POI (Purge Originator Indetification) согласно спецификации **RFC 6232**[32] посредством добавления TLV с указанной промежуточной системой IS (Intermediate System) для структур LSP, которые не содержат информацию о POI. Если система IS является инициатором очистки, **ПО Факел** добавляет TLV с идентификатором данной система в очередь для очистки.

- `set protocols isis set-attached-bit`

  Задает значение для бита ATT в структуре LSP для режима маршрутизатора станции согласно спецификации **RFC 3787**[33].

- `set protocols isis set-overload-bit`

  Задает значение для бита перегрузки, чтобы исключить прохождение через маршрутизатор транзитного трафика, согласно **RFC 3787**[34].

- `set protocols isis name default-information originate <ipv4|ipv6> level-1`

  Генерирует маршрут по умолчанию для маршрутизатора, который работает на уровне *level-1*.

- `set protocols isis name default-information originate <ipv4|ipv6> level-2`

  Генерирует маршрут по умолчанию для маршрутизатора, который работает на уровне *level-2*.

[31] https://datatracker.ietf.org/doc/html/rfc2763.html
[32] https://datatracker.ietf.org/doc/html/rfc6232.html
[33] https://datatracker.ietf.org/doc/html/rfc3787.html
[34] https://datatracker.ietf.org/doc/html/rfc3787.html

Настройка интерфейсов

- `set protocols isis interface <interface> circuit-type <level-1|level-1-2|level-2>`

  Устанавливает уровень, на котором работает сетевой интерфейс

- `set protocols isis interface <interface> hello-interval <seconds>`

  Задает для сетевого интерфейса временной интервал для отправки hello сообщений (1 - 600).

- `set protocols isis interface <interface> hello-multiplier <seconds>`

  Устанавливает множитель для периода удержания hello сообщений на выбранном интерфейса (2 - 100).

- `set protocols isis interface <interface> hello-padding`

  Настраивает смещение в hello пакетах для учета асимметричных MTU (Maximum Transmission Unit) от различных хостов согласно спецификации **RFC 3719**[35]. Использование команды позволяет избежать преждевременного установления соседства, когда MTU на одном из маршрутизаторов не отвечает требованиям к соседству на другом маршрутизаторе.

- `set protocols isis interface <interface> metric <metric>`

  Устанавливает метрику по умолчанию для цепочки маршрутизаторов (1 - 16777215). Максимальное значение зависит от ширины метрики.

- `set protocols isis interface <interface> network point-to-point`

  Задает тип сети маршрутизаторов, как «точка-точка». По умолчанию тип сети - широковещательная.

- `set protocols isis interface <interface> passive`

  Переводит выбранный интерфейс в пассивный режим.

- `set protocols isis interface <interface> password plaintext-password <text>`

  Настраивает для сетевого интерфейса аутентификацию по заданному паролю.

- `set protocols isis interface <interface> priority <number>`

  Задает для сетевого интерфейса приоритет выбора промежуточной системы DIS (Designated Intermediate System). Приоритет задается числом в диапазоне 0 - 127.

- `set protocols isis interface <interface> psnp-interval <number>`

  Задает временной интервал отправки пакетов PSNP (Partial Sequence Number Packets). Интервал задается в диапазоне 0 - 127.

- `set protocols isis interface <interface> no-three-way-handshake`

  Отключает согласование рукопожатия handshake для соединений «точка-точка» с соседствующими узлами, описание которого представлено в спецификации **RFC 5303**[36]. По умолчанию рукопожатие включено.

[35] https://datatracker.ietf.org/doc/html/rfc3719.html
[36] https://datatracker.ietf.org/doc/html/rfc5303.html

Настройка редистрибуции

- `set protocols isis redistribute ipv4 <route source> level-1`

  Выполняет редистрибуцию маршрутной информации для заданного источника в таблицы, используемые протоколом IS-IS, в качестве данных маршрутизатора станции.

- `set protocols isis redistribute ipv4 <route source> level-2`

  Выполняет редистрибуцию маршрутной информации для заданного источника в таблицы, используемые протоколом IS-IS, в качестве данных маршрутизатора области.

- `set protocols isis redistribute ipv4 <route source> <level-1|level-2> metric <number>`

  Задает метрику для маршрутов, в отношении которых выполнена редистрибуция для заданного источника. Метрика задается в диапазоне 1 - 16777215.

- `set protocols isis redistribute ipv4 <route source> <level-1|level-2> route-map <name>`

  Позволяет использовать определенную карту маршрутов для отбора маршрутов заданного источника, в отношении которых выполняется редистрибуция.

Важно

Операционная система поддерживает шесть источников маршрутной информации: bgp, connected, kernel, ospf, rip, static.

Настройка таймеров

- `set protocols isis lsp-gen-interval <seconds>`

  Задает минимальный временной интервал между генерацией одинаковых структур LSP. Интервал задается в диапазоне 1 - 120.

- `set protocols isis lsp-refresh-interval <seconds>`

  Задает временной интервал обновления структуры LSP. Обычно протокол IS-IS генерирует структуру LSP только при изменении состояния соединения, однако чтобы убедиться в сходимости маршрутных данных на всех маршрутизаторах, структуры LSP генерируются на регулярной основе вне зависимости от состояния соединений. Интервал задается в диапазоне 1 - 65235. По умолчанию - 900.

- `set protocols isis max-lsp-lifetime <seconds>`

  Задает максимальное время жизни структуры LSP. Время задается в диапазоне 350 - 65535. По умолчанию - 1200. Если в течение заданного времени структура LSP не обновляется, она удаляется из базы данных. Так как есть возможность установить временной интервал обновления структуры LSP, он должен быть меньше по значению, чем время жизни структуры, в противном случае структуры LSP будут удаляться до их обновления.

- `set protocols isis spf-interval <seconds>`

  Задает минимальный временной интервал между выполнением процедур поиска кратчайшего пути. Интервал задается в диапазоне 1 - 120.

- `set protocols isis spf-delay-ietf holddown <milliseconds>`
- `set protocols isis spf-delay-ietf init-delay <milliseconds>`
- `set protocols isis spf-delay-ietf long-delay <milliseconds>`
- `set protocols isis spf-delay-ietf short-delay <milliseconds>`
- `set protocols isis spf-delay-ietf time-to-learn <milliseconds>`

  Настраивают механизм конечного автомата, основной задачей которого является контроль времени выполнения процедур поиска кратчайшего пути при регистрации событий, характерных для протоколов IGP. Описание процедуры поиска кратчайшего пути представлено в спецификации **RFC 8405**[37].

[37] https://datatracker.ietf.org/doc/html/rfc8405.html

2.3.2.4 RIP

Описание

Протокол RIP (Routing Information Protocol) является распространенным протоколом из категории IGP протоколов для маршрутизации внутри локальной сети. Протокол RIP был разработан в 1970-х годах компанией Xerox как часть другого протокола маршрутизации - XNS (Xerox Network Systems). Протокол RIP является дистанционно-векторным протоколом и основан на алгоритме поиска кратчайшего пути Беллмана-Форда. Маршрутизатор с поддержкой протокола RIP периодически отправляет соседствующим узлам обновления маршрутных данных, обеспечивая таким образом схождение физической топологии сети. Каждое обновление содержит параметр - дистанцию до определенных подсетей, который рассылается по всем соседствующим узлам (другим маршрутизаторам).

Поддерживаются следующие версии протокола RIP:

- RIPv1 - описание представлено в спецификации **RFC 1058**[38];
- RIPv2 - описание представлено в спецификации **RFC 2453**[39].

Список команд

Основные настройки

- `set protocols rip network <A.B.C.D/M>`

  Активирует протокол RIP на интерфейсе, определенном указанной подсетью.

- `set protocols rip interface <interface>`

  Активирует протокол RIP на интерфейсе, указанном явно по имени. На указанном интерфейсе будут включены передача и получение пакетов по протоколу RIP.

- `set protocols rip neighbor <A.B.C.D>`

  Задает адрес соседствующего узла явно, если соседствующий узел не способен обрабатывать пакеты группового вещания (multicast). Не все маршрутизаторы могут обрабатывать пакеты группового вещания (multicast) - пакеты, которые адресованы целой сети или группе хостов в ней. В таких случаях необходимо устанавливать прямое соединение между маршрутизаторами.

- `set protocols rip passive-interface interface <interface>`

  Переводит интерфейс в пассивный режим. В пассивном режиме все входящие пакеты интерфейс обрабатывает обычным образом и операционная система не отправляет с него ни пакеты группового вещания (multicast) ни одноадресные пакеты (unicast) по протоколу RIP, за исключением пакетов в адрес заданного конкретного соседствующего узла.

- `set protocols rip passive-interface interface default`

  Переводит все интерфейсы в пассивный интерфейс.

Дополнительные настройки

- `set protocols rip default-distance <distance>`

  Задает административную дистанцию по умолчанию (1 - 255).

[38] https://datatracker.ietf.org/doc/html/rfc1058.html
[39] https://datatracker.ietf.org/doc/html/rfc2453.html

Примечание

Маршруты с административной дистанцией 255 фактический определяются операционной системой как отключенные и не устанавливаются в ядро.

- `set protocols rip network-distance <A.B.C.D/M> distance <distance>`

  Задает административную дистанцию для определенного префикса.

- `set protocols rip network-distance <A.B.C.D/M> access-list <name>`

  Задает список доступа для определенного префикса. Команда может использоваться вместе с командой `set protocols rip network-distance <A.B.C.D/M> distance <distance>`.

- `set protocols rip default-information originate`

  Генерирует маршрут по умолчанию.

- `set protocols rip distribute-list access-list <in|out> <number>`

  Накладывает фильтр на путь, определяемый протоколом RIP, с помощью списка доступа. Параметры `in` и `out` позволяют определить направление к которому применяется список доступа.

- `set protocols rip distribute-list interface <interface> access-list <in|out> <number>`

  Накладывает фильтр на путь, определяемый протоколом RIP, с помощью списка доступа. Можно указать интерфейс, к которому применяется список доступа.

- `set protocols rip distribute-list prefix-list <in|out> <name>`

  Накладывает фильтр на путь, определяемый протоколом RIP, с помощью списка префиксов. Параметры `in` и `out` позволяют определить направление к которому применяется список префиксов.

- `set protocols rip distribute-list interface <interface> prefix-list <in|out> <name>`

  Накладывает фильтр на путь, определяемый протоколом RIP, с помощью списка префиксов. Можно указать интерфейс, к которому применяется список префиксов.

- `set protocols rip route <A.B.C.D/M>`

  Задает статический маршрут только для внутреннего использования протоколом RIP.

Примечание

Команда применима только для операционной системы и подсистемы динамической маршрутизации FRR[40]. Рекомендуется использовать с осторожность и только продвинутым пользователям, которые знакомы с деталями технической реализации протокола RIP. В большинстве случаев рекомендуется создавать статический маршрут в операционной системе и выполнять его редистрибуцию в контекст протокола RIP с помощью команды `redistribute static`.

- `set protocols rip timers update <seconds>`

  Задает таймер обновления данных по протоколу RIP в диапазоне 5 - 2147483647. Значение таймера обновления по умолчанию - 30. По прошествии заданного количества секунд протокол RIP

[40] https://frrouting.org/

в инициативном порядке отправляет всем соседствующим узлам сообщение, содержащее полный список маршрутов из таблица маршрутизации.

- `set protocols rip timers timeout <seconds>`

  Задает тайм-аут в по истечении которого маршрут определяется как недоступный. Значение задается в диапазоне 5 - 2147483647, по умолчанию - 180. При этом маршрут остается в таблице маршрутизации еще некоторое время, чтобы соседствующие узлы были проинформированы об этом.

- `set protocols rip timers garbage-collection <seconds>`

  Задает таймер для окончательной очистки недоступных маршрутов. Значение задается в диапазоне 5 - 2147483647, по умолчанию - 120. По прошествии заданного количества секунд недоступный маршрут окончательно удаляется из таблицы маршрутизации.

Редистрибуция маршрутов

- `set protocols rip redistribute <route source>`

  Выполняет редистрибуцию маршрутной информации от определенного источника в таблицы, используемые протоколом RIP.

- `set protocols rip redistribute <route source> metric <metric>`

  Задает метрику для маршрутов, в отношении которых выполняется редистрибуция в диапазоне 1 - 16.

- `set protocols rip redistribute <route source> route-map <name>`

  Настраивает определенную карту для выбора маршрутов, в отношении которых выполняется редистрибуция.

- `set protocols rip default-metric <metric>`

  Изменяет значение метрики по умолчанию (число пересылок между узлами) для маршрутов, в отношении которых выполняется редистрибуция. Значение задается в диапазоне 1 - 16. Значение по умолчанию - 1. Команда не оказывает никакого влияния на маршрут до непосредственно подключенных к маршрутизатора подсетей - *connected*, даже если для него тоже определена редистрибуция посредством команды `redistribute connected`. Чтобы маршруты типа *connected* также подвергались редистрибуции, необходимо использовать команду `redistribute connected metric`.

Важно

Операционная система поддерживает шесть источников маршрутной информации: bgp, connected, kernel, ospf, rip, static.

Настройка интерфейсов

- `set interfaces <inttype> <intname> ip rip authentication plaintext-password <text>`

  Выбирает интерфейс, для которого в рамках протокола RIP будет выполняться базовая аутентификация - аутентификация по паролю. Длина пароля не должна превышать 16 символов.

- `set interfaces <inttype> <intname> ip rip authentication md5 <id> password <text>`

  Задает интерфейс, для которого в рамках протокола RIP будет выполняться аутентификация по ключу MD5. Длина ключа не должна превышать 16 символов.

- `set interfaces <inttype> <intname> ip rip split-horizon disable`

  Отключает на интерфейсе механизм *split horizon*, который обычно используется дистанционно-векторными протоколами для предотвращения петель в маршрутах, во избежание которых операционная система по умолчанию не анонсирует маршруты с интерфейса, на который они были получены ранее.

- `set interfaces <inttype> <intname> ip rip split-horizon poison-reverse`

  Включает обратное анонсирование источнику маршрутной информации маршрута, который был получен ранее от него, но с максимальной административной дистанцией. Такой механизм называется *Poison Reverse*. Если данный механизм работает совместно с механизмом *split horizon*, операционная система анонсирует маршруты с интерфейса, с которого они были получены, как недостижимые.

Мониторинг состояния

- `show ip rip`

  Выводит на экран маршруты, полученные в ходе использования протокола RIP.

  Пример работы команды show ip rip:

```
fakel@fakel:~$ show ip rip
Codes: R - RIP, C - connected, S - Static, O - OSPF, B - BGP
Sub-codes:
(n) - normal, (s) - static, (d) - default, (r) - redistribute,
(i) - interface

      Network        Next Hop    Metric   From        Tag   Time
C(i)  10.0.12.0/24   0.0.0.0     1        self        0
C(i)  10.0.13.0/24   0.0.0.0     1        self        0
R(n)  10.0.23.0/24   10.0.12.2   2        10.0.12.2   0     02:53
```

- `show ip rip status`

  Выводит на экран текущий статус механизма, реализующего протокол RIP. Статус включает такую информацию, как значения таймеров, заданные фильтры, версию протокола RIP, интерфейс, на котором запущен механизм и данные по соседствующим узлам.

  Пример работы команды show ip rip status:

```
fakel@fakel:~$ show ip rip status
Routing Protocol is ”rip”
Sending updates every 30 seconds with +/-50%, next due in 11 seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
Redistributing:
   Default version control: send version 2, receive any version
   Interface   Send   Recv   Key-chain
   eth0        2      1      2
   eth2        2      1      2
Routing for Networks:
   10.0.12.0/24
   eth0
Routing Information Sources:
   Gateway     BadPackets   BadRoutes   Distance   Last Update
   10.0.12.2   0            0           120        00:00:11
Distance: (default is 120)
```

2.3.2.5 Групповая рассылка

Операционная система обеспечивает групповую рассылку IP пакетов посредством поддержки следующих механизмов:

PIM и IGMP

Описание

Протокол PIM может быть настроен на любом интерфейсе каждого маршрутизатора. Каждый маршрутизатор должен иметь заданную точку коммуникационной встречи - *Rendevouz Point*, из которой будут впоследствии выстраиваться однонаправленные общие деревья для дальнейшего их распространения через групповые рассылки.

Трафик от источников в рамках групповой рассылки поступает в точку коммуникационной встречи, после чего получатели данного трафика извлекают его из общего с помощью протокола IGMP.

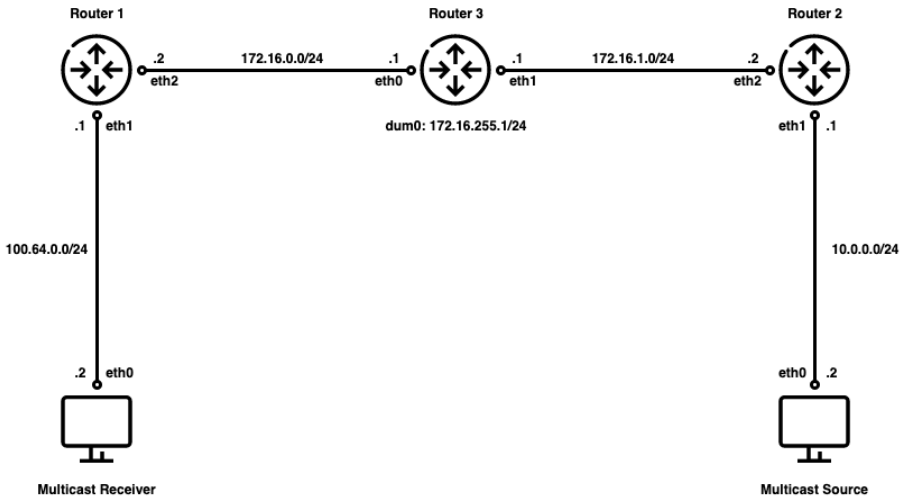
Получатели трафика в рамках групповой рассылки используют протокол IGMP для коммуникаций с ближайшим (локальным) маршрутизатором, поэтому кроме протокола PIM на каждом маршрутизаторе, который является получателем трафика в рамках групповой рассылки, должен быть также настроен протокол IGMP.

Операционная система поддерживает протокол IGMP версии 2 и версии 3, которая предоставляют возможность избирательных групповых рассылок на основе отправителя.

Настройка

Пример настройки

Пример базовой конфигурации групповых рассылок между тремя маршрутизаторами.



Настройка на маршрутизаторе 1:

```
set interfaces ethernet eth2 address '172.16.0.2/24'
set interfaces ethernet eth1 address '100.64.0.1/24'
set protocols ospf area 0 network '172.16.0.0/24'
set protocols ospf area 0 network '100.64.0.0/24'
set protocols igmp interface eth1
set protocols pim interface eth1
set protocols pim interface eth2
set protocols pim rp address 172.16.255.1 group '224.0.0.0/4'
```

Настройка на маршрутизаторе 2:

```
set interfaces ethernet eth1 address '10.0.0.1/24'
set interfaces ethernet eth2 address '172.16.1.2/24'
set protocols ospf area 0 network '10.0.0.0/24'
set protocols ospf area 0 network '172.16.1.0/24'
set protocols pim interface eth1
set protocols pim interface eth2
set protocols pim rp address 172.16.255.1 group '224.0.0.0/4'
```

Настройка на маршрутизаторе 3:

```
set interfaces dummy dum0 address '172.16.255.1/24'
set interfaces ethernet eth0 address '172.16.0.1/24'
set interfaces ethernet eth1 address '172.16.1.1/24'
set protocols ospf area 0 network '172.16.0.0/24'
set protocols ospf area 0 network '172.16.255.0/24'
set protocols ospf area 0 network '172.16.1.0/24'
set protocols pim interface dum0
set protocols pim interface eth0
set protocols pim interface eth1
set protocols pim rp address 172.16.255.1 group '224.0.0.0/4'
```

Список команд

Основные настройки

- `set protocols pim interface <interface-name>`

  Активирует использование протокола PIM на выбранном интерфейсе, чтобы обеспечить взаимодействие с соседствующими узлами в рамках протокола PIM.

- `set protocols pim rp address <address> group <multicast-address/mask-bits>`

  Настраивает точку коммуникационной встречи для протокола PIM с целью агрегации в ней сообщений групповой рассылки. Необходимо указать адрес точки. Можно указать префикс группы в качестве классификатора. Указанные значения должны быть общими для каждого маршрутизатора в сети с использованием протокола PIM.

- `set protocols igmp interface eth1`

  Активирует использованием протокола IGMP на выбранном интерфейсе, чтобы протокол PIM мог использовать получаемые с данного интерфейса отчеты и запросы по протоколу IGMP. По умолчанию используется протокол IGMP версии 3.

Детальные настройки

- `set protocols pim interface <interface> dr-priority <value>`

  Задает для интерфейса приоритет в рамках протокола PIM, который влияет на выбор узла сети в качестве основного маршрутизатора сегмента сети. Чем больше значение, тем выше приоритет при выборе основного маршрутизатора. Значение приоритета задается в диапазоне 1 -

4294967295. Значение по умолчанию по умолчанию - 1),

- `set protocols pim int <interface> hello <seconds>`

  Задает для интерфейса временной интервал отправки сообщений *Hello* в рамках протокола PIM. Значение интервала задается в диапазоне 1 - 180.

- `set protocols pim rp keep-alive-timer <seconds>`

  Задает тайм-аут для передачи потока данных о состоянии (S,G)[41] из базы TIB (Tree Information Base). Значение тайм-аута задается в диапазоне 31 - 60000. 31 секунда выбрана в качестве минимального значения, так как некоторые аппаратные платформы не способны эффективно обрабатывать поток данных в течение более, чем 30 секунд.

- `set protocols igmp interface <interface> join <multicast-address> source <IP-address>`

  Добавляет выбранный интерфейс в группу рассылки путем задания адреса групповой рассылки и IP адреса отправителя.

- `set protocols igmp interface <interface> query-interval <seconds>`

  Задает для интерфейса временной интервал для обработки запросов IGMP от хостов, которые будут использоваться протоколом PIM. Значение временного интервала задается в диапазоне 1 - 1800.

- `set protocols igmp interface <interface> query-max-response-time <deciseconds>`

  Задает для интерфейса тайм-аут для обработки входящих запросов IGMP. Если отчет не поступил на данный интерфейс в течение указанного времени, состояния (S,G) или (*,G)[42] из базы TIB считаются истекшими. Значение тайм-аута задается в диапазоне 10 - 250.

- `set protocols igmp interface <interface> version <version-number>`

  Определяет для выбранного интерфейса, какая версия протокола IGMP - 2 или 3 - будет использоваться. По умолчанию используется протокол IGMP версии 3.

[41] https://tools.ietf.org/html/rfc7761#section-4.1
[42] https://tools.ietf.org/html/rfc7761#section-4.1

IGMP прокси

Описание

IGMP (Internet Group Management Protocol) прокси отправляет сообщения IGMP от имени подключенных клиентов. Конфигурация IGMP прокси должна содержать только один интерфейс типа `upstream` и один или несколько интерфейсов типа `downstream`.

Настройка

Пример настройки

Внутренний (LAN) интерфейс *eth1* доступен только после трансляции адресов (NAT). Чтобы подписать подсеть *10.0.0.0/23*, которая подключена непосредственно к внешнему (WAN) интерфейсу *eth0* на получение групповых рассылок, необходимо сконфигурировать IGMP прокси.

```
set protocols igmp-proxy interface eth0 role upstream
set protocols igmp-proxy interface eth0 alt-subnet 10.0.0.0/23
set protocols igmp-proxy interface eth1 role downstream
```

Список команд

Основные настройки

- `set protocols igmp-proxy interface <interface> role <upstream | downstream>`

  Выбирает интерфейсы , на которых будет настроен IGMP.

  Интерфейсы могут быть настроены в качестве:

  - `upstream` - исходящий интерфейс, который используется для связи с источниками групповых рассылок.
  - `downstream` - интерфейсы, используемые для распространения данных по подсетям получателей групповых рассылок, в которых клиенты могут объединяться в группы для получения данных.

- `set protocols igmp-proxy interface <interface> alt-subnet <network>`

  Указывает альтернативный источник групповых рассылок и сообщений по протоколу IGMP. Адрес подсети должен быть указан в формате `A.B.C.D/M`. По умолчанию маршрутизатор получает данные от источников из той же подсети, что и интерфейс. Если источник групповых рассылок находится в удаленной подсети, ее адрес должен быть указан, чтобы трафик от такого источника был обработан. Это актуально для интерфейсов типа `upstream`, так как обычно источник групповых рассылок находится в удаленной подсети.

- `set protocols igmp-proxy disable-quickleave`

  Отключает режим, в котором система не отправляет сообщение *IGMP Leave* с интерфейса типа `upstream`, если это сообщение уже было получено на любом из интерфейсов типа `downstream`. В этом режиме система также не запрашивает отчеты о принадлежности к группе с интерфейсов типа `downstream`, и, если отчет все же получен, группы не объединяются повторно по отношению к интерфейсу типа `upstream`.

  Необходимо обеспечить работу системы в качестве фактического клиента групповой рассылки по

отношению к интерфейсу `upstream`, поэтому режим должен быть включен. Однако в этом случае велик риск значительного расхода доступной на интерфейсе полосы пропускания.

- `set protocols igmp-proxy disable`

  Отключает IGMP прокси.

- `restart igmp-proxy`

  Перезагружает IGMP прокси.

2.3.2.6 BFD

Описание

Задача протокола BFD (Bidirectional Forwarding Detection) - быстрое определение недоступности соседствующего узла и принятие соответствующих мер. Протокол BFD отправляет значительное количество небольших UDP пакетов, чтобы убедиться, что соседствующих узел по-прежнему доступен. Это позволяет избежать использования лишний раз таймеров, заданных для протоколов BGP и OSPF.

Базовое описание протокола представлено в спецификации **RFC 5880**[43], а описание его расширения - в спецификациях **RFC 5881**[44] и **RFC 5883**[45].

Список команд

Основные настройки

- `set protocols bfd peer <address>`

  Задает IP-адрес соседствующего узла.

- `set protocols bfd peer <address> echo-mode`

  Активирует режим передачи эхо-сообщений для выбранного узла.

- `set protocols bfd peer <address> multihop`

  Определяет соседствующий узел как не подключенный непосредственно.

- `set protocols bfd peer <address> source [address <address> | interface <interface>]`

  Закрепляет выбранный узел за определенным интерфейсом или адресом устройства. Использование команды является обязательным при построении сети с IPv6 адресацией.

- `set protocols bfd peer <address> interval echo-interval <10-60000>`

  Задает временной интервал для получения эхо-сообщений.

- `set protocols bfd peer <address> interval multiplier <2-255>`

  Задает множитель, который будет использован при определении временных интервалов.

- `set protocols bfd peer <address> interval [receive | transmit] <10-60000>`

  Задает временной интервал получения/передачи данных по протоколу BFD. Значение временного интервала задается в миллисекундах.

- `set protocols bfd peer <address> shutdown`

  Определяет соседствующий узел как отключенный.

Настройка BGP BFD

- `set protocols bgp <asn> neighbor <address> bfd`

  Активирует использование протокола BFD для отдельного соседствующего узла в контексте протокола BGP. Когда BFD-узел выходит из строя, он протокол BFD немедленно просит BGP выключить соединение с соседом, а когда он снова поднимается, уведомляет BGP о попытке соединения с ним.

[43] https://datatracker.ietf.org/doc/html/rfc5880.html
[44] https://datatracker.ietf.org/doc/html/rfc5881.html
[45] https://datatracker.ietf.org/doc/html/rfc5883.html

- `set protocols bgp <asn> peer-group <group> bfd`

  Активирует использование протокола BFD для группы соседствующих узлов в контексте протокола BGP. Когда BFD-узел, входящий в группу соседствующих узлов, выходит из строя, он протокол BFD немедленно просит BGP выключить соединение с соседом, а когда он снова поднимается, уведомляет BGP о попытке соединения с ним.

Настройка интеграции с OSPF

- `set interfaces ethernet <interface> ip ospf bfd`

  Активирует BFD в контексте протокола OSPF на интерфейсе. Каждый раз, когда обнаруживается новый сосед, создается BFD-пир для мониторинга состояния соединения и быстрой конвергенции.

Настройка интеграции с ISIS

- `set protocols isis <name> interface <interface> bfd`

  Активирует использование протокола BFD в контексте протокола ISIS интерфейсе. Каждый раз, когда обнаруживается новый сосед, создается BFD-пир для мониторинга состояния соединения и быстрой конвергенции.

Мониторинг состояния

- `show protocols bfd peer`

  Выводит на экран список соседствующих узлов для протокола BFD.

  Пример работы команды show protocols bfd peer:

```
fakel@fakel:~$ show ip rip status
BFD Peers:
   peer 198.51.100.33 vrf default interface eth4.100
      ID: 4182341893
      Remote ID: 12678929647
      Status: up
      Uptime: 1 month(s), 16 hour(s), 29 minute(s), 38 second(s)
      Diagnostics: ok
      Remote diagnostics: ok
      Local timers:
         Receive interval: 300ms
         Transmission interval: 300ms
         Echo transmission interval: 50ms
      Remote timers:
         Receive interval: 300ms
         Transmission interval: 300ms
         Echo transmission interval: 0ms

   peer 198.51.100.55 vrf default interface eth4.101
      ID: 4618932327
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
    Remote ID: 3312345688
    Status: up
    Uptime: 20 hour(s), 16 minute(s), 19 second(s)
    Diagnostics: ok
    Remote diagnostics: ok
    Local timers:
       Receive interval: 300ms
       Transmission interval: 300ms
       Echo transmission interval: 50ms
    Remote timers:
       Receive interval: 300ms
       Transmission interval: 300ms
       Echo transmission interval: 0ms
```

2.3.3 Политика маршрутизации

2.3.3.1 Описание

Политики маршрутизации могут использоваться для указания самому маршрутизатору или его соседствующим узлам, какие маршруты и их атрибуты должны быть помещены в таблицу маршрутизации.

Существуют различные варианты политик маршрутизации. Некоторые примеры приведены ниже.

- Установить некоторую метрику для маршрутов, полученных от конкретного соседствующего узла.
- Установить значения для некоторых атрибутов (например, `AS Path` или `Community`) для анонсируемых соседствующим узлам маршрутов.
- Установить предпочтение для маршрутов определенного протокола маршрутизации перед маршрутами другого протокола, работающего на том же маршрутизаторе.

Механизм PBR (Policy-Based Routing) позволяет назначать трафик для различных таблиц маршрутизации. Трафик может быть сопоставлен с помощью стандартных атрибутов 5-tuple (адрес отправителя, адрес получателя, порт отправителя, порт получателя, протокол).

2.3.3.2 Настройка

Пример настройки

Настройка PBR начинается с создания политики маршрутизации и применения созданной политики к механизму BGP:

```
# Create policy
set policy route-map setmet rule 2 action 'permit'
set policy route-map setmet rule 2 set as-path-prepend '2 2 2'

# Apply policy to BGP
set protocols bgp 1 neighbor 203.0.113.2 address-family ipv4-unicast route-map
  import 'setmet'
set protocols bgp 1 neighbor 203.0.113.2 address-family ipv4-unicast
  soft-reconfiguration 'inbound'
```

Используя команду `soft-reconfiguration`, можно добиться обновления политики без переключения соседствующего узла.

Далее - выполняется наполнение базы маршрутов по данным от соседствующих узлов до применения политики маршрутизации.

```
fakel@fakel:~$ show ip bgp
BGP table version is 0, local router ID is 192.168.56.101
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
*>  198.51.100.3/32  203.0.113.2           1             0 2 i < Path
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
Total number of prefixes 1
```

После применения политики маршрутизации убеждаемся в корректности маршрутной информации.

```
fakel@fakel:~$ sho ip b
BGP table version is 0, local router ID is 192.168.56.101
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, R Removed
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop            Metric LocPrf Weight Path
*>  198.51.100.3/32  203.0.113.2           1             0 2 2 2 2 i

Total number of prefixes 1
```

В результате можно наблюдать более длинный путь до автономной системы (значение атрибута AS Path).

В разделе *Примеры настройки политики маршрутизации* (страница 355) представлено описание других примеров для настройки политики маршрутизации в **ПО Факел**.

2.3.3.3 Список команд

Основные настройки

Примеры настройки политики маршрутизации

Прозрачный прокси

В следующем примере показано, как с помощью операционной системы можно перенаправить веб-трафик на внешний прозрачный прокси.

Настройка правила для перенаправления веб-трафика:

```
set policy route FILTER-WEB rule 1000 destination port 80
set policy route FILTER-WEB rule 1000 protocol tcp
set policy route FILTER-WEB rule 1000 set table 100
```

В результате создается политика маршрутизации `FILTER-WEB` с одним правилом, устанавливающим таблицу маршрутизации для соответствующего трафика (TCP порт с номером 80) с идентификатором *100* вместо таблицы маршрутизации по умолчанию.

Создание таблицы маршрутизации с идентификатором *100* и добавление в нее нового шлюза по умолчанию, который будет использоваться трафиком, соответствующим заданной политике маршрутизации:

```
set protocols static table 100 route 0.0.0.0/0 next-hop 10.255.0.2
```

Ознакомиться в результатом создания таблицы маршрутизации с идентификатором *100* можно с помощью команды `show ip route table 100`.

Последний шаг - применение политики маршрутизации к исходящему трафику на внутреннем (LAN) интерфейсе:

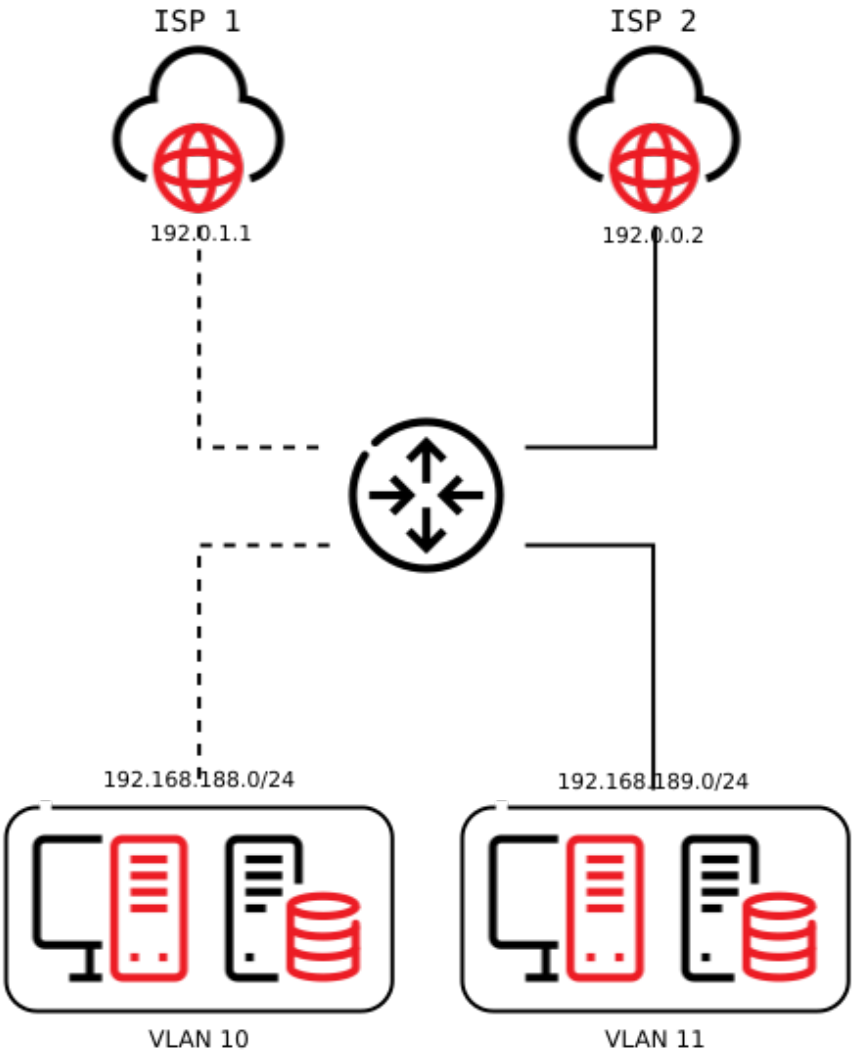
```
set interfaces ethernet eth1 policy route FILTER-WEB
```

Подключение к нескольким провайдерам

Функционирование механизма PBR операционной системы состоит в сопоставлении диапазонов IP-адресов источников и пересылке трафика с использованием различных таблиц маршрутизации.

Список таблиц маршрутизации, используемых в примере далее, включает:

- `table 10` - таблица маршрутизации для виртуальной сети *VLAN 10* (192.168.188.0/24);
- `table 11` - таблица маршрутизации для виртуальной сети *VLAN 11* (192.168.189.0/24);
- `main` - таблица маршрутизации, используемая компонентами **ПО Факел** и другими интерфейсами, не используемые механизмом PBR.



Добавление маршрутов по умолчанию в таблицы маршрутизации `table 10` и `table 11`:

```
set protocols static table 10 route 0.0.0.0/0 next-hop 192.0.2.1
set protocols static table 11 route 0.0.0.0/0 next-hop 192.0.2.2
```

Добавление политики маршрутизации, соответствующую адресам отправителей заданных виртуальных сетей VLAN с помощью следующих команд:

```
set policy route PBR rule 20 set table '10'
set policy route PBR rule 20 description 'Route VLAN10 traffic to table 10'
set policy route PBR rule 20 source address '192.168.188.0/24'

set policy route PBR rule 30 set table '11'
set policy route PBR rule 30 description 'Route VLAN11 traffic to table 11'
set policy route PBR rule 30 source address '192.168.189.0/24'
```

Применение политики маршрутизации к **входящему** трафику на интерфейсах VLAN:

```
set interfaces ethernet eth0 vif 10 policy route 'PBR'
set interfaces ethernet eth0 vif 11 policy route 'PBR'
```

Опционально можно исключить трафик между виртуальными сетями VLAN (межу *VLAN 10* и *VLAN 11*) из использования механизмом PBR:

```
set policy route PBR rule 10 description 'VLAN10 <-> VLAN11 shortcut'
set policy route PBR rule 10 destination address '192.168.188.0/24'
set policy route PBR rule 10 destination address '192.168.189.0/24'
set policy route PBR rule 10 set table 'main'
```

Указанные выше команды разрешают хостам из виртуальных сетей *VLAN 10* и *VLAN 11* взаимодействовать друг с другом посредством таблицы маршрутизации `main`.

Локальный маршрут

Следующий пример позволяет операционной системе использовать механизм PBR для трафика, отправителем которого является сам маршрутизатор. Такое решение подходит для нескольких провайдеров, и маршрутизатор будет отвечать с того же интерфейса, с которого был получен пакет. Также это решение применимо, если мы хотим, чтобы один VPN туннель проходил через одного провайдера, а второй - через другого.

- `203.0.113.0.254` - IP адрес на интерфейсе `eth1` в направлении провайдера *ISP1*.
- `192.168.2.254` - IP адрес на интерфейсе `eth2` в направлении провайдера *ISP2*.
- `table 10` - таблица маршрутизации, используемая для взаимодействия с провайдером *ISP1*.
- `table 11` - таблица маршрутизации, используемая для взаимодействия с провайдером *ISP2*

Настройка PBR для локального маршрута:

```
set policy local-route rule 101 set table '10'
set policy local-route rule 101 source '203.0.113.0.254'
set policy local-route rule 102 set table '11'
set policy local-route rule 102 source '192.0.2.254'
set protocols static table 10 route '0.0.0.0/0' next-hop '203.0.113.0.1'
set protocols static table 11 route '0.0.0.0/0' next-hop '192.0.2.2'
```

Необходимо добавить несколько IP адресов отправителей в одно правило с одинаковым приоритетом:

```
set policy local-route rule 101 set table '10'
set policy local-route rule 101 source '203.0.113.0.254'
set policy local-route rule 101 source '203.0.113.0.253'
set policy local-route rule 101 source '198.51.100.0/24'
```

2.3.4 MPLS

2.3.4.1 Описание

Механизм MPLS (Multi-Protocol Label Switching) представляет собой механизм перенаправления IP пакетов, отличающийся от стандартного. Вместо IP адресов для принятия решения о перенаправлении пакета на исходящий интерфейс маршрутизатор использует специальный заголовок длиной 32 бита (4 байта), который называется MPLS меткой. Данная метка размещается между заголовком Ethernet фрейма (L2) и заголовком IP пакета (L3). Возможно как статическое, так и динамическое размещение MPLS меток, однако в настоящем разделе рассматривается только динамическое размещение с использованием одного из подходящих для данных целей протоколов/механизмов: протокола LDP (Label Distribution Protocol), протокола RSVP (Resource Reservation Protocol), механизма SR (Segment Routing) с использованием протоколов OSPF или IS-IS. Указанные протокола используются фактически для формирования одноадресного пути до пункта назначения в сети, который идеологически схож с туннелем и именуется как коммутируемый на основе меток путь - LSP. Для упрощения понимания работы LSP можно провести его сравнение с GRE (Generic Routing Encapsulation) туннелем. Они отличаются с точки зрения технической реализации, но схожи между собой в части управления движением пакета через туннель. Рекомендуется рассматривать механизм MPLS как механизм туннелирования, позволяющий доставлять по сети различные типы пакетов, значительно упрощающий проектирование потоков и схем движения трафика в сети за счет использования протокола RSVP или механизма SR, и в основном упрощающий организацию движения потоков данных как внутри сети, так и при межсетевом взаимодействии.

Для получения более подробной информации о том, как работает механизм MPLS, рекомендуется ознакомиться с источником[46].

Примечание

Поддержка механизма MPLS в операционной системе имеет ряд ограничений. Например, механизм MPLS нельзя использовать совместно с механизмами защиты коммуникаций L3 VPN, L2 VPN, а также с механизмом динамического построения VPN сетей. Протокол RSVP нельзя использовать как базовый протокол маршрутизации в стеке по отношению к транспортному протоколу (ограничение компонента FRR[47], интегрированного в систему). В настоящий момент устройство под управлением операционной системы может быть сконфигурировано как MPLS маршрутизатор на последней миле.

Протокол LDP

Архитектура механизма MPLS не предусматривает использование одного конкретного протокола для определения LSP. Операционная система использует протокол LDP в реализации, заложенной в компонент FRR[48] и соответствующей спецификации **RFC 5036**[49]

Протокол LDP представляет собой сигнальный протокол, использующий в качестве транспорта TCP и динамически распределяющий MPLS метки, создающий таким образом LSP. Протокол LDP не является протоколом маршрутизации сам по себе, но он использует данные, полученные в результате работы других протоколов маршрутизации, для принятия решения о перенаправлении пакетов. Для корректно-

[46] https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching
[47] https://frrouting.org/
[48] https://frrouting.org/
[49] https://datatracker.ietf.org/doc/html/rfc5036.html

го использования протокола LDP на маршрутизаторе необходимо, чтобы другие маршрутизаторы также использовали данный протокол.

Для того, чтобы протокол LDP на маршрутизаторе обменивался анонсами меток с другими маршрутизаторами, устанавливается сессия TCP как с автоматически обнаруживаемыми, так и статически заданными маршрутизаторами. Протокол LDP предусматривает попытку установления TCP сессии с другими маршрутизаторами, используя для этого транспортные адреса, поэтому необходимо убедиться в том, что эти адреса присутствуют в таблице маршрутизации и являются достижимыми для обеспечения движения трафика.

Рекомендуется использовать одинаковые адреса для идентификации маршрутизатора в контексте протокола LDP и для автоматически обнаруживаемых маршрутизаторов, которые должны быть явно заданы в конфигурации протокола LDP в операционной системе.

Также необходимо помнить, что принципиальная реализация протокола LDP схожа с реализацией протокола BGP в том, что она использует TCP в качестве транспорта. Однако в отличие от протокола BGP реализация LDP не предусматривает возможность обновления оперативных данных. Это означает, что в случае изменения топологии соседствующих узлов необходимо вручную изменить конфигурацию протокола LDP, чтобы он функционировал корректно.

2.3.4.2 Настройка

Пример настройки

Пример настройки механизма MPLS:

```
set protocols ospf area 0 network '192.168.255.252/32'
set protocols ospf area 0 network '192.168.0.5/32'
set protocols ospf parameters router-id '192.168.255.252'
set protocols mpls interface 'eth1'
set protocols mpls ldp discovery transport-ipv4-address '192.168.255.252'
set protocols mpls ldp interface 'eth1'
set protocols mpls ldp interface 'lo'
set protocols mpls ldp router-id '192.168.255.252'
set interfaces ethernet eth1 address '192.168.0.5/31'
set interfaces loopback lo address '192.168.255.252/32'
```

2.3.4.3 Список команд

Основные настройки

- `set protocols mpls interface <interface>`

  Активирует использование механизма MPLS для выбранного интерфейса.

- `set protocols mpls ldp interface <interface>`

  Активирует использование протокола LDP на выбранном интерфейсе.

- `set protocols mpls ldp router-id <address>`

  Задет IP адрес, используемый в качестве идентификатора маршрутизатора на устройстве.

- `set protocols mpls ldp discovery transport-ipv4-address <address>`

  Задает IPv4 адрес в качестве транспортного, используемого протоколом LDP.

- `set protocols mpls ldp discovery transport-ipv6-address <address>`

  Задает IPv6 адрес в качестве транспортного, используемого протоколом LDP.

- `set protocols mpls ldp neighbor <address> password <password>`

  Настраивает параметры аутентификации для соседствующих узлов в контексте протокола LDP. Необходимо указать адрес соседствующего узла и пароль, который должен быть общим для соседствующих узлов.

- `set protocols mpls ldp neighbor <address> session-holdtime <seconds>`

  Задает время удержания сессии для соседствующих узлов в контексте протокола LDP. Необходимо указать адрес соседствующего узла и время удержания сессии в секундах. Чтобы изменения вступили в силу, перезагрузите соседствующий узел.

- `set protocols mpls ldp neighbor <address> ttl-security <disable | hop count>`

  Активирует механизм контроля TTL (Time-To-Live) для соседствующих узлов в контексте протокола LDP (включить механизм и задать количество пересылок между узлами, отключить механизм). По умолчанию количество пересылок - 255, что эквивалентно максимальному значению TTL.

- `set protocols mpls ldp discovery hello-ipv4-interval <seconds>`

  Задает временной интервал для отправки hello сообщений для протокола IPv4.

- `set protocols mpls ldp discovery hello-ipv4-holdtime <seconds>`

  Задает временной интервал отправки hello сообщений для протокола IPv4.

- `set protocols mpls ldp discovery hello-ipv6-interval <seconds>`

  Задает временной интервал удержания hello сообщений для протокола IPv4.

- `set protocols mpls ldp discovery hello-ipv6-holdtime <seconds>`

  Задает временной интервал удержания hello сообщений для протокола IPv4.

- `set protocols mpls ldp discovery session-ipv4-holdtime <seconds>`

  Задает временной интервал удержания TCP сессий для протокола IPv4.

- `set protocols mpls ldp discovery session-ipv6-holdtime <seconds>`

  Задает временной интервал удержания TCP сессий для протокола IPv6.

- `set protocols mpls ldp import ipv4 import-filter filter-access-list <access list number>`

  Настраивает импорт классов эквивалентности - FEC (Forwarding Equivalence Class) от соседствующих узлов в контексте протокола LDP для протокола IPv4.

- `set protocols mpls ldp import ipv6 import-filter filter-access-list6 <access list number>`

  Настраивает импорт классов эквивалентности - FEC от соседствующих узлов в контексте протокола LDP для протокола IPv6.

- `set protocols mpls ldp export ipv4 export-filter filter-access-list <access list number>`

  Настраивает экспорт классов FEC для соседствующих узлов в контексте протокола LDP для протокола IPv4.

- `set protocols mpls ldp export ipv6 export-filter filter-access-list6 <access list number>`

Настраивает экспорт классов FEC для соседствующих узлов в контексте протокола LDP для протокола IPv6.

- `set protocols mpls ldp export ipv4 explicit-null`

  Управляет анонсом классов FEC с меткой 0 для протокола IPv4. Метка 0 используется для явных нулевых операций в контексте протокола LDP.

- `set protocols mpls ldp export ipv6 explicit-null`

  Управляет анонсом классов FEC с меткой 0 для протокола IPv6. Метка 0 используется для явных нулевых операций в контексте протокола LDP.

- `set protocols mpls ldp allocation ipv4 access-list <access list number>`

  Задает фильтры, которые позволяют контролировать процесс размещения локальных классов FEC в контексте протокола LDP для протокола IPv4.

- `set protocols mpls ldp allocation ipv6 access-list6 <access list number>`

  Задает фильтры, которые позволяют контролировать процесс размещения локальных классов FEC в контексте протокола LDP для протокола IPv6.

- `set protocols mpls ldp parameters cisco-interop-tlv`

  Активирует режим использования формата данных, не соответствующего требованиям компании Cisco, который подразумевает отправку и интерпретацию структур TLV для коммуникаций по протоколу LDP поверх протокола IPv6. Описание данной особенности представлено в спецификации **RFC 7552**[50].

- `set protocols mpls ldp parameters ordered-control`

  Активирует режим упорядоченного распространения меток. По умолчанию компонент FRR[51] в составе операционной системы использует режим независимого распространения меток. Описание данной особенности представлено в спецификации **RFC 5036**[52].

- `set protocols mpls ldp parameters transport-prefer-ipv4`

  Активирует режим использования протокола IPv4 в качестве предпочтительного для TCP коммуникаций между соседствующими маршрутизаторами в контексте протокола LDP. Рекомендуется использовать эту команду в случае, если на интерфейсе задан как IPv4 адрес, так и IPv6 адрес.

- `set protocols mpls ldp targeted-neighbor ipv4 enable`

  Активирует режим принятия таргетированных LDP сессий данным маршрутизатором для протокола IPv4. В этом режиме маршрутизатор будет отвечать на любые попытки установления сессий, адресованных именно ему, за исключением локальных TCP соединений.

- `set protocols mpls ldp targeted-neighbor ipv6 enable`

  Активирует режим принятия таргетированных LDP сессий данным маршрутизатором для протокола IPv6. В этом режиме маршрутизатор будет отвечать на любые попытки установления сессий, адресованных именно ему, за исключением локальных TCP соединений.

- `set protocols mpls ldp targeted-neighbor ipv4 address <address>`

  Активирует режим инициирования таргетированных LDP сессий данным маршрутизатором для

[50] https://datatracker.ietf.org/doc/html/rfc7552.html
[51] https://frrouting.org/
[52] https://datatracker.ietf.org/doc/html/rfc5036.html

протокола IPv4. В этом режиме маршрутизатор будет инициировать установление сессий с другим конкретным маршрутизатором.

- `set protocols mpls ldp targeted-neighbor ipv6 address <address>`

  Активирует режим инициирования таргетированных LDP сессий данным маршрутизатором для протокола IPv6. В этом режиме маршрутизатор будет инициировать установление сессий с другим конкретным маршрутизатором.

- `set protocols mpls ldp targeted-neighbor ipv4 hello-holdtime <seconds>`

  Задает временной интервал удержания hello сообщений для протокола IPv4 определенным соседствующим маршрутизаторам, которые являются адресатами таргетированных LDP сессий.

- `set protocols mpls ldp targeted-neighbor ipv4 hello-interval <seconds>`

  Задает временной интервал отправки hello сообщений для протокола IPv4 определенным соседствующим маршрутизаторам, которые являются адресатами таргетированных LDP сессий.

- `set protocols mpls ldp targeted-neighbor ipv6 hello-holdtime <seconds>`

  Задает временной интервал удержания hello сообщений для протокола IPv6 определенным соседствующим маршрутизаторам, которые являются адресатами таргетированных LDP сессий.

- `set protocols mpls ldp targeted-neighbor ipv6 hello-interval <seconds>`

  Задает временной интервал отправки hello сообщений для протокола IPv6 определенным соседствующим маршрутизаторам, которые являются адресатами таргетированных LDP сессий.

- `reset mpls ldp neighbor <IPv4 or IPv6 address>`

  Сбрасывает LDP сессии, установленные с определенным соседствующим маршрутизатором в контексте протокола LDP по указанному адресу.

Мониторинг состояния

- `show mpls ldp binding`

  Выводит на экран информацию о метках из базы LIB (Label Information Base).

- `show mpls ldp discovery`

  Выводит на экран информацию о соседствующих маршрутизаторах в контексте протокола LDP, обнаруженных путем рассылки hello сообщений.

- `show mpls ldp interface`

  Выводит на экран информацию о текущем статусе протокола LDP на интерфейсах.

- `show mpls ldp neighbor`

  Выводит на экран общую информацию о соседствующих маршрутизаторах в контексте протокола LDP.

- `show mpls ldp neighbor detail`

  Выводит на экран детальную информацию о соседствующих маршрутизаторах в контексте протокола LDP.

2.3.5 Виртуальная маршрутизация

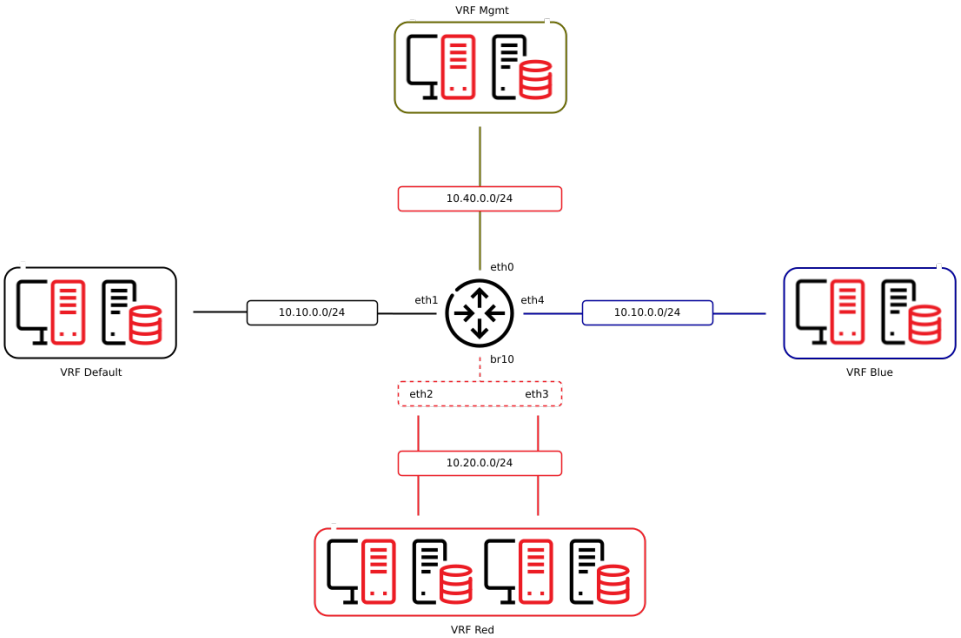
2.3.5.1 Описание

VRF (Virtual Routing and Forwarding) – технология, позволяющая реализовывать на базе одного физического маршрутизатора несколько виртуальных – каждого со своей независимой таблицей маршрутизации. Преимуществом виртуальной маршрутизации является полная изоляция маршрутов как между двумя виртуальными маршрутизаторами, так и между виртуальным и реальным. Устройства VRF совместно с правилами обработки трафика на уровне IP (*IP Rules*) позволяют создать виртуальные маршрутизаторы. При создании устройства VRF создается ассоциированная с ним таблица маршрутизации. После создания устройства VRF его необходимо привязать к определенному сетевому интерфейсу.

2.3.5.2 Настройка

Пример настройки

Пример топологии с использованием экземпляров VRF.



- Рабочая станция *PC1* располагается в зоне VRF *default* и выполняет роль файлового сервера.
- Рабочая станция *PC2* располагается в зоне VRF *blue* которая соответствует отделу разработки.
- Рабочие станции *PC3* и *PC4* подключены к мосту (bridge) на маршрутизаторе *R1*, который располагается в зоне VRF *red*, соответствующей отделу кадров.
- Маршрутизатор *R1* управляется через выделенную сеть, которая располагается в зоне VRF *mgmt*.

Применение настроек на маршрутизаторе:

```
set interfaces bridge br10 address '10.30.0.254/24'
set interfaces bridge br10 member interface eth3
set interfaces bridge br10 member interface eth4
set interfaces bridge br10 vrf 'red'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set interfaces ethernet eth0 address 'dhcp'
set interfaces ethernet eth0 vrf 'mgmt'
set interfaces ethernet eth1 address '10.0.0.254/24'
set interfaces ethernet eth2 address '10.20.0.254/24'
set interfaces ethernet eth2 vrf 'blue'

set protocols static interface-route 10.20.0.0/24 next-hop-interface eth2
 next-hop-vrf 'blue'
set protocols static interface-route 10.30.0.0/24 next-hop-interface br10
 next-hop-vrf 'red'
set protocols vrf blue static interface-route 10.0.0.0/24 next-hop-interface eth1
 next-hop-vrf 'default'
set protocols vrf red static interface-route 10.0.0.0/24 next-hop-interface eth1
 next-hop-vrf 'default'

set service ssh disable-host-validation
set service ssh vrf 'mgmt'

set system domain-name 'fakel.net'
set system host-name 'R1'
set system name-server 'eth0'

set vrf name blue table '3000'
set vrf name mgmt table '1000'
set vrf name red table '2000'
```

После применения настрое на физическом маршрутизаторе для каждого экземпляра VRF появится своя таблица маршрутизации:

Таблица маршрутизации по умолчанию:

```
admin@R1:~$ show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

C>* 10.0.0.0/24 is directly connected, eth1, 00:07:44
S>* 10.20.0.0/24 [1/0] is directly connected, eth2 (vrf blue), weight 1, 00:07:38
S>* 10.30.0.0/24 [1/0] is directly connected, br10 (vrf red), weight 1, 00:07:38
```

Таблица маршрутизации Red:

```
admin@R1:~$ show ip route vrf red
Codes: K - kernel route, C - connected, S - static, R - RIP,
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

VRF red:
K>* 0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 00:07:57
S>* 10.0.0.0/24 [1/0] is directly connected, eth1 (vrf default), weight 1, 00:07:40
C>* 10.30.0.0/24 is directly connected, br10, 00:07:54
```

Таблица маршрутизации Blue:

```
admin@R1:~$ show ip route vrf blue
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup

VRF blue:
K>* 0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 00:08:00
S>* 10.0.0.0/24 [1/0] is directly connected, eth1 (vrf default), weight 1, 00:07:44
C>* 10.20.0.0/24 is directly connected, eth2, 00:07:53
```

2.3.5.3 Список команд

Основные настройки

- `set vrf name <name>`

  Создает новый экземпляр VRF с именем указанным в параметре *<name>*. Заданное имя используется в дальнейшем при организации привязки сетевых интерфейсов к созданному экземпляру VRF.

- `set vrf name <name> table <id>`

  Связывает таблицу маршрутизации определенного идентификатора *<id>* с экземпляром VRF *<name>*.

Примечание

Заданный идентификатор таблицы маршрутизации не может быть изменен после того, как он был привязан к экземпляру VRF. Это возможно только при удалении экземпляра VRF и созданию нового экземпляра VRF.

- `set vrf bind-to-all`

  Активирует работу сервисов TCP и UDP, запущенных в контексте экземпляра VRF по умолчанию, также в контекстах всех остальных экземпляров VRF, не смотря на отсутствие фактической привязки к данным экземплярам VRF.

Примечание

По умолчанию при назначении портов все свободные сокеты связываются с экземпляром VRF по умолчанию. Такая конфигурация будет игнорироваться сетевыми пакетами, поступающими на сетевой интерфейс, связанный с другим экземпляром VRF.

• `set interfaces <dummy | ethernet | bonding | bridge | pppoe> <interface> vrf <name>`

Связывает сетевой интерфейс <*interface*> с экземпляром VRF <*name*>.

Настройка маршрутизации

Примечание

ПО Факел поддерживает использование устройств VRF только совместно со статической маршрутизацией. Использование совместно с динамической маршрутизацией не поддерживается.

Статические маршруты

• `set protocols vrf <name> static route <subnet> next-hop <address>`

Задает адрес <*address*> следующего маршрутизатора для статического маршрута IPv4 <*subnet*> в экземпляре VRF <*name*>. Для экземпляра VRF можно создавать несколько статических маршрутов IPv4.

• `set protocols vrf <name> static route <subnet> next-hop <address> disable`

Отключает использование записи со статическим маршрутом IPv4 <*subnet*> в экземпляре VRF <*name*>.

• `set protocols vrf <name> static route <subnet> next-hop <address> distance <distance>`

Задает административную дистанцию <*distance*> до следующего маршрутизатора <*address*> для маршрута IPv4 <*subnet*> в экземпляре VRF <*name*>. Маршруты с наименьшей административной дистанцией - в приоритете перед маршрутами с наибольшей административной дистанцией. Административную дистанцию можно определить в диапазоне от *1* до *255*. Значение административной дистанции по умолчанию - *1*.

• `set protocols vrf <name> static route6 <subnet> next-hop <address>`

Задает адрес <*address*> следующего маршрутизатора для статического маршрута IPv6 <*subnet*> в экземпляре VRF <*name*>. Для устройства VRF можно создавать несколько статических маршрутов IPv6.

• `set protocols vrf <name> static route6 <subnet> next-hop <address> disable`

Отключает использование записи со статическим маршрутом IPv6 <*subnet*> в экземпляре VRF <*name*>.

• `set protocols vrf <name> static route6 <subnet> next-hop <address> distance <distance>`

Задает административную дистанцию <*distance*> до следующего маршрутизатора <*address*> для

маршрута IPv6 <*subnet*> в экземпляре VRF <*name*>. Маршруты с наименьшей административной дистанцией - в приоритете перед маршрутами с наибольшей административной дистанцией. Административную дистанцию можно определить в диапазоне от *1* до *255*. Значение административной дистанции по умолчанию - *1*.

Примечание

Маршруты с административной дистанцией 255 фактически отключены и не заносятся в ядро **ПО Факел**.

Утечка маршрутов

• `set protocols vrf <name> static route <subnet> next-hop <address> next-hop-vrf <default | vrf-name>`

Добавляет статический маршрут IPv4 в таблицу маршрутизации экземпляра VRF <*name*> для доступа к подсети <*subnet*> через следующий маршрутизатор <*address*> с адресом, принадлежащим другому экземпляру VRF <*default* | *vrf-name*>. Используется в случае, если есть общие сервисы или маршруты, которые должны быть общими для нескольких экземпляров VRF.

• `set protocols vrf <name> static route6 <subnet> next-hop <address> next-hop-vrf <default | vrf-name>`

Добавляет статический маршрут IPv6 в таблицу маршрутизации экземпляра VRF <*name*> для доступа к подсети <*subnet*> через следующий маршрутизатор <*address*> с адресом, принадлежащим другому экземпляру VRF <*default* | *vrf-name*>. Используется в случае, если есть общие сервисы или маршруты, которые должны быть общими для нескольких экземпляров VRF.

Маршруты для интерфейсов

• `set protocols vrf <name> static interface-route <subnet> next-hop-interface <interface>`

Определяет интерфейс <*interface*> следующего маршрутизатора для статического маршрута IPv4 <*subnet*> на основе интерфейса для экземпляра VRF <*name*>. Интерфейс <*interface*> будет являться интерфейсом следующего узла, через который будет направляться трафик для заданной подсети <*subnet*>.

• `set protocols vrf <name> static interface-route <subnet> next-hop-interface <interface> disable`

Отключает использование статического маршрута IPv4 <*subnet*> на основе интерфейса <*interface*> для экземпляра VRF <*name*>.

• `set protocols vrf <name> static interface-route <subnet> next-hop-interface <interface> distance <distance>`

Задает административную дистанцию <*distance*> до следующего маршрутизатора на основе интерфейса <*interface*> для маршрута IPv4 <*subnet*> в экземпляре VRF <*name*>. Маршруты с наименьшей административной дистанцией - в приоритете перед маршрутами с наибольшей административной дистанцией. Административную дистанцию можно определить в диапазоне от *1* до *255*. Значение административной дистанции по умолчанию - *1*.

- `set protocols vrf <name> static interface-route6 <subnet> next-hop-interface <interface>`

  Определяет интерфейс <*interface*> следующего маршрутизатора для статического маршрута IPv6 <*subnet*> на основе интерфейса для экземпляра VRF <*name*>. Интерфейс <*interface*> будет являться интерфейсом следующего узла, через который будет направляться трафик для заданной подсети <*subnet*>.

- `set protocols vrf <name> static interface-route6 <subnet> next-hop-interface <interface> disable`

  Отключает использование статического маршрута IPv6 <*subnet*> на основе интерфейса <*interface*> для экземпляра VRF <*name*>.

- `set protocols vrf <name> static interface-route6 <subnet> next-hop-interface <interface> distance <distance>`

  Задает административную дистанцию <*distance*> до следующего маршрутизатора на основе интерфейса <*interface*> для маршрута IPv6 <*subnet*> в экземпляре VRF <*name*>. Маршруты с наименьшей административной дистанцией - в приоритете перед маршрутами с наибольшей административной дистанцией. Административную дистанцию можно определить в диапазоне от *1* до *255*. Значение административной дистанции по умолчанию - *1*.

Нулевой маршрут

Примечание

Нулевой маршрут - это маршрут, для которого система отбрасывает подходящие пакеты без ответа. Использование нулевого маршрута позволяет предотвратить утечку данных о топологии сети через публичные интерфейсы, но не мешает использовать ее в качестве более специфического маршрута внутри сети.

- `set protocols vrf <name> static route <subnet> blackhole`

  Создает нулевой маршрут IPv4 <*subnet*> в экземпляре VRF <*name*>.

- `set protocols vrf <name> static route <subnet> blackhole distance <distance>`

  Задает административную дистанцию <*distance*> для нулевого маршрута IPv4 <*subnet*> в экземпляре VRF <*name*>. Маршруты с наименьшей административной дистанцией - в приоритете перед маршрутами с наибольшей административной дистанцией.

- `set protocols vrf <name> static route6 <subnet> blackhole`

  Создает нулевой маршрут IPv6 <*subnet*> в экземпляре VRF <*name*>.

- `set protocols vrf <name> static route6 <subnet> blackhole distance <distance>`

  Задает административную дистанцию <*distance*> для нулевого маршрута IPv6 <*subnet*> в экземпляре VRF <*name*>. Маршруты с наименьшей административной дистанцией - в приоритете перед маршрутами с наибольшей административной дистанцией.

Мониторинг

- `show vrf`

  Выводит на экран список созданных экземпляров VRF.

  Пример работы команды show vrf:

```
fakel@fakel:~$ show vrf
VRF name          state     mac address        flags                     interfaces
--------          -----     -----------        -----                     ----------
blue              up        00:53:12:d8:74:24  noarp,master,up,lower_up
  dum200,eth0.302
red               up        00:53:de:02:df:aa  noarp,master,up,lower_up
  dum100,eth0.300,bond0.100,peth0
```

- `show vrf <name>`

  Выводит на экран информацию об определенном <*name*> экземпляре VRF с именем.

  Пример работы команды show vrf <name>:

```
fakel@fakel:~$ show vrf name blue
VRF name          state     mac address        flags                     interfaces
--------          -----     -----------        -----                     ----------
blue              up        00:53:12:d8:74:24  noarp,master,up,lower_up
  dum200,eth0.302
```

- `show ip route vrf <name>`

  Выводит на экран содержимое таблицы маршрутизации IPv4 для определенного <*name*> экземпляра VRF.

  Пример работы команды show ip route vrf <name>:

```
fakel@fakel:~$ show ip route vrf blue
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR, f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

VRF blue:
K   0.0.0.0/0 [255/8192] unreachable (ICMP unreachable), 00:00:50
S>* 172.16.0.0/16 [1/0] via 192.0.2.1, dum1, 00:00:02
C>* 192.0.2.0/24 is directly connected, dum1, 00:00:06
```

- `show ipv6 route vrf <name>`

  Выводит на экран содержимое таблицы маршрутизации IPv6 для определенного <*name*> экземпляра VRF.

  Пример работы команды show ipv6 route vrf <name>:

```
fakel@fakel:~$ show ipv6 route vrf red
Codes: K - kernel route, C - connected, S - static, R - RIPng,
       O - OSPFv3, I - IS-IS, B - BGP, N - NHRP, T - Table,
       v - VNC, V - VNC-Direct, A - Babel, D - SHARP, F - PBR,
       f - OpenFabric,
       > - selected route, * - FIB route, q - queued route, r - rejected route

VRF red:
K   ::/0 [255/8192] unreachable (ICMP unreachable), 00:43:20
C>* 2001:db8::/64 is directly connected, dum1, 00:02:19
C>* fe80::/64 is directly connected, dum1, 00:43:19
K>* ff00::/8 [0/256] is directly connected, dum1, 00:43:19
```

- `ping <host> vrf <name>`

  Проверяет доступности или недоступности сетевого узла.

Пример работы команды ping <host> vrf <name>:

```
fakel@fakel:~$ ping 192.0.2.1 vrf red
PING 192.0.2.1 (192.0.2.1) 56(84) bytes of data.
64 bytes from 192.0.2.1: icmp_seq=1 ttl=64 time=0.070 ms
64 bytes from 192.0.2.1: icmp_seq=2 ttl=64 time=0.078 ms
^C
--- 192.0.2.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 0.070/0.074/0.078/0.004 ms
```

- `traceroute vrf <name> [ipv4 | ipv6] <host>`

  Отображает маршрут следования данных до определенного хоста. При использовании опции IPv4 или IPv6 отображаются пакеты к семейству IP адресов данного хоста. Эта опция полезна, когда указанный хост представляет собой имя хоста, а не IP адрес.

2.4 Защищенные коммуникации

В **ПО Факел** Туннелирование трафика (защищенные коммуникации между устройствами) реализовано следующими механизмами:

- *Стек протоколов IPsec* (страница 372)
- *Сервер L2TP* (страница 377)
- *Сервер OpenConnect* (страница 383)
- *Сервер PPTP* (страница 385)
- *Ключевая схема RSA* (страница 387)
- *DMVPN* (страница 397)
- *Site-to-Site VPN* (страница 404)

2.4.1 Стек протоколов IPsec

2.4.1.1 Описание

Использование протокола GRE поверх стека протоколов IPSec (протокола IPIP, SIT или любого другого протокола без контроля соединений поверх стека протоколов IPSec) является распространенным способом защиты трафика внутри туннеля.

Преимущество этой схемы заключается в том, что вы получаете реальный интерфейс с собственным адресом, что облегчает настройку статических маршрутов или использование протоколов динамической маршрутизации без необходимости модификации политик IPSec. Другим преимуществом является значительное упрощение взаимодействия между маршрутизаторами, которое может быть затруднено при использовании обычного IPSec, поскольку внешний адрес маршрутизатора обычно не соответствует политике IPSec при типичной настройке site-to-site, и для него необходимо добавлять специальные параметры конфигурации или изменять адрес источника для исходящего трафика приложений. Протокол GRE поверх стека протоколов IPSec не имеет такой проблемы и полностью прозрачен для приложений.

Протокол GRE, IPIP, SIT, а также стек протоколов IPSec являются общепринятыми стандартами, что позволяет легко реализовать эту схему между **ПО Факел** и любым другим маршрутизатором с поддержкой тех же функций.

Предположим, что выбран протокол GRE. При этом стек протоколов IPSec будет использовать аутентификацию по общему секретному ключу (Pre-shared Secret), а для шифрования и контроля целостности будут использоваться алгоритмы AES-128 и SHA-1 соответственно. При необходимости данную конфигурацию можно изменить.

2.4.1.2 Настройка

Пример настройки

IPsec с использованием GRE

Первый вариант развертывания VPN - настройка политики IPSec для учета пакетов протокола GRE, которыми обмениваются внешние адреса маршрутизаторов. Это лучший вариант, если оба маршрутизатора имеют статические внешние адреса.

Предположим, что маршрутизатор LEFT (условно «левый») имеет внешний адрес `192.0.2.10` на интерфейсе `eth0`, а маршрутизатор RIGHT (условно «правый») - `203.0.113.45`.

Далее представлены команды, которые необходимо выполнить на маршрутизаторе 1.

```
# Настройки GRE туннеля
set interfaces tunnel tun0 encapsulation gre
set interfaces tunnel tun0 source-address 192.0.2.10
set interfaces tunnel tun0 remote 203.0.113.45
set interfaces tunnel tun0 address 10.10.10.1/30

# Настройка интерфейса IPSec
set vpn ipsec ipsec-interfaces interface eth0

# Настройка группы алгоритмов IKE
set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group '2'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set vpn ipsec ike-group MyIKEGroup proposal 1 encryption 'aes128'
set vpn ipsec ike-group MyIKEGroup proposal 1 hash 'sha1'

# Группа настроек алгоритмов ESP
set vpn ipsec esp-group MyESPGroup proposal 1 encryption 'aes128'
set vpn ipsec esp-group MyESPGroup proposal 1 hash 'sha1'

# Настройка туннеля IPsec
set vpn ipsec site-to-site peer 203.0.113.45 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 203.0.113.45 authentication pre-shared-secret
  MYSECRETKEY
set vpn ipsec site-to-site peer 203.0.113.45 ike-group MyIKEGroup
set vpn ipsec site-to-site peer 203.0.113.45 default-esp-group MyESPGroup
set vpn ipsec site-to-site peer 203.0.113.45 local-address 192.0.2.10

# Настройка политики IPSec с учетом GRE
set vpn ipsec site-to-site peer 203.0.113.45 tunnel 1 protocol gre
```

На маршрутизаторе RIGHT необходимо выполнить те же команды, только поменять адреса `local` и `remote` местами.

Построение туннелей с интерфейсов Loopback

Описанная выше схема не работает, если один из маршрутизаторов имеет динамический внешний адрес. Классическим решением этой проблемы является задание адреса на интерфейсе Loopback и использование его в качестве адреса источника для GRE туннеля, а затем настройка политики IPsec для соответствия этим адрес на Loopback интерфейсах.

Мы предполагаем, что маршрутизатор LEFT имеет статический адрес `192.0.2.10` на интерфейсе `eth0`, а маршрутизатор RIGHT имеет динамический адрес на интерфейсе `eth0`.

Далее представлены команды, которые необходимо выполнить на маршрутизаторе LEFT для настройки GRE туннеля.

```
set interfaces loopback lo address 192.168.99.1/32
set interfaces tunnel tun0 encapsulation gre
set interfaces tunnel tun0 address 10.10.10.1/30
set interfaces tunnel tun0 source-address 192.168.99.1
set interfaces tunnel tun0 remote 192.168.99.2
```

Далее представлены команды, которые необходимо выполнить на маршрутизаторе RIGHT для настройки GRE туннеля.

```
set interfaces loopback lo address 192.168.99.2/32
set interfaces tunnel tun0 encapsulation gre
set interfaces tunnel tun0 address 10.10.10.2/30
set interfaces tunnel tun0 source-address 192.168.99.2
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set interfaces tunnel tun0 remote 192.168.99.1
```

Далее необходимо выполнить настройку использования стека протоколов IPSec. Однако теперь необходимо обеспечить работу политики IPsec с динамическим адресом на стороне маршрутизатора RIGHT. Сложность состоит в том, что аутентификация с использованием общего секретного ключа (Pre-shared Secret) не работает с динамическим адресом, поэтому необходимо использовать ключ RSA.

Во-первых, на маршрутизаторе LEFT необходимо использовать команду `generate vpn rsa-key bits 2048`. Длину ключа можно выбрать отличную от представленной в примере.

```
fakel@left# run generate vpn rsa-key bits 2048
Generating rsa-key to /config/ipsec.d/rsa-keys/localhost.key

Your new local RSA key has been generated
The public portion of the key is:

0sAQO2335[long string here]
```

Затем - на маршрутизаторе RIGHT необходимо добавить сформированный ключ RSA в конфигурацию.

```
fakel@right# set vpn rsa-keys rsa-key-name LEFT rsa-key KEYGOESHERE
```

Теперь можно выполнить настройку политики IPSec. Для этого теперь необходимо использовать идентификатор маршрутизатора RIGHT вместо адреса (динамического).

Далее представлены команды, которые необходимо выполнить на маршрутизаторе LEFT (статический адрес).

```
set vpn rsa-keys rsa-key-name RIGHT rsa-key <PUBLIC KEY FROM THE RIGHT>
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec esp-group MyESPGroup proposal 1 encryption aes128
set vpn ipsec esp-group MyESPGroup proposal 1 hash sha1
set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group 2
set vpn ipsec ike-group MyIKEGroup proposal 1 encryption aes128
set vpn ipsec ike-group MyIKEGroup proposal 1 hash sha1
set vpn ipsec site-to-site peer @RIGHT authentication mode rsa
set vpn ipsec site-to-site peer @RIGHT authentication rsa-key-name RIGHT
set vpn ipsec site-to-site peer @RIGHT default-esp-group MyESPGroup
set vpn ipsec site-to-site peer @RIGHT ike-group MyIKEGroup
set vpn ipsec site-to-site peer @RIGHT local-address 192.0.2.10
set vpn ipsec site-to-site peer @RIGHT connection-type respond
set vpn ipsec site-to-site peer @RIGHT tunnel 1 local prefix 192.168.99.1/32  #
  Дополнительный адрес интерфейса Loopback на данном маршрутизаторе
set vpn ipsec site-to-site peer @RIGHT tunnel 1 remote prefix 192.168.99.2/32 #
  Дополнительный адрес интерфейса Loopback на удаленном маршрутизаторе
```

Далее - представлены команды, которые необходимо выполнить на маршрутизаторе RIGHT (динамический адрес).

```
set vpn rsa-keys rsa-key-name LEFT rsa-key <PUBLIC KEY FROM THE LEFT>
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec esp-group MyESPGroup proposal 1 encryption aes128
set vpn ipsec esp-group MyESPGroup proposal 1 hash sha1
set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group 2
set vpn ipsec ike-group MyIKEGroup proposal 1 encryption aes128
set vpn ipsec ike-group MyIKEGroup proposal 1 hash sha1
set vpn ipsec site-to-site peer 192.0.2.10 authentication id @RIGHT
set vpn ipsec site-to-site peer 192.0.2.10 authentication mode rsa
set vpn ipsec site-to-site peer 192.0.2.10 authentication rsa-key-name LEFT
set vpn ipsec site-to-site peer 192.0.2.10 authentication remote-id LEFT
set vpn ipsec site-to-site peer 192.0.2.10 connection-type initiate
set vpn ipsec site-to-site peer 192.0.2.10 default-esp-group MyESPGroup
set vpn ipsec site-to-site peer 192.0.2.10 ike-group MyIKEGroup
set vpn ipsec site-to-site peer 192.0.2.10 local-address any
set vpn ipsec site-to-site peer 192.0.2.10 tunnel 1 local prefix 192.168.99.2/32  #
 Дополнительный адрес интерфейса Loopback на данном маршрутизаторе
set vpn ipsec site-to-site peer 192.0.2.10 tunnel 1 remote prefix 192.168.99.1/32 #
 Дополнительный адрес интерфейса Loopback на удаленном маршрутизаторе
```

2.4.1.3 Список команд

Настройки GRE туннеля

- `set interfaces tunnel tunN encapsulation gre`
- `set interfaces tunnel tunN source-address <address>`
- `set interfaces tunnel tunN remote <address>`
- `set interfaces tunnel tunN address <address>`

Настройка интерфейса IPSec

- `set vpn ipsec ipsec-interfaces interface eth0`

Настройка группы алгоритмов IKE

- `set vpn ipsec ike-group <text> proposal <165535> dh-group <number>`
- `set vpn ipsec ike-group <text> proposal <165535> encryption <type>`
- `set vpn ipsec ike-group <text> proposal <165535> hash <type>`

Группа настроек алгоритмов ESP

- `set vpn ipsec esp-group <text> proposal <165535> encryption <number>`
- `set vpn ipsec esp-group <text> proposal <165535> hash <number>`

Настройка туннеля IPsec

- `set vpn ipsec site-to-site peer <address> authentication mode pre-shared-secret`
- `set vpn ipsec site-to-site peer <address> authentication pre-shared-secret <secret-key>`
- `set vpn ipsec site-to-site peer <address> ike-group <text>`
- `set vpn ipsec site-to-site peer <address> default-esp-group <text>`
    - `set vpn ipsec site-to-site peer <address> local-address <x.x.x.x>`

2.4.2 Сервер L2TP

2.4.2.1 Описание

Для обеспечения функциональности L2TP сервера в **ПО Факел** используется механизм accel-ppp[53]. Данный механизм может использоваться как с локальной аутентификацией, так и совместно с подключенным сервером RADIUS.

2.4.2.2 Настройка

Пример настройки

IPSec с использованием L2TP

Пример настройки простого использования протокола L2TP поверх стека протоколов IPsec для защищенного удаленного доступа (VPN).

Пример настройки L2TP:

```
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec nat-traversal enable
set vpn ipsec nat-networks allowed-network 0.0.0.0/0
set vpn l2tp remote-access outside-address 192.0.2.2
set vpn l2tp remote-access client-ip-pool start 192.168.255.2
set vpn l2tp remote-access client-ip-pool stop 192.168.255.254
set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret>
set vpn l2tp remote-access authentication mode local
set vpn l2tp remote-access authentication local-users username test password 'test'
```

В данном примере предполагается, что внешний адрес будет `192.0.2.2`.

Если на внешнем интерфейсе установлена локальная политика межсетевого экрана, то необходимо разрешить сетевой трафик по указанным ниже портам:

- Номер порта UDP 500 (для протокола IKE);
- Номер протокола IP 50 (для протокола ESP);
- Номер порта UDP 1701 (для стека протоколов IPsec);
- Номер порта UDP 4500 (для механизма NAT-Traversal).

Разрешение сетевого трафика по порту UDP 4500 необходимо для работы механизма NAT-Traversal (NAT-T), когда между VPN сервером и VPN клиентом находится шлюз, выполняющий трансляцию адресов (NAT). В этом случае сетевые пакеты ESP дополнительно упаковываются в UDP для обеспечения работы стека протоколов IPSec.

Пример настройки локальной политики межсетевого экрана:

```
set firewall name OUTSIDE-LOCAL rule 40 action 'accept'
set firewall name OUTSIDE-LOCAL rule 40 protocol 'esp'
set firewall name OUTSIDE-LOCAL rule 41 action 'accept'
```

(продолжается на следующей странице)

[53] https://accel-ppp.org/

(продолжение с предыдущей страницы)

```
set firewall name OUTSIDE-LOCAL rule 41 destination port '500'
set firewall name OUTSIDE-LOCAL rule 41 protocol 'udp'
set firewall name OUTSIDE-LOCAL rule 42 action 'accept'
set firewall name OUTSIDE-LOCAL rule 42 destination port '4500'
set firewall name OUTSIDE-LOCAL rule 42 protocol 'udp'
set firewall name OUTSIDE-LOCAL rule 43 action 'accept'
set firewall name OUTSIDE-LOCAL rule 43 destination port '1701'
set firewall name OUTSIDE-LOCAL rule 43 ipsec 'match-ipsec'
set firewall name OUTSIDE-LOCAL rule 43 protocol 'udp'
```

Для разрешения VPN клиенту подключаться через указанный внешний адрес также необходимо наличие правила трансляции (NAT).

Пример настройки правила трансляции:

```
set nat source rule 110 outbound-interface 'eth0'
set nat source rule 110 source address '192.168.255.0/24'
set nat source rule 110 translation address masquerade
```

VPN клиент обычно запрашивает параметры конфигурации, в числе которых может быть и список DNS серверов для клиента.

Пример настройки DNS сервера для VPN клиентов:

```
set vpn l2tp remote-access name-server '198.51.100.8'
set vpn l2tp remote-access name-server '198.51.100.4'
```

Список установленных соединений можно посмотреть с помощью команды `show vpn remote-access` или команды `show l2tp-server sessions` в режиме Администрирования.

Пример работы команды show vpn remote-access:

```
fakel@fakel:~$ show vpn remote-access
ifname | username | calling-sid  |      ip       | rate-limit | type | comp | state
   |  uptime
-------+----------+--------------+---------------+------------+------+------+-------
  -+----------
ppp0   | fakel     | 192.168.0.36 | 192.168.255.1 |            | l2tp |      |
  active | 00:06:13
```

Сервер доступа LNS (L2TP Network Server)

Сервер доступа LNS зачастую используется для подключения к серверу LAC (L2TP Access Concentrator).

Пример настройки сервера доступа LNS:

```
set vpn l2tp remote-access outside-address 192.0.2.2
set vpn l2tp remote-access client-ip-pool start 192.168.255.2
set vpn l2tp remote-access client-ip-pool stop 192.168.255.254
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set vpn l2tp remote-access lns shared-secret 'secret'
set vpn l2tp remote-access ccp-disable
set vpn l2tp remote-access authentication mode local
set vpn l2tp remote-access authentication local-users username test password 'test'
```

В приведенном примере в качестве внешнего IP адреса используется `192.0.2.2`. Для сервера LAC обычно требуется пароль аутентификации, который в приведенной в примере конфигурации задан как `lns shared-secret 'secret'`. Данная настройка требует отключения протокола управления сжатием (Compression Control Protocol, CCP), что достигается командой `set vpn l2tp remote-access ccp-disable`.

Ограничение полосы пропускания

Лимиты пропускной способности могут быть установлены как для локальных пользователей так и для пользователей RADIUS с помощью специальных атрибутов.

Пример настройки ограничений полосы пропускания для локальных пользователей:

```
set vpn l2tp remote-access outside-address 192.0.2.2
set vpn l2tp remote-access client-ip-pool start 192.168.255.2
set vpn l2tp remote-access client-ip-pool stop 192.168.255.254
set vpn l2tp remote-access authentication mode local
set vpn l2tp remote-access authentication local-users username test password test
set vpn l2tp remote-access authentication local-users username test rate-limit
  download 20480
set vpn l2tp remote-access authentication local-users username test rate-limit
  upload 10240
```

Лимиты пропускной способности устанавливаются в единицах кбит/с (килобит в секунду).

Настроенные лимиты можно посмотреть с помощью команды `show vpn remote-access` в режиме Администрирования.

Пример работы команды show vpn remote-access:

```
fakel@fakel:~$ show vpn remote-access
ifname | username | calling-sid  |      ip       | rate-limit  | type | comp |
  state  |  uptime
-------+----------+--------------+---------------+-------------+------+------+------
  --+-----------
ppp0   | test     | 192.168.0.36 | 192.168.255.2 | 20480/10240 | l2tp |      |
  active | 00:06:30
```

2.4.2.3 Список команд

Основные настройки

- `set vpn ipsec ipsec-interfaces interface <ethN>`

- set vpn ipsec nat-traversal enable
- set vpn ipsec nat-networks allowed-network <x.x.x.x/x>
- set vpn l2tp remote-access outside-address <x.x.x.x>
- set vpn l2tp remote-access client-ip-pool start <x.x.x.x>
- set vpn l2tp remote-access client-ip-pool stop <x.x.x.x>
- set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret
- set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret <secret>
- set vpn l2tp remote-access authentication mode local
- set vpn l2tp remote-access authentication local-users username <text-name> password <text-password>
- set vpn l2tp remote-access name-server '198.51.100.8'
- set vpn l2tp remote-access lns shared-secret 'secret'
- set vpn l2tp remote-access ccp-disable
- set vpn l2tp remote-access authentication local-users username test rate-limit download 20480
- set vpn l2tp remote-access authentication local-users username test rate-limit upload 10240

Мониторинг состояния

- show vpn remote-access

Аутентификация RADIUS

Описание

Чтобы использовать аутентификацию на основе протокола RADIUS, необходимо изменить режим аутентификации в конфигурации. Предыдущие настройки, например, локальные пользователи, по-прежнему остаются в конфигурации, однако они не используются, если режим был изменен с локального на RADIUS. После изменения режима на локальный все локальные учетные записи будут снова использоваться.

```
set vpn l2tp remote-access authentication mode <local|radius>
```

Поскольку одиночный RADIUS сервер будет являться единой точкой отказа в случае выхода из строя, можно настроить несколько RADIUS серверов, которые будут последовательно опрашиваться.

```
set vpn l2tp remote-access authentication radius server 10.0.0.1 key 'foo'
set vpn l2tp remote-access authentication radius server 10.0.0.2 key 'foo'
```

Примечание

Некоторые RADIUS сервера используют список контроля доступа, который разрешает запросы от определенных RADIUS клиентов. Убедитесь, что ваш маршрутизатор с **ПО Факел** добавлен в список разрешенных RADIUS клиентов.

Адрес отправителя

Если в качестве внутреннего протокола маршрутизации (IGP) используется протокол OSPF, то всегда используется ближайший интерфейс, подключенный к RADIUS серверу. В **ПО Факел** можно привязать все исходящие RADIUS запросы к одному IP адресу источника, например, к интерфейсу Dummy.

```
set vpn l2tp remote-access authentication radius source-address 10.0.0.3
```

Приведенная выше команда будет использовать адрес `10.0.0.3` в качестве исходного IP адреса для всех RADIUS запросов на этом устройстве.

Примечание

Параметр `source-address` должен быть ассоциирован с одним из интерфейсов **ПО Факел**. Рекомендуется использовать интерфейс Dummy.

Ограничение полосы пропускания

Для ограничения полосы пропускания в части пользователей RADIUS необходимо использовать параметр `rate-limit`.

```
set vpn l2tp remote-access authentication radius rate-limit enable
```

Для ограничения полосы пропускания в протоколе RADIUS предусмотрен параметр `Filter-Id`, значение которого можно переопределять.

```
set vpn l2tp remote-access authentication radius rate-limit attribute
 Download-Speed
```

Примечание

При задании пользовательских параметров в протоколе RADIUS необходимо объявить их в специальных словарях как стороне RADIUS сервера, так и на стороне RADIUS клиента, которым в нашем примере является маршрутизатор с **ПО Факел**. Словари RADIUS в **ПО Факел** располагаются по следующему пути: `/usr/share/accel-ppp/radius/`.

Расширенные функции RADIUS

Значения параметров протокола RADIUS, полученных от сервера, имеют более высокий приоритет по сравнению со значениями, заданными для тех же параметров в конфигурации через *Командная строка* (страница 17).

Распределение IP адресов между клиентами

Если RADIUS сервер возвращает параметр `Framed-IP-Address`, то IP адрес в качестве его значения будет выделен клиенту, а параметр `ip-pool` в конфигурации CLI игнорируется.

Переименование интерфейсов клиентов

Если RADIUS сервер возвращает параметр `NAS-Port-Id`, то в результате туннельные интерфейсы PPP будут переименованы.

Примечание

Значение параметра `NAS-Port-Id` должно быть длиной не более 16 символов. В противном случае интерфейс не будет переименован.

Список команд

Основные настройки

- `set vpn l2tp remote-access authentication mode <local|radius>`
- `set vpn l2tp remote-access authentication radius server <x.x.x.x> key <text>`
- `set vpn l2tp remote-access authentication radius source-address <x.x.x.x>`
- `set vpn l2tp remote-access authentication radius rate-limit enable`
- `set vpn l2tp remote-access authentication radius rate-limit attribute Download-Speed`

2.4.3 Сервер OpenConnect

2.4.3.1 Описание

ПО Факел поддерживает работу маршрутизатора в режиме OpenConnect VPN сервера. Данный сервер позволяет установить с маршрутизатором SSL/TLS соединение и обеспечить полный доступ к защищаемой (корпоративной) сети. Такой подход к организации VPN объединяет конечных пользователей и ресурсы в защищаемой (корпоративной) сети в виртуальную сеть с контролем доступа, основанным только на информации сетевого уровня, такой как IP адрес отправителя и номер порта. Таким образом достигается необходимая степень защиты всех типов трафика для устройств между открытыми и защищаемыми (корпоративными) сетями, а также шифрование с помощью протоколов SSL/TLS.

Удаленный пользователь с помощью VPN клиента с поддержкой OpenConnect подключается к маршрутизатору и получает IP адрес из заданного пула адресов, получая доступ к ресурсам защищаемой (корпоративной) сети.

Примечание

Все сертификаты должны размещаться в **ПО Факел** по следующему пути `/config/auth`. Если сертификаты размещаются не в каталоге `/config`, они не будут перенесены при обновлении ПО.

2.4.3.2 Настройка

Пример настройки

В первую очередь необходимо сформировать сертификат, который будет удостоверять подлинность пользователей, пытающихся получить доступ к ресурсам защищаемой (корпоративной) сети через SSL/TLS туннели. Следующая команда позволяет создать сертификаты, выпущенные внутренним центром сертификации, которые будут размещены по следующему пути `/config/auth`.

```
openssl req -newkey rsa:4096 -new -nodes -x509 -days 3650 -keyout /
  config/auth/server.key -out /config/auth/server.crt
openssl req -new -x509 -key /config/auth/server.key -out /config/auth/ca.crt
```

Можно также создать сертификат с помощью инструмента certbot[54] - простого в использовании клиента, который получает сертификат из - Let's Encrypt[55] - открытого центра - сертификации, созданного консорциумом организаций, и размещает его на веб-сервере.

```
sudo certbot certonly --standalone --preferred-challenges http -d <domain name>
```

После того, как сертификат подготовлен, можно переходить к настройке сервера OpenConnect.

- Используется локальный пользователь с логином `user4` и паролем `SecretPassword`.
- VPN клиенту выделяется IP адрес из пула `100.64.0.0/24`.
- IP адрес шлюза должен быть адресом одного из интерфейсов маршрутизатора.

```
set vpn openconnect authentication local-users username user4 password
  'SecretPassword'
```

(продолжается на следующей странице)

[54] https://certbot.eff.org/
[55] https://letsencrypt.org/ru/

(продолжение с предыдущей страницы)

```
set vpn openconnect authentication mode 'local'
set vpn openconnect network-settings client-ip-settings subnet '100.64.0.0/24'
set vpn openconnect network-settings name-server '10.1.1.1'
set vpn openconnect network-settings name-server '10.1.1.2'
set vpn openconnect ssl ca-cert-file '/config/auth/fullchain.pem'
set vpn openconnect ssl cert-file '/config/auth/cert.pem'
set vpn openconnect ssl key-file '/config/auth/privkey.pem'
```

После применения изменений, внесенных в конфигурацию, необходимо убедиться в том, что подключение VPN клиента выполнено успешно.

```
fakel@fakel:~$ show openconnect-server sessions

interface    username    ip            remote IP      RX        TX        state
   uptime
-----------  ----------  ------------  -------------  --------  --------  ---------
   --------
sslvpn0      user4       100.64.0.105  xx.xxx.49.253  127.3 KB  160.0 KB  connected
   12m:28s
```

Примечание

В качестве совместимого VPN клиента может использоваться клиент Cisco (R) AnyConnect (R).

2.4.3.3 Список команд

Основные настройки

- `set vpn openconnect authentication local-users username <user> password <pass>`
- `set vpn openconnect authentication mode <local|radius>`
- `set vpn openconnect network-settings client-ip-settings subnet <subnet>`
- `set vpn openconnect network-settings name-server <address>`
- `set vpn openconnect network-settings name-server <address>`
- `set vpn openconnect ssl ca-cert-file <file>`
- `set vpn openconnect ssl cert-file <file>`
- `set vpn openconnect ssl key-file <file>`

2.4.4 Сервер PPTP

2.4.4.1 Описание

Протокол PPTP (Point-to-Point Tunneling Protocol) реализован в **ПО Факел** только для обеспечения обратной совместимости. PPTP имеет множество известных проблем с безопасностью, и вместо него необходимо использовать одну из многих других современных реализаций VPN.

По умолчанию если не задана иная конфигурация, то для аутентификации используется протокол *MS-CHAP v2*, а для шифрования - протокол *MPPE* с разрядностью 128 бит и без контроля соединений. Если в конфигурации не задан адрес шлюза, то используется наименьший IP адрес из пула адресов клиента, заданного подсетью с маской `/24`. Например, в приведенном ниже примере это будет IP адрес `192.168.0.1`.

2.4.4.2 Настройка

Пример настройки

Пример настройки на стороне сервера

```
set vpn pptp remote-access authentication local-users username test password 'test'
set vpn pptp remote-access authentication mode 'local'
set vpn pptp remote-access client-ip-pool start '192.168.0.10'
set vpn pptp remote-access client-ip-pool stop '192.168.0.15'
set vpn pptp remote-access gateway-address '10.100.100.1'
set vpn pptp remote-access outside-address '10.1.1.120'
```

Пример настройки на стороне клиента

В данному примере рассматривается настройка PPTP клиента в операционной среде Debian 9.

Выполните установку клиентского ПО с помощью менеджера пакетов `apt` и выполните команду `pptpsetup`, чтобы сформировать начальную конфигурацию.

```
apt-get install pptp-linux
pptpsetup --create TESTTUNNEL --server 10.1.1.120 --username test --password test --
  encrypt
pon TESTTUNNEL
```

Команда `TESTTUNNEL` позволяет установить PPTP туннель с удаленным хостом (PPTP сервером).

Текущее состояние сессий (туннелей) можно вывести на экран следующим образом.

```
run sh pptp-server sessions
ifname | username | calling-sid |      ip      | type | comp | state  |  uptime
-------+----------+-------------+--------------+------+------+--------+----------
ppp0   | test     | 10.1.1.99   | 192.168.0.10 | pptp | mppe | active | 00:00:58
```

2.4.4.3 Список команд

Основные настройки

- `set vpn pptp remote-access authentication local-users username <name> password <text-password>`
- `set vpn pptp remote-access authentication mode <local | radius>`
- `set vpn pptp remote-access client-ip-pool start <x.x.x.x>`
- `set vpn pptp remote-access client-ip-pool stop <x.x.x.x>`
- `set vpn pptp remote-access gateway-address <x.x.x.x>`
- `set vpn pptp remote-access outside-address <x.x.x.x>`

2.4.5 Ключевая схема RSA

2.4.5.1 Описание

Ключевая схема RSA может использоваться для таких сервисов, как обмен ключами и для организации шифрования. Для того чтобы стек протоколов IPSec работал с динамическими адресами с одной и другой стороны, необходимо использовать ключи RSA для аутентификации. Настройка данной ключевой схемы проста и осуществляется быстро.

2.4.5.2 Настройка

Пример настройки

Пример настройки RSA между двумя маршрутизаторами.

Сначала на обоих маршрутизаторах необходимо выполнить команду `generate vpn rsa-key bits 2048` в режиме Администрирования. Опционально можно выбрать длину ключа, отличную от значения по умолчанию - 2048.

```
fakel@left# run generate vpn rsa-key bits 2048
Generating rsa-key to /config/ipsec.d/rsa-keys/localhost.key

Your new local RSA key has been generated
The public portion of the key is:

0sAQO2335[long string here]
```

Обязательно скопируйте или запиши данный ключ RSA, так как его нужно будет на противоположный маршрутизатор.

```
set vpn rsa-keys rsa-key-name LEFT rsa-key KEYGOESHERE
```

После подготовки RSA ключей, можно переходить к настройке IPsec.

Основные моменты:

1. Поскольку оба маршрутизатора не знают своих активных публичных адресов, нужно установить локальный адрес пира в значение «any».
2. На инициаторе нужно установить адрес пира в его публичный адрес, а на ответчике - только id.
3. На инициаторе нужно установить опцию remote-id, чтобы он мог правильно идентифицировать IKE-трафик от ответчика.
4. На ответчике нужно установить локальный id, чтобы инициатор мог знать, кто с ним разговаривает, чтобы точка №3 работала.
5. Включить обход NAT с обеих сторон, выполнив команду `set vpn ipsec nat-traversal enable`.

Команды для настройки первого маршрутизатора:

```
set vpn rsa-keys rsa-key-name RIGHT rsa-key <PUBLIC KEY FROM THE RIGHT>
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec nat-traversal 'enable'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set vpn ipsec esp-group MyESPGroup proposal 1 encryption aes128
set vpn ipsec esp-group MyESPGroup proposal 1 hash sha1
set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group 2
set vpn ipsec ike-group MyIKEGroup proposal 1 encryption aes128
set vpn ipsec ike-group MyIKEGroup proposal 1 hash sha1
set vpn ipsec site-to-site peer 192.0.2.60 authentication mode rsa
set vpn ipsec site-to-site peer 192.0.2.60 authentication id @LEFT
set vpn ipsec site-to-site peer 192.0.2.60 authentication rsa-key-name RIGHT
set vpn ipsec site-to-site peer 192.0.2.60 authentication remote-id RIGHT
set vpn ipsec site-to-site peer 192.0.2.60 default-esp-group MyESPGroup
set vpn ipsec site-to-site peer 192.0.2.60 ike-group MyIKEGroup
set vpn ipsec site-to-site peer 192.0.2.60 local-address any
set vpn ipsec site-to-site peer 192.0.2.60 connection-type initiate
set vpn ipsec site-to-site peer 192.0.2.60 tunnel 1 local prefix 192.168.99.1/32
set vpn ipsec site-to-site peer 192.0.2.60 tunnel 1 remote prefix 192.168.99.2/32
```

Команды для настройки второго маршрутизатора:.

```
set vpn rsa-keys rsa-key-name LEFT rsa-key <PUBLIC KEY FROM THE LEFT>
set vpn ipsec ipsec-interfaces interface eth0
set vpn ipsec nat-traversal 'enable'
set vpn ipsec esp-group MyESPGroup proposal 1 encryption aes128
set vpn ipsec esp-group MyESPGroup proposal 1 hash sha1
set vpn ipsec ike-group MyIKEGroup proposal 1 dh-group 2
set vpn ipsec ike-group MyIKEGroup proposal 1 encryption aes128
set vpn ipsec ike-group MyIKEGroup proposal 1 hash sha1
set vpn ipsec site-to-site peer @LEFT authentication id @RIGHT
set vpn ipsec site-to-site peer @LEFT authentication mode rsa
set vpn ipsec site-to-site peer @LEFT authentication rsa-key-name LEFT
set vpn ipsec site-to-site peer @LEFT connection-type respond
set vpn ipsec site-to-site peer @LEFT default-esp-group MyESPGroup
set vpn ipsec site-to-site peer @LEFT ike-group MyIKEGroup
set vpn ipsec site-to-site peer @LEFT local-address any
set vpn ipsec site-to-site peer @LEFT tunnel 1 local prefix 192.168.99.2/32
set vpn ipsec site-to-site peer @LEFT tunnel 1 remote prefix 192.168.99.1/32
```

2.4.5.3 Список команд

Основные настройки

- `set vpn rsa-keys rsa-key-name <name> rsa-key <text>`
- `set vpn ipsec ipsec-interfaces interface <ethN>`
- `set vpn ipsec nat-traversal <enable | disable>`
- `set vpn ipsec esp-group <text> proposal <1-65535> encryption <type>`

- set vpn ipsec esp-group <text> proposal <1-65535> hash <type>
- set vpn ipsec ike-group <text> proposal <1-65535> dh-group <number>
- set vpn ipsec ike-group <text> proposal <1-65535> encryption <type>
- set vpn ipsec ike-group <text> proposal <1-65535> hash <type>
- set vpn ipsec site-to-site peer <x.x.x.x> authentication mode <pre-shared-secret | rsa | x509>
- set vpn ipsec site-to-site peer <x.x.x.x> authentication id <test>
- set vpn ipsec site-to-site peer <x.x.x.x> authentication rsa-key-name <text>
- set vpn ipsec site-to-site peer <x.x.x.x> authentication remote-id <text>
- set vpn ipsec site-to-site peer <x.x.x.x> default-esp-group <text>
- set vpn ipsec site-to-site peer <x.x.x.x> ike-group <text>
- set vpn ipsec site-to-site peer <x.x.x.x> local-address <x.x.x.x>
- set vpn ipsec site-to-site peer <x.x.x.x> connection-type <initiate | respond>
- set vpn ipsec site-to-site peer <x.x.x.x> tunnel <0-4294967295> local prefix <x.x.x.x/x>
- set vpn ipsec site-to-site peer <x.x.x.x> tunnel <0-4294967295> remote prefix <x.x.x.x/x>

2.4.6 Сервер SSTP

2.4.6.1 Описание

Протокол SSTP (Secure Socket Tunneling Protocol) - протокол построения VPN, обеспечивающий механизм передачи PPP трафика по SSL/TLS туннелю. SSL/TLS обеспечивает безопасность на транспортном уровне с согласованием ключей, шифрованием и проверкой целостности трафика. Использование SSL/TLS через TCP-порт 443 позволяет протоколу SSTP проходить практически через любой межсетевой экран и прокси-сервер, за исключением веб-прокси с аутентификацией.

Протокол SSTP доступен к использованию в операционных системах Linux, BSD и Windows.

Для обеспечения функциональности SSTP сервера в **ПО Факел** используется механизм accel-ppp[56]. Данный механизм может использоваться как с локальной аутентификацией, так и совместно с подключенным сервером RADIUS.

Поскольку протокол SSTP позволяет передавать PPP трафик по SSL/TLS туннелю, для организации VPN необходимо использовать сертификаты с открытой подписью, а также инфраструктуру PKI.

Примечание

Все сертификаты должны размещаться в **ПО Факел** по следующему пути `/config/auth`. Если сертификаты размещаются не в каталоге `/config`, они не будут перенесены при обновлении ПО.

2.4.6.2 Настройка

Пример настройки

В данном примере рассматриваться порядок конфигурирования SSTP сервера в составе **ПО Факел** с учетом следующих особенностей:

- используется локальная учетная запись пользователя с логином `foo` и паролем `bar`;
- IP адрес для клиента будет выделяться из пула, определенного подсетью `192.0.2.0/25`.

Подготовка сертификатов

Первым шагом необходимо подготовить сертификата УЦ, закрытого ключа и сертификата сервера SSTP.

Для генерации сертификата УЦ, закрытого ключа и сертификата сервера SSTP выполните следующие команды:

```
fakel@fakel:~$ mkdir -p /config/user-data/sstp
fakel@fakel:~$ openssl req -newkey rsa:4096 -new -nodes -x509 -days 3650 -keyout /
  config/user-data/sstp/server.key -out /config/user-data/sstp/server.crt

Generating a 4096 bit RSA private key
.......................++
.....................................................................++
Writing new private key to 'server.key'
[...]
```

(продолжается на следующей странице)

[56] https://accel-ppp.org/

(продолжение с предыдущей страницы)

```
Country Name (2 letter code) [RU]:
State or Province Name (full name) [Some-Region]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Some Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

fakel@fakel:~$ openssl req -new -x509 -key /config/user-data/sstp/server.key -out /
  config/user-data/sstp/ca.crt
[...]
Country Name (2 letter code) [RU]:
State or Province Name (full name) [Some-Region]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Some Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

Настройка SSTP на маршрутизаторе

После того, как сертификаты будут готовы можно переходить к настройке SSTP.

Команды для настройки SSTP на маршрутизаторе:

```
set vpn sstp authentication local-users username foo password bar
set vpn sstp authentication mode local
set vpn sstp gateway-address 192.0.2.254
set vpn sstp client-ip-pool subnet 192.0.2.0/25
set vpn sstp name-server 10.0.0.1
set vpn sstp name-server 10.0.0.2
set vpn sstp ssl ca-cert-file /config/auth/ca.crt
set vpn sstp ssl cert-file /config/auth/server.crt
set vpn sstp ssl key-file /config/auth/server.key
```

Проверка работы SSTP

После конфигурирования SSTP сервера необходимо выполнить базовую проверку его работы. Для этого можно воспользоваться SSTP клиентом для операционной системы Linux - sstpc[57]. Данные клиент потребует наличия соответствующего конфигурационного файла.

В примере далее показано использование для базовой проверки протокола *MS-CHAP v2*.

```
$ cat /etc/ppp/peers/fakel
usepeerdns
```

(продолжается на следующей странице)

[57] https://github.com/reliablehosting/sstp-client

(продолжение с предыдущей страницы)

```
#require-mppe
#require-pap
require-mschap-v2
noauth
lock
refuse-pap
refuse-eap
refuse-chap
refuse-mschap
#refuse-mschap-v2
nobsdcomp
nodeflate
debug
```

Теперь можно попробовать выполнить подключение клиента с помощью команды `sstpc --log-level 4 --log-stderr --user foo --password bar vpn.example.ru -- call fakel`. Детальная информация по попытке подключения представлена в примере ниже.

```
$ sstpc --log-level 4 --log-stderr --user foo --password bar vpn.example.ru -- call
  fakel

Mar 22 13:29:12 sstpc[12344]: Resolved vpn.example.ru to 192.0.2.1
Mar 22 13:29:12 sstpc[12344]: Connected to vpn.example.ru
Mar 22 13:29:12 sstpc[12344]: Sending Connect-Request Message
Mar 22 13:29:12 sstpc[12344]: SEND SSTP CRTL PKT(14)
Mar 22 13:29:12 sstpc[12344]:    TYPE(1): CONNECT REQUEST, ATTR(1):
Mar 22 13:29:12 sstpc[12344]:       ENCAP PROTO(1): 6
Mar 22 13:29:12 sstpc[12344]: RECV SSTP CRTL PKT(48)
Mar 22 13:29:12 sstpc[12344]:    TYPE(2): CONNECT ACK, ATTR(1):
Mar 22 13:29:12 sstpc[12344]:       CRYPTO BIND REQ(4): 40
Mar 22 13:29:12 sstpc[12344]: Started PPP Link Negotiation
Mar 22 13:29:15 sstpc[12344]: Sending Connected Message
Mar 22 13:29:15 sstpc[12344]: SEND SSTP CRTL PKT(112)
Mar 22 13:29:15 sstpc[12344]:    TYPE(4): CONNECTED, ATTR(1):
Mar 22 13:29:15 sstpc[12344]:       CRYPTO BIND(3): 104
Mar 22 13:29:15 sstpc[12344]: Connection Established

$ ip addr show ppp0
164: ppp0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1452 qdisc fq_codel state
  UNKNOWN group default qlen 3
    link/ppp  promiscuity 0
    inet 100.64.2.2 peer 100.64.1.1/32 scope global ppp0
       valid_lft forever preferred_lft forever
```

2.4.6.3 Список команд

Основные настройки

- `set vpn sstp authentication local-users username <user> password <pass>`

  Создает учетную запись пользователя с логином <user> для локальной аутентификации. Пароль пользователя будет иметь значение <pass>.

- `set vpn sstp authentication local-users username <user> disable`

  Отключает учетную запись пользователя с логином <user>.

- `set vpn sstp authentication local-users username <user> static-ip <address>`

  Назначает учетной записи пользователя с логином <user> статический IP адрес <address>.

- `set vpn sstp authentication local-users username <user> rate-limit download <bandwidth>`

  Ограничивает полосу пропускания при скачивании данных для учетной записи пользователя с логином <user> в единицах кбит/с (килобит в секунду).

- `set vpn sstp authentication local-users username <user> rate-limit upload <bandwidth>`

  Ограничивает полосу пропускания при загрузке данных для учетной записи пользователя с логином <user> в единицах кбит/с (килобит в секунду).

- `set vpn sstp authentication protocols <pap | chap | mschap | mschap-v2>`

  Задает требования аутентификации узла-участника VPN с помощью одного из следующих протоколов: *PAP*, *CHAP*, *MS-CHAP*, *MS-CHAP v2*.

- `set vpn sstp authentication mode <local | radius>`

  Задает режим аутентификации (<local> - локальных пользователей, <radius> - пользователей RADIUS). В заданном режиме будут обрабатываться все запросы.

  - <local> - все запросы на аутентификацию будут обрабатываться локально.
  - <radius> - все запросы на аутентификацию будут обрабатываться
  - сконфигурированным RADIUS сервером.

- `set vpn sstp gateway-address <gateway>`

  Задает IP адрес узла <gateway>, который будет использоваться в качестве локального адреса для PPP интерфейса.

- `set vpn sstp client-ip-pool subnet <subnet>`

  Задает IP адрес подсети <subnet>, которая будет использоваться в качестве пула адресов для всех подключающихся клиентов.

- `set vpn sstp client-ipv6-pool prefix <address> mask <number-of-bits>`

  Задает пул IPv6, из которого SSTP клиент будет получать IPv6 префикс заданной длины (маску) для определения конечной точки SSTP на своей стороне. Длина маски может быть задана в диапазоне от 48 до 128 бит, значение по умолчанию - 64 бит.

- `set vpn sstp client-ipv6-pool delegate <address> delegation-prefix <number-of-bits>`

  Настраивает механизма делегирования префикса DHCPv6 согласно **RFC 3633**[58] в контексте про-

токола SSTP. Для этого необходимо задать пул IPv6 и длину префикса делегирования. Из заданного пула будут выделяться IPv6 подсети определенной размерности. Длина префикса делегирования может быть задана от 32 до 64 бит.

- `set vpn sstp name-server <address>`

  При использовании данной команды подключенный клиент должен использовать адрес `<address>` в качестве адреса DNS сервера. Эта команда принимает адреса как IPv4, так и IPv6. Для IPv4 может быть настроено до двух DNS серверов, для IPv6 - до трех.

Настройка сертификатов SSL/TLS

- `set vpn sstp ssl ca-cert-file <file>`

  Задает путь до файла `<file>` сертификата УЦ.

- `set vpn sstp ssl cert-file <file>`

  Задает путь до файла `<file>` сертификата сервера (открытый ключ).

- `set vpn sstp ssl key-file <file>`

  Задает путь до файла `<file>` с закрытым ключом сервера.

Настройка PPP

- `set vpn sstp ppp-options lcp-echo-failure <number>`

  Задает максимальное количество `<number>` сообщений *Echo Request* по протоколу LCP (Link Control Protocol), по достижении которого PPP сессия будет сброшена.

- `set vpn sstp ppp-options lcp-echo-interval <interval>`

  Задает периодичность `<interval>` в секундах отправки модулем PPP сообщения *Echo Request* по протоколу LCP. При значении 0 модуль PPP не будет отправлять сообщения *Echo Request*.

- `set vpn sstp ppp-options lcp-echo-timeout <timeout>`

  Задает время `<timeout>` ожидания активности любых узлов-участников VPN. При использовании опции `lcp-echo-timeout` для модуля PPP активируется режим адаптивной функциональности *LCP Echo Request*, а значение опции `lcp-echo-failure` игнорируется.

- `set vpn sstp ppp-options mppe <require | prefer | deny>`

  Определяет один из следующих режимов использования протокола шифрования MPPE (Microsoft Point-to-Point Encryption):

  - `require` - ожидать от клиента подтверждения использования протокола MPPE, если клиент такого подтверждения не дает, то соединение сбрасывается;
  - `prefer` - ожидать от клиента подтверждения использования протокола MPPE, если клиент такого подтверждения не дает, то соединение сохраняется;
  - `deny` - не использовать протокол MPPE.

  Если режим не указан явно, то по умолчанию модуль PPP не запрашивает подтверждения от клиента, но допускает использование протокола MPPE по его инициативе.

[58] https://datatracker.ietf.org/doc/html/rfc3633.html

Примечание

Обратите внимание, что RADIUS сервер может переопределять значение данной опции значением атрибута `MS-MPPE-Encryption-Policy`.

Настройка аутентификации RADIUS

Подключение к серверу

- `set vpn sstp authentication radius server <server> port <port>`

  Определяет RADIUS сервер `<server>` и задает порт `<port>` для отправки запросов на аутентификацию.

- `set vpn sstp authentication radius server <server> key <secret>`

  Определяет RADIUS сервер `<server>` и задает общий ключ `<secret>` для защиты коммуникаций с сервером.

- `set vpn sstp authentication radius server <server> fail-time <time>`

  Помечает настроенный RADIUS сервер `<server>` как «не в сети» на заданный в секундах промежуток времени `<time>`.

- `set vpn sstp authentication radius server <server> disable`

  Отключает настроенный RADIUS сервер `<server>`.

Параметры работы

- `set vpn sstp authentication radius acct-timeout <timeout>`

  Определяет время ожидания `<timeout>` в секундах ответа на пакеты *Interim Update* от RADIUS сервера. По умолчанию - 3 секунды.

- `set vpn sstp authentication radius dynamic-author server <address>`

  Задает IP адрес `<address>` для сервера *Dynamic Authorization Extension (DM/CoA)*.

- `set vpn sstp authentication radius dynamic-author port <port>`

  Задает порт `<port>` для подключения к серверу *Dynamic Authorization Extension (DM/CoA)*.

- `set vpn sstp authentication radius dynamic-author key <secret>`

  Задает общий ключ `<secret>` для защиты коммуникаций с сервером *Dynamic Authorization Extension (DM/CoA)*.

- `set vpn sstp authentication radius max-try <number>`

  Определяет количество `<number>` попыток передачи серверу запросов *Access Request* и *Accounting Request*.

- `set vpn sstp authentication radius timeout <timeout>`

  Определяет время ожидания `<timeout>` в секундах ответа от сервера.

- `set vpn sstp authentication radius nas-identifier <identifier>`

  Задает значение идентификатора `NAS-Identifier`, который будет передан RADIUS серверу соответствующим атрибутом и должен соответствовать запросам *Dynamic Authorization Extension (DM/CoA)*.

- `set vpn sstp authentication radius nas-ip-address <address>`

  Определяет значение адреса `NAS-IP-Address`, который будет передан RADIUS серверу соответствующим атрибутом и должен соответствовать запросам *Dynamic Authorization Extension (DM/CoA)*. Также указанный адрес будет выбран в качестве адреса сервера *Dynamic Authorization Extension (DM/CoA)*.

- `set vpn sstp authentication radius source-address <address>`

  Задает IPv4 адрес `<address>` отправителя, который будет использоваться при формирования запросов на аутентификацию к RADIUS серверу.

- `set vpn sstp authentication radius rate-limit attribute <attribute>`

  Определяет в каком из атрибутов `<attribute>` RADIUS сервера будет храниться предельное значение полосы пропускания. По умолчанию таким атрибутом является атрибут `Filter-Id`.

- `set vpn sstp authentication radius rate-limit enable`

  Включает ограничение полосы пропускания средствами RADIUS сервера.

- `set vpn sstp authentication radius rate-limit vendor`

  Включает использование справочника атрибутов RADIUS сервера, который должен располагаться по следующему пути `/usr/share/accel-ppp/radius`.

2.4.7 DMVPN

2.4.7.1 Описание

DMVPN (Dynamic Multipoint Virtual Private Network) - технология динамического построения VPN, первоначально разработанная компанией Cisco. Хотя ее реализация и была в некоторой степени закрытой, лежащие в ее основе технологии в действительности основаны на вполне конкретных стандартах. В основе данной технологии лежит использование следующих протоколов:

- NHRP (Next Hop Resolution Protocol) - **RFC 2332**[59];
- mGRE (Multipoint Generic Routing Encapsulation) - **RFC 1702**[60];
- IPSec (IP Security) - **RFC 4301**[61].

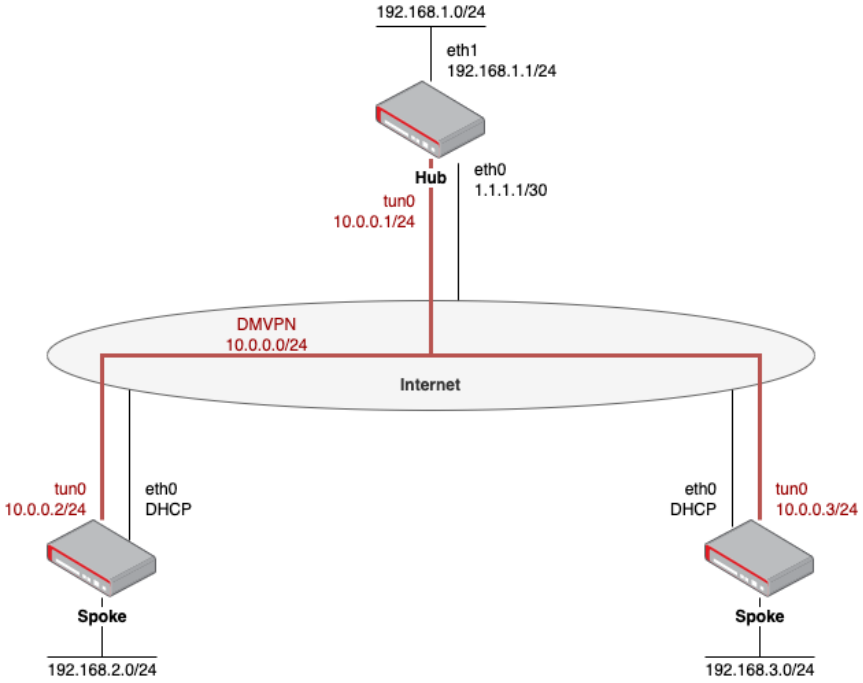
Протокол NHRP обеспечивает механизм динамического обнаружения конечных точек туннеля (поиск и их регистрация), протокол mGRE обеспечивает непосредственно инкапсуляцию данных, передаваемых по туннелю, а стек протоколов IPSec обеспечивает обмен ключами и криптографическую защиту передаваемых данных.

Другими словами, DMVPN обеспечивает возможность создания динамически связной VPN сети без предварительной (статической) настройки всех возможных конечных точек туннеля.

Примечание

Технология DMVPN автоматизирует только процесс обнаружения и настройки конечных точек туннеля. Полноценное решение также включает в себя использование протокола маршрутизации. Особенно хорошо для использования в данной технологии подходит протокол динамической маршрутизации BGP.

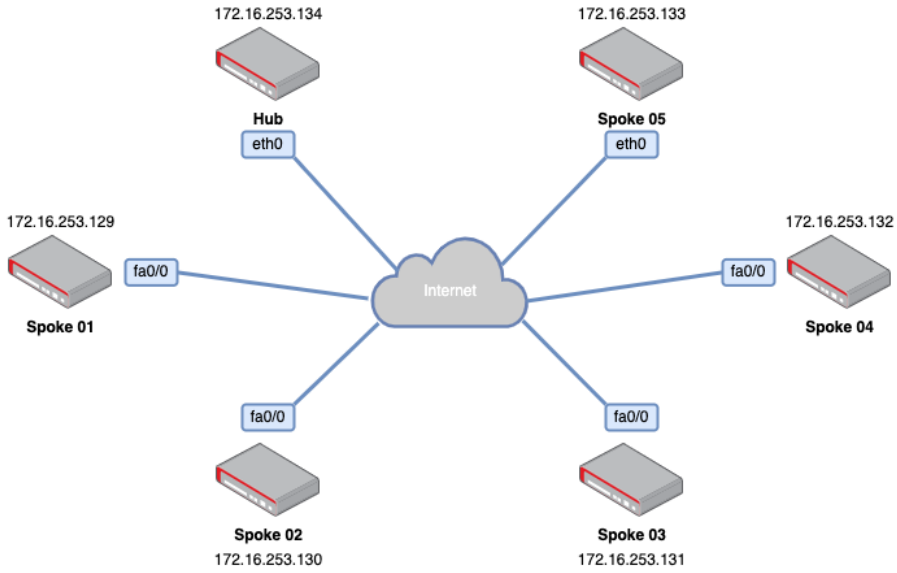
[59] https://datatracker.ietf.org/doc/html/rfc2332.html
[60] https://datatracker.ietf.org/doc/html/rfc1702.html
[61] https://datatracker.ietf.org/doc/html/rfc4301.html



2.4.7.2 Настройка

Пример настройки

Данный пример подразумевает использование устройства под управлением **ПО Факел** в качестве центрального узла (Hub), устройства под управлением **ПО Факел** в качестве одного из оконечных узлов (Spoke 05), а также устройств под управлением операционной системы Cisco IOS в качестве остальных оконечных узлов (Spoke 01 - 04).



Каждый узел (Hub, Spoke 01 - 05) использует IP адрес из подсети `172.16.253.128/29`.

Используемый в конфигурации ниже IP адрес `192.0.2.1`, являющийся глобальным адресом, по которому доступен центральный узел (Hub) для каждого из оконечных узлов (Spoke).

Центральный узел (Hub)

```
set interfaces ethernet eth0 address 192.0.2.1/24
set interfaces tunnel tun100 address '172.16.253.134/29'
set interfaces tunnel tun100 encapsulation 'gre'
set interfaces tunnel tun100 source-address '192.0.2.1'
set interfaces tunnel tun100 multicast 'enable'
set interfaces tunnel tun100 parameters ip key '1'
set protocols nhrp tunnel tun100 cisco-authentication 'secret'
set protocols nhrp tunnel tun100 holding-time '300'
set protocols nhrp tunnel tun100 multicast 'dynamic'
set protocols nhrp tunnel tun100 redirect
set protocols nhrp tunnel tun100 shortcut
set vpn ipsec esp-group ESP-HUB compression 'disable'
set vpn ipsec esp-group ESP-HUB lifetime '1800'
set vpn ipsec esp-group ESP-HUB mode 'transport'
set vpn ipsec esp-group ESP-HUB pfs 'dh-group2'
set vpn ipsec esp-group ESP-HUB proposal 1 encryption 'aes256'
set vpn ipsec esp-group ESP-HUB proposal 1 hash 'sha1'
set vpn ipsec esp-group ESP-HUB proposal 2 encryption '3des'
set vpn ipsec esp-group ESP-HUB proposal 2 hash 'md5'
set vpn ipsec ike-group IKE-HUB ikev2-reauth 'no'
set vpn ipsec ike-group IKE-HUB key-exchange 'ikev1'
set vpn ipsec ike-group IKE-HUB lifetime '3600'
set vpn ipsec ike-group IKE-HUB proposal 1 dh-group '2'
set vpn ipsec ike-group IKE-HUB proposal 1 encryption 'aes256'
set vpn ipsec ike-group IKE-HUB proposal 1 hash 'sha1'
set vpn ipsec ike-group IKE-HUB proposal 2 dh-group '2'
set vpn ipsec ike-group IKE-HUB proposal 2 encryption 'aes128'
set vpn ipsec ike-group IKE-HUB proposal 2 hash 'sha1'
set vpn ipsec ipsec-interfaces interface 'eth0'
set vpn ipsec profile NHRPVPN authentication mode 'pre-shared-secret'
set vpn ipsec profile NHRPVPN authentication pre-shared-secret 'secret'
set vpn ipsec profile NHRPVPN bind tunnel 'tun100'
set vpn ipsec profile NHRPVPN esp-group 'ESP-HUB'
set vpn ipsec profile NHRPVPN ike-group 'IKE-HUB'
```

Оконечные узлы (Spoke)

Конфигурации отдельных оконечных узлов будут отличаться только локальным IP адресом на интерфейсе `tun10`.

Узлы Spoke 01 - 04:

```
crypto keyring DMVPN
   pre-shared-key address 192.0.2.1 key secret
!
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
crypto isakmp policy 10
   encr aes 256
   authentication pre-share
   group 2
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 30 30 periodic
crypto isakmp profile DMVPN
   keyring DMVPN
   match identity address 192.0.2.1 255.255.255.255
!
crypto ipsec transform-set DMVPN-AES256 esp-aes 256 esp-sha-hmac
   mode transport
!
crypto ipsec profile DMVPN
   set security-association idle-time 720
   set transform-set DMVPN-AES256
   set isakmp-profile DMVPN
!
interface Tunnel10
   ! individual spoke tunnel IP must change
   ip address 172.16.253.129 255.255.255.248
   no ip redirects
   ip nhrp authentication secret
   ip nhrp map 172.16.253.134 192.0.2.1
   ip nhrp map multicast 192.0.2.1
   ip nhrp network-id 1
   ip nhrp holdtime 600
   ip nhrp nhs 172.16.253.134
   ip nhrp registration timeout 75
   tunnel source FastEthernet0/0
   tunnel mode gre multipoint
   tunnel protection ipsec profile DMVPN
   tunnel key 1
!
interface FastEthernet0/0
   ip address dhcp
   duplex half
```

Узел Spoke 05:

Устройство под управлением **ПО Факел** также может использовать технологию DMVPN в режиме оконечного узла (Spoke).

```
set interfaces ethernet eth0 address 'dhcp'
set interfaces tunnel tun100 address '172.16.253.133/29'
set interfaces tunnel tun100 source-address 0.0.0.0
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set interfaces tunnel tun100 encapsulation 'gre'
set interfaces tunnel tun100 multicast 'enable'
set interfaces tunnel tun100 parameters ip key '1'
set protocols nhrp tunnel tun100 cisco-authentication 'secret'
set protocols nhrp tunnel tun100 holding-time '300'
set protocols nhrp tunnel tun100 map 172.16.253.134/29 nbma-address '192.0.2.1'
set protocols nhrp tunnel tun100 map 172.16.253.134/29 register
set protocols nhrp tunnel tun100 multicast 'nhs'
set protocols nhrp tunnel tun100 redirect
set protocols nhrp tunnel tun100 shortcut
set vpn ipsec esp-group ESP-HUB compression 'disable'
set vpn ipsec esp-group ESP-HUB lifetime '1800'
set vpn ipsec esp-group ESP-HUB mode 'transport'
set vpn ipsec esp-group ESP-HUB pfs 'dh-group2'
set vpn ipsec esp-group ESP-HUB proposal 1 encryption 'aes256'
set vpn ipsec esp-group ESP-HUB proposal 1 hash 'sha1'
set vpn ipsec esp-group ESP-HUB proposal 2 encryption '3des'
set vpn ipsec esp-group ESP-HUB proposal 2 hash 'md5'
set vpn ipsec ike-group IKE-HUB close-action 'none'
set vpn ipsec ike-group IKE-HUB ikev2-reauth 'no'
set vpn ipsec ike-group IKE-HUB key-exchange 'ikev1'
set vpn ipsec ike-group IKE-HUB lifetime '3600'
set vpn ipsec ike-group IKE-HUB proposal 1 dh-group '2'
set vpn ipsec ike-group IKE-HUB proposal 1 encryption 'aes256'
set vpn ipsec ike-group IKE-HUB proposal 1 hash 'sha1'
set vpn ipsec ike-group IKE-HUB proposal 2 dh-group '2'
set vpn ipsec ike-group IKE-HUB proposal 2 encryption 'aes128'
set vpn ipsec ike-group IKE-HUB proposal 2 hash 'sha1'
set vpn ipsec ipsec-interfaces interface 'eth0'
set vpn ipsec profile NHRPVPN authentication mode 'pre-shared-secret'
set vpn ipsec profile NHRPVPN authentication pre-shared-secret 'secret'
set vpn ipsec profile NHRPVPN bind tunnel 'tun100'
set vpn ipsec profile NHRPVPN esp-group 'ESP-HUB'
set vpn ipsec profile NHRPVPN ike-group 'IKE-HUB'
```

2.4.7.3 Список команд

Основные настройки

- Обратитесь к разделу документации *Интерфейс туннеля* (страница 215) для детального ознакомления со связанными настройками туннелей.
- Обратитесь к разделу документации *Стек протоколов IPsec* (страница 372) для детального ознакомления со связанными настройками стека протоколов IPSec.

- `set protocols nhrp tunnel <tunnel> cisco-authentication <secret>`

  Активирует аутентификацию для коммуникаций по протоколу NHRP, аналогичную реализации DMVPN от компании Cisco. При этом в исходящие пакеты NHRP вставляется секретный ключ в

виде открытого текста. Входящие пакеты NHRP на соответствующем интерфейсе отбрасываются, если в них нет данного ключа. Максимальная длина секретного ключа - 8 символов.

- `set protocols nhrp tunnel <tunnel> dynamic-map <address> nbma-domain-name <fqdn>`

  Определяет, что NBMA (Non-Broadcast Multiple-Access Network) адреса серверов следующего узла определены в параметре `nbma-domain-name`. Для каждой записи механизм реализации протокола NHRP создает динамическую запись NHS (Next Hop Server).

  Каждая динамическая запись NHS получает информацию о соседнем участнике VPN сети с настроенным сетевым адресом и обнаруженным адресом NBMA.

  Первый запрос *Registration Request* посылается на широковещательный адрес, а реальный адрес сервера динамически определяется из первого ответа *Registration Reply*.

- `set protocols nhrp tunnel <tunnel> holding-time <timeout>`

  Определяет время удержания запросов *Registration Request* и ответов *Resolution Reply*, отправляемых с данного интерфейса. Время удержания указывается в секундах и по умолчанию равно двум часам.

- `set protocols nhrp tunnel <tunnel> map cisco`

  Данную команда используется, если соседний участник VPN сети является устройством под управлением операционной системы Cisco IOS. При использовании данной команды будет статически зафиксировано значение параметра *Registration Request ID*, чтобы в случае изменения адреса NBMA соответствующий запрос *Purge Request* был отправлен. Данная команда используется, как правило, для обхода ограничения устройства под управлением операционной системы Cisco IOS, которое требует соответствия между параметром *Purge Request ID* и оригинальным параметром *Registration Request ID*.

- `set protocols nhrp tunnel <tunnel> map nbma-address <address>`

  Задает для соседнего участника VPN сети статическое соответствие адреса, используемого протоколом, адресу NBMA.

  Если маска для префикса IP задана, то реализации протокола NHRP будет использовать данного участника VPN сети в качестве следующего узла при отправке запросов *Resolution Requests*, соответствующих указанной подсети.

  Заданный адрес является IP адресом или именем FQDN центрального узла (Hub).

- `set protocols nhrp tunnel <tunnel> map register`

  Определяет, путем использования необязательного параметра `register`, что запрос *Registration Request* должен быть отправлен данному участнику VPN сети при запуске механизма. Параметр `register`, однако, является обязательным при настройке оконечного узла (Spoke).

- `set protocols nhrp tunnel <tunnel> multicast <dynamic | nhs>`

  Определяет, каким образом реализация протокола NHRP будет осуществлять «мягкое» переключение трафика группового вещания. На данный момент реализация протокола NHRP предусматривает перехват трафика группового вещания при помощи пакетного сокета и его отправки обратно соответствующему получателю, что требует значительных затрат ресурсов процессора.

  Использование записей NHS приведет к тому, что весь трафик группового вещания будет перенаправлен каждому статически заданному следующему узлу.

  Лучшие практики предписывают пересылать трафик группового вещания всем участникам VPN сети, с которыми установлено прямое соединение. Альтернативно можно использовать данную

команду несколько раз для каждого адреса, используемого протоколом, на который должен быть отправлен трафик группового вещания.

Предупреждение

Будьте внимательны при настройке обработки трафика группового вещания при использовании множественных записей NHS.

- `set protocols nhrp tunnel <tunnel> non-caching`

  Отключает кэширование информации об участниках VPN сети, получаемой из перенаправляемых пакетов NHRP *Resolution Reply*. Использование данной команды может потребление памяти на больших NBMA подсетях.

- `set protocols nhrp tunnel <tunnel> redirect`

  Включает отправку пакетов NHRP *Traffic Indication* по аналогии с реализацией от компании Cisco. Если эта функция включена и реализация протокола NHRP обнаруживает перенаправленный пакет, то механизм отправит сообщение оригинальному отправителю сообщение с указанием на необходимость создания прямого соединения с получателем. Другими словами данная функция является эквивалентом сообщения *ICMP Redirect*.

- `set protocols nhrp tunnel <tunnel> shortcut`

  Создает «короткий» (shortcut) маршрут. Полученный пакет NHRP *Traffic Indication* инициирует процесс разрешения и установления «короткого» маршрута.

- `set protocols nhrp tunnel <tunnel> shortcut-destination`

  Предписывает реализации протокола NHRP авторизованно отвечать на пакеты NHRP *Resolution Requests*, направленные на адреса данного интерфейса вместо перенаправления пакетов. Это позволяет создавать «короткие» маршруты к подсетям, расположенным за этим интерфейсом. Данная команда должна быть использована для каждого интерфейса в отдельности.

- `set protocols nhrp tunnel <tunnel> shortcut-target <address>`

  Определяет префикс сети за пределами NBMA, для которого GRE интерфейс будет выступать в качестве шлюза. Такой подход является альтернативным определению локальных интерфейсов с флагом `shortcut-destination`.

- `set protocols nhrp tunnel <tunnel> shortcut-target <address> holding-time <timeout>`

  Определяет время удержания запросов *Registration Request* и ответов *Resolution Reply*, отправляемых с данного интерфейса или целевого узла, доступного через «короткий» маршрут. Время удержания указывается в секундах и по умолчанию равно двум часам.

2.4.8 Site-to-Site VPN

2.4.8.1 Описание

Подход к построению VPN сети Site-to-Site подразумевает добавление удаленных участников VPN сети, которые могут быть сконфигурированы для обмена зашифрованной информацией между ними и устройством под управлением **ПО Факел** или подключенными к ним сетями.

Для конфигурирования Site-to-Site подключений необходимо добавить участников VPN сети с помощью команды `set vpn ipsec site-to-site`.

Удаленный участник VPN сети может быть идентифицирован с помощью следующих данных:

- IPv4 или IPv6 адреса. Этот способ является самым простым и используется в случае назначения участникам VPN сети статических публичных IP адресов.
- Имя хоста. Этот способ аналогичен предыдущему, только с одним отличием - указывается DNS имя участника VPN сети вместо IP адреса. Используется в случае, если участник имеет публичный IP адрес и DNS имя, но IP адрес может иногда изменяться.
- Идентификатор удаленного участника VPN сети. Этот способ не предусматривает задания IP-адреса или DNS имени участника VPN сети. Используется в случае, если участник не имеет доступных публичных IP адресов (например, в случае использования трансляции адресов - NAT) или IP адреса могут быть изменены.

Каждый участник VPN сети Site-to-Site располагает следующим набором параметров:

- `authentication` - набор параметров аутентификации между устройством под управлением **ПО Факел** и удаленным участником VPN сети:
  - `id` - локальный идентификатор устройства под управлением **ПО Факел**. Если данный параметр задан, то в процессе аутентификации он будет направлен удаленному участнику VPN сети;
  - `mode` - режим аутентификации между устройством под управлением **ПО Факел** и удаленным участником VPN сети:
    - `pre-shared-secret` - последовательность символов, представляющая собой общий секретный ключ, который должен быть одинаковым как для локальной, так и для удаленной стороны защищенной коммуникации;
    - `rsa` - общий RSA ключ, который должен быть определен в секции `set vpn rsa-keys` конфигурации;
    - `x509` - инфраструктура сертификатов, используемая для аутентификации.
  - `pre-shared-secret` - общий секретный ключ, используется в случае, если задан параметр `mode pre-shared-secret`;
  - `remote-id` - идентификатор удаленного участника VPN сети, который используется вместо DNS имени или IP адреса. Данный параметр рекомендуется использовать в случае, если удаленный участник VPN сети находится за устройством с настроенным механизмом трансляции адресов (NAT) или если задан параметр `mode x509`;
  - `rsa-key-name` - общий RSA ключ, используемый для аутентификации, который должен быть определен в секции `set vpn rsa-keys` конфигурации;

  - `use-x509-id` - признак использования локального идентификатора из сертификата *X.509*. Данный параметр не может быть использован совместно с заданным параметром `id`;
  - `x509` - набор параметров аутентификации с использованием сертификатов *X.509*:
    * `ca-cert-file` - путь до файла сертификата удостоверяющего центра. Используется для аутентификации удаленного участника VPN сети;
    * `cert-file` - путь до файла сертификата, используемого для аутентификации локального участника VPN сети по отношению к удаленному участнику;
    * `crl-file` - путь до файла со списком отозванных сертификатов, который используется для проверки действительности сертификата удаленного участника VPN сети;
    * `key` - закрытый ключ, который используется для аутентификации локального участника VPN сети по отношению к удаленному участнику:
      · `file` - путь до контейнера с закрытым ключом;
      · `password` - пароль для доступа к контейнеру с закрытым ключом (опционально).
- `connection-type` - режим взаимодействия устройства под управлением **ПО Факел** с удаленными участниками VPN сети:
  - `initiate` - режим, при котором устройство пытается установить соединение с удаленным участником VPN сети сразу после применения конфигурации и после перезагрузки. В этом режиме соединение не будет установлено повторно в случае его разрыва. Рекомендуется использовать только совместно механизмом DPD (Dead Peer Detection) или другими механизмами контроля соединений.
  - `respond` - режим, при котором устройство не пытается установить соединение с удаленным участником VPN сети. В этом режиме IPSec-сессия будет установлена по инициативе удаленного участника. Рекомендуется использовать в случае, если отсутствует прямое подключение к удаленному участнику, например, из-за того, что он находится за межсетевым экраном или устройством с настроенным механизмом трансляции адресов (NAT).
- `default-esp-group` - группа алгоритмов для протокола ESP по умолчанию, которая будет использована при шифровании передаваемых данных. Группа может быть переопределена отдельными настройками туннеля или VTI интерфейса;
- `description` - краткое описание для локального участника VPN сети;
- `dhcp-interface` - признак использования IP адреса, полученного локальным участником VPN сети по протоколу DHCP, для установления IPSec сессий вместо адреса, указанного в параметре `local-address`;
- `force-encapsulation` - признак принудительной инкапсуляции ESP пакетов в UDP. Рекомендуется использовать в случае, если между локальным и удаленным участниками VPN сети находится межсетевой экран или устройство с настроенным механизмом трансляции адресом (NAT), которое не может обрабатывать ESP пакеты;
- `ike-group` - группа алгоритмов для протокола IKE, которая будет использована при обмене ключами;
- `ikev2-reauth` - режим повторной аутентификации удаленного участника VPN сети при смене ключей, которая выполняется только в рамках протокола IKEv2:

  - `yes` - режим, при котором со сменой ключей осуществляется попытка повторного создания всех ранее созданных записей в новой таблице SA (Security Associations);
  - `no` - режим, при котором со сменой ключей не происходит изменений изменений в части записей таблицы SA;
  - `inherit` - режим, при котором со сменой ключей используется порядок действий по умолчанию, обусловленный выбранной группой алгоритмов для протокола IKE.
- `local-address` - локальный IP адрес для подключения к данному участнику VPN сети. При значении `any` используется IP адрес интерфейса, на который указывает маршрут по умолчанию.
- `tunnel` - классификатор трафика, при соответствии которому принимается решение о шифровании данных, перед их передачей другому участнике VPN сети:
  - `disable` - признак отключения данного туннеля;
  - `esp-group` - группа алгоритмов для протокола ESP по отношению к выбранному туннелю;
  - `local` - локальный отправитель трафика, для которого выполняется шифрование перед передачей данному участнику VPN сети:
    - `port` - номер порта отправителя, учитывается только при совместном использовании с параметром `prefix`;
    - `prefix` - IP адрес сети на локальной стороне.
  - `protocol` - протокол, для которого выполняется шифрование перед передачей данному участнике VPN сети;
  - `remote` - удаленный получатель трафика, для которого выполняется шифрование перед передачей данному участнику VPN сети:
    - `port` - номер порта отправителя, учитывается только при совместном использовании с параметром `prefix`;
    - `prefix` - IP адрес сети на удаленной стороне.
- `vti` - набор параметров использования VTI интерфейса для шифрования трафика. Любой трафик, который будет отправлен на VTI интерфейс, будет зашифрован и отправлен данному участнику VPN сети. Использование VTI интерфейса упрощает настройку механизма IPSec и предоставляет некоторую гибкость в сложных сценариях использования, а также позволяет динамически добавлять и удалять сети, доступные через удаленного участника VPN сети, так как в этом режиме для устройства не требуется создание дополнительных записей в таблице SA или политик SP (Security Policy) для каждой удаленной сети:
  - `bind` - параметр, который позволяет выбрать и привязать к данному участнике VPN сети определенный VTI интерфейс;
  - `esp-group` - группа алгоритмов для протокола ESP, которая будет использована для шифрования трафика, проходящего через данный VTI интерфейс.

2.4.8.2 Настройка

Пример настройки

Протокол IKEv1

В данном примере рассматривается настройка взаимодействия двух устройств, которые для удобства обозначены **Левой стороной** и **Правой стороной** соответственно, при следующих условиях:

- в качестве внешнего (WAN) интерфейса рассматривается интерфейс `eth1`;
- левая подсеть с адресом `192.168.0.0/24` рассматривается как сеть головного офиса;
- локальный IP адрес левой стороны `198.51.100.3` рассматривается как внешний (WAN) IP адрес головного офиса;
- правая подсеть с адресом `10.0.0.0/24` рассматривается как сеть удаленного филиала;
- локальный IP адрес правой стороны `203.0.113.2` рассматривается как внешний (WAN) IP адрес удаленного филиала;

```
# hq side
set vpn ipsec esp-group office-srv-esp compression 'disable'
set vpn ipsec esp-group office-srv-esp lifetime '1800'
set vpn ipsec esp-group office-srv-esp mode 'tunnel'
set vpn ipsec esp-group office-srv-esp pfs 'enable'
set vpn ipsec esp-group office-srv-esp proposal 1 encryption 'aes256'
set vpn ipsec esp-group office-srv-esp proposal 1 hash 'sha1'
set vpn ipsec ike-group office-srv-ike ikev2-reauth 'no'
set vpn ipsec ike-group office-srv-ike key-exchange 'ikev1'
set vpn ipsec ike-group office-srv-ike lifetime '3600'
set vpn ipsec ike-group office-srv-ike proposal 1 encryption 'aes256'
set vpn ipsec ike-group office-srv-ike proposal 1 hash 'sha1'
set vpn ipsec ipsec-interfaces interface 'eth1'
set vpn ipsec site-to-site peer 203.0.113.2 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 203.0.113.2 authentication pre-shared-secret
  'SomePreSharedKey'
set vpn ipsec site-to-site peer 203.0.113.2 ike-group 'office-srv-ike'
set vpn ipsec site-to-site peer 203.0.113.2 local-address '198.51.100.3'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 allow-public-networks 'disable
  '
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 esp-group 'office-srv-esp'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 local prefix '192.168.0.0/24'
set vpn ipsec site-to-site peer 203.0.113.2 tunnel 0 remote prefix '10.0.0.0/21'
```

```
# branch side
set vpn ipsec esp-group office-srv-esp compression 'disable'
set vpn ipsec esp-group office-srv-esp lifetime '1800'
set vpn ipsec esp-group office-srv-esp mode 'tunnel'
set vpn ipsec esp-group office-srv-esp pfs 'enable'
set vpn ipsec esp-group office-srv-esp proposal 1 encryption 'aes256'
set vpn ipsec esp-group office-srv-esp proposal 1 hash 'sha1'
set vpn ipsec ike-group office-srv-ike ikev2-reauth 'no'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set vpn ipsec ike-group office-srv-ike key-exchange 'ikev1'
set vpn ipsec ike-group office-srv-ike lifetime '3600'
set vpn ipsec ike-group office-srv-ike proposal 1 encryption 'aes256'
set vpn ipsec ike-group office-srv-ike proposal 1 hash 'sha1'
set vpn ipsec ipsec-interfaces interface 'eth1'
set vpn ipsec site-to-site peer 198.51.100.3 authentication mode 'pre-shared-secret
  '
set vpn ipsec site-to-site peer 198.51.100.3 authentication pre-shared-secret
  'SomePreSharedKey'
set vpn ipsec site-to-site peer 198.51.100.3 ike-group 'office-srv-ike'
set vpn ipsec site-to-site peer 198.51.100.3 local-address '203.0.113.2'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 allow-nat-networks 'disable'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 allow-public-networks
  'disable'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 esp-group 'office-srv-esp'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 local prefix '10.0.0.0/21'
set vpn ipsec site-to-site peer 198.51.100.3 tunnel 0 remote prefix '192.168.0.0/24
  '
```

После этого необходимо убедиться в результатах конфигурирования.

```
fakel@hq:~$ show vpn ike sa
Peer ID / IP                            Local ID / IP
------------                            -------------
203.0.113.2                             198.51.100.3

State   Encrypt   Hash   D-H Grp   NAT-T   A-Time   L-Time
-----   -------   ----   -------   -----   ------   ------
up      aes256    sha1   5         no      734      3600

fakel@hq:~$ show vpn ipsec sa
Peer ID / IP                            Local ID / IP
------------                            -------------
203.0.113.2                             198.51.100.3

Tunnel   State   Bytes Out/In   Encrypt   Hash   NAT-T   A-Time   L-Time   Proto
------   -----   ------------   -------   ----   -----   ------   ------   -----
0        up      7.5M/230.6K    aes256    sha1   no      567      1800     all
```

При настроенных правилах трансляции адреса отправителя (SNAT) на интерфейсе `eth1` необходимо добавить исключающее правило.

```
# hq side
set nat source rule 10 destination address '10.0.0.0/24'
set nat source rule 10 'exclude'
set nat source rule 10 outbound-interface 'eth1'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set nat source rule 10 source address '192.168.0.0/24'
```

```
# branch side
set nat source rule 10 destination address '192.168.0.0/24'
set nat source rule 10 'exclude'
set nat source rule 10 outbound-interface 'eth1'
set nat source rule 10 source address '10.0.0.0/24'
```

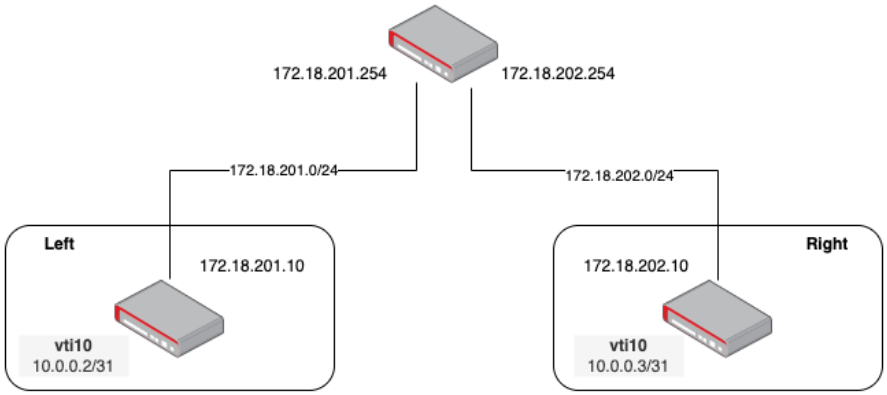
Для прохождения трафика, адресованного клиентским хостам, необходимо добавить соответствующие разрешающие правила фильтрации.

```
# hq side
set firewall name OUTSIDE-LOCAL rule 32 action 'accept'
set firewall name OUTSIDE-LOCAL rule 32 source address '10.0.0.0/24'
```

```
# branch side
set firewall name OUTSIDE-LOCAL rule 32 action 'accept'
set firewall name OUTSIDE-LOCAL rule 32 source address '192.168.0.0/24'
```

Протокол IKEv2

Рассмотрим следующую топологию сети.



Примечание

Использование маски /31 для подсети туннеля допускается подключений «точка-точка» согласно RFC 3021[62].

Настройки на левой стороне:

[62] https://datatracker.ietf.org/doc/html/rfc3021.html

```
set interfaces vti vti10 address '10.0.0.2/31'
set vpn ipsec esp-group ESP_DEFAULT compression 'disable'
set vpn ipsec esp-group ESP_DEFAULT lifetime '3600'
set vpn ipsec esp-group ESP_DEFAULT mode 'tunnel'
set vpn ipsec esp-group ESP_DEFAULT pfs 'dh-group19'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection action 'hold'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection interval '30'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection timeout '120'
set vpn ipsec ike-group IKEv2_DEFAULT ikev2-reauth 'no'
set vpn ipsec ike-group IKEv2_DEFAULT key-exchange 'ikev2'
set vpn ipsec ike-group IKEv2_DEFAULT lifetime '10800'
set vpn ipsec ike-group IKEv2_DEFAULT mobike 'disable'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 dh-group '19'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ipsec-interfaces interface 'eth0.201'
set vpn ipsec site-to-site peer 172.18.202.10 authentication id '172.18.201.10'
set vpn ipsec site-to-site peer 172.18.202.10 authentication mode
  'pre-shared-secret'
set vpn ipsec site-to-site peer 172.18.202.10 authentication pre-shared-secret
  'secretkey'
set vpn ipsec site-to-site peer 172.18.202.10 authentication remote-id
  '172.18.202.10'
set vpn ipsec site-to-site peer 172.18.202.10 connection-type 'initiate'
set vpn ipsec site-to-site peer 172.18.202.10 ike-group 'IKEv2_DEFAULT'
set vpn ipsec site-to-site peer 172.18.202.10 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 172.18.202.10 local-address '172.18.201.10'
set vpn ipsec site-to-site peer 172.18.202.10 vti bind 'vti10'
set vpn ipsec site-to-site peer 172.18.202.10 vti esp-group 'ESP_DEFAULT'
```

Настройки на правой стороне:

```
set interfaces vti vti10 address '10.0.0.3/31'
set vpn ipsec esp-group ESP_DEFAULT compression 'disable'
set vpn ipsec esp-group ESP_DEFAULT lifetime '3600'
set vpn ipsec esp-group ESP_DEFAULT mode 'tunnel'
set vpn ipsec esp-group ESP_DEFAULT pfs 'dh-group19'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec esp-group ESP_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection action 'hold'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection interval '30'
set vpn ipsec ike-group IKEv2_DEFAULT dead-peer-detection timeout '120'
set vpn ipsec ike-group IKEv2_DEFAULT ikev2-reauth 'no'
set vpn ipsec ike-group IKEv2_DEFAULT key-exchange 'ikev2'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

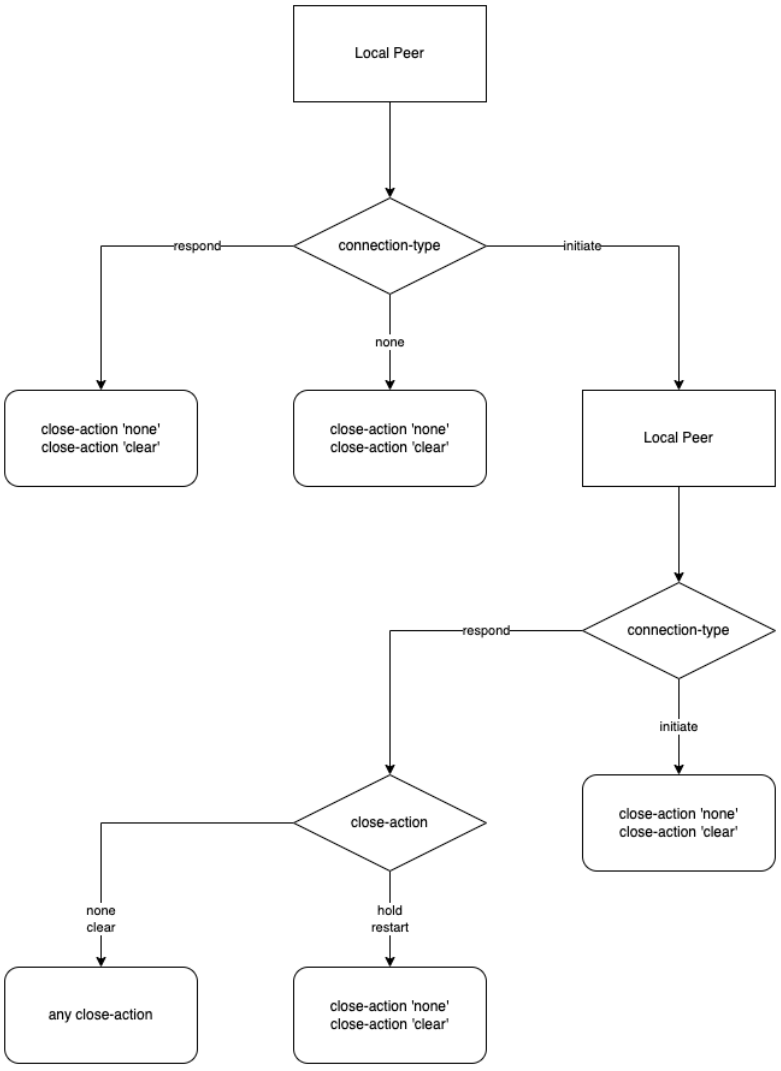
```
set vpn ipsec ike-group IKEv2_DEFAULT lifetime '10800'
set vpn ipsec ike-group IKEv2_DEFAULT mobike 'disable'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 dh-group '19'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 encryption 'aes256gcm128'
set vpn ipsec ike-group IKEv2_DEFAULT proposal 10 hash 'sha256'
set vpn ipsec ipsec-interfaces interface 'eth0.202'
set vpn ipsec site-to-site peer 172.18.201.10 authentication id '172.18.202.10'
set vpn ipsec site-to-site peer 172.18.201.10 authentication mode
  'pre-shared-secret'
set vpn ipsec site-to-site peer 172.18.201.10 authentication pre-shared-secret
  'secretkey'
set vpn ipsec site-to-site peer 172.18.201.10 authentication remote-id
  '172.18.201.10'
set vpn ipsec site-to-site peer 172.18.201.10 connection-type 'initiate'
set vpn ipsec site-to-site peer 172.18.201.10 ike-group 'IKEv2_DEFAULT'
set vpn ipsec site-to-site peer 172.18.201.10 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 172.18.201.10 local-address '172.18.202.10'
set vpn ipsec site-to-site peer 172.18.201.10 vti bind 'vti10'
set vpn ipsec site-to-site peer 172.18.201.10 vti esp-group 'ESP_DEFAULT'
```

В данном примере используются ключевые параметры, представленные ниже.

- `authentication local-id/remote-id` - идентификация IKE используется для валидации устройств участников VPN в процессе фазы согласования IKE. Если вы не будете использовать параметры `local-id` или `remote-id`, по умолчанию устройство будет использовать IPv4 или IPv6 адрес, соответствующий локальному или удаленному участнику VPN сети соответственно. В некоторых сетевых конфигурация, например, если используется интерфейс IPSec с динамическим адресом или устройство находится за другим устройством с настроенным механизмом трансляции адресов (NAT), идентификатор IKE, полученный от участника VPN сети, не будет совпадать со шлюзом IKE, настроенным на устройстве. Это может привести к сбою валидации в ходе Фазы 1 IKE. Поэтому очень важно убедиться в том, что параметры `local-id` или `remote-id` заданы, а также в том, что идентификатор IKE соответствует значению `remote-id`, сконфигурированному на другом участнике VPN сети
- `disable-route-autoinstall` - данная опция отключает использование маршрутов, установленных в таблице по умолчанию с идентификатором 220 для поддержки маршрутизации в топологии Site-to-Site. Данная таблица в основном используется при настройке VTI интерфейсов.
- `dead-peer-detection action = clear | hold | restart` - данная опция предусматривает периодическую отправку участнику VPN сети сообщений *R_U_THERE* (IKEv1) и пустых сообщений *INFORMATIONAL* (IKEv2) для проверки работоспособности. Значения `clear`, `hold` и `restart` активируют механизм DPD и определяют действия при истечении соответствующего тайм-аута. При использовании значения `clear` соединение разрывается без каких-либо дальнейших действий. При использовании значения `hold` устанавливается политика перехвата подходящего трафика с попыткой повторного согласования соединения по запросу. При использовании значения `restart` выполняется безусловная попытка повторного согласования соединения.
- `close-action = none | clear | hold | restart` - данная опция определяет действие, ко-

торое необходимо предпринять в случае, если удаленный участник VPN сети непредвиденно удаляет дочернюю запись SA (CHILD_SA). Значение `close` не должно использоваться, если участник VPN сети использует повторную аутентификацию или уникальные идентификаторы. Когда данная опция установлена для участников, необходимо внимательно выбирать режим взаимодействия, задаваемый параметром `connection-type`. Например, если опция установлена для обоих участников VPN сети, то оба участника будут пытаться инициировать и удерживать открытыми соединения, соответствующие каждой дочерней записи SA (CHILD_SA). Это может привести к нестабильной работе устройства или исчерпанию ресурсов процессора и памяти.

Представленная ниже схема алгоритма отражает возможные комбинации в зависимости от конфигурации участника VPN сети.



Аналогичные комбинации применимы и в случае использования механизма DPD.

2.4.8.3 Список команд

Базовые настройки

- set vpn ipsec esp-group <text> compression <enable | disable>
- set vpn ipsec esp-group <text> lifetime <30-86400>
- set vpn ipsec esp-group <text> mode <tunnel | transport>
- set vpn ipsec esp-group <text> pfs <enable | disable | dh-groupN>
- set vpn ipsec esp-group <text> proposal <1-65535> encryption <type>
- set vpn ipsec esp-group <text> proposal <1-65535> hash <type>
- set vpn ipsec ike-group <text> ikev2-reauth <yes | no>
- set vpn ipsec ike-group <text> key-exchange <ikev1 | ikev2>
- set vpn ipsec ike-group <text> lifetime <30-86400>
- set vpn ipsec ike-group <text> proposal <1-65535> encryption <type>
- set vpn ipsec ike-group <text> proposal <1-65535> hash <type>
- set vpn ipsec ipsec-interfaces interface <ethN>
- set vpn ipsec site-to-site peer <x.x.x.x> authentication mode <pre-shared-secret | rsa | x509>'
- set vpn ipsec site-to-site peer <x.x.x.x> authentication pre-shared-secret <text>
- set vpn ipsec site-to-site peer <x.x.x.x> ike-group <text>
- set vpn ipsec site-to-site peer <x.x.x.x> local-address <x.x.x.x>
- set vpn ipsec site-to-site peer <x.x.x.x> tunnel <0-4294967295> allow-nat-networks <enable | disable>
- set vpn ipsec site-to-site peer <x.x.x.x> tunnel <0-4294967295> allow-public-networks <enable | disable>
- set vpn ipsec site-to-site peer <x.x.x.x> tunnel <0-4294967295> esp-group <text>
- set vpn ipsec site-to-site peer <x.x.x.x> tunnel <0-4294967295> local prefix <x.x.x.x/x>
- set vpn ipsec site-to-site peer <x.x.x.x> tunnel <0-4294967295> remote prefix <x.x.x.x/x>
- set interfaces vti <vtiN> address <x.x.x.x/x>
- set vpn ipsec ike-group <text> dead-peer-detection action <hold | clear | restart>
- set vpn ipsec ike-group <text> dead-peer-detection interval <2-86400>

- set vpn ipsec ike-group <text> dead-peer-detection timeout <2-86400>
- set vpn ipsec ike-group <text> mobike <enable | disable>
- set vpn ipsec ike-group <text> proposal <1-65535> dh-group <number>
- set vpn ipsec site-to-site peer <x.x.x.x> authentication id <x.x.x.x>
- set vpn ipsec site-to-site peer <x.x.x.x> authentication remote-id <x.x.x.x>
- set vpn ipsec site-to-site peer <x.x.x.x> connection-type <initiate | respond>
- set vpn ipsec site-to-site peer <x.x.x.x> ike-group <text>
- set vpn ipsec site-to-site peer <x.x.x.x> ikev2-reauth <yes | no | inherit>
- set vpn ipsec site-to-site peer <x.x.x.x> local-address <x.x.x.x>
- set vpn ipsec site-to-site peer <x.x.x.x> vti bind <vtiN>
- set vpn ipsec site-to-site peer <x.x.x.x> vti esp-group <text>

2.5 Контроль трафика

В **ПО Факел** контроль трафика реализован следующими механизмами:

- *Межсетевой экран* (страница 416)
- *Преобразование сетевых адресов (NAT)* (страница 584)

2.5.1 Межсетевой экран

2.5.1.1 Обзор

Межсетевой экран на маршрутизаторе Факел — это встроенный инструмент анализа и фильтрации трафика. Обеспечивает защиту сети и отслеживает пакеты на всех этапах: с момента попадания на сетевой интерфейс и до передачи целевому приложению или другому устройству.

Более подробно каждая функция описана в соответствующем подразделе.

Список основных функций:

- фильтрация IPv4- и IPv6-трафика согласно установленным правилам,
- фильтрация согласно группам межсетевого экрана,
- фильтрация согласно зонам доступа,
- фильтрация согласно таблицам потоков,
- работа в режиме моста,
- анализ трафика и журналирование событий.

Маршрутизатор Факел распределяет пакеты по *потокам* — направлениям движения трафика. Существуют три основных потока: INPUT, FORWARD и OUTPUT. INPUT — для трафика, которому будет разрешен доступ во внутреннюю сеть маршрутизатора Факел. OUTPUT — это трафик, который маршрутизатор Факел инициирует сам и отправляет во внешнюю сеть. FORWARD — пропускает трафик мимо межсетевого экрана. Исключением являются зоны доступа, где вместо потока FORWARD используется поток LOCAL, который обозначает приложения, сервисы и процессы, запущенные на маршрутизаторе Факел.

Правила фильтрации настраиваются отдельно для каждого потока. База правил способна хранить до 999999 уникальных фильтрующих значений. В соответствии с заданными правилами пакеты будут допущены во внутреннюю сеть, отброшены или перенаправлены. Поддерживаются протоколы IPv4 и IPv6.

Компоненты межсетевого экрана настраиваются отдельно. Однако есть ряд команд, которые оказывают влияние на все элементы системы и применяются *глобально*. Этот раздел описывает глобальные команды.

2.5.1.2 Пример настройки

Шаг	Команда	Описание
1	set firewall global-options all-ping `enable`	Включает отправку ответов на служебные ICMP-сообщения, адресованные локальным сервисам
2	set firewall global-options state-policy established action `accept`	Разрешает во внутреннюю сеть все входящие пакеты от установленных соединений
3	set firewall global-options state-policy invalid action `drop`	Отбрасывает без оповещения отправителя все входящие пакеты с неправильной информацией о TCP-состоянии
4	set firewall global-options state-policy related action `accept`	Разрешает все входящие пакеты, которые относятся к уже установленным соединениям, но не но не принадлежат к основному потоку, будут допущены во внутреннюю сеть

2.5.1.3 Список команд

Режим «Конфигурирование»

firewall global-options all-ping [<enable> | <disable>]

Описание:

Включает или выключает отправку ответов на служебные ICMP-сообщения, адресованные локальным сервисам. Команда не будет иметь эффекта, если на межсетевом экране настроены правила, блокирующие ответы на служебные ICMP-сообщения.

Синтаксис:

- set firewall global-options all-ping `[<enable> | <disable>]`
- delete firewall global-options all-ping `[<enable> | <disable>]`
- show firewall global-options all-ping

Аргументы:

- `<enable>` — включает или выключает отправку ответов на служебные ICMP-сообщения;
- `<disable>` — выключает отправку ответов на служебные ICMP-сообщения.

Режим: «Конфигурирование».

Примечание

Команда работает только на потоке LOCAL.

---

firewall global-options apply-to-bridged-traffic [<ipv4> | <ipv6>]

Описание:

Применяет к IPv4- или IPv6-трафику, проходящему через межсетевой экран в режиме моста те же правила, которые применяются и к обычному трафику.

Синтаксис:

- set firewall global-options apply-to-bridged-traffic `[<ipv4> | <ipv6>]`
- delete firewall global-options apply-to-bridged-traffic `[<ipv4> | <ipv6>]`
- show firewall global-options apply-to-bridged-traffic

Аргументы:

- <ipv4> — применяет правила к IPv4-трафику;
- <ipv6> — применяет правила к IPv6-трафику.

Режим: «Конфигурирование».

---

firewall global-options broadcast-ping [<enable> | <disable>]

Описание:

Включает или выключает отправку ответов на широковещательные ICMP-сообщения.

Изменяет следующие параметры: *net.ipv4.icmp_echo_ignore_broadcasts*.

Синтаксис:

- set firewall global-options broadcast-ping [<enable> | <disable>]
- delete firewall global-options broadcast-ping [<enable> | <disable>]
- show firewall global-options broadcast-ping

Аргументы:

- <enable> — включает отправку ответов на широковещательные ICMP-сообщения;
- <disable> — выключает отправку ответов на широковещательные ICMP-сообщения.

Режим: «Конфигурирование».

---

firewall global-options ip-src-route [<enable> | <disable>]

Описание:

Включает или выключает маршрутизацию от источника для IPv4-трафика.

Изменяет следующие параметры ядра: *net.ipv4.conf.all.accept_source_route*.

Синтаксис:

- set firewall global-options ip-src-route [<enable> | <disable>]
- delete firewall global-options ip-src-route [<enable> | <disable>]
- show firewall global-options ip-src-route

Аргументы:

- <enable> — включает маршрутизацию от источника;
- <disable> — выключает маршрутизацию от источника.

Режим: «Конфигурирование».

---

firewall global-options ipv6-src-route [<enable> | <disable>]

Описание:

Включает или отключает маршрутизацию от источника для IPv6-трафика.

Изменяет следующие параметры ядра: *net.ipv6.conf.all.accept_source_route*.

Синтаксис:

- set firewall global-options ipv6-src-route [<enable> | <disable>]
- delete firewall global-options ipv6-src-route [<enable> | <disable>]
- show firewall global-options ipv6-src-route

Аргументы:

- <enable> — включает маршрутизацию от источника;
- <disable> — выключает маршрутизацию от источника.

Режим: «Конфигурирование».

---

firewall global-options receive-redirects [<enable> | <disable>]

Описание:

Включает или выключает прием ICMP-сообщений для перенаправления IPv4-трафика.

Изменяет следующие параметры ядра: *net.ipv4.conf.all.accept_source_route*.

Синтаксис:

- set firewall global-options receive-redirects [<enable> | <disable>]
- delete firewall global-options receive-redirects [<enable> | <disable>]
- show firewall global-options receive-redirects

Аргументы:

- <enable> — включает прием ICMP-сообщений для перенаправления IPv4-трафика;
- <disable> — выключает прием ICMP-сообщений для перенаправления IPv4-трафика.

Режим: «Конфигурирование».

---

firewall global-options resolver-cache

Описание:

Сохраняет в локальный кэш IP-адреса, недавно полученные от DNS-преобразователя.

Синтаксис:

- set firewall global-options resolver-cache
- delete firewall global-options resolver-cache
- show firewall global-options

Режим: «Конфигурирование».

---

firewall global-options resolver-interval <10-3600>

Описание:

Задает периодичность, с которой межсетевой экран будет обращаться к DNS-преобразователю для получения IP-адреса ресурса.

Синтаксис:

- set firewall global-options resolver-interval <10-3600>
- delete firewall global-options resolver-interval <10-3600>
- show firewall global-options resolver-interval

Аргументы:

- <10-3600> — временной интервал. Формат: секунды. Диапазон значений: от 10 до 3600. Значение по умолчанию: 300 секунд.

Режим: «Конфигурирование».

---

firewall global-options ipv6-receive-redirects [<enable> | <disable>]

Описание:

Включает или выключает прием ICMP-сообщений для перенаправления IPv6-трафика.

Изменяет следующие параметры ядра: *net.ipv6.conf.all.accept_source_route*.

Синтаксис:

- set firewall global-options ipv6-receive-redirects [<enable> | <disable>]
- delete firewall global-options ipv6-receive-redirects [<enable> | <disable>]
- show firewall global-options ipv6-receive-redirects

Аргументы:

- <enable> — включает прием ICMP-сообщений для перенаправления IPv6-трафика;
- <disable> — выключает прием ICMP-сообщений для перенаправления IPv6-трафика.

Режим: «Конфигурирование».

---

firewall global-options send-redirects [<enable> | <disable>]

Описание:

Включает или выключает отправку ICMP-сообщений для перенаправления IPv4-трафика.

Изменяет следующие параметры: *net.ipv4.conf.all.send_redirects*.

Синтаксис:

- set firewall global-options send-redirects `[<enable> | <disable>]`
- delete firewall global-options send-redirects `[<enable> | <disable>]`
- show firewall global-options send-redirects

Аргументы:

- `<enable>` — включает отправку ICMP-сообщений для перенаправления IPv4-трафика;
- `<disable>`— выключает отправку ICMP-сообщений для перенаправления IPv4-трафика.

Режим: «Конфигурирование».

---

firewall global-options log-martians [<enable> | <disable>]

Описание:

Включает или выключает журналирование IPv4-пакетов с заведомо некорректными адресами.

Изменяет следующие параметры ядра: *net.ipv4.conf.all.log_martians*.

Синтаксис:

- set firewall global-options log-martians `[<enable> | <disable>]`
- delete firewall global-options log-martians `[<enable> | <disable>]`
- show firewall global-options log-martians

Аргументы:

- `<enable>` — включает журналирование IPv4-пакетов с заведомо некорректными адресами;
- `<disable>` — выключает журналирование IPv4-пакетов с заведомо некорректными адресами.

Режим: «Конфигурирование».

---

firewall global-options syn-cookies [<enable> | <disable>]

Описание:

Включает или выключает механизм защиты SYN-cookie для IPv4 TCP.

Изменяет следующие параметры ядра: *net.ipv4.tcp_syncookies*.

Синтаксис:

- set firewall global-options syn-cookies [<enable> | <disable>]
- delete firewall global-options syn-cookies [<enable> | <disable>]
- show firewall global-options syn-cookies

Аргументы:

- <enable> — включает механизм защиты SYN-cookie для IPv4 TCP;
- <disable> — выключает механизм защиты SYN-cookie для IPv4 TCP.

Режим: «Конфигурирование».

---

firewall global-options twa-hazards-protection [<enable> | <disable>]

Описание:

Включает или выключает защиту от атаки в режиме ожидания после закрытия TCP-сессии. Если защита включена, система будет работать в соответствии с требованиями RFC 1337.

Изменяет следующие параметры ядра: *net.ipv4.tcp_rfc1337*.

Синтаксис:

- set firewall global-options twa-hazards-protection [<enable> | <disable>]
- delete firewall global-options twa-hazards-protection [<enable> | <disable>]
- show firewall global-options twa-hazards-protection

Аргументы:

- <enable> — включает защиту от атаки в режиме ожидания после закрытия TCP-сессии;
- <disable> — выключает защиту от атаки в режиме ожидания после закрытия TCP-сессии.

Режим: «Конфигурирование».

---

firewall global-options state-policy established action [<accept> | <drop> | <reject>]

Описание:

Включает различные режимы допуска входящих пакетов от установленных соединений.

Синтаксис:

- set firewall global-options state-policy established action [<accept> | <drop> | <reject>]
- delete firewall global-options state-policy established action [<accept> | <drop> | <reject>]
- show firewall global-options state-policy established action [<accept> | <drop> | <reject>]

Аргументы:

- <accept> — все входящие пакеты от установленных соединений будут допущены во внутреннюю сеть;

- <drop> — все входящие пакеты от установленных соединений будут отброшены без оповещения отправителя;
- <reject> — все входящие пакеты от установленных соединений будут отброшены, а отправитель получит сообщение о недоступности адреса назначения.

Режим: «Конфигурирование».

---

firewall global-options state-policy established log

Описание:

Включает журналирование для установленных соединений.

Синтаксис:

- set firewall global-options state-policy established log
- delete firewall global-options state-policy established log
- show firewall global-options state-policy established

Режим: «Конфигурирование».

---

firewall global-options state-policy established log-level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]

Описание:

Устанавливает, какие события система будет журналировать при поступлении трафика от установленных соединений.

Синтаксис:

- set firewall global-options state-policy established log-level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- delete firewall global-options state-policy established log-level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- show firewall global-options state-policy established log-level

Аргументы:

- <emerg> — самый высокий уровень опасности. Система не отвечает. Пример: нарушена безопасность периметра сети, потерян контроль над межсетевым экраном;
- <alert> — система находится под серьезной угрозой. Немедленно предпримите необходимые действия. Пример: большой наплыв трафика, вероятность DDoS-атаки;
- <crit> — система находится в критическом состоянии. Если не предпринять действий, состояние системы ухудшится. Пример: классификатор не применился к правилу;

- <err> — ошибка в работе системы. Система продолжит работать, однако потребует внимания. Пример: заканчивается место на диске;
- <warn> — предупреждение. Возможно, система столкнулась с проблемой. Пример: большинство входящих пакетов отвергнуты, отредактируйте правила фильтрации;
- <notice> — уведомление. Состояние системы в норме. Возможно, были изменены некоторые компоненты системы или система была обновлена. Пример: успешно обновлены правила фильтрации;
- <info> — информационные сообщения о статусе системы. Состояние системы в норме. Пример: межсетевой экран работает в штатном режиме;
- <debug> — детализированная отладочная информация. Пример: система выводит информацию об IP-адресах, адресах источника и назначения, протоколах передачи и т.д.

Режим: «Конфигурирование».

---

firewall global-options state-policy invalid action [<accept> | <drop> | <reject>]

Описание: Устанавливает, какие действия должна предпринять система при обнаружении пакетов с неправильной информацией о TCP-состоянии.

Синтаксис:

- set firewall global-options state-policy invalid action [<accept> | <drop> | <reject>]
- delete firewall global-options state-policy invalid action [<accept> | <drop> | <reject>]
- show firewall global-options state-policy invalid action

Аргументы:

- <accept> — все входящие пакеты с неправильной информацией о TCP-состоянии будут допущены во внутреннюю сеть;
- <drop> — все входящие пакеты с неправильной информацией о TCP-состоянии будут отброшены без оповещения отправителя;
- <reject> — все входящие пакеты с неправильной информацией о TCP-состоянии будут отброшены, а отправитель получит сообщение о недоступности адреса назначения.

Режим: «Конфигурирование».

---

firewall global-options state-policy invalid log

Описание:

Включает журналирование недопустимых пакетов.

Синтаксис:

- set firewall global-options state-policy invalid log
- delete firewall global-options state-policy invalid log

- show firewall global-options state-policy invalid

Режим: «Конфигурирование».

---

firewall global-options state-policy invalid log-level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]

Описание:

Устанавливает, какие события система будет журналировать при поступлении недопустимых пакетов.

Синтаксис:

- set firewall global-options state-policy invalid log-level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- delete firewall global-options state-policy invalid log-level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- show firewall global-options state-policy invalid log-level

Аргументы:

- <emerg> — самый высокий уровень опасности. Система не отвечает. Пример: нарушена безопасность периметра сети, потерян контроль над межсетевым экраном;
- <alert> — система находится под серьезной угрозой. Немедленно предпримите необходимые действия. Пример: большой наплыв трафика, вероятность DDoS-атаки;
- <crit> — система находится в критическом состоянии. Если не предпринять действий, состояние системы ухудшится. Пример: классификатор не применился к правилу;
- <err> — ошибка в работе системы. Система продолжит работать, однако потребует внимания. Пример: заканчивается место на диске;
- <warn> — предупреждение. Возможно, система столкнулась с проблемой. Пример: большинство входящих пакетов отвергнуты, отредактируйте правила фильтрации;
- <notice> — уведомление. Состояние системы в норме. Возможно, были изменены некоторые компоненты системы или система была обновлена. Пример: успешно обновлены правила фильтрации;
- <info> — информационные сообщения о статусе системы. Состояние системы в норме. Пример: межсетевой экран работает в штатном режиме;
- <debug> — детализированная отладочная информация. Пример: система выводит информацию об IP-адресах, адресах источника и назначения, протоколах передачи и т.д.

Режим: «Конфигурирование».

---

firewall global-options state-policy related action [<accept> | <drop> | <reject>]

Описание:

Указывает маршрутизатору, что делать с пакетами, которые являются производными от установленных соединений, но не принадлежат к основному потоку. Примеры таких пакетов: ICMP-сообщения, DNS-ответы, вспомогательные VPN-соединения, FTP-соединения для передачи данных.

Синтаксис:

- set firewall global-options state-policy related action [<accept> | <drop> | <reject>]
- delete firewall global-options state-policy related action [<accept> | <drop> | <reject>]
- show firewall global-options state-policy related action

Аргументы:

- <accept> — все производные пакеты от установленных соединений будут допущены во внутреннюю сеть;
- <drop> — все производные пакеты от установленных соединений будут отброшены без оповещения отправителя;
- <reject> — все производные пакеты от установленных соединений будут отброшены, а отправитель получит сообщение о недоступности адреса назначения.

Режим: «Конфигурирование».

---

firewall global-options state-policy related log

Описание:

Включает журналирование пакетов, которые являются производными от установленных соединениям, но не принадлежат к основному потоку. Примеры таких пакетов: ICMP-сообщения, DNS-ответы, вспомогательные VPN-соединения, FTP-соединения для передачи данных.

Синтаксис:

- set firewall global-options state-policy related log
- delete firewall global-options state-policy related log
- show firewall global-options state-policy related

Режим: «Конфигурирование».

---

firewall global-options state-policy related log-level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]

Описание:

Устанавливает, какие события система будет журналировать при поступлении пакетов, которые являются производными от установленных соединений, но не принадлежат к основному потоку.

Синтаксис:

- set firewall global-options state-policy related log-level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- delete firewall global-options state-policy related log-level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- show firewall global-options state-policy related log-level

Аргументы:

- <emerg> — самый высокий уровень опасности. Система не отвечает. Пример: нарушена безопасность периметра сети, потерян контроль над межсетевым экраном;
- <alert> — система находится под серьезной угрозой. Немедленно предпримите необходимые действия. Пример: большой наплыв трафика, вероятность DDoS-атаки;
- <crit> — система находится в критическом состоянии. Если не предпринять действий, состояние системы ухудшится. Пример: классификатор не применился к правилу;
- <err> — ошибка в работе системы. Система продолжит работать, однако потребует внимания. Пример: заканчивается место на диске;
- <warn> — предупреждение. Возможно, система столкнулась с проблемой. Пример: большинство входящих пакетов отвергнуты, отредактируйте правила фильтрации;
- <notice> — уведомление. Состояние системы в норме. Возможно, были изменены некоторые компоненты системы или система была обновлена. Пример: успешно обновлены правила фильтрации;
- <info> — информационные сообщения о статусе системы. Состояние системы в норме. Пример: межсетевой экран работает в штатном режиме;
- <debug> — детализированная отладочная информация. Пример: система выводит информацию об IP-адресах, адресах источника и назначения, протоколах передачи и т.д.

Режим: «Конфигурирование».

Правила фильтрации по протоколам IPv4 и IPv6

Обзор

Для каждого потока, зоны или интерфейса можно создать правило фильтрации трафика по протоколам IPv4 и IPv6. Чтобы маршрутизатор начал обрабатывать правило, ему необходимо присвоить *порядковый номер* от 1 до 999999. Маршрутизатор считывает правила по порядку, т.е. срабатывает первое подошедшее правило и соблюдается последовательность. Если присвоить правилам одинаковые номера, то они будут сгруппированы и объединены в логическую *цепочку*. Маршрутизатор будет воспринимать такую цепочку как единое целое. Несколько правил с порядковыми номерами можно объединить в один *набор правил* и присвоить ему имя.

Если пакет определенного потока подпадет под правило, к нему применится соответствующее действие. Если не указать действие для правила, то ПО Факел применит действие по умолчанию. По умолчанию правила на потоках принимают трафик (accept), а созданные наборы правил — отбрасывают (drop).

Каждое правило имеет уникальный *классификатор* — признак, по которому будет проходить фильтрация. Например, классификатором может быть IP-адрес, порт или протокол. Значения перечисляются через запятую. Чтобы инвертировать список значений, используйте перед аргументом символ «!».

Отдельное внимание стоит уделить настройке механизма SYNPROXY. Чтобы он заработал, выполните ряд условий:

- обеспечьте полнодуплексное соединение между клиентом и сервером;
- включите SYN-куки и отметки времени на протоколе TCP;
- отключите режим loose на модуле conntrack.

Пример настройки

Шаг	Команда	Описание
1	set firewall ipv4 forward filter default-action `drop`	По умолчанию отбрасывает входящие IPv4-пакеты на потоке FORWARD
2	set firewall ipv4 forward filter rule 10 action `accept`	Создает правило на потоке FORWARD с порядковым номером 10 и принимает входящие пакеты
3	set firewall ipv4 forward filter rule 10 protocol `tcp`	Добавляет правило с порядковым номером 10 в цепочку правил и выбирает протокол TCP для передачи данных
4	set firewall ipv4 forward filter rule 10 source address `192.168.1.0/24`	Добавляет правило с порядковым номером 10 в цепочку правил и указывает диапазон IPv4-адресов с префиксом `192.168.1.0/24` в качестве источника. Адреса выбранного диапазона получат доступ к потоку FORWARD.
5	set firewall ipv4 forward filter rule 10 description `Allow SSH from LAN`	Добавляет правило с порядковым номером 10 в цепочку правил и задает описание `Allow SSH from LAN`

Список команд

Режим «Конфигурирование»

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> action [<accept> | <continue> | <drop> | <jump> | <queue> | <reject> | <return> | <synproxy>]

Описание:

Создает правило и применяет выбранное действие к трафику на указанном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> action [<accept> | <continue> | <drop> | <jump> | <queue> | <reject> | <return> | <synproxy>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> action [<accept> | <continue> | <drop> | <jump> | <queue> | <reject> | <return> | <synproxy>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> action

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <accept> — принимает пакет во внутреннюю сеть;
- <continue> — применяет к пакету следующее правило;
- <drop> — отбрасывает пакет без оповещения;
- <reject> — отбрасывает пакет и оповещает отправителя;
- <jump> — переходит на другой набор правил;
- <return> — выходит из текущей цепочки, возвращается в исходную и применяет следующее правило исходной цепочки;
- <queue> — передает пакет процессам в пользовательском пространстве;
- <synproxy> — включает механизм SYNPROXY для защиты от атаки SYN-flood. Межсетевой экран задержит установление трехстороннего рукопожатия SYN-ACK до тех пор, пока клиент не подтвердит свое намерение установить соединение. Если клиент не подтвердит желание связаться с сервером, соединение установлено не будет.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> action [<accept> | <continue> | <drop> | <jump> | <queue> | <reject> | <return>]

Описание:

Создает набор правил и применяет выбранное действие к трафику.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> action [<accept> | <continue> | <drop> | <jump> | <queue> | <reject> | <return>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> action [<accept> | <continue> | <drop> | <jump> | <queue> | <reject> | <return>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> action

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <accept> — принимает пакет во внутреннюю сеть;
- <continue> — применяет к пакету следующее правило;
- <drop> — отбрасывает пакет без оповещения;
- <reject> — отбрасывает пакет и оповещает отправителя;
- <jump> — переходит на другой набор правил;
- <return> — выходит из текущей цепочки, возвращается в исходную и применяет следующее правило исходной цепочки;
- <queue> — передает пакет процессам в пользовательском пространстве;
- <synproxy> — включает механизм SYNPROXY для защиты от атаки SYN-flood. Межсетевой экран задержит установление трехстороннего рукопожатия SYN-ACK до тех пор, пока клиент не подтвердит свое намерение установить соединение. Если клиент не подтвердит желание связаться с сервером, соединение установлено не будет.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> jump-target <text>

Описание:

Создает правило и переходит на другой набор правил.

Предварительно необходимо для аргумента action задать значение <jump>.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> jump-target <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> jump-target <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> jump-target

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя другого набора правил, куда будет перенаправлен трафик.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> jump-target <text>

Описание:

Создает набор правил и переходит на другой набор правил. Предварительно необходимо для аргумента action задать значение <jump>.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> jump-target <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> jump-target <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> jump-target

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя другого набора правил, куда будет перенаправлен трафик для дальнейшей обработки.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> queue <0-65535>

Описание:

Создает правило и отправляет трафик с выбранного потока на указанную очередь в ядро. По мере освобождения очереди пакеты будут передаваться на обработку процессу в пользовательском пространстве.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <0-65535> — номер очереди. Формат: целое число или диапазон чисел. Диапазон значений: от 0 до 65535.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue <0-65535>

Описание:

Создает набор правил и отправляет трафик на указанную очередь в ядро. По мере освобождения очереди пакеты будут передаваться на обработку процессу в пользовательском пространстве.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue <0-65535>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue <0-65535>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;

- <0-65535> — номер очереди. Формат: целое число или диапазон чисел. Диапазон значений: от 0 до 65535.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> queue-options bypass

Описание:

Создает правило и не отправляет трафик с выбранного потока на указанную очередь в ядро. Пакеты будут сразу передаваться на обработку процессу в пользовательском пространстве.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> queue-options bypass
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> queue-options bypass
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> queue-options

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue-options bypass

Описание:

Создает набор правил и не отправляет пакеты IPv4 или IPv6 на указанную очередь в ядро. Пакеты будут сразу передаваться на обработку процессу в пользовательском пространстве.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue-options bypass

- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue-options bypass
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue-options

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> queue-options fanout

Описание:

Создает правило и распределяет трафик IPv4 или IPv6 равномерно между разными очередями на выбранном потоке.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> queue-options fanout
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> queue-options fanout
- show set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> queue-options

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue-options fanout

Описание:

Создает набор правил и распределяет трафик IPv4 или IPv6 равномерно между разными очередями.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue-options fanout
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue-options fanout
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> queue-options

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter default-action [<accept> | <drop>]

Описание:

Устанавливает действие по умолчанию, которое применится, если пакеты IPv4 или IPv6 не будут соответствовать ни одному правилу на выбранном потоке. Для потоков INPUT, FORWARD и OUTPUT доступны только действия accept и drop.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter default-action [<accept> | <drop>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter default-action [<accept> | <drop>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter default-action

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;

- <accept> — принимает пакет во внутреннюю сеть;
- <drop> — отбрасывает пакет без оповещения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> default-action [<accept> | <drop> | <jump> | <queue> | <reject> | <return>]

Описание:

Создает набор правил и устанавливает действие по умолчанию, которое применится, если трафик не будет соответствовать ни одному правилу.

Если выбрано значение <jump>, то необходимо дополнительно указать в default-jump-target другой набор правил, на который следует перейти.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> default-action [<accept> | <drop> | <jump> | <queue> | <reject> | <return>]
- delete firewall [<ipv4> | <ipv6>] name <name> default-action [<accept> | <drop> | <jump> | <queue> | <reject> | <return>]
- show firewall [<ipv4> | <ipv6>] name <name> default-action

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <accept> — принимает пакет во внутреннюю сеть;
- <continue> — применяет к пакету следующее правило;
- <drop> — отбрасывает пакет без оповещения;
- <jump> — переходит на другой набор правил;
- <queue> — передает пакет процессам в пользовательском пространстве;
- <reject> — отбрасывает пакет и оповещает отправителя;
- <return> — выходит из текущей цепочки, возвращается в исходную и применяет следующее правило исходной цепочки;

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> default-jump-target <text>

Описание:

Создает набор правил и по умолчанию переходит на другой набор правил.

Предварительно необходимо для аргумента default-action задать значение `jump`.

Синтаксис:

- set firewall `[<ipv4> | <ipv6>]` name `<name>` default-jump-target `<text>`
- delete firewall `[<ipv4> | <ipv6>]` name `<name>` default-jump-target `<text>`
- show firewall `[<ipv4> | <ipv6>]` name `<name>` default-jump-target

Аргументы:

- `<ipv4>` — IPv4-трафик;
- `<ipv6>` — IPv6-трафик;
- `<name>` — имя исходного набора правил;
- `<text>` — имя другого набора правил, куда будет перенаправлен трафик.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log

Описание:

Включает журналирование, когда сработает указанное правило на выбранном потоке.

Синтаксис:

- set firewall `[<ipv4> | <ipv6>]` `[<forward> | <input> | <output>]` filter rule `<1-999999>` log
- delete firewall `[<ipv4> | <ipv6>]` `[<forward> | <input> | <output>]` filter rule `<1-999999>` log
- show firewall `[<ipv4> | <ipv6>]` `[<forward> | <input> | <output>]` filter rule `<1-999999>`

Аргументы:

- `<ipv4>` — IPv4-трафик;
- `<ipv6>` — IPv6-трафик;
- `<forward>` — поток FORWARD;
- `<input>` — поток INPUT;
- `<output>` — поток OUTPUT;
- `<1-999999>` — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log

Описание:

Включает журналирование, когда сработает указанный набор правил.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter default-log

Описание:

Включает журналирование на выбранном потоке, когда применяется действие по умолчанию.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter default-log
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter default-log
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> default-log

Описание:

Создает набор правил и включает журналирование тогда, когда применяется действие по умолчанию.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> default-log
- delete firewall [<ipv4> | <ipv6>] name <name> default-log
- show firewall [<ipv4> | <ipv6>] name <name>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]

Описание:

Создает правило и устанавливает, какие события система будет журналировать при поступлении трафика от установленных соединений на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options log-level

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <emerg> — самый высокий уровень опасности. Система не отвечает. Пример: нарушена безопасность периметра сети, потерян контроль над межсетевым экраном;

- <alert> — система находится под серьезной угрозой. Немедленно предпримите необходимые действия. Пример: большой наплыв трафика, вероятность DDoS-атаки;
- <crit> — система находится в критическом состоянии. Если не предпринять действий, состояние системы ухудшится. Пример: классификатор не применился к правилу;
- <err> — ошибка в работе системы. Система продолжит работать, однако потребует внимания. Пример: заканчивается место на диске;
- <warn> — предупреждение. Возможно, система столкнулась с проблемой. Пример: большинство входящих пакетов отвергнуты, отредактируйте правила фильтрации;
- <notice> — уведомление. Состояние системы в норме. Возможно, были изменены некоторые компоненты системы или система была обновлена. Пример: успешно обновлены правила фильтрации;
- <info> — информационные сообщения о статусе системы. Состояние системы в норме. Пример: межсетевой экран работает в штатном режиме;
- <debug> — детализированная отладочная информация. Пример: система выводит информацию об IP-адресах, адресах источника и назначения, протоколах передачи и т.д.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]

Описание:

Создает набор правил и устанавливает, какие события система будет журналировать при поступлении пакетов данных от установленных соединений.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options level

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <1-999999> — порядковый номер правила;
- <name> — имя набора правил.
- <emerg> — самый высокий уровень опасности. Система не отвечает. Пример: нарушена безопасность периметра сети, потерян контроль над межсетевым экраном;
- <alert> — система находится под серьезной угрозой. Немедленно предпримите необходимые действия. Пример: большой наплыв трафика, вероятность DDoS-атаки;

- <crit> — система находится в критическом состоянии. Если не предпринять действий, состояние системы ухудшится. Пример: классификатор не применился к правилу;
- <err> — ошибка в работе системы. Система продолжит работать, однако потребует внимания. Пример: заканчивается место на диске;
- <warn> — предупреждение. Возможно, система столкнулась с проблемой. Пример: большинство входящих пакетов отвергнуты, отредактируйте правила фильтрации;
- <notice> — уведомление. Состояние системы в норме. Возможно, были изменены некоторые компоненты системы или система была обновлена. Пример: успешно обновлены правила фильтрации;
- <info> — информационные сообщения о статусе системы. Состояние системы в норме. Пример: межсетевой экран работает в штатном режиме;
- <debug> — детализированная отладочная информация. Пример: система выводит информацию об IP-адресах, адресах источника и назначения, протоколах передачи и т.д.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options group <0-65535>

Описание:

Создает правило и группу, которая будет вести журналирование на выбранном потоке.

Предварительно необходимо включить журналирование через аргумент log.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options group <0-65535>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options group <0-65535>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <0-65535> — номер группы, которая будет вести журналирование.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options group <0-65535>

Описание:

Создает набор правил и группу, которая будет вести журналирование.

Предварительно необходимо включить журналирование через аргумент log.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options group <0-65535>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options group <0-65535>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <0-65535> — номер группы, которая будет вести журналирование.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options snapshot-length <0-9000>

Описание:

Создает правило и устанавливает, насколько детально группа правил будет вести журналирование на выбранном потоке.

Предварительно необходимо включить журналирование через аргумент log и указать через аргумент log-options group группу, которая будет вести журналирование.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options snapshot-length <0-9000>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options snapshot-length <0-9000>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options snapshot-length

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;

- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <0-9000> — размер полезной нагрузки пакета в байтах, которая будет включена в сообщения netlink. Диапазон значений: от 0 до 9000. Чем выше число, тем подробнее группа будет вести журналирование.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options snapshot-length <0-9000>

Описание:

Создает набор правил и устанавливает, насколько детально группа будет вести журналирование.

Предварительно необходимо включить журналирование через аргумент log и указать через аргумент log-options group группу, которая будет вести журналирование.

Синтаксис: * set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options snapshot-length <0-9000> * delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options snapshot-length <0-9000> * show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options snapshot-length

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <0-9000> — размер полезной нагрузки пакета в байтах, которая будет включена в сообщения netlink. Диапазон значений: от 0 до 9000. Чем выше число, тем подробнее группа будет вести журналирование.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options queue-threshold <0-65535>

Описание:

Создает правило и устанавливает порог на количество записей в журнал событий при поступлении трафика на выбранный поток. По мере освобождения очереди, записи журнала событий будут передаваться процессу в пользовательское пространство.

Предварительно необходимо включить журналирование через аргумент log и указать через аргумент log-options group группу, которая будет вести журналирование.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options queue-threshold <0-65535>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options queue-threshold <0-65535>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> log-options queue-threshold

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <0-65535> — максимальное число записей в журнал.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options queue-threshold <0-65535>

Описание:

Создает набор правил и устанавливает порог на количество записей в журнал событий при поступлении трафика. По мере освобождения очереди, записи журнала событий будут передаваться процессу в пользовательское пространство.

Предварительно необходимо включить журналирование через аргумент log и указать через аргумент log-options group группу, которая будет вести журналирование.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options queue-threshold <0-65535>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options queue-threshold <0-65535>
- show * set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> log-options queue-threshold

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;

- <1-999999> — порядковый номер правила;
- <0-65535> — максимальное число записей в журнал.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> description <text>

Описание:

Создает правило и добавляет к нему описание.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> description <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> description <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> description

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — описание правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> description <text>

Описание:

Создает набор правил и добавляет к нему описание.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> description <text>
- delete firewall [<ipv4> | <ipv6>] name <name> description <text>
- show firewall [<ipv4> | <ipv6>] name <name> description

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <text> — описание набора правил

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> disable

Описание:

Отключает правило для трафика на выбранном потоке, но сохраняет конфигурацию.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> disable
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> disable
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> disable

Описание:

Отключает набор правил, но сохраняет конфигурацию.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> disable
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> disable
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> connection-status nat [<destination> | <source>]

Описание:

Создает правило на выбранном потоке и фильтрует трафик, который принадлежит к исходящему (SNAT) или входящему (DNAT) направлению NAT.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule :code:`<1-999999> connection-status nat [<destination> | <source>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule :code:`<1-999999> connection-status nat [<destination> | <source>]
- show set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule :code:`<1-999999> connection-status nat

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <source> — трафик на исходящем направлении NAT (SNAT);
- <destination> — трафик на входящем направлении NAT (DNAT).

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> connection-status nat [<destination> | <source>]

Описание:

Создает набор правил и фильтрует трафик, который принадлежит к исходящему (SNAT) или входящему (DNAT) направлению NAT.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> connection-status nat [<destination> | <source>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> connection-status nat [<destination> | <source>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> connection-status nat

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <source> — трафик на исходящем направлении NAT (SNAT);
- <destination> — трафик на входящем направлении NAT (DNAT).

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> connection-mark <1-2147483647>

Описание:

Создает правило и устанавливает числовую метку для фильтрации соединений на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> connection-mark <1-2147483647>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> connection-mark <1-2147483647>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> connection-mark

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <1-2147483647> — числовая метка соединения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> connection-mark <1-2147483647>

Описание:

Создает набор правил и устанавливает числовую метку для фильтрации соединений.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> connection-mark <1-2147483647>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> connection-mark <1-2147483647>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> connection-mark

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <1-2147483647> — числовая метка соединения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> conntrack-helper [<ftp> | <h323> | <pptp> | <nfs> | <sip> | <tftp> | <sqlnet>]

Описание:

Создает правило и включает на выбранном потоке вспомогательный модуль conntrack, который детально анализирует и отслеживает трафик с различных протоколов передачи данных.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> conntrack-helper [<ftp> | <h323> | <pptp> | <nfs> | <sip> | <tftp> | <sqlnet>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> conntrack-helper [<ftp> | <h323> | <pptp> | <nfs> | <sip> | <tftp> | <sqlnet>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> conntrack-helper

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <ftp> — анализ трафика по протоколу FTP;
- <h323> — анализ трафика по протоколу H.323;
- <pptp> — анализ трафика по протоколу PPTP;
- <nfs> — анализ трафика по протоколу NFS;
- <sip> — анализ трафика по протоколу SIP;
- <tftp> — анализ трафика по протоколу TFTP;
- <sqlnet> — анализ трафика по протоколу SQLNET.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> conntrack-helper [<ftp> | <h323> | <pptp> | <nfs> | <sip> | <tftp> | <sqlnet>]

Описание:

Создает набор правил и включает вспомогательный модуль conntrack, который детально анализирует и отслеживает трафик с различных протоколов передачи данных.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> conntrack-helper [<ftp> | <h323> | <pptp> | <nfs> | <sip> | <tftp> | <sqlnet>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> conntrack-helper [<ftp> | <h323> | <pptp> | <nfs> | <sip> | <tftp> | <sqlnet>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> conntrack-helper

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <ftp> — анализ трафика по протоколу FTP;
- <h323> — анализ трафика по протоколу H.323;
- <pptp> — анализ трафика по протоколу PPTP;

- <nfs> — анализ трафика по протоколу NFS;
- <sip> — анализ трафика по протоколу SIP;
- <tftp> — анализ трафика по протоколу TFTP;
- <sqlnet> — анализ трафика по протоколу SQLNET.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source address [<address> | <addressrange> | <CIDR>]

Описание:

Создает правило и задает адрес или диапазон адресов источника для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source address [<address> | <addressrange> | <CIDR>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source address [<address> | <addressrange> | <CIDR>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source address

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес источника. Формат: x.x.x.x;
- <addressrange> — диапазон из IPv4-адресов источника. Формат: x.x.x.x — x.x.x.x;
- <CIDR> — диапазон из IPv4-адресов с префиксом подсети. Формат CIDR: x.x.x.x/x.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source address [<address> | <addressrange> | <CIDR>]

Описание:

Создает набор правил и задает адрес или диапазон адресов источника для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source address [<address> | <addressrange> | <CIDR>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source address [<address> | <addressrange> | <CIDR>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source address

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес источника. Формат: x.x.x.x;
- <addressrange> — диапазон из IPv4-адресов источника. Формат: x.x.x.x — x.x.x.x;
- <CIDR> — диапазон из IPv4-адресов с префиксом подсети. Формат CIDR: x.x.x.x/x.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination address [<address> | <addressrange> | <CIDR>]

Описание:

Создает правило и задает адрес или диапазон адресов назначения для фильтрации трафика на выбранном потоке.

Синтаксис: * set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination address [<address> | <addressrange> | <CIDR>] * delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination address [<address> | <addressrange> | <CIDR>] * show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination address

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес назначения. Формат: x.x.x.x;
- <addressrange> — диапазон из IPv4-адресов назначения. Формат: x.x.x.x — x.x.x.x;

- <CIDR> — диапазон из IPv4-адресов назначения с префиксом подсети. Формат CIDR: x.x.x.x/x.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination address [<address> | <addressrange> | <CIDR>]

Описание:

Создает набор правил и задает адрес или диапазон адресов назначения для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination address [<address> | <addressrange> | <CIDR>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination address [<address> | <addressrange> | <CIDR>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination address

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес назначения. Формат: x.x.x.x;
- <addressrange> — диапазон из IPv4-адресов назначения. Формат: x.x.x.x — x.x.x.x;
- <CIDR> — диапазон из IPv4-адресов назначения с префиксом подсети. Формат CIDR: x.x.x.x/x.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source address-mask <address>

Описание:

Создает правило и задает маску подсети в качестве источника для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source address-mask [address]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source address-mask [address]

- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source address-mask

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <address> — маска подсети источника. Формат: x.x.x.x.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source address-mask <address>

Описание:

Создает набор правил и задает маску подсети в качестве источника для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source address-mask [address]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source address-mask [address]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source address-mask

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <address> — маска подсети источника. Формат: x.x.x.x.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination address-mask <address>

Описание:

Создает правило и задает маску подсети в качестве назначения для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination address-mask [address]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination address-mask [address]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination address-mask

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <address> — маска подсети назначения. Формат: x.x.x.x.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination address-mask <address>

Описание:

Создает правило и задает маску подсети в качестве назначения для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination address-mask [address]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination address-mask [address]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination address-mask

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <address> — маска подсети назначения. Формат: x.x.x.x.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source fqdn <fqdn>

Описание:

Создает правило и задает полное доменное имя в качестве источника для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source fqdn <fqdn>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source fqdn <fqdn>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source fqdn

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <fqdn> — полное доменное имя источника.

Режим: «Конфигурирование».

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source fqdn <fqdn>

Описание:

Создает набор правил и задает полное доменное имя в качестве источника для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source fqdn <fqdn>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source fqdn
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source fqdn

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <fqdn> — полное доменное имя источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination fqdn <fqdn>

Описание:

Создает правило и задает полное доменное имя назначения для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination fqdn <fqdn>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination fqdn <fqdn>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination fqdn

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <fqdn> — полное доменное имя назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination fqdn <fqdn>

Описание:

Создает набор правил и задает полное доменное имя назначения для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination fqdn <fqdn>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination fqdn <fqdn>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination fqdn

Аргументы:

- <ipv4> — IPv4-трафик;

- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <fqdn> — полное доменное имя назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source geoip country-code <country>

Описание:

Создает правило и указывает страну, IP-адреса источника которой будут фильтроваться на выбранном потоке.

Чтобы обновить базу данных стран с IP-адресами, выполните команду *update geoip* в режиме администрирования.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source geoip country-code <country>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source geoip country-code <country>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source geoip country-code

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <country> — название страны. Формат: ISO 3166-1 alpha-2. Пример: jp (Япония).

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source geoip country-code <country>

Описание:

Создает набор правил и указывает страну, IP-адреса источника которой будут фильтроваться.

Чтобы обновить базу данных стран с IP-адресами, выполните команду *update geoip* в режиме администрирования.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source geoip country-code <country>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source geoip country-code <country>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source geoip country-code

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <country> — название страны. Формат: ISO 3166-1 alpha-2. Пример: jp (Япония).

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source geoip inverse-match

Описание:

Создает правило и инвертирует список стран, IP-адреса источника которых будут фильтроваться на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source geoip inverse-match
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source geoip inverse-match
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source geoip

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source geoip inverse-match

Описание:

Создает набор правил и инвертирует список стран, IP-адреса источника которых будут фильтроваться.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source geoip inverse-match
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source geoip inverse-match
- firewall firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source geoip

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination geoip country-code <country>

Описание:

Создает правило и указывает страну, IP-адреса назначения которой будут фильтроваться на выбранном потоке.

Чтобы обновить базу данных стран с IP-адресами, выполните команду *update geoip* в режиме администрирования.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination geoip country-code <country>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination geoip country-code <country>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination geoip country-code

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;

- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <country> — название страны. Формат: ISO 3166-1 alpha-2. Пример: jp (Япония).

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination geoip country-code <country>

Описание:

Создает правило и указывает страну, IP-адреса назначения которой будут фильтроваться.

Чтобы обновить базу данных стран с IP-адресами, выполните команду *update geoip* в режиме администрирования.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] <name> filter rule <1-999999> destination geoip country-code <country>
- delete firewall [<ipv4> | <ipv6>] <name> filter rule <1-999999> destination geoip country-code <country>
- show firewall [<ipv4> | <ipv6>] <name> filter rule <1-999999> destination geoip country-code

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <country> — название страны. Формат: ISO 3166-1 alpha-2. Пример: jp (Япония).

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination geoip inverse-match

Описание:

Создает правило и инвертирует список стран, IP-адреса назначения которых будут фильтроваться на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination geoip inverse-match
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination geoip inverse-match
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination geoip

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination geoip inverse-match

Описание:

Создает набор правил и инвертирует список стран, IP-адреса назначения которых будут фильтроваться.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination geoip inverse-match
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination geoip inverse-match
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination geoip

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source mac-address <mac-address>

Описание:

Создает правило и задает MAC-адрес источника для фильтрации трафика на выбранном потоке.

Синтаксис:

- set [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source mac-address <mac-address>
- delete [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source mac-address <mac-address>
- show [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source mac-address

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <mac-address> — MAC-адрес.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source mac-address <mac-address>

Описание:

Создает набор правил и задает MAC-адрес источника для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source mac-address <mac-address>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source mac-address <mac-address>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source mac-address

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <mac-address> — MAC-адрес. Формат: xx.xx.xx.xx.xx.xx.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source port [<text> | <1-65535> | <start-end>]

Описание:

Создает правило и задает порт источника для фильтрации трафика на выбранном потоке.

Синтаксис:

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source port [<text> | <1-65535> | <start-end>] * delete [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source port [<text> | <1-65535> | <start-end>] * show [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source port

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя порта источника, указанное в директории /etc/services;
- <1-65535> — номер порта источника. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон из портов источника. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Примечание

Аргументы можно совместить через запятую. Пример: http, 80, 95-100.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source port [<text> | <1-65535> | <start-end>]

Описание:

Создает набор правил и задает порт источника для фильтрации трафика.

Синтаксис:

- set [<ipv4> | <ipv6>] name <name> rule <1-999999> source port [<text> | <1-65535> | <start-end>]

- delete [<ipv4> | <ipv6>] name <name> rule <1-999999> source port [<text> | <1-65535> | <start-end>]
- show [<ipv4> | <ipv6>] name <name> rule <1-999999> source port

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя порта источника, указанное в директории /etc/services;
- <1-65535> — номер порта источника. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон из портов источника. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination port [<text> | <1-65535> | <start-end>]

Описание:

Создает правило и задает порт назначения для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination port [<text> | <1-65535> | <start-end>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination port [<text> | <1-65535> | <start-end>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination port

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя порта источника, указанное в директории /etc/services;
- <1-65535> — номер порта источника. Диапазон значений: от 1 до 65535;

- <start-end> — диапазон из портов источника. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination port [<text> | <1-65535> | <start-end>]

Описание:

Создает набор правил и задает порт назначения для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination port [<text> | <1-65535> | <start-end>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination port [<text> | <1-65535> | <start-end>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination port

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя порта источника, указанное в директории /etc/services;
- <1-65535> — номер порта источника. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон из портов источника. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group address-group [<name> | <!name>]

Описание:

Создает правило и использует группу IP-адресов в качестве источника для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group address-group [<name> | <!name>]

- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group address-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group address-group

Аргументы:

- `<ipv4>` — IPv4-трафик;
- `<ipv6>` — IPv6-трафик;
- `<forward>` — поток FORWARD;
- `<input>` — поток INPUT;
- `<output>` — поток OUTPUT;
- `<1-999999>` — порядковый номер правила;
- `<name>` — имя группы IP-адресов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group address-group [<name> | <!name>]

Описание:

Создает набор правил и использует группу IP-адресов в качестве источника для фильтрации трафика.

Синтаксис:

- set firewall `[<ipv4> | <ipv6>]` name `<name>` rule `<1-999999>` source group address-group `[<name> | <!name>]`
- delete firewall `[<ipv4> | <ipv6>]` name `<name>` rule `<1-999999>` source group address-group `[<name> | <!name>]`
- show firewall `[<ipv4> | <ipv6>]` name `<name>` rule `<1-999999>` source group address-group

Аргументы:

- `<ipv4>` — IPv4-трафик;
- `<ipv6>` — IPv6-трафик;
- `<name>` — имя набора правил;
- `<1-999999>` — порядковый номер правила;
- `<name>` — имя группы IP-адресов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group address-group [<name> | <!name>]

Описание:

Создает правило и использует группу IP-адресов в качестве назначения для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group address-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group address-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group address-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <name> — имя группы IP-адресов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group address-group [<name> | <!name>]

Описание:

Создает набор правил и использует группу IP-адресов в качестве назначения для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group address-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group address-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group address-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <name> — имя группы IP-адресов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group dynamic-address-group <text>

Описание:

Создает правило и использует динамическую группу IP-адресов в качестве источника для фильтрации трафика на выбранном потоке. Подробнее работа динамических групп описана в разделе *Группы* (страница 523).

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group dynamic-address-group <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group dynamic-address-group <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group dynamic-address-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input>· — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы IP-адресов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group dynamic-address-group <text>

Описание:

Создает набор правил и использует динамическую группу IP-адресов в качестве источника для фильтрации трафика. Подробнее работа динамических групп описана в разделе *Группы* (страница 523).

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group dynamic-address-group <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group dynamic-address-group <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group dynamic-address-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы IP-адресов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group dynamic-address-group <text>

Описание:

Создает правило и использует динамическую группу IP-адресов в качестве назначения для фильтрации трафика на выбранном потоке. Подробнее работа динамических групп описана в разделе *Группы* (страница 523).

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group dynamic-address-group <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group dynamic-address-group <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group dynamic-address-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;

- <text> — имя динамической группы IP-адресов, которая будет использоваться в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group dynamic-address-group <text>

Описание:

Создает набор правил и использует динамическую группу IP-адресов в качестве назначения для фильтрации трафика. Подробнее работа динамических групп описана в разделе *Группы* (страница 523).

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group dynamic-address-group <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group dynamic-address-group <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group dynamic-address-group <text>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы IP-адресов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group network-group <text>

Описание:

Создает правило и использует группу подсетей в качестве источника для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group network-group <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group network-group <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group network-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя группы подсетей в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group network-group <text>

Описание:

Создает правило и использует группу подсетей в качестве источника для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group network-group <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group network-group <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group network-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя группы подсетей в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group network-group <text>

Описание:

Создает правило и использует группу подсетей в качестве назначения для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group network-group <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group network-group <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group network-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя группы подсетей в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group network-group <text>

Описание:

Создает правило и использует группу подсетей в качестве назначения для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group network-group <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group network-group <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group network-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя группы портов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group port-group [<name> | <!name>]

Описание:

Создает правило и использует группу портов в качестве источника для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group port-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group port-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group port-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя группы портов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group port-group [<name> | <!name>]

Описание:

Создает набор правил и использует группу портов в качестве источника для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group port-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group port-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group port-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <name> — имя группы портов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group port-group [<name> | <!name>]

Описание:

Создает правило и использует группу портов в качестве назначения для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group port-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group port-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group port-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <name> — имя группы портов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group port-group [<name> | <!name>]

Описание:

Создает набор правил и использует группу портов в качестве назначения для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group port-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group port-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group port-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <name> — имя группы портов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group domain-group [<name> | <!name>]

Описание:

Создает правило и использует группу доменов в качестве источника для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group domain-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group domain-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group domain-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <name> — имя группы доменов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group domain-group [<name> | <!name>]

Описание:

Создает правило и использует группу доменов в качестве источника для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group domain-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group domain-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group domain-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <name> — имя группы доменов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group domain-group [<name> | <!name>]

Описание:

Создает правило и использует группу доменов в качестве назначения для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] :code:`[<forward> | <input> | <output>] filter rule *<1-999999>* destination group domain-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] :code:`[<forward> | <input> | <output>] filter rule *<1-999999>* destination group domain-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] :code:`[<forward> | <input> | <output>] filter rule *<1-999999>* destination group domain-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;

- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <name> — имя группы доменов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group domain-group [<name> | <!name>]

Описание:

Создает набор правил и использует группу доменов в качестве назначения для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group domain-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group domain-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group domain-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <name> — имя группы доменов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group mac-group [<name> | <!name>]

Описание:

Создает правило и использует группу MAC-адресов в качестве источника для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group mac-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group mac-group [<name> | <!name>]

- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> source group mac-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <name> — имя группы MAC-адресов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group mac-group [<name> | <!name>]

Описание:

Создает набор правил и использует группу MAC-адресов в качестве источника для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group mac-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group mac-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> source group mac-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <name> — имя группы MAC-адресов в качестве источника.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group mac-group [<name> | <!name>]

Описание:

Создает правило и использует группу MAC-адресов в качестве назначения для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group mac-group [[<name> | <!name>]]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group mac-group [[<name> | <!name>]]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> destination group mac-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <name> — имя группы MAC-адресов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group mac-group [<name> | <!name>]

Описание:

Создает набор правил и использует группу MAC-адресов в качестве назначения для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group mac-group [<name> | <!name>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group mac-group [<name> | <!name>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> destination group mac-group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <name> — имя группы MAC-адресов в качестве назначения.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> dscp [<0-63> | <start-end>]

Описание:

Создает правило и задает значение DSCP для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> dscp [<0-63> | <start-end>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> dscp [<0-63> | <start-end>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> dscp

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <0-63> — значение DSCP. Диапазон значений: от 0 до 63;
- <start-end> — диапазон значений DSCP. Формат: целое число или диапазон чисел. Диапазон значений: от 0 до 63.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> dscp [<0-63> | <start-end>]

Описание:

Создает набор правил и задает значение DSCP для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> dscp [<0-63> | <start-end>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> dscp [<0-63> | <start-end>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> dscp

Аргументы:

- <ipv4> — IPv4-трафик;

- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <0-63> — значение DSCP. Диапазон значений: от 0 до 63;
- <start-end> — диапазон значений DSCP. Формат: целое число или диапазон чисел. Диапазон значений: от 0 до 63.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> dscp-exclude [<0-63> | <start-end>]

Описание:

Создает правило и исключает значения DSCP для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> dscp-exclude [<0-63> | <start-end>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> dscp-exclude [<0-63> | <start-end>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> dscp-exclude

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <0-63> — значение DSCP. Диапазон значений: от 0 до 63;
- <start-end> — диапазон значений DSCP. Формат: целое число или диапазон чисел. Диапазон значений: от 0 до 63.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> dscp-exclude [<0-63> | <start-end>]

Описание:

Создает набор правил и исключает значения DSCP для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> dscp-exclude [<0-63> | <start-end>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> dscp-exclude [<0-63> | <start-end>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> dscp-exclude

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <0-63> — значение DSCP. Диапазон значений: от 0 до 63;
- <start-end> — диапазон значений DSCP. Формат: целое число или диапазон чисел. Диапазон значений: от 0 до 63.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> fragment [<match-frag> | <match-non-frag>]

Описание:

Создает правило и устанавливает фильтрацию для фрагментированного или нефрагментированного трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> fragment [<match-frag> | <match-non-frag>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> fragment [<match-frag> | <match-non-frag>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> fragment

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <match-frag> — фрагментированный трафик;
- <match-non-frag> — нефрагментированный трафик.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> fragment [<match-frag> | <match-non-frag>]

Описание:

Создает набор правил и устанавливает фильтрацию для фрагментированного или нефрагментированного трафика.

Синтаксис:

- set firewall name <name> rule <1-999999> fragment [<match-frag> | <match-non-frag>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> fragment [<match-frag> | <match-non-frag>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> fragment

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <match-frag> — фрагментированный трафик;
- <match-non-frag> — нефрагментированный трафик.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> icmp [code <code> | type <type> | type-name <text>]

Описание:

Создает правило и задает код или тип служебных ICMP-сообщений для фильтрации трафика на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> icmp [code <code> | type <type> | type-name <text>]

- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> icmp [code <code> | type <type> | type-name <text>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> icmp [code | type | type-name]

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <code> — код ICMP-сообщений;
- <type> — тип ICMP-сообщений;
- <text> — имя типа ICMP-сообщений.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> icmp [code <0-255> | type <0-255> | type-name <text>]

Описание:

Создает набор правил и задает код или тип служебных ICMP-сообщений для фильтрации трафика.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> icmp [code <0-255> | type <0-255> | type-name <text>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> icmp [code <0-255> | type <0-255> | type-name <text>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> icmp [code | type | type-name]

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <code> — код ICMP-сообщений;
- <type> — тип ICMP-сообщений;

- <text> — имя типа ICMP-сообщений.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> inbound-interface name <iface>

Описание:

Создает правило и выбирает интерфейс, через который трафик поступает на межсетевой экран на выбранный поток.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> inbound-interface name <iface>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> inbound-interface name <iface>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> inbound-interface name

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <iface> — интерфейс, через который трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов.

Режим: «Конфигурирование».

Примечание

Если интерфейс размещен на нестандартном VRF-экземпляре, то необходимо указать имя этого VRF-экземпляра. Пример: *set firewall ipv4 forward filter rule 10 inbound-interface name ACCEPT*‘

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> inbound-interface name <iface>

Описание:

Создает набор правил и выбирает интерфейс, через который трафик поступает на межсетевой экран.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> inbound-interface name <iface>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> inbound-interface name <iface>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> inbound-interface name

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <iface> — интерфейс, через который трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> inbound-interface group <iface_group>

Описание:

Создает правило на указанном потоке и выбирает группу интерфейсов, через которую трафик поступает на межсетевой экран на выбранный поток.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> inbound-interface group <iface_group>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> inbound-interface group <iface_group>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> inbound-interface group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <iface_group> — группа интерфейсов, через которую трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> inbound-interface group <iface_group>

Описание:

Создает набор правил и выбирает группу интерфейсов, через которую трафик поступает на межсетевой экран.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> inbound-interface group <iface_group>
- delete firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> inbound-interface group <iface_group>
- show firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> inbound-interface group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <iface_group> — группа интерфейсов, через которую трафик поступает на межсетевой экран.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> outbound-interface <iface>

Описание:

Создает правило на указанном потоке и выбирает интерфейс, через который трафик исходит с межсетевого экрана.

!!!УТОЧНИТЬ про OUTBOUND!!!

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> outbound-interface <iface>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> outbound-interface <iface>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> outbound-interface

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <iface> — интерфейс, через который трафик исходит с межсетевого экрана. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> outbound-interface <iface>

Описание:

Создает набор правил на указанном потоке и выбирает интерфейс, через который трафик исходит с межсетевого экрана.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> outbound-interface <iface>
- delete firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> outbound-interface <iface>
- show firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> outbound-interface

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <iface> — интерфейс, через который трафик исходит с межсетевого экрана. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> outbound-interface group <iface_group>

Описание:

Создает правило на указанном потоке и выбирает группу интерфейсов, через которую трафик исходит с межсетевого экрана.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> outbound-interface group <iface_group>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> outbound-interface group <iface_group>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> outbound-interface group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <iface_group> — группа интерфейсов, через которую трафик исходит с межсетевого экрана.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> outbound-interface group <iface_group>

Описание:

Создает набор правил и выбирает группу интерфейсов, через которую трафик исходит с межсетевого экрана.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> outbound-interface group <iface_group>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> outbound-interface group <iface_group>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> outbound-interface group

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <iface_group> — группа интерфейсов, через которую трафик исходит с межсетевого экрана.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> ipsec [match-ipsec-in | match-ipsec-out | match-none-in | match-none-out]

Описание:

Создает правило и выбирает пакеты на указанном потоке, которые используют набор протоколов IPsec.

!!!ОБРАТИТЬ ВНИМАНИЕ!!!

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> ipsec [match-ipsec-in | match-ipsec-out | match-none-in | match-none-out]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> ipsec [match-ipsec-in | match-ipsec-out | match-none-in | match-none-out]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> ipsec

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <match-ipsec-in>— применяет правило к входящим IPsec-пакетам;
- <match-ipsec-out> — применяет правило к исходящим IPsec-пакетам;
- <match-none-in> — применяет правило к любым пакетам кроме входящих IPsec-пакетов;
- <match-none-out> — применяет правило к любым пакетам кроме исходящих IPsec-пакетов.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> ipsec [<match-ipsec-in> | <match-ipsec-out> | <match-none-in> | <match-none-out>]

Описание:

Создает набор правил и выбирает пакеты, которые используют набор протоколов IPsec.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> ipsec [match-ipsec-in | match-ipsec-out | match-none-in | match-none-out]

- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> ipsec [match-ipsec-in | match-ipsec-out | match-none-in | match-none-out]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> ipsec

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <match-ipsec-in>— применяет правило к входящим IPsec-пакетам;
- <match-ipsec-out> — применяет правило к исходящим IPsec-пакетам;
- <match-none-in> — применяет правило к любым пакетам кроме входящих IPsec-пакетов;
- <match-none-out> — применяет правило к любым пакетам кроме исходящих IPsec-пакетов.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> limit burst <0-4294967295>

Описание:

Создает правило и задает количество пакетов, для обработки которых маршрутизатор кратковременно увеличит пропускную способность на выбранном потоке. По завершении операции пропускная способность вернется к прежнему уровню.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> limit burst <0-4294967295>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> limit burst <0-4294967295>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> limit burst

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;

- <0-4294967295> — количество пакетов, для обработки которых маршрутизатор кратковременно увеличит пропускную способность. Диапазон значений: от 0 до 4294967295.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> limit burst <0-4294967295>

Описание:

Создает набор правил и задает количество пакетов, для обработки которых маршрутизатор кратковременно увеличит пропускную способность. По завершении операции пропускная способность вернется к прежнему уровню.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> limit burst <0-4294967295>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> limit burst <0-4294967295>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> limit burst

Аргументы: * <ipv4> — IPv4-трафик; * <ipv6> — IPv6-трафик; * <name> — имя набора правил; * <1-999999> — порядковый номер правила; * <0-4294967295> — количество пакетов, для обработки которых маршрутизатор кратковременно увеличит пропускную способность. Диапазон значений: от 0 до 4294967295.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> limit rate <text>

Описание:

Создает правило и устанавливает ограничение на скорость обработки пакетов на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> limit rate <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> limit rate <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> limit rate

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;

- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — ограничение на скорость обработки пакетов. Формат: целое число/единица времени. Пример: 10/minute.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> limit rate <text>

Описание:

Создает набор правил и устанавливает ограничение на скорость обработки пакетов.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> limit rate <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> limit rate <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> limit rate <text>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — ограничение на скорость обработки пакетов. Формат: целое число/единица времени. Пример: 10/minute.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-length <text>

Описание:

Создает правило и устанавливает допустимый размер пакета на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-length <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-length <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-length

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — размер пакета. Формат: целое число или диапазон чисел. Диапазон значений: от 1 до 65535.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> packet-length <text>

Описание:

Создает набор правил и устанавливает допустимый размер пакета.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> packet-length <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> packet-length <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> packet-length

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — размер пакета. Формат: целое число или диапазон чисел. Диапазон значений: от 1 до 65535.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-length-exclude <text>

Описание:

Создает правило и не фильтрует пакеты определенного размера на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-length-exclude <text>

- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-length-exclude <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-length-exclude

Аргументы:

- `<ipv4>` — IPv4-трафик;
- `<ipv6>` — IPv6-трафик;
- `<forward>` — поток FORWARD;
- `<input>` — поток INPUT;
- `<output>` — поток OUTPUT;
- `<1-999999>` — порядковый номер правила;
- `<text>` — размер пакета. Формат: целое число или диапазон чисел. Диапазон значений: от 1 до 65535.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> packet-length-exclude <text>

Описание:

Создает набор правил и не фильтрует пакеты определенного размера.

Синтаксис:

- set firewall `[<ipv4> | <ipv6>]` name `<name>` rule `<1-999999>` packet-length-exclude `<text>`
- delete firewall `[<ipv4> | <ipv6>]` name `<name>` rule `<1-999999>` packet-length-exclude `<text>`
- show firewall `[<ipv4> | <ipv6>]` name `<name>` rule `<1-999999>` packet-length-exclude

Аргументы:

- `<ipv4>` — IPv4-трафик;
- `<ipv6>` — IPv6-трафик;
- `<name>` — имя набора правил;
- `<1-999999>` — порядковый номер правила;
- `<text>` — размер пакета. Формат: целое число или диапазон чисел. Диапазон значений: от 1 до 65535.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]

Описание: Создает правило и выбирает тип вещания пакетов для фильтрации на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> packet-type

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <broadcast> — broadcast-вещание;
- <host> — пакеты, адресованные межсетевому экрану;
- <multicast> — multicast-вещание;
- <other> — остальные типы вещания.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]

Описание:

Создает набор правил и выбирает тип вещания пакетов для фильтрации.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> packet-type

Аргументы:

- <ipv4> — IPv4-трафик;

- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <broadcast> — broadcast-вещание;
- <host> — пакеты, адресованные межсетевому экрану;
- <multicast> — multicast-вещание;
- <other> — остальные типы вещания.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> protocol [<text> | <0-255> | <all> | <tcp_udp>]

Описание:

Создает правило и выбирает протокол передачи данных для фильтрации на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> protocol [<text> | <0-255> | <all> | <tcp_udp>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> protocol [<text> | <0-255> | <all> | <tcp_udp>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> protocol

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя протокола, указанное в директории /etc/protocols;
- <0-255> — идентификационный номер;
- <all> — трафик со всех протоколов;
- <tcp_udp> — выбирает между протоколом TCP или UDP.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> protocol [<text> | <0-255> | <all> | <tcp_udp>]

Описание:

Создает набор правил и выбирает протокол передачи данных для фильтрации.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> protocol [<text> | <0-255> | <all> | <tcp_udp>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> protocol [<text> | <0-255> | <all> | <tcp_udp>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> protocol

Аргументы:

- `<ipv4>` — IPv4-трафик;
- `<ipv6>` — IPv6-трафик;
- `<name>` — имя набора правил;
- `<1-999999>` — порядковый номер правила;
- `<0-255>` — идентификационный номер;
- `<all>` — трафик со всех протоколов;
- `<tcp_udp>` — выбирает между протоколом TCP или UDP.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent count <1-255>

Описание:

Создает правило и задает, сколько должно поступить обращений с IP-адреса источника, чтобы правило применилось к трафику на выбранном потоке.

!!!УТОЧНИТЬ!!!

Синтаксис:

- set firewall `[<ipv4> | <ipv6>] [<forward> | <input> | <output>]` filter rule `<1-999999>` recent count `<1-255>`
- delete firewall `[<ipv4> | <ipv6>] [<forward> | <input> | <output>]` filter rule `<1-999999>` recent count `<1-255>`
- show firewall `[<ipv4> | <ipv6>] [<forward> | <input> | <output>]` filter rule `<1-999999>` recent count

Аргументы:

- `<ipv4>` — IPv4-трафик;

- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <1-255> — количество одинаковых соединений.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent count <1-255>

Описание:

Создает набор правил и задает, сколько должно поступить обращений с IP-адреса источника, чтобы правило применилось к трафику на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent count <1-255>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent count <1-255>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent count

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <1-255> — количество одинаковых соединений.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent time [<second> | <minute> | <hour>]

Описание:

Создает правило и задает время, в течение которого межсетевой экран будет запоминать количество обращений с IP-адреса источника на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent time [<second> | <minute> | <hour>]

- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent time [<second> | <minute> | <hour>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent time

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <second> — время в секундах;
- <minute> — время в минутах;
- <hour> — время в часах.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent time [<second> | <minute> | <hour>]

Описание:

Создает набор правил и задает время, в течение которого межсетевой экран будет запоминать количество обращений с IP-адреса источника.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent time [<second> | <minute> | <hour>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent time [<second> | <minute> | <hour>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent time

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <second> — время в секундах;
- <minute> — время в минутах;
- <hour> — время в часах.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> tcp flags [<ack> | <cwr> | <ecn> | <fin> | <not> | <psh> | <rst> | <syn> | <urg>]

Описание:

Создает правило и устанавливает флаг для TCP-пакетов на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> tcp flags [<ack> | <cwr> | <ecn> | <fin> | <not> | <psh> | <rst> | <syn> | <urg>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> tcp flags [<ack> | <cwr> | <ecn> | <fin> | <not> | <psh> | <rst> | <syn> | <urg>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> tcp flags

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <ack> — флаг ACKNOWLEDGEMENT. Подтверждает получение пакета с флагом SYN;
- <cwr> — флаг CONGESTION WINDOW REDUCED. Обозначает уменьшение размера окна насыщения в ответ на ECN;
- <ecn> — флаг EXPLICIT CONGESTION NOTIFICATION — Echo. Уведомляет о явном перенасыщении. Получатель подтвердит, что был уведомлен;
- <fin> — флаг FINISH. Уведомляет об окончании передачи данных с одной стороны;
- <not> — флаг NOT. Инвертирует список значений, работает как отрицание. Пример: *set firewall ipv4 input fulter rule 12 tcp flags not fin*;
- <psh> — флаг PUSH. Требует незамедлительно доставить пакет без отправки на очередь;
- <rst> — флаг RESET. Обрывает соединение;
- <syn> — флаг SYN. Начинает трехсторонний процесс установления TCP-соединения;
- <urg> — флаг URGENT. Обозначает пакеты с высоким приоритетом.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> tcp flags [<ack> | <cwr> | <ecn> | <fin> | <not> | <psh> | <rst> | <syn> | <urg>]

Описание:

Создает набор правил и устанавливает флаг для TCP-пакетов.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> tcp flags [not] <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> tcp flags [not] <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> tcp flags [not] <text>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <ack> — флаг ACKNOWLEDGEMENT. Подтверждает получение пакета с флагом SYN;
- <cwr> — флаг CONGESTION WINDOW REDUCED. Обозначает уменьшение размера окна насыщения в ответ на ECN;
- <ecn> — флаг EXPLICIT CONGESTION NOTIFICATION — Echo. Уведомляет о явном перенасыщении. Получатель подтвердит, что был уведомлен;
- <fin> — флаг FINISH. Уведомляет об окончании передачи данных с одной стороны;
- <not> — флаг NOT. Инвертирует список значений, работает как отрицание. Пример: *set firewall ipv4 input fulter rule 12 tcp flags not fin*;
- <psh> — флаг PUSH. Требует незамедлительно доставить пакет без отправки на очередь;
- <rst> — флаг RESET. Обрывает соединение;
- <syn> — флаг SYN. Начинает трехсторонний процесс установления TCP-соединения;
- <urg> — флаг URGENT. Обозначает пакеты с высоким приоритетом.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> state [<established> | <invalid> | <new> | <related>]

Описание:

Создает правило и задает статус TCP-соединения на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> state [<established> | <invalid> | <new> | <related>]

- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> state [<established> | <invalid> | <new> | <related>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> state

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <established> — установленные TCP-соединения;
- <invalid> — неустановленные TCP-соединения;
- <new> — новые соединения. Начальный этап трехстороннего процесса установления TCP-соединения;
- <related> — соединения, производные от установленных.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> state [<established> | <invalid> | <new> | <related>]

Описание:

Создает набор правил и задает статус TCP-соединения.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> state [<established> | <invalid> | <new> | <related>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> state [<established> | <invalid> | <new> | <related>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> state

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <established> — установленные TCP-соединения;

- <invalid> — неустановленные TCP-соединения;
- <new> — новые соединения. Начальный этап трехстороннего процесса установления TCP-соединения;
- <related> — соединения, производные от установленных.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time startdate <text>

Описание:

Включает правило на выбранном потоке в заданную дату.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time startdate <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time startdate <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time startdate

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — дата включения. Формат: ГГГГ-ММ-ДД.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time startdate <text>

Описание:

Включает набор правил в заданную дату.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time startdate <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time startdate <text>

- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time startdate

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — дата включения. Формат: ГГГГ-ММ-ДД.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time starttime <text>

Описание:

Включает правило на выбранном потоке в заданное время.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time starttime <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time starttime <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time starttime

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — время включения. Формат: ЧЧ-ММ-СС.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time starttime <text>

Описание:

Включает набор правил в заданное время.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time starttime <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time starttime <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time starttime

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — время включения. Формат: ЧЧ-ММ-СС.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time stopdate <text>

Описание:

Выключает правило на выбранном потоке в заданную дату.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time stopdate <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time stopdate <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time stopdate

Аргументы:

- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — дата выключения. Формат: ГГГГ-ММ-ДД.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time stopdate <text>

Описание:

Выключает набор правил в заданную дату.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time stopdate <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time stopdate <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time stopdate

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.
- <text> — дата выключения. Формат: ГГГГ-ММ-ДД.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time stoptime <text>

Описание:

Выключает правило на выбранном потоке в заданное время.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time stoptime <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time stoptime <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time stoptime

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — время выключения. Формат: ЧЧ-ММ-СС.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time stoptime <text>

Описание:

Выключает набор правил в заданное время.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time stoptime <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time stoptime <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time stoptime

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — время выключения. Формат: ЧЧ-ММ-СС.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time weekdays <text>

Описание:

Включает правило на выбранном потоке в заданный день недели.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time weekdays <text>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time weekdays <text>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> time weekdays

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;

- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — день недели. Формат: день недели на английском языке или соответствующий порядковый номер. Пример: Monday или 1, Wednesday или 3.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time weekdays <text>

Описание:

Включает набор правил в заданный день недели.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time weekdays <text>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time weekdays <text>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> time weekdays

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — день недели. Формат: день недели на английском языке или соответствующий порядковый номер. Пример: Monday или 1, Wednesday или 3.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> ttl [<eq> | <gt> | <lt> | <0-255>]

Описание:

Создает правило и задает время жизни IP-пакета на выбранном потоке. После того как IP-пакет пройдет один узел сети, его время жизни сократится на одно значение.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> ttl [<eq> | <gt> | <lt> | <0-255>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> ttl [<eq> | <gt> | <lt> | <0-255>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> ttl

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <eq> — равно заданного времени жизни;
- <gt> — больше заданного времени жизни;
- <lt> — меньше заданного времени жизни;
- <0-255> — время жизни IP-пакета. Формат: количество пройденных маршрутизаторов. Диапазон значений: от 1 до 255. Число 0 копирует значение из IP-заголовка.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> ttl [<eq> | <gt> | <lt> | <0-255>]

Описание:

Создает набор правил и задает время жизни IP-пакета. После того как IP-пакет пройдет один узел сети, его время жизни сократится на одно значение.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> ttl [<eq> | <gt> | <lt> | <0-255>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> ttl [<eq> | <gt> | <lt> | <0-255>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> ttl

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <eq> — равно заданного времени жизни;
- <gt> — больше заданного времени жизни;
- <lt> — меньше заданного времени жизни;
- <0-255> — время жизни IP-пакета. Формат: количество пройденных маршрутизаторов. Диапазон значений: от 1 до 255. Число 0 копирует значение из IP-заголовка.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent count <1-255>

Описание:

Создает правило и задает максимально допустимое число соединений от одного источника на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent count <1-255>
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent count <1-255>
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent count

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <1-255> — максимально допустимое число соединений от одного источника на выбранном потоке.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent count <1-255>

Описание:

Создает набор правил и задает максимально допустимое число соединений от одного источника на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent count <1-255>
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent count <1-255>
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent count

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-255> — максимально допустимое число соединений от одного источника на выбранном потоке.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent time [<second> | <minute> | <hour>]

Описание:

Создает правило и задает время, в течение которого допускаются соединения от одного источника на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent time [<second> | <minute> | <hour>]
- delete firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent time [<second> | <minute> | <hour>]
- show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999> recent time

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <second> — время в секундах;
- <minute> — время в минутах;
- <hour> — время в часах.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent time [<second> | <minute> | <hour>]

Описание:

Создает набор правил и задает время, в течение которого допускаются соединения от одного источника на выбранном потоке.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent time [<second> | <minute> | <hour>]
- delete firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent time [<second> | <minute> | <hour>]
- show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999> recent time

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <second> — время в секундах;
- <minute> — время в минутах;
- <hour> — время в часах.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<input> | <forward> | <output>] filter rule <1-999999> synproxy tcp mss <501-65535>

Описание:

Создает правило и устанавливает на выбранном потоке максимальный размер сегмента при передаче пакетов по протоколу TCP с использованием механизма SYNPROXY.

Предварительно необходимо для аргумента action задать значение synproxy, а для аргумента protocol значение tcp.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [input | forward] filter rule <1-999999> synproxy tcp mss <501-65535>
- delete firewall [<ipv4> | <ipv6>] [input | forward] filter rule <1-999999> synproxy tcp mss <501-65535>
- show firewall [<ipv4> | <ipv6>] [input | forward] filter rule <1-999999> synproxy tcp mss

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <501-65535> — максимальный размера сегмента при передаче пакетов по протоколу TCP с использованием механизма SYNPROXY.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> synproxy tcp mss <501-65535>

Описание:

Создает набор правил и устанавливает максимальный размер сегмента при передаче пакетов по протоколу TCP с использованием механизма SYNPROXY.

Предварительно необходимо для аргумента action задать значение synproxy, а для аргумента protocol значение tcp.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> synproxy tcp mss <501-65535>
- delete firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> synproxy tcp mss <501-65535>
- show firewall [<ipv4> | <ipv6>] name <name> filter rule <1-999999> synproxy tcp mss

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <501-65535> — максимальный размера сегмента при передаче пакетов по протоколу TCP с использованием механизма SYNPROXY.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<input> | <forward> | <output>] filter rule <1-999999> synproxy tcp window-scale <1-14>

Описание:

Создает правило и включает на выбранном потоке механизм автоматического масштабирования размера окна на протоколе TCP. Позволяет отправлять пакеты большего размера, перед тем как получатель отправит ответный TCP-сегмент с флагом ACK. Уменьшает количество передаваемых служебных TCP-сегментов.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [input | forward] filter rule <1-999999> synproxy tcp window-scale <1-14>
- delete firewall [<ipv4> | <ipv6>] [input | forward] filter rule <1-999999> synproxy tcp window-scale <1-14>
- show firewall [<ipv4> | <ipv6>] [input | forward] filter rule <1-999999> synproxy tcp window-scale

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <1-14> — фактор масштабирования размера окна на протоколе TCP. Размер окна на протоколе TCP увеличится в заданное число раз.

Режим: «Конфигурирование».

---

firewall [<ipv4> | <ipv6>] [<input> | <forward> | <output>] filter rule <1-999999> synproxy tcp window-scale <1-14>

Описание:

Создает набор правил и включает механизм автоматического масштабирования размера окна на протоколе TCP. Позволяет отправлять пакеты большего размера, перед тем как получатель отправит ответный TCP-сегмент с флагом ACK. Уменьшает количество передаваемых служебных TCP-сегментов.

Синтаксис:

- set firewall [<ipv4> | <ipv6>] [input | forward] filter rule <1-999999> synproxy tcp window-scale <1-14>
- delete firewall [<ipv4> | <ipv6>] [input | forward] filter rule <1-999999> synproxy tcp window-scale <1-14>

- show firewall [<ipv4> | <ipv6>] [input | forward] filter rule <1-999999> synproxy tcp window-scale

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <1-14> — фактор масштабирования размера окна на протоколе TCP. Размер окна на протоколе TCP увеличится в заданное число раз.

Режим: «Конфигурирование».

Режим «Администрирование»

show firewall

Описание:

Отображает детальную информацию о конфигурации межсетевого экрана.

Синтаксис:

show firewall

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall summary

Описание:

Отображает сводную информацию о конфигурации межсетевого экрана.

Синтаксис:

show firewall summary

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter

Описание:

Отображает информацию об активных правилах на выбранном потоке.

Синтаксис:

show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall [<ipv4> | <ipv6>] name <name>

Описание:

Отображает информацию об активных правилах на указанном наборе правил.

Синтаксис:

show firewall [<ipv4> | <ipv6>] name <name>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999>

Описание:

Отображает информацию о конкретном правиле на выбранном потоке.

Синтаксис:

show firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999>

Описание:

Отображает информацию об активном наборе правил.

Синтаксис:

show firewall [<ipv4> | <ipv6>] name <name> rule <1-999999>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall statistics

Описание:

Отображает статистику всех правил с последнего запуска системы.

Синтаксис:

show firewall statistics

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall

Описание:

Отображает все записи в журнале регистрации событий.

Синтаксис:

show log firewall

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall [<ipv4> | <ipv6>]

Описание:

Отображает записи в журнале регистрации событий для трафика по протоколам IPv4 или IPv6.

Синтаксис:

show log firewall [<ipv4> | <ipv6>]

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>]

Описание:

Отображает записи в журнале регистрации событий для трафика на выбранном потоке.

Синтаксис:

show log firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>]

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall [<ipv4> | <ipv6>] name <name>

Отображает записи в журнале регистрации событий для конкретного набора правил.

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999>

Описание:

Отображает записи в журнале регистрации событий для конкретнго правила на выбранном потоке.

Синтаксис:

show log firewall [<ipv4> | <ipv6>] [<forward> | <input> | <output>] filter rule <1-999999>

Аргументы: * <ipv4> — IPv4-трафик; * <ipv6> — IPv6-трафик; * <forward> — поток FORWARD; * <input> — поток INPUT; * <output> — поток OUTPUT; * <1-999999> — порядковый номер правила.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall [<ipv4> | <ipv6>] name <name> rule <1-999999>

Описание:

Отображает записи в журнале регистрации событий для набора правил.

Синтаксис:

show log firewall [<ipv4> | <ipv6>] name <name> rule <1-999999>

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <name> — имя набора правил;

- <1-999999> — порядковый номер правила;

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

update geoip

Описание:

Обновляет базу данных GeoIP.

Синтаксис:

update geoip

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Группы

Обзор

В межсетевом экране группа объединяет несколько сетевых объектов одного типа. К таким объектами относятся IP-адреса на протоколах IPv4 и IPv6, порты, MAC-адреса, домены, интерфейсы.

Правила применяются ко всей группе как к логически единому элементу. Достаточно объединить объекты в группу и задать одно правило, вместо того чтобы создавать правила по несколько раз для каждого объекта.

Другие компоненты межсетевого экрана, такие как nat, nat66 смогут в своих правилах указать созданную группу в качестве источника или назначения.

В **динамическую группу** IP-адреса добавляются автоматически из правил. Например, если правило пропускает пакеты от определенных IP-адресов, то эти адреса будут включены в динамическую группу. Предварительно необходимо создать динамическую группу, а затем отдельной командой связать ее с правилом.

IP-адреса могут добавляться и удаляться из динамической группы по истечении времени. Время жизни IP-адреса в составе группы задается отдельной командой при добавлении адресов в динамическую группу. Если интервал не задать, то адрес останется в группе до следующей перезагрузки системы или до тех пор, пока не будет изменена конфигурация межсетевого экрана.

Особая техника защиты в динамических группах — простукивание портов (port knocking). Группа будет скрывать порт от внешних подключений и ожидать специально заданную последовательность обращений. При получении требуемых обращений, межсетевой экран откроет скрытый порт.

Пример настройки групп

Шаг	Команда	Описание
1	set firewall group network-group MANAGEMENT-NET description `management network`	Создает группу IPv4-сетей, присваивает ей имя MANAGEMENT-NET и добавляет описание `management network`
2	set firewall group network-group MANAGEMENT-NET network `172.16.1.0/24`	Добавляет в группу MANAGEMENT-NET IPv4-адреса с префиксом подсети `172.16.1.0/24`
3	set firewall ipv4 forward filter rule 100 description `Allow devices to management network`	Создает правило на потоке FORWARD с порядковым номером 100 и добавляет описание `Allow devices to management network`
4	set firewall ipv4 forward filter rule 100 action `accept`	Добавляет правило с порядковым номером 100 в цепочку правил и разрешает входящий трафик
5	set firewall ipv4 forward filter rule 100 source group network-group `MANAGEMENT-NET`	Добавляет правило с порядковым номером 100 в цепочку правил и указывает группу подсетей `MANAGEMENT-NET` в качестве источника
6	set firewall ipv4 forward filter rule 100 destination address `0.0.0.0/0`	Добавляет правило с порядковым номером 100 в цепочку правил и разрешает трафик во все остальные сети. Трафик на потоке FORWARD из группы подсетей MANAGEMENT-NET будет маршрутизироваться во все остальные подсети

Пример использования техники простукивания портов

Шаг	Команда	Описание
1	set firewall group dynamic-group address-group PN_01	Создает динамическую группу IPv4-адресов и присваивает ей имя PN_01
	set firewall group dynamic-group address-group PN_02	Создает динамическую группу IPv4-адресов и присваивает ей имя PN_02
2	set firewall ipv4 input filter default-action drop	Создает правило на потоке INPUT и по умолчанию отбрасывает входящий трафик
3	set firewall ipv4 input filter rule 5 action accept	Создает правило на потоке INPUT с порядковым номером 5 и разрешает входящий трафик
	set firewall ipv4 input filter rule 5 state established enable	Добавляет правило с порядковым номером 5 в цепочку правил и разрешает трафик от установленных TCP-соединений
	set firewall ipv4 input filter rule 5 state related enable	Добавляет правило с порядковым номером 5 в цепочку правил и разрешает трафик от производных TCP-соединений
4	set firewall ipv4 input filter rule 10 action drop	Создает правило с порядковым номером 10 на потоке INPUT и отбрасывает входящий трафик
	set firewall ipv4 input filter rule 10 add-address-to-group source-address address-group PN_01	Добавляет правило с порядковым номером 10 в цепочку правил и добавляет в динамическую группу PN_01 IPv4-адрес источника
	set firewall ipv4 input filter rule 10 add-address-to-group source-address timeout 2m	Добавляет правило с порядковым номером 10 в цепочку правил и устанавливает для IPv4-адреса в составе динамической группы время жизни в 2 минуты
	set firewall ipv4 input filter rule 10 description Port_knock 01	Добавляет правило с порядковым номером 10 в цепочку правил и добавляет описание Port_knock 01
	set firewall ipv4 input filter rule 10 destination port 9990	Добавляет правило с порядковым номером 10 в цепочку правил и задает порт назначения 9990
	set firewall ipv4 input filter rule 10 protocol tcp	Добавляет правило с порядковым номером 10 в цепочку правил и выбирает протокол TCP для передачи данных
5	set firewall ipv4 input filter rule 20 action drop	Создает правило с порядковым номером 20 на потоке INPUT и отбрасывает весь входящий трафик
	set firewall ipv4 input filter rule 20 add-address-to-group source-address address-group PN_02	Добавляет правило с порядковым номером 20 в цепочку правил и добавляет в динамическую группу PN_02 IPv4-адрес источника
	set firewall ipv4 input filter rule 20 add-address-to-group source-address timeout 3m	Добавляет правило с порядковым номером 20 в цепочку правил и устанавливает для IPv4-адреса в составе динамической группы время жизни в 3 минуты
	set firewall ipv4 input filter rule 20 destination port 9991	Добавляет правило с порядковым номером 20 в цепочку правил и задает порт назначения 9991
	set firewall ipv4 input filter rule 20 protocol tcp	Добавляет правило с порядковым номером 20 в цепочку правил и выбирает протокол TCP для передачи данных
	set firewall ipv4 input filter rule 20 source group dynamic-address-group PN_01	Добавляет правило с порядковым номером 20 в цепочку правил и выбирает динамическую группу PN_01 в качестве источника
6	set firewall ipv4 input filter rule 30 action accept	Создает правило с порядковым номером 30 на потоке INPUT и разрешает входящий трафик
	set firewall ipv4 input filter rule 30 description Open SSH for successful knock	Добавляет правило с порядковым номером 30 в цепочку правил и добавляет описание Open SSH for successful knock
	set firewall ipv4 input filter rule 30 destination port 22	Добавляет правило с порядковым номером 30 в цепочку правил и задает порт назначения 22
	set firewall ipv4 input filter rule 30 protocol tcp	Добавляет правило с порядковым номером 30 в цепочку правил и выбирает протокол TCP для передачи данных
	set firewall ipv4 input filter rule 30	Добавляет правило с порядковым номером 30 в цепочку пра-

Краткое содержание примера:

- создаются две динамические группы;
- по умолчанию запрещается входящий трафик;
- трафик от установленных и производных TCP-соединений разрешается;
- если устройство обратится на порт 9990, МСЭ запомнит его IPv4-адрес на 2 минуты;
- если после обращения на порт 9990 устройство обратится на порт 9991, МСЭ запомнит его IPv4-адрес и откроет доступ по SSH на 3 минуты.

Список команд

Режим «Конфигурирование»

firewall group address-group <text> address <address>

Описание:

Создает группу IPv4-адресов, присваивает ей имя и добавляет в нее IPv4-адреса или диапазон IPv4-адресов.

Синтаксис:

- set firewall group address-group `<text>` address `<address>`
- delete firewall group address-group `<text>` address `<address>`
- show firewall group address-group `<text>` address

Аргументы:

- `<text>` — имя группы;
- `<address>` — IPv4-адрес или диапазон IPv4-адресов. Формат: x.x.x.x или x.x.x.x — x.x.x.x.

Режим: «Конфигурирование».

---

firewall group address-group <text> description <text>

Описание:

Создает группу IPv4-адресов, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group address-group <text> description <text>

- delete firewall group address-group <text> description <text>
- show firewall group address-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall group ipv6-address-group <text> address <address>

Описание:

Создает группу IPv6-адресов, присваивает ей имя и добавляет в нее IPv6-адреса или диапазон IPv6-адресов.

Синтаксис:

- set firewall group ipv6-address-group <text> address <address>
- delete firewall group ipv6-address-group <text> address <address>
- show firewall group ipv6-address-group <text> address

Аргументы:

- <text> — имя группы;
- <address> — IPv6-адрес или диапазон IPv6-адресов.

Режим: «Конфигурирование».

---

firewall group ipv6-address-group <text> description <text>

Описание:

Создает группу IPv6-адресов, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group ipv6-address-group <text> description <text>
- delete firewall group ipv6-address-group <text> description <text>
- show firewall group ipv6-address-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall group network-group <text> network <CIDR>

Описание:

Создает группу IPv4-сетей, присваивает ей имя и добавляет в нее IPv4-адреса с префиксом подсети в формате CIDR.

Синтаксис:

- set firewall group network-group <text> network <CIDR>
- delete firewall group network-group <text> network <CIDR>
- show firewall group network-group <text> network

Аргументы:

- <text> — имя группы;
- <CIDR> — диапазон из IPv4-адресов с префиксом подсети. Формат CIDR: x.x.x.x/x.

Режим: «Конфигурирование».

---

firewall group network-group <text> description <text>

Описание:

Создает группу IPv4-сетей, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group network-group <text> description <text>
- delete firewall group network-group <text> description <text>
- show firewall group network-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall group ipv6-network-group <text> network <CIDR>

Описание:

Создает группу IPv6-сетей, присваивает ей имя и добавляет в нее IPv6-адреса с префиксом подсети в формате CIDR.

Синтаксис:

- set firewall group ipv6-network-group <text> network <CIDR>

- delete firewall group ipv6-network-group <text> network <CIDR>
- show firewall group ipv6-network-group <text> network

Аргументы:

- <text> — имя группы;
- <CIDR> — диапазон из IPv6-адресов с префиксом подсети. Формат CIDR: x.x.x.x/x.

Режим: «Конфигурирование».

---

firewall group ipv6-network-group <text> description <text>

Описание:

Создает группу IPv6-сетей, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group ipv6-network-group <text> description <text>
- delete firewall group ipv6-network-group <text> description <text>
- show firewall group ipv6-network-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall group interface-group <text> interface <text>

Описание:

Создает группу интерфейсов, присваивает ей имя и добавляет в нее выбранный интерфейс.

Синтаксис:

- set firewall group interface-group <text> interface <text>
- delete firewall group interface-group <text> interface <text>
- show firewall group interface-group <text> interface

Аргументы:

- <text> — имя группы;
- <text> — имя интерфейса, который будет включен в состав группы.

Режим: «Конфигурирование».

---

firewall group interface-group <text> description <text>

Описание:

Создает группу интерфейсов, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group interface-group <text> description <text>
- delete firewall group interface-group <text> description <text>
- show firewall group interface-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall group port-group <text> port [<portname> | <portnumber> | <startport-endport>]

Описание:

Создает группу портов, присваивает ей имя и добавляет в нее порт или диапазон портов.

Синтаксис:

- set firewall group port-group <text> port [<portname> | <portnumber> | <startport-endport>]
- delete firewall group port-group <text> port [<portname> | <portnumber> | <startport-endport>]
- show firewall group port-group <text> port

Аргументы:

- <text> — имя группы;
- <portname> — имя порта, указанное в директории /etc/services;
- <portnumber> — номер порта;
- <startpoint-endpoint> — диапазон номеров портов. Формат: x.x.x.x — x.x.x.x.

Режим: «Конфигурирование».

---

firewall group port-group <text> description <text>

Описание:

Создает группу портов, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group port-group <text> description <text>
- delete firewall group port-group <text> description <text>
- show firewall group port-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall group mac-group <text> mac-address <mac-address>

Описание:

Создает группу MAC-адресов, присваивает ей имя и добавляет в нее MAC-адрес.

Синтаксис:

- set firewall group mac-group <text> mac-address <mac-address>
- delete firewall group mac-group <text> mac-address <mac-address>
- show firewall group mac-group <text> mac-address

Аргументы: * <text> — имя группы; * <mac-address> — MAC-адрес.

Режим: «Конфигурирование».

---

firewall group mac-group <text> description <text>

Описание:

Создает группу MAC-адресов, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group mac-group <text> description <text>
- delete firewall group mac-group <text> description <text>
- show firewall group mac-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall group domain-group <text> address <domain>

Описание:

Создает группу доменов, присваивает ей имя и добавляет в нее доменное имя.

Синтаксис:

- set firewall group domain-group <text> address <domain>
- delete firewall group domain-group <text> address <domain>
- show firewall group domain-group <text> address

Аргументы:

- <text> — имя группы;
- <domain> — доменное имя, которое будет добавлено в группу.

Режим: «Конфигурирование».

---

firewall group domain-group <text> description <text>

Описание:

Создает группу доменов, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group domain-group <text> description <text>
- delete firewall group domain-group <text> description <text>
- show firewall group domain-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall group dynamic-group address-group <text>

Описание:

Создает динамическую группу IPv4-адресов и присваивает ей имя.

Синтаксис:

- set firewall group dynamic-group address-group <text>
- delete firewall group dynamic-group address-group <text>

- show firewall group dynamic-group address-group

Аргументы:

- <text> — имя группы.

Режим: «Конфигурирование».

---

firewall group dynamic-group address-group <text> description <text>

Описание:

Создает динамическую группу IPv4-адресов, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group dynamic-group address-group <text> description <text>
- delete firewall group dynamic-group address-group <text> description <text>
- show firewall group dynamic-group address-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall group dynamic-group ipv6-address-group <text>

Описание:

Создает динамическую группу IPv6-адресов и присваивает ей имя.

Синтаксис:

- set firewall group dynamic-group ipv6-address-group <text>
- delete firewall group dynamic-group ipv6-address-group <text>
- show firewall group dynamic-group ipv6-address-group

Аргументы:

- <text> — имя группы.

Режим: «Конфигурирование».

---

firewall group dynamic-group ipv6-address-group <text> description <text>

Описание:

Создает динамическую группу IPv6-адресов, присваивает ей имя и добавляет описание.

Синтаксис:

- set firewall group dynamic-group ipv6-address-group <text> description <text>
- delete firewall group dynamic-group ipv6-address-group <text> description <text>
- show * set firewall group dynamic-group ipv6-address-group <text> description

Аргументы:

- <text> — имя группы;
- <text> — описание группы.

Режим: «Конфигурирование».

---

firewall ipv4 [<forward> | <input> | <output>] filter rule <1-999999> add-address-to-group source-address address-group <text>

Описание:

Автоматически добавит IPv4-адрес источника в динамическую группу, если на выбранном потоке сработает правило с указанным номером.

Синтаксис:

- set firewall ipv4 [<forward> | <input> | <output>] filter rule <1-999999> add-address-to-group source-address address-group <text>
- delete firewall ipv4 [<forward> | <input> | <output>] filter rule <1-999999> add-address-to-group source-address address-group <text>
- show firewall ipv4 [<forward> | <input> | <output>] filter rule <1-999999> add-address-to-group source-address address-group

Аргументы:

- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы.

Режим: «Конфигурирование».

---

firewall ipv4 name <name> rule <1-999999> add-address-to-group source-address address-group <text>

Описание:

Автоматически добавит IPv4-адрес источника в динамическую группу, если сработает правило из набора правил.

Синтаксис:

- set firewall ipv4 name <name> rule <1-999999> add-address-to-group source-address address-group <text>
- delete firewall ipv4 name <name> rule <1-999999> add-address-to-group source-address address-group <text>
- show firewall ipv4 name <name> rule <1-999999> add-address-to-group source-address address-group

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы.

Режим: «Конфигурирование».

---

firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group source-address address-group <text>

Описание:

Автоматически добавит IPv6-адрес источника в динамическую группу, если на выбранном потоке сработает правило с указанным номером.

Синтаксис:

- set firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group source-address address-group <text>
- delete firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group source-address address-group <text>
- show firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group source-address address-group

Аргументы:

- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;

- <text> — имя динамической группы.

Режим: «Конфигурирование».

---

firewall ipv6 name <name> rule <1-999999> add-address-to-group source-address address-group <text>

Описание:

Автоматически добавит IPv6-адрес источника в динамическую группу, если сработает правило из набора правил.

Синтаксис:

- set firewall ipv6 name <name> rule <1-999999> add-address-to-group source-address address-group <text>
- delete firewall ipv6 name <name> rule <1-999999> add-address-to-group source-address address-group <text>
- show firewall ipv6 name <name> rule <1-999999> add-address-to-group source-address address-group

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы.

Режим: «Конфигурирование».

---

firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group destination-address address-group <text>

Описание:

Автоматически добавит IPv4-адрес назначения в динамическую группу, если на выбранном потоке сработает правило с указанным номером.

Синтаксис:

- set firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group destination-address address-group <text>
- delete firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group destination-address address-group <text>
- show firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group destination-address address-group

Аргументы:

- <forward> — поток FORWARD;

- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы.

Режим: «Конфигурирование».

---

firewall ipv4 name <name> rule <1-999999> add-address-to-group destination-address address-group <text>

Описание:

Автоматически добавит IPv4-адрес назначения в динамическую группу, если сработает правило из набора правил.

Синтаксис:

- set firewall ipv4 name <name> rule <1-999999> add-address-to-group destination-address address-group <text>
- delete firewall ipv4 name <name> rule <1-999999> add-address-to-group destination-address address-group <text>
- show firewall ipv4 name <name> rule <1-999999> add-address-to-group destination-address address-group

Аргументы: * <name> — имя набора правил; * <1-999999> — порядковый номер правила; * <text> — имя динамической группы.

Режим: «Конфигурирование».

---

firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group destination-address address-group <text>

Описание:

Автоматически добавит IPv6-адрес назначения в динамическую группу, если на выбранном потоке сработает правило с указанным номером.

Синтаксис:

- set firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group destination-address address-group <text>
- delete firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group destination-address address-group <text>
- show firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group destination-address address-group

Аргументы:

- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы.

Режим: «Конфигурирование».

---

firewall ipv6 name <name> rule <1-999999> add-address-to-group destination-address address-group <text>

Описание:

Автоматически добавит IPv6-адрес назначения в динамическую группу, если сработает правило из набора правил.

Синтаксис:

- set firewall ipv6 name <name> rule <1-999999> add-address-to-group destination-address address-group <text>
- delete firewall ipv6 name <name> rule <1-999999> add-address-to-group destination-address address-group <text>
- show firewall ipv6 name <name> rule <1-999999> add-address-to-group destination-address address-group

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы.

Режим: «Конфигурирование».

---

firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>

Описание:

Автоматически добавит IPv4-адрес назначения или источника в динамическую группу, если на выбранном потоке сработает правило с указанным номером. Также задает время жизни IPv4-адреса в составе динамической группы.

Синтаксис:

- set firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>
- delete firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>
- show firewall ipv4 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout

Аргументы:

- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;
- <destination-address> — IPv4-адрес назначения;
- <source-address> — IPv4-адрес источника;
- <text> — имя динамической группы;
- <timeout> — интервал, после которого IPv4-адрес будет удален из динамической группы.

Формат:
<число>s — секунды;
<число>m — минуты;
<число>h — часы;
<число>d — дни.

Режим: «Конфигурирование».

---

firewall ipv4 name <name> rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>

Описание:

Автоматически добавит IPv4-адрес назначения или источника в динамическую группу, если сработает правило из набора правил. Также задает время жизни IPv4-адреса в составе динамической группы.

Синтаксис:

- set firewall ipv4 name <name> rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>
- delete firewall ipv4 name <name> rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>
- show firewall ipv4 name <name> rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы.
- <destination-address> — IPv4-адрес назначения;
- <source-address> — IPv4-адрес источника;
- <text> — имя динамической группы;
- <timeout> — интервал, после которого IPv4-адрес будет удален из динамической группы.

Формат:
<число>s — секунды;
<число>m — минуты;
<число>h — часы;
<число>d — дни.

Режим: «Конфигурирование».

---

firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>

Описание:
Автоматически добавит IPv6-адрес назначения или источника в динамическую группу, если на выбранном потоке сработает правило с указанным номером. Также задает время жизни IPv6-адреса в составе динамической группы.

Синтаксис:

- set firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>
- delete firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>
- show firewall ipv6 [forward | input | output] filter rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout

Аргументы:

- <forward> — поток FORWARD;
- <input> — поток INPUT;
- <output> — поток OUTPUT;
- <1-999999> — порядковый номер правила;

- <destination-address> — IPv6-адрес назначения;
- <source-address> — IPv6-адрес источника;
- <text> — имя динамической группы;
- <timeout> — интервал, после которого IPv6-адрес будет удален из динамической группы.

Формат:
<число>s — секунды;
<число>m — минуты;
<число>h — часы;
<число>d — дни.

Режим: «Конфигурирование».

---

firewall ipv6 name <name> rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>

Описание:

Автоматически добавит IPv6-адрес назначения или источника в динамическую группу, если сработает правило из набора правил. Также задает время жизни IPv6-адреса в составе динамической группы.

Синтаксис:

firewall ipv6 name <name> rule <1-999999> add-address-to-group [destination-address | source-address] address-group <text> timeout <timeout>

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя динамической группы.
- <destination-address> — IPv6-адрес назначения;
- <source-address> — IPv6-адрес источника;
- <text> — имя динамической группы;
- <timeout> — интервал, после которого IPv6-адрес будет удален из динамической группы.

Формат:
<число>s — секунды;
<число>m — минуты;
<число>h — часы;
<число>d — дни.

Режим: «Конфигурирование».

Режим «Администрирование»

firewall group

Описание:

Отображает сводную информацию о всех группах на межсетевом экране.

Синтаксис:

- show firewall group

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

firewall group <text>

Описание:

Отображает сводную информацию о конкретной группе на межсетевом экране.

Синтаксис:

- show firewall group `<text>`

Аргументы:

- `<text>` — имя группы на межсетевом экране.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

firewall group detail

Описание:

Отображает детальную информацию о всех группах на межсетевом экране.

Синтаксис:

- show firewall group detail

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

firewall group <text> detail

Описание:

Отображает детальную информацию о конкретной группе на межсетевом экране.

Синтаксис:

- show firewall group `<text>` detail

Аргументы:

- `<text>` — имя группы на межсетевом экране.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Зоны

Обзор

Зона доступа объединяет в себе несколько интерфейсов и делит сетевую инфраструктуру на сегменты с разным уровнем доступа для трафика. На границах зоны устанавливаются правила фильтрации. Когда трафик переходит из одной зоны в другую, межсетевой экран проверяет пакеты на соответствие заданным правилам.

Поток LOCAL также можно настроить как зону доступа. Это позволит дополнительно защитить входящие и исходящие соединения для процессов внутри маршрутизатора Факел.

Ряд особенностей при настройке зон:

- Сначала необходимо создать зону, а затем добавить в нее интерфейс;
- Один интерфейс может быть назначен только одной зоне;
- На интерфейсе должен быть разрешен входящий и исходящий трафик;
- Движение трафика между зонами зависит от заданных наборов правил;
- Только интерфейсы внутри зоны могут общаться друг с другом. Интерфейсы вне зоны не смогут связаться с интерфейсами внутри зоны;
- Необходимо задать отдельные наборы правил на границах зон для входящего и исходящего трафика.

Совет

Рекомендуем настраивать зоны зеркально и создавать один набор правил для каждой пары зон.

Пример настройки

Шаг	Команда	Описание
1. Настроить интерфейсы Ethernet	set interfaces ethernet `eth0` address `dhcp`	DHCPv4-сервер автоматически назначит IPv4-адрес интерфейсу Ethernet `eth0`
	set interfaces ethernet `eth1` address `192.168.1.1/24`	Назначает интерфейсу Ethernet `eth1` диапазон IPv4-адресов с префиксом подсети 192.168.1.1/24
	set interfaces ethernet `eth2` address `192.168.2.1/24`	Назначает интерфейсу Ethernet `eth2` диапазон IPv4-адресов с префиксом подсети 192.168.2.1/24
2. Создать зоны доступа	set firewall zone WAN description `Internet`	Создает зону доступа с именем WAN и добавляет описание `Internet`
	set firewall zone WAN interface `eth0`	Добавляет в зону WAN интерфейс `eth0`
	set firewall zone LAN description `Local network`	Создает зону доступа с именем LAN и добавляет описание `Local network`
	set firewall zone LAN interface `eth1`	Добавляет в зону доступа LAN интерфейс `eth1`
	set firewall zone LAN interface `eth2`	Добавляет в зону доступа LAN интерфейс `eth2`
3. Настроить движение трафика из зоны LAN в WAN	set firewall ipv4 name LAN-to-WAN default-action `drop`	Создает набор правил с именем LAN-to-WAN и по умолчанию отбрасывает IPv4-трафик при переходе из зоны LAN в WAN
	set firewall ipv4 name LAN-to-WAN rule 10 action `accept`	Создает набор правил с именем LAN-to-WAN, создает правило с порядковым номером 10 и принимает IPv4-трафик при переходе из зоны LAN в WAN
	set firewall ipv4 name LAN-to-WAN rule 10 state established `enable`	Добавляет в набор правил с именем LAN-to-WAN правило с порядковым номером 10 и разрешает трафику от установленных соединений переходить из LAN в WAN
	set firewall ipv4 name LAN-to-WAN rule 10 state related `enable`	Добавляет в набор правил с именем LAN-to-WAN правило с порядковым номером 10 и разрешает трафику от производных соединений переходить из LAN в WAN
	set firewall ipv4 name LAN-to-WAN rule 20 action `accept`	Добавляет в набор правил с именем с именем LAN-to-WAN правиол с порядковым номером 20 и принимает IPv4-трафик при переходе из зоны LAN в WAN
	set firewall ipv4 name LAN-to-WAN rule 20 description `Allow DNS, HTTP, HTTPS, Email`	Добавляет в набор правил с именем LAN-to-WAN правило с порядковым номером 20 и добавляет описание `Allow DNS, HTTP, HTTPS, Email`
	set firewall ipv4 name LAN-to-WAN rule 20 protocol `tcp_udp`	Добавляет в набор правил с именем LAN-to-WAN правило с порядковым номером 20 и выбирает соединения по протоколам TCP и UDP
	set firewall ipv4 name LAN-to-WAN rule 20 destination port `53,80,443,465,587,993,995`	Добавляет в набор правил с именем LAN-to-WAN правило с порядковым номером 20 и указывает порты назначения `53,80,443,465,587,993,995`
4. Настроить движение трафика из зоны WAN в	set firewall ipv4 name WAN-to-LAN default-action `drop`	Создает набор правил с именем WAN-to-LAN и по умолчанию отбрасывает трафик при переходе из WAN в LAN

Список команд

Режим «Конфигурирование»

firewall zone <name>

Описание:

Создает зону с указанным именем.

Синтаксис:

- set firewall zone <name>
- delete firewall zone <name>
- show firewall zone

Аргументы:

- <name>— имя зоны.

Режим: «Конфигурирование».

---

firewall zone <name> interface <interface>

Описание:

Добавляет интерфейс в состав зоны.

Синтаксис:

- set firewall zone <name> interface <interface>
- delete firewall zone <name> interface <interface>
- show firewall zone <name> interface

Аргументы:

- <name>— имя зоны;
- <interface> — имя интерфейса, который будет добавлен с состав зоны.

Режим: «Конфигурирование».

---

firewall zone <name> local-zone

Описание:

Использует поток LOCAL в качестве зоны. Позволяет настраивать фильтрацию входящих и исходящих соединений для процессов внутри маршрутизатора Факел. В локальную зону нельзя добавить интерфейсы. Создать можно только одну локальную зону.

Синтаксис:

- set firewall zone <name> local-zone
- delete firewall zone <name> local-zone
- show firewall zone <name>

Аргументы:

- <name>— имя локальной зоны.

Режим: «Конфигурирование».

---

firewall zone <name> default-action [drop | reject]

Описание:

Устанавливает действие по умолчанию для трафика, адресованного выбранной зоне. Действия по умолчанию автоматически не применяются к трафику из зоны источника.

Синтаксис:

- set firewall zone <name> default-action `[drop | reject]`
- delete firewall zone <name> default-action `[drop | reject]`
- show firewall zone <name> default-action

Аргументы:

- <name>— имя зоны;
- <drop> — отбрасывает пакет без оповещения. Значение по умолчанию;
- <reject> — отбрасывает пакет и оповещает отправителя.

Режим: «Конфигурирование».

---

firewall zone <name> default-log

Описание:

Включает журналирование для выбранной зоны тогда, когда применяется действие по умолчанию.

Синтаксис:

firewall zone <name> default-log firewall zone <name> default-log firewall zone <name> default-log

Аргументы:

- <name> — имя зоны.

Режим: «Конфигурирование».

---

firewall zone <name> description <text>

Описание:

Добавляет описание выбранной зоне.

Синтаксис:

- set firewall zone <name> description <text>
- delete firewall zone <name> description <text>
- show firewall zone <name> description

Аргументы:

- <name> — имя зоны;
- <text> — описание зоны.

Режим: «Конфигурирование».

---

firewall zone <destination-zone> from <source-zone> firewall name <ipv4-rule-set-name>

Описание:

Применяет набор правил фильтрации к пакетам IPv4, когда трафик переходит из зоны источника в зону назначения.

Синтаксис:

set firewall zone <destination-zone> from <source-zone> firewall name <ipv4-rule-set-name>
delete firewall zone <destination-zone> from <source-zone> firewall name <ipv4-rule-set-name>
show firewall zone <destination-zone> from <source-zone> firewall name

Аргументы:

- <destination-zone> — имя зоны назначения;
- <source-zone> — имя зоны источника;
- <ipv4-rule-set-name> — имя набора правил фильтрации для пакетов IPv4. Задается командой *set firewall ipv4 name <name> rule <1-999999> [...]*

Режим: «Конфигурирование».

---

firewall zone <destination-zone> from <source-zone> firewall ipv6-name <ipv6-rule-set-name>

Описание:

Применяет набор правил фильтрации к пакетам IPv6, когда трафик переходит из зоны источника в зону назначения.

Синтаксис:

- set firewall zone <destination-zone> from <source-zone> firewall ipv6-name <ipv6-rule-set-name>
- delete firewall zone <destination-zone> from <source-zone> firewall ipv6-name <ipv6-rule-set-name>
- show firewall zone <destination-zone> from <source-zone> firewall ipv6-name

Аргументы:

- <destination-zone> — зона назначения;
- <source-zone> — зона источника;
- <ipv6-rule-set-name> — имя набора правил фильтрации для пакетов IPv6. Задается командой *set firewall ipv6 name <name> rule <1-999999> [...]*

Режим: «Конфигурирование».

Режим «Администрирование»

show firewall zone-policy

Описание:

Отображает сводную информацию о всех зонах на межсетевом экране.

Синтаксис:

- show firewall zone-policy

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall zone-policy zone <zone>

Описание:

Отображает сводную информацию о конкретной зоне на межсетевом экране.

Синтаксис:

show firewall zone-policy zone <zone>

Аргументы:

- <zone> — имя зоны.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Режим моста

Обзор

В режиме моста межсетевой экран анализирует и фильтрует трафик на втором уровне модели OSI. Режим объединяет физические или виртуальные интерфейсы, сетевые сегменты в одно логическое целое. Данные между объединенными участниками пересылаются прозрачно, без препятствий и вне зависимости от протокола их передачи. Интерфейсы на двух сегментах не знают, что между ними проложен сетевой мост и думают, что соединены друг с другом напрямую. Подробно настройка интерфейсов моста описана в разделе *Интерфейс сетевого моста* (страница 141)

Как и базовый режим межсетевого экрана, режим моста использует правила, классификаторы, поддерживает создание пользовательских наборов правил. Однако синтаксис и набор функций в двух режимах несколько отличаются. В режиме моста задать правила можно лишь для потока FORWARD, остальные потоки работают в автоматическом режиме.

Поток INPUT обозначает трафик, который поступает на интерфейс. Если пакеты адресуются на порт интерфейса в составе межсетевого экрана в режиме моста, то они будут допущены до следующего потока — BRIDGE. На потоке BRIDGE маршрутизатор анализирует пакет и устанавливает, кому он адресован. Правила фильтрации применяются на следующем потоке FORWARD. Если трафик будет соответствовать правилам, он будет допущен до адресата. Если нет, то будет направлен на поток OUTPUT, т.е. на выход межсетевого экрана.

База правил фильтрации способна хранить до 999999 уникальных фильтрующих значений. В соответствии с заданными правилами пакеты будут допущены во внутреннюю сеть, отброшены или перенаправлены. По умолчанию правила на потоках принимают трафик (accept), а созданные наборы правил — отбрасывают (drop).

Примечание

Если вместо MAC-адреса пакеты будут адресованы IP-адресу интерфейса в составе межсетевого экрана в режиме моста, то маршрутизатор не направит данные адресату, а передаст такие пакеты на анализ межсетевому экрану в базовом режиме.

Пример настройки

Шаг	Команда	Описание
1	set firewall bridge forward filter default-action `drop`	По умолчанию отбрасывает пакеты на потоке FORWARD
	set firewall bridge forward filter default-log	Включает журналирование на потоке FORWARD, когда применится действие по умолчанию
2	set firewall bridge forward filter rule 10 action `continue`	Создает правило с порядковым номером 10 на потоке FORWARD и применяет следующее правило. Трафик, пришедший на интерфейс eth2 с VLAN ID 22, передается дальше для следующих правил.
	set firewall bridge forward filter rule 10 inbound-interface name `eth2`	Добавляет правило с порядковым номером 10 в цепочку правил и выбирает внутренний интерфейс `eth2`
	set firewall bridge forward filter rule 10 vlan id 22	Добавляет правило с порядковым номером 10 в цепочку правил и выбирает VLAN-интерфейс с идентификатором 22
3	set firewall bridge forward filter rule 20 action `drop`	Создает правило с порядковым номером 20 на потоке FORWARD и отбрасывает пакеты. Трафик из группы интерфейсов TRUNK-RIGHT с VLAN ID 60 отбрасывается. Это имеет приоритет над последующими разрешающими правилами.
	set firewall bridge forward filter rule 20 inbound-interface group `TRUNK-RIGHT`	Добавляет правило с порядковым номером 20 в цепочку правил и выбирает группу входных интерфейсов `TRUNK-RIGHT`
	set firewall bridge forward filter rule 20 vlan id `60`	Добавляет правило с порядковым номером 20 в цепочку правил и выбирает VLAN-интерфейс с идентификатором `60`
4	set firewall bridge forward filter rule 30 action `jump`	Создает правило с порядковым номером 30 и переходит на другой набор правил. Весь трафик, который отправляется с любых других интерфейсов кроме, переходит на обработку на пользовательский набор правил TEST. После обработки в наборе правил TEST фильтрация вернется к следующему правилу (35) на потоке FORWARD.
	set firewall bridge forward filter rule 30 jump-target `TEST`	Добавляет правило с порядковым номером 30 в цепочку правил и переходит на набор правил `TEST`
	set firewall bridge forward filter rule 30 outbound-interface name `!eth1`	Добавляет правило с порядковым номером 30 в цепочку правил и выбирает все выходные интерфейсы кроме `eth1`
5	set firewall bridge forward filter rule 35 action `accept`	Создает правило с порядковым номером 35 и принимает пакеты
	set firewall bridge forward filter rule 35 vlan id `11`	Добавляет правило с порядковым номером 35 в цепочку правил и выбирает VLAN-интерфейс с идентификатором `11`
6	set firewall bridge forward filter rule 40 action `continue`	Создает правило с порядковым номером 40 и применяет следующее правило
	set firewall bridge forward filter rule 40 destination mac-address `66:55:44:33:22:11`	Добавляет правило с порядковым номером 40 в цепочку правил и задает MAC-адрес назначения `66:55:44:33:22:11`

Список команд

Режим «Конфигурирование»

firewall bridge forward filter rule <1-999999> [<accept> | <continue> | <drop> | <jump> | <queue> | <return>]

Описание:

Создает правило и применяет выбранное действие к трафику на потоке FORWARD.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> [<accept> | <continue> | <drop> | <jump> | <queue> | <return>]
- delete firewall bridge forward filter rule <1-999999> [<accept> | <continue> | <drop> | <jump> | <queue> | <return>]
- show firewall bridge forward filter rule <1-999999> action

Аргументы:

- `<1-999999>` — порядковый номер правила;
- `<accept>` — принимает пакет во внутреннюю сеть;
- `<continue>` — применяет к пакету следующее правило;
- `<drop>` — отбрасывает пакет без оповещения;
- `<reject>` — отбрасывает пакет и оповещает отправителя;
- `<jump>` — переходит на другой набор правил;
- `<return>` — выходит из текущей цепочки, возвращается в исходную и применяет следующее правило исходной цепочки;
- `<queue>` — передает пакет процессам в пользовательском пространстве.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> action [<accept> | <continue> | <drop> | <jump> | <queue> | <return>]

Описание:

Создает набор правил и применяет выбранное действие к трафику.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> action [<accept> | <continue> | <drop> | <jump> | <queue> | return]
- delete firewall bridge name <name> rule <1-999999> action [<accept> | <continue> | <drop> | <jump> | <queue> | return]
- show firewall bridge name <name> rule <1-999999> action

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <accept> — принимает пакет во внутреннюю сеть;
- <continue> — применяет к пакету следующее правило;
- <drop> — отбрасывает пакет без оповещения;
- <reject> — отбрасывает пакет и оповещает отправителя;
- <jump> — переходит на другой набор правил;
- <return> — выходит из текущей цепочки, возвращается в исходную и применяет следующее правило исходной цепочки;
- <queue> — передает пакет процессам в пользовательском пространстве.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> jump-target <text>

Описание:

Создает правило и переходит на другой набор правил.

Предварительно необходимо для аргумента action задать значение jump.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> jump-target <text>
- delete firewall bridge forward filter rule <1-999999> jump-target <text>
- show firewall bridge forward filter rule <1-999999> jump-target

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя другого набора правил, куда будет перенаправлен трафик.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> jump-target <text>

Описание:

Создает набор правил и переходит на другой набор правил.

Предварительно необходимо для аргумента action задать значение jump.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> jump-target <text>
- delete firewall bridge name <name> rule <1-999999> jump-target <text>
- show firewall bridge name <name> rule <1-999999> jump-target

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <text> — имя другого набора правил, куда будет перенаправлен трафик.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> queue <0-65535>

Описание:

Создает правило и отправляет трафик с потока FORWARD на указанную очередь в ядро. По мере освобождения очереди пакеты будут передаваться на обработку процессу в пользовательском пространстве.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall bridge forward filter rule <1-999999> queue <0-65535>
- delete firewall bridge forward filter rule <1-999999> queue <0-65535>
- show firewall bridge forward filter rule <1-999999> queue

Аргументы:

- <1-999999> — порядковый номер правила;
- <0-65535> — номер очереди. Формат: целое число или диапазон чисел. Диапазон значений: от 0 до 65535.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> queue <0-65535>

Описание:

Создает набор правил и отправляет трафик на указанную очередь в ядро. По мере освобождения очереди пакеты будут передаваться на обработку процессу в пользовательском пространстве.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall bridge name <name> rule <1-999999> queue <0-65535>
- delete firewall bridge name <name> rule <1-999999> queue <0-65535>
- show firewall bridge name <name> rule <1-999999> queue

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <0-65535> — номер очереди. Формат: целое число или диапазон чисел. Диапазон значений: от 0 до 65535.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> queue-options bypass

Описание:

Создает правило и не отправляет трафик с потока FORWARD на указанную очередь в ядро. Пакеты будут сразу передаваться на обработку процессу в пользовательском пространстве.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall bridge forward filter rule <1-999999> queue-options bypass
- delete firewall bridge forward filter rule <1-999999> queue-options bypass
- show firewall bridge forward filter rule <1-999999> queue-options

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> queue-options bypass

Описание:

Создает набор правил и не отправляет пакеты на указанную очередь в ядро. Пакеты будут сразу передаваться на обработку процессу в пользовательском пространстве.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall bridge name <name> rule <1-999999> queue-options bypass
- delete firewall bridge name <name> rule <1-999999> queue-options bypass
- show firewall bridge name <name> rule <1-999999> queue-options

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> queue-options fanout

Описание:

Создает правило и распределяет трафик равномерно внутри одной очереди на потоке FORWARD.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall bridge forward filter rule <1-999999> queue-options fanout
- delete firewall bridge forward filter rule <1-999999> queue-options fanout
- show firewall bridge forward filter rule <1-999999> queue-options

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> queue-options fanout

Описание:

Создает набор правил и распределяет трафик равномерно внутри одной очереди.

Предварительно необходимо для аргумента action задать значение queue. Более подробно работа с очередями описана в разделе *Приоритизация трафика (QoS)* (страница 634).

Синтаксис:

- set firewall bridge name <name> rule <1-999999> queue-options fanout
- delete firewall bridge name <name> rule <1-999999> queue-options fanout
- show firewall bridge name <name> rule <1-999999> queue-options

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall bridge forward filter default-action [accept | drop]

Описание:

Создает правило и устанавливает действие по умолчанию, которое применится, если трафик на потоке FORWARD не будет соответствовать ни одному правилу.

Синтаксис:

- set firewall bridge forward filter default-action [<accept> | <drop>]
- delete firewall bridge forward filter default-action [<accept> | <drop>]
- show firewall bridge forward filter default-action

Аргументы:

- <accept> — принимает пакет во внутреннюю сеть;
- <drop> — отбрасывает пакет без оповещения.

Режим: «Конфигурирование».

---

firewall bridge name <name> default-action [<accept> | <continue> | <drop> | <jump> | <queue> | <return>]

Описание:

Создает набор правил и устанавливает действие по умолчанию, которое применится, если трафик не будет соответствовать ни одному правилу.

Синтаксис:

- set firewall bridge name <name> default-action [<accept> | <continue> | <drop> | <jump> | <queue> | <return>]
- delete firewall bridge name <name> default-action [<accept> | <continue> | <drop> | <jump> | <queue> | <return>]
- show firewall bridge name <name> default-action

Аргументы:

- <name> — имя набора правил;
- <accept> — принимает пакет во внутреннюю сеть;
- <continue> — применяет к пакету следующее правило;
- <drop> — отбрасывает пакет без оповещения;
- <jump> — переходит на другой набор правил;
- <queue> — передает пакет процессам в пользовательском пространстве;
- <return> — выходит из текущей цепочки, возвращается в исходную и применяет следующее правило исходной цепочки.

Режим: «Конфигурирование».

---

firewall bridge name <name> default-jump-target <text>

Описание:

Создает набор правил и по умолчанию переходит на другой набор правил.

Предварительно необходимо установить в качестве действия по умолчанию (default-jump-target) значение jump.

Синтаксис:

- set firewall bridge name <name> default-jump-target <text>
- delete firewall bridge name <name> default-jump-target <text>
- show firewall bridge name <name> default-jump-target

Аргументы:

- <name> — имя набора правил;
- <text> — имя другого набора правил, куда будет перенаправлен трафик.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> log

Описание:

Включает журналирование, когда на потоке FORWARD сработает указанное правило.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> log
- delete firewall bridge forward filter rule <1-999999> log
- show firewall bridge forward filter rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> log

Описание:

Включает журналирование, когда сработает указанное правило.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> log
- delete firewall bridge name <name> rule <1-999999> log
- show * set firewall bridge name <name> rule <1-999999>

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall bridge forward filter default-log

Описание:

Включает журналирование на потоке FORWARD, когда применяется действие по умолчанию.

Синтаксис:

- set firewall bridge forward filter default-log
- delete firewall bridge forward filter default-log
- show firewall bridge forward filter

Режим: «Конфигурирование».

---

firewall bridge name <name> default-log

Описание:

Присваивает имя набору правил и включает журналирование тогда, когда применяется действие по умолчанию.

Синтаксис:

- set firewall bridge name <name> default-log
- delete firewall bridge name <name> default-log
- show firewall bridge name <name>

Аргументы:

- <name> — имя набора правил.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]

Описание:

Создает правило и устанавливает, какие события система будет журналировать при поступлении трафика от установленных соединений на потоке FORWARD.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- delete firewall bridge forward filter rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- show firewall bridge forward filter rule <1-999999> log-options level

Аргументы:

- <1-999999> — порядковый номер правила;
- <emerg> — самый высокий уровень опасности. Система не отвечает. Пример: нарушена безопасность периметра сети, потерян контроль над межсетевым экраном;
- <alert> — система находится под серьезной угрозой. Немедленно предпримите необходимые действия. Пример: большой наплыв трафика, вероятность DDoS-атаки;
- <crit> — система находится в критическом состоянии. Если не предпринять действий, состояние системы ухудшится. Пример: классификатор не применился к правилу;
- <err> — ошибка в работе системы. Система продолжит работать, однако потребует внимания. Пример: заканчивается место на диске;
- <warn> — предупреждение. Возможно, система столкнулась с проблемой. Пример: большинство входящих пакетов отвергнуты, отредактируйте правила фильтрации;
- <notice> — уведомление. Состояние системы в норме. Возможно, были изменены некоторые компоненты системы или система была обновлена. Пример: успешно обновлены правила фильтрации;
- <info> — информационные сообщения о статусе системы. Состояние системы в норме. Пример: межсетевой экран работает в штатном режиме;
- <debug> — детализированная отладочная информация. Пример: система выводит информацию об IP-адресах, адресах источника и назначения, протоколах передачи и т.д.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]

Описание:

Создает набор правил и устанавливает, какие события система будет журналировать при поступлении пакетов данных от установленных соединений.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- delete firewall bridge name <name> rule <1-999999> log-options level [<emerg> | <alert> | <crit> | <err> | <warn> | <notice> | <info> | <debug>]
- show firewall bridge name <name> rule <1-999999> log-options level

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <emerg> — самый высокий уровень опасности. Система не отвечает. Пример: нарушена безопасность периметра сети, потерян контроль над межсетевым экраном;
- <alert> — система находится под серьезной угрозой. Немедленно предпримите необходимые действия. Пример: большой наплыв трафика, вероятность DDoS-атаки;
- <crit> — система находится в критическом состоянии. Если не предпринять действий, состояние системы ухудшится. Пример: классификатор не применился к правилу;
- <err> — ошибка в работе системы. Система продолжит работать, однако потребует внимания. Пример: заканчивается место на диске;
- <warn> — предупреждение. Возможно, система столкнулась с проблемой. Пример: большинство входящих пакетов отвергнуты, отредактируйте правила фильтрации;
- <notice> — уведомление. Состояние системы в норме. Возможно, были изменены некоторые компоненты системы или система была обновлена. Пример: успешно обновлены правила фильтрации;
- <info> — информационные сообщения о статусе системы. Состояние системы в норме. Пример: межсетевой экран работает в штатном режиме;
- <debug> — детализированная отладочная информация. Пример: система выводит информацию об IP-адресах, адресах источника и назначения, протоколах передачи и т.д.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> log-options group <0-65535>

Описание:

Создает правило и указывает группу правил, которая будет вести журналирование на потоке FORWARD.

Предварительно необходимо включить журналирование через аргумент log.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> log-options group <0-65535>
- delete firewall bridge forward filter rule <1-999999> log-options group <0-65535>
- show firewall bridge forward filter rule <1-999999> log-options group

Аргументы:

- <1-999999> — порядковый номер правила;
- <0-65535> — номер группы, которая будет вести журналирование.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> log-options group <0-65535>

Описание:

Создает набор правил и указывает группу правил, которая будет вести журналирование.

Предварительно необходимо включить журналирование через аргумент log.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> log-options group <0-65535>
- delete firewall bridge name <name> rule <1-999999> log-options group <0-65535>
- show firewall bridge name <name> rule <1-999999> log-options group

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <0-65535> — номер группы, которая будет вести журналирование.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> log-options snapshot-length <0-9000>

Описание:

Создает правило и устанавливает, насколько детально группа правил будет вести журналирование на потоке FORWARD.

Предварительно необходимо включить журналирование через аргумент log и указать группу правил.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> log-options snapshot-length <0-9000>
- delete firewall bridge forward filter rule <1-999999> log-options snapshot-length <0-9000>
- show firewall bridge forward filter rule <1-999999> log-options snapshot-length

Аргументы:

- <1-999999> — порядковый номер правила;
- <0-9000> — размер полезной нагрузки пакета в байтах, которая будет включена в сообщения netlink. Диапазон значений: от 0 до 9000. Чем выше число, тем подробнее группа будет вести журналирование.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> log-options snapshot-length <0-9000>

Описание:

Создает набор правил и устанавливает, насколько детально группа правил будет вести журналирование.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> log-options snapshot-length <0-9000>
- delete firewall bridge name <name> rule <1-999999> log-options snapshot-length <0-9000>
- show firewall bridge name <name> rule <1-999999> log-options snapshot-length

Аргументы:

- <name> — имя набора правил;
- <0-9000> — размер полезной нагрузки пакета в байтах, которая будет включена в сообщения netlink. Диапазон значений: от 0 до 9000. Чем выше число, тем подробнее группа будет вести журналирование.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> log-options queue-threshold <0-65535>

Описание:

Создает правило и устанавливает порог на количество записей в журнал событий при поступлении трафика на поток FORWARD. По мере освобождения очереди, записи журнала событий будут передаваться процессу в пользовательское пространство.

Предварительно необходимо включить журналирование через аргумент log и указать через аргумент log-options group группу, которая будет вести журналирование.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> log-options queue-threshold <0-65535>
- delete firewall bridge forward filter rule <1-999999> log-options queue-threshold <0-65535>
- show firewall bridge forward filter rule <1-999999> log-options queue-threshold

Аргументы:

- <1-999999> — порядковый номер правила;
- <0-65535> — максимальное число записей в журнал.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> log-options queue-threshold <0-65535>

Описание:

Создает набор правил и устанавливает порог на количество записей в журнал событий при поступлении трафика. По мере освобождения очереди, записи журнала событий будут передаваться процессу в пользовательское пространство.

Предварительно необходимо включить журналирование через аргумент log и указать через аргумент log-options group группу, которая будет вести журналирование.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> log-options queue-threshold <0-65535>
- delete firewall bridge name <name> rule <1-999999> log-options queue-threshold <0-65535>
- show firewall bridge name <name> rule <1-999999> log-options queue-threshold

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <0-65535> — максимальное число записей в журнал.

Режим: «Конфигурирование».

---

firewall bridge name <name> description <text>

Описание:

Создает набор правил и добавляет описание.

Синтаксис:

- set firewall bridge name <name> description <text>
- delete firewall bridge name <name> description <text>
- show firewall bridge name <name> description

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> disable

Описание:

Отключает правило для трафика на потоке FORWARD, но сохраняет конфигурацию.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> disable
- delete firewall bridge forward filter rule <1-999999> disable
- show firewall bridge forward filter rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-9999999> disable

Описание:

Отключает набор правил, но сохраняет конфигурацию.

Синтаксис:

- set firewall bridge name <name> rule <1-9999999> disable
- delete firewall bridge name <name> rule <1-9999999> disable
- show firewall bridge name <name> rule

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> destination mac-address <mac-address>

Описание:

Создает правило и задает MAC-адрес назначения для фильтрации трафика на потоке FORWARD.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> destination mac-address <mac-address>
- delete firewall bridge forward filter rule <1-999999> destination mac-address <mac-address>
- show firewall bridge forward filter rule <1-999999> destination mac-address

Аргументы:

- <1-999999> — порядковый номер правила;
- <mac-address> — MAC-адрес. Формат: xx.xx.xx.xx.xx.xx.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> destination mac-address <mac-address>

Описание:

Создает набор правил и задает MAC-адрес назначения для фильтрации трафика.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> destination mac-address <mac-address>
- delete firewall bridge name <name> rule <1-999999> destination mac-address <mac-address>
- show firewall bridge name <name> rule <1-999999> destination mac-address <mac-address>

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <mac-address> — MAC-адрес. Формат: xx.xx.xx.xx.xx.xx.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> source mac-address <mac-address>

Описание:

Создает правило и задает MAC-адрес источника для фильтрации трафика на потоке FORWARD.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> source mac-address <mac-address>

- delete firewall bridge forward filter rule <1-999999> source mac-address <mac-address>
- show firewall bridge forward filter rule <1-999999> source mac-address

Аргументы:

- <1-999999> — порядковый номер правила;
- <mac-address> — MAC-адрес. Формат: xx.xx.xx.xx.xx.xx.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> source mac-address <mac-address>

Описание:

Создает набор правил и задает MAC-адрес источника для фильтрации трафика.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> source mac-address <mac-address>
- delete firewall bridge name <name> rule <1-999999> source mac-address <mac-address>
- show firewall bridge name <name> rule <1-999999> source mac-address

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <mac-address> — MAC-адрес. Формат: xx.xx.xx.xx.xx.xx.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> inbound-interface name <iface>

Описание:

Создает правило на потоке FORWARD и выбирает входной интерфейс, через который трафик поступает на межсетевой экран.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> inbound-interface name <iface>
- delete firewall bridge forward filter rule <1-999999> inbound-interface name <iface>
- show firewall bridge forward filter rule <1-999999> inbound-interface name

Аргументы:

- <1-999999> — порядковый номер правила;
- <iface> — входной интерфейс, через который трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> inbound-interface name <iface>

Описание:

Создает набор правил и выбирает входной интерфейс, через который трафик поступает на межсетевой экран.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> inbound-interface name <iface>
- delete firewall bridge name <name> rule <1-999999> inbound-interface name <iface>
- show firewall bridge name <name> rule <1-999999> inbound-interface name

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <iface> — входной интерфейс, через который трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> inbound-interface group <iface_group>

Описание:

Создает правило на потоке FORWARD и выбирает группу входных интерфейсов, через которую трафик поступает на межсетевой экран.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> inbound-interface group <iface_group>
- delete firewall bridge forward filter rule <1-999999> inbound-interface group <iface_group>
- show firewall bridge forward filter rule <1-999999> inbound-interface group

Аргументы:

- <1-999999> — порядковый номер правила;
- <iface_group> — группа входных интерфейсов, через которую трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> inbound-interface group <iface_group>

Описание:

Создает набор правил и выбирает группу входных интерфейсов, через которую трафик поступает на межсетевой экран.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> inbound-interface group <iface_group>
- delete firewall bridge name <name> rule <1-999999> inbound-interface group <iface_group>
- show firewall bridge name <name> rule <1-999999> inbound-interface group

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <iface_group> — группа входных интерфейсов, через которую трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> outbound-interface name <iface>

Описание:

Создает правило на потоке FORWARD и выбирает выходной интерфейс, через который трафик исходит с межсетевого экрана.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> outbound-interface name <iface>
- delete firewall bridge forward filter rule <1-999999> outbound-interface name <iface>
- show firewall bridge forward filter rule <1-999999> outbound-interface name

Аргументы:

- <1-999999> — порядковый номер правила;
- <iface> — выходной интерфейс, через который трафик исходит с межсетевого экрана. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> outbound-interface name <iface>

Описание:

Создает набор правил и выбирает выходной интерфейс, через который трафик исходит с межсетевого экрана.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> outbound-interface name <iface>
- delete firewall bridge name <name> rule <1-999999> outbound-interface name <iface>
- show firewall bridge name <name> rule <1-999999> outbound-interface name

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <iface> — выходной интерфейс, через который трафик исходит с межсетевого экрана. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> outbound-interface group <iface_group>

Описание:

Создает правило на потоке FORWARD и выбирает группу выходных интерфейсов, через которую трафик исходит с межсетевого экрана.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> outbound-interface group <iface_group>
- delete firewall bridge forward filter rule <1-999999> outbound-interface group <iface_group>
- show firewall bridge forward filter rule <1-999999> outbound-interface group

Аргументы:

- <1-999999> — порядковый номер правила;
- <iface_group> — группа выходных интерфейсов, через которую трафик исходит с межсетевого экрана.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> outbound-interface group <iface_group>

Описание:

Создает набор правил и выбирает группу выходных интерфейсов, через которую трафик исходит с межсетевого экрана.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> outbound-interface group <iface_group>
- delete firewall bridge name <name> rule <1-999999> outbound-interface group <iface_group>
- show firewall bridge name <name> rule <1-999999> outbound-interface group

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <iface_group> — группа выходных интерфейсов, через которую трафик исходит с межсетевого экрана.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> vlan id [<0-4096> | <start-end>]

Описание:

Создает правило на потоке FORWARD и фильтрует трафик, который принадлежит определенному VLAN-интерфейсу или диапазону.

Синтаксис:

- set firewall bridge forward filter rule <1-999999> vlan id <0-4096>
- delete firewall bridge forward filter rule <1-999999> vlan id <0-4096>
- show firewall bridge forward filter rule <1-999999> vlan id

Аргументы:

- <1-999999> — порядковый номер правила;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4096.
- <start>-<end> — диапазон идентификаторов VLAN-интерфейсов. Диапазон значений: от 0 до 4096.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> vlan id [<0-4096> | <start-end>]

Описание:

Создает набор правил и фильтрует трафик, который принадлежит определенному VLAN-интерфейсу или диапазону.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> vlan id <0-4096>
- delete firewall bridge name <name> rule <1-999999> vlan id <0-4096>
- show firewall bridge name <name> rule <1-999999> vlan id

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <vlan-id> — идентификатор VLAN-интерфейса. Диапазон значений: от 0 до 4096.
- <start>-<end> — диапазон идентификаторов VLAN-интерфейсов. Диапазон значений: от 0 до 4096.

Режим: «Конфигурирование».

---

firewall bridge forward filter rule <1-999999> vlan priority [<0-7> | <start>-<end>]

Описание:

Синтаксис:

- set firewall bridge forward filter rule <1-999999> vlan priority [<0-7> | <start>-<end>]
- delete firewall bridge forward filter rule <1-999999> vlan priority [<0-7> | <start>-<end>]
- show firewall bridge forward filter rule <1-999999> vlan priority

Аргументы:

- <1-999999> — порядковый номер правила;
- <0-7> — приоритет VLAN (priority code point). Диапазон значений: от 0 до 7;
- <start-end> — диапазон приоритета VLAN (priority code point). Диапазон значений: от 0 до 7.

Режим: «Конфигурирование».

---

firewall bridge name <name> rule <1-999999> vlan priority [<0-7> | <start>-<end>]

Описание:

Создает набор правил и устанавливает приоритет VLAN (802.1p) для фильтрации трафика.

Синтаксис:

- set firewall bridge name <name> rule <1-999999> vlan priority [<0-7> | <start>-<end>]
- delete firewall bridge name <name> rule <1-999999> vlan priority [<0-7> | <start>-<end>]
- show firewall bridge name <name> rule <1-999999> vlan priority

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила;
- <0-7> — приоритет VLAN (priority code point). Диапазон значений: от 0 до 7;
- <start-end> — диапазон приоритета VLAN (priority code point). Диапазон значений: от 0 до 7.

Режим: «Конфигурирование».

Режим «Администрирование»

show firewall bridge

Описание:

Отображает детальную информацию о конфигурации межсетевого экрана режиме сетевого моста.

Синтаксис:

show firewall bridge

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall bridge forward filter

Описание:

Отображает информацию об активных правилах на потоке FORWARD.

Синтаксис:

show firewall bridge forward filter

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall bridge forward filter rule <1-999999>

Описание:

Отображает информацию об активном правиле на потоке FORWARD с указанным порядковым номером.

Синтаксис:

show firewall bridge forward filter rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall bridge name <name>

Описание:

Отображает информацию об активных наборах правил.

Синтаксис:

show firewall bridge name <name>

Аргументы:

- <name> — имя набора правил.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show firewall bridge name <name> rule <1-999999>

Описание:

Отображает информацию об активном наборе правил.

Синтаксис:

show firewall bridge name <name> rule <1-999999>

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall bridge

Описание:

Отображает все записи в журнале регистрации событий на межсетевом экране в режиме моста.

Синтаксис:

show log firewall bridge

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall bridge forward

Описание:

Отображает записи в журнале регистрации событий для трафика на потоке FORWARD.

Синтаксис:

show log firewall bridge forward

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall bridge forward filter

Описание:

Отображает записи в журнале регистрации событий для правил фильтрации.

Синтаксис:

show log firewall bridge forward filter

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall bridge name <name>

Описание:

Отображает записи в журнале регистрации событий для набора правил.

Синтаксис:

show log firewall bridge name <name>

Аргументы:

- <name> — имя набора правил.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall bridge forward filter rule <1-999999>

Описание:

Отображает записи в журнале регистрации событий для правила с указанным порядковым номером.

Синтаксис:

show log firewall bridge forward filter rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log firewall bridge name <name> rule <1-999999>

Описание:

Отображает записи в журнале регистрации событий для набора правил.

Синтаксис:

show log firewall bridge name <name> rule <1-999999>

Аргументы:

- <name> — имя набора правил;
- <1-999999> — порядковый номер правила.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Таблица потоков

Обзор

Таблица потоков — это механизм на межсетевом экране для отслеживания и оптимизации нагрузки.

По умолчанию каждый входящий пакет проходит стандартный путь фильтрации: анализируется и проверяется на соответствие правилам. Однако если на МСЭ поступит много трафика, то проверка на правила увеличит нагрузку на ЦП и приведет к снижению пропускной способности.

В таблице потоков МСЭ автоматически ведет учет соединений и их состояний с помощью механизма conntrack. Пакеты, относящиеся к учтенным соединениям в таблице, будут отправлены по короткому пути в обход стандартного пути для дальнейшей обработки.

Чтобы включить таблицу потоков, необходимо:

- Создать таблицу потоков;
- Добавить входной и выходной интерфейсы;
- Создать правило фильтрации с действием *offload* и указать таблицу потоков в *offload-target*.

Чтобы дополнительно сэкономить программные ресурсы МСЭ, включите аппаратную разгрузку. При этом сетевая карта устройства должна поддерживать соответствующий режим, иначе функция работать не будет.

Пример настройки

Шаг	Команда	Описание
1	set firewall flowtable FT01 interface `eth0`	Создает таблицу потоков FT01 и добавляет интерфейс `eth0`
2	set firewall flowtable FT01 interface `eth1`	Добавляет в таблицу потоков FT01 интерфейс `eth1`
3	set firewall ipv4 forward filter default-action `drop`	По умолчанию отбрасывает все входящие пакеты на потоке FORWARD
4	set firewall ipv4 forward filter rule 10 action `offload`	Создает правило с порядковым номером 10 и включает разгрузку на потоке FORWARD
5	set firewall ipv4 forward filter rule 10 offload-target `FT01`	Добавляет правило с порядковым номером 10 в цепочку правил и выбирает таблицу потоков `FT01` для разгрузки
6	set firewall ipv4 forward filter rule 10 state `established`	Добавляет правило с порядковым номером 10 в цепочку правил и выбирает установленные TCP-соединения на потоке FORWARD. После установления соединения пакеты будут переданы на таблицу потоков для разгрузки
7	set firewall ipv4 forward filter rule 10 state `related`	Добавляет правило с порядковым номером 10 в цепочку правил и выбирает производные TCP-соединения на потоке FORWARD. После установления соединения все производные соединения также будут передаваться на таблицу потоков для разгрузки
8	set firewall ipv4 forward filter rule 110 action `accept`	Создает правило с порядковым номером 110 и принимает входящий трафик на потоке FORWARD
9	set firewall ipv4 forward filter rule 110 destination address `192.0.2.100`	Добавляет правило с порядковым номером 110 в цепочку правил и указывает IPv4-адрес назначения `192.0.2.100`
10	set firewall ipv4 forward filter rule 110 destination port `1122`	Добавляет правило с порядковым номером 110 в цепочку правил и указывает порт назначения `1122`
11	set firewall ipv4 forward filter rule 110 inbound-interface name „eth0“	Добавляет правило с порядковым номером 110 в цепочку правил и указывает входной интерфейс `eth0`
12	set firewall ipv4 forward filter rule 110 protocol `tcp`	Добавляет правило с порядковым номером 110 в цепочку правил и выбирает протокол TCP для передачи данных

Список команд

Режим «Конфигурирование»

firewall flowtable <flow_table_name>

Описание:

Создает таблицу потоков.

Синтаксис:

- set firewall flowtable <flow_table_name>
- delete firewall flowtable <flow_table_name>
- show firewall flowtable

Аргументы:

- <flow_table_name> — имя таблицы потоков.

Режим: «Конфигурирование».

---

firewall flowtable <flow_table_name> interface <iface>

Описание:

Добавляет интерфейс в таблицу потоков.

Синтаксис:

- set firewall flowtable <flow_table_name> interface <iface>
- delete firewall flowtable <flow_table_name> interface <iface>
- show firewall flowtable <flow_table_name> interface

Аргументы:

- <flow_table_name> — имя таблицы потоков;
- <iface> — интерфейс, через который трафик поступает на межсетевой экран и который станет участником таблицы потоков. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

Примечание

МСЭ автоматически определит входные интерфейсы через специальный механизм перехвата. Входной и выходной интерфейсы добавляются одной общей командой.

---

firewall flowtable <flow_table_name> description <text>

Описание:

Добавляет описание для таблицы потоков.

Синтаксис:

- set firewall flowtable <flow_table_name> description <text>
- delete firewall flowtable <flow_table_name> description <text>
- show firewall flowtable <flow_table_name> description

Аргументы:

- <flow_table_name> — имя таблицы потоков;
- <text> — описание для таблицы потоков.

Режим: «Конфигурирование».

---

firewall flowtable <flow_table_name> offload <hardware | software>

Описание:

Включает аппаратную или программную разгрузку.

Синтаксис:

- set firewall flowtable <flow_table_name> offload <hardware | software>
- delete firewall flowtable <flow_table_name> offload <hardware | software>
- show firewall flowtable <flow_table_name> offload

Аргументы:

- <flow_table_name> — имя таблицы потоков;
- <hardware> — аппаратная разгрузка. Сетевая карта устройства должна поддерживать данный тип разгрузки;
- <software> — программная разгрузка. Значение по умолчанию.

Режим: «Конфигурирование».

---

firewall [ipv4 | ipv6] forward filter rule <1-999999> action offload

Описание:

Включает разгрузку при срабатывании указанного правила на потоке FORWARD.

Синтаксис:

- set firewall [ipv4 | ipv6] forward filter rule <1-999999> action offload
- delete firewall [ipv4 | ipv6] forward filter rule <1-999999> action offload
- show firewall [ipv4 | ipv6] forward filter rule <1-999999> action

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

firewall [ipv4 | ipv6] forward filter rule <1-999999> offload-target <text>

Описание:

Создает правило на потоке FORWARD и выбирает таблицу потоков, которая будет отслеживать соединения и направлять трафик на разгрузку. Если трафик подпадет под правило, он будет отправлен на таблицу потоков для разгрузки.

Синтаксис:

- set firewall [ipv4 | ipv6] forward filter rule <1-999999> offload-target <text>
- delete firewall [ipv4 | ipv6] forward filter rule <1-999999> offload-target <text>
- show firewall [ipv4 | ipv6] forward filter rule <1-999999> offload-target

Аргументы:

- <ipv4> — IPv4-трафик;
- <ipv6> — IPv6-трафик;
- <1-999999> — порядковый номер правила;
- <text> — таблица потоков для разгрузки.

Режим: «Конфигурирование».

2.5.2 Преобразование сетевых адресов (NAT)

2.5.2.1 Обзор

NAT — это технология, которая преобразует IP-адреса и/или порты в заголовках транзитных пакетов. Чаще всего используется для маршрутизации нескольких внутренних IP-адресов через общий внешний IP-адрес и для сокрытия внутренних адресов от внешних сетей.

NAT на маршрутизаторе Факел поддерживает три типа преобразования адресов:

- NAT44 — внутренний IPv4-адрес во внешний IPv4;
- NAT64 — внутренний IPv6-адрес во внешний IPv4;
- NAT66 — внутренний IPv4-адрес во внешний IPv4.

Направления преобразования

NAT преобразует адреса в соединениях трех направлений: исходящем (SNAT), входящем (DNAT) и двустороннем (Bi-NAT). В каждом случае маршрутизатор находится посередине, между внутренней и внешней сетью, и выполняет преобразования входящего и/или исходящего трафика в соответствии с заданными параметрами. Адрес, в который преобразуется исходный адрес называется *целевым адресом преобразования*.

Механизмы NAT

В NAT существуют четыре механизма: статический NAT, динамический NAT, преобразование порта (PAT) и переадресация порта (Port Forwarding).

Статический NAT (static NAT) на маршрутизаторе Факел преобразует один внутренний IP-адрес в один внешний и обратно. Если извне поступит ответный пакет, NAT произведет обратное преобразование и допустит трафик до получателя во внутренней сети. Для статического преобразования достаточно лишь задать внешний адрес — `destination` и внутренний адрес получателя — `translation`. По сути, статический NAT совмещает в себе SNAT и DNAT и является упрощенной формой преобразования. Статический NAT работает без указания портов, поэтому вы можете использовать его в связке с протоколами, которые не использует порты, например, GRE.

Динамический NAT на маршрутизаторе Факел преобразует один внутренний IP-адрес во внешний динамическим способом, т.е. внешний IP-адрес назначается клиенту в порядке живой очереди из таблицы NAT с доступными и заранее выделенными внешними IP-адресами.

Преобразование порта (PAT) на маршрутизаторе Факел меняет внутренний IP-адрес на внешний и добавляет уникальный номер порта, соответствующий конкретной машине во внутренней сети. При этом маршрутизатор будет отслеживать адреса соединений в таблице NAT. Когда пакет будет возвращаться по обратному пути, маршрутизатор допустит пакет до адресата во внутреннюю сеть, если обнаружит соответствующую запись в своей таблице NAT. Некоторые порты (80 или 22) заняты службами и PAT не может их использовать в качестве идентификатора. Однако это не является проблемой, поскольку диапазон значений в пространстве TCP/IP допускает до 65536 уникальных номеров.

Переадресация порта на маршрутизаторе Факел чаще используется в сценариях для входящего трафика. Когда пакет поступает на определенный порт, его внешний адрес преобразуется во внутренний с учетом идентификатора порта и допускается до конкретного получателя.

Правила преобразования NAT

Чтобы включить и настроить механизмы NAT, используйте правила преобразования. Правила создаются отдельно для каждого типа преобразования (NAT44, NAT64, NAT66).

В дополнение каждый тип позволяет задать правила отдельно для исходящего и входящего направлений преобразования и отдельно для статического NAT. Чтобы создать правило для двустороннего соединения, укажите правила с одинаковыми порядковыми номерами для исходящего и входящего соединений.

Информация по работе с правилами содержится в соответствующих разделах для каждого типа преобразования:

- *Настройка NAT44* (страница 587),
- *Настройка NAT64* (страница 623),
- *Настройка NAT66* (страница 628).

Настройка NAT перед VPN

Если поставщик услуг (ASP) требует доступ к своим сервисам через VPN и специально предоставленный IP-адрес источника, настройте NAT перед VPN. В такой конфигурации NAT будет сначала преобразовывать внутренние IP-адреса в адрес источника от поставщика услуг, а затем направлять трафик через VPN-туннель на сервер поставщика услуг.

Распределение нагрузки

В NAT встроена функция распределения нагрузки между устройствами внутри сети с разными IP-адресами. Сначала NAT преобразует внешний IP-адрес в *целевой адрес преобразования*, а затем адресует пакет устройству с конкретным IP-адресом внутри сети согласно выбранному весу устройства и на основе типа хэширования.

Для распределения нагрузки между устройствами с разными IP-адресами NAT использует хэш: набор уникальных символов-идентификаторов, которые маркируют соединения и позволяют пакетам с одного и того же источника попадать на один и тот же адрес назначения. Таким образом NAT поддерживает состояние сессии на сервере.

Символы хэша генерируются случайно или представляют собой разное сочетание данных пакетов: адресов и/или портов источника и назначения. По умолчанию работает случайная генерация.

Чтобы включить распределение нагрузки, укажите нужные IP-адреса устройств `load-balance backend` и вес каждого из них `load-balance backend x.x.x.x weight`. Вес означает процентную долю соединений, которая будет направлена на соответствующий сервер. Суммарный вес всех устройств должен равняться 100.

Утечка трафика при NAT

В некоторых случаях с внешнего интерфейса может исходить трафик, который не был преобразован через NAT и это может выглядеть как неработающий NAT, однако на самом деле система работает исправно. Такое поведение вызвано тем, что интерфейс продолжает посылать трафик с флагами состояния TCP-соединения: RST, FIN ACK, RST ACK даже после того, как МСЭ пометил соединение как INVALID. Эти сообщения о состоянии не представляют угрозу.

Чтобы полностью убрать утечку, настройте МСЭ так, чтобы он отбрасывал пакеты с меткой INVALID. Однако соединения с меткой INVALID могут быть полезны для поиска неисправностей и при просмотре журнала событий.

Обратный NAT

Иногда может возникнуть ситуация, когда внутренний интерфейс будет обращаться через NAT ко внешнему IP-адресу устройства, которое на самом деле расположено в той же сети, что и внутренний интер-

фейс и обладает своим внутренним IP-адресом. В таком случае NAT будет преобразовывать внутренние адреса во внешние и обратно, но устройство-адресат не получит пакеты. Возникнет замкнутый цикл.

Чтобы этого не происходило, используйте технику обратного NAT (Hairpin NAT), которая перехватывает исходящий пакет и меняет внешний адрес назначения на внутренний. Таким образом, трафик не выходит за пределы сети и маршрутизируется корректно.

Чтобы настроить обратный NAT, добавьте к уже существующим правилам исходящего трафика еще номер порта назначения, внутренний интерфейс назначения, тип протокола и адрес преобразования.

Настройка NAT44

Обзор

Технология NAT44 преобразует внутренний IPv4-адрес во внешний IPv4.

Чтобы включить и настроить механизм преобразования NAT44, используйте правила. Каждое правило состоит из *порядкового номера* и *классификатора*.

Чтобы маршрутизатор начал обрабатывать правило, ему необходимо присвоить *порядковый номер* от 1 до 999999. Маршрутизатор считывает правила по порядку, т.е. срабатывает первое подошедшее правило и соблюдается последовательность. Если присвоить правилам одинаковые номера, то они будут сгруппированы и объединены в логическую *цепочку*. Маршрутизатор будет воспринимать такую цепочку как единое целое. Чтобы изменить номер правила, используйте команду *rename*, для копирования — *copy*.

Примечание

Все новые изменения применятся к будущим соединениям. Ранее установленные соединения затронуты не будут.

Каждое правило имеет уникальный *классификатор* — признак, по которому будет проходить фильтрация. Классификатором может быть интерфейс, протокол, тип преобразования, исходный адрес и т.д. Перечислить значения можно через запятую. Чтобы инвертировать список значений, используйте символ «!».

Пример настройки NAT44

Шаг	Команда	Описание
1	set nat source rule 10 description `NAT to Internet`	Создает правило преобразования NAT44 для исходящего трафика с порядковым номером 10 и добавляет описание `NAT to Internet`
2	set nat source rule 10 destination address `0.0.0.0/0`	Добавляет правило с порядковым номером 10 в цепочку правил и задает адрес назначения `0.0.0.0/0`
3	set nat source rule 10 outbound-interface name `eth0`	Добавляет правило с порядковым номером 10 в цепочку правил и выбирает интерфейс `eth0` в качестве выходного
4	set nat source rule 10 source address `10.10.0.0/24`	Добавляет правило с порядковым номером 10 в цепочку правил и указывает адрес источника `10.10.0.0/24`
5	set nat source rule 10 translation address `masquerade`	Добавляет правило с порядковым номером 10 в цепочку правил и выбирает целевой адрес преобразования из списка доступных адресов. В конкретном случае в качестве целевого адреса преобразования выступит адрес, назначенный на eth0
6	set nat source rule 20 description `Internet`	Создает правило преобразования NAT44 для исходящего трафика с порядковым номером 20 и добавляет описание `Internet`
7	set nat source rule 20 destination address `0.0.0.0/0`	Добавляет правило с порядковым номером 20 в цепочку правил и указывает адрес назначения `0.0.0.0/0`
8	set nat source rule 20 destination port `http,https`	Добавляет правило с порядковым номером 20 в цепочку правил и указывает имя порта назначения
9	set nat source rule 20 outbound-interface name `eth0`	Добавляет правило с порядковым номером 20 в цепочку правил и выбирает интерфейс `eth0` в качестве выходного
10	set nat source rule 20 protocol `tcp`	Добавляет правило с порядковым номером 20 в цепочку правил и выбирает протокол TCP для передачи данных
11	set nat source rule 20 source address `17.10.110.0/24`	Добавляет правило с порядковым номером 20 в цепочку правил и указывает IPv4-адрес источника `17.10.110.0/24`
12	set nat source rule 20 translation address `masquerade`	Добавляет правило с порядковым номером 20 в цепочку правил и выбирает целевой адрес преобразования из списка доступных адресов. В конкретном случае в качестве целевого адреса преобразования выступит адрес, назначенный на eth0

Список команд

Режим «Конфигурирование»

nat destination rule <1-999999> description <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и добавляет описание.

Синтаксис:

- set nat destination rule <1-999999> description <text>
- delete nat destination rule <1-999999> description <text>
- show nat destination rule <1-999999> description

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — описание правила.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> destination address [<address> | <CIDR> | <addressrange>]

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве назначения IPv4-адрес или диапазон адресов, который будет преобразован.

Синтаксис:

- set nat destination rule <1-999999> destination address [<address> | <CIDR> | <addressrange>]
- delete nat destination rule <1-999999> destination address [<address> | <CIDR> | <addressrange>]
- show nat destination rule <1-999999> destination address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес назначения. Формат: x.x.x.x;
- <CIDR> — диапазон целевых адресов преобразования с префиксом подсети. Формат: x.x.x.x/x;

- <addressrange> — диапазон целевых адресов преобразования. Формат: x.x.x.x-x.x.x.x.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> destination group address-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве назначения группу IPv4-адресов, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> destination group address-group <text>
- delete nat destination rule <1-999999> destination group address-group <text>
- show nat destination rule <1-999999> destination group address-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя группы IPv4-адресов назначения.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> destination group domain-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве назначения группу доменов, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> destination group domain-group <text>
- delete nat destination rule <1-999999> destination group domain-group <text>
- show nat destination rule <1-999999> destination group domain-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя группы доменов.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> destination group mac-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве назначения группу MAC-адресов, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> destination group mac-group <text>
- delete nat destination rule <1-999999> destination group mac-group <text>
- show nat destination rule <1-999999> destination group mac-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя группы MAC-адресов.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> destination group network-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве назначения группу подсетей, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> destination group network-group <text>
- delete nat destination rule <1-999999> destination group network-group <text>
- show nat destination rule <1-999999> destination group network-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя группы подсетей.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> destination group port-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве назначения группу портов, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> destination group port-group <text>
- delete nat destination rule <1-999999> destination group port-group <text>
- show nat destination rule <1-999999> destination group port-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя группы портов.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> destination port [<text> | <1-65535> | <start-end> | <none>]

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве назначения порт, который будет преобразован.

Синтаксис:

- set nat destination rule <1-999999> destination port [<text> | <1-65535> | <start-end> | <none>]
- delete nat destination rule <1-999999> destination port [<text> | <1-65535> | <start-end> | <none>]
- show nat destination rule <1-999999> destination port

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя порта назначения, указанное в директории /etc/services;
- <1-65535> — номер порта назначения. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон портов назначения. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> disable

Описание:

Создает правило преобразования NAT44 для входящего трафика и выключает NAT44.

Синтаксис:

- set nat destination rule <1-999999> disable
- delete nat destination rule <1-999999> disable

- show nat destination rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> exclude

Описание:

Создает правило преобразования NAT44 для входящего трафика и не применяет преобразование к пакетам, подпадающим под правило.

Синтаксис:

- set nat destination rule <1-999999> exclude
- delete nat destination rule <1-999999> exclude
- show nat destination rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> inbound-interface group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и выбирает группу интерфейсов, через которую трафик поступает на маршрутизатор.

Синтаксис:

- set nat destination rule <1-999999> inbound-interface group <text>
- delete nat destination rule <1-999999> inbound-interface group <text>
- show nat destination rule <1-999999> inbound-interface group

Аргументы:

- <1-999999> — порядковый номер правила;
- <iface_group> — группа интерфейсов, через которую трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> inbound-interface name <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и выбирает интерфейс, через который трафик поступает на маршрутизатор.

Синтаксис:

- set nat destination rule <1-999999> inbound-interface name <text>
- delete nat destination rule <1-999999> inbound-interface name <text>
- show nat destination rule <1-999999> inbound-interface name

Аргументы:

- <1-999999> — порядковый номер правила;
- <iface> — интерфейс, через который трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> load-balance backend <address>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает IPv4-адрес устройства, участвующего в распределении разгрузки.

Синтаксис:

- set nat destination rule <1-999999> load-balance backend <address>
- delete nat destination rule <1-999999> load-balance backend <address>
- show nat destination rule <1-999999> load-balance backend

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес устройства, участвующего в распределении разгрузки.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> load-balance backend <address> weight <1-100>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает вес устройства с конкретным IPv4-адресом.

Синтаксис:

- set nat destination rule <1-999999> load-balance backend <address> weight <1-100>
- delete nat destination rule <1-999999> load-balance backend <address> weight <1-100>
- show nat destination rule <1-999999> load-balance backend <address> weight

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес устройства, участвующего в распределении разгрузки;
- <1-100> — вес устройства при распределении нагрузки. Сумма значений всех устройства должна составлять 100.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> load-balance hash source-address

Описание:

Создает правило преобразования NAT44 для входящего трафика и генерирует хэш на основе IPv4-адреса источника.

Синтаксис:

- set nat destination rule <1-999999> load-balance hash source-address
- delete nat destination rule <1-999999> load-balance hash source-address
- show nat destination rule <1-999999> load-balance hash

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> load-balance hash destination-address

Описание:

Создает правило преобразования NAT44 для входящего трафика и генерирует хэш на основе IPv4-адреса назначения.

Синтаксис:

- set nat destination rule <1-999999> load-balance hash destination-address
- delete nat destination rule <1-999999> load-balance hash destination-address
- show nat destination rule <1-999999> load-balance hash destination-address

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> load-balance hash source-port

Описание:

Создает правило преобразования NAT44 для входящего трафика и генерирует хэш на основе порта источника.

Синтаксис:

- set nat destination rule <1-999999> load-balance hash source-port
- delete nat destination rule <1-999999> load-balance hash source-port
- show nat destination rule <1-999999> load-balance hash

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> load-balance hash destination-port

Описание:

Создает правило преобразования NAT44 для входящего трафика и генерирует хэш на основе порта назначения.

Синтаксис:

- set nat destination rule <1-999999> load-balance hash destination-port
- delete nat destination rule <1-999999> load-balance hash destination-port
- show nat destination rule <1-999999> load-balance hash

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> load-balance hash random

Описание:

Создает правило преобразования NAT44 для входящего трафика и генерирует хэш случайным образом.

Синтаксис:

- set nat destination rule <1-999999> load-balance hash random
- delete nat destination rule <1-999999> load-balance hash random
- show nat destination rule <1-999999> load-balance hash

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> log

Описание:

Создает правило преобразования NAT44 для входящего трафика и включает журналирование.

Синтаксис:

- set nat destination rule <1-999999> log
- delete nat destination rule <1-999999> log
- show nat destination rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]

Описание:

Создает правило преобразования NAT44 для входящего трафика и задает тип вещания для преобразования.

Синтаксис:

- set nat destination rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]
- delete nat destination rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]
- show nat destination rule <1-999999> packet-type

Аргументы:

- <1-999999> — порядковый номер правила;
- <broadcast> — broadcast-вещание;
- <host> — вещание на локальный хост;

- <multicast> — multicast-вещание;
- <other> — вещание на другой хост.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> protocol <protocol>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает протокол трафика, подлежащего преобразованию.

Синтаксис:

- set nat destination rule <1-999999> protocol <protocol>
- delete nat destination rule <1-999999> protocol <protocol>
- show nat destination rule <1-999999> protocol

Аргументы:

- <1-999999> — порядковый номер правила;
- <protocol> — протокол трафика, который будет преобразован. Доступные протоколы: all, ip, hopopt, icmp, igmp, ggp, ipencap, st, tcp, egp, igp, pup, udp, tcp_udp, hmp, xns-idp, rdp, iso-tp4, dccp, xtp, ddp, idpr-cmtp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, esp, ah, skip, ipv6-icmp, ipv6-nonxt, ipv6-opts, rspf, vmtp, eigrp, ospf, ax.25, ipip, etherip, encap, 99, pim, ipcomp, vrrp, l2tp, isis, sctp, fc, mobility-header, udplite, mpls-in-ip, manet, hip, shim6, wesp, rohc, 0-255.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> source address <address>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве источника IPv4-адрес, который будет преобразован.

Синтаксис:

- set nat destination rule <1-999999> source address <address>
- delete nat destination rule <1-999999> source address <address>
- show nat destination rule <1-999999> source address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv4-адреса источника, который будет преобразован.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> source group address-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве источника группу IPv4-адресов, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> source group address-group <text>
- delete nat destination rule <1-999999> source group address-group <text>
- show nat destination rule <1-999999> source group address-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — группа IPv4-адресов в качестве источника.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> source group domain-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве источника группу доменов, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> source group domain-group <text>
- delete nat destination rule <1-999999> source group domain-group <text>
- show nat destination rule <1-999999> source group domain-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа доменов в качестве источника.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> source group mac-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве источника группу MAC-адресов, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> source group mac-group <text>
- delete nat destination rule <1-999999> source group mac-group <text>
- show nat destination rule <1-999999> source group mac-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа MAC-адресов в качестве источника.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> source group network-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве источника группу подсетей, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> source group network-group <text>
- delete nat destination rule <1-999999> source group network-group <text>
- show nat destination rule <1-999999> source group network-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа подсетей в качестве источника.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> source group port-group <text>

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве источника группу портов, которые будут преобразованы.

Синтаксис:

- set nat destination rule <1-999999> source group port-group <text>
- delete nat destination rule <1-999999> source group port-group <text>
- sho nat destination rule <1-999999> source group port-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа портов в качестве источника.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> source port [<text> | <1-65535> | <start-end> | <none>]

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает в качестве источника порт, который будет преобразован.

Синтаксис:

- set nat destination rule <1-999999> source port [<text> | <1-65535> | <start-end> | <none>]
- delete nat destination rule <1-999999> source port [<text> | <1-65535> | <start-end> | <none>]
- show nat destination rule <1-999999> source port

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя порта источника, указанное в директории /etc/services;
- <1-65535> — номер порта источника. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон из портов источника. Диапазон значений: от 1 до 65535. Пример: 1001-1005;
- <none> — выключает преобразование порта источника.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> translation address [<address> | <CIDR> | <addressrange>]

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает целевой адрес преобразования или диапазон адресов. NAT будет преобразовывать в указанный адрес.

Синтаксис:

- set nat destination rule <1-999999> translation address [<address> | <CIDR> | <addressrange>]
- delete nat destination rule <1-999999> translation address [<address> | <CIDR> | <addressrange>]
- show nat destination rule <1-999999> translation address

Аргументы:

- <1-999999> — порядковый номер правила;

- <address> — целевой адрес преобразования;
- <CIDR> — диапазон целевых адресов преобразования с префиксом подсети. Формат: x.x.x.x/x;
- <addressrange> — диапазон целевых адресов преобразования.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> translation options address-mapping [persistent | random]

Описание:

Создает правило преобразования NAT44 для входящего трафика и задает способ отображения адресов.

Синтаксис:

- set nat destination rule <1-999999> translation options address-mapping [persistent | random]
- delete nat destination rule <1-999999> translation options address-mapping [persistent | random]
- show nat destination rule <1-999999> translation options address-mapping

Аргументы:

- <1-999999> — порядковый номер правила;
- <persistent> — NAT будет преобразовывать адреса входящего трафика в один и тот же целевой адрес на протяжении всей сессии соединения;
- <random> — NAT будет выбирать целевой адрес преобразования в случайном порядке из списка адресов, доступных для преобразования.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> translation options port-mapping [<random> | <none>]

Описание:

Создает правило преобразования NAT44 для входящего трафика и задает способ отображения портов.

Синтаксис:

- set nat destination rule <1-999999> translation options port-mapping [<random> | <none>]
- delete nat destination rule <1-999999> translation options port-mapping [<random> | <none>]
- show nat destination rule <1-999999> translation options port-mapping

Аргументы:

- <1-999999> — порядковый номер правила;
- <random> — NAT будет выбирать целевой адрес преобразования в случайном порядке из списка адресов, доступных для преобразования;

- <none> — выключает отображение портов. Значение по умолчанию.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> translation port [<1-65535> | <start-end>]

Описание:

Создает правило преобразования NAT44 для входящего трафика и указывает целевой порт преобразования.

Синтаксис:

- set nat destination rule <1-999999> translation port [<1-65535> | <start-end>]
- delete nat destination rule <1-999999> translation port [<1-65535> | <start-end>]
- show nat destination rule <1-999999> translation port

Аргументы:

- <1-999999> — порядковый номер правила;
- <1-65535> — номер целевого порта преобразования. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон из целевых портов преобразования. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

---

nat destination rule <1-999999> translation redirect port [<1-65535> | <start-end>]

Описание:

Создает правило преобразования NAT44 для входящего трафика и перенаправляет трафик с одного целевого порта на другой.

Синтаксис:

- set nat destination rule <1-999999> translation redirect port [<1-65535> | <start-end>]
- delete nat destination rule <1-999999> translation redirect port [<1-65535> | <start-end>]
- show nat destination rule <1-999999> translation redirect port

Аргументы:

- <1-999999> — порядковый номер правила;
- <1-65535> — номер целевого порта преобразования, на который будет перенаправлен трафки. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон из целевых портов преобразования, на которые будет перенаправлен трафик. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

---

nat source rule <1-999999> description <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и добавляет описание.

Синтаксис:

- set nat source rule <1-999999> description <text>
- delete nat source rule <1-999999> description <text>
- show nat source rule <1-999999> description

Аргументы:

<1-999999> — порядковый номер правила; <text> — описание.

Режим: «Конфигурирование».

---

nat source rule <1-999999> destination address [<address> | <CIDR> | <addressrange>]

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве назначения IPv4-адрес или диапазон, который будет преобразован.

Синтаксис:

- set nat source rule <1-999999> destination address [<address> | <CIDR> | <addressrange>]
- delete nat source rule <1-999999> destination address [<address> | <CIDR> | <addressrange>]
- show nat source rule <1-999999> destination address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес назначения;
- <addressrange> — диапазон из IPv4-адресов источника. Формат: addressrange;
- <CIDR> — диапазон из IPv4-адресов с префиксом подсети. Формат: x.x.x.x/x.

Режим: «Конфигурирование».

---

nat source rule <1-999999> destination group address-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве назначения группу IPv4-адресов, которые будут преобразованы.

Синтаксис:

- set nat source rule destination group address-group <text>
- delete nat source rule <1-999999> destination group address-group <text>
- show nat source rule <1-999999> destination group address-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя группы IPv4-адресов в качестве назначения.

Режим: «Конфигурирование».

---

nat source rule <1-999999> destination group domain-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве назначения группу доменов, которые будут преобразованы.

Синтаксис:

- set nat source rule <1-999999> destination group domain-group <text>
- delete nat source rule <1-999999> destination group domain-group <text>
- show nat source rule <1-999999> destination group domain-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <name> — имя группы доменов в качестве назначения.

Режим: «Конфигурирование».

---

nat source rule <1-999999> destination group mac-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве назначения группу MAC-адресов, которые будут преобразованы.

Синтаксис:

- set nat source rule <1-999999> destination group mac-group <text>
- delete nat source rule <1-999999> destination group mac-group <text>
- show nat source rule <1-999999> destination group mac-group

Аргументы:

- <1-999999> — порядковый номер правила;

- <name> — имя группы MAC-адресов в качестве источника.

Режим: «Конфигурирование».

---

nat source rule <1-999999> destination group network-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве назначения группу подсетей, которые будут преобразованы.

Синтаксис:

- set nat source rule <1-999999> destination group network-group <text>
- delete nat source rule <1-999999> destination group network-group <text>
- show nat source rule <1-999999> destination group network-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя группы подсетей в качестве назначения.

Режим: «Конфигурирование».

---

nat source rule <1-999999> destination group port-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве назначения группу портов, которые будут преобразованы.

Синтаксис:

- set nat source rule <1-999999> destination group port-group <text>
- delete nat source rule <1-999999> destination group port-group <text>
- show nat source rule <1-999999> destination group port-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя группы портов в качестве назначения.

Режим: «Конфигурирование».

---

nat source rule <1-999999> destination port [<text> | <1-65535> | <start-end> | <none>]

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве назначения порт, который будет преобразован.

Синтаксис:

- set nat source rule <1-999999> destination port [<text> | <1-65535> | <start-end> | <none>]
- delete nat source rule <1-999999> destination port [<text> | <1-65535> | <start-end> | <none>]
- show nat source rule <1-999999> destination port

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя порта назначения, указанное в директории /etc/services;
- <1-65535> — номер порта назначения. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон портов назначения. Диапазон значений: от 1 до 65535. Пример: 1001-1005;
- <none> — выключает преобразование порта назначения.

Режим: «Конфигурирование».

---

nat source rule <1-999999> disable

Описание:

Создает правило преобразования NAT44 для исходящего трафика и выключает NAT44.

Синтаксис:

- set nat source rule <1-999999> disable
- delete nat source rule <1-999999> disable
- show nat source rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat source rule <1-999999> exclude

Описание:

Создает правило преобразования NAT44 для исходящего трафика и не применяет преобразование к пакетам, подпадающим под правило.

Синтаксис:

- set nat source rule <1-999999> exclude
- delete nat source rule <1-999999> exclude
- show nat source rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat source rule <1-999999> load-balance backend <address>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает IPv4-адрес устройства, участвующего в распределении разгрузки.

Синтаксис:

- set nat source rule <1-999999> load-balance backend <address>
- delete nat source rule <1-999999> load-balance backend <address>
- show nat source rule <1-999999> load-balance backend

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес устройства, участвующего в распределении разгрузки.

Режим: «Конфигурирование».

---

nat source rule <1-999999> load-balance backend <address> weight <1-100>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает вес устройства с конкретным IPv4-адресом.

Синтаксис:

- set nat source rule <1-999999> load-balance backend <address> weight <1-100>

- delete nat source rule <1-999999> load-balance backend <address> weight <1-100>
- show nat source rule <1-999999> load-balance backend <address>

Аргументы:

- <1-999999> — порядковый номер правила;
- <address>— IPv4-адрес устройства, участвующего в распределении разгрузки;
- <1-100> — вес устройства. Суммарный вес всех устройств должен равняться 100.

Режим: «Конфигурирование».

---

nat source rule <1-999999> load-balance hash source-address

Описание:

Создает правило преобразования NAT44 для исходящего трафика и генерирует хэш на основе IPv4-адреса источника.

Синтаксис:

- set nat source rule <1-999999> load-balance hash source-address
- delete nat source rule <1-999999> load-balance hash source-address
- show nat source rule <1-999999> load-balance hash

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat source rule <1-999999> load-balance hash destination-address

Описание:

Создает правило преобразования NAT44 для исходящего трафика и генерирует хэш на основе IPv4-адреса назначения.

Синтаксис:

- set nat source rule <1-999999> load-balance hash destination-address
- delete nat source rule <1-999999> load-balance hash destination-address
- show nat source rule <1-999999> load-balance hash

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat source rule <1-999999> load-balance hash source-port

Описание:

Создает правило преобразования NAT44 для исходящего трафика и генерирует хэш на основе порта источника.

Синтаксис:

- set nat source rule <1-999999> load-balance hash source-port
- delete nat source rule <1-999999> load-balance hash source-port
- show nat source rule <1-999999> load-balance hash

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat source rule <1-999999> load-balance hash destination-port

Описание:

Создает правило преобразования NAT44 для исходящего трафика и генерирует хэш на основе порта назначения.

Синтаксис:

- set nat source rule <1-999999> load-balance hash destination-port
- delete nat source rule <1-999999> load-balance hash destination-port
- show nat source rule <1-999999> load-balance hash

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat source rule <1-999999> load-balance hash random

Описание:

Создает правило преобразования NAT44 для исходящего трафика и генерирует хэш случайным образом.

Синтаксис:

- set nat source rule <1-999999> load-balance hash random
- delete nat source rule <1-999999> load-balance hash random

- show nat source rule <1-999999> load-balance hash

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat source rule <1-999999> log

Описание:

Создает правило преобразования NAT44 для исходящего трафика и включает журналирование.

Синтаксис:

- set nat source rule <1-999999> log
- delete nat source rule <1-999999> log
- show nat source rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat source rule <1-999999> outbound-interface group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и выбирает группу интерфейсов, через которую трафик исходит с маршрутизатора.

Синтаксис:

- set nat source rule <1-999999> outbound-interface group <text>
- delete nat source rule <1-999999> outbound-interface group <text>
- show nat source rule <1-999999> outbound-interface group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа интерфейсов, через которую трафик исходит с маршрутизатора.

Режим: «Конфигурирование».

---

nat source rule <1-999999> outbound-interface name <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и выбирает интерфейс, через который трафик исходит с маршрутизатора.

Синтаксис:

- set nat source rule <1-999999> outbound-interface name <text>
- delete nat source rule <1-999999> outbound-interface name <text>
- show nat source rule <1-999999> outbound-interface name

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — интерфейс, через который трафик исходит с маршрутизатора.

Режим: «Конфигурирование».

---

nat source rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]

Описание:

Создает правило преобразования NAT44 для исходящего трафика и задает тип вещания для преобразования.

Синтаксис:

- set nat source rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]
- delete source rule <1-999999> packet-type [<broadcast> | <host> | <multicast> | <other>]
- show source rule <1-999999> packet-type

Аргументы:

- <1-999999> — порядковый номер правила;
- <broadcast> — broadcast-вещание;
- <host> — вещание на локальный хост;
- <multicast> — multicast-вещание;
- <other> — вещание на другой хост.

Режим: «Конфигурирование».

---

nat source rule <1-999999> protocol <protocol>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает протокол трафика, подлежащего преобразованию.

Синтаксис:

- set nat source rule <1-999999> protocol <protocol>
- delete nat source rule <1-999999> protocol <protocol>
- show nat source rule <1-999999> protocol

Аргументы:

- <1-999999> — порядковый номер правила;
- <protocol> — протокол трафика, который будет преобразован. Доступные протоколы: all, ip, hopopt, icmp, igmp, ggp, ipencap, st, tcp, egp, igp, pup, udp, tcp_udp, hmp, xns-idp, rdp, iso-tp4, dccp, xtp, ddp, idpr-cmtp, ipv6, ipv6-route, ipv6-frag, idrp, rsvp, gre, esp, ah, skip, ipv6-icmp, ipv6-nonxt, ipv6-opts, rspf, vmtp, eigrp, ospf, ax.25, ipip, etherip, encap, 99, pim, ipcomp, vrrp, l2tp, isis, sctp, fc, mobility-header, udplite, mpls-in-ip, manet, hip, shim6, wesp, rohc, 0-255.

Режим: «Конфигурирование».

---

nat source rule <1-999999> source address [<address> | <CIDR> | <addressrange>]

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве источника IPv4-адрес, который будет преобразован.

Синтаксис:

- set nat source rule <1-999999> source address [<address> | <CIDR> | <addressrange>]
- delete nat source rule <1-999999> source address [<address> | <CIDR> | <addressrange>]
- show nat source rule <1-999999> source address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес источника;
- <CIDR> — диапазон IPv4-адресов с префиксом подсети. Формат: x.x.x.x/x;
- <addressrange> — диапазон целевых адресов преобразования.

Режим: «Конфигурирование».

---

nat source rule <1-999999> source group address-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве источника группу IPv4-адресов, которые будут преобразованы.

Синтаксис:

- set nat source rule <1-999999> source group address-group <text>
- delete nat source rule <1-999999> source group address-group <text>
- show nat source rule <1-999999> source group address-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа IPv4-адресов источника.

Режим: «Конфигурирование».

---

nat source rule <1-999999> source group domain-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве источника группу доменов, которые будут преобразованы.

Синтаксис:

- set nat source rule <1-999999> source group domain-group <text>
- delete nat source rule <1-999999> source group domain-group <text>
- show nat source rule <1-999999> source group domain-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа доменов в качестве источника.

Режим: «Конфигурирование».

---

nat source rule <1-999999> source group mac-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве источника группу MAC-адресов, которые будут преобразованы.

Синтаксис:

- set nat source rule <1-999999> source group mac-group <text>
- delete nat source rule <1-999999> source group mac-group <text>
- show nat source rule <1-999999> source group mac-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа MAC-адресов в качестве источника.

Режим: «Конфигурирование».

---

nat source rule <1-999999> source group network-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве источника группу подсетей, которые будут преобразованы.

Синтаксис:

- set nat source rule <1-999999> source group network-group <text>
- delete nat source rule <1-999999> source group network-group <text>
- show nat source rule <1-999999> source group network-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа подсетей в качестве источника.

Режим: «Конфигурирование».

---

nat source rule <1-999999> source group port-group <text>

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве источника группу портов, которые будут преобразованы.

Синтаксис:

- set nat source rule <1-999999> source group port-group <text>
- delete nat source rule <1-999999> source group port-group <text>
- show nat source rule <1-999999> source group port-group

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — группа портов в качестве источника.

Режим: «Конфигурирование».

---

nat source rule <1-999999> source port [<text> | <1-65535> | <start-end> | <none>]

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает в качестве источника порт, который будет преобразован.

Синтаксис:

- set nat source rule <1-999999> source port [<text> | <1-65535> | <start-end> | <none>]
- delete nat source rule <1-999999> source port [<text> | <1-65535> | <start-end> | <none>]
- show nat source rule <1-999999> source port

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя порта источника, указанное в директории /etc/services;
- <1-65535> — номер порта источника. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон из портов источника. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

---

nat source rule <1-999999> translation address [<address> | <CIDR> | <addressrange> | <masquerade>]

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает целевой адрес преобразования или диапазон адресов. NAT будет преобразовывать в указанный адрес.

Синтаксис:

- set nat source rule <1-999999> translation address [<address> | <CIDR> | <addressrange> | <masquerade>]
- delete nat source rule <1-999999> translation address [<address> | <CIDR> | <addressrange> | <masquerade>]
- show nat source rule <1-999999> translation address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес источника;
- <CIDR> — диапазон целевых адресов преобразования с префиксом подсети. Формат: x.x.x.x/x;

- <addressrange> — диапазон целевых адресов преобразования;
- <masquerade> — целевой адрес будет выбран из списка доступных адресов в NAT таблице.

Режим: «Конфигурирование».

---

nat source rule <1-999999> translation options address-mapping [persistent | random]

Описание:

Создает правило преобразования NAT44 для исходящего трафика и задает способ отображения адресов.

Синтаксис:

- set nat source rule <1-999999> translation options address-mapping [<persistent> | <random>]
- delete nat source rule <1-999999> translation options address-mapping [<persistent> | <random>]
- show nat source rule <1-999999> translation options address-mapping

Аргументы:

- <1-999999> — порядковый номер правила;
- <persistent> — NAT будет преобразовывать адреса входящего трафика в один и тот же целевой адрес на протяжении всей сессии соединения;
- <random> — NAT будет выбирать целевой адрес преобразования в случайном порядке из списка адресов, доступных для преобразования.

Режим: «Конфигурирование».

---

nat source rule <1-999999> translation options port-mapping [<random> | <none>]

Описание:

Создает правило преобразования NAT44 для исходящего трафика и задает способ отображения портов.

Синтаксис:

- set nat source rule <1-999999> translation options port-mapping [<random> | <none>]
- delete nat source rule <1-999999> translation options port-mapping [<random> | <none>]
- show nat source rule <1-999999> translation options port-mapping

Аргументы:

- <random> — NAT будет отображать порты случайными номерами;
- <none> — выключает отображение портов. Значение по умолчанию.

Режим: «Конфигурирование».

---

nat source rule <1-999999> translation port [<1-65535> | <start-end>]

Описание:

Создает правило преобразования NAT44 для исходящего трафика и указывает целевой порт преобразования.

Синтаксис:

- set nat source rule <1-999999> translation port [<1-65535> | <start-end>]
- delete nat source rule <1-999999> translation port [<1-65535> | <start-end>]
- show nat source rule <1-999999> translation port

Аргументы:

- <1-999999> — порядковый номер правила;
- <1-65535> — номер целевого порта преобразования. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон из целевых портов преобразования. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

---

nat static rule <1-999999> description <text>

Описание:

Создает правило для статического преобразования и добавляет описание.

Синтаксис:

- set nat static rule <1-999999> description <text>
- delete nat static rule <1-999999> description <text>
- show nat static rule <1-999999> description

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — описание для правила.

Режим: «Конфигурирование».

---

nat static rule <1-999999> destination address [<address> | <CIDR>]

Описание:

Создает правило для статического преобразования и указывает в качестве назначения IPv4-адрес или диапазон, который будет преобразован.

Синтаксис:

- set nat static rule <1-999999> destination address [<address> | <CIDR>]
- delete nat static rule <1-999999> destination address [<address> | <CIDR>]
- show nat static rule <1-999999> destination address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv4-адрес назначения, который будет преобразован;
- <CIDR> — диапазон IPv4-адресов назначения с префиксом подсети, которые будут преобразованы. Формат: x.x.x.x/x.

Режим: «Конфигурирование».

---

nat static rule <1-999999> inbound-interface [<text> | <any> | <eth0> | <lo>]

Описание:

Создает правило для статического преобразования и выбирает интерфейс, через который трафик поступает на маршрутизатор.

Синтаксис:

- set nat static rule <1-999999> inbound-interface [<text> | <any> | <eth0> | <lo>]
- delete nat static rule <1-999999> inbound-interface [<text> | <any> | <eth0> | <lo>]
- show nat static rule <1-999999> inbound-interface

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя конкретного интерфейса, через который трафик поступает на маршрутизатор;
- <any> — любой доступный интерфейс, через который трафик поступает на маршрутизатор;
- <eth0> — интерфейс eth0;
- <lo> — интерфейс Loopback.

Режим: «Конфигурирование».

---

nat static rule <1-999999> log

Описание:

Создает правило для статического преобразования и включает журналирование.

Синтаксис:

- set nat static rule <1-999999> log

- delete nat static rule <1-999999> log
- show nat static rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat static translation address [<address> | <CIDR>]

Описание:

Создает правило для статического преобразования и указывает целевой адрес преобразования или диапазон адресов.

Синтаксис:

- set nat static translation address [<address> | <CIDR>]
- delete nat static translation address [<address> | <CIDR>]
- show nat static translation address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — целевой IPv4-адрес преобразования;
- <CIDR> — диапазон целевых адресов преобразования с префиксом подсети. Формат: x.x.x.x/x.

Режим: «Конфигурирование».

Режим «Администрирование»

show nat destination rules

Описание:

Отображает активные правила на входящем направлении NAT.

Синтаксис:

show nat destination rules

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show nat destination statistics

Описание:

Отображает статистику по активным правилам на входящем направлении NAT.

Синтаксис:

show nat destination statistics

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show nat destination translations address <address>

Описание:

Отображает активную конфигурацию для указанного целевого адреса преобразования на входящем направлении NAT.

Синтаксис:

show nat destination translations address `<address>`

Аргументы:

- `<address>` — целевой адрес преобразования.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show nat source rules

Описание:

Отображает активные правила на исходящем направлении NAT.

Синтаксис:

show nat source rules

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show nat source statistics

Описание:

Отображает статистику по активным правилам на исходящем направлении NAT.

Синтаксис:

show nat source statistics

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show nat source translations address <address>

Описание:

Отображает активную конфигурацию для указанного целевого адреса преобразования на исходящем направлении NAT.

Синтаксис:

show nat source translations address <address>

Аргументы:

- <address> — целевой адрес преобразования.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

Настройка NAT64

Обзор

Технология NAT64 преобразует внутренний IPv6-адрес во внешний IPv4.

Чтобы включить и настроить механизм преобразования NAT64, используйте правила. Каждое правило состоит из *порядкового номера* и *классификатора*.

Чтобы маршрутизатор начал обрабатывать правило, ему необходимо присвоить *порядковый номер* от 1 до 999999. Маршрутизатор считывает правила по порядку, т.е. срабатывает первое подошедшее правило и соблюдается последовательность. Если присвоить правилам одинаковые номера, то они будут сгруппированы и объединены в логическую *цепочку*. Маршрутизатор будет воспринимать такую цепочку как единое целое. Чтобы изменить номер правила, используйте команду *rename*, для копирования — *copy*.

Примечание

Все новые изменения применятся к будущим соединениям. Ранее установленные соединения затронуты не будут.

Каждое правило имеет уникальный *классификатор* — признак, по которому будет проходить фильтрация. Классификатором может быть интерфейс, протокол, тип преобразования, исходный адрес и т.д. Перечислить значения можно через запятую. Чтобы инвертировать список значений, используйте символ «!».

Список команд

Режим «Конфигурирование»

nat64 source rule <1-999999> description <text>

Описание:

Создает правило преобразования NAT64 для исходящего трафика и добавляет описание.

Синтаксис:

- set nat64 source rule <1-999999> description <text>
- delete nat64 source rule <1-999999> description <text>
- show nat64 source rule <1-999999> description

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — описание правила.

Режим: «Конфигурирование».

nat64 source rule <1-999999> disable

Описание:

Создает правило преобразования NAT64 для исходящего трафика и выключает NAT64.

Синтаксис:

- set nat64 source rule <1-999999> disable
- delete nat64 source rule <1-999999> disable
- show nat64 source rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat64 source rule <1-999999> match mark <1-2147483647>

Описание:

Создает правило преобразования NAT64 для исходящего трафика и преобразует трафик, который соответствует метке соединения fwmark.

Синтаксис:

- set nat64 source rule <1-999999> match mark <1-2147483647>
- delete nat64 source rule <1-999999> match mark <1-2147483647>
- show nat64 source rule <1-999999> match mark

Аргументы:

- <1-999999> — порядковый номер правила;
- <1-2147483647> — числовая метка соединения fwmark.

Режим: «Конфигурирование».

---

nat64 source rule <1-999999> source prefix <h:h:h:h:h:h:h:h:/x>

Описание:

Создает правило преобразования NAT64 для исходящего трафика и указывает в качестве источника префикс IPv6-адреса, который будет преобразован.

Синтаксис:

- set nat64 source rule <1-999999> source prefix <h:h:h:h:h:h:h:h:/x>
- delete nat64 source rule <1-999999> source prefix <h:h:h:h:h:h:h:h:/x>
- show nat64 source rule <1-999999> source prefix

Аргументы:

- <1-999999> — порядковый номер правила;
- <h:h:h:h:h:h:h:h:/x> — префикс IPv6-адреса, который будет преобразован.

Режим: «Конфигурирование».

---

nat64 source rule <1-999999> translation pool <1-999999> address [<address> | <CIDR>]

Описание:

Создает правило преобразования NAT64 для исходящего трафика, присваивает номер пулу целевых IPv4-адресов преобразования и указывает IPv4-адрес преобразования или диапазон адресов.

Синтаксис:

- set nat64 source rule <1-999999> translation pool <1-999999> address [<address> | <CIDR>]
- delete nat64 source rule <1-999999> translation pool <1-999999> address [<address> | <CIDR>]
- show nat64 source rule <1-999999> translation pool <1-999999> address

Аргументы:

- <1-999999> — порядковый номер правила;
- <1-999999> — номер пула целевых IPv4-адресов;
- <address> — целевой IPv4-адрес преобразования;
- <CIDR> — диапазон целевых IPv4-адресов преобразования с префиксом подсети. Формат: x.x.x.x/x.

Режим: «Конфигурирование».

---

nat64 source rule <1-999999> translation pool <1-999999> description <text>

Описание:

Создает правило преобразования NAT64 для исходящего трафика, присваивает номер пулу целевых адресов преобразования и добавляет описание.

Синтаксис:

- set nat64 source rule <1-999999> translation pool <1-999999> description <text>
- delete nat64 source rule <1-999999> translation pool <1-999999> description <text>

- show nat64 source rule <1-999999> translation pool <1-999999> description

Аргументы:

- <1-999999> — порядковый номер правила;
- <1-999999> — номер пула целевых IPv4-адресов;
- <text> — описание пула целевых IPv4-адресов преобразования.

Режим: «Конфигурирование».

---

nat64 source rule <1-999999> translation pool <1-999999> disable

Описание:

Создает правило преобразования NAT64 для исходящего трафика, присваивает номер пулу целевых адресов преобразования и выключает NAT64.

Синтаксис:

- set nat64 source rule <1-999999> translation pool <1-999999> disable
- delete nat64 source rule <1-999999> translation pool <1-999999> disable
- show nat64 source rule <1-999999> translation pool <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила;
- <1-999999> — номер пула целевых IPv4-адресов.

Режим: «Конфигурирование».

---

nat64 source rule <1-999999> translation pool <1-999999> port [<1-65535> | <start-end>]

Описание:

Создает правило преобразования NAT64 для исходящего трафика, присваивает номер пулу целевых адресов преобразования и указывает целевой порт преобразования.

Синтаксис:

- set nat64 source rule <1-999999> translation pool <1-999999> port [<1-65535> | <start-end>]
- delete nat64 source rule <1-999999> translation pool <1-999999> port [<1-65535> | <start-end>]
- show nat64 source rule <1-999999> translation pool <1-999999> port

Аргументы:

- <1-999999> — порядковый номер правила;

- <1-999999> — номер пула целевых IPv4-адресов;
- <1-65535> — целевой порт преобразования. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон целевых портов преобразований.

Режим: «Конфигурирование».

---

nat64 source rule <1-999999> translation pool <1-999999> protocol [<icmp> | <tcp> | <udp>]

Описание:

Создает правило преобразования NAT64 для исходящего трафика, присваивает номер пулу целевых адресов преобразования и указывает протокол трафика, подлежащего преобразованию.

Синтаксис:

- set nat64 source rule <1-999999> translation pool <1-999999> protocol [<icmp> | <tcp> | <udp>]
- delete nat64 source rule <1-999999> translation pool <1-999999> protocol [<icmp> | <tcp> | <udp>]
- show nat64 source rule <1-999999> translation pool <1-999999> protocol

Аргументы:

- <1-999999> — порядковый номер правила;
- <1-999999> — номер пула целевых IPv4-адресов;
- <icmp> — протокол ICMP;
- <tcp> — протокол TCP;
- <udp> — протокол UDP.

Режим: «Конфигурирование».

Настройка NAT66

Обзор

Технология NAT66 преобразует внутренний IPv6-адрес во внешний IPv6.

Чтобы включить и настроить механизм преобразования NAT66, используйте правила. Каждое правило состоит из *порядкового номера* и *классификатора*.

Чтобы маршрутизатор начал обрабатывать правило, ему необходимо присвоить *порядковый номер* от 1 до 999999. Маршрутизатор считывает правила по порядку, т.е. срабатывает первое подошедшее правило и соблюдается последовательность. Если присвоить правилам одинаковые номера, то они будут сгруппированы и объединены в логическую *цепочку*. Маршрутизатор будет воспринимать такую цепочку как единое целое. Чтобы изменить номер правила, используйте команду *rename*, для копирования — *copy*.

Примечание

Все новые изменения применятся к будущим соединениям. Ранее установленные соединения затронуты не будут.

Каждое правило имеет уникальный *классификатор* — признак, по которому будет проходить фильтрация. Классификатором может быть интерфейс, протокол, тип преобразования, исходный и т.д. Перечислить значения можно через запятую. Чтобы инвертировать список значений, используйте символ «!».

Список команд

Режим «Конфигурирование»

nat66 destination rule <1-999999> description <text>

Описание:

Создает правило преобразования NAT66 для входящего трафика и добавляет описание.

Синтаксис:

- set nat66 destination rule <1-999999> description <text>
- delete nat66 destination rule <1-999999> description <text>
- show nat66 destination rule <1-999999> description

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — описание правила.

Режим: «Конфигурирование».

nat66 destination rule <1-999999> destination address [<address> | <CIDR>]

Описание:

Создает правило преобразования NAT66 для входящего трафика и указывает в качестве назначения IPv6-адрес или диапазон, который будет преобразован.

Синтаксис:

- set nat66 destination rule <1-999999> destination address [<address> | <CIDR> | <addressrange>]
- delete nat66 destination rule <1-999999> destination address [<address> | <CIDR> | <addressrange>]
- show nat66 destination rule <1-999999> destination address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv6-адрес назначения. Формат: h.h.h.h.h.h.h.h;
- <CIDR> — диапазон из IPv6-адресов назначения с префиксом подсети. Формат CIDR: h.h.h.h.h.h.h.h/x.

Режим: «Конфигурирование».

---

nat66 destination rule <1-999999> destination port [<text> | <1-65535> | <start-end> | <none>]

Описание:

Создает правило преобразования NAT66 для входящего трафика и указывает в качестве назначения порт, который будет преобразован.

Синтаксис:

- set nat66 destination rule <1-999999> destination port [<text> | <1-65535> | <start-end> | <none>]
- delete nat66 destination rule <1-999999> destination port [<text> | <1-65535> | <start-end> | <none>]
- show nat66 destination rule <1-999999> destination port

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя порта назначения, указанное в директории /etc/services;
- <1-65535> — номер порта назначения. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон портов назначения. Диапазон значений: от 1 до 65535. Пример: 1001-1005;
- <none> — выключает преобразование порта назначения.

Режим: «Конфигурирование».

---

nat66 destination rule <1-999999> disable

Описание:

Создает правило преобразования NAT66 для входящего трафика и выключает NAT66.

Синтаксис:

- set nat66 destination rule <1-999999> disable
- delete nat66 destination rule <1-999999> disable
- show nat66 destination rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правила.

Режим: «Конфигурирование».

---

nat66 destination rule <1-999999> exclude

Описание:

Создает правило преобразования NAT66 для входящего трафика и не применяет преобразование к пакетам, подпадающим под правило.

Синтаксис:

- set nat66 destination rule <1-999999> exclude
- delete nat66 destination rule <1-999999> exclude
- show nat66 destination rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правил.

Режим: «Конфигурирование».

---

nat66 destination rule <1-999999> inbound-interface name <iface>

Описание:

Создает правило преобразования NAT66 для входящего трафика и выбирает интерфейс, через который трафик поступает на маршрутизатор.

Синтаксис:

- set nat66 destination rule <1-999999> inbound-interface name <iface>
- delete nat66 destination rule <1-999999> inbound-interface name <iface>
- show nat66 destination rule <1-999999> inbound-interface name

Аргументы:

- <1-999999> — порядковый номер правил;
- <iface> — интерфейс, через который трафик поступает на межсетевой экран. Используйте подстановочный знак «*», чтобы отобразить любой последующий набор символов в названии.

Режим: «Конфигурирование».

---

nat66 destination rule <1-999999> log

Описание:

Создает правило преобразования NAT66 для входящего трафика и включает журналирование.

Синтаксис:

- set nat66 destination rule <1-999999> log
- delete nat66 destination rule <1-999999> log
- show nat66 destination rule <1-999999>

Аргументы:

- <1-999999> — порядковый номер правил.

Режим: «Конфигурирование».

---

nat66 destination rule <1-999999> protocol <protocol>

Описание:

Создает правило преобразования NAT66 для входящего трафика и указывает протокол трафика, подлежащего преобразованию.

Синтаксис:

- set nat66 destination rule <1-999999> protocol <protocol>
- delete nat66 destination rule <1-999999> protocol <protocol>
- show nat66 destination rule <1-999999> protocol

Аргументы:

- <1-999999> — порядковый номер правила;
- <protocol> — протокол трафика, который будет преобразован. Доступные протоколы: all, tcp_udp, 0-255, ah, ax.25, dccp, ddp, egp, eigrp, encap, esp, etherip, ethernet, fc, ggp, gre, hip, hmp,

hopopt, icmp, idpr-cmtp, idrp, igmp, igp, ip, ipcomp, ipencap, ipip, ipv6, ipv6-frag, ipv6-icmp, ipv6-nonxt, ipv6-opts, ipv6-route, isis, iso-tp4, l2tp, manet, mobility-header, mpls-in-ip, mptcp, ospf, pim, pup, rdp, rohc, rspf, rsvp, sctp, shim6, skip, st, tcp, udp, udplite, vmtp, vrrp, wesp, xns-idp, xtp.

Режим: «Конфигурирование».

---

nat66 destination rule <1-999999> source address [<address> | <CIDR>]

Описание:

Создает правило преобразования NAT66 для входящего трафика и указывает в качестве источника IPv6-адрес, который будет преобразован.

Синтаксис:

- set nat66 destination rule <1-999999> source address [<address> | <CIDR>]
- delete nat66 destination rule <1-999999> source address [<address> | <CIDR>]
- show nat66 destination rule <1-999999> source address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv6-адрес в качестве источника. Формат: h:h:h:h:h:h:h:h;
- <CIDR> — диапазон IPv6-адресов с префиксом подсети. Формат CIDR: h:h:h:h:h:h:h:h/x.

Режим: «Конфигурирование».

---

nat66 destination rule <1-999999> source port [<text> | <1-65535> | <start-end> | <none>]

Описание:

Создает правило преобразования NAT66 для входящего трафика и указывает в качестве источника порт, который будет преобразован.

Синтаксис:

- set nat66 destination rule <1-999999> source port [<text> | <1-65535> | <start-end> | <none>]
- delete nat66 destination rule <1-999999> source port [<text> | <1-65535> | <start-end> | <none>]
- show nat66 destination rule <1-999999> source port

Аргументы:

- <1-999999> — порядковый номер правила;
- <text> — имя порта источника, указанное в директории /etc/services;
- <1-65535> — номер порта источника. Диапазон значений: от 1 до 65535;

- <start-end> — диапазон из портов источника. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

---

set nat66 destination rule <1-999999> translation address [<address> | <CIDR>]

Описание:

Создает правило преобразования NAT66 для входящего трафика и указывает целевой адрес преобразования или диапазон адресов. NAT будет преобразовывать в указанный адрес.

Синтаксис:

- set nat66 destination rule <1-999999> translation address [<address> | <CIDR>]
- delete nat66 destination rule <1-999999> translation address [<address> | <CIDR>]
- show nat66 destination rule <1-999999> translation address

Аргументы:

- <1-999999> — порядковый номер правила;
- <address> — IPv6-адрес в качестве источника. Формат: h:h:h:h:h:h:h:h;
- <CIDR> — диапазон IPv6-адресов с префиксом подсети. Формат: h:h:h:h:h:h:h:h/x.

Режим: «Конфигурирование».

---

nat66 destination rule <1-999999> translation port [<1-65535> | <start-end>]

Описание:

Создает правило преобразования NAT66 для входящего трафика и указывает целевой порт преобразования.

Синтаксис:

- set nat66 destination rule <1-999999> translation port [<1-65535> | <start-end>]
- delete nat66 destination rule <1-999999> translation port [<1-65535> | <start-end>]
- show nat66 destination rule <1-999999> translation port

Аргументы:

- <1-999999> — порядковый номер правила;
- <1-65535> — номер целевого порта преобразования. Диапазон значений: от 1 до 65535;
- <start-end> — диапазон из целевых портов преобразования. Диапазон значений: от 1 до 65535. Пример: 1001-1005.

Режим: «Конфигурирование».

2.6 Приоритизация трафика (QoS)

Понятие QoS (Quality of Service) включает, как правило, шейпинг (ограничение и распределение пропускной способности) трафика, распределение пакетов по очередям или их отбрасывание, которые необходимы, например, для устранения узких мест в канале путем установления более высокого приоритета для определенного класса трафика перед другим классом.

2.6.1 Общие принципы работы

Для того, чтобы механизм QoS в составе **ПО Факел** функционировал корректно, необходимо выполнить следующие шаги:

- создать политику обработки трафика;
- применить политику обработки трафика к входящему или исходящему интерфейсу.

Перед изучением возможностей настройки политики, необходимо разобраться с единицами измерения трафика, а также с понятием класса трафика.

2.6.1.1 Единицы измерения

При настройке политики обработки трафика необходимо задавать скорость передачи данных. При этом следует выбирать корректные единицы измерения для соответствия фактического результата работы ожидаемому. **ПО Факел** оперирует различными префиксами и суффиксами единиц измерения, описание которых представлено в разделах ниже.

Префиксы

Префиксы могут указываться как в *десятичном* в формате, так и в *двоичном* формате.

```
kbit  (10^3)      kilobit per second
mbit  (10^6)      megabit per second
gbit  (10^9)      gigabit per second
tbit  (10^12)     terabit per second

kbps  (8*10^3)    kilobyte per second
mbps  (8*10^6)    megabyte per second
gbps  (8*10^9)    gigabyte per second
tbps  (8*10^12)   terabyte per second
```

```
 kibit (2^10 = 1024)     kibibit per second
 mibit (2^20 = 1024^2)   mebibit per second
 gibit (2^30 = 1024^3)   gibibit per second
tbit  (2^40 = 1024^4)   tebibit per second

 kibps (1024*8)          kibibyte (KiB) per second
 mibps (1024^2*8)        mebibyte (MiB) per second
gibps (1024^3*8)        gibibyte (GiB) per second
tibps (1024^4*8)        tebibyte (TiB) per second
```

Суффиксы

Суффиксы могут указываться как в единицах *бит* (для краткого обозначения используется `bit`), так и в единицах *байт* (для обозначения используется `b`).

```
kbit (kilobits per second)
mbit (megabits per second)
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
gbit (gigabits per second)
 tbit (terabits per second)
```

```
kbps (kilobytes per second)
mbps (megabytes per second)
gbps (gigabytes per second)
```

2.6.1.2 Классы

Политики QOS позволяют классифицировать трафик в соответствии с заданными параметрами. Таким образом, класс - это определенный тип трафика, который можно указывать в политике.

В общем случае классификация трафика выполняется для обеспечения корректной его обработки.

Классификация трафика

Для того чтобы определить, какой трафик ассоциируется с тем или иным классом, определяются критерии соответствия (классификатор). Пакет ассоциируется с определенным классом в том случае, если обнаруживается правило с подходящим классификатором (аналогично тому, как функционирует межсетевой экран).

Каждый класс обладает числовым идентификатором, который задается при его настройке.

Примечание

Необходимо понимать, что назначение одного и того же идентификатора класса может быть разным для разных типов политики обработки трафика. Обычно при задании политики требуется указать числовой идентификатор класса, значение которого само по себе не несет никакого смысла, однако это не является обязательным условием для всех политик. Числовой идентификатор класса в очереди определенного приоритета не только идентифицирует сам класс, но также определяет приоритет.

```
set traffic-policy <policy> <policy-name> class <class-ID> match
 <class-matching-rule-name>
```

В приведенной выше команде мы задаем тип политики, с которой будем работать, и выбранное для нее имя; класс (чтобы можно было различать некоторый трафик) и идентифицируемый номер для этого класса; затем мы настраиваем правило соответствия (или фильтр) и имя для него.

В представленной выше команде задается тип политики обработки трафика, имя, класс (для дифференциации определенного трафика) и идентификатор данного класса. Затем для правила задается классификатор и имя правила.

Класс может иметь несколько классификаторов.

```
set traffic-policy shaper MY-SHAPER class 30 match HTTP
set traffic-policy shaper MY-SHAPER class 30 match HTTPs
```

Классификатор может содержать множественные критерии соответствия, а трафик будет считаться по-

дошедшим, если подходят все заданные критерии одновременно.

Пример:

```
set traffic-policy shaper MY-SHAPER class 30 match HTTP ip protocol tcp
set traffic-policy shaper MY-SHAPER class 30 match HTTP ip source port 80
```

В данном примере показано задание классификатора для трафика по протоколу TCP с номером порта отправителя 80.

При задании классификатора доступны следующие параметры, определяющие подходящий трафик:

- интерфейс (имя интерфейса);
- протокол Ethernet (номер протокола, MAC адрес отправителя, MAC адрес получателя);
- протокол IPv4 (метка DSCP, максимальная длина пакета, номер протокола, IP адрес отправителя, IP адрес получателя, номер порта отправителя, номер порта получателя, флаги TCP);
- протокол IPv6 (метка DSCP, максимальная длина тела пакета, номер протокола, IP адрес отправителя, IP адрес получателя, номер порта отправителя, номер порта получателя, флаги TCP);
- метка межсетевого экрана;
- идентификатор VLAN (VLAN ID).

При задании классификатора можно использовать клавишу Tab для вывода на экран информации о доступных для использования параметрах.

```
fakel@fakel# set traffic-policy shaper MY-SHAPER class 30 match MY-FIRST-FILTER
Possible completions:
   description  Description for this match
>  ether        Ethernet header match
   interface    Interface name for this match
>  ip           Match IP protocol header
>  ipv6         Match IPV6 header
   mark         Match on mark applied by firewall
   vif          Virtual Local Area Network (VLAN) ID for this match
```

Для классификатора также можно указать текстовое описание.

```
set traffic-policy shaper MY-SHAPER class 30 match MY-FIRST-FILTER description ”My
  filter description”
```

Примечание

Классификатору с указанными параметрами протокола IPv4 (например, по протоколу TCP) будут соответствовать IPv4 пакеты с заголовком длиной 20 байт, которые, как правило, составляют большую часть трафика IPv4.

Примечание

Классификатору с указанными параметрами протокола IPv6 будут соответствовать IPv6 пакеты без расширения заголовка.

Класс по умолчанию

Довольно часто возникает необходимость конфигурирования обработки трафика по умолчанию. Такому трафику может соответствовать и класс по умолчанию в силу характера обработки трафика. К классу по умолчанию относится любой трафик, который невозможно отнести ни к одному из других определенных классов, поэтому можно сказать, что данный класс - открытый, то есть он является классом, для которого явно не задан ни один из классификаторов.

2.6.1.3 Действие над трафиком

После того как для класса настроен фильтр, необходимо также определить, что делать с трафиком этого класса, какой специфический режим обработки трафика ему назначить.

```
fakel@fakel# set traffic-policy shaper MY-SHAPER class 30
Possible completions:
   bandwidth      Bandwidth used for this class
   burst          Burst size for this class (default: 15kb)
   ceiling        Bandwidth limit for this class
   codel-quantum  fq-codel - Number of bytes used as 'deficit' (default 1514)
   description    Description for this traffic class
   flows          fq-codel - Number of flows (default 1024)
   interval       fq-codel - Interval (milliseconds) used to measure the delay
  (default 100)
+> match          Class matching rule name
   priority       Priority for usage of excess bandwidth
   queue-limit    Maximum queue size (packets)
   queue-type     Queue type for this class
   set-dscp       Change the Differentiated Services (DiffServ) field in the IP
  header
   target         fq-codel - Acceptable minimum queue delay (milliseconds)
```

Например, с помощью команды `set traffic-policy shaper MY-SHAPER class 30 set-dscp EF` можно изменить значение метки DSCP для пакетов данного класса на *Expedite Forwarding*.

Допустимые значения для метки DSCP описаны в спецификациях **RFC 2474**[63] и **RFC 4595**[64].

[63] https://datatracker.ietf.org/doc/html/rfc2474.html
[64] https://datatracker.ietf.org/doc/html/rfc4595.html

Двоичное значение	Десятичное значение	Коэффициент отбрасывания	Описание
000000	0	–	Best Effort
001010	10	Низкий	Assured Forwarding (AF) 11
001100	12	Средний	Assured Forwarding (AF) 12
001110	14	Высокий	Assured Forwarding (AF) 13
010010	18	Низкий	Assured Forwarding (AF) 21
010100	20	Средний	Assured Forwarding (AF) 22
010110	22	Высокий	Assured Forwarding (AF) 23
011010	26	Низкий	Assured Forwarding (AF) 31
011100	28	Средний	Assured Forwarding (AF) 32
011110	30	Высокий	Assured Forwarding (AF) 33
100010	34	Низкий	Assured Forwarding (AF) 41
100100	36	Средний	Assured Forwarding (AF) 42
100110	38	Высокий	Assured Forwarding (AF) 43
101110	46	–	Expedited forwarding (EF)

2.6.1.4 Встраивание политики

Часто возникает необходимость встроить одну политику в другую. То же самое можно сделать и в отношение политик обработки трафика, привязывая новую политику к определенному классу. Например, можно применить разные политики к разным классам сконфигурированной ранее политики **Round Robin**.

Типовым примером встраивания является применение ряда политик к интерфейсу, который является узким местом в контексте проходящего через него трафика. Если же маршрутизатор не подключен непосредственно к узкому месту, а находится за несколько узлов от него, то можно выполнить эмуляцию узкого место, встроив политику без шейпинга, в политику с шейпингом на основе классов, чтобы она начала действовать.

Привязать политику обработки трафика к классу можно с помощью параметра `queue-type`.

```
set traffic-policy shaper FQ-SHAPER bandwidth 4gbit
set traffic-policy shaper FQ-SHAPER default bandwidth 100%
set traffic-policy shaper FQ-SHAPER default queue-type fq-codel
```

Из примера выше видно, что параметр `queue-type` допускает различные комбинации. Также его можно использовать в нескольких политиках.

Примечание

Некоторые политики уже содержат внутри себя другие встроенные политики. Такой политикой является политика «Shaper», каждый из классов которой использует политику **FQ-CoDel** до тех пор, пока она не будет переопределена.

2.6.2 Создание политики обработки трафика

ПО Факел позволяет обрабатывать трафик различными способами:

- *Политика Drop Tail* (страница 641)
- *Политика Fair Queue* (страница 642)
- *Политика FQ-CoDel* (страница 644)
- *Политика Limiter* (страница 646)
- *Политика Network Emulator* (страница 648)
- *Политика Priority Queue* (страница 649)
- *Политика Random Detect* (страница 651)
- *Политика Rate Control* (страница 654)
- *Политика Round Robin* (страница 655)
- *Политика Shaper* (страница 657)

Можно настроить любое количество политик, но для каждого интерфейса, входящего или исходящего с учетом направления трафика, можно применить только одну политику.

Некоторые политики обработки трафика могут быть объединены с помощью встраивания, после чего встроенная политика будет применена к классу трафика, соответствующему основной политике.

Подсказка

Если необходимо выбрать политику для исходящего трафика, но при этом нет понимания, какая именно политика необходима в конкретном случае, скорее всего стоит остановить выбор на политике **Shaper**, оставив по умолчанию встроенную в ее очереди политику **FQ-CoDel**.

2.6.2.1 Политика Drop Tail

Описание

Дисциплина очередей: First In First Out (FIFO).

Применяется к: исходящему трафику.

Очереди политики **Drop Tail** - самый простой вариант реализации, который можно применить к трафику. Перед отправкой трафик должен пройти через конечную очередь. Необходимо определить, сколько пакетов должна содержать конечная очередь.

Перед отправкой пакет должен пройти через конечную очередь, поэтому он перемещается на последнюю позицию в очереди. Когда пакет полностью пройдет через очередь, он покинет ее, освободив место, и в конечном итоге будет передан сетевой карте для отправки.

Несмотря на то, что политика **Drop Tail** не замедляет передачу пакетов, при большом их количестве часть из них может быть отброшена при поступлении на последнюю позицию очереди. Это может произойти, если в очереди нет достаточного количества свободных места из-за того, что пакеты занимают первые позиции в очереди.

Данная политика требует наименьших ресурсов при одном и том же объеме трафика, но используется крайне редко из-за наименьшей пользы от нее при обработке трафика.

Список команд

Основные настройки

- `set traffic-policy drop-tail <policy-name> queue-limit <number-of-packets>`

  Создает политику фильтрации трафика типа **Drop Tail**. Необходимо указать уникальное имя для данной политики, а также - размер очереди, то есть количество пакетов, которое она может содержать (максимальный размер - 4294967295).

2.6.2.2 Политика Fair Queue

Описание

Дисциплина очередей: Stochastic Fairness Queuing (SFQ).

Применяется к: исходящему трафику.

Политика **Fair Queue** подразумевает использование планировщика пакетов, который распределяет пакеты по очередям на основе потоков, то есть балансирует трафик в равной степени между дочерними очередями, чтобы пакеты из каждого потока отправлялись строго по очереди, не позволяя таким образом одному потоку преобладать над другими.

Для распределения трафика по очередям политика **Fair Queue** использует классификатор, основанный на адресе отправителя, адресе получателя и номере порта отправителя. Алгоритм распределения использует специальные хэш-корзины. Каждый пакет должен принадлежать уникальному потоку. Поскольку несколько потоков могут попасть в одну и ту же хэш-корзину, алгоритм хэширования задействуется через настраиваемые интервалы времени времени, поэтому преобладание одного потока над другим возможно, но только в течение некоторого времени. Однако при использовании алгоритма хэширования возможно переупорядочение пакетов. Рекомендуемое значение временного интервала составляет 10 секунд.

Один из вариантов использования политики **Fair Queue** - снижение эффективности атак типа DoS (Denial of Service).

Список команд

Основные настройки

- `set traffic-policy fair-queue <policy-name>`

  Задает уникальное имя для политики фильтрации трафика типа **Fair Queue**.

- `set traffic-policy fair-queue <policy-name> hash-interval <seconds>`\`

  Задает время в секундах, через которое будет задействован алгоритм хэширования (максимальное время - 4294967295).

Примечание

При завершении очереди каждая хэш-корзина с данными используется в кольцевом порядке следования. Можно также сконфигурировать длину очереди.

- `set traffic-policy fair-queue <policy-name> queue-limit <limit>`

  Задает максимальное количество пакетов, ожидающих обработки в очереди. Любые другие пакеты будут отброшены.

Примечание

Политика **Fair Queue** - политика без шейпинга, поэтому она будет полезна только в случае, если исходящий интерфейс действительно перегружается трафиком. В противном случае **ПО Факел** не будет оперировать очередью и политика не будет иметь никакого эффекта. Если в канале есть до-

ступная для использования полоса пропускания, то можно встроить политику **Fair Queue** в другую политику с шейпингом на основе классов, чтобы убедиться в том, что **ПО Факел** оперирует очередью.

2.6.2.3 Политика FQ-CoDel

Описание

Дисциплина очередей: Fair/Flow Queue CoDel (FQ-CoDel).

Применяется к: исходящему трафику.

Политика **FQ-CoDel** распределяет трафик по 1024 FIFO очередям и направлена на обеспечение наилучшего качества между ними. При использовании данной политики по возможности сохраняется небольшая длина очередей.

Политика **FQ-CoDel** направлена на борьбу с переполнение буфера и на снижение задержек без необходимости задания сложной конфигурации. Данная политика используется по умолчанию для интерфейсов в некоторых дистрибутивах операционной систем Linux.

Политика использует стохастическую (случайную) модель распределения для классификации входящих пакетов на различные потоки и используется для обеспечения равных долей пропускной способности всем потокам, использующим очередь. Каждый поток обрабатывается в соответствии с дисциплиной CoDel. Переупорядочение пакетов в составе потока исключено, так как дисциплина CoDel использует внутреннюю очередь FIFO.

В основе политики **FQ-CoDel** лежит модифицированный планировщик очередей Deficit Round Robin (DRR) с алгоритмом CoDel Active Queue Management (AQM), работающим с каждой очередью.

Примечание

Политика **FQ-Codel** - политика без шейпинга, поэтому она будет полезна только в том случае, если исходящий интерфейс действительно перегружается трафиком. В противном случае **ПО Факел** не будет оперировать очередью, и политика не будет иметь никакого эффекта. Если в канале есть доступная для использования полоса пропускания, то можно встроить **FQ-Codel** в другую политику с шейпингом на основе классов, чтобы убедиться в том, **ПО Факел** оперирует очередью. Рекомендуется встраивать политику **FQ-CoDel** в политику **Shaper**.

Политика **FQ-CoDel** может эффективно использоваться с параметрами по умолчанию на скорости 10 Гбит/сек. Для других скоростей может потребоваться изменение параметров.

При скорости 1 Гбит/сек и ниже рекомендуется уменьшить значение параметра `queue-limit` до 1000 пакетов или меньше.

При скорости 10 Мбит/сек рекомендуется установить значение параметра `queue-limit` в 600 пакетов.

При скорости 100 Мбит/сек и выше, если политика **FQ-CoDel** встроена в политику **Shaper** рекомендуется установить значение параметра `quantum` в 8000 байт, чтобы снизить нагрузку на процессор.

При скорости менее 40 Мбит/сек рекомендуется установить уменьшить значение параметра `quantum` до 300 байт.

При скорости менее 3 Мбит/сек кроме задания значения параметра `quantum` в 300 байт рекомендуется также увеличить значение параметра `target` до 15 миллисекунд и значение параметра `interval` до 150 миллисекунд.

Далее представлен пример пример использования политики **FQ-CoDel**, встроенной в политику **Shaper**:

```
set traffic-policy shaper FQ-CODEL-SHAPER bandwidth 2gbit
set traffic-policy shaper FQ-CODEL-SHAPER default bandwidth 100%
set traffic-policy shaper FQ-CODEL-SHAPER default queue-type fq-codel
```

Список команд

Основные настройки

- `set traffic-policy fq-codel <policy name>`

  Задает уникальное имя для политики фильтрации трафика типа **FQ-CoDel**.

- `set traffic-policy fq-codel <policy name> codel-quantum <bytes>`

  Задает максимальное количество байт (по умолчанию - 1514), извлекаемых из очереди за один раз.

- `set traffic-policy fq-codel <policy name> flows <number-of-flows>`

  Задает количество дочерних очередей (по умолчанию - 1024), в которые будут помещаться классифицированные пакеты.

- `set traffic-policy fq-codel <policy name> interval <miliseconds>`

  Задает период времени в миллисекундах (по умолчанию - 100), используемый управляющим циклом CoDel для обнаружения устоявшихся очередей, чтобы исключить значительное увеличение минимально определенной задержки.

- `set traffic-policy fq-codel <policy-name> queue-limit <number-of-packets>`\`

  Задает предельный размер очереди в пакетах (по умолчанию - 10240). При достижении предельного размера все новые пакеты отбрасываются.

- `set traffic-policy fq-codel <policy-name> target <miliseconds>`\`

  Задает минимально допустимую задержку в миллисекундах (по умолчанию - 5) для ожидающей/устоявшейся очереди. Задержка определяется путем отслеживания минимальной задержки отдельной очереди, с которой сталкиваются проходящие через нее пакеты.

2.6.2.4 Политика Limiter

Описание

Дисциплина очередей: Ingress Policer.

Применяется к: входящему трафику.

Политика **Limiter** использует классы (на самом деле дисциплина очередей, применяемая для обработки входящего трафика, является бесклассовой политикой, но классификаторы могут успешной применяться совместно с ней).

Политика **Limiter** подразумевает простое ограничение входящих потоков трафика. Можно определить несколько классов трафика и применить к каждому классу свои ограничения. Не смотря на то, что внутри ограничителя используется механизм токен-корзин, он не имеет возможность удерживать пакеты, как это делает механизм шейпинга. Трафик, превышающий установленные ограничения полосы пропускания, отбрасывается напрямую. Также для политики **Limiter** может быть настроен максимально допустимый всплеск (burst) трафика.

Вы можете создать классы в количестве до 4090 штук с различными параметрами, а также политику по умолчанию, которая будет применена к любому трафику, не подошедшему под созданные классы.

Примечание

При необходимости применить к входящему трафику шейпинг, рекомендуется ознакомиться с разделом *Обработка входящего трафика* (страница 661).

Список команд

Основные настройки

- `set traffic-policy limiter <policy-name>`

  Задает уникальное имя для политики фильтрации трафика типа **Limiter**

- `set traffic-policy limiter <policy-name> class <class ID>`

  Задает числовой идентификатор класса (1 - 4090).

- `set traffic-policy limiter <policy-name> class <class ID> match <match-name> description <description>`

  Задает имя соответствующему классу правила, а также его текстовое описание.

- `set traffic-policy limiter <policy-name> class <class-ID> bandwidth <rate>`

  Задает максимально допустимую полосу пропускания для класса.

- `set traffic-policy limiter <policy-name> class <class-ID> burst <burst-size>`

  Задает размер всплеска (burst) трафика в байтах для класса (по умолчанию - 15).

- `set traffic-policy limiter <policy-name> default bandwidth <rate>`

  Задает максимально допустимую полосу пропускания для политики по умолчанию.

- `set traffic-policy limiter <policy-name> default burst <burst-size>`

  Задает размер всплеска (burst) трафика в байтах для политики по умолчанию (по умолчанию - 15).

- `set traffic-policy limiter <policy-name> class <class ID> priority <value>`

  Задает приоритет соответствующего классу правила (0 - 20, значение по умолчанию - 20). Чем ниже значение, тем выше приоритет.

2.6.2.5 Политика Network Emulator

Описание

Дисциплина очередей: Token Bucket Filter (TBF).

Applies to: исходящему трафику.

Политика **Network Emulator** имитирует условия эксплуатации реальной сети. При использовании данной политики есть возможность сконфигурировать такие параметры, как пропускную способность, всплеск (burst) трафика, задержку при передаче данных, потери пакетов, долю неправильных или пакетов с нарушением порядка следования.

Данная политика может быть полезна при определении поведения приложения в определенных условиях эксплуатации сети.

Список команд

Основные настройки

- `set traffic-policy network-emulator <policy-name>`

  Задает уникальное имя для политики фильтрации трафика типа **Network Emulator**

- `set traffic-policy network-emulator <policy-name> bandwidth <rate>`

  Задает пропускную способность для политики фильтрации трафика типа **Network Emulator**

- `set traffic-policy network-emulator <policy-name> burst <burst-size>`

  Задает размер всплеска (burst) трафика в байтах (по умолчанию - 15), который будет учитываться только при заданной пропускной способности.

- `set traffic-policy network-emulator <policy-name> network-delay <delay>`

  Задает задержку в миллисекундах при прохождении пакетов через интерфейс (по умолчанию - 50), которая будет учитываться только при заданной пропускной способности.

- `set traffic-policy network-emulator <policy-name> packet-corruption <percent>`

  Задает в процентном соотношении количество неправильных пакетов. На случайно позиции в структуре таких пакетов будет размещаться случайная ошибки в соответствии с заданной долей.

- `set traffic-policy network-emulator <policy-name> packet-loss <percent>`

  Задает значение допустимой потери пакетов в процентах.

- `set traffic-policy network-emulator <policy-name> packet-reordering <percent>`

  Задает количество пакетов, порядок следования которых нарушается, в процентах.

- `set traffic-policy network-emulator <policy-name> queue-limit <limit>`

  Задает количество пакетов (1 - 4294967295), которое может содержать очередь в отдельный момент времени.

2.6.2.6 Политика Priority Queue

Описание

Дисциплина очередей: PRIO.

Применяется к: исходящему трафику.

Политика **Priority Queue** является политикой на основе классов, которая не вносит задержек в движение пакетов, так как она не является политикой с шейпингом. При использовании данной политики пакеты извлекаются из очередей в соответствии с заданным приоритетом.

Примечание

Политика **Priority Queue**, как и любая другая политика без шейпинга, полезна только в случае, если достигнут предел пропускной способности исходящего интерфейса. Если этого не произошло, **ПО Факел** не использует очередь, и политика не будет действовать. Однако даже если физический канал располагает доступной полосой пропускания, можно встроить политику **Priority Queue** в другую политику с шейпингом на основе классов, чтобы убедиться в том, **ПО Факел** оперирует очередью. В этом случае пакеты могут получать приоритеты согласно метке DSCP.

Можно назначить до 7 очередей, определенных как классы, с различными приоритетами. Пакет помещаются в очереди в соответствии с заданным классификатором. Пакеты извлекаются из очередей в указанном порядке. Если классы с более высоким приоритетом переполняются, то пакеты из классов с приоритетом ниже, будут переданы дальше, только после снижения нагрузки на классы с более высоким приоритетом.

Примечание

Политика **Priority Queue** предусматривает задание числового идентификатора класса для обозначения приоритета (1 - 7). Чем ниже значение, тем выше приоритет.

Как и в случае с другими политиками, можно указать различные типы соответствующих классам правил.

```
fakel@fakel# set traffic-policy priority-queue MY-PRIO class 3 match MY-MATCH-RULE
Possible completions:
   description  Description for this match
>  ether        Ethernet header match
   interface    Interface name for this match
>  ip           Match IP protocol header
>  ipv6         Match IPV6 header
   mark         Match on mark applied by firewall
   vif          Virtual Local Area Network (VLAN) ID for this match
```

Как и в случае с другими политиками, можно встраивать в классы (включая класс по умолчанию) политики **Priority Queue** другие политики с помощью параметра `queue-type`.

```
fakel@fakel# set traffic-policy priority-queue MY-PRIO class 3 queue-type
Possible completions:
   fq-codel       Fair Queue Codel
   fair-queue     Stochastic Fair Queue (SFQ)
   drop-tail      First-In-First-Out (FIFO)
   priority       Priority queueing based on DSCP
   random-detect  Random Early Detection (RED)
```

Список команд

Основные настройки

• `set traffic-policy priority-queue <policy-name> class <class-ID> queue-limit <limit>`

Создает политику **Priority Queue**. Задает уникальное имя для данной политики и числовой идентификатор класса (1 - 7). Можно указать максимально допустимый размер очереди, по достижении которого все новые пакеты отбрасываются.

2.6.2.7 Политика Random Detect

Описание

Дисциплина очередей: Random Early Drop (RED).

Применяется к: исходящему трафику.

При использовании политики **Random Detect** пакеты случайным образом отбрасываются из очереди перед тем, как она будет заполнена. Такое поведение особенно актуально для коммуникаций по протоколу TCP, так как отбрасывание пакетов может служить сигналом их отправителю, чтобы он снизил скорость передачи.

В отличие от стандартной дисциплины RED политика **Random Detect** обеспечивает различные виртуальные очереди на основе значения параметра *IP Precedence* таким образом, что некоторые виртуальные очереди отбрасывают большее количество пакетов, чем другие.

Это достигается путем использования первых трех бит поля ToS (Type of Service) для определения потоков данных. Решение принимается в соответствии с установленным значением параметра *IP Precedence*, то есть установленным приоритетом.

Параметр *IP Precedence* определен в спецификации **RFC 791**[65].

Приоритет	Описание
7	Network Control
6	Internetwork Control
5	CRITIC / ECP
4	Flash Override
3	Flash
2	Immediate
1	Priority
0	Routine

Политика **Random Detect** может быть полезной при «тяжелых» профилях трафика, особенно на магистральных каналах, чтобы избежать их перегрузки, но только при условии, что все коммуникации используют протокол TCP (отброшенные пакеты будут переданы повторно, но с пониженной интенсивностью).

Если средний размер очереди ниже значения параметра `min-threshold`, поступающий пакет будет помещен в очередь.

Если средний размер очереди находится в диапазоне значений параметров `min-threshold` и `max-threshold`, поступающий пакет будет либо помещен в очередь, либо отброшен. Результат будет определен значением параметра `mark-probability`.

Если текущий размер очереди превышает значение параметра `queue-limit`, пакеты буду отбрасываться. Средний размер очереди зависит от предыдущего ее размера и текущего.

Если значение параметра `max-threshold` установлено, а значение параметра `min-threshold` - нет, последний определяется как 50% от значения параметра `max-threshold`.

[65] https://datatracker.ietf.org/doc/html/rfc791.html

В общем случае рекомендуется устанавливать следующие значения для данных параметров: `min-threshold` < `max-threshold` < `queue-limit`.

Список команд

Основные настройки

- `set traffic-policy random-detect <policy-name>`

  Задает уникальное имя для политики фильтрации трафика типа **Random Detect**.

- `set traffic-policy random-detect <policy-name> bandwidth <bandwidth>`

  Задает значение доступной полосы пропускания для политики фильтрации трафика типа **Random Detect**, значение которой будет использоваться для расчета среднего размера очереди после некоторого времени ее простоя. Рекомендуется указывать полосу пропускания в соответствии с полосой пропускания сетевого интерфейса. Политика **Random Detect** не является политикой с шейпингом.

- `set traffic-policy random-detect <policy-name> precedence <IP-precedence-value>`

  Задает значение параметра *IP Precedence* для виртуальной очереди.

Примечание

Чем больше значение параметра *IP Precedence*, тем выше приоритет.

- `set traffic-policy random-detect <policy-name> precedence <IP-precedence-value> average-packet <bytes>`

  Задает средний размер пакета в байтах (по умолчанию - 1024).

- `set traffic-policy random-detect <policy-name> precedence <IP-precedence-value> mark-probability <value>`

  Задает вероятность отбрасывания пакетов путем указания значения N в распределении 1/N (по умолчанию - 10).

- `set traffic-policy random-detect <policy-name> precedence <IP-precedence-value> maximum-threshold <packets>`

  Задает максимальное пороговое количество пакетов для случайного отбрасывания (0 - 4096, по умолчанию - 18). При заданном пороговом количестве вероятность отбрасывания будет максимальной.

- `set traffic-policy random-detect <policy-name> precedence <IP-precedence-value> minimum-threshold <packets>`

  Задает минимальное пороговое количество пакетов для случайного отбрасывания (0 - 4096). Если заданное пороговое значение превышается, пакеты становятся кандидатами на отбрасывание.

Значения по умолчанию минимального порогового количества пакетов представлены в таблице ниже в разрезе приоритетов:

Приоритет	Значение по умолчанию
7	16
6	15
5	14
4	13
3	12
2	11
1	10
0	9

- `set traffic-policy random-detect <policy-name> precedence <IP-precedence-value> queue-limit <packets>`

  Задает максимальный размер очереди в пакетах (1 - 4294967295), при достижении которого все новые пакеты отбрасываются.

2.6.2.8 Политика Rate Control

Описание

Дисциплина очередей: Token Bucket Filter (TBF).

Применяется к: исходящему трафику.

Политика **Rate Control** является бесклассовой политикой, ограничивающей поток пакетов установленной скоростью, то есть по сути это - политика с шейпингом, которая не распределяет трафик по очередям. Обработка трафика осуществляется путем контроля расхода токенов. Токены в некоторой степени соответствуют количеству байт обработанных данных.

Допускаются кратковременные всплески трафика, которые приводят к превышению заданного лимита. При создании политика **Rate Control** накапливает токены, количество которых соответствует объему всплеска трафика при однократном проходе трафика через механизм TBF. Токены поступают с постоянной скоростью до тех пор, пока токен-корзина не будет наполнена.

Политика **Rate Control** незначительно влияет на загрузку процессора. Рекомендуется использовать данную политику, если есть необходимость замедлить движение (обработку) трафика.

Список команд

Основные настройки

- `set traffic-policy rate-control <policy-name>`

  Задает уникальное имя для политики фильтрации трафика типа **Rate Control**.

- `set traffic-policy rate-control <policy-name> bandwidth <rate>`

  Задает лимит скорости для политики фильтрации трафика типа **Rate Control**.

- `set traffic-policy rate-control <policy-name> burst <burst-size>`

  Задает в байтах размер токен-корзины, которая будет использоваться для обработки всплесков трафика.

Примечание

Для сетевых адаптеров компании Intel с технической пропускной способностью в 10 Мбит/сек необходимо иметь буфер емкостью в 100 КБ, чтобы была возможность достичь заданной скорости. Буфер меньшей емкости довольно скоро приведет к отбрасыванию пакетов.

- `set traffic-policy rate-control <policy-name> latency`

  Задает максимально допустимую задержку в миллисекундах пакетов в очереди (по умолчанию - 50).

2.6.2.9 Политика Round Robin

Описание

Дисциплина очередей: Deficit Round Robin (DRR).

Применяется к: исходящему трафику.

Политика **Round Robin** является распределяющей политикой на основе классов, которая распределяет трафик по различным классам (максимальное количество классов - 4096). Можно встроить политику **Round Robin** в каждый из доступных классов, включая класс по умолчанию.

Каждому классу назначается специальный счетчик дефицита данных (количество байт, которое может быть передано в рамках потока при его обработке), инициализируемый параметром - квантом. Квант - это настраиваемый параметр, который представляет собой фиксированное количество байт, предоставляемых счетчику на каждом цикле его работы. Затем политика **Round Robin** начинает перемещать указатель по очередям. Если счетчик дефицита данных превышает размер пакета в начале очереди, пакет будет отправлен, а значение счетчика - уменьшено на размер пакета. Затем размер следующего пакета снова сравнивается со значением счетчика, и процесс повторяется. Как только очередь окажется пустой или текущего значения счетчика будет недостаточно для сравнения, указатель будет перемещен к следующей очереди. Если очередь пустая, то значение счетчика дефицита данных сбрасывается к нулевому значению.

На каждом цикле работы счетчик дефицита данных добавляет квант, поэтому даже большие по размеру пакеты могут быть обработаны в очереди.

Политика **Round Robin** может быть встроена в класс другой политики с помощью параметра `queue-type`.

```
fakel@fakel# set traffic-policy round-robin DRR class 10 queue-type
Possible completions:
   fq-codel    Fair Queue Codel
   fair-queue  Stochastic Fair Queue (SFQ)
   drop-tail   First-In-First-Out (FIFO)
   priority    Priority queueing based on DSCP
```

Список команд

Основные настройки

- `set traffic-policy round-robin <policy name>`

  Задает уникальное имя для политики фильтрации трафика типа **Round Robin**.

- `set traffic-policy round-robin <policy name> class <class-ID>`

  Задает числовой идентификатор класса для политики фильтрации трафика типа **Round Robin**.

- `set traffic-policy round-robin <policy name> class <class-ID> quantum <packets>`

  Задает квант для определенного идентификатора класса, значение которого будет добавляться на каждом цикле работы счетчика дефицита данных.

- `set traffic-policy round-robin <policy name> class <class ID> queue-limit <packets>`

Задает размер очереди в пакетах.

2.6.2.10 Политика Shaper

Описание

Дисциплина очередей: Hierarchical Token Bucket (HTB).

Применяется к: исходящему трафику.

Политика **Shaper** не гарантирует низкую задержку, но гарантирует определенную полосу пропускания для различных классов трафика, а также позволяет распределить трафик при соблюдении данных гарантий.

Каждый класс предоставляет гарантированную часть полосы пропускания, определенную для политики целиком. Другие классы оперируют оставшейся полосой пропускания, доступной в политике.

Если гарантированная полоса пропускания обеспечена, а загрузка трафиком ее не превышает, то может быть использован параметр `ceiling`, который определяет выделяемую долю полосы пропускания. Если гарантированная полоса пропускания обеспечена, и несколько классов используют заданный для них параметр `ceiling`, то можно использовать параметр `priority` для распределения дополнительного трафика в определенном порядке. Параметр `priority` представляет собой число от 0 до 7. Чем ниже значение параметра `priority`, тем выше приоритет.

Политика **Shaper** может быть встроена в класс другой политики с помощью параметра `queue-type`.

```
fakel@fakel# set traffic-policy shaper HTB class 10 queue-type
Possible completions:
   fq-codel       Fair Queue Codel
   fair-queue     Stochastic Fair Queue (SFQ)
   drop-tail      First-In-First-Out (FIFO)
   priority       Priority queueing based on DSCP
   random-detect  Random Early Detection (RED)
```

```
fakel@fakel# set traffic-policy shaper HTB class 10
Possible completions:
   bandwidth      Bandwidth used for this class
   burst          Burst size for this class (default: 15kb)
   ceiling        Bandwidth limit for this class
   codel-quantum  fq-codel - Number of bytes used as 'deficit' (default 1514)
   description    Description for this traffic class
   flows          fq-codel - Number of flows (default 1024)
   interval       fq-codel - Interval (milliseconds) used to measure the delay
  (default 100)
+> match          Class matching rule name
   priority       Priority for usage of excess bandwidth
   queue-limit    Maximum queue size (packets)
   queue-type     Queue type for this class
   set-dscp       Change the Differentiated Services (DiffServ) field in the IP
  header
   target         fq-codel - Acceptable minimum queue delay (milliseconds)
```

Примечание

Если сконфигурирован класс для трафика, источником которого является технология VoIP, не рекомендуется задавать для него параметр `ceiling`. В противном случае новые звонки могут не пройти из-за того, что полоса пропускания уже поделена между остальными классами.

Далее представлен пример использования политики **Shaper** с приоритетами.

```
set traffic-policy shaper MY-HTB bandwidth '50mbit'
set traffic-policy shaper MY-HTB class 10 bandwidth '20%'
set traffic-policy shaper MY-HTB class 10 match DSCP ip dscp 'EF'
set traffic-policy shaper MY-HTB class 10 queue-type 'fq-codel'
set traffic-policy shaper MY-HTB class 20 bandwidth '10%'
set traffic-policy shaper MY-HTB class 20 ceiling '50%'
set traffic-policy shaper MY-HTB class 20 match PORT666 ip destination port '666'
set traffic-policy shaper MY-HTB class 20 priority '3'
set traffic-policy shaper MY-HTB class 20 queue-type 'fair-queue'
set traffic-policy shaper MY-HTB class 30 bandwidth '10%'
set traffic-policy shaper MY-HTB class 30 ceiling '50%'
set traffic-policy shaper MY-HTB class 30 match ADDRESS30 ip source address
  '192.168.30.0/24'
set traffic-policy shaper MY-HTB class 30 priority '5'
set traffic-policy shaper MY-HTB class 30 queue-type 'fair-queue'
set traffic-policy shaper MY-HTB default bandwidth '10%'
set traffic-policy shaper MY-HTB default ceiling '100%'
set traffic-policy shaper MY-HTB default priority '7'
set traffic-policy shaper MY-HTB default queue-type 'fair-queue'
```

Список команд

Основные настройки

`# set traffic-policy shaper <policy-name>`

Задает уникальное имя для политики фильтрации трафика типа **Shaper**.

`# set traffic-policy shaper <policy-name> bandwidth <rate>`

Устанавливает гарантированную полосу пропускания для всего трафика без учета классов.

`# set traffic-policy shaper <policy-name> class <class-ID>`

Задает числовой идентификатор класса для политики фильтрации трафика типа **Shaper**.

`# set traffic-policy shaper <policy-name> class <class-ID> bandwidth <rate>`

Устанавливает гарантированную полосу пропускания для трафика определенного класса.

`# set traffic-policy shaper <policy-name> class <class-ID> burst <bytes>`

Задает размер токен-корзины в байтах (по умолчанию - 15 КБ), которая будет использована при передаче трафика на скорости параметра *ceiling*.

`# set traffic-policy shaper <policy-name> class <class-ID> ceiling <bandwidth>`

Задает максимально возможную скорость для определенного класса.

```
# set traffic-policy shaper <policy-name> class <class-ID> priority <0-7>
```

Устанавливает приоритет (по умолчанию - 0) использования доступной полосы пропускания при условии, что обеспечена гарантированная полоса.

2.6.3 Применение политики

После конфигурирования политики обработки трафика ее необходимо применить к соответствующему интерфейсу:

```
set interfaces etherhet eth0 traffic-policy out WAN-OUT
```

К отдельному интерфейсу и для определенного направления движения трафика может быть применена только одна политика обработки трафика, но одну и ту же политику можно применять к различным интерфейсам и для других направлений движения трафика.

```
set interfaces ethernet eth0 traffic-policy in WAN-IN
set interfaces etherhet eth0 traffic-policy out WAN-OUT
set interfaces etherhet eth1 traffic-policy in LAN-IN
set interfaces etherhet eth1 traffic-policy out LAN-OUT
set interfaces ethernet eth2 traffic-policy in LAN-IN
set interfaces ethernet eth2 traffic-policy out LAN-OUT
set interfaces etherhet eth3 traffic-policy in TWO-WAY-POLICY
set interfaces etherhet eth3 traffic-policy out TWO-WAY-POLICY
set interfaces etherhet eth4 traffic-policy in TWO-WAY-POLICY
set interfaces etherhet eth4 traffic-policy out TWO-WAY-POLICY
```

- `show queueing <interface-type> <interface-name>`

  Выводит информацию о результатах работы политик обработки трафика, примененных к интерфейсу. Информация содержит счетчики пакетов в разрезе каждой политики и каждого сконфигурированного класса.

2.6.4 Обработка входящего трафика

Применяется к: входящему трафику.

Для обработки входящего трафика на интерфейсе может быть использована только одна политика - политика **Limiter**. Отсутствует возможность применения какой-либо политики с шейпингом к входящему трафику на любом интерфейсе, так как их реализация ограничивается работой только с исходящим трафиком.

Однако есть сценарий, когда можно применить политику с шейпингом к входящему трафику путем его перенаправления на специальный виртуальный интерфейс (Intermediate Functional Block[66]). Идея состоит в том, что к виртуальному интерфейсу применяется политика, в том числе политика с шейпингом, направленная на обработку исходящего трафика.

Далее представлен пример того, как можно организовать шейпинг входящего трафика:

```
set traffic-policy shaper MY-INGRESS-SHAPING bandwidth 1000kbit
set traffic-policy shaper MY-INGRESS-SHAPING default bandwidth 1000kbit
set traffic-policy shaper MY-INGRESS-SHAPING default queue-type fair-queue

set interfaces input ifb0 traffic-policy out MY-INGRESS-SHAPING
set interfaces ethernet eth0 redirect ifb0
```

Предупреждение

Механизм *Intermediate Functional Block* необходимо настраивать только после того, как будет заданы все остальные параметры конфигурации политики обработки трафика. В противном случае возникнет ошибка `RTNETLINK answer: File exists`, которую можно устранить только с помощью команды `sudo ip link delete ifb0`.

[66] https://www.linuxfoundation.org/collaborate/workgroups/networking/ifb

2.7 Отказоустойчивость

В **ПО Факел** отказоустойчивость обеспечивается путем использования следующих механизмов:

- *VRRP* (страница 663)
- *Балансировка WAN-каналов* (страница 671)

2.7.1 VRRP

2.7.1.1 Описание

Протокол VRRP (Virtual Router Redundancy Protocol) позволяет организовать избыточность на уровне маршрутизаторов в формате активный-резервный. Протокол VRRP объединяет несколько маршрутизаторов в отказоустойчивый кластер. Все маршрутизаторы, которые являются участниками отказоустойчивого кластера имеют общий виртуальный адрес IP (VIP) адрес и общий номер группы или VRID (Virtual Router Identifier). Один маршрутизатор может состоять в нескольких группах, каждая из которых должна иметь свою уникальную пару VIP/VRID. Все маршрутизаторы делятся на два типа: VRRP Master и VRRP Backup.

- **VRRP Master** — это маршрутизатор, который занимается пересылкой пакетов для данного виртуальной группы.
- **VRRP Backup** — это маршрутизатор, который ожидает пакет от Master. Если пакеты от Master перестают приходить, Backup пытается перейти в состояние Master.

При запуске маршрутизаторы обмениваются сообщениями, выбирая таким образом между собой активного. Активным становится тот маршрутизатор который имеет наивысший приоритет. Виртуальный IP адрес назначается активному маршрутизатору. Все остальные маршрутизаторы с приоритетом ниже становятся резервными. В процессе работы активный маршрутизатор рассылает остальным маршрутизаторам keepalive пакеты на широковещательный адрес 224.0.0.18, чтобы сообщить Backup маршрутизаторам, что он работает. Master отправляет сообщения согласно таймеру advertise-interval, равный по умолчанию 1 секунде. В качестве MAC адреса отправителя используется адрес группы 00:00:5E:00:01:xx, где xx — VRID в шестнадцатеричном формате. Если Backup маршрутизаторы не получают сообщения в течении трех advertise-interval (количество интервалов определяется параметром failure-count), то новым Master становится маршрутизатор с наибольшим приоритетом. Если в группе появится Backup маршрутизатор с более высоким приоритетом, то он перехватит роль Master у маршрутизатора с более низким приоритетом. Однако, когда у Backup маршрутизатора, который имеет более высокий приоритет активирован параметр no-preempt, такой Backup маршрутизатор не станет перехватывать роль у Master маршрутизатора. VRRP приоритет задается в значениях от 1 до 254. Значение 0 зарезервировано для случаев, когда Master необходимо снять с себя ответственность за маршрутизацию. Значение 255 устанавливается маршрутизатору владельцу VIP. Если VRRP-маршрутизатор является владельцем VIP адреса, то он всегда перехватывает роль Master. Приоритет по умолчанию равен 100, но может задаваться административно. VRRP маршрутизатор может иметь три состояния:

- Initialize
- Backup
- Master

VRRP маршрутизатор изменяет свои состояния последовательное.

В состоянии Initialize маршрутизатор ожидает начала работы. Если этот маршрутизатор является владельцем VIP адреса (приоритет равен 255), то маршрутизатор отправляет сообщения о том что он становится Master. Он также отправляет gratuitous ARP-запрос, в котором MAC-адрес источника равен адресу виртуального маршрутизатора. Затем он переходит в состояние Master. Если маршрутизатор не является владельцем VIP, то он переходит в состояние Backup.

В состоянии Backup маршрутизатор ожидает пакеты от Master маршрутизатора. Маршрутизатор в этом состоянии не отвечает на ARP-запросы от VIP-адреса. Также он не принимает пакеты, у которых в каче-

стве адреса назначения стоит MAC-адрес виртуального маршрутизатора.

Если Backup не получает сообщения от Master в течение количества advertise-interval, заданных в параметре failure-count (по умолчанию установлено значение 3 интервала), то он отправляет VRRP сообщение о том, что собирается стать Master. Затем этот маршрутизатор отправляет широковещательное VRRP сообщение, в котором MAC-адрес источника равен адресу этого виртуального маршрутизатора. В данном сообщении маршрутизатор указывает свой приоритет.

В состоянии Master маршрутизатор обрабатывает пакеты, адресованные виртуальному маршрутизатору. Он так же отвечает на ARP-запросы к VIP. Master маршрутизатор рассылает VRRP сообщения каждые advertise-interval (по умолчанию значение равно 1 секунде), чтобы подтвердить что он работает.

Если к одному сетевому интерфейсу привязывается несколько VRRP групп, каждая из них должна иметь уникальное значение VRID, однако есть возможность указывать дублирующиеся между разными сетевыми интерфейсами значения VRID, хотя рекомендуется так не делать во избежание проблем с распознаванием групп.

Протокол VRRP выполняет свои функции в одном из двух режимов:

- С наследование роли Master - если маршрутизатор с наивысшим приоритетом
- выходит из строя, а затем восстанавливает свою работу, маршрутизатор с приоритетом ниже возвращает ему роль активного.
- Без наследования роли Master - маршрутизатор, которому была назначена
- роль активного, сохраняет ее и назначенный виртуальный IP адрес вне зависимости от поведения маршрутизатора с приоритетом выше.

2.7.1.2 Настройка

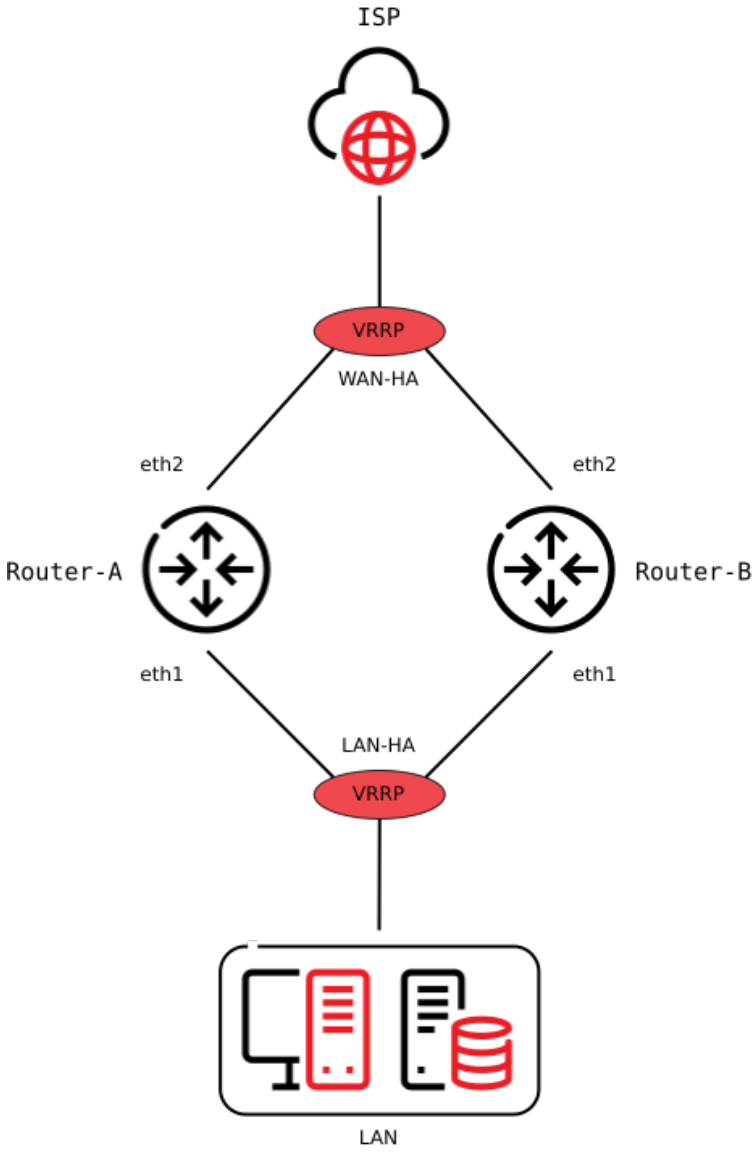
Алгоритм настройки VRRP группы:

1. Указать IP адреса и задать описание интерфейсов физических интерфейсов маршрутизатора
2. Задать имя и описание для VRRP группы
3. Указать физический интерфейс маршрутизатора, который будет являться участником VRRP группы
4. Определить приоритет маршрутизатора для VRRP группы
5. Задать виртуальный адрес VIP для VRRP группы
6. Указать общий номер VRRP группы VRID
7. Выполнить аналогичные настройки на втором маршрутизаторе

Пример настройки

В качестве примера рассмотрим ситуацию, когда есть два маршрутизатора (Router-A и Router-B) у которых внешние WAN интерфейсы объединены в одну VRRP группу, а внутренние LAN интерфейсы в другую VRRP группу. Маршрутизатор Router-A будет иметь наивысший приоритет и являть Master маршрутизатором. В случае выхода из строя маршрутизатора Router-A роль Master перейдет к маршрутизатору Router-B. Если маршрутизатор Router-A восстанавливает работоспособное состояние, роль Master снова переходит к нему, а маршрутизатору Router-B возвращается роль Backup.

Настройка маршрутизаторов будет выполнена в соответствии со схемой, представленной ниже:



Исходные данные для настройки VRRP группы:

- `192.168.100.1/29` - адрес внутреннего LAN интерфейса eth0 на первом маршрутизатора Router-A
- `10.250.44.1/29` - адрес внешнего WAN интерфейса eth1 на первом маршрутизатора Router-A
- `192.168.100.2/29` - адрес внутреннего LAN интерфейса eth0 на первом маршрутизатора Router-B
- `10.250.44.2/29` - адрес внешнего WAN интерфейса eth1 на первом маршрутизатора Router-B
- `LAN-HA` - имя VRRP группы, которая объединяет внутренние интерфейсы маршрутизаторов Router-A и Router-B
- `WAN-HA` - имя VRRP группы, которая объединяет внешние интерфейсы маршрутизаторов Router-A и Router-B
- `192.168.100.6/29` - виртуальный адрес (VIP) для внутреннего LAN интерфейса VRRP группы LAN-HA

- `10.250.44.6/29` - виртуальный адрес (VIP) для внешнего WAN интерфейса VRRP группы WAN-HA
- `210` - номер VRID для VRRP группы LAN-HA
- `220` - номер VRID для VRRP группы WAN-HA
- `10` - приоритет для VRRP групп на маршрутизаторе Router-A
- `5` - приоритет для VRRP групп на маршрутизаторе Router-B

Команды для настройки

Список команд для настройки VRRP групп на маршрутизаторе Router-A:

```
set interfaces ethernet eth1 address '192.168.100.1/29'
set interfaces ethernet eth1 description 'LAN'
set interfaces ethernet eth2 address '10.250.44.1/29'
set interfaces ethernet eth2 description 'WAN'
set high-availability vrrp group LAN-HA description 'LAN Interface Hight
 Availability'
set high-availability vrrp group LAN-HA interface 'eth1'
set high-availability vrrp group LAN-HA priority '10'
set high-availability vrrp group LAN-HA virtual-address 192.168.100.6/29
set high-availability vrrp group LAN-HA vrid '210'
set high-availability vrrp group WAN-HA description 'LAN Interface Hight
 Availability'
set high-availability vrrp group WAN-HA interface 'eth2'
set high-availability vrrp group WAN-HA priority '10'
set high-availability vrrp group WAN-HA virtual-address 10.250.44.6/29
set high-availability vrrp group WAN-HA vrid '220'
```

Список команд для настройки VRRP групп на маршрутизаторе Router-A:

```
set interfaces ethernet eth1 address '192.168.100.2/29'
set interfaces ethernet eth1 description 'LAN'
set interfaces ethernet eth2 address '10.250.44.2/29'
set interfaces ethernet eth2 description 'WAN'
set high-availability vrrp group LAN-HA description 'LAN Interface Hight
 Availability'
set high-availability vrrp group LAN-HA interface 'eth1'
set high-availability vrrp group LAN-HA priority '5'
set high-availability vrrp group LAN-HA virtual-address 192.168.100.6/29
set high-availability vrrp group LAN-HA vrid '210'
set high-availability vrrp group WAN-HA description 'LAN Interface Hight
 Availability'
set high-availability vrrp group WAN-HA interface 'eth2'
set high-availability vrrp group WAN-HA priority '5'
set high-availability vrrp group WAN-HA virtual-address 10.250.44.6/29
set high-availability vrrp group WAN-HA vrid '220'
```

2.7.1.3 Список команд

Основные настройки

- `set high-availability vrrp group <name> vrid <id>`

  Задает имя <*name*> и идентификатор <*id*> для VRRP группы

- `set high-availability vrrp group <name> interface <interface>`

  Добавляет сетевой интерфейс <*interface*> для VRRP группы <*name*>

- `set high-availability vrrp group <>name> virtual-address <address>`

  Добавляет виртуальный адрес <*address*> для VRRP группы <*name*>

Примечание

Значение параметра *virtual-address* представлено IPv4 адресом.

- `set high-availability vrrp group <name> disable`

  Отключает определенную группу VRRP <*name*>.

Примечание

Дезактивированная группа VRRP будет полностью исключена из процесса VRRP, равно как и маршрутизатор, входящий в группу с данным VRID. Информация о дезактивированной группе VRRP также не будет присутствовать в выводе на экран результатов выполнения соответствующих команд в эксплуатационном режиме, а сама группа больше не будет выполнять роль резервной.

Дополнительные настройки

- `set high-availability vrrp group <name> priority <number>`

  Задает приоритет <*number*> для VRRP группы <*name*>

Примечание

Значение приоритета должно быть представлено целым числом в диапазон от 1 до 255. Наивысшее значение приоритета определяет, какой из маршрутизаторов будет определен как активный при очередной процедуре выбора.

- `set high-availability vrrp group <name> no-preempt`

  Переводит протокол VRRP в режим без наследования роли. По умолчанию протокол VRRP выполняет свои функции в режиме с наследованием роли.

- `set high-availability vrrp group <name> preempt-delay <number>`

  Задает временной интервал для задержки перед изменением роли наследования маршрутизатора с наивысшим приоритетом.

- `set high-availability vrrp group <name> peer-address <address>`

  Задает адрес <address> для одноадресной (unicast) рассылки в VRRP группе <name>

- `set high-availability vrrp group <name> hello-source-address <address>`

  Задает адрес источника <address> для рассылки *hello* пакетов в VRRP группе <name>

- `set high-availability vrrp group <name> rfc3768-compatibility`

  Создает новый VRRP интерфейс, которому автоматически назначаются виртуальный IP адрес и виртуальный MAC адрес.

Примечание

RFC 3768[67] определяет порядок задания и использования виртуальных MAC адресов для каждого маршрутизатора в процессе VRRP. Виртуальный MAC адрес используется в качестве адреса отправителя для всех периодических сообщений, источником которых является активный маршрутизатор.

Мониторинг

- `show vrrp`

  Выводит на экран информацию о созданной группе VRRP.

  Пример работы команды show vrrp:

```
fakel@fakel:~$ run show vrrp
Name        Interface      VRID  State    Last Transition
----------  -----------  ------  -------  -----------------
Foo         eth1             10  MASTER   2s
```

[67] https://datatracker.ietf.org/doc/html/rfc3768.html

Использование скриптов

Функциональность протокола VRRP может быть расширена посредством пользовательских bash скриптов. **ПО Факел** поддерживает использования двух типов скриптов: скриптов контроля (health check) и скриптов состояния. Скрипты контроля (health check) подразумевают выполнение пользовательских проверок в дополнение к стандартной проверке доступности активного маршрутизатора. Скрипты состояния подразумевают изменение состояния, при котором активный маршрутизатор становится резервным или выходит из строя, и наоборот. Скрипты состояния могут быть использованы, например, для активации или дезактивации определенных сервисов.

Скрипты контроля

Пример, представленный ниже, показывает настройку процесса VRRP на использование скрипта контроля, размещенного по следующему пути `/config/scripts/vrrp-check.sh script` каждый 60 секунд с последующим переводом группы VRRP в состояние неисправной, если результат проверки будет неудачный (то есть скрипт завершается с ненулевым состоянием) три раза подряд.

```
set high-availability vrrp group Foo health-check script /
  config/scripts/vrrp-check.sh
set high-availability vrrp group Foo health-check interval 60
set high-availability vrrp group Foo health-check failure-count 3
```

Скрипты состояния

Скрипты состояния позволяют реализовать такие действия, как, например, запуск или остановку сервисов или даже изменение конфигурации **ПО Факел** в случае, если процесс VRRP фиксирует изменение состояния. Пример, представленный ниже, показывает настройку процесса VRRP на использование скрипта состояния, размещенного по следующему пути `/config/scripts/vrrp-fail.sh` с аргументом Foo при переводе группы VRRP в состояние неисправной, а также скрипта, размещенного по следующему пути `/config/scripts/vrrp-master.sh`, когда маршрутизатор становится активным.

```
set high-availability vrrp group Foo transition-script backup ”/
  config/scripts/vrrp-fail.sh Foo”
set high-availability vrrp group Foo transition-script fault ”/
  config/scripts/vrrp-fail.sh Foo”
set high-availability vrrp group Foo transition-script master ”/
  config/scripts/vrrp-master.sh Foo”
```

Синхронные группы

Синхронные группы позволяют объединять отдельные группы VRRP для синхронизации их состояний.

```
edit high-availability vrrp
set sync-group MAIN member VLAN9
set sync-group MAIN member VLAN20
```

В примере далее представлена конфигурация, при которой в случае изменения состояния для группы *VLAN9* также изменяется состояние группы *VLAN20*.

```
vrrp {
    group VLAN9 {
        interface eth0.9
        virtual-address 10.9.1.1/24
        priority 200
        vrid 9
    }
    group VLAN20 {
        interface eth0.20
        priority 200
        virtual-address 10.20.20.1/24
        vrid 20
    }
    sync-group MAIN {
        member VLAN20
        member VLAN9
    }
}
```

Предупреждение

Все элементы синхронной группы должны быть сконфигурированы одинаковым образом. Если для одной из групп VRRP в составе синхронной группы заданы значения приоритета или задержки перед наследованием роли (активный/резервный), отличные от значений для других групп, это может привести к бесконечному циклу изменения состояний групп.

2.7.2 Балансировка WAN-каналов

2.7.2.1 Описание

Исходящий по отношению к маршрутизатору трафик может быть распределен между двумя или более исходящими сетевыми интерфейсами. Если на одном из путей прохождения трафика происходит сбой, то такой путь исключается из таблицы маршрутизации, а трафик перераспределяется между оставшимися работоспособными путями. При восстановлении пути прохождения трафика после сбоя он снова добавляется в таблицу маршрутизации и используется сервисом балансировки трафика. Сервис балансировки трафика автоматически добавляет маршруты для каждого пути прохождения трафика в таблицу балансировки и распределяет трафик между всеми сконфигурированными сетевыми интерфейсами маршрутизатора, руководствуясь их текущим состоянием и заданным администратором весом.

Минимально необходимая конфигурация для балансировки WAN каналов должна включать:

- определенный сетевой интерфейс маршрутизатора с заданным адресом и адресом следующего узла;
- одно правило балансировки с заданными сетевыми интерфейсами LAN (*inbound-interface*) и WAN (*interface*) соответственно.

Примечание

Балансировку WAN каналов не рекомендуется использовать совместно с протоколами динамической маршрутизации, так как сервис балансировки создает дополнительные таблицы маршрутизации и правила межсетевого экрана, которые могут быть не совместимы с протоколами динамической маршрутизации.

Правила балансировки

Сетевые интерфейсы, их вес и тип трафика, подлежащего балансировке - эти данные указываются в наборах правил балансировки. Правила балансировки применяются в порядке их следования в списке к исходящим по отношению к маршрутизатору сетевым пакетам. При совпадении данных пакета и классификатора определенного правила балансировки этот пакет перенаправляется далее через сетевой интерфейс, указанный в этом правиле. Если для пакета не обнаружено ни одного совпадения, то он перенаправляется далее согласно маршрутам, указанным в системной таблице маршрутизации. Администратор может изменять номер правила балансировка, перемещая его таким образом в списке.

В следующем примере демонстрируется создание правила балансировки, которому может быть назначен номер в интервале от 1 до 9999.

```
fakel@fakel# set load-balancing wan rule 1
Possible completions:
description             Description for this rule
> destination           Destination
exclude                 Exclude packets matching this rule from wan load balance
failover                Enable failover for packets matching this rule from wan
  load balance
inbound-interface       Inbound interface name (e.g., "eth0") [REQUIRED]
+> interface            Interface name [REQUIRED]
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
> limit                 Enable packet limit for this rule
per-packet-balancing    Option to match traffic per-packet instead of the default,
  per-flow
protocol                Protocol to match
> source                Source information
```

Вес сетевого интерфейса

Пример, представленный выше, может быть расширен путем добавления веса сетевым интерфейсам, заданным в правиле балансировки. Предположим, что пропускная способность интерфейса *eth0* больше пропускной способности интерфейса *eth1*. По умолчанию весь исходящий по отношению к маршрутизатору трафик случайным образом распределяется между всеми доступными исходящими сетевыми интерфейсами. Веса могут быть использованы для того, чтобы сделать балансировку определенной.

```
set load-balancing wan rule 1 interface eth0 weight 2
set load-balancing wan rule 1 interface eth1 weight 1
```

Таким образом 66% исходящего трафика будет перенаправляться через сетевой интерфейс *eth0*, а 33% - через сетевой интерфейс *eth1*.

Ограничение пропускной способности

Пропускная способность для исходящего трафика может быть искусственно ограничена посредством использования параметра *limit* для отдельного правила балансировки.

```
set load-balancing wan rule <rule> limit <parameter>
```

Дополнительно с параметром *limit* могут быть указаны следующие параметры:

- *threshold* - пороговое значение пропускной способности. Указывается в формате *ДО* (*below*) и *ОТ* (*above*) определенного значения;
- *period* - период времени, за который выполняется расчет. Возможные значения - *second* (по умолчанию), *minute*, *hour*;
- *burst* - количество сетевых пакетов, допустимое для превышения порогового значения пропускной способности в рамках заданного периода времени (*period*);
- *rate* - количество сетевых пакетов. Значение по умолчанию - 5.

Балансировка пакетов или потоков

Для исходящего трафика по умолчанию выполняется балансировка потоков целиком. Для работы в таком режиме используется механизм отслеживания соединений по IP адресам отправителя и получателя, а также по номерам портов отправителя и получателя. Каждый поток ассоциируется с определенным сетевым интерфейсом в соответствии с заданными правилами балансировки, в результате чего все сетевые пакеты, соответствующие данному потоку перенаправляются через этот интерфейс. Преимуществом данного режима работы является сохранение порядка пакетов при использовании разных скоростей передачи данных для разных подключений.

Балансировка пакетов для исходящего трафика позволяет достичь лучших показателей, но только в случае, если нарушение порядка пакетов не влияет на работоспособность сетевой инфраструктуры. Данный режим может быть активирован для отдельного правила балансировки с помощью параметра *per-packet-balancing*.

```
set load-balancing wan rule <rule> per-packet-balancing
```

Исключение трафика из балансировки

В некоторых случаях может возникнуть необходимость исключить трафик из балансировки. Это может быть сделано посредством использования параметра *exclude* для отдельного правила балансировки.

```
set load-balancing wan rule <rule> exclude
```

В результате при совпадении данных трафика и классификатора такого правила к этому трафику не применяется балансировки, а сам он маршрутизируется согласно записям в системной таблице маршрутизации.

Контроль работоспособности

Работоспособность WAN каналов (сетевых интерфейсов и путей прохождения трафика), используемых сервисом балансировки, периодически проверяется посредством:

- Отправки сообщения *ICMP Echo Request* удаленным хостам
- Контроля времени жизни сетевого пакета (TTL)
- Выполнения специального пользовательского скрипта.

Если WAN канал не проходит проверку, он исключается из списка используемых сервисом балансировки. Для включения проверки WAN канала необходимо использовать команду *set load-balancing wan interface-health <interface>*.

```
fakel@fakel# set load-balancing wan interface-health <interface>
Possible completions:
failure-count    Failure count
nexthop          Outbound interface nexthop address. Can be 'dhcp or ip address'
  [REQUIRED]
success-count    Success count
+> test          Rule number
```

Для обеспечения выполнения проверки необходимо указать адрес шлюза, через который будет доступен хост-получатель. Параметр *ipv4-address* может принимать значение *dhcp*.

```
set load-balancing wan interface-health <interface> nexthop <ipv4-address>
```

Необходимо также задать количество неудачных результатов проверки, по достижении которого WAN канал будет помечен, как недоступный, и количество успешных проверок, по достижению которого WAN канал будет снова отмечен, как доступный. Количество данных проверок задается с помощью параметров *failure-count* и *success-count* соответственно. Допустимые значения данных параметров находятся в диапазоне от 1 до 10. Значение по умолчанию - 1.

```
set load-balancing wan interface-health <interface> failure-count <number>
set load-balancing wan interface-health <interface> success-count <number>
```

Каждая проверка настраивается для отдельного хоста-получателя и подразумевает выполнение соответствующего конфигурации теста. В случае, если необходимо выполнять проверку с использованием нескольких хостов-получателей, необходимо сконфигурировать несколько тестов, каждый из которых будет выполняться в определенном порядке.

```
fakel@fakel# set load-balancing wan interface-health eth1 test 0
Possible completions:
resp-time    Ping response time (seconds)
target       Health target address
test-script  Path to user defined script
ttl-limit    Ttl limit (hop count)
type         WLB test type
```

При настройке тестов необходимо задать следующие параметры:

- *resp-time* - максимальное время ожидания ответа на сообщение *ICMP Echo Request* в секундах. Допустимые значения находятся в диапазоне от 1 до 30. Значение по умолчанию - 5;
- *target* - идентификатор хоста-получателя, в адрес которого будут отправляться сообщения *ICMP Echo Request*. Допустимые значения - адрес IPv4 или символьное имя хоста;
- *test-script* - пользовательский скрипт, описывающий характер проверки. Скрипт должен возвращать 0 для обозначения успешного результата и отличное от 0 значение - для неудачного результата. Стандартное расположение скриптов - `/config/scripts`. При использования нестандартного расположения необходимо указывать полный путь до файла скрипта;
- *ttl-limit* - количество переходов между каждой парой шлюзов на пути к хосту-получателю, которое используется для тестов с использованием протокола UDP и атрибута TTL. Критерием успешности является получение в ответ сообщения *ICMP Time Expired*. Значение по умолчанию - 1;
- *type* - тип теста. Допустимое значение - одно из списка (*ping*, *ttl*, *script*).

Трансляция адреса отправителя

По умолчанию при балансировке WAN каналов IP адрес отправителя каждого исходящего сетевого пакета с запросом заменяется IP адресом соответствующего сетевого интерфейса для того, чтобы обеспечить получение ответа на тот же сетевой интерфейс. Это достигается за счет автоматической генерации правил трансляции адреса отправителя (SNAT), которые применяются только к трафику, к которому был применен механизм балансировки. В случаях, когда такое поведение является нежелательным, механизм автоматической генерации правил SNAT может быть отключен.

```
set load-balancing wan disable-source-nat
```

Привязанные соединения

Входящие соединения могут некорректно обрабатываться WAN каналами при отправке ответа на запрос клиента.

При получении на определенном сетевом интерфейсе входящего сетевого пакета с запросом от клиента может потребоваться, чтобы пакет с ответом отправлялся с того же сетевого интерфейса. Это достигается за счет использования параметра *sticky-connections* при настройке балансировке WAN каналов.

```
set load-balancing wan sticky-connections inbound
```

Отказоустойчивость

В режиме отказоустойчивости один из WAN каналов и соответствующий ему сетевой интерфейс объявляется активным, а остальные - резервными. В этом случае вместо балансировки трафика между всеми работоспособными WAN каналами трафик передается только по активному. В случае отказа активного WAN канала на эту роль выбирается другой из списка резервных на основе состояния и веса интерфейса. Оставшиеся WAN каналы становятся резервными по отношению к новому активному. Роли WAN каналов и соответствующих им интерфейсов могут быть также выбраны на основе порядка правил балансировки, для которых необходимо указывать параметр *failover*.

```
set load-balancing wan rule <number> failover
```

Так как перераспределение установленных ранее сессий между активным и резервными WAN каналами автоматически не выполняется, необходимо производить очистку таблицы соединений с помощью команды *flush-connections* при каждом изменении состояния соединения.

```
set load-balancing wan flush-connections
```

Предупреждение

Очистка таблица соединений приведет к тому, что будет выполняться балансировка пакетов вместо балансировки потоков до момента повторного установления соединений.

2.7.2.2 Настройка

Пример настройки

В качестве примера рассмотрим ситуацию, когда есть два сетевых интерфейса WAN, сконфигурированных по протоколу DHCP, и один LAN интерфейс (*eth2*).

```
set load-balancing wan interface-health eth0 nexthop 'dhcp'
set load-balancing wan interface-health eth1 nexthop 'dhcp'
set load-balancing wan rule 1 inbound-interface 'eth2'
set load-balancing wan rule 1 interface eth0
set load-balancing wan rule 1 interface eth1
```

2.7.2.3 Список команд

Основные настройки

- `set load-balancing wan interface-health <interface>`

  Активирует механизм проверки WAN канала для внешнего интерфейса маршрутизатора *<interface>*.

- `set load-balancing wan interface-health <interface> nexthop <address|dhcp>`

  Задает адрес следующего маршрутизатора *<address|dhcp>*, который будет использован для проверки состояния канала.

- `set load-balancing wan rule <rule>`

  Создает правило *<id>* для балансировки WAN интерфейсов.

- `set load-balancing wan rule <rule> inbound-interface <interface>`

  Определяет внутренний LAN интерфейс *<interface>* для правила балансировки *<rule>*.

- `set load-balancing wan rule <rule> interface <interface>`

  Определяет внешний WAN интерфейс *<interface>* для правила балансировки *<rule>*.

- `set load-balancing wan rule <rule> interface <interface> weight <number>`

  Задает вес *<number>* внешнего WAN интерфейса *<interface>* для правила балансировки *<rule>*.

- `set load-balancing wan rule <rule> limit <parameter>`

  Задает значение *<parameter>* ограничения пропускной способности для исходящего трафика в правиле балансировки *<rule>*.

- `set load-balancing wan rule <rule> per-packet-balancing`

  Активирует механизм балансировки пакетов для исходящего трафика в определенном правиле балансировки *<rule>*

- `set load-balancing wan rule <rule> exclude`

  Исключает трафик, определенный в правиле *<rule>* из балансировки.

- `set load-balancing wan interface-health <interface> failure-count <number>`

  Задает количество неудачных результатов проверки <*number*>, по достижении которого WAN канал будет помечен, как недоступный. Допустимые значения данного параметра находятся в диапазоне от 1 до 10. Значение по умолчанию - 1.

- `set load-balancing wan interface-health <interface> success-count <number>`

  Задает количество успешных результатов проверки <*number*>, по достижению которого WAN канал будет снова отмечен, как доступный. Допустимые значения данного параметра находятся в диапазоне от 1 до 10. Значение по умолчанию - 1.

- `set load-balancing wan interface-health <interface> test <number>`

  Создает тест <number> для проверки работоспособности канала внешнего интерфейса маршрутизатора <interface>.

- `set load-balancing wan interface-health <interface> test <id> resp-time <number>`

  Задает значение максимального времени ожидания ответа на сообщение *ICMP Echo Request* в секундах. Допустимые значения находятся в диапазоне от 1 до 30. Значение по умолчанию - 5.

- `set load-balancing wan interface-health <interface> test <id> target <text>`

  Задает идентификатор хоста-получателя, в адрес которого будут отправляться сообщения ICMP Echo Request. Допустимые значения - адрес IPv4 или символьное имя хоста.

- `set load-balancing wan interface-health <interface> test <id> test-script <text>`

  Добавляет пользовательский скрипт <*text*>, описывающий характер проверки. Скрипт должен возвращать 0 для обозначения успешного результата и значение отличное от 0 - для неудачного результата. Стандартное расположение скриптов - /config/scripts. При использования нестандартного расположения необходимо указывать полный путь до файла скрипта.

- `set load-balancing wan interface-health <interface> test <id> ttl-limit <number>`

  Определяет количество переходов между каждой парой шлюзов на пути к хосту-получателю, которое используется для тестов с использованием протокола UDP и атрибута TTL. Критерием успешности является получение в ответ сообщения ICMP Time Expired. Значение по умолчанию - 1;

- `set load-balancing wan interface-health <interface> test <id>  type <ping|ttl|script>`

  Определяет тип теста. Допустимое значение - ping, ttl, script.

- `set load-balancing wan disable-source-nat`

  Отключает настройки правил SNAT для механизма балансировки WAN каналов.

- `set load-balancing wan sticky-connections inbound`

  Активирует механизм привязки соединения к конкретному интерфейсу. При получении на определенном сетевом интерфейсе входящего сетевого пакета с запросом от клиента, пакет с ответом отправлялся с того же сетевого интерфейса.

- `set load-balancing wan rule <number> failover`

  Активирует режим отказоустойчивости для правила балансировки <number>.

- `set load-balancing wan flush-connections`

  Выполняет очистку таблицы соединений при изменении состояния активного канала WAN.

- `restart wan-load-balance`

  Выполняет перезапуск сервиса балансировки.

Мониторинг

- `show wan-load-balance`

  Выводит информацию о работе сервиса балансировки, включая типы тестов и список хостов-получателей.

  При выводе на экран соответствующей информации используются следующие символы для обозначения результатов тестов:

  - + - тест пройден успешно;
  - - - тест не пройден из-за ошибки;
  - пустое значение - ни один из тестов не пройден

  Пример работы команды show wan-load-balance:

```
fakel@fakel:~$ show wan-load-balance
Interface:  eth0
Status:  failed
Last Status Change:  Tue Jun 11 20:12:19 2019
- Test:  ping  Target:
    Last Interface Success: 55s
    Last Interface Failure: 0s
    # Interface Failure(s): 5

Interface:  eth1
Status:  active
Last Status Change:  Tue Jun 11 20:06:42 2019
+ Test:  ping  Target:
    Last Interface Success: 0s
    Last Interface Failure: 6m26s
    # Interface Failure(s): 0
```

- `show wan-load-balance connection`

  Выводит информацию о трафике, к которому был применен механизм балансировки.

  Пример работы команды show wan-load-balance connection:

```
fakel@fakel:~$ show wan-load-balance connection
conntrack v1.4.2 (conntrack-tools): 3 flow entries have been shown.
Type    State           Src                     Dst                     Packets
  Bytes
tcp     TIME_WAIT       10.1.1.13:38040         203.0.113.2:80          203.0.113.2
   192.168.188.71
udp                     10.1.1.13:41891         198.51.100.3:53
  198.51.100.3 192.168.188.71
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
udp                     10.1.1.13:55437         198.51.100.3:53
  198.51.100.3 192.168.188.71
```

2.8 Сервисы

- ***Сервисные механизмы*** **(страница 681)**
  - *Удаленное управление по протоколу SSH* (страница 682)
  - *Протокол SNMP* (страница 693)
  - *Протокол ARP* (страница 699)
  - *Отслеживание соединений* (страница 702)
  - *Консольный сервер* (страница 707)
  - *DHCP сервер* (страница 713)
  - *Ретранслятор DHCP* (страница 710)
  - *Перенаправляющий DNS сервер* (страница 726)
  - *Динамический DNS* (страница 730)
  - *Широковещательная ретрансляция UDP* (страница 700)
- ***Системные механизмы*** **(страница 733)**
  - *Информация об устройстве* (страница 737)
  - *Протокол сетевого времени* (страница 735)
  - *Системный DNS* (страница 734)
  - *Управление пользователями* (страница 739)

2.8.1 Сервисные механизмы

2.8.1.1 Удаленное управление по протоколу SSH

Обзор

SSH — сетевой протокол прикладного уровня для организации удаленного и безопасного соединения между клиентом и сервером.

Соединение по SSH позволяет безопасно подключаться к маршрутизатору Факел, управлять системой, удаленно выполнять команды, прокладывать TCP-туннели для передачи данных и т.д.

Перед установлением SSH-соединения клиент и сервер связываются по протоколу TCP и договариваются о том, какие алгоритмы будут использоваться для шифрования связи, обмена SSH-ключами и т.п.

Далее запускается процесс обмена SSH-ключами. В результате клиент получает закрытый ключ, а сервер — открытый. Для установления SSH-соединения необходимо, чтобы открытый ключ соответствовал закрытому. После того как клиент и сервер успешно обменялись ключами, SSH-сессия готова к запуску.

После установления SSH-соединения администратор сможет настроить метод аутентификации. Доступна аутентификация по паролю, по ключевой паре или по IP-адресу (не рекомендуется).

По умолчанию для подключения и передачи файлов по SSH используется TCP-порт 22. При настройке SSH-службы администратор может изменить номер TCP-порта на любой другой.

Пример настройки

Шаг	Команда	Описание
1	set service ssh port 2022	Указывает порт 2022, на котором будет работать служба SSH
2	set service ssh listen-address 192.168.100.2	Задает IP-адрес 192.168.100.2, на котором будет прослушиваться работа SSH-сервера
3	set service ssh access-control allow user new_user	Назначает пользователя new_user, которому будет разрешен удаленный доступ по протоколу SSH
4	set system login user new_user authentication plaintext-password	Устанавливает метод аутентификации по паролю для пользователя new_user

Список команд

Режим «Конфигурирование»

service ssh port <port>

Описание:

Указывает порт, на котором будет работать служба SSH.

Синтаксис:

- set service ssh port <port>

- delete service ssh port <port>
- show service ssh port

Аргументы:

- <port> — номер порта, на котором будет работать служба SSH. Формат: целое число. Диапазон значений: от 1001 до 65535.

Режим: «Конфигурирование».

---

service ssh listen-address <address>

Описание:

Задает IP-адрес, на котором будет прослушиваться работа SSH-сервера.

Синтаксис:

- set service ssh listen-address <address>
- delete service ssh listen-address <address>
- show service ssh listen-address

Аргументы:

- <address> — IP-адрес, на котором будет прослушиваться работа SSH-сервера. Можно задать несколько значений.

Режим: «Конфигурирование».

---

service ssh ciphers <cipher>

Описание:

Устанавливает алгоритм шифрования SSH-соединения.

Синтаксис:

- set service ssh ciphers <cipher>
- delete service ssh ciphers <cipher>
- show service ssh ciphers

Аргументы:

- <cipher> — алгоритм шифрования SSH-соединения. Можно задать несколько значений.

  Поддерживаемые значения: 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, arcfour128, arcfour256, arcfour, blowfish-cbc, cast128-cbc

Режим: «Конфигурирование».

---

service ssh disable-password-authentication

Описание:

Отключает аутентификацию на основе пароля. Пользователи смогут установить SSH-соединение только с помощью SSH-ключа.

Синтаксис:

- set service ssh disable-password-authentication
- delete service ssh disable-password-authentication
- show service ssh

Режим: «Конфигурирование».

---

service ssh disable-host-validation

Описание:

Отключает проверку хоста через обратный DNS-запрос.

Синтаксис:

- set service ssh disable-host-validation
- delete service ssh disable-host-validation
- show service ssh

Режим: «Конфигурирование».

Совет

Если проверка через обратный запрос недоступна, отключите проверку хоста. Это ускорит время входа в систему.

---

service ssh mac <mac>

Описание:

Устанавливает MAC-алгоритм, чтобы защитить целостность данных при передаче по протоколу SSH.

Синтаксис:

- set service ssh macs `<mac>`
- delete service ssh macs `<mac>`
- show service ssh macs

Аргументы:

- <mac> — тип MAC-алгоритма. Можно задать несколько значений.

  Поддерживаемые значения: `hmac-md5, hmac-md5-96, hmac-ripemd160, hmac-sha1, hmac-sha1-96, hmac-sha2-256, hmac-sha2-512, umac-64@openssh.com, umac-128@openssh.com, hmac-md5-etm@openssh.com, hmac-md5-96-etm@openssh.com, hmac-ripemd160-etm@openssh.com, hmac-sha1-etm@openssh.com, hmac-sha1-96-etm@openssh.com, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, umac-64-etm@openssh.com, umac-128-etm@openssh.com`

Режим: «Конфигурирование».

---

service ssh access-control <allow | deny> <group | user> <name>

Описание:

Разрешает или запрещает пользователю или группе пользователей подключаться удаленно по протоколу SSH.

Синтаксис:

- set service ssh access-control `<allow | deny> <group | user> <name>`
- delete service ssh access-control `<allow | deny> <group | user> <name>`
- show service ssh access-control

Аргументы:

- `<allow>` — разрешает пользователю или группе пользователей удаленно подключаться по SSH;
- <deny> — запрещает пользователю или группе пользователе удаленно подключаться по SSH;
- `<group>` — название группы пользователей;
- `<user>` — имя пользователя.

Режим: «Конфигурирование».

---

service ssh client-keepalive-interval <interval>

Описание:

Задает интервал отправки keepalive-сообщений от сервера к клиенту.

Синтаксис:

- set service ssh client-keepalive-interval `<interval>`
- delete service ssh client-keepalive-interval `<interval>`
- show service ssh client-keepalive-interval

Аргументы:

- `<interval>` — интервал между отправкой keepalive-сообщений. Формат: секунды.

Режим: «Конфигурирование».

---

service ssh key-exchange <kex>

Описание:

Устанавливает алгоритм обмена ключами, который будет использоваться для аутентификации по SSH.

Синтаксис:

- set service ssh key-exchange <kex>
- delete service ssh key-exchange <kex>
- show service ssh key-exchange

Аргументы:

- <kex> — тип алгоритма для обмена ключами.

  Поддерживаемые значения: `diffie-hellman-group1-sha1`, `diffie-hellman-group14-sha1`, `diffie-hellman-group14-sha256`, `diffie-hellman-group16-sha512`, `diffie-hellman-group18-sha512`, `diffie-hellman-group-exchange-sha1`, `diffie-hellman-group-exchange-sha256`, `ecdh-sha2-nistp256`, `ecdh-sha2-nistp384`, `ecdh-sha2-nistp521`, `curve25519-sha256`, `curve25519-sha256@libssh.org`

Режим: «Конфигурирование».

---

service ssh loglevel <quiet | fatal | error | info | verbose>

Описание:

Задает уровень журналирования для службы SSHD.

Синтаксис:

- set service ssh loglevel `<quiet | fatal | error | info | verbose>`
- delete service ssh loglevel `<quiet | fatal | error | info | verbose>`
- show service ssh loglevel

Аргументы:

- `<quiet>` — никакие записи из журнала регистрации событий не будут отображаться;
- `<fatal>` — будут отображаться только критические ошибки из журнала регистрации событий;
- `<error>` — будут отображаться только средние и критические ошибки из журнала регистрации событий;

- <info> — будут отображаться все записи из журнала регистрации событий. Значение по умолчанию;
- <verbose> — будут отображаться только записи неудачных попыток входа в систему.

Режим: «Конфигурирование».

---

service ssh vrf <name>

Описание:

Устанавливает службу SSH на VRF-экземпляр.

Синтаксис:

- set service ssh vrf <name>
- delete service ssh vrf <name>
- show service ssh vrf

Аргументы:

- <name> — имя VRF-экземпляра.

Режим: «Конфигурирование».

---

service ssh pubkey-accepted-algorithm <name>

Описание:

Устанавливает подписной алгоритм, который будет использоваться для аутентификации открытого ключа.

Синтаксис:

- set service ssh pubkey-accepted-algorithm <name>
- delete service ssh pubkey-accepted-algorithm <name>
- show service ssh pubkey-accepted-algorithm

Аргументы:

- <name> — тип подписного алгоритма.

  Поддерживаемые значения: `ssh-ed25519, ssh-ed25519-cert-v01@openssh.com, sk-ssh-ed25519@openssh.com, sk-ssh-ed25519-cert-v01@openssh.com, ecdsa-sha2-nistp256, ecdsa-sha2-nistp256-cert-v01@openssh.com, ecdsa-sha2-nistp384, ecdsa-sha2-nistp384-cert-v01@openssh.com, ecdsa-sha2-nistp521, ecdsa-sha2-nistp521-cert-v01@openssh.com, sk-ecdsa-sha2-nistp256@openssh.com, sk-ecdsa-sha2-nistp256-cert-v01@openssh.com, webauthn-sk-ecdsa-sha2-nistp256@openssh.com, ssh-dss,`

```
ssh-dss-cert-v01@openssh.com, ssh-rsa, ssh-rsa-cert-v01@openssh.
com, rsa-sha2-256, rsa-sha2-256-cert-v01@openssh.com, rsa-sha2-512,
rsa-sha2-512-cert-v01@openssh.com
```

Режим: «Конфигурирование».

---

service ssh dynamic-protection

Описание:

Включает динамическую защиту SSH-соединения.

Синтаксис:

- set service ssh dynamic protection
- delete service ssh dynamic protection
- show service ssh dynamic protection

Режим: «Конфигурирование».

---

service ssh dynamic-protection allow-from <address | prefix>

Описание:

Задает список IP-адресов и сетей, которым всегда будет разрешен доступ к SSH-серверу.

Синтаксис:

- set service ssh dynamic-protection allow-from `<address | prefix>`
- delete service ssh dynamic-protection allow-from `<address | prefix>`
- show service ssh dynamic-protection allow-from

Аргументы:

- `<address>` — IP-адрес;
- `<prefix>` — префикс сети.

Режим: «Конфигурирование».

---

service ssh dynamic-protection block-time <sec>

Описание:

Блокирует IP-адрес источника на заданное время.

Синтаксис:

- set service ssh dynamic protection block-time <sec>
- delete service ssh dynamic protection block-time <sec>
- show service ssh dynamic protection block-time

Аргументы:

- <sec> — время блокировки IP-адреса источника. Формат: секунды. Значение по умолчанию: 120 секунд. Время каждой последующей блокировки увеличивается в 1,5 раза.

Режим: «Конфигурирование».

---

service ssh dynamic-protection detect-time <sec>

Описание:

Запоминает IP-адрес источника на заданное время перед сбросом его оценки.

Синтаксис:

- set service ssh dynamic-protection detect-time <sec>
- delete service ssh dynamic-protection detect-time <sec>
- show service ssh dynamic-protection detect-time

Аргументы:

- <sec> — время запоминания IP-адреса источника. Формат: секунды. Значение по умолчанию: 1800 секунд.

Режим: «Конфигурирование».

---

service ssh dynamic-protection threshold <sec>

Описание:

Блокирует IP-адрес источника на заданное время, когда совокупное количество атак превышает порог.

Синтаксис:

- set service ssh dynamic-protection threshold <sec>
- delete service ssh dynamic-protection threshold <sec>
- show service ssh dynamic-protection threshold

Аргументы:

- <sec> — время блокировки IP-адрес источника. Формат: секунды. Значение по умолчанию: 30 секунд.

Режим: «Конфигурирование».

Режим «Администрирование»

restart ssh

Описание:

Перезапускает службу SSHD в фоновом режиме. Не влияет на активную сессию.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

generate ssh server-key

Описание:

Заново генерирует фрагменты открытого и закрытого SSH-ключей.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

> **Важно**
>
> После выполнения команды обновите файлы known_hosts в клиенте, поскольку команда сгенерирует новый открытый SSH-ключ.

---

generate ssh client-key /path/to/private_key

Описание:

Генерирует новую пару открытого и закрытого SSH-ключей и записывает их значения в указанный файл. Если ключи с таким именем уже созданы, то они будут перезаписаны ключами с новыми значениями.

Аргументы:

- `/path/to/private_key` — путь к директории, в которую будут сохранены файлы открытого и закрытого SSH-ключей.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

generate public-key-command user <username> path <location>

Описание:

Генерирует команды, которые позволят использовать открытый SSH-ключ со встроенной аутентификацией. Первой сгенерированной командой будет `configure`, поскольку для выполнения остальных сгенерированных команд потребуется вход в режим «Конфигурирование».

Аргументы:

- `<username>` — имя пользователя;
- `<location>` — адрес, по которому будет сохранен открытый SSH-ключ. Может быть как локальной директорией, так и URL-адресом. Поддерживаемые протоколы: FTP, FTPS, HTTP, HTTPS, SCP/SFTP, TFTP.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log ssh

Описание:

Отображает записи журнала регистрации событий на SSH-сервере.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

monitor log ssh

Описание:

Следит за появлением новых записей в журнале регистрации событий на SSH-сервере.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show log ssh dynamic-protection

Описание:

Отображает записи журнала регистрации событий для SSH-соединения с динамической защитой.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

monitor log ssh dynamic-protection

Описание:

Следит за появлением новых записей в журнале регистрации событий для SSH-соединения с динамической защитой.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show ssh dynamic-protection

Описание:

Отображает список IP-адресов, которые в настоящий момент заблокированы динамической защитой SSH-соединения.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show ssh fingerprints

Описание:

Отображает отпечаток открытого SSH-ключа для SSH-сервера.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

---

show ssh fingertips ascii

Описание:

Отображает отпечаток и ASCII-графику открытого SSH-ключа для SSH-сервера.

Режим: «Администрирование».

Уровень привилегий: «Администратор».

2.8.1.2 Протокол SNMP

Описание

SNMP (Simple Network Management Protocol) — это стандартный протокол, который применяется для мониторинга и управления сетевыми устройствами. К устройствам, которые обычно поддерживают SNMP, относятся кабельные модемы, маршрутизаторы, коммутаторы, серверы, рабочие станции, принтеры и т.д.

Протокол SNMP широко используется в сетевом управлении для мониторинга сети. Протокол предоставляет управляющие данные в виде переменных в системах, организованных в базе управленческой информации MIB (Management Information Base), которые описывают состояние и конфигурацию системы. Затем эти переменные могут быть запрошены удаленно (и в некоторых случаях изменены) управляющими приложениями.

Существуют три основные версии протокола SNMP. SNMPv1 — это начальная версия протокола. Более поздние версии, SNMPv2c и SNMPv3, содержат улучшения в производительности, гибкости и безопасности. SNMP является компонентом пакета интернет-протоколов, определенного Рабочей группой разработчиков Интернета IETF (Internet Engineering Task Force). Пакет состоит из набора стандартов для управления сетью, включая протокол прикладного уровня, схему базы данных и набор объектов данных.

Основные понятия

При обычном использовании SNMP на одном или нескольких устройствах управления, называемых менеджерами, выполняются задачи мониторинга или управления группой узлов или устройством в компьютерной сети. Каждая управляемая система содержит программный компонент, называемый агентом, который передает информацию менеджеру по протоколу SNMP.

Сеть, управляемая по протоколу SNMP, состоит из трех ключевых компонентов:

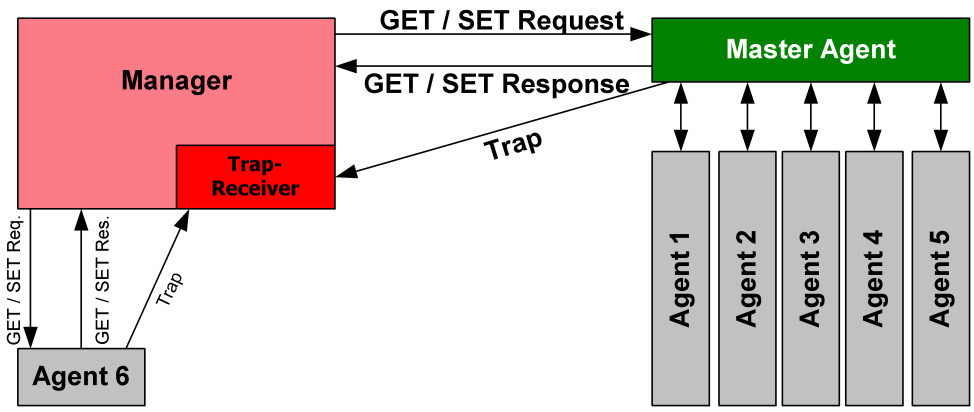
- Управляемые устройства;
- Агент — программное обеспечение, работающее на управляемых устройствах;
- Станция сетевого управления (NMS) — управляющее программное обеспечение.

Управляемое устройство — это сетевой узел, в котором реализован интерфейс SNMP, обеспечивающий однонаправленный (только чтение) или двунаправленный (чтение и запись) доступ к специфической информации узла. Управляемые устройства обмениваются информацией о конкретном узле с NMS. Иногда называемые сетевыми элементами, управляемые устройства могут быть любого типа, в частности, маршрутизаторы, серверы доступа, коммутаторы, кабельные модемы, мосты, концентраторы, IP-телефоны, IP-видеокамеры, компьютерные узлы и принтеры.

Агент — это программный модуль сетевого управления, который находится на управляемом устройстве. Агент обладает локальными знаниями об управляющей информации и переводит ее в специальную форму SNMP или из нее.

Станция управления сетью выполняет задачи мониторинга и управления подключенными устройствами. Для управления сетью NMS требует большую часть ресурсов обработки и памяти. В любой управляемой сети может существовать одна или несколько NMS.

SNMP поддерживает как IPv4, так и IPv6.



Версии протокола SNMP

ПО Факел поддерживает SNMPv2 (версия 2) и SNMPv3 (версия 3), причем SNMPv3 рекомендуется из-за повышенной безопасности (аутентификация и шифрование).

SNMPv2

SNMPv2 — наиболее часто используемая версия. Для авторизации клиентов SNMP использует концепцию сообществ (community). Сообщества могут иметь авторизацию только на чтение (это наиболее распространенный вариант) или на чтение и запись. SNMP может работать синхронно или асинхронно. При синхронной связи система мониторинга периодически опрашивает маршрутизатор. При асинхронном — маршрутизатор отправляет хосту мониторинга уведомления «ловушки» (trap). SNMPv2 не поддерживает никаких механизмов аутентификации, кроме адреса источника клиента, поэтому необходимо указать адреса клиентов, которым разрешен мониторинг маршрутизатора. Обратите внимание, что SNMPv2 также не поддерживает шифрование и всегда отправляет данные в виде обычного текста.

Основные настройки SNMPv2

- `set service snmp community routers authorization ro`

  Определяет сообщество `routers` с авторизацией только на чтение.

- `set service snmp community routers network 192.0.2.0/24`
- `set service snmp community routers network 2001::db8:ffff:eeee::/64`

  Подключение к мониторингу из сетей `192.0.2.0/24`, `2001::db8:ffff:eeee::/64`.

- `set service snmp community routers client 203.0.113.10`
- `set service snmp community routers client 203.0.113.20`

  Разрешение доступа к мониторингу с адресов `203.0.113.10`, `203.0.113.20`.

- `set service snmp location "Moscow"`
- `set service snmp contact "example@example.ru"`

  Добавление дополнительной информации о маршрутизаторе.

- `set service snmp trap-target 203.0.113.10`

  Определение отправления `trap`, если это необходимо.

- `set service snmp listen-address 172.16.254.36 port 161`
- `set service snmp listen-address 2001:db8::f00::1`

  Назначение определенных портов и адресов для прослушивания. По умолчанию используется порт 161.

SNMPv3

В протоколе SNMPv3 (версия 3) представлен целый ряд новых функций, связанных с безопасностью, которые отсутствовали в предыдущих версиях. Безопасность была одним из самых слабых мест SNMP до версии 3. Аутентификация в SNMP версий 1 и 2 представляет собой не более чем пароль (строка сообщества), передаваемый открытым текстом между менеджером и агентом. Каждое сообщение SNMPv3 содержит параметры безопасности, которые кодируются в виде октетной строки. Значение этих параметров безопасности зависит от используемой модели безопасности. Подход к обеспечению безопасности в SNMPv3 направлен на:

- Конфиденциальность. Шифрует и предотвращает прослушивание неавторизованным источником;
- Целостность. Предотвращает подделку пакета во время передачи и включает дополнительный механизм защиты от воспроизведения пакетов;
- Аутентификация. Проверяет, что сообщение получено от достоверного источника.

Для примера настроим демона SNMP для прослушивания с адреса `192.0.2.1`. Создадим пользователя `fakel` с паролем `fakel12345678`. Новый пользователь будет использовать протоколы SHA/AES для аутентификации и обеспечения конфиденциальности.

```
set service snmp listen-address 192.0.2.1
set service snmp location 'Fakel Datacenter'
set service snmp v3 engineid '000000000000000000000002'
set service snmp v3 group default mode 'ro'
set service snmp v3 group default view 'default'
set service snmp v3 user fakel auth plaintext-password 'fakel12345678'
set service snmp v3 user fakel auth type 'sha'
set service snmp v3 user fakel group 'default'
set service snmp v3 user fakel privacy plaintext-password 'fakel12345678'
set service snmp v3 user fakel privacy type 'aes'
set service snmp v3 view default oid 1
```

После добавления паролей в настройки в открытом виде, они будут захэшированы и сохранены в вашей конфигурации. Итоговая конфигурация CLI будет выглядеть следующим образом:

```
Fakel@fakel# show service snmp
 listen-address 192.0.2.1 {
 }
 location ”Fakel Datacenter”
 v3 {
     engineid 000000000000000000000002
     group default {
         mode ro
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
        view default
    }
    user fakel {
        auth {
            encrypted-password 4e52fe55fd011c9c51ae2c65f4b78ca93dcafdfe
            type sha
        }
        group default
        privacy {
            encrypted-password 4e52fe55fd011c9c51ae2c65f4b78ca93dcafdfe
            type aes
        }
    }
    view default {
        oid 1 {
        }
    }
}
```

Чтобы проверить корректную настройку SNMPv3 с любой системы на базе Linux, выполните следующую команду:

- `snmpwalk -v 3 -u fakel -a SHA -A fakel12345678 -x AES -X fakel12345678 -l authPriv 192.0.2.1 .1`

Чтобы расширить функциональность SNMP-агента, можно выполнять пользовательские сценарии при каждом вызове агента. Для этого используйте команды расширения. Необходимо создать функциональный скрипт, затем загрузить его в **ПО Факел** командой `scp <your_script.sh> fakel@fakel:/config/user-data`. После того как скрипт загружен, его нужно настроить с помощью команды ниже.

- `set service snmp script-extensions extension-name my-extension script your_script.sh`
- `commit`

OID `.1.3.6.1.4.1.8072.1.3.2.3.1.1.4.116.101.115.116` после вызова будет содержать вывод расширения

```
root@fakel:/home/fakel# snmpwalk -v2c  -c public 127.0.0.1 nsExtendOutput1
NET-SNMP-EXTEND-MIB::nsExtendOutput1Line."my-extension" = STRING: hello
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."my-extension" = STRING: hello
NET-SNMP-EXTEND-MIB::nsExtendOutNumLines."my-extension" = INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendResult."my-extension" = INTEGER: 0
```

Мониторинг устройств в Zabbix

Импорт шаблона в Zabbix

Для мониторинга по SNMP в Zabbix можно использовать шаблон Fakel_by_SNMP:

- YML
- XML
- JSON

Данный шаблон подходит для версии Zabbix 6.0.

Для импорта шаблона в систему мониторинга необходимо зайти в меню раздела Data collection, выбрать вкладку Templates. В правом верхнем углу необходимо нажать на кнопку Import и выбрать скачанный ранее файл в любом разрешении (.xml, .json, .yaml). При необходимости добавить/убрать галочки с импортируемых объектов. Нажать кнопку Import. Импортируемый шаблон загрузится в группу шаблонов Templates/Network device, имя Fakel by SNMP.

Добавление узла на мониторинг

Для добавления нового узла в систему мониторинга необходимо зайти в меню Data collection, выбрать вкладку Hosts.

В правом верхнем углу нажать кнопку Create host.

В появившемся новом окне New host заполнить разделы:

- Host name — уникальное имя хоста для системы мониторинга Zabbix;
- Visible name — при необходимости скорректировать видимое имя узла;
- Templates — в строке поиска вбить имя шаблона Fakel by SNMP и выбрать импортированный шаблон в выпадающем списке;
- Host group — в строке поиска вбить имя группы, в которой будет находиться создаваемый узел. Если группа еще не создана, можно в строке поиска написать новое имя группы и она автоматически создастся в Zabbix в разделе Host group;
- Interface — нажать кнопку add и выбрать SNMP. В появившемся разделе заполнить пункты:
  1. IP address — добавить IP-адрес узла. Если мониторинг будет осуществляться по DNS-имени, то необходимо заполнить пункт DNS name. В пункте Connect to выбрать DNS. При необходимости изменить порт (по умолчанию порт: 161);
  2. В разделе SNMP version выбрать настроенную на устройстве версию SNMP.
  - При выборе SNMPv2 необходимо ввести значение SNMP community, которое настраивалось на маршрутизаторе;
  - При выборе SNMPv3 необходимо заполнить пункты Security name, Security level, выбрать authPriv. В пункте Authentication protocol выбрать один из протоколов MD5/SHA, в пункте Authentication passphrase добавить пароль, который был настроен на устройстве. В пункте Privacy protocol выбрать один из протоколов DES/AES, в пункте Privacy passphrase добавить пароль, который был настроен на устройстве.
- При необходимости снять галочку Use combined requests;

- При необходимости заполнить раздел Description, выбрать из списка Monitored by proxy необходимый proxy-сервер;
- Нажать кнопку Add.

Просмотр информации об узле

Для просмотра информации, полученной по протоколу SNMP, необходимо зайти во вкладку Monitoring, выбрать пункт Hosts. В появившемся списке узлов, стоящих на мониторинге, выбрать необходимый маршрутизатор и левой кнопкой мыши нажать на имя этого узла. В появившемся списке можно выбрать:

- Dashboards — для просмотра общей информации об устройстве (трафик на интерфейсах, загрузка дисков, CPU и т.д.);
- Problems — информация об активных проблемах (триггерах) на узле;
- Last data — вся информация, полученная от устройства по протоколу SNMP по выбранному шаблону;
- Graphs — автоматически созданные графики для выбранного устройства.

Корректировка шаблона или узла

Примечание

Если информация, настроенная в шаблоне, избыточна, можно скорректировать шаблон или элементы данных в выбранном узле или шаблоне.

Для корректировки отображения информации на **одном узле** необходимо зайти во вкладку Data collection, выбрать пункт Hosts. Рядом с выбранным узлом нажать на Items. В появившемся списке поставить галочки рядом с неиспользуемыми элементами данных, внизу нажать кнопку Disable. Деактивированные элементы данных больше не будут отображаться в Latest data. Для корректировки отображения автообнаруженных элементов данных необходимо выбрать Discovery выбранного узла. В появившемся списке напротив нужного Discovery rule выбрать Item prototypes. В появившемся списке в разделах Create enable и Discover в необходимых пунктах поставить значение No. Деактивированные элементы данных не будут отображаться в Latest data.

Для корректировки автообнаруженных элементов или элементов данных **для всех узлов**, использующих шаблон Fakel by SNMP, необходимо зайти в раздел Data collection, выбрать пункт Templates. Рядом с выбранным шаблоном нажать на Items. В появившемся списке поставить галочки рядом с неиспользуемыми элементами данных, внизу нажать кнопку Disable. Деактивированные элементы данных больше не будут отображаться в Latest data. Для корректировки отображения автообнаруженных элементов данных необходимо выбрать Discovery. В появившемся списке напротив нужного Discovery rule выбрать Item prototypes. В появившемся списке в разделах Create enable и Discovery в необходимых пунктах поставить значение No. Деактивированные элементы данных не будут отображаться в Latest data.

2.8.1.3 Протокол ARP

Описание

Протокол ARP (Address Resolution Protocol) является коммуникационным протоколом, который используется для обнаружения адресов канального уровня, таких как MAC адрес, ассоциированных с адресами сетевого уровня, такими как IP адрес. Такая ассоциация является критически важной для обеспечения функционирования стека протоколов IP. Протокол ARP был впервые определен в спецификации **RFC 826**[68], получившей в итоге статус стандарта STD 37.

В сетях, построенных на основе протокола IPv6, функциональность протокола ARP обеспечивается другим протоколом - NDP (Neighbor Discovery Protocol).

Для работы с записями ARP таблицы необходимо использовать команды, описание которых представлено в разделах ниже.

Список команд

Основные настройки

- `set protocols static arp <address> hwaddr <mac>`

  Создает статическую запись в ARP таблице, определяющую постоянную ассоциацию между IP адресом `<address>` и MAC адресом `<mac>`.

Мониторинг состояния

- `show protocols static arp`

  Выводит на экран все записи ARP таблицы по всем интерфейсам.

  Пример работы команды show protocols static arp:

```
fakel@fakel:~$ show protocols static arp
Address      HWtype   HWaddress           Flags Mask   Iface
10.1.1.1     ether    00:53:00:de:23:2e   C            eth1
10.1.1.100   ether    00:53:00:de:23:aa   CM           eth1
```

- `show protocols static arp interface <iface_name>`

  Выводит на экран записи ARP таблицы для конкретного интерфейса `<iface_name>`.

  Пример работы команды show protocols static arp interface eth1:

```
fakel@fakel:~$ show protocols static arp interface eth1
Address      HWtype   HWaddress           Flags Mask   Iface
10.1.1.1     ether    00:53:00:de:23:2e   C            eth1
10.1.1.100   ether    00:53:00:de:23:aa   CM           eth1
```

[68] https://datatracker.ietf.org/doc/html/rfc826.html

2.8.1.4 Широковещательная ретрансляция UDP

Описание

Некоторые производители используют широковещательные рассылки для идентификации своего оборудования в пределах одного сегмента локальной сети. При разделении сети на несколько сегментов (VLAN) теряется возможность идентификации оборудования.

Для того, чтобы решить проблему обмена широковещательными UDP сообщения между различными сегментами локальной сети используется механизм широковещательной ретрансляция UDP (UDP broadcast relay).

Каждый UDP-порт, который будет заниматься обменом широковещательными UDP сообщениями, требует одного уникального идентификатора. **ПО Факел** поддерживаем 99 идентификаторов.

Настройка

Пример настройки

Пример настройки пересылки широковещательных пакетов, полученных на UDP-порт 1900 сетевых интерфейсов *eth3*, *eth4* или *eth5*, на все остальные сетевые интерфейсы интерфейсы.

Список команд для настройки:

```
set service broadcast-relay id 1 description 'SONOS'
set service broadcast-relay id 1 interface 'eth3'
set service broadcast-relay id 1 interface 'eth4'
set service broadcast-relay id 1 interface 'eth5'
set service broadcast-relay id 1 port '1900'
```

Список команд

Основные настройки

- `set service broadcast-relay id <n> description <description>`

  Добавляет описание `<description>` для каждого уникального идентификатора `<n>` сервиса широковещательной ретрансляции. Описание удобно использовать, когда в системе настроено нескольких различных портов или приложений.

- `set service broadcast-relay id <n> interface <interface>`

  Определяет интерфейс, который будет использоваться для приема и ретрансляции отдельных широковещательных пакетов.

- `set service broadcast-relay id <n> address <ipv4-address>`

  Устанавливает IP-адрес источника `<ipv4-address>` пересылаемых пакетов, в противном случае используется исходный адрес отправителя.

- `set service broadcast-relay id <n> port <port>`

  Задает номер UDP-порта, который будет использоваться вашим приложением.

- `set service broadcast-relay id <n> disable`

  Отключает определенный экземпляр `<n>` широковещательной ретрансляции без удаления из конфигурации устройства.

- `set service broadcast-relay disable`

  Отключает сервис широковещательной ретрансляции, не удаляя его из текущей конфигурации.

Примечание

Вы можете запустить службу ретрансляции широковещательных пакетов UDP на нескольких маршрутизаторах, подключенных к одной подсети. Широковещательного шторма пакетов при ретрансляции UDP не происходит.

2.8.1.5 Отслеживание соединений

Описание

Одной из важных функций, построенных на основе фреймворка Netfilter, является отслеживание соединений (conntrack-sync). Отслеживание соединений позволяет ядру отслеживать все логические сетевые соединения или сеансы и, таким образом, соотносить все пакеты, которые могут составлять это соединение. NAT опирается на эту информацию, чтобы переводить все связанные пакеты одинаковым образом, а iptables может использовать эту информацию для работы в качестве межсетевого экрана с контролем состояния.

Однако состояние соединения совершенно не зависит от состояния верхнего уровня, например, от состояния TCP или SCTP. Отчасти это объясняется тем, что при простой пересылке пакетов, т.е. без локальной доставки, механизм TCP может быть вообще не задействован. Эвристика для таких протоколов часто основана на заданном значении тайм-аута бездействия, по истечении которого соединение Netfilter разрывается.

Каждое соединение Netfilter однозначно идентифицируется кортежем (протокол третьего уровня, адрес источника, адрес назначения, протокол четвертого уровня, ключ четвертого уровня). Ключ уровня-4 зависит от транспортного протокола; для TCP/UDP это номера портов, для туннелей это может быть их туннельный идентификатор, но в остальных случаях он равен нулю, как если бы он не был частью кортежа. Для того чтобы во всех случаях можно было проверить TCP-порт, пакеты будут в обязательном порядке подвергаться дефрагментации.

Для синхронизации трафика можно использовать как Многоадресную (Multicast), так и Одноадресную (Unicast) рассылки. В большинстве приведенных ниже примеров используется Multicast, но можно указать и unicast, используя ключ peer после конкретного интерфейса, как в следующем примере:

```
set service conntrack-sync interface eth0 peer 192.168.0.250
```

Настройка

Пример настройки

Следующий пример представляет собой простую настройку службы отслеживания состояния между двумя маршрутизаторами.

Вставка картинки

Список команд для настройки службы отслеживания состояния на 1-ом и 2-ом маршрутизаторах:

```
.. option:: • set high-availablilty vrrp group internal virtual-address ... etc ...
.. option:: • set high-availability vrrp sync-group syncgrp member 'internal'
.. option:: • set service conntrack-sync accept-protocol 'tcp'
.. option:: • set service conntrack-sync accept-protocol 'udp'
.. option:: • set service conntrack-sync accept-protocol 'icmp'
.. option:: • set service conntrack-sync failover-mechanism vrrp sync-group
  'syncgrp'
.. option:: • set service conntrack-sync interface 'eth0'
.. option:: • set service conntrack-sync mcast-group '225.0.0.50'
```

На основном маршрутизаторе информация о состоянии активных соединений представлена во внут-

реннем кэше таблицы *conntrack-sync*. Такое же количество активных соединений должно присутствовать во внешнем кэше таблицы *conntrack-sync* резервного маршрутизатора. Для получения информации о количестве активных соединений используется команда `show conntrack-sync statistics`.

Проверка состояния активных соединений на основном маршрутизаторе:

```
$ show conntrack-sync statistics

Main Table Statistics:

cache internal:
current active connections:              10
connections created:                   8517    failed:           0
connections updated:                    127    failed:           0
connections destroyed:                 8507    failed:           0

cache external:
current active connections:               0
connections created:                      0    failed:           0
connections updated:                      0    failed:           0
connections destroyed:                    0    failed:           0

traffic processed:
                  0 Bytes                         0 Pckts

multicast traffic (active device=eth0):
              868780 Bytes sent               224136 Bytes recv
               20595 Pckts sent                14034 Pckts recv
                   0 Error send                    0 Error recv

message tracking:
                  0 Malformed msgs                    0 Lost msgs
```

Проверка состояния активных соединений на основном маршрутизаторе:

```
$ show conntrack-sync statistics

Main Table Statistics:

cache internal:
current active connections:               0
connections created:                      0    failed:           0
connections updated:                      0    failed:           0
connections destroyed:                    0    failed:           0

cache external:
current active connections:              10
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
connections created:                    888    failed:            0
connections updated:                    134    failed:            0
connections destroyed:                  878    failed:            0

traffic processed:
                  0 Bytes                          0 Pckts

multicast traffic (active device=eth0):
              234184 Bytes sent               907504 Bytes recv
               14663 Pckts sent                21495 Pckts recv
                   0 Error send                    0 Error recv

message tracking:
                  0 Malformed msgs                   0 Lost msgs
```

Список команд

Основные настройки

- `set service conntrack-sync accept-protocol <proto>`

  Определяет протоколы <proto>, для которых будут синхронизироваться локальные записи службы отслеживания состояния.

  Поддерживаемые протоколы: tcp, sctp, dccp, udp, icmp and ipv6-icmp.

- `set service conntrack-sync event-listen-queue-size <size>`

  Задает максимальный размера очереди для локальных событий службы отслеживания состояния, который может быть достигнут. Значение размера очереди для прослушивания локальных событий службы отслеживания состояния задается в Мегабайтах.

- `set service conntrack-sync expect-sync <all|ftp|h323|nfs|sip|sqlnet>`

  Определяет протокол, для которого необходимо синхронизировать записи ожиданий.

- `set service conntrack-sync failover-mechanism vrrp sync-group <group>`

  Активирует механизм отказоустойчивости, используемый для службы отслеживания состояния. Поддерживается только протокол VRRP.

- `set service conntrack-sync ignore-address <x.x.x.x>`

  Задает IP-адрес или подсеть <x.x.x.x>, для которых локальные записи службы отслеживания состояния не будут синхронизироваться.

- `set service conntrack-sync interface <name>`

  Определяет интерфейс <name>, используемый для синхронизации записей службы отслеживания состояния.

- `set service conntrack-sync interface <name> port <port>`

  Задает номер порта <port> для интерфейса <name>, используемого для синхронизации записей службы отслеживания состояния.

- `set service conntrack-sync listen-address <ipv4address>`

  Задает локальный IPv4-адрес `<ipv4address>` прослушивания входящих соединений для службы отслеживания состояния.

- `set service conntrack-sync mcast-group <x.x.x.x>`

  Задает адрес для группы Многоадресной трансляции `<x.x.x.x>`, используемой для синхронизации записей службы отслеживания состояния. По умолчанию используется адрес 225.0.0.50.

- `set service conntrack-sync interface <name> peer <address>`

  Задает адрес узла `<address>` отправки Одноадресных UDP сообщений для службы отслеживания состояния, если не используется конфигурация Многоадресной трансляции, описанная выше.

- `set service conntrack-sync sync-queue-size <size>`

  Задает размер очереди `<size>` для синхронизации записей системы отслеживания состояния.Значение задается в Мегабайтах.

- `set service conntrack-sync disable-external-cache`

  Отключает внешний кэш и напрямую передает состояния потока в систему отслеживания соединений в ядро резервного межсетевого экрана.

Мониторинг состояния

- `show conntrack table ipv4`

  Выводит таблицу системы отслеживания состояния для протокола IPv4-.

  Пример работы команды show conntrack table ipv4:

```
fakel@fakel:~$ show conntrack table ipv4

TCP state codes: SS - SYN SENT, SR - SYN RECEIVED, ES - ESTABLISHED,
                 FW - FIN WAIT, CW - CLOSE WAIT, LA - LAST ACK,
                 TW - TIME WAIT, CL - CLOSE, LI - LISTEN

CONN ID    Source                Destination           Protocol         TIMEOUT
1015736576 10.35.100.87:58172    172.31.20.12:22       tcp [6] ES       430279
1006235648 10.35.101.221:57483   172.31.120.21:22      tcp [6] ES       413310
1006237088 10.100.68.100         172.31.120.21         icmp [1]         29
1015734848 10.35.100.87:56282    172.31.20.12:22       tcp [6] ES       300
1015734272 172.31.20.12:60286    239.10.10.14:694      udp [17]         29
1006239392 10.35.101.221         172.31.120.21         icmp [1]         29
```

Примечание

Если в таблице отсутствуют записи об активных соединениях и выдается предупреждение, значит, система отслеживания состояния не включена. Чтобы включить систему отслеживания состояния, достаточно создать правило трансляции NAT или правило межсетевого экрана.

- `show conntrack-sync cache external`

  Выводит записи внешнего кэша синхронизации соединений системы отслеживания состояния

- `show conntrack-sync cache internal`

  Выводит записи внутреннего кэша синхронизации соединений системы отслеживания состояния

- `show conntrack-sync statistics`

  Выводит актуальную статистику системы отслеживания соединений.

  Пример работы команды show conntrack-sync statistics:

```
fakel@fakel:~$ show conntrack-sync statistics

Main Table Statistics:

cache internal:
current active connections:           19606
connections created:                 6298470    failed:           0
connections updated:                 3786793    failed:           0
connections destroyed:               6278864    failed:           0

cache external:
current active connections:           15771
connections created:                 1660193    failed:           0
connections updated:                   77204    failed:           0
connections destroyed:               1644422    failed:           0

traffic processed:
                  0 Bytes                         0 Pckts

multicast traffic (active device=eth0.5):
           976826240 Bytes sent            212898000 Bytes recv
             8302333 Pckts sent              2009929 Pckts recv
                   0 Error send                    0 Error recv

message tracking:
                  0 Malformed msgs                  263 Lost msgs
```

- `show conntrack-sync status`

  Выводит информацию об актуальном состоянии системы отслеживания соединений.

  Пример работы команды show conntrack-sync status:

```
fakel@fakel:~$ show conntrack-sync status

sync-interface        : eth0.5
failover-mechanism    : vrrp [sync-group GEFOEKOM]
last state transition : no transition yet!
ExpectationSync       : disabled
```

2.8.1.6 Консольный сервер

Описание

ПО Факел может выступать в качестве устройства внеполосного управления, обеспечивающего удаленный доступ по протоколу SSH к непосредственно подключенным последовательным интерфейсам.

В качестве последовательных интерфейсов могут выступать как интерфейсы, напрямую подключенные к процессору или чипсету (в Linux это чаще всего называется ttyS-интерфейсом), так и любые другие преобразователи USB в последовательные интерфейсы (микросхемы Prolific PL2303 или FTDI FT232/FT4232).

Список команд

Основные настройки

Примечание

Между компьютерами чаще всего используется конфигурация «8N1»: восемь битов символов, с одним стартовым битом, одним стоповым битом и без бита четности. Таким образом, для передачи одного символа используется 10 бод, и деление скорости передачи сигнала на десять дает общую скорость передачи в символах в секунду. Это также является настройкой по умолчанию, если ни одна из этих опций не задана.

- `set service console-server device <device> data-bits [7 | 8]`

  Задает значение битов данных `[7 | 8]` для передачи информации через последовательный порт <devise>. Если этот параметр не задан, то по умолчанию будет установлено значение 8.

- `set service console-server device <device> description <string>`

  Добавляет описание `<string>` для последовательного порта <device>, которое помогает идентифицировать подключенное периферийное устройство.

- `set service console-server device <device> parity [even | odd | none]`

  Устанавливает параметр четности `[even | odd | none]` для последовательного порта <device>. Если этот параметр не задан, то в качестве значения по умолчанию он будет установлен параметр none.

- `set service console-server device <device> stop-bits [1 | 2]`

  Задает параметр стопового бита `[1 | 2]` для последовательного порта <device>. Если этот параметр не задан, то по умолчанию будет установлено значение 1.

- `set service console-server device <device> speed [ 300 | 1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200 ]`

  Определяет скорость передачи данных `[ 300 | 1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200 ]` для последовательного порта <device>.

Примечание

Преобразователи USB в последовательный порт выполняют большую часть своей работы в программном обеспечении, поэтому следует внимательно относиться к выбранной скорости передачи

данных, так как иногда они не могут справиться с ожидаемой скоростью.

Настройка удаленного доступа

Примечание

Пользователь может напрямую подключиться через SSH к настроенному последовательному порту.

- `set service console-server device <device> ssh port <port>`

  Открывает TCP порт `<port>` последовательного порта `<device>` для подключения по SSH. После успешной аутентификации пользователь будет переброшен непосредственно на подключенное через последовательный порт устройство.

Подсказка

К одному и тому же последовательному устройству могут подключаться несколько пользователей, но запись в консольный порт разрешена только одному.

Мониторинг состояния

- `show console-server ports`

  Выводит информацию о настроенных последовательных портах и конфигурацию соответствующих этим портам интерфейсов.

  Пример работы команды show console-server ports:

```
fakel@fakel:~$ show console-server ports
 usb0b2.4p1.0             on /dev/serial/by-bus/usb0b2.4p1.0@ at   9600n
```

- `show console-server user`

  Выводит информацию о подключенных к последовательным портам пользователях.

  Пример работы команды show console-server user:

```
fakel@fakel:~$ show console-server user
 usb0b2.4p1.0               up   fakel@localhost
```

- `connect console <device>`

  Локальное подключение к последовательному порту `<device>`.

  Пример работы команды connect console <device>:

```
fakel@fakel-r1:~$ connect console usb0b2.4p1.0
 [Enter `^Ec?' for help]
 [-- MOTD -- Console Server]

fakel-r2 login:
```

Подсказка

К одному и тому же последовательному порту могут подключаться несколько пользователей, но запись в консольный порт разрешена только одному.

Подсказка

Последовательность `^Ec?` интерпретируется как сочетание клавиш: `Ctrl+E` с `?`. Для выхода из сеанса используйте последовательность клавиш: `Ctrl+E` с.

- `show log console-server`

  Выводит на экран журнал событий консольного сервера.

2.8.1.7 Ретранслятор DHCP

Описание

Устройство на базе **ПО Факел** можно настроить на работу в качестве агента ретрансляции DHCP. После настройки агента ретрансляции DHCP маршрутизатор начинает пересылать DHCP запросы на внешний DHCP сервер. Агент ретрансляции DHCP работает с адресами IPv4 и IPv6.

На всех интерфейсах, используемые для ретрансляции DHCP, должны быть настроены IP адреса.

Настройка

Пример настройки

Пример настройки для протокола IPv4

Пример настройки агента ретрансляции DHCP для протокола IPv4 со следующими параметрами:

- Прослушивание запросов DHCP настроено на интерфейсе `eth1`.
- DHCP-сервер расположен по IPv4-адресу *10.0.1.4*, который доступен через интерфейс `eth2`.
- Маршрутизатор получает запросы DHCP клиентов на интерфейс `eth1` и передает их на сервер *10.0.1.4* через интерфейс `eth2`.

Вставка рисунка...

Пример настройки агента ретранслятора DHCP:

```
set service dhcp-relay interface eth1
set service dhcp-relay interface eth2
set service dhcp-relay server 10.0.1.4
set service dhcp-relay relay-options relay-agents-packets discard
```

Сформированная конфигурация агента ретранслятора DHCP будет выглядеть следующим образом:

```
fakel@fakel# show service dhcp-relay

    interface eth1
    interface eth2
    server 10.0.1.4
    relay-options {
       relay-agents-packets discard
    }
```

Пример настройки для протокола IPv6

Пример настройки агента ретрансляции DHCP для протокола IPv6 со следующими параметрами:

- Запросы DHCPv6 принимаются маршрутизатором на прослушивающем интерфейсе `eth1`.
- Запросы DHCPv6 направляются через интерфейс `eth2`.
- Внешний DHCPv6-сервер находится по адресу *2001:db8::4*

Вставка рисунка...

Пример настройки агента ретранслятора DHCP:

```
set service dhcpv6-relay listen-interface eth1
set service dhcpv6-relay upstream-interface eth2
set service dhcpv6-relay upstream-interface eth2 address 2001:db8::4
```

Сформированная конфигурация агента ретранслятора DHCP будет выглядеть следующим образом:

```
fakel@fakel# show service dhcpv6-relay

    listen-interface eth1 {
    }
    upstream-interface eth2 {
        address 2001:db8::4
    }
```

Список команд

Настройки для протокола IPv4

- `set service dhcp-relay interface <interface>`

  Определяет интерфейсы `<interface>`, участвующие в процессе ретрансляции DHCP, включая интерфейс для связи с DHCP-сервером.

- `set service dhcp-relay server <server>`

  Задает IP адрес DHCP `<server>`, который будет обрабатывать ретранслированные пакеты.

- `restart dhcp relay-agent`

  Перезапускает службу ретрансляции DHCP.

Дополнительные настройки для протокола IPv4

- `set service dhcp-relay relay-options hop-count <count>`

  Задает максимальное количество переходов `<count>`, после которого пакеты будут отброшены. Значение задается в диапазоне 0-255. Значение по умолчанию 10.

- `set service dhcp-relay relay-options max-size <size>`

  Задает максимальный размер DHCP-пакетов `<size>`, включающих информацию об агенте ретрансляции. Если размер DHCP-пакета превышает это значение, он будет передан без добавления информации об агенте ретрансляции. Значение задается в диапазоне 64-1400. Значение по умолчанию 576.

- `set service dhcp-relay relay-options relay-agents-packets <append | discard | forward | replace>`

  Существует четыре типа политики перенаправления DHCP-пакетов:

  - **append**: Агенту ретрансляции разрешается добавлять свою собственную информацию о ретрансляции в полученный DHCP-пакет, не обращая внимания на уже имеющуюся в пакете информацию о ретрансляции.

- **discard**: Полученные пакеты, уже содержащие информацию о ретрансляции, будут отброшены.
- **forward**: Все пакеты пересылаются, уже имеющаяся ретрансляционная информация игнорируется.
- **replace**: Ретранслируемая информация, уже присутствующая в пакете, удаляется и заменяется собственным набором ретранслируемой информации маршрутизатора.

Настройки для протокола IPv6

- `set service dhcpv6-relay listen-interface <interface>`

  Устанавливает интерфейс `<interface>` в качестве прослушивающего интерфейса для ретрансляции DHCPv6. В качестве прослушивающего интерфейса можно указать несколько интерфейсов.

- `set service dhcpv6-relay upstream-interface <interface> address <server>`

  Определяет интерфейс `<interface>`, который будет принимать ответы от DHCP сервера `<server>` и других агентов ретрансляции.

- `restart dhcpv6 relay-agent`

  Перезапускает службу ретрансляции DHCPv6.

Дополнительные настройки для протокола IPv4

- `set service dhcpv6-relay max-hop-count <count>`

  Задает значение максимального количества переходов до отбрасывания пакетов `<count>`. Значение по умолчанию: 10

- `set service dhcpv6-relay use-interface-id-option`

  Если этот параметр установлен, то агент ретрансляции будет вставлять идентификатор интерфейса. Эта опция устанавливается автоматически, если используется более одного прослушивающего интерфейса.

2.8.1.8 DHCP сервер

Протокол DHCP позволяет производить автоматическую настройку сети на компьютерах и других устройствах. DHCP это стандартный протокол в сети с архитектурой «клиент-сервер», который динамически назначает IP-адреса и другую необходимую информацию конфигурации для новых устройств в сети. **ПО Факел** может выступать в качестве DHCP-сервера для назначения IPv4 и IPv6 адресов устройствам в локальной сети.

- *IPv4 сервер* (страница 714)
- *IPv6 сервер* (страница 721)

IPv4 сервер

Описание

Служба DHCP может обслуживать несколько общих сетей, причем каждая общая сеть имеет одну или несколько подсетей. Каждая подсеть должна быть настроена на интерфейсе устройства, который выступает в качестве DHCP сервера. Для определения пула динамических адресов внутри подсети задается специальный диапазон адресов. Можно определить несколько диапазонов адресов. Статические привязки используются для назначения статических адресов клиентам на основе их MAC-адресов.

Необработанные параметры

Необработанные параметры могут быть переданы в `shared-network-name`, `subnet` и `static-mapping`:

```
set service dhcp-server shared-network-name <name> shared-network-parameters
   <text>       Additional shared-network parameters for DHCP server.
set service dhcp-server shared-network-name <name> subnet <subnet>
  subnet-parameters
   <text>       Additional subnet parameters for DHCP server.
set service dhcp-server shared-network-name <name> subnet <subnet> static-mapping
  <description> static-mapping-parameters
   <text>       Additional static-mapping parameters for DHCP server.
                Will be placed inside the ”host” block of the mapping.
```

Эти параметры напрямую передаются в файл *dhcpd.conf* под тем узлом конфигурации, в котором они определены. Они не проверяются, поэтому ошибка в исходных параметрах не будет отловлена скриптами операционной системы и приведет к невозможности запуска службы *dhcpd*. Необходимо всегда проверять корректность внесенных параметров перед фиксацией конфигурации устройства.

Кавычки можно использовать внутри значений параметров, заменив все символы кавычек строкой `"`.

Настройка

Алгоритм настройки

Описание алгоритма настройки...

Пример настройки

Пример настройки **ПО Факел**, который будет выступать в качестве DHCP сервера локальной сети. DHCP сервер будет передавать устройствам внутри локальной сети информацию о назначенном им IP адресе, а также адресах DNS сервера и шлюза по умолчанию.

Для настройки службы DHCP будут использоваться следующие параметры:

- Для шлюза по умолчанию и DNS сервера будет использоваться адрес `192.168.0.1/24`
- Диапазон адресов `192.168.0.2/24 - 192.168.0.8/24` будет зарезервирован для назначения статических адресов

- Клиентам DHCP будут назначены IP-адреса в диапазоне `192.168.0.9 - 192.168.0.254` с доменным именем `internal-network`
- Срок действия аренды DHCP составляет один день (86400 секунд)
- Только узлы из локальной сети `192.168.0.0/24` могут использовать DNS сервер

Список команд для настройки DHCP сервера:

```
set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24
  default-router '192.168.0.1'
set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24 name-server
  '192.168.0.1'
set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24 domain-name
  'fakel.net'
set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24 lease '86400'
set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24 range 0 start
  192.168.0.9
set service dhcp-server shared-network-name LAN subnet 192.168.0.0/24 range 0 stop
  '192.168.0.254'

set service dns forwarding cache-size '0'
set service dns forwarding listen-address '192.168.0.1'
set service dns forwarding allow-from '192.168.0.0/24'
```

Отказоустойчивый кластер DHCP

Параметры для настройки отказоустойчивого кластера DHCP:

- Отказоустойчивый сервер DHCP будет настроен для подсети `192.0.2.0/24`
- Для шлюза по умолчанию и DNS сервера будет настроен адрес `192.0.2.254`
- Для адреса основного участника отказоустойчивого кластера DHCP будет настроен адрес `192.168.189.252`
- Для адреса резервного участника отказоустойчивого кластера DHCP будет настроен адрес `192.168.189.253`
- DHCP сервер будет выдавать клиентам адреса из диапазона `192.168.189.10` - `192.168.189.250`

Список общих команд для настройки отказоустойчивого кластера DHCP:

```
set service dhcp-server shared-network-name NET-SHARED subnet 192.0.2.0/24
  default-router '192.0.2.254'
set service dhcp-server shared-network-name NET-SHARED subnet 192.0.2.0/24
  name-server '192.0.2.254'
set service dhcp-server shared-network-name NET-SHARED subnet 192.0.2.0/24
  domain-name 'example.org'
set service dhcp-server shared-network-name NET-SHARED subnet 192.0.2.0/24 range 0
  start '192.0.2.10'
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
set service dhcp-server shared-network-name NET-SHARED subnet 192.0.2.0/24 range 0
  stop '192.0.2.250'
set service dhcp-server shared-network-name NET-SHARED subnet 192.0.2.0/24
  enable-failover
```

Список команд для настройки основного участника отказоустойчивого кластера DHCP:

```
set service dhcp-server failover source-address '192.168.189.252'
set service dhcp-server failover name 'NET-SHARED'
set service dhcp-server failover remote '192.168.189.253'
set service dhcp-server failover status 'primary'
```

Список команд для настройки резервного участника отказоустойчивого кластера DHCP:

```
set service dhcp-server failover source-address '192.168.189.253'
set service dhcp-server failover name 'NET-SHARED'
set service dhcp-server failover remote '192.168.189.252'
set service dhcp-server failover status 'secondary'
```

Список команд

Основные настройки

- `set service dhcp-server hostfile-update`

  Обновляет файл */etc/hosts*, добавляя актуальные DNS записи для каждого клиента.

  Запись будет иметь формат: <*shared-network-name*>_<*hostname*>.<*domain-name*>

- `set service dhcp-server host-decl-name`

  При записи в файл */etc/hosts* исключает значение <*shared-network-name*>_ из DNS записи клиента, используя только имя хоста и имя домена: <*hostname*>.<*domain-name*>

- `set service dhcp-server shared-network-name <name> domain-name <domain-name>`

  Устанавливает доменное имя <domain-name> для хостов, которые будут получать адреса из подсети <name. Доменное имя будет добавлено к имени хоста клиента для формирования полностью определенного доменного имени (FQDN).

- `set service dhcp-server shared-network-name <name> domain-search <domain-name>`

  Задает дополнительные доменные имена, которые образуют список доменов, используемых при поиске хостов в локальной сети по доменному имени. Если эта опция не указана, то по умолчанию используется единственный домен, указанный в параметре domain-name.

- `set service dhcp-server shared-network-name <name> name-server <address>`

  Устанавливает адрес DNS сервера, который будут получать адреса из подсети <name>. Поддерживается возможность указать несколько адресов для использования различных DNS серверов.

- `set service dhcp-server shared-network-name <name> ping-check`

  Активирует механизм проверки ICMP для подсети <subnet> из которой DHCP сервер будет выдавать адреса.

Примечание

Если свободных адресов для назначения клиентам нет, но есть IP-адреса, в использовании которых отказано, DHCP-сервер будет пытаться вернуть и использовать такие IP-адрес независимо от значения параметра `abandon-lease-time`.

- `set service dhcp-server listen-address <address>`

  Устанавливает адрес `<address>` для прослушивания DHCP сервером входящих запросов от клиентов.

Настройка индивидуальной подсети

- `set service dhcp-server shared-network-name <name> authoritative`

  При активации данного параметра, устройство будет являться единственным DHCP сервером для данной сети `<name>`.

- `set service dhcp-server shared-network-name <name> subnet <subnet> default-router <address>`

  Устанавливает адрес шлюза по умолчанию `<address>` для хостов, которые будут получать адреса из подсети `<subnet>`.

- `set service dhcp-server shared-network-name <name> subnet <subnet> name-server <address>`

  Устанавливает адрес DNS сервера `<address>` для хостов, которые будут получать адреса из подсети `<subnet>`. Поддерживается возможность указать несколько адресов для использования различных DNS серверов.

- `set service dhcp-server shared-network-name <name> subnet <subnet> lease <time>`

  Определяет время аренды IP адреса `<time>`, получаемого по DHCP, для хоста из подсети `<subnet>`. Значение используемое по умолчанию - 86400 секунд, что соответствует одному дню.

- `set service dhcp-server shared-network-name <name> subnet <subnet> range <n> start <address>`

  Задает начальный адрес `<address>` из диапазона адресов для DHCP сервера с идентификатором диапазона `<n>`. Адреса для аренды будут выделяться из пула адресов `<subnet>`.

- `set service dhcp-server shared-network-name <name> subnet <subnet> range <n> stop <address>`

  Задает конечный адрес `<address>` из диапазона адресов для DHCP сервера с идентификатором диапазона `<n>`. Адреса для аренды будут выделяться из пула адресов `<subnet>`.

- `set service dhcp-server shared-network-name <name> subnet <subnet> exclude <address>`

  Задает адрес `<address>`, который будет исключен для выдачи DHCP сервером из подсети `<subnet>`. Поддерживается возможность указать несколько адресов для исключения.

- `set service dhcp-server shared-network-name <name> subnet <subnet> domain-name <domain-name>`

  Устанавливает доменное имя `<domain-name>` для хостов, которые будут получать адреса из под-

сети <name>. Доменное имя будет добавлено к имени хоста клиента для формирования полностью определенного доменного имени (FQDN).

- `set service dhcp-server shared-network-name <name> subnet <subnet> domain-search <domain-name>`

  Задает дополнительные доменные имена <domain-name> , которые образуют список доменов, используемых при поиске хостов в локальной сети по доменному имени. Если эта опция не указана, то по умолчанию используется единственный домен, указанный в параметре domain-name.

- `set service dhcp-server shared-network-name <name> subnet <subnet> ping-check`

  Активирует механизм проверки ICMP для подсети <subnet> из которой DHCP сервер будет выдавать адреса.

- `set service dhcp-server shared-network-name <name> subnet <subnet> enable-failover`

  Активирует механизм отказоустойчивости службы DHCP для пула адресов <subnet>.

Настройка механизма отказоустойчивости DHCP

- `set service dhcp-server failover source-address <address>`

  Устанавливает локальный адрес <address>, используемый при обмене данными с резервным DHCP сервером на котором настроен механизм отказоустойчивости.

- `set service dhcp-server failover remote <address>`

  Устанавливает адрес резервного DHCP сервера <address>, используемый при обмене данными с основным DHCP сервером на котором настроен механизм отказоустойчивости.

- `set service dhcp-server failover name <name>`

  Задает общее имя <name> кластера отказоустойчивости DHCP сервера.

Примечание

Общее имя <name> должно быть идентичным у всех участников кластера отказоустойчивости DHCP сервера.

- `set service dhcp-server failover status <primary | secondary>`

  Задает роль DHCP сервера <primary | secondary> в кластере отказоустойчивости.

Примечание

Для того чтобы основной и резервный DHCP сервера могли синхронизировать свои таблицы арендованных адресов, они должны иметь возможность обращаться друг к другу по TCP порту 647.

Подсказка

Обмен таблицами арендованных адресов между участниками кластера отказоустойчивости DHCP сервера не шифруется и не аутентифицируется. Поскольку большинство DHCP серверов находятся в защищенной локальной сети организации, это будет избыточным. Если обмен информацией между

участниками кластера отказоустойчивости DHCP сервера проходит через незащищенные каналы связи, рекомендуется использовать защищенный VPN туннель, чтобы гарантировать, что передача данных не будет скомпрометирована.

Настройка статической привязки

Можно задать статическое назначение DHCP для каждого узла. Для этого потребуется MAC-адрес станции и желаемый IP-адрес. Адрес должен находиться внутри определения подсети, но может выходить за пределы оператора диапазона.

- `set service dhcp-server shared-network-name <name> subnet <subnet> static-mapping <description> mac-address <address>`

  Создает статическую привязку DHCP `<description>`, которая будет действовать для хоста, идентифицируемого по его MAC-адресу `<address>`.

- `set service dhcp-server shared-network-name <name> subnet <subnet> static-mapping <description> ip-address <address>`

  Задает адрес узла для статической привязки DHCP `<description>`. Адрес должен находиться внутри заданной подсети `<subnet>`, но может выходить за пределы динамического диапазона, созданного с помощью команды `set service dhcp-server shared-network-name <name> subnet <subnet> range <n>`. Если адрес не указан, то используется адрес из динамического пула.

Мониторинг и эксплуатация

- `show log dhcp server`

  Выводит на экран журнал событий службы DHCP сервера

- `show log dhcp client`

  Выводит на экран журнал событий всех процессов DHCP клиента

- `show log dhcp client interface <interface>`

  Выводит на экран журнал событий процесса DHCP клиента для указанного интерфейса `<interface>`.

- `restart dhcp server`

  Перезагружает службу DHCP сервера.

- `show dhcp server statistics`

  Выводит на экран статистику работы службы DHCP сервера.

  Пример работы команды show dhcp server statistics:

```
fakel@fakel:~$ show dhcp server statistics
Pool           Size    Leases    Available  Usage
-----------  ------  --------  -----------  -------
dhcpexample      99         2           97  2%
```

- `show dhcp server statistics pool <pool>`

  Выводит на экран статистику работы службы DHCP сервера для указанного пула `<pool>`.

- `show dhcp server leases`

  Выводит на экран информацию обо всех арендованных адресах, выданных DHCP сервером.

  Пример работы команды show dhcp server leases:

  fakel@fakel:~$ show dhcp server leases IP address Hardware address State Lease start Lease expiration Remaining Pool Hostname ––––– ––––––– ––- ––––––– ––––––– ––––- ––––– ––– 192.0.2.104 00:53:01:dd:ee:ff active 2019/12/05 14:24:23 2019/12/06 02:24:23 6:05:35 dhcpexample test1 192.0.2.115 00:53:01:ae:af:bf active 2019/12/05 18:02:37 2019/12/06 06:02:37 9:43:49 dhcpexample test2

Подсказка

При использовании команды `show dhcp server leases` информация о статической привязке адреса к определенному хосту не отображается. Чтобы получить информацию обо всех арендованных адресах, используйте команду `show dhcp server leases state all`.

- `show dhcp server leases pool <pool>`

  Выводит на экран информацию обо всех арендованных адресах, выданных DHCP сервером для указанного пула <pool>.

- `show dhcp server leases sort <key>`

  Сортирует вывод информации обо всех арендованных адресах по указанному ключу <key>.

  Возможные варианты ключей: ip, hardware_address, state, start, end, remaining, pool, hostname (по умолчанию = ip)

- `show dhcp server leases state <state>`

  Выводит информацию обо всех арендованных адресах с указанным состоянием <state>.

  Возможные состояния: all, active, free, expired, released, abandoned, reset, backup (по умолчанию = active)

IPv6 сервер

Описание

DHCPv6 - версия протокола DHCP для работы с IPv6. Этот протокол назначает как IPv6 адреса, так и другие параметры настройки сети, такие, как адрес DNS или доменное имя. DHCPv6 может назначать IPv6 адреса через ретранслятор. DHCPv6 сервер также может обеспечить сервис DHCPv6 без состояния отслеживания SLAAC, при котором клиенту могут быть назначены параметры конфигурации, такие как адрес DNS-сервера и доменное имя без назначения IPv6-адреса.

Настройка

Алгоритм настройки

Описание алгоритма настройки...

Пример настройки

Пулы адресов

В следующем примере описан один из сценариев настройки **ПО Факел** в качестве сервера DHCPv6.

Параметры для настройки сервера DHCPv6:

- Публикуемая сеть с именем `NET1` обслуживает подсеть `2001:db8::/64`.
- Подсеть `2001:db8::/64` подключена к интерфейсу `eth1`
- Адрес DNS сервера `2001:db8::ffff`
- Пул адресов будет состоять из диапазона `2001:db8::100` - `2001:db8::199`
- Значение для времени аренды адресов будет оставлено по умолчанию и составит 24 часа

Список команд для настройки сервера DHCPv6:

```
set service dhcpv6-server shared-network-name 'NET1' subnet 2001:db8::/64
 address-range start 2001:db8::100 stop 2001:db8::199
set service dhcpv6-server shared-network-name 'NET1' subnet 2001:db8::/64
 name-server 2001:db8::ffff
```

Конфигурация операционной системы будет выглядеть следующим образом:

```
fakel@fakel:~$ show service dhcpv6-server
    shared-network-name NET1 {
        subnet 2001:db8::/64 {
           address-range {
              start 2001:db8::100 {
                 stop 2001:db8::199
              }
           }
           name-server 2001:db8::ffff
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
        }
    }
```

Статическая привязка

В следующем примере описан сценарий настройки для сопоставления конкретных IPv6-адресов с конкретными хостами, через создание статической привязки. In order to map specific IPv6 addresses to specific hosts static mappings can be created. The following example explains the process.

Параметры для настройки сервера DHCPv6:

- Для сопоставления адреса с узлом используется IPv6 адрес `2001:db8::101`
- Для сопоставления адреса с узлом используется IPv6 префикс `2001:db8:0:101::/64`
- Для узла будет назначено имя `client1`.

Подсказка

Идентификатор представляет собой DUID устройства: разделенный двоеточием шестнадцатеричный список. Если устройство уже имеет динамическую аренду у DHCPv6 сервера, его DUID можно найти с помощью команды `show service dhcpv6 server leases`. DUID начинается с 5-го октета (после 4-го двоеточия) IAID_DUID.

Список команд для настройки сервера DHCPv6:

```
set service dhcpv6-server shared-network-name 'NET1' subnet 2001:db8::/64
 static-mapping client1 ipv6-address 2001:db8::101
set service dhcpv6-server shared-network-name 'NET1' subnet 2001:db8::/64
 static-mapping client1 ipv6-prefix 2001:db8:0:101::/64
set service dhcpv6-server shared-network-name 'NET1' subnet 2001:db8::/64
 static-mapping client1 identifier 00:01:00:01:12:34:56:78:aa:bb:cc:dd:ee:ff
```

Конфигурация операционной системы будет выглядеть следующим образом:

```
fakel@fakel:~$ show service dhcp-server shared-network-name NET1
   shared-network-name NET1 {
       subnet 2001:db8::/64 {
          name-server 2001:db8:111::111
          address-range {
              start 2001:db8::100 {
                 stop 2001:db8::199 {
              }
          }
          static-mapping client1 {
             ipv6-address 2001:db8::101
             identifier 00:01:00:01:12:34:56:78:aa:bb:cc:dd:ee:ff
          }
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
      }
    }
```

Список команд

Основные настройки

- `set service dhcpv6-server preference <preference value>`

  Задает приоритет `<preference value>` для выбора DHCP сервера. Приоритет задается в случае если клиенты, получающие сообщения об аренде адреса от нескольких DHCP серверов. Клиент выбирают DHCP сервер с наибольшим значением приоритета. Значение задается в диапазоне 0 - 255.

- `set service dhcpv6-server shared-network-name <name> subnet <prefix> lease-time {default | maximum | minimum}`

  Задает время аренды `{default | maximum | minimum}` DHCPv6 сервера. По умолчанию время аренды DHCPv6 сервера составляет 24 часа. Это значение можно изменить, указав время по умолчанию, максимальное время и минимальное время. Все значения должны быть указаны в секундах.

- `set service dhcpv6-server shared-network-name <name> subnet <prefix> nis-domain <domain-name>`

  Задает домен сетевой информационной системы NIS `<domain-name>` для клиентов DHCPv6.

- `set service dhcpv6-server shared-network-name <name> subnet <prefix> nisplus-domain <domain-name>`

  Задает домен сетевой информационной системы NIS+ `<domain-name>` для клиентов DHCPv6.

- `set service dhcpv6-server shared-network-name <name> subnet <prefix> nis-server <address>`

  Устанавливает адрес сервера сетевой информационной системы NIS `<address>` для клиентов DHCPv6.

- `set service dhcpv6-server shared-network-name <name> subnet <prefix> nisplus-server <address>`

  Устанавливает адрес сервера сетевой информационной системы NIS+ `<address>` для клиентов DHCPv6.

- `set service dhcpv6-server shared-network-name <name> subnet <prefix> sip-server <address | fqdn>`

  Устанавливает адрес SIP сервера `<address | fqdn>` для клиентов DHCPv6.

- `set service dhcpv6-server shared-network-name <name> subnet <prefix> sntp-server-address <address>`

  Устанавливает адрес SNTP сервера `<address | fqdn>` для клиентов DHCPv6.

Настройка индивидуальных префиксов для клиентов

- `set service dhcpv6-server shared-network-name <name> subnet <prefix> prefix-delegation start <address> prefix-length <length>`

  Устанавливает размер префиксов `<length>` для клиентов в подсети `<prefix>` при их запросе на делегирование префиксов.

- `set service dhcpv6-server shared-network-name <name> subnet <prefix> prefix-delegation start <start-address> stop <stop-address>`

  Устанавливает начальный `<start-address>` и конечный `<stop-address>` адреса для клиентов в подсети `<prefix>` при их запросе на делегирование префиксов.

Мониторинг состояния

- `show log dhcpv6 server`

  Выводит на экран журнал событий службы DHCPv6 сервера

- `show log dhcpv6 client`

  Выводит на экран журнал событий всех процессов DHCPv6 клиента

- `show log dhcpv6 client interface <interface>`

  Выводит на экран журнал событий процесса DHCPv6 клиента для указанного интерфейса `<interface>`.

- `restart dhcpv6 server`

  Перезагружает службу DHCP сервера.

- `show dhcpv6 server status`

  Выводит на экран информацию о статусе работы DHCPv6 сервера.

- `show dhcpv6 server leases`

  Выводит на экран информацию обо всех арендованных адресах, выданных DHCPv6 сервером.

  Пример работы команды show dhcpv6 server leases:

```
fakel@fakel:~$ show dhcpv6 server leases
IPv6 address   State    Last communication    Lease expiration     Remaining
  Type           Pool   IAID_DUID
-------------  -------  --------------------  ------------------  -----------  ----
  ---------  -----  ----------------------------------------
2001:db8::101  active   2019/12/05 19:40:10   2019/12/06 07:40:10  11:45:21
  non-temporary  NET1   98:76:54:32:00:01:00:01:12:34:56:78:aa:bb:cc:dd:ee:ff
2001:db8::102  active   2019/12/05 14:01:23   2019/12/06 02:01:23  6:06:34
  non-temporary  NET1   87:65:43:21:00:01:00:01:11:22:33:44:fa:fb:fc:fd:fe:ff
```

Подсказка

При использовании команды `show dhcpv6 server leases` информация о статической привязке адреса к определенному хосту не отображается. Чтобы получить информацию обо всех арендованных адресах, используйте команду `show dhcpv6 server leases state all`.

- `show dhcpv6 server leases pool <pool>`

  Выводит на экран информацию обо всех арендованных адресах, выданных DHCPv6 сервером для указанного пула `<pool>`.

- `show dhcpv6 server leases sort <key>`

  Сортирует вывод информации обо всех арендованных адресах по указанному ключу `<key>`.

  Возможные варианты ключей: ip, hardware_address, state, start, end, remaining, pool, hostname (по умолчанию = ip)

- `show dhcpv6 server leases state <state>`

  Выводит информацию обо всех арендованных адресах с указанным состоянием `<state>`.

  Возможные состояния: all, active, free, expired, released, abandoned, reset, backup (по умолчанию = active)

2.8.1.9 Перенаправляющий DNS сервер

Описание

Перенаправляющий DNS сервер — перенаправляет полученные рекурсивные запросы вышестоящему кэширующему серверу в виде рекурсивных запросов. Используется преимущественно для снижения нагрузки на кэширующий DNS сервер. Перенаправляющий (Forwarding) DNS-сервер имеет следующие свойства:

- Способность обрабатывать рекурсивные запросы без выполнения самой рекурсии
- Предоставлять локальный кэш в ближайшем сетевом расположении
- Увеличивает гибкость в определении локального доменного пространства

В **ПО Факел** перенаправляющий DNS сервер не требует наличия вышестоящего DNS сервера. Он может выступать как в качестве полноценного рекурсивного DNS сервера, так и пересылать запросы на настраиваемые вышестоящие DNS серверы.

Настройка

Пример настройки

Пример настройки разделенного DNS (split DNS) для домена example.com.

Для настройки разделенного DNS будут использоваться следующие параметры:

- Все DNS запросы для домена `example.com` должны перенаправляться на DNS сервер по адресу `192.0.2.254` и `2001:db8:cafe::1`
- Все остальные DNS запросы будут перенаправлены на другой набор DNS серверов по адресам `192.0.2.1`, `192.0.2.2`, `2001:db8::1:ffff` и `2001:db8::2:ffff`
- Перенаправляющий DNS сервер будет прослушивать запросы только по адресам внутреннего интерфейса `eth1` - `192.168.1.254` для IPv4 и `2001:db8::ffff` для IPv6.
- Перенаправляющий DNS сервер будет принимать запросы на поиск только из внутренних подсетей - `192.168.1.0/24` и `2001:db8::/64`
- Перенаправляющий DNS сервер будет передавать обратные запросы на поиск для зон `10.in-addr.arpa`, `168.192.in-addr.arpa`, `16-31.172.in-addr.arpa` на вышестоящий сервер.

Список команд для настройки:

```
set service dns forwarding domain example.com server 192.0.2.254
set service dns forwarding domain example.com server 2001:db8:cafe::1
set service dns forwarding name-server 192.0.2.1
set service dns forwarding name-server 192.0.2.2
set service dns forwarding name-server 2001:db8::1:ffff
set service dns forwarding name-server 2001:db8::2:ffff
set service dns forwarding listen-address 192.168.1.254
set service dns forwarding listen-address 2001:db8::ffff
set service dns forwarding allow-from 192.168.1.0/24
set service dns forwarding allow-from 2001:db8::/64
set service dns forwarding no-serve-rfc1918
```

Список команд

Основные настройки

- `set service dns forwarding system`

  Перенаправляет входящие DNS запросы на DNS сервера, которые настроенные в операционной системы.

- `set service dns forwarding dhcp <interface>`

  Определяет интерфейс `<interface>`, на который DHCP клиенты направляют DNS запросы.

- `set service dns forwarding name-server <address>`

  Задает адрес DNS сервера `<address>`, на который будут передаваться все DNS запросы. Поддерживается возможность указать несколько адресов для использования различных DNS серверов.

- `set service dns forwarding domain <domain-name> server <address>`

  Перенаправляет полученные запросы для определенного домена <domain-name> на заданный DNS сервер `<address>`. Поддерживается возможность указать несколько адресов для использования различных DNS серверов. Этот параметр можно использовать для настройки разделенного DNS.

Примечание

Этот параметр работает для зон с обратным поиском `18.172.in-addr.arpa`.

- `set service dns forwarding domain <domain-name> addnta`

  Активирует механизм NTA (Negative Trust Anchor) для определенного домена `<domain-name>`. Этот параметр должен быть установлен, если домен не поддерживает `DNSSEC`.

- `set service dns forwarding domain <domain-name> recursion-desired`

  Устанавливает RD (Recursion Desired) бит для запросов к вышестоящему DNS серверу.

- `set service dns forwarding allow-from <network>`

  Задает адрес сети `<network>`, в которой узлам разрешено использовать перенаправляющий DNS сервер.

- `set service dns forwarding dnssec <off | process-no-validate | process | log-fail | validate>`

  Устанавливает уровень для параметра DNSSEC `<off | process-no-validate | process | log-fail | validate>`.

  Перенаправляющий DNS сервер имеет 5 различных уровней обработки DNSSEC:

  - **off** - В этом режиме обработка DNSSEC не производится. Перенаправляющий DNS сервер не будет устанавливать бит DNSSEC OK (DO) в исходящих запросах и будет игнорировать биты DO и AD в запросах.
  - **process-no-validate** - В этом режиме перенаправляющий DNS сервер будет устанавливать DO-бит в исходящих запросах и предоставлять RR-наборы, связанные с DNSSEC (NSEC, RRSIG), клиентам, которые их запрашивают (с помощью DO-бита в запросе), за исключением зон, предоставляемых с помощью настройки зон для авторизации. В этом режиме он не будет выполнять никаких проверок, даже по запросу клиента.

- **process** - Если для параметра dnssec установлено значение *process*, то поведение перенаправляющего DNS сервера будет аналогично поведению в режиме *process-no-validate*. Однако перенаправляющий DNS сервер попытается проверить данные, если в запросе установлен хотя бы один из битов DO или AD. В этом случае он установит в ответе бит AD, если данные проверены успешно, или пошлет SERVFAIL, если проверка окажется ошибочной.
- **log-fail** - В этом режиме перенаправляющий DNS сервер будет пытаться проверить все данные, получаемые с доверенных серверов, независимо от запросов клиента по DNSSEC, и записывать результат проверки в журнал. Этот режим можно использовать для определения дополнительной нагрузки и количества возможных фиктивных ответов перед включением полноценной проверки. Ответы на запросы клиента аналогичны процессу.
- **validate** - Наивысший режим обработки DNSSEC. В этом режиме все запросы будут проверяться и в случае обнаружения не легитимных данных будет отправлен ответ SERVFAIL, независимо от запроса клиента.

Примечание

Популярный инструмент Dig для Unix/Linux устанавливает AD-бит в запросе. Это может привести к неожиданным результатам запроса при тестировании. В этом случае нужно указать параметр +noad в командной строке dig.

Примечание

CD бит корректно выполняется для *process* и *validate*. Для *log-fail* сбои также будут регистрироваться.

- `set service dns forwarding ignore-hosts-file`

  Отключает поиска по имени узла из файла /etc/hosts для перенаправляющего DNS сервера.

- `set service dns forwarding cache-size <0-2147483647>`

  Задает максимальное значение для количества записей DNS кэша `<0-2147483647>`. По умолчанию для максимального количества записей установлено значение 10000.

- `set service dns forwarding negative-ttl <0-7200>`

  Задает максимальное время кэширования `<0-7200>` для отрицательных записей. По умолчанию для максимального времени кэширования установлено значение 3600 секунд.

  Примечание

  Запрос, на который нет подтвержденного ответа, кэшируется, чтобы впоследствии быстро исключить DNS запись, не создавая большой нагрузки на удаленный сервер.

- `set service dns forwarding listen-address <address>`

  Устанавливает локальные адреса IPv4 или IPv6 `<address>`, к которым будет привязан перенаправляющий DNS сервер. Этого адреса DNS сервер будет использовать для прослушивания входящих соединений.

- `set service dns forwarding source-address <address>`

Устанавливает локальные адреса IPv4 или IPv6 <address>, используемые в качестве адреса источника для отправки запросов. С этого адреса DNS сервер будет отправлять перенаправленные на него исходящие DNS запросы.

- `set service dns forwarding no-serve-rfc1918`

  Активирует параметр, который делает перенаправляющий DNS сервер неизвестным для зон: 10.in-addr.arpa, 168.192.in-addr.arpa, 16-31.172.in-addr.arpa, что позволяет использовать вышестоящие DNS-серверы для обратного поиска этих зон.

Мониторинг и эксплуатация

- `reset dns forwarding <all | domain>`

  Сбрасывает локальную базу данных кэша переадресации DNS. Можно сбросить кэш для всех записей или только для записей, относящихся к определенному домену.

- `restart dns forwarding`

  Перезапускает процесс перенаправляющего DNS сервера. При этом также аннулируется локальный кэш переадресации DNS.

- `show dns forwarding`

  Выводит на экран статистику работы перенаправляющего DNS сервера.

2.8.1.10 Динамический DNS

Описание

ПО Факел умеет обновлять удаленную DNS запись, когда интерфейс получает новый IP адрес. Для этого в состав **ПО Факел** входит клиент *ddclient*.

Клиент *ddclient* использует два метода обновления DNS записей. Первый из них, в соответствии с RFC 2136, посылает обновления непосредственно демону DNS. Во втором случае используется сторонний сервис, например DynDNS.com или любой другой подобный сайт. Этот метод использует HTTP запросы для передачи нового IP адреса. В **ПО Факел** можно настроить оба способа.

Настройка

Пример настройки

Пример настройки динамической смены DNS записи.

Для настройки динамической смены DNS будут выполните следующие настройки:

- Зарегистрируйте DNS запись `example.fakel.io` на DNS сервере `ns1.fakel.io`.
- Используйте файл ключей аутентификации по адресу `/config/auth/my.key`.
- Установить TTL равным 300 секундам
- Register DNS record `example.fakel.io` on DNS server `ns1.fakel.io`
- Use auth key file at `/config/auth/my.key`
- Set TTL to 300 seconds

```
fakel@fakel# show service dns dynamic
 interface eth0.7 {
     rfc2136 Fakel-DNS {
         key /config/auth/my.key
         record example.fakel.io
         server ns1.fakel.io
         ttl 300
         zone fakel.io
     }
 }
```

В результате будет получена следующая запись конфигурации ddclient:

```
#
# ddclient configuration for interface ”eth0.7”:
#
use=if, if=eth0.7

# RFC2136 dynamic DNS configuration for example.fakel.io.ns1.fakel.io
server=ns1.fakel.io
protocol=nsupdate
password=/config/auth/my.key
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
ttl=300
zone=fakel.io
example.fakel.io
```

Примечание

Можно также поддерживать в актуальном состоянии различные зоны DNS. Для этого достаточно создать новый узел конфигурации: `set service dns dynamic interface <interface> rfc2136 <other-service-name>`.

Список команд

Основные настройки

- `set service dns dynamic interface <interface> rfc2136 <service-name>`

  Создает новую конфигурацию обновления DNS для RFC 2136, которая будет обновлять IP-адрес, назначенный `<interface>` на сервисе, настроенном в разделе `<service-name>`.

- `set service dns dynamic interface <interface> rfc2136 <service-name> key <keyfile>`

  Определяет файл `<keyfile>`, содержащий секретный ключ RNDC, совместно используемый с удаленным DNS сервером. Это опция является обязательной.

- `set service dns dynamic interface <interface> rfc2136 <service-name> server <server>`

  Задает интерфейс, имя сервиса и адрес DNS сервера, используемые при обновлении данного динамического назначения.

- `set service dns dynamic interface <interface> rfc2136 <service-name> zone <zone>`

  Задает обновляемую DNS `<zone>`. Это опция является обязательной.

- `set service dns dynamic interface <interface> rfc2136 <service-name> record <record>`

  Задает DNS запись `<record>`, которая должна обновляться. Этот параметр может быть задан несколько раз. Это опция является обязательной.

- `set service dns dynamic interface <interface> rfc2136 <service-name> ttl <ttl>`

  Задает значение TTL `<ttl>` для записи ресурса. Значение по умолчанию равно 600 секундам.

Настройка сервисов на основе HTTP

- `set service dns dynamic interface <interface> service <service> host-name <hostname>`

  Определяет динамическое имя хоста `<hostname>`, идентифицированным по определенному сервису `<service>`, при изменении IP адреса на интерфейсе `<interface>`.

- `set service dns dynamic interface <interface> service <service> login <username>`

  Задает имя пользователя“<username>“, используемое при аутентификации запроса на обновление для службы определенной в поле `<service>`.

- `set service dns dynamic interface <interface> service <service> password <password>`

  Задает пароль <password>, используемый при аутентификации запроса на обновление для службы определенной в поле <service>.

- `set service dns dynamic interface <interface> service <service> protocol <protocol>`

  Определяет протокол <protocol>, используемый при аутентификации запроса на обновление для службы определенной в поле <service>.

- `set service dns dynamic interface <interface> service <service> server <server>`

  Определяет сервер <server>, используемый при аутентификации запроса на обновление для службы определенной в поле <service>.

- `set service dns dynamic interface <interface> service <service> zone <zone>`

  Задает зону DNS <zone> для обновления. Это параметр доступен только для CloudFlare.

Настройка для работы с NAT

По умолчанию ddclient обновляет динамическую dns-запись, используя IP-адрес, непосредственно подключенный к интерфейсу. Если ваше устройство находится за NAT, то запись будет обновлена и будет указывать на ваш внутренний IP адрес.

Чтобы ddclient определял внешние IP адреса необходимо выполнить следующие настройки:

- `set service dns dynamic interface <interface> use-web url <url>`

  Задает значение параметра <url> для определения вашего IP адреса. ddclient загрузит <url> и попытается извлечь ваш IP адрес из ответа.

- `set service dns dynamic interface <interface> use-web skip <pattern>`

  Задает значение параметра <pattern>. Клиент ddclient будет пропускать все адреса, расположенные до строки, заданной в поле <pattern>.

2.8.2 Системные механизмы

2.8.2.1 Системный DNS

Описание

В этом разделе описывается настройка DNS в системе, а именно:

- Серверы имен DNS
- Порядок поиска доменов

Для того чтобы система могла использовать и заполнять неквалифицированные имена хостов, можно определить список, который будет использоваться для поиска доменов.

Настройка

Пример настройки

В данном примере используется несколько серверов OpenNIC, два IPv4 адреса и два IPv6 адреса.

Список команд для настройки:

```
set system name-server 176.9.37.132
set system name-server 195.10.195.195
set system name-server 2a01:4f8:161:3441::1
set system name-server 2a00:f826:8:2::195
```

Система настроена на попытку завершения домена в следующем порядке: `fakel.io` (первый), `fakel.net` (второй) и `fakel.network` (последний).

Список команд для настройки:

```
set system domain-search domain fakel.io
set system domain-search domain fakel.net
set system domain-search domain fakel.network
```

Список команд

Основные настройки

- `set system name-server <address>`

  С помощью этой команды можно указать DNS сервер для системы, который будет использоваться для поиска DNS. Можно добавить несколько DNS серверов, настраивая по одному. Поддерживаются адреса как IPv4, так и IPv6.

- `set system domain-search domain <domain>`

  С помощью этой команды можно определить домены по одному, чтобы система использовала их для завершения неквалифицированных имен хостов. Максимум: 6 записей.

Примечание

Доменные имена могут включать буквы, цифры, дефисы и точки, максимальная длина которых составляет 253 символа.

2.8.2.2 Протокол сетевого времени

Описание

NTP (Network Time Protocol) - сетевой протокол для синхронизации часов между компьютерными системами в сетях передачи данных с пакетной коммутацией и переменной задержкой. NTP, работающий с 1985 года, является одним из старейших протоколов Интернета, используемых в настоящее время.

NTP предназначен для синхронизации всех компьютеров-участников с точностью до нескольких миллисекунд от UTC. Для выбора серверов точного времени используется алгоритм пересечения, представляющий собой модифицированную версию алгоритма Марзулло, и предназначенный для уменьшения влияния переменных сетевых задержек. Обычно NTP может поддерживать время с точностью до десятков миллисекунд в общедоступном Интернете, а в локальных сетях при идеальных условиях может достигать точности более одной миллисекунды. Асимметричные маршруты и перегруженность сети могут приводить к ошибкам в 100 мс и более.

Протокол обычно описывается в терминах модели «клиент-сервер», но может также легко использоваться в одноранговых отношениях, когда оба участника рассматривают друг друга в качестве потенциального источника времени. Реализации передают и получают временные метки с помощью UDP-порта с номером 123.

NTP предупреждает о предстоящей корректировке високосной секунды, но информация о локальных часовых поясах или переходе на летнее время не передается.

В настоящее время используется протокол версии 4 (NTPv4), который является предлагаемым стандартом и документирован в RFC 5905. Он обратно совместим с версией 3, описанной в RFC 1305.

Список команд

Основные настройки

- `set system ntp server <address>`

  Настройте один или несколько серверов для синхронизации. Имя сервера может быть как IP адресом, так и FQDN.

  По умолчанию установлено 3 NTP-сервера, которые можно изменить.

  - `0.pool.ntp.org`
  - `1.pool.ntp.org`
  - `2.pool.ntp.org`

- `system ntp server <address> <noselect | pool | preempt | prefer>`

  Настройте один или несколько атрибутов для данного NTP сервера:

  - `noselect` помечает сервер как неиспользуемый, за исключением целей отображения. Сервер отбрасывается алгоритмом выбора.
  - `pool` мобилизует постоянную ассоциацию клиентского режима с рядом удаленных серверов.
  - `preempt` вытесняемая ассоциация является расходуемой.
  - `prefer` помечает сервер как предпочтительный. При прочих равных условиях именно этот хост будет выбран для синхронизации среди множества корректно работающих хостов.

- `system ntp listen-address <address>`

  Процесс NTP будет прослушивать только указанный IP-адрес. Вы должны указать <адрес> и, опционально, разрешенных клиентов. Можно настроить несколько адресов прослушивания.

- `system ntp allow-clients address <address>`

  Список сетей или клиентских адресов, которым разрешено связываться с данным NTP сервером.

  Можно настроить несколько сетей.

- `system ntp vrf <name>`

  Задает NTP сервер для экземпляра VRF.

2.8.2.3 Информация об устройстве

Описание

В этом разделе описывается информация о хостах системы и способы их настройки, рассматриваются следующие темы:

- Имя устройства
- Домен
- IP-адрес
- Псевдонимы

Имя устройства

Имя устройства - это метка, присваиваемая сетевому устройству в сети и используемая для отличия одного устройства от другого в определенных сетях или в Интернете. С другой стороны, это будет имя, которое отображается в приглашении командной строки.

Доменное имя

Доменное имя - это метка, присвоенная компьютерной сети, и поэтому оно уникально. **ПО Факел** добавляет доменное имя в качестве суффикса к любому неквалифицированному имени. Например, если вы задали доменное имя example.com, а отправляете ICMP запрос на неквалифицированное имя `crux`, то **ПО Факел** квалифицирует это имя как `crux.example.com`.

Статическое сопоставление имени устройства

В **ПО Факел** поддерживается возможность сопоставить IP адрес с именем устройства для локального разрешения имен. Это эквивалент записей файла /etc/hosts.

Примечание

Не редактируйте вручную файл /etc/hosts. Этот файл будет автоматически регенерироваться при загрузке на основе настроек, указанных в данном разделе, а значит, все внесенные вручную правки будут потеряны. Вместо этого настройте статическое сопоставление хостов следующим образом.

Список команд

Основные настройки

- `set system host-name <hostname>`

  Устанавливает имя устройства `<hostname>`. Имя устройства может содержать до 63 символов. Имя устройства должно начинаться и заканчиваться буквой или цифрой и иметь в качестве внутренних символов только буквы, цифры или дефис.

  По умолчанию используется имя хоста `fakel`.

- `system domain-name <domain>`

  Устанавливает доменное имя системы. Доменное имя должно начинаться и заканчиваться буквой или цифрой и иметь в качестве внутренних символов только буквы, цифры или дефис.

- `set system static-host-mapping host-name <hostname> inet <address>`

  Создает статическое сопоставление имени устройства, которое всегда будет разрешать имя `<hostname>` в IP адрес `<address>`.

- `set system static-host-mapping host-name <hostname> alias <alias>`

  Создает псевдоним `<alias>` для настроенного статического отображения имени устройства `<hostname>`. Таким образом, адрес, настроенный как `set system static-host-mapping host-name <hostname> inet <address>`, может быть доступен через несколько имен.

  Для каждого имени хоста можно указать несколько псевдонимов.

2.8.2.4 Управление пользователями

Описание

Учетная запись пользователя по умолчанию `fakel`, а также вновь создаваемые учетные записи пользователей имеют все возможности для настройки системы. Все учетные записи имеют права `sudo` и, следовательно, могут работать в системе в качестве привилегированного пользователя.

Поддерживаются как локально администрируемые, так и удаленно администрируемые учетные записи RADIUS.

В крупных инсталляциях нецелесообразно настраивать каждого пользователя отдельно на каждой системе. **ПО Факел** поддерживает использование серверов RADIUS для аутентификации пользователей.

Аутентификация на основе ключа

Настоятельно рекомендуется использовать аутентификацию по ключу SSH. По умолчанию существует только один пользователь `fakel`, которому можно назначить любое количество ключей. Создать ssh-ключ можно с помощью команды `ssh-keygen` на локальной машине, которая (по умолчанию) сохранит его в файле `~/.ssh/id_rsa.pub`.

Каждый SSH-ключ состоит из трех частей:

`ssh-rsa AAAAB3NzaC1yc2EAAAABAA...VBD5lKwEWB username@host.example.com.`

Используются только тип `ssh-rsa` и ключ `AAAB3N...`. Обратите внимание, что длина ключа обычно составляет несколько сотен символов, и его придется копировать и вставлять. Некоторые эмуляторы терминалов могут случайно разбить его на несколько строк. Будьте внимательны при вставке, чтобы он вставлялся только в одну строку. Третья часть является просто идентификатором и служит для справки.

Настройка

Пример настройки

В следующем примере и `User1`, и `User2` смогут подключаться к **ПО Факел** по SSH под именем пользователя `fakel`, используя свои собственные ключи. `User1` имеет ограничение на подключение только с одного IP адреса.

Список команд для настройки:

```
set system login user fakel authentication public-keys 'User1' key ”AAAAB3Nz...KwEW
  ”
set system login user fakel authentication public-keys 'User1' type ssh-rsa
set system login user fakel authentication public-keys 'User1' options
  ”from=&quot;192.168.0.100&quot;”
set system login user fakel authentication public-keys 'User2' key ”AAAAQ39x...fbV3
  ”
set system login user fakel authentication public-keys 'User2' type ssh-rsa
```

Список команд

Основные настройки

- `system login user <name> full-name “<string>”`

  Создает нового системного пользователя с именем пользователя <name> и реальным именем, заданным в поле <string>.

- `system login user <name> authentication plaintext-password <password>`

  Устанавливает пароль пользователя <name> в открытом виде для данной системы. Пароль в открытом виде будет автоматически переведен в защищенный хэшированный пароль и нигде не будет сохранен в открытом виде.

- `system login user <name> authentication encrypted-password <password>`

  Устанавливает зашифрованный пароль для заданного имени пользователя <name>. Это удобно для переноса хэшированного пароля из системы в систему.

Настройки аутентификации на основе ключей

- `system login user <username> authentication public-keys <identifier> key <key>`

  Назначает связку открытых ключей SSH <key>, идентифицированную по ключу <identifier>, локальному пользователю <username>.

- `system login user <username> authentication public-keys <identifier> type <type>`

  Каждая часть открытого ключа SSH, на которую ссылается <identifier>, требует настройки <type> используемого открытого ключа. Этот тип может быть любым из:

  - `ecdsa-sha2-nistp256`
  - `ecdsa-sha2-nistp384`
  - `ecdsa-sha2-nistp521`
  - `ssh-dss`
  - `ssh-ed25519`
  - `ssh-rsa`

Примечание

Вы можете назначить несколько ключей одному и тому же пользователю, используя уникальный идентификатор для каждого SSH-ключа.

- `system login user <username> authentication public-keys <identifier> options <options>`

  Задает параметры для данного открытого ключа `<identifier>`.

Настройка авторизации через RADIUS

- `set system login radius server <address> key <secret>`

  Устанавливает `<address>` пользователя RADIUS-сервера с секретом `pre-shared-secret`, заданным в поле `<secret>`. Можно указать несколько серверов.

- `set system login radius server <address> port <port>`

  Определяет порт `<port>`, через который можно связаться с сервером RADIUS `<address>`. По умолчанию это значение равно 1812.

- `set system login radius server <address> timeout <timeout>`

  Установите `<timeout>` в секундах при запросе к серверу RADIUS `<address>`.

- `set system login radius server <address> disable`

  Временно отключает определенный сервер RADIUS `<address>`.

- `set system login radius source-address <address>`

  Серверы RADIUS могут быть усилены путем разрешения подключения только определенных IP адресов. Для этого можно настроить адрес источника каждого запроса RADIUS. Если этот параметр не задан, то входящие соединения с сервером RADIUS будут использовать ближайший адрес интерфейса, указывающий на сервер, что приводит к ошибкам в сетях OSPF, например, при отказе канала связи и использовании резервного маршрута.

Подсказка

Если вы хотите, чтобы пользователи-администраторы проходили аутентификацию через RADIUS, необходимо отправить атрибут `Cisco-AV-Pair shell:priv-lvl=15`. Без этого атрибута вы получите только обычных, непривилегированных пользователей системы.

Настройка баннера входа в систему

Вы можете установить баннер с сообщением после или перед входом в систему для отображения определенной информации для данной системы.

- `set system login banner pre-login <message>`

  Устанавливает сообщение `<message>`, которое будет показано при подключении по SSH и перед входом пользователя в систему.

- `set system login banner post-login <message>`

  Устанавливает сообщение <message>, которое будет показано после входа пользователя в систему.

Примечание

Чтобы создать новую строку в сообщении для входа в систему, необходимо экранировать символ новой строки с помощью \\\n.

2.9 Встроенные контейнеры

ПО Факел использует встроенный механизм контейнеризации без фоновых процессов.

2.9.1 Конфигурирование

```
# set container name <name> image
```

Данная команда позволяет задать имя образа в реестре образов.

```
set container name mysql-server image mysql:8.0
```

Если реестр образов не указан, в качестве него будет использован ресурс *Docker.io* до тех пор, пока реестр не будет явно указан с помощью команды `set container registry <name>` или пока реестр не будет задан как часть имени образа.

```
set container name mysql-server image quay.io/mysql:8.0
```

```
# set container name <name> allow-host-networks
```

Данная команда позволяет обеспечить доступ контейнера к сетевому стеку хоста. Сетевой стек контейнера не изолирован от сетевого стека хоста и использует IP адрес хоста.

Следующие команды транслируются в команды с параметром `--net host` при работе с контейнерами.

Примечание

Обратите внимание, что параметр `allow-host-networks` не может быть использован совместно с параметром `network`.

```
# set container name <name> network <networkname>
```

Данная команда позволяет подключить к контейнеру пользовательскую сеть. При этом только одна сеть может быть указана в команде и она должна быть предварительно создана.

```
# set container name <name> network <networkname> address <address>
```

Данная команда позволяет опционально задать статический IPv4 ..

или IPv6

адрес для контейнера. Задаваемый адрес должен быть из подсети, определенной префиксом указанной в команде сети.

Примечание

Обратите внимание, что адрес первого хоста (X.X.X.1) зарезервирован механизмом и не может быть использован.

```
# set container name <name> description <text>
```

Данная команда позволяет задать текстовое описание для созданного контейнера.

```
# set container name <name> environment <key> value <value>
```

Данная команда позволяет добавить для контейнера пользовательские переменные окружения. С помощью данной команды можно добавить несколько переменных окружения одновременно.

Следующие команды транслируются в команды с параметром `-e key=value` при работе с контейнерами.

```
set container name mysql-server environment MYSQL_DATABASE value 'zabbix'
set container name mysql-server environment MYSQL_USER value 'zabbix'
set container name mysql-server environment MYSQL_PASSWORD value 'zabbix_pwd'
set container name mysql-server environment MYSQL_ROOT_PASSWORD value 'root_pwd'
```

```
# set container name <name> port <portname> source <portnumber>
```

```
# set container name <name> port <portname> destination <portnumber>
```

```
# set container name <name> port <portname> protocol <tcp | udp>
```

Данные команды позволяют опубликовать во внешней сети определенный порт контейнера.

```
set container name zabbix-web-nginx-mysql port http source 80
set container name zabbix-web-nginx-mysql port http destination 8080
set container name zabbix-web-nginx-mysql port http protocol tcp
```

```
# set container name <name> volume <volumename> source <path>
```

```
# set container name <name> volume <volumename> destination <path>
```

Данные команды позволяют монтировать к контейнеру определенный раздел.

```
set container name coredns volume 'corefile' source /config/coredns/Corefile
set container name coredns volume 'corefile' destination /etc/Corefile
```

```
# set container name <name> volume <volumename> mode <ro | rw>
```

Данная команда позволяет установить режим доступа к разделу (*ro* - только чтение, *rw* - чтение и запись), по умолчанию - *ro*.

```
# set container name <name> restart [no | on-failure | always]
```

Данная команда позволяет задать условия перезапуска контейнера при выходе. Для выбора доступно одно из следующих условий:

- `no` - не перезапускать контейнер.
- `on-failure` - перезапускать контейнер, если получено ненулевое
- значение кода выхода (по умолчанию количество попыток перезапуска не ограничено).
- `always` - перезапускать контейнер вне зависимости от значения
- кода выхода (по умолчанию количество попыток перезапуска не ограничено).

```
# set container name <name> memory <MB>
```

Данная команда позволяет ограничить объем оперативной памяти (RAM) хоста, выделяемый для контейнера. Значение по умолчанию составляет 512 Мбайт. Используйте значение 0 Мбайт, чтобы полностью снять ограничение.

```
# set container name <name> device <devicename> source <path>
```

```
# set container name <name> device <devicename> destination <path>
```

Данные команды позволяют монтировать к контейнеру устройство, являющееся частью аппаратного обеспечения хоста.

```
# set container name <name> cap-add <text>
```

Данная команда позволяет назначить контейнеру определенные уровни доступа и полномочия. Для назначения доступны следующие варианты:

- `net-admin` - сетевые настройки (сетевые интерфейсы, межсетевой экран, таблицы маршрутизации).
- `net-bind-service` - назначение сокета привилегированным портам (номера портов меньше 1024).
- `net-raw` - создание «сырых» (raw) сокетов.
- `setpcap` - назначение уровней доступа (из привязанных или унаследованных наборов).
- `sys-admin` - администрирование (использование утилит `quotactl`, `mount`, `sethostname`, `setdomainame`).
- `sys-time` - установка системного времени.

```
# set container name <name> disable
```

Данная команда позволяет отключить контейнер.

```
# set container network <networkname>
```

Данная команда позволяет создать для контейнера сеть с заданным именем.

```
# set container registry <name>
```

Данная команда позволяет добавить реестр образов в список неквалифицированных реестров для поиска подходящих образов. По умолчанию для любого образа, имя которого не содержит явное указанием на реестр, **ПО Факел** будет использовать ресурс *Docker.io* в качестве реестра образов.

2.9.2 Команды эксплуатационного режима

```
$ add container image <containername>
```

Данная команда позволяет извлечь новый образ для контейнера из реестра.

```
$ show container
```

Данная команда позволяет вывести на экран список всех активных контейнеров.

```
$ show container image
```

Данная команда позволяет вывести на экран список всех образов, размещенных локально на диске устройства.

```
$ show container log <containername>
```

Данная команда позволяет вывести на экран список событий, зарегистрированных в ходе работы выбранного контейнера.

```
$ show container network
```

Данная команда позволяет вывести на экран список доступных для контейнера сетей.

```
$ restart container <containername>
```

Данная команда позволяет перезапустить выбранный контейнер.

```
$ update container image <containername>
```

Данная команда позволяет обновить образ выбранного контейнера.

2.9.3 Пример конфигурации

Далее представлен пример[69] настроек на основе официальной документации на систему Zabbix с поправкой на синтаксис команд **ПО Факел**.

```
set container network zabbix-net prefix 172.20.0.0/16
set container network zabbix-net description 'Network for Zabbix component
  containers'

set container name mysql-server image mysql:8.0
set container name mysql-server network zabbix-net

set container name mysql-server environment 'MYSQL_DATABASE' value 'zabbix'
set container name mysql-server environment 'MYSQL_USER' value 'zabbix'
set container name mysql-server environment 'MYSQL_PASSWORD' value 'zabbix_pwd'
set container name mysql-server environment 'MYSQL_ROOT_PASSWORD' value 'root_pwd'

set container name zabbix-java-gateway image
  zabbix/zabbix-java-gateway:alpine-5.2-latest
set container name zabbix-java-gateway network zabbix-net

set container name zabbix-server-mysql image
  zabbix/zabbix-server-mysql:alpine-5.2-latest
set container name zabbix-server-mysql network zabbix-net

set container name zabbix-server-mysql environment 'DB_SERVER_HOST' value
  'mysql-server'
set container name zabbix-server-mysql environment 'MYSQL_DATABASE' value 'zabbix'
set container name zabbix-server-mysql environment 'MYSQL_USER' value 'zabbix'
set container name zabbix-server-mysql environment 'MYSQL_PASSWORD' value
  'zabbix_pwd'
set container name zabbix-server-mysql environment 'MYSQL_ROOT_PASSWORD' value
```

(продолжается на следующей странице)

[69] https://www.zabbix.com/documentation/current/manual/installation/containers

(продолжение с предыдущей страницы)

```
  'root_pwd'
set container name zabbix-server-mysql environment 'ZBX_JAVAGATEWAY' value
  'zabbix-java-gateway'

set container name zabbix-server-mysql port zabbix source 10051
set container name zabbix-server-mysql port zabbix destination 10051

set container name zabbix-web-nginx-mysql image
  zabbix/zabbix-web-nginx-mysql:alpine-5.2-latest
set container name zabbix-web-nginx-mysql network zabbix-net

set container name zabbix-web-nginx-mysql environment 'MYSQL_DATABASE' value
  'zabbix'
set container name zabbix-web-nginx-mysql environment 'ZBX_SERVER_HOST' value
  'zabbix-server-mysql'
set container name zabbix-web-nginx-mysql environment 'DB_SERVER_HOST' value
  'mysql-server'
set container name zabbix-web-nginx-mysql environment 'MYSQL_USER' value 'zabbix'
set container name zabbix-web-nginx-mysql environment 'MYSQL_PASSWORD' value
  'zabbix_pwd'
set container name zabbix-web-nginx-mysql environment 'MYSQL_ROOT_PASSWORD' value
  'root_pwd'

set container name zabbix-web-nginx-mysql port http source 80
set container name zabbix-web-nginx-mysql port http destination 8080
```

2.10 Эксплуатация

2.10.1 Управление лицензиями ПО Факел

Система управления лицензиями в **ПО Факел** обеспечивает возможность регистрации экземпляра программного обеспечения для целей учета и активации дополнительных возможностей.

2.10.1.1 Общие сведения

Для активации **ПО Факел** используются лицензионные ключи, представляющие собой комбинацию букв и цифр, хранящихся в виде текстовых строк (лицензионных строк). Одна упомянутая строка может содержать один лицензионный ключ. Один ключ может активировать один экземпляр ПО Факел. Лицензионные ключи поставляются посредством электронных средств связи, таких как электронная почта.

Установка лицензии

Установка лицензии проходит в режиме Конфигурирования **ПО Факел**.

```
# set license add 'license_string'
```

Команда позволяет установить лицензию для приобретенного экземпляра **ПО Факел**.

> **Примечание**
>
> Если введена некорректная строка лицензии, то на экран будет выведено сообщение *License is invalid and can not be imported*

Просмотр лицензий

Просмотр лицензий **ПО Факел** выполняется в режиме Администрирования.

```
$ show license
```

Команда позволяет вывести на экран текущие лицензии приобретенного экземпляра **ПО Факел**.

```
fakel@fakel:~$ show license
|      LicId       |     CliId     | LicType  | Status  | DaysLeft |
|------------------|---------------|----------|---------|----------   |
| 0                | 0             | trial    | active  | 29          |


Total number of licenses: 1
```

Удаление лицензий

Удаление лицензии проходит в режиме Конфигурирования **ПО Факел**.

```
# set license del 'license_string'
```

Команда позволяет удалить установленную лицензию для приобретенного экземпляра **ПО Факел**.

2.10.2 Общие сведения

ПО Факел предоставляет администратору широкий спектр команд, выполняемых в эксплуатационном режиме, для получения информации о работе системы.

2.10.2.1 Аппаратное обеспечение

Интерфейсы USB

Ранее последовательные интерфейсы были определены как устройства `ttySx` и `ttyUSBx`, где `x` - номер экземпляра последовательного интерфейса. Было установлено, что между загрузками распределение на шине последовательных USB интерфейсов может отличаться в зависимости от того, какой драйвер был загружен операционной системой первым. При наличии последовательных интерфейсов не только для подключения последовательной консоли, но и для поддержки функциональности интерфейсов WWAN (Wireless Wide Area Network) данная особенность приводила к возникновению проблем в использовании устройств.

Для того, чтобы решить проблемы с определением устройств в системе, а также с учетом того, что конвертеры из USB в последовательный интерфейс не имеют встроенного на производстве номера, такие конвертеры определяются в системе как непосредственно подключенные к корневому концентратору USB и к шине соответственно. Такое поведение характерно для многих дистрибутивов операционных систем Linux последних версий.

```
$ show hardware usb
```

Данная команда позволяет вывести на экран иерархически упорядоченную информацию обо всех подключенных USB устройствах.

Примечание

Если устройство было отключено и подключено повторно, то ему будут присвоены новые идентификаторы `Port`, `Dev` и `If`.

```
fakel@fakel:~$ show hardware usb
/:  Bus 03.Port 1: Dev 1, Class=root_hub, Driver=ehci-pci/2p, 480M
   |__ Port 1: Dev 2, If 0, Class=Hub, Driver=hub/4p, 480M
      |__ Port 3: Dev 4, If 0, Class=Vendor Specific Class, Driver=qcserial, 480M
      |__ Port 3: Dev 4, If 2, Class=Vendor Specific Class, Driver=qcserial, 480M
      |__ Port 3: Dev 4, If 3, Class=Vendor Specific Class, Driver=qcserial, 480M
      |__ Port 3: Dev 4, If 8, Class=Vendor Specific Class, Driver=qmi_wwan, 480M
/:  Bus 02.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 5000M
/:  Bus 01.Port 1: Dev 1, Class=root_hub, Driver=xhci_hcd/2p, 480M
   |__ Port 1: Dev 2, If 0, Class=Vendor Specific Class, Driver=pl2303, 12M
   |__ Port 2: Dev 3, If 0, Class=Hub, Driver=hub/4p, 480M
      |__ Port 4: Dev 5, If 2, Class=Vendor Specific Class, Driver=ftdi_sio, 480M
      |__ Port 4: Dev 5, If 0, Class=Vendor Specific Class, Driver=ftdi_sio, 480M
      |__ Port 4: Dev 5, If 3, Class=Vendor Specific Class, Driver=ftdi_sio, 480M
      |__ Port 4: Dev 5, If 1, Class=Vendor Specific Class, Driver=ftdi_sio, 480M
      |__ Port 3: Dev 4, If 0, Class=Hub, Driver=hub/4p, 480M
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
        |__ Port 3: Dev 6, If 0, Class=Hub, Driver=hub/4p, 480M
           |__ Port 4: Dev 8, If 2, Class=Vendor Specific Class, Driver=ftdi_sio,
 480M
           |__ Port 4: Dev 8, If 0, Class=Vendor Specific Class, Driver=ftdi_sio,
 480M
           |__ Port 4: Dev 8, If 3, Class=Vendor Specific Class, Driver=ftdi_sio,
 480M
           |__ Port 4: Dev 8, If 1, Class=Vendor Specific Class, Driver=ftdi_sio,
 480M
        |__ Port 4: Dev 7, If 3, Class=Vendor Specific Class, Driver=ftdi_sio,
 480M
        |__ Port 4: Dev 7, If 1, Class=Vendor Specific Class, Driver=ftdi_sio,
 480M
        |__ Port 4: Dev 7, If 2, Class=Vendor Specific Class, Driver=ftdi_sio,
 480M
        |__ Port 4: Dev 7, If 0, Class=Vendor Specific Class, Driver=ftdi_sio,
 480M
```

```
$ show hardware usb serial
```

Данная команда позволяет вывести на экран список всех подключенных последовательных USB устройств. Имя устройства (например, `usb0b2.4p1.0`) может быть использовано при обращении к последовательной консоли.

```
fakel@fakel$ show hardware usb serial
Device           Model               Vendor
------           ------              ------
usb0b4p1.0       FT232R_USB_UART     Future Technology Devices International, Ltd
usb0b4p1.1       FT232R_USB_UART     Future Technology Devices International, Ltd
usb0b4p1.2       FT232R_USB_UART     Future Technology Devices International, Ltd
```

2.10.2.2 Версия ПО Факел

```
$ show version
```

Данная команда позволяет вывести на экран информацию о версии и номере сборки **ПО Факел**. Эта информация также включает кодовое обозначение релиза.

```
Version:          Fakel release-1.0.2
Release:          1

Built by:         root@runner-9ksjjge3s-project-61-concurrent-0
Built on:         Wed 24 Jan 2024 07:23 UTC
Build UUID:       bea28a60-5a08-4a17-b61c-d52bdff1d262
Build commit ID:  2aaec83cfe645a

Architecture:     x86_64
```

(продолжается на следующей странице)

(продолжение с предыдущей страницы)

```
Boot via:         installed image
System type:      bare metal

Hardware vendor:  newplatforms
Hardware model:   NP-1008i
Hardware S/N:     SC21B001231009F9
Hardware UUID:    Unknown

Copyright:        IT Route, LLC
```

```
$ show version kernel
```

Данная команда позволяет вывести на экран информацию о версии ядра операционной системы Linux, дистрибутив которой лежит в основе **ПО Факел**.

```
fakel@fakel:~$ show version kernel
6.1.82-amd64-fakel
```

```
$ show version frr
```

Данная команда позволяет вывести на экран информацию о встроенной в **ПО Факел** подсистеме маршрутизации FRR[70], которая представляет собой архитектурный слой управления потоками данных (Control Plane) и является продуктом дальнейшего развития таких открытых (GNU) программных проектов маршрутизации, как Zebra и Quagga.

```
fakel@fakel:~$ show version frr
FRRouting 9.1 (infra-gw-01) on Linux(6.1.82-amd64-fakel).
Copyright 1996-2005 Kunihiro Ishiguro, et al.
```

[70] https://frrouting.org/

2.10.3 Параметры загрузки

Предупреждение

Возможности, описание которых представлено в данном разделе, могут оказать существенное влияние на работу системы, например, их использование может привести к прерыванию работы основных подсистем в составе ПО **Факел**. Необходимо использовать данные возможности с осторожностью и только в случаях, когда это действительно необходимо.

ПО Факел предоставляет управлять рядом параметров ядра операционной системы на этапе загрузки. Чтобы добавить параметр, необходимо выбрать соответствующий пункт в меню загрузчика операционной системы GRUB, нажать клавишу e, отредактировать строку параметров, затем использовать сочетание клавиш `Ctrl + X` для загрузки операционной системы.

2.10.3.1 Произвольный файл конфигурации

ПО Факел можно сообщить путь до произвольного файла конфигурации вместо `/config/config.boot`. Если указанный файл не существует или система не может его прочитать, происходит возврат **ПО Факел** к конфигурации по умолчанию. При чтении файла система не проводит проверку его структуры, поэтому очень важно обеспечить корректность файла конфигурации самостоятельно.

```
fakel-config=/path/to/file
```

Для загрузки файла конфигурации по умолчанию, наличие которого предусмотрено в **ПО Факел** на производстве, необходимо указать следующее значение для данной опции:

```
fakel-config=/opt/fakel/etc/config.boot.default
```

2.10.3.2 Отключение шагов загрузки

Использование данных опций приводит к пропуску определенных шагов при загрузке **ПО Факел**. Перед использованием опций рекомендуется детально ознакомиться с процессом загрузки, включая полный перечень шагов, из которых он состоит.

no-fakel-migrate
: При использовании данной опции не выполняется миграция конфигурации при обновлении версии ПО.

no-fakel-firewall
: При использовании данной опции не выполняется инициализация правил межсетевого экрана.

2.10.4 Восстановление пароля

Используя консоль, перезапустите маршрутизатор под управлением **ПО Факел**. После этого на экран будет выведено меню загрузчика операционной системы GRUB. Выберите необходимый пункт меню и нажмите клавишу `Enter`. Такой пункт должен содержать в названии текст «Lost password change».

После этого **ПО Факел** будут запущены утилиты восстановления `stand-alone` и `user-password`, которые запросят подтверждение сброса пароля локального пользователя системы.

```
Do you wish to reset the admin password? (y or n)
y
Which admin account do you want to reset? [fakel]
my_username
Enter my_username password:
Retype my_username password:
System will reboot in 10 seconds...
```

2.10.5 Дисковый массив

Дисковый массив - RAID (Redundant Array of Independent Disks) - использует два или более жестких диска для улучшения скоростных показателей операций чтения и записи, размещения больших объемов данных или обеспечения отказоустойчивости. Механизм RAID поддерживает несколько схем организации накопителей, каждая из которых отличается комбинацией характеристик емкости, надежности и производительности. **ПО Факел** поддерживает схему RAID 1. Схема RAID 1 позволяет использовать два или более жестких диска для зеркалирования областей хранения данных, чтобы обеспечить отказоустойчивость. В схеме RAID 1 каждый сектор одного диска дублируется сектором всех остальных дисков. Схема RAID 1 функционирует даже при наличии одного жесткого диска, то есть система продолжит работу в том числе при выполнении замены диска, если данная операция поддерживается аппаратной платформой. Схема RAID 1 может быть реализована либо с использование специализированного аппаратного обеспечения, либо программно.

ПО Факел поддерживает программную реализацию схемы RAID 1 из двух жестких дисков, а также предоставляет следующие возможности:

- обнаружение и уведомление об ошибках в работе жесткого диска;
- обеспечение работоспособности системы при сбоях одного из жестких дисков;
- обеспечение загрузки системы при сбоях одного из жестких дисков;
- замена жесткого диска после сбоев и инициализация повторной сборки дискового массива RAID;
- отслеживание статуса повторной сборки дискового массива RAID .

2.10.5.1 Варианты установки

Утилита установки **ПО Факел** предоставляет несколько вариантов установки на дисковый массив, собранный по схеме RAID 1:

- установка системы для создания дискового массива RAID 1;
- использование системных команд Linux для создания дискового массива RAID 1 перед установкой системы;
- использование предварительно созданного дискового массива RAID 1.

Примечание

Перед окончательной установкой на платформу **ПО Факел** работает в режиме live-установки.

2.10.5.2 Конфигурирование

Один диск и штатная установка

При установке **ПО Факел** утилита автоматически определяет наличие двух дисков, не являющихся частью дискового массива. В этом случае утилита установки предложит настроить дисковый массив RAID 1 и будет ожидать подтверждения.

```
Would you like to configure RAID 1 mirroring on them?
```

Если потребность в настройке дискового массива RAID 1 отсутствует, то необходимо ввести команду `No` в диалоге, после чего установка пойдет в штатном режиме.

Два и более пустых дисков

При установке **ПО Факел** утилита автоматически определяет наличие двух дисков, не являющихся частью дискового массива. В этом случае утилита установки предложит сконфигурировать дисковый массив RAID 1 и будет ожидать подтверждения.

```
Would you like to configure RAID 1 mirroring on them?
```

Для создания дискового массива RAID 1 необходимо ввести команду `Yes` в диалоге. Если утилита обнаруживает наличие некоторой файловой системы в разделах, которые должны быть использованы схемой RAID 1, то она запросит подтверждение продолжения процесса создания дискового массива RAID 1.

```
Continue creating array?
```

Если есть потребность перезаписать уже имеющуюся в разделах файловую систему, необходимо ввести команду `Yes`. В этом случае утилита выведет предупреждение, что все данные на обоих жестких дисках будут стерты, и будет ожидать подтверждения данного действия.

```
Are you sure you want to do this?
```

Если есть потребность сохранить текущую конфигурацию **ПО Факел** после завершения ее установки, необходимо ввести команду `Yes`. Если такой потребности нет, то необходимо ввести `No`, после чего текущая конфигурация будет удалена.

```
Would you like me to save the data on it before I delete it?
```

После всех принятых решений установка продолжится в штатном режиме.

Уже имеющийся дисковый массив

При установке **ПО Факел** утилита автоматически определяет наличие сконфигурированного ранее дискового массива RAID 1 и предлагает использовать его.

```
Would you like to use this one?
```

Если есть потребность разобрать имеющийся дисковый массив RAID 1, необходимо ввести команду `No`. После этого утилита установки автоматически определит наличие двух одинаковых жестких дисков и предложит сконфигурировать дисковый массив RAID 1, ожидая подтверждения.

```
Would you like to configure RAID 1 mirroring on them?
```

Если есть потребность отказаться от повторной сборки дискового массива RAID 1, необходимо ввести команду `No`. После этого утилита установки запросит имя раздела, на который необходимо установить систему.

```
Which partition should I install the root on? [sda1]:
```

После указания имени раздела утилита установки запросит подтверждения сохранения текущей конфигурации **ПО Факел**.

```
Would you like me to save the data on it before I delete it?
```

Если есть потребность сохранить текущую конфигурацию ПО Факел

после завершения ее установки, необходимо ввести команду Yes. Если такой потребности нет, то необходимо ввести No, после чего текущая конфигурация будет удалена.

После всех принятых решений установка продолжится в штатном режиме.

Обнаружение сбоев и замена диска

ПО Факел автоматически обнаруживает сбои диска в составе дискового массива RAID 1 и сообщает об этом посредством вывода сообщений в системной консоли. Удостовериться в сбое можно с помощью команды `show raid`.

Для замены диска после сбоев в составе дискового массива RAID 1 необходимо выполнить следующие действия:

1. Программно исключить диск из дискового массива с помощью следующей команды.

   ```
   $ delete raid <raid-1-device> member <disk-partition>
   ```

   Параметр `raid-1-device` - имя устройства в составе дискового массива RAID 1 (например, `md0`). Параметр `disk-parition` - имя раздела диска (например, `sdb2`).

2. Физически извлечь диск из системы. Если система не поддерживает возможность горячей замены дисков, потребуется сначала выключить систему.
3. Заменить диск на новый той же емкости или больше.
4. Форматировать новый диск перед добавлением в дисковый массив RAID 1 с помощью следующей команды.

```
$ format disk <disk-device1> like <disk-device2>
```

   Параметр `disk-device1` - имя нового диска (например, `sdb`). Параметр `disk-device2` - имя оставшегося в дисковом массиве устройства, функционирующего корректно (например, `sda`).

5. Программно включить новый диск в дисковый массив RAID 1 с помощью следующей команды.

```
$ add raid <raid-1-device> member <disk-partition>
```

   Параметр `raid-1-device` - имя устройства в составе дискового массива RAID 1 (например, `md0`). Параметр `disk-parition` - имя раздела диска (например, `sdb2`).

2.10.5.3 Эксплуатация

В данном разделе представлено описание возможностей по добавлению разделы диска в дисковый массив RAID 1, инициализации процесса зеркалирования, проверке текущего статуса и отображению подробной информации о дисковом массиве.

```
$ add raid <raid-1-device> member <disk-partition>
```

Данная команда позволяет добавить раздел диска в состав дискового массива RAID 1. Добавление раздела в дисковый массив приведет к запуску процесса зеркалирования, при котором все данные на существующем разделе будут скопированы на новый раздел.

```
$ format disk <disk-device1> like <disk-device2>
```

Данная команда позволяет подготовить диск к включению в предварительно собранный дисковый массив RAID 1 (устройство disk-device2 уже входит в состав дискового массива) посредством его форматирования.

```
$ show raid <raid-1-device>
```

Данная команда позволяет вывести на экран общую информацию о дисковом массиве и его составе, а также информацию о ходе процесса зеркалирования.

```
fakel@fakel:~$ show raid md0
/dev/md0:
   Version : 00.90
   Creation Time : Wed Oct 29 09:19:09 2008
   Raid Level : raid1
   Array Size : 1044800 (1020.48 MiB 1069.88 MB)
   Used Dev Size : 1044800 (1020.48 MiB 1069.88 MB)
   Raid Devices : 2
   Total Devices : 2
   Preferred Minor : 0
   Persistence : Superblock is persistent
   Update Time : Wed Oct 29 19:34:23 2008
   State : active, degraded, recovering
   Active Devices : 1
   Working Devices : 2
   Failed Devices : 0
   Spare Devices : 1
   Rebuild Status : 17% complete
   UUID : 981abd77:9f8c8dd8:fdbf4de4:3436c70f
   Events : 0.103

   Number   Major   Minor   RaidDevice   State
   0        8       1       0            active sync        /dev/sda1
   2        8       17      1            spare rebuilding   /dev/sdb1
```

```
$ show disk <disk-device>
```

Данная команда позволяет вывести на экран информацию о результатах форматирования жесткого диска.

```
fakel@fakel:~$ show disk sda format
Disk /dev/sda: 1073 MB, 1073741824 bytes
85 heads, 9 sectors/track, 2741 cylinders
Units = cylinders of 765 * 512 = 391680 bytes
Disk identifier: 0x000b7179
Device Boot     Start     End      Blocks       Id     System
/dev/sda1       6         2737     1044922+     fd     Linux raid autodetect
```

История изменений ПО

3.1 Версия 2.1

Версия 2.1 направлена на расширение сетевого функционала и повышение стабильности системы на высокопроизводительных платформах. Ключевые изменения включают внедрение поддержки базового стека протоколов (L3 VPN, Multicast, QoS), оптимизацию работы с памятью и исправление ошибок в работе механизмов агрегирования каналов и передачи трафика.

3.1.1 Версия 2.1.0 от 27 января 2026 г.

3.1.1.1 Исправленные ошибки

- FVE: Устранена проблема деградации трафика и кратковременных прерываний передачи (длительностью 10–60 сек).
- FVE: Исправлены ошибки логики работы агрегированных интерфейсов, повышена отказоустойчивость Bond-групп.
- FVE: Скорректирована нумерация и маппинг физических портов SFP+ для аппаратных платформ серий M500 и M1000.
- Включает исправленные ошибки версии 1.2.0

3.1.1.2 Новые функции и улучшения

- FVE: Реализована поддержка протоколов: - IpSec IPv4; - QoS IPv4; - VRF IPv4; - PIM/IGMP IPv4.
- FVE: Оптимизирован алгоритм распределения ресурсов между Data Plane и Control Plane.
- LIC: Добавлена поддержка и валидация лицензионных ключей обновленного формата (v1.1)
- NET: Реализована работа сценариев динамических Multipoint VPN сетей (Сценарий DMVPN).
- Включает новые функции и улучшения версии 1.2.0

3.1.1.3 Известные проблемы

- FVE: Не поддерживается обработка соединений по протоколу IPv6.
- FVE: Не поддерживается механизм защиты соединений synproxy.
- FVE: Не поддерживается MSS clamping для транзитного трафика.

- FVE: Ограничен функционал межсетевого экрана. Не поддерживается: - принудительное отключение контроля состояния соединений для правил фильтрации; - пользовательские цепочки правил; - вердикты continue, reject, jump, return; - глобальные опции; - фильтрация пакетов в режиме bridge firewall; - механизм обработки сетевых соединений flowtables; - использование зон в правилах.
- FVE: Ограничен функционал трансляции адресов. Не поддерживается: - механизм распределения нагрузки Load balance; - NAT64/NAT66;
- FVE: Не поддерживается механизм Policy based route.
- Включает известные проблемы версии 1.2.0

3.2 Версия 2.0

Новая версия программного обеспечения маршрутизатора Факел реализует собственные механизмы обработки сетевых соединений

В данной версии впервые используется собственный Dataplane-движок Fakel Vector Engine (FVE).

3.2.1 Версия 2.0.0 от 27 сентября 2024 г.

3.2.1.1 Новые функции и улучшения

- FVE: Произведен переход на высокопроизводительный Dataplane-движок FVE.

3.2.1.2 Известные проблемы

- FVE: Не поддерживается обработка соединений по протоколу IPv6.
- FVE: Не поддерживается работа механизма VRF.
- FVE: Не поддерживается механизм защиты соединений synproxy.
- FVE: Не поддерживается MSS clamping для транзитного трафика.
- FVE: Ограничен функционал межсетевого экрана. Не поддерживается: - принудительное отключение контроля состояния соединений для правил фильтрации; - пользовательские цепочки правил; - вердикты continue, reject, jump, return; - глобальные опции; - фильтрация пакетов в режиме bridge firewall; - механизм обработки сетевых соединений flowtables; - использование зон в правилах.
- FVE: Ограничен функционал трансляции адресов. Не поддерживается: - механизм распределения нагрузки Load balance; - NAT64/NAT66;
- FVE: Не поддерживается механизм Policy based route.
- FVE: Передача трафика может прерываться 10-60 секунд.
- SYS: Нумерация интерфейсов SFP+ не соответствует указанным значениям на лицевой панели устройств M500 и M1000.

3.3 Версия 1.2

В новой версии 1.2 внедрены механизмы управления полномочиями администраторов, расширены возможности динамической маршрутизации, обновлены системные пакеты и улучшена стабильность работы маршрутизатора.

3.3.1 Версия 1.2.0 от 11 августа 2025 г.

3.3.1.1 Исправленные ошибки

- PKI: Исправление необязательного force для принудительного обновления сертификатов certbot.
- NAT: Исправлено формирование ignore-правил для множественных портов.
- DHCP/DHCPv6: Исправлены аварийные остановки демона DHCPD и порядок запуска сервисов.
- RTR: Исправлен запрос default route при одном DHCPv6.
- RTR: Исправлено предупреждения о неверных area-type в OSPF.
- VRF: Исправление таблицы 254 по умолчанию.
- FW: Исправлено некорректная обработка диапазонов IP при формировании правил фильтрации.
- LOG: Исправления TCP-режима в демоне Syslog.
- MON: исправлена верификация *engineid* в SNMPv3.

3.3.1.2 Новые функции и улучшения

- QOS: Расширена политика CAKE и добавлен фильтр по EtherType.
- RTR: Реализована поддержка redistribute table для альтернативных таблиц маршрутизации.
- VRF: Возможность использовать route-map для inter-VRF «route leaking».
- LOG: Добавлена поддержка source-address для удалённых хостов.
- RTR: Добавлен match source-vrf и улучшена валидация импорта маршрутов между VRF.
- VPN: В IPSec добавлена генерация traffic-selector для VTI и поддержка iOS18 профилей (ExtendedAuthEnabled).
- SYS: Kea DHCP обновлён до 2.6.1-2.

3.4 Версия 1.1

Обновление ПО 1.1 продолжает развивать сетевые возможности маршрутизатора Факел. В этом выпуске изменена концепция межсетевого экрана, расширены возможности динамической маршрутизации и повышена стабильность работы ПО.

3.4.1 Версия 1.1.1 от 02 ноября 2024 г.

3.4.1.1 Исправленные ошибки

- VPN: Восстановлена работа режима TCP Only для VPN-сервера openconnect.

3.4.1.2 Новые функции и улучшения

- SYS: Синхронизировано ядро Linux версии 6.1.108 с репозиторием Центра верификации ОС Linux.
- NAT: Добавлен механизм трансляции NAT64 между протоколами IPv4 и IPv6.
- VRF: Добавлена поддержка протоколов динамической маршрутизации в VRF.
- RTR: Добавлен протокол динамической маршрутизации Babel.
- RTR: Добавлен протокол динамической маршрутизации PIM (Protocol-Independent Multicast) для IPv4 и IPv6.
- NET: Добавлен балансировщик нагрузки LVS (Linux Virtual Server).
- NET: Добавлен реверс-прокси для сервисов HTTP/HTTPS.
- MON: Добавлен встроенный агент для системы мониторинга Zabbix.
- FW: Добавлен механизм конфигурирования глобальных правил для межсетевого экрана.
- FW: Добавлена возможность использования зон интерфейсов в правилах межсетевого экрана.
- SYS: Добавлена возможность откатиться к предыдущей версии конфигурации без необходимости перезагрузки.
- LIC: Добавлена система лицензирования программного обеспечения маршрутизатора Факел

3.4.1.3 Известные проблемы

- RTR: Некорректно работает анонс маршрутов BGP в сценарии EVPN.

3.4.2 Версия 1.1.2 от 12 ноября 2024 г.

3.4.2.1 Исправленные ошибки

- RTR: Некорректно работает анонс маршрутов BGP в сценарии EVPN.
- SYS: Корректное имя пользователя при загрузке в режиме восстановления.

3.4.3 Версия 1.1.3 от 29 мая 2025 г.

3.4.3.1 Исправленные ошибки

- SYS: Нумерация интерфейсов SFP+ не соответствует указанным значениям на лицевой панели устройств M500 и M1000.
- RTR: Не запускается демон маршрутизации PIMd после перезагрузки устройства.

Алфавитный указатель

Не-алфавитный

#
    опция командной строки, 36, 313325, 658, 659, 743745, 749
$
    опция командной строки, 326328, 745, 746, 749752, 757, 758
-
    опция командной строки, 36
•
    опция командной строки, 2022, 24, 26, 27, 2935, 37, 281283, 285, 287289, 292304, 306309, 331, 332, 335342, 346351, 359362, 365370, 375, 376, 379, 380, 382, 384, 386, 388, 389, 393396, 401403, 413, 414, 641, 642, 645648, 650, 652655, 660, 667, 668, 676678, 694696, 699, 700, 704709, 711, 712, 716720, 723725, 727729, 731, 732, 734738, 740, 741

O

опция командной строки
    #, 36, 313325, 658, 659, 743745, 749
    $, 326328, 745, 746, 749752, 757, 758
    -, 36
    •, 2022, 24, 26, 27, 2935, 37, 281283, 285, 287289, 292304, 306309, 331, 332, 335342, 346351, 359362, 365370, 375, 376, 379, 380, 382, 384, 386, 388, 389, 393396, 401403, 413, 414, 641, 642, 645648, 650, 652655, 660, 667, 668, 676678, 694696, 699, 700, 704709, 711, 712, 716720, 723725, 727729, 731, 732, 734738, 740, 741

N

no-fakel-firewall, **753**
no-fakel-migrate, **753**

R

RFC
    RFC 791, 651
    RFC 826, 699
    RFC 1058, 339
    RFC 1195, 333
    RFC 1583, 294
    RFC 1702, 397
    RFC 1930, 310
    RFC 2328, 291
    RFC 2332, 397
    RFC 2439, 321
    RFC 2453, 339
    RFC 2474, 638
    RFC 2763, 335
    RFC 3021, 409
    RFC 3137, 294
    RFC 3509, 294
    RFC 3633, 393
    RFC 3719, 336
    RFC 3768, 668
    RFC 3787, 335
    RFC 4301, 397
    RFC 4456, 325
    RFC 4595, 638
    RFC 5036, 358, 361
    RFC 5065, 325
    RFC 5082, 317
    RFC 5291, 324
    RFC 5303, 336
    RFC 5308, 333
    RFC 5340, 291
    RFC 5880, 350
    RFC 5881, 350
    RFC 5883, 350
    RFC 6232, 335
    RFC 6480, 329

RFC 6793, 310
RFC 7552, 361
RFC 7606, 325
RFC 8210, 329
RFC 8405, 338