Содержание

Обработка трафика по VLAN

Данные `vlan group` перенесены из UDR в SDR. Глобальные правила для `vlan drop`, `vlan pass`, `vlan hide`, `vlan permit`, заданные прежней CLI-командой `vlan group`, сконвертированы и перенесены из UDR в SDR с удалением из UDR.

1. Дроп трафика без анализа из конкретного VLAN:

```
fdpi_cli vlan rule add <id> perm drop
```

2. Дроп трафика с предварительным анализом, но без передачи в статистике Netflow из конкретного VLAN (Используется для работы с асимметричным трафиком, когда на площадку подается дубль трафика с другой площадки. Необходимо провести анализ и дропнуть трафик, чтобы он не попал в статистику):

```
fdpi_cli vlan rule add <id> perm hide
```

3. Пропуск трафика без какого-либо анализа из конкретного VLAN:

```
fdpi_cli vlan rule add <id> perm pass
```

4. Вывод существующих настроек в UDR:

```
fdpi_cli vlan rule dump
```

Для вывода правил только определённого типа (например, только `perm`) используется параметр `[type]`:

```
fdpi_cli vlan rule dump perm
```

Пример вывода команды:

```
# fdpi_cli vlan rule dump
1000  perm hide
2000  perm drop
3000  perm pass
4000  perm hide
```

В данном примере видно, что все протоколы, относящиеся к VLAN 1000 и 4000 попадают под влияние hide, то есть трафик с одной площадки дублируется на другую площадку; VLAN 2000 — трафик дропается, VLAN 3000 — трафик пропускается.

Подробнее в разделе Настройка Service-Name для VLAN

VLAN Rule

VLAN Rule позволяет гибко управлять сетевым трафиком на уровне VLAN и QinQ, назначать определенные политики обработки пакетов для отдельных VLAN, диапазонов VLAN или QinQ-туннелей.

Типы правил

Поддерживаются следующие типы правил:

- `dhcp` — управляет обработкой DHCP-запросов.
  - `dhcp enable` — разрешить обработку DHCP-запросов в данном VLAN/QinQ.
  - `dhcp disable` — запретить обработку DHCP. Все DHCP-пакеты в этом VLAN/QinQ будут отбрасываться.
- `perm` — определяет базовую обработку всего трафика в VLAN/QinQ.
  - `drop` — полностью отбрасывать все пакеты. Пакеты не проходят дальнейшую обработку и не попадают в статистику Netflow.
  - `pass` — пропускать пакеты без обработки. Пакеты учитываются в статистике Netflow.
  - `accept` — пропускать пакеты для дальнейшей полной обработки в системе. Пакеты учитываются в статистике Netflow.
  - `hide` — пакет проходит внутренние этапы обработки (с исключениями), но после обработки в любом случае отбрасывается. При этом:
    - пакет не попадает в статистику Netflow;
    - не применяются услуги 9, 12, 15, 18, NAT, а также полисинг (общий и канальный);
    - пакет не записывается через ajb — в IPFIX, SIP, FTP и др.
- `pppoe` — управляет обработкой PPPoE-пакетов. Поддерживается фильтрация по Service-Name, в том числе для QinQ-туннелей. Доступны следующие действия:
  - `enable` — разрешить обработку PPPoE.
  - `drop` — дропать пакеты PPPoE.
  - `pass` — пропустить пакеты PPPoE насквозь без обработки.
  - `delay N` — устанавливать PPPoE-сессию с задержкой в N секунд ($0 < N < 16$). Правила могут быть заданы как для всего PPPoE-трафика в диапазоне VLAN/QinQ, так и для конкретного Service-Name.

Синтаксис описания диапазонов VLAN/QinQ

Правила применяются к диапазонам, которые задаются в следующем формате:

- Для одиночного VLAN: `156`
- Для диапазона VLAN: `56-78` (VLAN с 56 по 78 включительно)
- Для любого VLAN: `*` или `any`
- Для QinQ:
  - `67.*` или `67.any` — S-VLAN=67, любой C-VLAN.
  - `*.68` или `any.68` — любой S-VLAN, C-VLAN=68.
  - `*.*` или `any.any` — любой QinQ.
  - `12-156.78-90` — диапазон S-VLAN [12..156], диапазон C-VLAN [78..90].

- `609.1-199` — S-VLAN=609, диапазон C-VLAN [1..199].

Правила для обычных VLAN (`67`) и QinQ (`67.*`) являются независимыми и не пересекаются.

Поддержка Service-Name для QinQ
Правила с Service-Name корректно работают для QinQ:

- Правила без селективности по CVLAN: `SVLAN.*` с указанием Service-Name и без него.
- Полный QinQ (`SVLAN.CVLAN`) с селективностью по Service-Name.

Приоритет правил

Если диапазоны нескольких правил пересекаются, система определяет итоговое действие по принципу "от общего к частному":

1. Сначала применяются правила с самыми широкими диапазонами (например, 1-4095 или any.any).
2. Затем правила с более узкими диапазонами (например, 100-200) могут переопределить действие, заданное общими правилами.

Пример:
Следующие правила создадут политику: "Запретить DHCP для всех VLAN в диапазоне 300-700, но разрешить его для VLAN 645 и диапазона 430-439".

```
vlan rule add 300-700 dhcp disable
vlan rule add 645 dhcp enable
vlan rule add 430-439 dhcp enable
```

Управление

- `vlan rule add` — добавление нового правила в SDR.
  Синтаксис для PPPoE:
  - Добавление правила для всего PPPoE-трафика в диапазоне:

    ```
    vlan rule add <Range> pppoe [enable | drop | pass | delay N]
    ```

  - Добавление правила для конкретного Service-Name:

    ```
    vlan rule add <Range> pppoe sname <Service-Name> [enable | drop |
    pass | delay N]
    ```

    Здесь `<Service-Name>` — имя PPPoE Service-Name в одинарных или двойных кавычках (можно без кавычек, если является идентификатором: `[a-zA-Z_][a-zA-Z_0-9]*`).

- `vlan rule modify` — изменение существующего правила в SDR (аналогичный синтаксис).

- `vlan rule delete` — удаление правила из SDR.
- `vlan rule show` — показывает все правила для указанного VLAN/QinQ. В выводе отображаются не только общие действия для PPPoE, но и все разрешения для отдельных Service-Name.
- `vlan rule dump` — выводит дамп всех правил в SDR. Для фильтрации вывода по типу правил используется параметр `[type]` (например, `vlan rule dump perm`).
- `vlan rule purge vlan/qinq/all` — очистка SDR VLAN/QinQ или обоих.
- `vlan rule apply` — применение правил; по умолчанию правила применяются спустя 5 минут после последней модификации SDR.

При использовании * в CLI для QinQ-диапазонов рекомендуется заключать выражение в кавычки (например, `'*.68'`) или использовать ключевое слово any (например, `any.68`), чтобы избежать некорректной интерпретации символа * оболочкой bash.

Особенности применения изменений: Изменения правил, внесенные командами add, `modify` или `delete`, сохраняются в SDR и автоматически применяются системой спустя 5 минут после последней модификации. Команда `vlan rule apply` позволяет применить их принудительно, но не чаще одного раза в минуту.

Использование VLAN Rule в L2-балансировщике

Правила VLAN также могут применяться компонентом **L2-балансировщик** для фильтрации пакетов. Это позволяет на этапе балансировки трафика отсеивать ненужные VLAN/QinQ до их попадания в основные обрабатывающие модули.

Пример:
Требуется дропнуть трафик по номеру одиночного тега 133, а также по qinq S-tag 266.
Для этого выполнить команды:

1. Дроп трафика, тег которого равняется 133:

   ```
   fdpi_cli vlan rule add 133 perm drop
   ```

   Будет дропнут весь трафик, в котором есть одиночный тег 133 (трафик Q-in-Q не будет затронут)

2. Дроп трафика, Service-тег которого равняется 266:

   ```
   fdpi_cli vlan rule add '266:*' perm drop
   ```

   Будет дропнут весь трафик, в котором есть двойной тег, S-тег которого равняется 266 и любым C-тег (266:0-4095)