Содержание

Обработка трафика по VLAN 3
VLAN Rule 3
Типы правил 4
Синтаксис описания диапазонов VLAN/QinQ 4
Приоритет правил 4
Управление 5

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
```

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.
  - `pass` / `accept` — пропускать пакеты для дальнейшей обработки в системе.
  - `hide` — (специфичное действие системы, например, скрыть VLAN от широковещательных запросов).

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.

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
- `vlan rule modify` — изменение существующего правила в SDR
- `vlan rule delete` — удаление правила из SDR
- `vlan rule show` — показывает все правила для указанного VLAN/QinQ
- `vlan rule dump` — выводит дамп всех правил в SDR
- `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.