Содержание

Настройка экспорта NetFlow с netflow_dev 3
Общие настройки экспрота статистики 3
NetFlow по протоколам 4
NetFlow по направлениям 4
NetFlow для биллинга 4
Полный NetFlow 5
Отправка template в IPFIX 6
Пример конфигурации 6

Настройка экспорта NetFlow с netflow_dev

Изменение настроек или отключение опции осуществляется с помощью редактирования файла конфигурации `/etc/dpi/fastdpi.conf`.

Параметры NetFlow являются холодными и требуется перезапуск сервиса.

Общие настройки экспрота статистики

Включение сбора и экспорта статистики:

```
netflow=1
```

- 0 или не указано - опция отключена
- 1 - экспорт статистики по протоколам (номерам портов)
- 2 - экспорт статистики по направлениям (номерам автономных систем)
- 4 - экспорт статистики для биллинга
- 8 - экспорт полной статистики по сессиям

3 = 1 + 2 — одновременный экспорт статистики по протоколам и по направлениям (аналогично для других вариантов)
12 = 8 + 4 — одновременный экспорт Full NetFlow и биллинговой статистики. В частности используется дла RADIUS Accaunting

Имя сетевого интерфейса, через который будет отправляться netflow со статистикой:

```
netflow_dev=eth2
```

Периодичность экспорта данных (в секундах):

```
netflow_timeout=10
```

Нужно выделить отдельный коллектор для каждого типа, чтобы данные не смешивались!

Параметры IPFIX/Netflow можно изменять без перезагрузки fastDPI.
Конфигурационный параметр `ipfix_reserved` позволяет зарезервировать необходимую память для возможности включения/измененения параметров IPFIX/Netflow.
В случае задания параметров IPFIX/Netflow в конфигруационном файле, автоматически включается резервирование памяти для IPFIX/Netflow, параметры и новые типы экспортеров IPFIX/Netflow можно изменять без перезагрузки

fastDPI.

NetFlow по протоколам

IP адрес и номер порта коллектора NetFlow со статистикой **по протоколам**:

```
netflow_collector=192.168.0.1:9997
```

NetFlow по направлениям

IP адрес и номер порта коллектора NetFlow со статистикой **по направлениям**:

```
netflow_as_collector=192.168.0.1:9998
```

Направления по которым производится сбор статистики и агрегация:

```
netflow_as_direction=1
```

- 1 - только для внешних автономных систем (подходит для домовых операторов, так как с одной из сторон кроме самого оператора других автономных систем нет)
- 2 - только для внутренних автономных систем
- 3 = 1 + 2 - подходит для транзитных операторов, но так как по AS производится независимая агрегация, то в экпортируемую статистику данные попадут 2 раза - для каждой из AS, участников передачи

NetFlow для биллинга

IP адрес и номер порта коллектора NetFlow со **статистикой для биллинга**, нужно выделить отдельный коллектор, чтобы данные не смешивались с другой статистикой:

```
netflow_bill_collector=192.168.0.1:9995
```

Биллинговая статистика передается только по абонентам, которым подключена услуга 9.
В IPFIX не передается информация о host IP:port, с которым абонент обменивается информацией.

Определение формата передаваемой информации:

```
netflow_bill_collector_type=2
```

- 0 - netflow_v5 (default)
- 1 - ipfix udp
- 2 - ipfix tcp

По умолчанию считается полный объем передаваемой информации, включая заголовки пакетов L1-L7, чтобы учитывались payload и только L3-L7 заголовки необходимо указать параметр:

```
netflow_bill_method=1
```

В netflow поле TOS статистики для биллинга передается класс трафика, назначенный DPI, который можно использовать для создания гибких тарифных планов.

Полный NetFlow

IP адрес и номер порта коллектора **NetFlow с полной статистикой**, нужно выделить отдельный коллектор, чтобы данные не смешивались с другой статистикой:

```
netflow_full_collector=192.168.0.1:9996
netflow_passive_timeout=30
netflow_active_timeout=300
```

где

- netflow_passive_timeout=30 время ожидания активности в сессии после которого, если не было активности, сессия считается завершенной и происходит передача по ней информации
- netflow_active_timeout=300 время, через которое сообщается информация по длинным сессиям (т.е. фактически длинные сессии разбиваются на фрагменты данной продолжительности)

В формате netflow5 в полной статистике сохранены оригинальные номера портов, а информация о детектированных протоколах передается в обычно неиспользуемых байтах 46-47. Если требуется проанализировать используемые протоколы, то можно установить настройку, по которой информация о протоколах будет передаваться в номере порта:

```
netflow_full_port_swap=1
```

Для совместимости со старыми коллекторами эта настройка действует и для формата ipfix, но использовать ее совместно с ipfix не рекомендуется, т.к. информация о протоколе передается в ipfix в отдельном специальном поле.

Рекомендуем использовать передачу Полного NetFlow в формате IPFIX через TCP. Протокол NetFlow не гарантирует доставку пакетов (т.к. работает поверх udp) и

если коллектор не справляется с приемом данных, то часть пакетов просто теряется. Передача полной статистики netflow для канала 10G требует от коллектора возможности принимать данные со скоростью не менее 60 Мбит/с. Проверьте возможности вашего коллектора перед направлением на него netflow трафика. В тоже время при передаче netflow из dpi могут кратковременно возникать пики до 100 Мбит/с. Такой поток данных без потерь способны принять немногие коллекторы, например, nfsen/nfdump.

Чтобы сгладить пики и равномернее распределить нагрузку на коллектор установите настроечный параметр

```
netflow_rate_limit=60
```

где 60 это максимальный поток netflow в Мбит/с.

Значение параметра следует устанавливать исходя из расчета: 6 Мбит/с на каждый 1G внешнего канала. Установка недостаточной величины приведет к отбрасыванию данных уже на стороне DPI. Информация об этом событии будет зафиксирована в логе **/var/log/dpi/fastdpi_alert.log**.

Отправка template в IPFIX

1. Транспортный протокол TCP.
   Template отправляется один раз после установления TCP-сессии.
2. Транспортный протокол UDP.
   Template отправляется по умолчанию каждые 20 секунд. Регулируется параметром `ipfix_udp_template_timer`.

Пример конфигурации

Пример настройки описан в разделе QoE Stor: Конфигурация DPI