Содержание

Настройка экспорта Full NetFlow в формате IPFIX

Общие обязательные настройки отправки NetFlow

Включение сбора и экспорта статистики:

```
netflow=1
```

- 0 или не указано - опция отключена
- 1 - экспорт статистики по протоколам (номерам портов), подробнее в разделе Настройка экспорта NetFlow по протоколам, направлениям и биллингу
- 2 - экспорт статистики по направлениям (номерам автономных систем), подробнее в разделе Настройка экспорта NetFlow по протоколам, направлениям и биллингу
- 4 - экспорт статистики для биллинга, подробнее в разделе Настройка экспорта NetFlow по протоколам, направлениям и биллингу
- 8 - экспорт полной статистики по сессиям, Full NetFlow в формате NetFlow v5 или IPFIX

Одновременный экспорт Full NetFlow и биллинговой статистики включается через битовую маску netflow=12 (8 + 4). Статистика для биллинга конвертируется в RADIUS Accounting через FastPCRF при включении enable_acct=1. Настройка RADIUS Accounting

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

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

```
netflow_dev=eth2
```

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.

Для приема, обработки и хранения IPFIX рекомендуется использовать Программный продукт для сбора статистики QoE Store и Графический интерфейс DPIUI2.

Для сбора информации в формате IPFIX подойдет любой универсальных IPFIX коллектор, понимающий шаблоны, или утилита IPFIX Receiver.

Общие дополнительные настройки отправки NetFlow

Периодичность экспорта данных (в секундах):

```
netflow_timeout=10
```

Время ожидания сессии:

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

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

```
netflow_rate_limit=900
```

где 900 это максимальный поток netflow в Мбит/с.

Значение параметра следует устанавливать исходя из расчета: что каждый DPI генерирует IPFIX поток на скорости от 0,5% до 1% от скорости реального трафика.
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**.

Настройка Full NetFlow

Указать IP адрес и номер порта коллектора **Full NetFlow**, нужно выделить отдельный коллектор для каждого FastDPI, чтобы данные не смешивались с другой статистикой:

```
netflow_full_collector=192.168.0.1:9996
```

Указать формат экспорта **Full NetFlow**:

```
netflow_full_collector_type=2
```

Возможные значения:

- **0** - экспорт в формате NetFlow5 (значение по умолчанию).
- **1** - экспорт IPFIX на UDP коллектор.
- **2** - экспорт IPFIX на TCP коллектор.

Рекомендуем использовать передачу Full NetFlow в формате IPFIX через TCP (значение параметра 2).
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 **Full NetFlow** для трафика на DPI в 10G требует от коллектора возможности принимать данные со скоростью не менее 60 Мбит/с.
Проверьте возможности вашего коллектора перед направлением на него **Full NetFlow** статистики. В тоже время при передаче **Full NetFlow** из DPI могут кратковременно возникать пики до 100 Мбит/с при всплесках количества сессий.

Дополнительные параметры Full NetFlow

Параметр `netflow_tos_format` определяет формат данных поля TOS в IPFIX. Возможные значения:

- **0** - передается 3 bit (значение по умолчанию).
- **1** - передается 6 bit (полный DSCP).

Параметр `netflow_plc_stat` определяет набор передаваемых данных статистики отброшенных пакетов согласно правил полисинга или drop. Параметр является битовой маской.
По умолчанию маска имеет значение **0x07** — передается статистика по отброшенным данным сессионного + абонентского + полисинга виртуальных каналов.


Влияет на формирование счетчиков DROPPED_BYTES и DROPPED_PACKETS.
Значения, из которых складывается маска:

- **0xff** - передается любой drop
- **0** - не считать
- **1** - считать для сессионного полисинга
- **2** - считать для абонентского полисинга
- **4** - считать для полисинга виртуальных каналов
- **8** - считать при отбросе (drop) пакетов по протоколу
- **16** - считать во всех иных случаях

Параметр `ipfix_mtu_limit` задает максимальный размер пакета UDP при отправке IPFIX. По умолчанию равен минимальному размеру MTU используемых для отправки интерфейсов.

В параметре `tethering_ttl_allowed = 128:64` указывается список допустимых значений TTL для трафика от абонента, которые не считаются tethering. Значения перечисляются через ':'. Количество значений до 256 (0-255).

Шаблон экспорта в формате IPFIX (Netflow v10) для протокола IPv4

Шаблон экспорта для IPv4						
№	**Кол-во байт**	**Тип данных**	**IANA**	**Описание**	**Примечание**	**Использование в QoEStor**
1	8	int64	0	OCTET_DELTA_COUNT	Аналог в NetFlow v9 IN_BYTES	Используется
2	8	int64	0	PACKET_DELTA_COUNT	Аналог в NetFlow v9 IN_PKTS	Используется
4	1	int8	0	PROTOCOL_IDENTIFIER	Аналог в NetFlow v9 PROTOCOL	Используется
5	1	int8	0	IP_CLASS_OF_SERVICE	Аналог в NetFlow v9 TOS	Используется
7	2	int16	0	SOURCE_TRANSPORT_PORT	Аналог в NetFlow v9 L4_SRC_PORT	Используется
8	4	int32	0	SOURCE_IPV4_ADDRESS	Аналог в NetFlow v9 IPV4_SRC_ADDR	Используется
11	2	int16	0	DESTINATION_TRANSPORT_PORT	Аналог в NetFlow v9 L4_DST_PORT	Используется
12	4	int32	0	DESTINATION_IPV4_ADDRESS	Аналог в NetFlow v9 IPV4_DST_ADDR	Используется
16	4	int32	0	BGP_SOURCE_AS_NUMBER	Аналог в NetFlow v9 SRC_AS	Используется
17	4	int32	0	BGP_DESTINATION_AS_NUMBER	Аналог в NetFlow v9 DST_AS	Используется
152	8	int64	0	FLOW_START_MILLISECOND		Используется
153	8	int64	0	FLOW_END_MILLISECOND		Используется
10	2	int16	0	INPUT_SNMP	Аналог в NetFlow v9 IngressInterface	Используется
14	2	int16	0	OUTPUT_SNMP	Аналог в NetFlow v9 EgressInterface	Используется
60	1	int8	0	IP_VERSION	Аналог в NetFlow v9 IP_PROTOCOL_VERSION	Используется
2000	8	int64	43823	SESSION_ID		Используется
2001	-	string	43823	HTTP_HOST или CN_HTTPS		Используется
2002	2	int16	43823	DPI_PROTOCOL		Используется
2003	-	string	43823	LOGIN	Аналог в Radius User-Name	Используется
225	4	int32	0	POST_NAT_SOURCE_IPV4_ADDRESS		Используется
227	2	int16	0	POST_NAPT_SOURCE_TRANSPORT_PORT		Используется
2010	2	int16	43823	FRGMT_DELTA_PACKS	Дельта фрагментированных пакетов.	Используется
2011	2	int16	43823	REPEAT_DELTA_PACK	Дельта ретрансмиссий.	Используется
2012	4	int32	43823	PACKET_DELIVER_TIME	Задержка (RTT/2) в мс (RTT=round-trip time).	Используется
2016	2	int16	43823	BRIDGE_CHANNEL_NUM	Номер канала (vchannel) или моста. Если в конфигурации DPI настроены vchannel, то будет передаваться номер канала, иначе номер моста.	Используется

Шаблон экспорта для IPv4						
№	**Кол-во байт**	**Тип данных**	**IANA**	**Описание**	**Примечание**	**Использование в QoEStor**
6	2	int16	0	TCP_FLAGS	Биты управления TCP	Используется
58	2	int16	0	SRC_VLAN	VLAN ID	Используется
59	2	int16	0	DST_VLAN	Post VLAN ID	Используется
56	6	mac_address	0	SRC_MAC	MAC-адрес источника	Используется
57	6	mac_address	0	DST_MAC	MAC-адрес получателя	Используется
2017	-	raw	43823	MPLS Lables		Используется
132	8	int64	0	DROPPED_BYTES	Дельта-счет сброшенных октетов. *Например: данные сбрасываются на T1 и на T2 минуте. Дельта будет показывать разницу количества октетов между T1 и T2 минутой.*	Используется
133	8	int64	0	DROPPED_PACKETS	Дельта-счет сброшенных пакетов. *Например: данные сбрасываются на T1 и на T2 минуте. Дельта будет показывать разницу количества пакетов между T1 и T2 минутой.*	Используется
2019	1	int8	43823	originalTOS	Оригинальное значение TOS из IP заголовка	Используется
192	1	int8	0	IP_TTL	TTL пакетов	Используется
2020	2	int16	43823	RATING_GROUP	Номер rating group	Используется
2021				SERVICE_FLAGS	Информация о метках, которые получил flow в DPI. Детектированный tethering сообщается по IPFIX в бите 1 поля `service_flags`. Доступны 63 бита для дальнейшего использования	Используется
2022				DETECTION_FLAGS	Зарезервировано под метод детекции	Используется
2023				ACTION_FLAGS	Зарезервировано под передачу информации о действиях с flow	Используется

Шаблон экспорта в формате IPFIX (Netflow v10) для протокола IPv6

Шаблон аналогичен IPv4 за исключением того, отсутствуют поля: ***SOURCE_IPV4_ADDRESS*, *DESTINATION_IPV4_ADDRESSs*, *POST_NAT_SOURCE_IPV4_ADDRESS*, *POST_NAT_SOURCE_TRANSPORT_PORT***, – и присутствуют следующие:

Шаблон экспорта для IPv6					
№	**Кол-во байт**	**Тип данных**	**IANA**	**Описание**	**Примечание**
27	16	int128	0	SOURCE_IPV6_ADDRESS	Аналог в NetFlow v9 IPV6_SRC_ADDR
28	16	int128	0	DESTINATION_IPV6_ADDRESS	Аналог в NetFlow v9 IPV6_DST_ADDR

Настройка Netflow v5

В формате Netflow v5 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.