Содержание

1 Общее описание

СКАТ DPI поддерживает выгрузку статистики в форматах:

- IPFIX (NetFlow v10)
- NetFlow v5

IPFIX

Экспорт статистики для биллинга, полной статистики по сессиям. Формат выгрузки описан в разделе Настройка экспорта в формате IPFIX.
Для приема, обработки и хранения NetFlow предлагаем использовать программный продукт для сбора статистики QoE Store и графический интерфейс DPIUI2.

В разделе логирования с помощью IPFIX описан экспорт метаинформации:

- ClickStream
- SIP
- FTP
- мессенджеров (XMPP)
- почтовых протоколов (POP,IMAP,SMTP)
- сырых нераспарсенных метаданных

NetFlow v5

Данный формат поддерживается большинством бесплатных и коммерческих средств для сбора и анализа статистики. Для удобства пользователей мы поставляем бесплатное ПО для просмотра и анализа статистики - слегка адаптированную версию nfsen, дополненную информацией об именах протоколов и автономных систем.

Передача DPI информации в формате netflow5 имеет ряд особенностей:

1. Для передачи информации об используемом протоколе используется поле dstport (номер порта). Когда это возможно используется номер порта, закрепленный за протоколом ассоциацией IANA, но для протоколов со свободным номером (торренты, скайп и т.п.) выделен специальный номер в верхнем диапазоне (49152-65534), зарезервированном IANA для приватных портов. Если протокол определить не удалось, ему назначается номер порта 65535.
2. Статистика по протоколам передается в агрегированном виде, т.е. DPI накапливает статистику по протоколу, объединяя информацию по разным сессиям, а потом с заданной периодичностью передает ее на коллектор. Это позволяет существенно снизить объем передаваемой информацией.
3. Информация о направлениях передается в поле dst_as (номер автономной системы)

4. Статистика по направлениям передается в агрегированном виде, т.е. DPI накапливает статистику по направлению (номеру AS), объединяя информацию по разным сессиям, а потом с заданной периодичностью передает ее на коллектор. Это позволяет существенно снизить объем передаваемой информацией.