Содержание

Журналирование NAT трансляций

Экспорт трансляций на внешние коллекторы в формате IPFIX

Для анализа данных по совершенным NAT трансляциям на внешних системах, можно экспортировать эти данных по сети в формате IPFIX (aka NetFlow v10)

Экспорт NAT трансляций настраивается следующими параметрами:

```
ipfix_dev=em1
ipfix_nat_udp_collectors=1.2.3.4:1500,1.2.3.5:1501
ipfix_nat_tcp_collectors=1.2.3.6:9418
```

где

- **em1** - имя сетевого интерфейса для экспорта.
- **ipfix_nat_udp_collectors** - адреса UDP коллекторов, поддерживается до 2шт.
- **ipfix_nat_tcp_collectors** - адреса TCP коллекторов, поддерживается до 2шт.

Формат IPFIX шаблона для экспорта NAT трансляций					
ID	**IANA**	**Кол-во байт**	**Тип данных**	**Описание**	**Примечание**
323	0	8	int64	SYSTEM_TIME_WHEN_THE_EVENT_OCCURRED	Системное время, когда произошло событие
4	0	1	int8	PROTOCOL_IDENTIFIER	Идентификатор протокола транспортного уровня
230	0	1	int8	TYPE_OF_EVENT	Тип события
8	0	4	IPv4	SOURCE_IPV4_ADDRESS	Адрес отправителя
225	0	4	IPv4	POST_NAT_SOURCE_IPV4_ADDRESS	Адрес отправителя после NAT
7	0	2	int16	SOURCE_PORT	Порт отправителя
227	0	2	int16	POST_NAPT_SOURCE_TRANSPORT_PORT	Порт отправителя после NAT
12	0	4	IPv4	DESTINATION_IPV4_ADDRESS	Адрес получателя
11	0	2	int16	DESTINATION_TRANSPORT_PORT	Порт получателя
2000	43823	8	int64	SESSION_ID	Идентификатор сессии
2003	43823	-	string	LOGIN	User name при входе в систему

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

Также информация о NAT трансляциях передается в полях postNATsourceIPv4Address и

postNAPTsourceTransportPort при экспорте полного Netflow

Ведение журнала трансляций в текстовом формате

Для записи NAT трансляций в текстовый лог на сервере СКАТ в конфигурационном файле */etc/dpi/fastdpi.conf* настраиваются следующие параметры:

```
ajb_save_nat=1
ajb_save_nat_format=ts:ssid:event:login:proto:ipsrc:portsrc:ipsrcpostnat:por
tsrcpostnat:ipdst:portdst
ajb_nat_path=/var/dump/dpi
ajb_nat_ftimeout=30
```

где

- ajb_save_nat=1 активировать запись трансляций в текстовый лог
- ajb_nat_path=/var/dump/dpi место размещения файлов с записью логов (по умолчанию /var/dump/dpi)
- ajb_nat_ftimeout=30 периодичность записи
- ajb_save_nat_format=ts:ssid:event:login:proto:ipsrc:portsrc:ipsrcpostnat:portsrcpostnat:ipdst:portdst список и порядок записываемых полей, где
  - ts - временная метка
  - ssid - идентификатор сессии (для связи с данными Netflow/IPFIX по объемам)
  - event - событие : 1 - NAT44 Session create, 2 - NAT44 Session delete
  - login - login абонента
  - ipsrc - IP адрес источника запроса (абонента)
  - portsrc - порт источника запроса (абонента)
  - ipsrcpostnat - IP адрес источника запроса (абонента) после NAT трансляции
  - portsrcpostnat - порт источника запроса (абонента) после NAT трансляции
  - ipdst - IP адрес получателя запроса (хоста)
  - portdst - порт получателя запроса (хоста)

Файловая система для записи логов должна быть быстрой и локальной (никаких NFS и других remote), данный вариант журналирования рекомендуется только в целях кратковременной диагностики

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`.