

Содержание

2 Экспорт трансляций на внешние коллекторы в формате IPFIX	3
---	----------

2 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
- ipfix_nat_tcp_collectors адреса tcp коллекторов

Формат IPFIX шаблона для экспорта NAT трансляций

ID	IANA	Кол-во байт	Тип данных	Описание
323	0	8	int64	SYSTEM TIME WHEN THE EVENT OCCURRED
4	0	1	int8	PROTOCOLIDENTIFIER
230	0	1	int8	TYPE OF EVENT
8	0	4	IP v4	SOURCEIPV4ADDRESS
225	0	4	IP v4	POSTNATSOURCEIPV4ADDRESS
7	0	2	int16	SOURCE PORT
227	0	2	int16	POSTNAPTSOURCETRANSPORTPORT
12	0	4	IP v4	DESTINATIONIPV4ADDRESS
11	0	2	int16	DESTINATIONTRANSPORTPORT
2000	43823	8	int64	SESSION_ID
2003	43823		string	LOGIN

Для сбора информации в формате IPFIX подойдет любой универсальный IPFIX коллектор, который понимает шаблоны, или утилита [IPFIX Receiver](#)