Table of Contents

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