Содержание

NAT flow export

1 Export NAT flows in IPFIX (Netflow 10)

For data analisys on NAT flows on external systems IPFIX export is available (aka netflow v10).

Settings of NAT flows export:

```
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
```

here

- **em1** - network device name for export
- **ipfix_nat_udp_collectors** - addresses of udp collectors
- **ipfix_nat_tcp_collectors** - addresses of tcp collectors

IPFIX template for NAT flows export				
ID	**IANA**	**Size**	**Type**	**Description**
323	0	8	int64	SYSTEM_TIME_WHEN_THE_EVENT_OCCURRED
4	0	1	int8	PROTOCOL_IDENTIFIER
230	0	1	int8	TYPE_OF_EVENT
8	0	4	IP v4	SOURCE_IPV4_ADDRESS
225	0	4	IP v4	POST_NAT_SOURCE_IPV4_ADDRESS
7	0	2	int16	SOURCE_PORT
227	0	2	int16	POST_NAPT_SOURCE_TRANSPORT_PORT
12	0	4	IP v4	DESTINATION_IPV4_ADDRESS
11	0	2	int16	DESTINATION_TRANSPORT_PORT
2000	43823	8	int64	SESSION_ID
2003	43823		string	LOGIN

To collect information in IPFIX any universal collector can be used or IPFIX Receiver utility.

Also NAT information is transmited in fields postNATsourceIPv4Address and postNAPTsourceTransportPort in IPFIX export full Netflow

2 Export NAT flows in text file

Settings for NAT flow export in text file on Stingray Service Gateway DPI server are in the configuration file /etc/dpi/fastdpi.conf:

```
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
```

here

- ajb_save_nat=1 activate export NAT flows in text file
- ajb_nat_path=/var/dump/dpi directory for files with NAT flows (default /var/dump/dpi)
- ajb_nat_ftimeout=30 time period of records
- ajb_save_nat_format=ts:ssid:event:login:proto:ipsrc:portsrc:ipsrcpostnat:portsrcpostnat:ipdst:portdst list and order of recorder fields, here
    - ts - timestamp
    - ssid - session id (for link with Netflow/IPFIX by volume)
    - event - event : 1 - NAT44 Session create, 2 - NAT44 Session delete
    - login - subscriber login
    - ipsrc - IP address of request source (subscriber)
    - portsrc - port of request source (subscriber)
    - ipsrcpostnat - IP address of request source (subscriber) after NAT translation
    - portsrcpostnat - port of request source (subscriber) after NAT translation
    - ipdst - destination IP address (host)
    - portdst - destination port (host).

 file system for writing logs must be fast and local (no NFS and other remotes), this type of journaling is recommended only for short-term diagnostics