Содержание

2 Configuration

The system allows to record the traffic for selected protocols in PCAP format. It can save also metadata of HTTP requests, SIP, FTP in log files.

PCAP

To start recording IP or CIDR traffic (0.0.0.0/0 - to record all traffic)

```
ajb_save_ip=192.168.0.0/24
```

This is a "hot" parameter, so this list can be changed with the command: **service fastdpi reload**

If you set the configuration parameter

```
ajb_reserved=1
```

the memory for the record buffer is allocated in advance (on DPI start) and you can start and stop data recording on the run. You only need to change parameters ajb_save_url, ajb_save_udpi and ajb_save_ip.

To record the data in PCAP format: please use the following parameters in configuration file */etc/dpi/fastdpi.conf*:

```
ajb_save_udpi=1
ajb_save_udpi_proto=OSPFIGP:ospf-lite
ajb_udpi_path=/var/dump/dpi
ajb_save_ip=192.168.0.0/24
```

Here:

- ajb_save_udpi=1 - activate the traffic recording for a list of protocols
- ajb_udpi_path=/var/dump/dpi - is a directory to place log files (/var/dump/dpi by default)
- ajb_save_udpi_proto=OSPFIGP:ospf-lite - is a list of protocols to record as test or numerical identificators. This is a hot parameter. It can be changed on the run by command **service fastdpi reload**.

You can also activate service 12 (traffic recording) individually for each subscriber.

Pcap files index mask

- 0 - not created
- 1 - via IPv4
- 2 - via IPv6
- 3 - via both IPv4 and IPv6.

```
ajb_pcap_ind_mask=0 // not created
ajb_pcap_ind_mask=1 // via IPv4
ajb_pcap_ind_mask=2 // via IPv6
ajb_pcap_ind_mask=3 // via both IPv4 and IPv6
```

This is a hot parameter. It can be changed on the run by command **service fastdpi reload**.

HTTP

To record HTTP requests' metadata: please use the following parameters in configuration file */etc/dpi/fastdpi.conf*:

```
ajb_save_url=-1
ajb_save_url_format=ts:prg:login:ipsrc:ipdst:host:path:ref:uagent:cookie:tph
ost:blockd:method
ajb_url_path=/var/dump/dpi
ajb_url_ftimeout=30
```

Here:

- ajb_save_url=-1 - activate recording of HTTP metadata
- ajb_url_path=/var/dump/dpi - is the directory to place files with these records (/var/dump/dpi by default)
- ajb_url_ftimeout=30 - recording frequency
- ajb_save_url_format=ts:prg:login:ipsrc:ipdst:host:path:ref:uagent:cookie - is the list of metadata to record:

```

ts - is a time stamp
prg - is: id of the active services at the moment of request
login - subscriber's login
ipsrc - subscriber's IP address
ipdst - host IP address (that of the request's addressee)
host - the host name (Host field)
path - the path to the requested resource (URI)
ref - where from (Referer field)
uagent - browser's type (User-Agent field)
cookie - Cookie
ssid - session ID (for binding with Netflow/IPFIX volume data)
tphost - data type of Host (HTTP=1/CNAME=2/SNI=3/QUIC=4)
blockd - bit mask, sign of blocking/forwarding (0x3 - for HTTP, 0x1 - for
others)
method - method 1 - GET, 2 - POST, 3 - PUT, 4 - DELETE (avaliable starting
from 6.0 version)
```

SSL/TLS

To record SSL/TLS requests' metadata: please use the following parameters in configuration file

/etc/dpi/fastdpi.conf:

```
ajb_save_ssl=-1
```

Here flag mask for saving SSL:

- 0 - not saved
- 1 - sni (SSL)
- 2 - cname
- 3 - sni (QUIC)

-1 - to record everything

```
ajb_save_ssl_format=ts:prg:login:ipsrc:ipdst:host:tphost:blockd:method
ajb_ssl_path=/var/dump/dpi
ajb_ssl_ftimeout=30
```

Here:

- ajb_save_url=-1 - activate recording of HTTP metadata
- ajb_url_path=/var/dump/dpi - is the directory to place files with these records (/var/dump/dpi by default)
- ajb_url_ftimeout=30 - recording frequency
- ajb_save_url_format=ts:prg:login:ipsrc:ipdst:host:path:ref:uagent:cookie:tphost:blockd:method - is the list of metadata to record:

```

ts - is a time stamp
prg - id of the active services at the moment of request
login - subscriber's login
ipsrc - subscriber's IP address
ipdst - host IP address (that of the request's addressee)
host - the host name (Host/CNAME/SNI/QUIC field)
path - the path to the requested resource (URI)
ref - where from (Referer field)
uagent - browser's type (User-Agent field)
cookie - Cookie
ssid - session ID (for binding with Netflow/IPFIX volume data)
tphost - data type of Host (HTTP=1/CNAME=2/SNI=3/QUIC=4)
blockd - bit mask, sign of blocking/forwarding (0x3 - for HTTP, 0x1 - for
others)
method - method 1 - GET, 2 - POST, 3 - PUT, 4 - DELETE (avaliable starting
from 6.0 version)
```

SIP

To record SIP requests' metadata: please use the following parameters in configuration file */etc/dpi/fastdpi.conf*:

```
ajb_save_sip=1
```

```
ajb_sip_ftimeout=15
ajb_sip_path=/home/sip
ajb_save_sip_format=ts:ssid:ipsrc:ipdst:login:msg:scode:from:to:callid:uagent
```

Here:

- ajb_save_sip=1 activate the SIP metadata recording in a file
- ajb_sip_path==/home/sip directory for SIP metadata files (default /var/dump/dpi)
- ajb_sip_ftimeout=15 record timeout between files
- ajb_save_sip_format=ts:ssid:ipsrc:ipdst:login:msg:scode:from:to:callid:uagent list of SIP metadate fields, here

```
ts - time stamp
ssid - session identifier (it's used to link to Netflow/IPFIX data to get bytes volume)
ipsrc - subscribers' IP
ipdst - server IP
login - subscribers' LOGIN (from RADIUS)
msg - message type
scode - status-code
from - phone/identifier of calling party
to - phone/identifier of called party
callid - call identifier
uagent - type of handset (User-Agent)
```