# Содержание

Configuring local record PCAP, HTTP, SSL/TLS, SIP	3
PCAP	
PCAP by IP and CIDR	
PCAP by VLAN	
HTTP	
SSL/TLS	
SIP	

# Configuring local record PCAP, HTTP, SSL/TLS, SIP

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

## **PCAP**

## **PCAP** by IP and CIDR

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



ajb\_save\_ip works independently of the subscriber on the input itself and writes all subscriber traffic before services and policing were applied to it.

If you set the configuration parameter

```
ajb_reserved=1
```

the memory for the record buffer is allocated in advance (at 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
```

#### 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.



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**.

### **PCAP by VLAN**

PCAP recording by VLAN is controlled by the parameter:

```
ajb_save_vlan
```

Possible values:

- n record to PCAP only with the condition vlan-id == n (qinq will not be recorded, even if svlan-id == n)
- n.m record to PCAP only if svlan-id == n, cvlan-id == m
- n.0 record to PCAP if svlan-id == n, cvlan-id == any

Only one active selection rule for recording is supported.

Rotation is performed under general conditions (similar to ajb save ip).

## **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:tphost:blockd:method is the list of metadata to record:
  - ts timestamp
  - prg id of currently active services
  - ∘ *login* subscriber's login
  - *ipsrc* IP address of the request source (subscriber)
  - *ipdst* IP address of the request recipient (host)
  - host host name (field Host/CNAME/SNI/QUIC)
  - path path to the requested resource (URI) on the host
  - ref referral source (Referer field)
  - uagent browser type (User-Agent field)
  - cookie cookies (Cookie field)
  - ssid session identifier (for connection with Netflow/IPFIX volume data)
  - tphost data type in the Host field (HTTP=1/CNAME=2/SNI=3/QUIC=4)
  - blockd bit mask, blocking/redirect sign (0x3 for HTTP, 0x1 for the rest)
  - method method 1 GET, 2 POST, 3 PUT, 4 DELETE (the field is available from version 6.0)

## 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 ssl=-1 enable SSL/TLS metadata recording
- ajb ssl path=/var/dump/dpi the location of the files with the record (by default /var/dump/dpi)
- ajb ssl ftimeout=30 recording frequency
- ajb\_save\_ssl\_format=ts:prg:login:ipsrc:ipdst:host:path:ref:uagent:cookie:tphost:blockd:method list of metadata to write, where
  - ts timestamp

- prg id of currently active services
- ∘ *login* subscriber's login
- *ipsrc* IP address of the request source (subscriber)
- *ipdst* IP address of the request recipient (host)
- host host name (field Host/CNAME/SNI/QUIC)
- path path to the requested resource (URI) on the host (where applicable)
- ref referral source (Referer field) (where it is applicable)
- *uagent* browser type (User-Agent field)(where it is applicable)
- o cookie cookies (Cookie field) (where it is applicable)
- ssid session identifier (for connection with Netflow/IPFIX volume data)
- tphost data type in the Host field (HTTP=1/CNAME=2/SNI=3/QUIC=4)
- blockd bit mask, blocking/redirect sign (0x3 for HTTP, 0x1 for the rest)
- method method 1 GET, 2 POST, 3 PUT, 4 DELETE (the field is available from version 6.0) (where it is applicable)

</code>

### 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:uagen
t
```

#### Here:

- ajb\_save\_sip=1 enable writing SIP metadata
- ajb sip path==/home/sip the location of the files with the record (by default /var/dump/dpi)
- ajb sip ftimeout=15 recording frequency
- ajb\_save\_sip\_format=ts:ssid:ipsrc:ipdst:login:msg:scode:from:to:callid:uagent list of metadata to write, where
  - ts timestamp
  - ssid session identifier (for connection with Netflow/IPFIX volume data)
  - *ipsrc* subscriber's IP
  - o ipdst Server IP
  - login subscriber's LOGIN
  - ∘ *msg* message type
  - scode status code
  - from number/id of the caller
  - to number/identifier of the callee
  - o callid call identifier
  - uagent type of subscriber device (User-Agent)