Table of Contents

2 Настройки	
PCAP	

2 Настройки

Система позволяет записывать трафик по выбранным протоколам в РСАР-формате, а также логировать метаданные HTTP запросов, SIP, FTP.

PCAP

Активировать запись трафика по IP или CIDR (0.0.0.0/0 - для записи всего трафика)

```
ajb_save_ip=192.168.0.0/24
```

Это горячий параметр и данный список можно изменять на лету командой **service fastdpi** reload

Если указать настроечный параметр

```
ajb_reserved=1
```

то память под буфер записи резервируется заранее (при старте DPI) и становиться возможным активировать и останавливать запись данных на лету, изменяя значение параметров ajb save url, ajb save udpi и ajb save ip

Для записи данных в РСАР формате в конфигурационно файле /etc/dpi/fastdpi.conf настраиваются следующие параметры:

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

где

- ajb save udpi=1 активировать запись трафика по списку протоколов
- ajb_udpi_path=/var/dump/dpi место размещения файлов с записью (по умолчанию /var/dump/dpi)
- ajb_save_udpi_proto=OSPFIGP:ospf-lite список записываемых протоколов в виде тестовых или цифровых идентификаторов, это горячее поле и данный список можно изменять на лету командой service fastdpi reload



Также можно подключать услугу 12 (запись трафика) индивидуально по каждому абоненту.

Маска создания индексов для рсар файлов:

- 0 не создаются
- 1 по IPv4

- 2 по IPv6
- 3 по IPv4 и по IPv6

```
ajb_pcap_ind_mask=0 // не создаются
ajb_pcap_ind_mask=1 // по IPv4
ajb_pcap_ind_mask=2 // по IPv6
ajb_pcap_ind_mask=3 // по IPv4 и по IPv6
```

Это горячее поле и данный список можно изменять на лету командой service fastdpi reload

HTTP

Для записи метаданных HTTP запросов в конфигурационном файле /etc/dpi/fastdpi.conf настраиваются следующие параметры:

```
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
```

где

- ajb save url=-1 активировать запись метаданных HTTP
- ajb_url_path=/var/dump/dpi место размещения файлов с записью (по умолчанию /var/dump/dpi)
- ajb url ftimeout=30 периодичность записи
- ajb_save_url_format=ts:prg:login:ipsrc:ipdst:host:path:ref:uagent:cookie:tphost:blockd:method список записываемых метаданных, где
 - ∘ *ts* временная метка
 - ∘ *prg* id активных в данных момент сервисов
 - ∘ login login абонента
 - ipsrc IP адрес источника запроса (абонента)
 - ∘ *ipdst* IP адрес получателя запроса (хоста)
 - host имя хоста (поле Host/CNAME/SNI/QUIC)
 - path путь к запрашиваемому на хосте ресурсу (URI)
 - ∘ ref источник перехода (поле Referer)
 - uagent тип браузера (поле User-Agent)
 - ∘ cookie куки (поле Cookie)
 - ssid идентификатор сессии (для связи с данными Netflow/IPFIX по объемам)
 - ∘ tphost тип данных в поле Host (HTTP=1/CNAME=2/SNI=3/QUIC=4)
 - blockd битовая маска, признак блокировки/переадресации (0х3 для HTTP, 0х1 для остального)
 - ∘ *method* метод 1 GET, 2 POST, 3 PUT, 4 DELETE (поле доступно с версии 6.0)

SSL/TLS

Для записи метаданных SSL/TLS запросов в конфигурационном файле /etc/dpi/fastdpi.conf настраиваются следующие параметры:

```
ajb save ssl=-1
```

где маска флагов сохранения SSL:

- 0 не сохранять
- 1 sni (SSL)
- 2 cname
- 4 sni (QUIC)

т.е. -1 - писать все

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

где

- ajb save ssl=-1 активировать запись метаданных SSL/TLS
- ajb_ssl_path=/var/dump/dpi место размещения файлов с записью (по умолчанию /var/dump/dpi)
- ajb_ssl_ftimeout=30 периодичность записи
- ajb_save_ssl_format=ts:prg:login:ipsrc:ipdst:host:path:ref:uagent:cookie:tphost:blockd:method список записываемых метаданных, где
 - ts временная метка
 - ∘ prg id активных в данных момент сервисов
 - ∘ login login абонента
 - ∘ *ipsrc* IP адрес источника запроса (абонента)
 - ∘ *ipdst* IP адрес получателя запроса (хоста)
 - ∘ host имя хоста (поле Host/CNAME/SNI/QUIC)
 - path путь к запрашиваемому на хосте ресурсу (URI)(там где применимо)
 - ∘ ref источник перехода (поле Referer)(там где применимо)
 - uagent тип браузера (поле User-Agent)(там где применимо)
 - ∘ cookie куки (поле Cookie)(там где применимо)
 - ssid идентификатор сессии (для связи с данными Netflow/IPFIX по объемам)
 - ∘ tphost тип данных в поле Host (HTTP=1/CNAME=2/SNI=3/QUIC=4)
 - blockd битовая маска, признак блокировки/переадресации (0х3 для HTTP, 0х1 для остального)
 - method метод 1 GET, 2 POST, 3 PUT, 4 DELETE (поле доступно с версии 6.0)(там где применимо)

SIP

Для записи метаданных SIP в конфигурационном файле /etc/dpi/fastdpi.conf настраиваются следующие параметры:

```
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
```

где

- ajb_save_sip=1 активировать запись метаданных SIP
- ajb_sip_path==/home/sip место размещения файлов с записью (по умолчанию /var/dump/dpi)
- ajb sip ftimeout=15 периодичность записи
- ajb_save_sip_format=ts:ssid:ipsrc:ipdst:login:msg:scode:from:to:callid:uagent список записываемых метаданных, где
 - ∘ *ts* временная метка
 - ssid идентификатор сессии (для связи с данными Netflow/IPFIX по объемам)
 - ∘ ipsrc IP абонента
 - ∘ ipdst IP сервера
 - ∘ login LOGIN абонента
 - ∘ *msg* тип сообщения
 - ∘ scode статус-код
 - from номер/идентификатор вызывающего абонент
 - to номер/идентификатор вызываемого абонент
 - ∘ callid идентификатор вызова
 - uagent тип абонентского устройства (User-Agent)