Содержание

Настройка локальной записи PCAP и статистики по HTTP, SSL/TLS, SIP

Система позволяет записывать трафик по выбранным протоколам в PCAP-формате, а также логировать метаданные HTTP запросов, SSL/TLS, SIP.

PCAP

PCAP по IP и CIDR

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**

`ajb_save_ip` работает независимо от абонента на самом входе и пишет весь абонентский трафик до того как к нему были применены сервисы и полисинг.

Если указать настроечный параметр

```
ajb_reserved=1
```

то память под буфер записи резервируется заранее (при старте DPI) и становится 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 PCAP 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, для записи всего трафика используется параметр

everything

Для применения параметров выполнить **service fastdpi reload**

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

Маска создания индексов для pcap 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**

PCAP по VLAN

Управление записью PCAP по VLAN осуществляется параметром:

```
ajb_save_vlan
```

Возможные значения:

- `n` — запись в PCAP только с условием `vlan-id == n` (qinq записываться не будет, даже если `svlan-id == n`)
- `n.m` — запись в PCAP только при `svlan-id == n`, `cvlan-id == m`
- `n.0` — запись в PCAP при `svlan-id == n`, `cvlan-id == any`

Поддерживается одна активная запись отбора для записи.
Ротация осуществляется на общих условиях (аналогично `ajb_save_ip`).

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 (0x3 - для HTTP, 0x1 - 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 (0x3 - для HTTP, 0x1 - 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:uagent
```

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)