

Содержание

| | |
|--|----|
| Экспорт Clickstream, Мета информации, DNS в формате IPFIX | 3 |
| <i>Настройка экспорта Clickstream</i> | 3 |
| IPFIX шаблона экспорта Clickstream | 4 |
| <i>Настройка экспорта метаданных</i> | 6 |
| Форматы IPFIX шаблона экспорта метаданных | 6 |
| <i>DNS</i> | 9 |
| <i>Отправка template в IPFIX</i> | 11 |

Экспорт Clickstream, Meta информации, DNS в формате IPFIX

Для анализа данных Clickstream (сведения о посещениях абонентами страниц web сайтов) и SIP (сведения о voip переговорах) на внешних системах, можно экспортировать эти данных по сети в формате IPFIX.

Со списком соответствия между протоколом и номером порта в NetFlow5 можно ознакомиться [здесь](#).

Для сбора информации в формате IPFIX подойдет любой универсальный IPFIX коллектор, понимающий шаблоны, или утилита [IPFIX Receiver](#).

Для приема, обработки и хранения ClickStream рекомендуется использовать [программный продукт для сбора статистики QoE Store](#) и [графический интерфейс DPIUI2](#).

При недостаточном качестве канала связи между СКАТ и NetFlow/IPFIX коллектором СКАТ пропускает отправку части статистики для сохранения производительности. При пропуске чанка информации в `fastdpi_alert.log` выводится сообщение:

```
[NFLW] very long operation ....
```

С версии 12.0 появилась статистика отправки информации по NetFlow/IPFIX (дополнительная секция в `fastdpi_stat.log`):

```
[STAT    ][2022/11/20-17:55:03:213770] Statistics on NFLW_export :  
{a/b/c%/d/e}
```

a - количество выполнения циклов отправки
b - количество циклов отправки, когда время, затраченное на отправку превысило период выполнения циклов
c - процент превышения количества циклов отправки: $100 * b/a$
d - время в микросекундах максимальной продолжительности цикла отправки
e - время в микросекундах периода отправки статистики (значение параметра `'netflow_timeout'` (параметр задается в секундах))

Пример:

```
[STAT    ][2022/11/20-17:55:03:213770] Statistics on NFLW_export :  
{7/0/0.00%/45297us/30008163us}
```

Настройка экспорта Clickstream

Экспорт Clickstream настраивается следующими параметрами:

```
ipfix_dev=em1  
ipfix_udp_collectors=1.2.3.4:1500,1.2.3.5:1501  
ipfix_tcp_collectors=1.2.3.6:9418
```

dbg_log_mask=0x80

где

- **em1** — имя сетевого интерфейса для экспорта.
- **ipfix_udp_collectors** — адреса UDP коллекторов.
- **ipfix_tcp_collectors** — адреса TCP коллекторов.
- **dbg_log_mask=0x80** — вывод статистической информации об экспорте в лог.

IPFIX шаблона экспорта Clickstream

Формат IPFIX шаблонов для IPv6 отличается форматом полей IP_SOURCE и IP_DESTINATION.

| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
|---|-------------|-------------|-------|-------------------------|--|
| 1103 | 16 | IPv6 | 43823 | IP_SOURCE | Адрес отправителя |
| 1104 | 16 | IPv6 | 43823 | IP_DESTINATION | Адрес получателя |
| Формат IPFIX шаблона экспорта Clickstream | | | | | |
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 1001 | 4 | int32 | 43823 | TIME_STAMP | Метка времени |
| 1002 | - | string | 43823 | LOGIN | Вход в систему |
| 1003 | 4 | IPv4 | 43823 | IP_SOURCE | Адрес отправителя |
| 1004 | 4 | IPv4 | 43823 | IP_DESTINATION | Адрес получателя |
| 1005 | - | string | 43823 | HOSTNAME/CNAME/SNI | Имя хоста/каноническое имя/индикация имени сервера |
| 1006 | - | string | 43823 | PATH | Переменная окружения |
| 1007 | - | string | 43823 | REFER | Заголовок запроса клиента |
| 1008 | - | string | 43823 | USER_AGENT | Пользовательский агент |
| 1009 | - | string | 43823 | COOKIE | Кúки |
| 2000 | 8 | int64 | 43823 | SESSION_ID | Идентификатор сессии |
| 1010 | 8 | int64 | 43823 | LOCKED | Заблокированный |
| 1011 | 1 | int8 | 43823 | HOST_TYPE | Тип хоста |
| 1012 | 1 | int8 | 43823 | METHOD | Метод |
| 1013 | 2 | int16 | 43823 | PORT_SOURCE | Порт отправителя |
| 1014 | 2 | int16 | 43823 | PORT_DESTINATION | Порт получателя |
| 2016 | 2 | int16 | 43823 | BRIDGE_CHANNEL_NUM | Номер канала (vchannel) или моста. Если в конфигурации DPI настроены vchannel, то будет передаваться номер канала, иначе номер моста |
| 1024 | 2 | int16 | 43823 | CipherSuitesLen | Размер в байтах набора доступных методов шифрования CipherSuites в сообщении Client Hello |
| 1025 | - | raw | 43823 | CipherSuites | Массив CipherSuites в Client Hello (max 16 значений) |
| 58 | 2 | int16 | - | VLAN_ID | VLAN |
| 59 | 2 | int16 | - | POST_VLAN_ID | POST VLAN |
| 56 | 6 | mac_address | - | Source MAC Address | |
| 57 | 6 | mac_adress | - | Destination MAC Address | |

| | | | | | |
|------|---|-------|-------|--------------|--|
| 2017 | - | raw | 43823 | MPLS Labels | |
| 2018 | 4 | int32 | 43823 | TCP Sequence | |

Примечание:

- LOCKED = 1 - заблокирован по HTTPS, 2 - редирект HTTP, 3 - заблокирован по HTTP (передается битовой маской)
- HOST_TYPE = 1 в случае HTTP, 2 — CNAME, 3 — SNI, 4 — QUIC
- METHOD = 1 — GET, 2 — POST, 3 — PUT, 4 — DELETE

При включенном настроечном параметре `http_parse_reply=1` дополнительно будет передаваться информация из ответов на запросы. Связать их с ответами можно по идентификатору сессии `SESSION_ID`, учитывая порядок следования.

| Формат IPFIX шаблона экспорта Clickstream для ответов HTTP ¹⁾ | | | | | |
|---|-------------|-------------|-------|-------------------------|--|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 1001 | 4 | int32 | 43823 | TIME_STAMP | Метка времени |
| 1002 | - | string | 43823 | LOGIN | Вход в систему |
| 1003 | 4 | IPv4 | 43823 | IP_SOURCE | Адрес отправителя |
| 1004 | 4 | IPv4 | 43823 | IP_DESTINATION | Адрес получателя |
| 1020 | 4 | int32 | 43823 | RESULT_CODE | Код результата |
| 1021 | 8 | int64 | 43823 | CONTENT_LENGTH | Количество пересылаемых байт |
| 1022 | - | string | 43823 | CONTENT_TYPE | Тип передаваемых данных |
| 2000 | 8 | int64 | 43823 | SESSION_ID | Идентификатор сессии |
| 1023 | - | string | 43823 | LOCATION | |
| 2016 | 2 | int16 | 43823 | BRIDGE_CHANNEL_NUM | Номер канала (vchannel) или моста. Если в конфигурации DPI настроены vchannel, то будет передаваться номер канала, иначе номер моста |
| 58 | 2 | int16 | - | VlanId | VLAN |
| 59 | 2 | int16 | - | postVlanID | POST VLAN |
| 56 | 6 | mac_address | - | Source MAC Address | |
| 57 | 6 | mac_adress | - | Destination MAC Address | |
| 2017 | - | raw | 43823 | MPLS Labels | |

При включенном настроечном параметре `ssl_parse_reply=1` дополнительно будет передаваться информация из ответов на запросы. Связать их с ответами можно по идентификатору сессии `SESSION_ID` с учетом порядка следования.

| Формат IPFIX шаблона экспорта Clickstream для ответов по SSL/TLS, HTTPS ²⁾ | | | | | |
|--|-------------|------------|-------|----------------|----------------------|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 1001 | 4 | int32 | 43823 | TIME_STAMP | Метка времени |
| 1002 | - | string | 43823 | LOGIN | Вход в систему |
| 1003 | 4 | IPv4 | 43823 | IP_SOURCE | Адрес отправителя |
| 1004 | 4 | IPv4 | 43823 | IP_DESTINATION | Адрес получателя |
| 2000 | 8 | int64 | 43823 | SESSION_ID | Идентификатор сессии |

| Формат IPFIX шаблона экспорта Clickstream для ответов по SSL/TLS, HTTPS ²⁾ | | | | | |
|---|-------------|-------------|-------|-------------------------|--|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 1030 | 2 | int16 | 43823 | SSL_VERSION | Версия SSL |
| 1031 | 2 | int16 | 43823 | CIPHER_SUITE | Набор шифров |
| 1032 | 1 | int8 | 43823 | COMPRESSION_METHOD | Метод сжатия |
| 2016 | 2 | int16 | 43823 | BRIDGE_CHANNEL_NUM | Номер канала (vchannel) или моста. Если в конфигурации DPI настроены vchannel, то будет передаваться номер канала, иначе номер моста |
| 58 | 2 | int16 | - | VlanId | VLAN |
| 59 | 2 | int16 | - | postVlanID | POST VLAN |
| 56 | 6 | mac_address | - | Source MAC Address | |
| 57 | 6 | mac_adress | - | Destination MAC Address | |
| 2017 | - | raw | 43823 | MPLS Labels | |
| 1011 | 1 | int8 | 43823 | type_host | |
| 1005 | - | string | 43823 | cname | |

Настройка экспорта метаданных

Экспорт метаданных других протоколов для COPM настраивается следующими параметрами:

```
ipfix_dev=em1
ipfix_meta_udp_collectors=1.2.3.4:1500,1.2.3.5:1501
ipfix_meta_tcp_collectors=1.2.3.6:9418
dbg_log_mask=0x80
```

где

- **em1** — имя сетевого интерфейса для экспорта.
- **ipfix_meta_udp_collectors** — адреса UDP коллекторов.
- **ipfix_meta_tcp_collectors** — адреса TCP коллекторов.
- **dbg_log_mask=0x80** — вывод статистической информации об экспорте в лог.

Форматы IPFIX шаблона экспорта метаданных

| Формат IPFIX шаблона экспорта метаданных SIP | | | | | |
|--|-------------|------------|-------|-------------|----------------------|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 1001 | 4 | int32 | 43823 | TIME_STAMP | Метка времени |
| 1002 | - | string | 43823 | LOGIN | Вход в систему |
| 1003 | 4 | IPv4 | 43823 | IP_SRC | Адрес отправителя |
| 1004 | 4 | IPv4 | 43823 | IP_DST | Адрес получателя |
| 2000 | 8 | int64 | 43823 | SESSION_ID | Идентификатор сессии |
| 3000 | - | string | 43823 | MSG_CODE | Msg код |
| 3001 | 2 | int16 | 43823 | STATUS_CODE | Код состояния |

| Формат IPFIX шаблона экспорта метаданных SIP | | | | | |
|--|-------------|-------------|-------|-------------------------|---------------------------------------|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 3002 | - | string | 43823 | URI | Унифицированный идентификатор ресурса |
| 3003 | - | string | 43823 | FROM | |
| 3004 | - | string | 43823 | TO | |
| 3005 | - | string | 43823 | CALLID | Идентификатор вызова |
| 3006 | - | string | 43823 | UAGENT | Клиентское приложение |
| 3007 | - | string | 43823 | CTYPE | Тип передаваемого контента |
| 3008 | - | string | 43823 | GATEWAYS | Список шлюзов |
| 58 | 2 | int16 | - | VlanId | VLAN |
| 59 | 2 | int16 | - | postVlanID | POST VLAN |
| 56 | 6 | mac_address | - | Source MAC Address | |
| 57 | 6 | mac_address | - | Destination MAC Address | |
| 2017 | - | raw | 43823 | MPLS Labels | |

Примечание:

IP_SRC — IP_SOURCE.

IP_DST — IP_DESTINATION.

GATEWAYS — список шлюзов (IP или hostname), разделенных запятой.

| Формат IPFIX шаблона экспорта метаданных FTP | | | | | |
|--|-------------|-------------|-------|-------------------------|----------------------|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 1001 | 4 | int32 | 43823 | TIME_STAMP | Метка времени |
| 1002 | - | string | 43823 | LOGIN | Вход в систему |
| 1003 | 4 | IPv4 | 43823 | IP_SRC | Адрес отправителя |
| 1004 | 4 | IPv4 | 43823 | IP_DST | Адрес получателя |
| 2000 | 8 | int64 | 43823 | SESSION_ID | Идентификатор сессии |
| 3050 | - | string | 43823 | SERVER_NAME | Имя сервера |
| 3051 | - | string | 43823 | USER | Пользователь |
| 3052 | - | string | 43823 | PASSWORD | Пароль |
| 3053 | 1 | int8 | 43823 | MODE | Режим |
| 1020 | 4 | int32 | 43823 | RESULT CODE | Код результата |
| 58 | 2 | int16 | - | VlanId | VLAN |
| 59 | 2 | int16 | - | postVlanID | POST VLAN |
| 56 | 6 | mac_address | - | Source MAC Address | |
| 57 | 6 | mac_address | - | Destination MAC Address | |
| 2017 | - | raw | 43823 | MPLS Labels | |

Примечание: поле MODE содержит тип FTP соединения: (0 — активный, 1 — пассивный).

| Формат IPFIX шаблона экспорта метаданных мессенджеров (XMPP) | | | | | |
|--|-------------|------------|-------|------------|-------------------|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 1001 | 4 | int32 | 43823 | TIME_STAMP | Метка времени |
| 1002 | - | string | 43823 | LOGIN | Вход в систему |
| 1003 | 4 | IPv4 | 43823 | IP_SRC | Адрес отправителя |
| 1004 | 4 | IPv4 | 43823 | IP_DST | Адрес получателя |

| Формат IPFIX шаблона экспорта метаданных мессенджеров (XMPP) | | | | | |
|--|-------------|-------------|-------|-------------------------|------------------------------|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 2000 | 8 | int64 | 43823 | SESSION_ID | Идентификатор сессии |
| 3100 | - | string | 43823 | IM_LOGIN | |
| 3101 | - | string | 43823 | IM_PASSW | |
| 3102 | - | string | 43823 | IM_SCREEN_NAME | Экранное имя |
| 3103 | - | string | 43823 | IM_UIN | Универсальный интернет-номер |
| 3104 | 1 | int8 | 43823 | IM_PROTOCOL | Тип используемого протокола |
| 3105 | - | string | 43823 | IM_RECEIVERS | Получатель |
| 1020 | 4 | int32 | 43823 | RESULT_CODE | Код результата |
| 58 | 2 | int16 | - | VlanId | VLAN |
| 59 | 2 | int16 | - | postVlanID | POST VLAN |
| 56 | 6 | mac_address | - | Source MAC Address | |
| 57 | 6 | mac_adress | - | Destination MAC Address | |
| 2017 | - | raw | 43823 | MPLS Labels | |

Примечание: поле IM_PROTOCOL содержит тип используемого протокола: 0 — ICQ, 7 — XMPP, 106 — ZELLO/

| Формат IPFIX шаблона экспорта метаданных почтовых протоколов (POP, IMAP, SMTP) | | | | | |
|--|-------------|-------------|-------|-------------------------|--------------------------|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 1001 | 4 | int32 | 43823 | TIME_STAMP | Метка времени |
| 1002 | - | string | 43823 | LOGIN | Вход в систему |
| 1003 | 4 | IPv4 | 43823 | IP_SRC | Адрес отправителя |
| 1004 | 4 | IPv4 | 43823 | IP_DST | Адрес получателя |
| 2000 | 8 | int64 | 43823 | SESSION_ID | Идентификатор сессий |
| 3150 | - | string | 43823 | MAIL_SENDER | Отправитель |
| 3151 | - | string | 43823 | MAIL_RECEIVER | Получатель |
| 3152 | - | string | 43823 | MAIL_CC | Получатель копии |
| 3153 | - | string | 43823 | MAIL_SUBJECT | Тема письма |
| 3154 | - | string | 43823 | MAIL_SERVERS | Сервера |
| 3155 | - | string | 43823 | MAIL_REPLY | Ответы на сообщения |
| 3156 | 1 | int8 | 43823 | EVENT | Тип события |
| 3157 | 1 | int8 | 43823 | ATTACHMENT | Признак наличия вложения |
| 3158 | 1 | int8 | 43823 | MAIL_PROTOCOL | Почтовый протокол |
| 1020 | 4 | int32 | 43823 | RESULT_CODE | Код результата |
| 58 | 2 | int16 | - | VlanId | VLAN |
| 59 | 2 | int16 | - | postVlanID | POST VLAN |
| 56 | 6 | mac_address | - | Source MAC Address | |
| 57 | 6 | mac_adress | - | Destination MAC Address | |
| 2017 | - | raw | 43823 | MPLS Labels | |

Примечание: поле EVENT указывает тип события: 1 — send, 2 — receive, ATTACHMENT — признак наличия вложения: mail_protocol = 0 — smtp, 1 — pop3, 2 — imap.

| Формат IPFIX шаблона экспорта сырых нераспарсенных метаданных | | | | | |
|---|-------------|-------------|-------|--------------------------|------------------------------------|
| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
| 1001 | 4 | int32 | 43823 | TIME_STAMP | Метка времени |
| 1002 | - | string | 43823 | LOGIN | Вход в систему |
| 1003 | 4 | IPv4 | 43823 | IP_SRC | Адрес отправителя |
| 1004 | 4 | IPv4 | 43823 | IP_DST | Адрес получателя |
| 2000 | 8 | int64 | 43823 | SESSION_ID | Идентификатор сессии |
| 2013 | 1 | int8 | 43823 | FLW_DIR | Направление пакета по интерфейсам |
| 2014 | 1 | int8 | 43823 | DIR_DATA | Направление пакета по сессии |
| 2015 | 2 | int16 | 43823 | VDPI_PROTO | Протокол, который определил dpi |
| 2900 | 2 | int16 | 43823 | META_PROTO | Внутренний идентификатор протокола |
| 2901 | - | string | 43823 | RAW_DATA | Сырые данные |
| 4 | 1 | int8 | - | protocolIdentifier | PROTOCOL |
| 7 | 2 | int16 | - | sourceTransportPort | |
| 11 | 2 | int16 | - | destinationTransportPort | |
| 6 | 2 | int16 | - | tcpControlBits | |
| 2018 | 4 | int32 | - | TCP Sequence | |
| 58 | 2 | int16 | - | VlanId | VLAN |
| 59 | 2 | int16 | - | postVlanID | POST VLAN |
| 56 | 6 | mac_address | - | Source MAC Address | |
| 57 | 6 | mac_adress | - | Destination MAC Address | |
| 2017 | - | raw | 43823 | MPLS Labels | |

Примечание:

- **FLW_DIR** — направление пакета по интерфейсам: 0: subs -> inet, 1: inet -> subs.
- **DIR_DATA** — направление пакета по сессии: для TCP 0: клиент -> сервер, 1: сервер -> клиент, для UDP — от кого первый пакет зафиксирован, тот и считается клиентом.
- **VDPI_PROTO** — протокол, определяющий DPI.
- **META_PROTO** — внутренний идентификатор протокола (3 — SIP, 4 — FTP, 5 — SMTP, 6 — POP3, 7 — IMAP, 8 — XMPP, 9 — ICQ, 10 — RSS, 11 — NNTP, 12 — H323, 13 — ZELLO).
- **RAW_DATA** — сырые данные.

Для агрегации raw_data, clickstream, http_reply и ssl_reply с данными по сессиям требуется дополнительная обработка или выполнение запроса по БД с ключом Session_ID, или поддержка в утилите rcollector.

DNS

Экспорт DNS настраивается следующими параметрами:

```
ipfix_dev=em1
ipfix_dns_udp_collectors=1.2.3.4:1234
ipfix_dns_tcp_collectors=1.2.3.6:4567
```

где

- **em1** — имя сетевого интерфейса для экспорта.
- **ipfix_dns_udp_collectors** — адреса UDP коллекторов.
- **ipfix_dns_tcp_collectors** — адреса TCP коллекторов.

Формат IPFIX шаблонов для IPV6 отличается форматом полей IP_SOURCE и IP_DESTINATION.

| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
|------|-------------|------------|-------|----------------|-------------------|
| 1103 | 16 | IPv6 | 43823 | IP_SOURCE | Адрес отправителя |
| 1104 | 16 | IPv6 | 43823 | IP_DESTINATION | Адрес получателя |

Формат IPFIX шаблона экспорта DNS

| № | Кол-во байт | Тип данных | IANA | Описание | Примечание |
|------|-------------|-------------|-------|-------------------------|--|
| 1001 | 4 | int32 | 43823 | TIME_STAMP | Метка времени |
| 1002 | - | string | 43823 | LOGIN | Вход в систему |
| 1003 | 4 | IPv4 | 43823 | IP_SOURCE | Адрес отправителя |
| 1004 | 4 | IPv4 | 43823 | IP_DESTINATION | Адрес получателя |
| 1013 | 2 | int16 | 43823 | SOURCE PORT | |
| 1014 | 2 | int16 | 43823 | DESTINATION PORT | |
| 2000 | 8 | int64 | 43823 | SESSION_ID | Идентификатор сессии |
| 3200 | 1 | int8 | 43823 | UDP/TCP | Транспорт: 0 — UDP, 1 — TCP |
| 3201 | - | string | 43823 | DOMAIN | |
| 3202 | 2 | int16 | 43823 | RRCLASS | |
| 3203 | 2 | int16 | 43823 | RRTYPE | |
| 3204 | 4 | int32 | 43823 | TTL | |
| 3205 | - | raw | 43823 | RDATA | |
| 58 | 2 | int16 | - | VlanId | VLAN |
| 59 | 2 | int16 | - | postVlanID | POST VLAN |
| 56 | 6 | mac_address | - | Source MAC Address | |
| 57 | 6 | mac_adress | - | Destination MAC Address | |
| 2017 | - | raw | 43823 | MPLS Labels | |
| 2016 | 2 | int16 | 43823 | BRIDGE_CHANNEL_NUM | Номер канала (vchannel) или моста. Если в конфигурации DPI настроены vchannel, то будет передаваться номер канала, иначе номер моста |

Альтернативой является сохранение данных в локальном текстовом логге:

- **ajb_save_dns** — флаг записи в текстовый файл.
- **ajb_dns_ftimeout** — таймаут (в минутах) переключения на следующий файл.
- **ajb_dns_bufsize** — буфер записи в файл.
- **ajb_dns_fsize** — ограничение на размер файла.
- **ajb_dns_path** — путь к записываемому файлу.

Переключение на следующий файл происходит, когда размер файла достигнет **ajb_dns_fsize** или файл непустой и прошло время **ajb_dns_ftimeout**

ajb_save_dns_format: формат записи в текстовый файл

- **ts** — время.
- **ipsrc** — ip_source.
- **ipdst** — ip_destination.
- **ssid** — session_id.
- **login** — логин.
- **host** — name, которого запрашивали информацию.
- **rrtype** — RR types.
- **rrclass** — RR class.
- **ttl** — TTL.
- **rdlen** — размер rdata.
- **rdata** — ресурс.
- **psrc** — port source.
- **pdst** — port destination.
- **transport** — как получен DNS запрос.

По умолчанию:

ts:ssid:login:ipsrc:ipdst:psrc:pdst:transport:host:rrtype:rrclass:ttl:rdlen:rdata

Отправка template в IPFIX

1. Транспортный протокол TCP.
Template отправляется один раз после установления TCP-сессии.
2. Транспортный протокол UDP.
Template отправляется по умолчанию каждые 20 секунд. Регулируется параметром `ipfix_udp_template_timer`.

¹⁾ ²⁾

для варианта с IPv6 см. выше отличие