Содержание

PCAP, IPFIX Export (Clickstream, DNS, SIP metadata, FTP)

The option allows real-time recording of network traffic and can be used to monitor traffic for diagnostic purposes, analyze security threats and conduct market research. Traffic for diagnostic purposes, security threat analysis and market research.

Please note that when recording traffic, increased demands are placed on the disk subsystem. It also consumes additional memory and CPU resources.

For Clickstream data analisys (subscribers' http requests) and SIP (VOIP unciphered data) on external systems IPFIX export is available.

A list of the correspondence between the Protocol and the port number in netfow5 can be found here.

Any universal IPFIX collector that accepts templates or the IPFIX Receiver utility is suitable for collecting information in IPFIX format.

To receive, process and store ClickStream, we suggest using the QoE Store software and DPIUI2 graphical interface.

If the link quality between SSG and NetFlow/IPFIX collector is insufficient, SSG skips sending some statistics to save performance. A message is displayed in `fastdpi_alert.log` when a chunk of information is skipped:

```
[NFLW] very long operation ….
```

Starting from version 12.0, the statistics for sending NetFlow/IPFIX information is now available (additional section in fastdpi_stat.log):

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

    a - number of sending cycles
    b - number of sending cycles, when the time spent on sending exceeded
the cycle execution period
    c - percentage of exceeding the number of sending cycles: 100 * b/a
    d - time of maximum sending cycle duration, microseconds
    e - time of the period of sending statistics, microseconds
(''netflow_timeout'' parameter value (the parameter is set in seconds)).

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

ClickStream export Setup

Clickstream experts is configured by following parameters:

```
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
```

here

- **em1** — NIC using for export.
- **ipfix_udp_collectors** — IP of udp collectors.
- **ipfix_tcp_collectors** — IP of tcp collectors.
- **dbg_log_mask=0x80** — logging statistics about export.

The `ipfix_mtu_limit` parameter sets the maximum UDP packet size when sending IPFIX. By default, it equals the minimum MTU of the interfaces used for sending.

IPFIX format template for Clickstream

The format of IPFIX templates for IPV6 differs only in the **IP_SOURCE** and **IP_DESTINATION** fields.

№	Size in bytes	Type	IANA	Description	Note
1003	16	IPv6	43823	IP_SOURCE	Sender address
1004	16	IPv6	43823	IP_DESTINATION	Recipient address

IPFIX format template for Clickstream					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
1001	4	int32	43823	TIME_STAMP	
1002	-	string	43823	LOGIN	
1003	4	IPv4	43823	IP_SOURCE	Sender address
1004	4	IPv4	43823	IP_DESTINATION	Recipient address
1005	-	string	43823	HOSTNAME/CNAME	
1006	-	string	43823	PATH	
1007	-	string	43823	REFER	
1008	-	string	43823	USER_AGENT	
1009	-	string	43823	COOCKIE	
2000	8	int64	43823	SESSION_ID	
1010	8	int64	43823	LOCKED	
1011	1	int8	43823	HOST_TYPE	
1012	1	int8	43823	METHOD	
1013	2	int16	43823	PORT_SOURCE	Sender port
1014	2	int16	43823	PORT_DESTINATION	Recipient port

IPFIX format template for Clickstream					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
2016	2	int16	43823	BRIDGE_CHANNEL_NUM	Channel number (vchannel) or bridge. If vchannel is configured in the DPI configuration, then the channel number will be transmitted, otherwise the bridge number. Used in QoEStor.
1024	2	int16	43823	CipherSuitesLen	Size in bytes of the set of available CipherSuites encryption methods in the Client Hello message
1025	-	raw	43823	CipherSuites	CipherSuites array in Client Hello (max 16 values)
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	
2018	4	int32	43823	TCP Sequence	

ND:

- LOCKED = 1 — blocked by HTTPS, 2 — HTTP redirect, 3 — blocked by HTTP (transmitted by bitmask)
- HOST TYPE = 1 in case of HTTP, 2 — CNAME, 3 — SNI, 4 — QUIC
- METHOD = 1 — GET, 2 — POST, 3 — PUT, 4 — DELETE

If the configuration parameter `http_parse_reply=1` is enabled, information from responses to requests will be additionally transmitted. You can associate them with responses by the session identifier **SESSION_ID**, taking into account the order.

Clickstream export template IPFIX format for HTTP responses[1)]					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
1001	4	int32	43823	TIME_STAMP	
1002	-	string	43823	LOGIN	
1003	4	IPv4	43823	IP_SOURCE	
1004	4	IPv4	43823	IP_DESTINATION	
1020	4	int32	43823	RESULT_CODE	
1021	8	int64	43823	CONTENT_LENGTH	
1022	-	string	43823	CONTENT_TYPE	
2000	8	int64	43823	SESSION_ID	
1023	-	string	43823	LOCATION	
2016	2	int16	43823	BRIDGE_CHANNEL_NUM	Channel (vchannel) or bridge number. If vchannel is set in the DPI configuration, the channel number will be transmitted, otherwise the bridge number will be transmitted
58	2	int16	-	VlanId	VLAN
59	2	int16	-	postVlanID	POST VLAN

Clickstream export template IPFIX format for HTTP responses[1)]					
№	Size in bytes	Type	IANA	Description	Note
56	6	mac_address	-	Source MAC Address	
57	6	mac_adress	-	Destination MAC Address	
2017	-	raw	43823	MPLS Labels	

If the configuration parameter `ssl_parse_reply=1` is enabled, information from responses to requests will be additionally transmitted. You can associate them with responses by the session identifier **SESSION_ID**, taking into account the order.

Clickstream export template IPFIX format for responses over SSL/TLS, HTTPS[2)]					
№	Size in bytes	Type	IANA	Description	Note
1001	4	int32	43823	TIME_STAMP	
1002	-	string	43823	LOGIN	
1003	4	IPv4	43823	IP_SOURCE	
1004	4	IPv4	43823	IP_DESTINATION	
2000	8	int64	43823	SESSION_ID	
1030	2	int16	43823	SSL_VERSION	
1031	2	int16	43823	CIPHER_SUITE	
1032	1	int8	43823	COMPRESSION_METHOD	
2016	2	int16	43823	BRIDGE_CHANNEL_NUM	Channel (vchannel) or bridge number. If vchannel is set in the DPI configuration, the channel number will be transmitted, otherwise the bridge number will be transmitted
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	

Metadata Export Setting

Export of metadata of other protocols for SORM is configured by the following parameters

```
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
```

where

- **em1** — network interface name for export
- **ipfix_meta_udp_collectors** — udp addresses of collectors

- **`ipfix_meta_tcp_collectors`** — tcp addresses of collectors
- **`dbg_log_mask=0x80`** — output of statistical information about export to the log

IPFIX metadata export template formats

SIP metadata export template IPFIX format					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
1001	4	int32	43823	TIME_STAMP	
1002	-	string	43823	LOGIN	
1003	4	IPv4	43823	IP_SRC	Sender's address
1004	4	IPv4	43823	IP_DST	Recipient's address
2000	8	int64	43823	SESSION_ID	
3000	-	string	43823	MSG_CODE	
3001	2	int16	43823	STATUS_CODE	
3002	-	string	43823	URI	Uniform Resource Identifier
3003	-	string	43823	FROM	
3004	-	string	43823	TO	
3005	-	string	43823	CALLID	
3006	-	string	43823	UAGENT	Client application
3007	-	string	43823	CTYPE	Type of content to be transmitted
3008	-	string	43823	GATEWAYS	
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	

Notes:
IP_SRC — IP SOURCE
IP_DST — IP DESTINATION
GATEWAYS — comma separated list of gateways (IP or hostname)

FTP Metadata Export Template IPFIX Format					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
1001	4	int32	43823	TIME_STAMP	
1002	-	string	43823	LOGIN	
1003	4	IPv4	43823	IP_SRC	Sender's address
1004	4	IPv4	43823	IP_DST	Recipient's address
2000	8	int64	43823	SESSION_ID	
3050	-	string	43823	SERVER_NAME	
3051	-	string	43823	USER	
3052	-	string	43823	PASSWORD	
3053	1	int8	43823	MODE	
1020	4	int32	43823	RESULT_CODE	
58	2	int16	-	VlanId	VLAN
59	2	int16	-	postVlanID	POST VLAN
56	6	mac_address	-	Source MAC Address	

FTP Metadata Export Template IPFIX Format					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
57	6	mac_adress	-	Destination MAC Address	
2017	-	raw	43823	MPLS Labels	

Note: the MODE field contains the FTP connection type 0 — active, 1 — passive

Messenger Metadata Export Template IPFIX Format (XMPP)					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
1001	4	int32	43823	TIME_STAMP	
1002	-	string	43823	LOGIN	
1003	4	IPv4	43823	IP_SRC	Sender's address
1004	4	IPv4	43823	IP_DST	Recipient's address
2000	8	int64	43823	SESSION_ID	
3100	-	string	43823	IM_LOGIN	
3101	-	string	43823	IM_PASSW	
3102	-	string	43823	IM_SCREEN_NAME	
3103	-	string	43823	IM_UIN	Universal Internet number
3104	1	int8	43823	IM_PROTOCOL	Type of protocol used
3105	-	string	43823	IM_RECEIVERS	
1020	4	int32	43823	RESULT_CODE	
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	

Note: the IM_PROTOCOL field contains the type of protocol used: 0 — ICQ, 7 — XMPP, 106 — ZELLO

IPFIX format of mail protocol metadata export template (POP, IMAP, SMTP)					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
1001	4	int32	43823	TIME_STAMP	
1002	-	string	43823	LOGIN	
1003	4	IPv4	43823	IP_SRC	Sender's address
1004	4	IPv4	43823	IP_DST	Recipient's address
2000	8	int64	43823	SESSION_ID	
3150	-	string	43823	MAIL_SENDER	
3151	-	string	43823	MAIL_RECEIVER	
3152	-	string	43823	MAIL_CC	Recipient of the copy
3153	-	string	43823	MAIL_SUBJECT	
3154	-	string	43823	MAIL_SERVERS	
3155	-	string	43823	MAIL_REPLY	
3156	1	int8	43823	EVENT	Event type
3157	1	int8	43823	ATTACHMENT	Indication of attachment
3158	1	int8	43823	MAIL_PROTOCOL	
1020	4	int32	43823	RESULT_CODE	
58	2	int16	-	VlanId	VLAN

IPFIX format of mail protocol metadata export template (POP, IMAP, SMTP)					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
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	

Note: the EVENT field indicates the event type 1 — send, 2 — receive,
ATTACHMENT sign of an attachment, mail_protocol = 0 — smtp, 1 — pop3, 2 — imap

The raw unparsed metadata export template IPFIX format					
№	**Size in bytes**	**Type**	**IANA**	**Description**	**Note**
1001	4	int32	43823	TIME_STAMP	
1002	-	string	43823	LOGIN	
1003	4	IPv4	43823	IP_SRC	Sender's address
1004	4	IPv4	43823	IP_DST	Recipient's address
2000	8	int64	43823	SESSION_ID	
2013	1	int8	43823	FLW_DIR	Directing the packet across interfaces
2014	1	int8	43823	DIR_DATA	Forwarding a packet by session
2015	2	int16	43823	VDPI_PROTO	The protocol that determined the DPI
2900	2	int16	43823	META_PROTO	Internal protocol identifier
2901	-	string	43823	RAW_DATA	
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	

Note:

- **FLW_DIR** — direction of packet on interfaces : 0 : subs → inet, 1 : inet → subs
- **DIR_DATA** — direction of the packet by session: for TCP 0 : client → server, 1 : server → client, for UDP — from whom the first packet was recorded, he is considered the client
- **VDPI_PROTO** — protocol that defined DPI
- **META_PROTO** — internal protocol identifier (3 — SIP, 4 — FTP, 5 — SMTP, 6 — POP3, 7 — IMAP, 8 — XMPP, 9 — ICQ, 10 — RSS, 11 — NNTP, 12 — H323, 13 — ZELLO)
- **RAW_DATA** — raw data

Aggregating `raw_data`, `clickstream`, `http_reply` and `ssl_reply` with session data requires additional processing or executing a database query with the `session_id` key, or support in the `rcollector` utility.

Configuring the export of DNS responses or DNS queries

DNS export is configured with the following settings:

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

where

- **em1** — the name of the network interface to export.
- **ipfix_dns_udp_collectors** — UDP addresses of collectors.
- **ipfix_dns_tcp_collectors** — TCP collector addresses.

The format of IPFIX templates for IPV6 differs in the format of the IP_SOURCE and IP_DESTINATION fields.

№	Number of bytes	Data type	IANA	Description	Note
1103	16	IPv6	43823	IP_SOURCE	Sender's address
1104	16	IPv6	43823	IP_DESTINATION	Recipient's address

DNS Export Template IPFIX Format					
№	**Number of bytes**	**Data type**	**IANA**	**Description**	**Note**
1001	4	int32	43823	TIME_STAMP	Timestamp
1002	-	string	43823	LOGIN	Log in
1003	4	IPv4	43823	IP_SOURCE	Sender's address
1004	4	IPv4	43823	IP_DESTINATION	Recipient's address
1013	2	int16	43823	SOURCE PORT	
1014	2	int16	43823	DESTINATION PORT	
2000	8	int64	43823	SESSION_ID	Session ID
3200	1	int8	43823	UDP/TCP	Transport: 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	Channel (vchannel) or bridge number. If vchannel is set in the DPI configuration, the channel number will be transmitted, otherwise the bridge number will be transmitted
224	8	uint64	-	ipTotalLength	Total IP packet size
3206	2	uint16	43823	DNS transaction id	DNS Transaction ID

An alternative is to save the data in a local text log. Parameters:

- **ajb_save_dns** — a bit flag that controls whether to log to a text file and enable sending DNS queries via IPFIX.
  - **ajb_save_dns=0** — do not save
  - **ajb_save_dns=1** — enable saving DNS responses to a file
  - **ajb_save_dns=2** — enables sending DNS queries via IPFIX
  - **ajb_save_dns=3** — enables sending DNS requests via IPFIX and saving DNS responses to a file

The filter for DNS **request** types to be sent via IPFIX is specified by the `ajb_save_dns_request_types` parameter. Values can be specified as ranges using a hyphen, as a list separated by commas, or as the keywords `all` (any value) and `none` (filter all values). By default, the parameter is set to `all`.
The filter for DNS **response** types to be sent via IPFIX is specified by the `ajb_save_dns_answer_types` parameter. Values can be specified as ranges using hyphens, lists separated by commas, and the keywords `all` (any value) and `none` (filter all values). By default, the parameter is set to `1,5,28`.

- **ajb_dns_ftimeout** — timeout (minutes) for switching to the next file
- **ajb_dns_bufsize** — file write buffer
- **ajb_dns_fsize** — file size limit
- **ajb_dns_path** — path where to write

Switching to the next file occurs when the file size reaches `ajb_dns_fsize` or the file is not empty and `ajb_dns_ftimeout` has passed

`ajb_save_dns_format`: format for writing to a text file

- **ts** - time
- **ipsrc** — ip source
- **ipdst** — ip destination
- **ssid** — session id
- **login** — understandable

- **host** — the name of which the information was requested
- **rrtype** — RR types
- **rrclass** — RR class
- **ttl** — TTL
- **rdlen** — rdata size
- **rdata** — the resource itself
- **psrc** — port source
- **pdst** — port destination
- **transport** — how the DNS query was received.

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

Sending Template in IPFIX

1. Transport protocol TCP.
   The Template is sent once after the TCP session is established.
2. Transport protocol UDP.
   The Template is sent by default every 20 seconds. This is controlled by the `ipfix_udp_template_timer` parameter.

[1)]

for the IPv6 variant see difference above

[2)]

for the IPv6 variant, see difference above