

Содержание

3 IPFIX export	3
<i>ClickStream export Setup</i>	3
<i>IPFIX format template for Clickstream</i>	3

3 IPFIX export

For Clickstream data analysis (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 netflow5 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](#).

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

IPFIX format template for Clickstream

The format of IPFIX templates for IPV6 differs only in the IP SOURCE and IP DESTINATION fields.

Nº	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

Nº	Size in bytes	Type	IANA	Description	Note
1001	4	int32	43823	TIMESTAMP	
1002	-	string	43823	LOGIN	
1003	4	ipv4	43823	IP SOURCE	
1004	4	ipv4	43823	IP DESTINATION	
1005	-	string	43823	HOSTNAME/CNAME	

Nº	Size in bytes	Type	IANA	Description	Note
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	
2016	2	int16	43823	BRIDGECHANNELNUM	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.

ND:

- LOCKED contains the blocking mark if its value !=0,
- HOST TYPE = 1 in case of HTTP, 2 - CNAME, 3 - SNI, 4 - QUIC
- METHOD = 1 - GET, 2 - POST, 3 - PUT, 4 - DELETE

Clickstream is useful not only local authorities but ISP also for subscriber interest profiles, top of sites, ads targeting, prevent outflow of subscribers etc.

SIP metadata export is configured by 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
```

here em1 NIC for data export

ipfix_meta_udp_collectors IP of udp collectors

ipfix_meta_tcp_collectors IP of tcp collectors

dbg_log_mask=0x80 logging statistics about export

IPFIX format template for export SIP metadata

Nº	Size in Bytes	Type	IANA	Description	Note
0	4	int32	1001	timestamp	
1	-	string	1002	Login	
2	4	ipv4	1003	ip_src	
3	4	ipv4	1004	ip_dst	
4	8	int64	2000	session_id	
5	-	string	3000	msg code	
6	2	int16	3001	status code	
7	-	string	3002	uri	
8	-	string	3003	from	
9	-	string	3004	to	

Nº	Size in Bytes	Type	IANA	Description	Note
10		- string	3005	callid	
11		- string	3006	uagent	
12		- string	3007	ctype	

IPFIX template for FTP metadata export

Nº	size	type	IANA	description	Note
1001	4	int32	43823	timestamp	
1002	-	string	43823	Login	
1003	4	ipv4	43823	ip_src	
1004	4	ipv4	43823	ip_dst	
2000	8	int64	43823	session_id	
3050	-	string	43823	server name	
3051	-	string	43823	user	
3052	-	string	43823	password	
3053	1	int8	43823	mode	



the mode field contains the type of ftp connection 0 - active, 1 - passive

IPFIX template for short messages metadata protocols (XMPP)

Nº	size	type	IANA	description	Note
1001	4	int32	43823	timestamp	
1002	-	string	43823	Login	
1003	4	ipv4	43823	ip_src	
1004	4	ipv4	43823	ip_dst	
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	
3104	1	int8	43823	im_protocol	
3105	-	string	43823	im_receivers	



the im_protocol field contains the type of used protocol: 7 - XMPP

IPFIX template for export EMAIL metadata protocols (POP,IMAP,SMTP)

Nº	size	type	IANA	description	Note
1001	4	int32	43823	timestamp	
1002	-	string	43823	Login	
1003	4	ipv4	43823	ip_src	
1004	4	ipv4	43823	ip_dst	
2000	8	int64	43823	session_id	
3150	-	string	43823	mail_sender	

№	size	type	IANA	description	Note
3151	-	string	43823	mail_receiver	
3152	-	string	43823	mail_cc	
3153	-	string	43823	mail_subject	
3154	-	string	43823	mail_servers	
3155	-	string	43823	mail_reply	
3156	1	int8	43823	event	
3157	1	int8	43823	attachment	
3158	1	int8	43823	mail_protocol	



the event field contains the type of event 1 - send, 2 - receive



the attachment field contains the attachment mark



mail_protocol = 0 - smtp, 1 - pop3, 2 - imap

For receiving export with IPFIX protocol can be used any universal IPFIX collector, for instance - [CESNET ipfixcol](#) or our utility [IPFIX Receiver](#)