Содержание

3 IPFIX export

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.

ClickStream export Setup

Clickstream experts is configured by folowing 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.

№	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	TIMESTAMP	
1002	-	string	43823	LOGIN	
1003	4	ipv4	43823	IP SOURCE	
1004	4	ipv4	43823	IP DESTINATION	

№	Size in bytes	Type	IANA	Description	Note
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
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 (0x3 for HTTP, 0x1 for everything else),
- 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
1001	4	int32	43823	TIMESTAMP
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

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
1001	4	int32	43823	TIMESTAMP
1002	-	string	43823	LOGIN

№	Size in bytes	Type	IANA	Description
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

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
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
3000	-	string	43823	MSG CODE
3001	2	int16	43823	STATUS CODE
3002	-	string	43823	URI
3003	-	string	43823	FROM
3004	-	string	43823	TO
3005	-	string	43823	CALLID
3006	-	string	43823	UAGENT
3007	-	string	43823	CTYPE
3008	-	string	43823	GATEWAYS

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
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
1020	4	int32	43823	RESULT CODE

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
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
1020	4	int32	43823	RESULT CODE

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
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
3151	-	string	43823	MAIL_RECEIVER

№	Size in bytes	Type	IANA	Description
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
1020	4	int32	43823	RESULT CODE

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
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
2013	1	int8	43823	FLW_DIR
2014	1	int8	43823	DIR_DATA
2015	2	int16	43823	VDPI_PROTO
2900	2	int16	43823	META_PROTO
2901	-	string	43823	RAW_DATA

Note: field

- *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.

DNS

Parameters:

- *ajb_save_dns* - flag for writing to a text file
- *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.

Now:

```
//
// transport for DNS
//
typedef enum en_dns_transport : u_int8_t
{
edns_udp=0
edns_tcp=1,
edns_max = 2,
} en_dns_transport_t;
```

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

```
// IPFIX collectors. Format as usual:
ipfix_dns_udp_collectors
ipfix_dns_tcp_collectors
```

dbg_log_mask for fastdpi - Mainly used for debugging and troubleshooting:

```
enum: uint64_t {
brg_lgmsk_dpi = 0x01, // display dpi statistics
brg_lgmsk_mem_usage = 0x02, // display statistics on memory usage
brg_lgmsk_plc = 0x04, // output policing statistics
brg_lgmsk_clstr_wthr = 0x08, // print statistics on cluster worker threads
brg_lgmsk_ajb = 0x10, // display statistics on the use of ajb buffers
brg_lgmsk_stat_ddos = 0x20, // display statistics on DDOS parameters
brg_lgmsk_call_udr = 0x40, // output to alert the results of the UDR call
```

```
function
brg_lgmsk_ipfix = 0x80, // Show IPFIX statistics
brg_lgmsk_flow = 0x100, // Data output by flow (session output)
brg_lgmsk_ip_proto = 0x200, // output statistics by ip type
brg_lgmsk_eth_type = 0x400, // display statistics by type of ethernet packet
brg_lgmsk_slice_stat = 0x800, // print slice statistics for flow and IP
brg_lgmsk_dna_cluster = 0x1000, // debug DNA cluster creation
brg_lgmsk_lock_stat = 0x2000, // multicluster lock statistics
brg_lgmsk_all_cpu_stat = 0x4000, // load statistics for all cores
brg_lgmsk_load_vchannels= 0x8000, // vcahnnels loading statistics
brg_lgmsk_redirect = 0x10000,// redirect operations
brg_lgmsk_dna_cluster_stat= 0x20000, // record statistics for
pfring_zc_stats
brg_lgmsk_nat = 0x40000, // NAT initialization
brg_lgmsk_bind = 0x80000, // bind operations
brg_lgmsk_stat_nat_whbl = 0x100000, // output NAT statistics on white block
brg_lgmsk_print_ip = 0x200000, // Printing IP data to the statistics file
brg_lgmsk_print_nat = 0x400000, // Print NAT data to statistics file
brg_lgmsk_check_nat = 0x800000, // check NAT
brg_lgmsk_tm_nflw_ipfix = 0x1000000, // output netflow/ipfix send time
brg_lgmsk_stat_nat = 0x2000000, // output NAT statistics to fastdpi_stat.log
brg_lgmsk_tod_brg_sync = 0x4000000, // trace time synchronization
gettimeofday <--> rtdsc

brg_lgmsk_ctrlopt = 0x8000000, // Display data for CTRLOPT in statistics

brg_lgmsk_auth = 0x10000000,// authorization statistics for local users
brg_lgmsk_apartment = 0x20000000, // apartment statistics
brg_lgmsk_conmon = 0x40000000, // print connection monitor traces to alert
brg_lgmsk_task_scheduler= 0x80000000, // output scheduler traces to alert
brg_lgmsk_tfrwd =0x100000000, // print statistics for trafix forward
};
```

1)

for IPv6 variant see difference above

2)

for the IPv6 variant, see difference above