Содержание

3 Экспорт 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 NetFow5 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.

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

Формат IPFIX шаблона экспорта Clickstream					
№	**Кол-во байт**	**Тип данных**	**IANA**	**Описание**	**Примечание**
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	Ку́ки
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	-	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	
2018	4	int32	43823	TCP Sequence	

Примечание: LOCKED – битовая маска, содержит признак того, был ли ресурс заблокирован или переадресован (0x3 для HTTP, 0x1 для остального).
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

Формат IPFIX шаблона экспорта Clickstream для ответов HTTP [1)]					
№	Кол-во байт	Тип данных	IANA	Описание	Примечание
2000	8	int64	43823	SESSION_ID	Идентификатор сессии

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
1030	2	int16	43823	SSL_VERSION	Версия SSL
1031	2	int16	43823	CIPHER_SUITE	Набор шифров
1032	1	int8	43823	COMPRESSION_METHOD	Метод сжатия

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

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

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
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

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**	**Т ип 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

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**	**Т ип 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

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 клиентом считается.
- ***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 утилилите rcollector.

DNS

Параметры:

- ***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 записывающему 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 пролучен DNS запрос.

Сейчас:

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

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

```
// IPFIX коллекторы. Формат как обычно:
ipfix_dns_udp_collectors
ipfix_dns_tcp_collectors
```

"*dbg_log_mask*" для fastdpi - Используется в основном для отладки и поиска проблем:

```
enum: uint64_t {
brg_lgmsk_dpi = 0x01, // Вывод статистики dpi.
brg_lgmsk_mem_usage = 0x02, // Вывод статистики использования памяти.
brg_lgmsk_plc = 0x04, // Вывод статистики Policingai.
brg_lgmsk_clstr_wthr = 0x08, // Вывод статистики по рабочим потокам кластера.
brg_lgmsk_ajb = 0x10, // Вывод статистики использования буферов ajb.
brg_lgmsk_stat_ddos = 0x20, // Вывод статистики по параметрам DDOS.
brg_lgmsk_call_udr = 0x40, // Вывод результатов функции обращения к UDR в alert.
brg_lgmsk_ipfix = 0x80, // Вывод статистики по IPFIX.
brg_lgmsk_flow = 0x100, // Вывод данных по flow ( вывод сессий ).
brg_lgmsk_ip_proto = 0x200, // Ввывод статистики по типу IP.
brg_lgmsk_eth_type = 0x400, // Вывод статистики по типу Ethernet пакета.
brg_lgmsk_slice_stat = 0x800, // Вывод статистики по slice для flow и IP.
brg_lgmsk_dna_cluster = 0x1000, // Отладка создания DNA-кластера.
brg_lgmsk_lock_stat = 0x2000, // Статистика блокировок для мультикластера.
brg_lgmsk_all_cpu_stat = 0x4000, // Статистика загруженности по всем ядрам.
brg_lgmsk_load_vchannels= 0x8000, // Статистика загрузки vcahnnels.
brg_lgmsk_redirect = 0x10000,// Операции с переадресацией.
brg_lgmsk_dna_cluster_stat= 0x20000, // Запись статистики для pfring_zc_stats.
brg_lgmsk_nat = 0x40000, // Инициализация NAT.
brg_lgmsk_bind = 0x80000, // Операции bind.
brg_lgmsk_stat_nat_whbl = 0x100000, // Вывод статистики NAT по белому блоку.
brg_lgmsk_print_ip = 0x200000, // Вывод данных по IP в файл статистики.
brg_lgmsk_print_nat = 0x400000, // Вывод данных по NAT в файл статистики.
brg_lgmsk_check_nat = 0x800000, // Проверка NAT.
brg_lgmsk_tm_nflw_ipfix = 0x1000000, // Вывод времени отправки netflow/ipfix.
brg_lgmsk_stat_nat = 0x2000000, // Вывод статистики NAT в fastdpi_stat.log.
brg_lgmsk_tod_brg_sync = 0x4000000, // Трассировка синхронизации времени
gettimeofday. <--> rtdsc

brg_lgmsk_ctrlopt = 0x8000000, // Вывод в статисику данных для CTRLOPT.

brg_lgmsk_auth = 0x10000000,// Статистика авторизаций локальных пользователей.
brg_lgmsk_apartment = 0x20000000, // Статистика по апартаментам.
brg_lgmsk_conmon = 0x40000000, // Вывод трейсов монитора соединений в alert.
brg_lgmsk_task_scheduler= 0x80000000, // Вывод трейсов планировщика в alert.
brg_lgmsk_tfrwd =0x100000000, // Вывод статистики для trafix forward.
};
```

[1], [2]
для варианта с IPv6 см. выше отличие