# **Table of Contents**

5 Конфигурация	. 3
Конфигурация IPFIX ресиверов	. 3
Конфигурация DPI	7

# 5 Конфигурация

# Конфигурация IPFIX ресиверов

Настройка ipfix ресиверов через файл .env

```
/var/qoestor/backend/.env
```

Стандартная конфигурация выглядит следующим образом

```
#Ipfix form DPI 0
IPFIX_FULLFLOW_PORT_TYPE[0]=tcp
IPFIX_FULLFLOW_PORT[0]=1500
#IPFIX_FULLFLOW_ROTATE_MINUTES[0]=10
#IPFIX_FULLFLOW_ROTATE_DELAY_SECONDS[0]=0
#IPFIX_FULLFLOW_FW_MAX_QUEUE_SIZE[0]=10
#IPFIX_FULLFLOW_DUMP_INSERT_PROCESSES[0]=0
#IPFIX_FULLFLOW_EXPORT[0]=10.0.0.2/9920/tcp,10.0.0.3/3440/udp
```

IPFIX\_CLICKSTREAM\_PORT\_TYPE[0]=tcp IPFIX\_CLICKSTREAM\_PORT[0]=1501 #IPFIX\_CLICKSTREAM\_ROTATE\_MINUTES[0]=12 #IPFIX\_CLICKSTREAM\_ROTATE\_DELAY\_SECONDS[0]=400 #IPFIX\_CLICKSTREAM\_FW\_MAX\_QUEUE\_SIZE[0]=10 #IPFIX\_CLICKSTREAM\_FW\_MAX\_QUEUE\_SIZE[0]=10 #IPFIX\_CLICKSTREAM\_DUMP\_INSERT\_PROCESSES[0]=0 #IPFIX\_CLICKSTREAM\_EXPORT[0]=10.0.0.2/9921/tcp,10.0.0.3/3441/udp

```
IPFIX_GTPFLOW_PORT_TYPE[0]=tcp
IPFIX_GTPFLOW_PORT[0]=1502
#IPFIX_GTPFLOW_ROTATE_MINUTES[0]=10
#IPFIX_GTPFLOW_ROTATE_DELAY_SECONDS[0]=0
#IPFIX_GTPFLOW_FW_MAX_QUEUE_SIZE[0]=10
#IPFIX_GTPFLOW_DUMP_INSERT_PROCESSES[0]=0
#IPFIX_GTPFLOW_EXPORT[0]=10.0.0.2/9921/tcp,10.0.0.3/3441/udp
```

```
IPFIX_NATFLOW_PORT_TYPE[0]=tcp
IPFIX_NATFLOW_PORT[0]=1503
#IPFIX_NATFLOW_ROTATE_MINUTES[0]=10
#IPFIX_NATFLOW_ROTATE_DELAY_SECONDS[0]=0
#IPFIX_NATFLOW_FW_MAX_QUEUE_SIZE[0]=10
#IPFIX_NATFLOW_DUMP_INSERT_PROCESSES[0]=0
#IPFIX_NATFLOW_EXPORT[0]=10.0.0.2/9921/tcp,10.0.0.3/3441/udp
```

#Traffic direction definition
# 0 - as is
# 1 - by AS (for fullflow only)
# 2 - by CIDR (for fullflow and clickstream)
# 3 - by both: AS and CIDR
# 4 - any: AS or CIDR

TRAFFIC DIR DEF MODE=0 #Subscriber filter # 0 - no filter # 1 - by AS (for fullflow only) # 2 - by CIDR (for fullflow and clickstream) # 3 - by both: AS and CIDR # 4 - any: AS or CIDR SUBSCRIBER FILTER MODE=0 #Subscriber exclude # 0 - no exclude # 1 - by AS (for fullflow only) # 2 - by CIDR (for fullflow and clickstream) # 3 - by both: AS and CIDR # 4 - any: AS or CIDR SUBSCRIBER EXCLUDE MODE=0 #Enable host (url) categories dics autoload URLS CATEGORIES DIC AUTOLOAD ENABLED=1 #Enable asnum dic autoload ASNUM\_DIC\_AUTOLOAD\_ENABLED=1 #Enable auto replacing Login with vchannel on insert # 0 - Disabled # 1 - Enabled # 2 - Enabled if Login is empty ULR REPLACE LOGIN WITH VCHANNEL=0 # Use dictionary when replacing login ULR USE DIC WHEN REPLACING LOGIN=0 # Enable autoload of vchannel name dic ULR VCHANNEL NAME DIC AUTOLOAD ENABLED=0 # vchannel name dic remote url ULR\_VCHANNEL\_NAME\_DIC\_URL= #Import NAT events from fullflow NAT IMPORT\_FROM\_FULLFLOW # 0 - Disabled # 1 - Enabled

#Fields to save when aggregating NAT log (bitmask)
# 0x1 - Save protocol ID
# 0x2 - Save event type,
# 0x4 - Save source ipv4,
# 0x8 - Save source port,
# 0x10 - Save destination ipv4,
# 0x20 - Save destination port,

```
# 0x40 - Save post NAT source ipv4,
# 0x80 - Save post NAT source_port,
# 0x100 - Save session ID,
# 0x200 - Save login,
# 0x400 - Save DPI ID
NAT_AGG_LOG_FIELDS_TO_SAVE_BITMASK=0
#Time interval for aggregating NAT logs
NAT_AGG_LOG_GROUP_TIME_INTERVAL
# 1 - 1 minute
# 5 - 5 minutes
# 10 - 10 minutes
# 15 - 15 minutes
# 30 - 30 minutes
# 60 - 60 minutes
```

В представленной конфигурации настроен запуск fullflow и clickstream ресиверов на udp сокетах 1500 и 1501 соответственно. «0» в индексе массива означает, что прием идет от DPI под номером 0.



#### Список параметров

- IPFIX\_FULLFLOW\_PORT\_TYPE[i] и IPFIX\_CLICKSTREAM\_PORT\_TYPE[i] определяют тип трафика, принимаемого на порту: tcp или udp. Рекомендуется ставить tcp.
- IPFIX\_FULLFLOW\_PORT[i] и IPFIX\_CLICKSTREAM\_PORT[i] определяют номер порта.
- TRAFFIC\_DIR\_DEF\_MODE и SUBSCRIBER\_FILTER\_MODE определяет режим фильтрации абонентов согласно справочникам asnum\_local\_dic и subnets\_local\_dic. Значения TRAFFIC\_DIR\_DEF\_MODE=0 и SUBSCRIBER\_FILTER\_MODE=0 означают, что вычислять направление трафика и фильтровать абонентов не требуется.
- SUBSCRIBER\_EXCLUDE\_MODE определяет режим фильтрации абонентов согласно справочникам asnum\_exclude\_dic и subnets\_exclude\_dic. Значение SUBSCRIBER\_EXCLUDE\_MODE=0 означает, что фильтрация не требуется.
- IPFIX\_FULLFLOW\_EXPORT[i] и IPFIX\_CLICKSTREAM\_EXPORT[i] дают возможность настроить экспорт на сторонние ресиверы. Формат ip/port/proto[,ip/port/proto].
- IPFIX\_FULLFLOW\_ROTATE\_MINUTES[i] и IPFIX\_CLICKSTREAM\_ROTATE\_MINUTES[i] дают возможность настроить период ротации дампов и запись их в БД. По умолчанию это 10 минут для fullflow и 12 минут для clickstream.
- IPFIX\_FULLFLOW\_ROTATE\_DELAY\_SECONDS[i] и IPFIX\_CLICKSTREAM\_ROTATE\_DELAY\_SECONDS[i] дают возможность настроить задержку вставки данных на определенное количество секунд. По умолчанию для fullflow – 0 секунд, для clickstream – 400 секунд. Задержка для clickstream относительно fullflow нужна, чтобы обеспечить соединения логов fullflow и clickstream для обогащения статистических отчетов.

• IPFIX\_FULLFLOW\_FW\_MAX\_QUEUE\_SIZE[i] и IPFIX\_CLICKSTREAM\_FW\_MAX\_QUEUE\_SIZE[i] определяют максимальный размер очереди на ресиверах. Лучше не трогать.



Если конфигурация изменилась, необходимо запустить скрипт sudo sh /var/qoestor/backend/qoestor-config.sh

#### Следующий пример конфигурации позволяет настроить прием от нескольких DPI

#Ipfix form DPI 0
IPFIX\_FULLFLOW\_PORT\_TYPE[0]=tcp
IPFIX FULLFLOW PORT[0]=1500

IPFIX\_CLICKSTREAM\_PORT\_TYPE[0]=tcp
IPFIX\_CLICKSTREAM\_PORT[0]=1501

#Ipfix form DPI 1
IPFIX\_FULLFLOW\_PORT\_TYPE[1]=tcp
IPFIX\_FULLFLOW\_PORT[1]=1510

IPFIX\_CLICKSTREAM\_PORT\_TYPE[1]=tcp
IPFIX\_CLICKSTREAM\_PORT[1]=1511

#Ipfix form DPI 2
IPFIX\_FULLFLOW\_PORT\_TYPE[2]=tcp
IPFIX\_FULLFLOW\_PORT[2]=1520

IPFIX\_CLICKSTREAM\_PORT\_TYPE[2]=tcp
IPFIX\_CLICKSTREAM\_PORT[2]=1521

### Пример конфигурации, когда требуется определение абонентов по CIDR

Данная конфигурация актуальна в случаях, когда СКАТ DPI установлен на зеркале.

TRAFFIC\_DIR\_DEF\_MODE=2
SUBSCRIBER\_FILTER\_MODE=2

Не забудьте настроить справочник subnets\_local\_dic для этого примера конфигурации!

#### Пример конфигурации, когда настроен экспорт на сторонние ресиверы

IPFIX\_FULLFLOW\_PORT\_TYPE[0]=tcp
IPFIX\_FULLFLOW\_PORT[0]=1500
IPFIX\_FULLFLOW\_EXPORT[0]=10.0.0.2/1600/tcp

IPFIX\_CLICKSTREAM\_PORT\_TYPE[0]=tcp
IPFIX\_CLICKSTREAM\_PORT[0]=1501
IPFIX\_CLICKSTREAM\_EXPORT[0]=10.0.0.2/1601/tcp

Перезапуск всех ресиверов можно выполнить командой

sudo sh /var/qoestor/backend/qoestor-config.sh

Если требуется перезапуск ресиверов по отдельности, это можно сделать через перезапуск сервисов, например так

• Для CentOS 7

```
systemctl restart qoestor_fullflow_0.service
systemctl restart qoestor_clickstream_0.service
```

• Для CentOS 6

```
service qoestor_fullflow_0 stop
service qoestor_clickstream_0 stop
service qoestor_fullflow_0 start
service qoestor_clickstream_0 start
```

#### Остановка ресиверов

• Для CentOS 7

```
systemctl stop qoestor_fullflow_0.service
systemctl stop qoestor_clickstream_0.service
```

• Для CentOS 6

```
service qoestor_clickstream_0 stop
service qoestor_fullflow_0 stop
```

#### Остановка и запуск БД clickhouse

• Остановка

sudo /etc/init.d/clickhouse-server stop

• Запуск

```
sudo /etc/init.d/clickhouse-server restart
```

## Конфигурация DPI

#### Настройка экспорта

Версия DPI платформы д.б. не ниже 8.1.

Экспорт ipfix можно настроить, напрямую отредактировав файл fastdpi.conf на dpi.

```
netflow=8
netflow_dev=em1
netflow_timeout=10
netflow_full_collector_type=2
netflow_full_port_swap=0
netflow_full_collector=YOUR_QOESTOR_IP:1500
ipfix_dev=em1
ipfix_tcp_collectors=YOUR_QOESTOR_IP:1501
```

#### Потребуется рестарт fastdpi, чтобы изменения вступили в силу.

# Учтите, что параметр netflow - это битовая маска. Допускает несколько разных значений. Подробнее смотрите тут Настройка экспорта IPFIX

Также вы можете выполнить настройку с помощью DPIUI2 - dpiui2. Версия dpiui2 д.б не ниже 2.1.0.

Чтобы выполнить настройку с помощью DPIUI2, откройте раздел Управление DPI → Конфигурация. Откройте вкладку Сбор и анализ статистики по протоколам и направлениям.

Установите параметр neflow в Экспорт полной статистики по сессиям. См. рис. ниже.



Введите сокет fullflow ресивера в параметре netflow\_full\_collector. Параметр netflow\_full\_collector\_type должен быть установлен в "Экспорт ipfix на udp колллектор", а параметр netflow\_full\_port\_swap оставьте пустым или равным "Сохранять оригинальные номера

/ПРАВЛЕНИЕ DPI / КОНФИГУРАЦИЯ			
Kandjurypasjan			
@ Cospaners ti ▲ D	3 D Copris 🔶 Proper		
6C Hactpolios	Сбер и анализ статистики по протоколам и направлениями		
Ofeane	Для внешена автонолемы систем, Для внутренны автонолемых систем		
Фильтрация по реестру запрещенных сайтов	If agree vomentopa netfory coloranetwork no warpapresents (reffers_as_collector)		
Сбор н аналия статистики по протоковам и направлениям	192.168.0.1.9998		
Разметка преоретета трафека в завековности от протокола	IP agget vormer topa netflow to characterized gas destaware (netflow_bill_collector)		
Оптимизация использования внешних каналов доступа	192.168.0.1.9996		
Бескаровка и замена рекламы	Metog yvera noreseok warpyace (verflov.bill.method)		
Behuik onecos o Captive Portal			
Уведолление абонентов	Oppmar sectopra noneoro netflow (wetflow_full_collector_type) Sectopri ipfix waitep icontexting		
Kaunpotanne	IP agree somerropa netfore c nonoli cramectivoli (netfore.full.collector)		
Deaujerte ot DoS e DDoS attax:			
Oneparaposali COPU	Тайнаут наактивной сиссии в сикундая (netflow, pazzive, timeout)		
Cochester	20		
	Tailwayt astronoid caccoure coxyeque (netflow, active, interest) 80		
	Перидавать неформацию о тротокопах в номере горта (netflow_full_port_swap)		

Введите сокет clickstream ресивера в параметре ipfix\_udp\_collectors. См. рис. ниже.

УПРИВЛЕНИЕ DPI / КОНФИГУРАЦИЯ				
Kodarypaqun				
E Cospanero ti 🚓 D	🖓 🔲 Форма 🚸 Редактор			
60 Hacrpolios	Chrysanopował COPM			
OSware	192.168.0.0/24			
Фильтрация по реестру запрещенных сайтов	Activelycearts Januis wetagareaux HTTP (a)D, Jave, (4)			
Сбор и анализ статастики по тротоколам и направлениям				
Разметка прекратета трафика в завесямости от протокола	Стихон записнованных натаданных (а)скачески/"Jorman)			
Оттехнация использования внешних каналов доступа	ts:prg/lagin.jpsrc.ipdst.host.path.ref.uagent.cosikie.tphast.blackd.method			
Блакаровка в замена рекламы	Mecro passegases dalinos o satercivo sertagaseus (ajb.url.path)			
Benuil snacos a Captive Portal	Learned a final second s			
Уведолление абонентов	Phas certexents serrephetice gas compasses clicks/warm vepes (pfix (pfix_dev) emit			
Kaunpobanne	IP Inte governoe was (mort) convectops of is clickstream (pfx.udo.collectors)			
Daugeta ot DoS e DDoS atas:	<ul> <li>Prima prevenue many (view) of automotopic gain gain section many (processing-consecutive)</li> <li>172.01.195.98 (1991)172.01.195.97 (1990)</li> <li>IP anna gooversion many (respri) scorescropa (pflix clickstream) (pflix,tpp,collectors)</li> </ul>			
Oneparteposali COPM				
Систелиные				
	IP или должное или (ropt) колчектора (pfu meta clickstwam (ipfx,meta,udp,collectors)			
	172.31.155.95.1500,172.31.155.97.1999			
	IP una goarence una (ropt) sonnestopa (pfu neta clickstream ((pfix_meta_top_collectors)			
	172 01 105 00 1501 172 01 105 07 1000			

Нажмите Сохранить. Перезапустите fast\_dpi.См. рис. ниже.



#### Присвоение номера DPI

Откройте раздел Управление оборудованием → Оборудование. Для каждого устройства введите Индентификатор на ipfix коллекторе. См. рис. ниже.

$\triangleleft$	C	KAT DPI : Tes	t stand .34 -			
		УПРАВЛЕНИЕ ОРІ +	ОТ УПРАВЛЕНИЕ УСЛУГАМИ + Е	🛛 ООЕ АНАЛИТИКА -		
=	УПРАВЛЕНИЕ ОБОРУДОВАНИЕМ / ОБОРУДОВАНИЕ					
	+					
	Оборудование					
		Название		lp		
		Настройки об	борудования	10.0171.0		
		Название *		10.000		
		Test stand .34				
		lp *	Порт *			
			22			
		Логин *	Пароль •			
		arusnak				
		Sudo пользовател				
	(e) Настройки ірfіх					
		Идентификатор на				
	0					
			Сохранить			

## Настройка подключения DPIUI2 к QoE Stor

Чтобы просматривать QoE отчеты, необходимо настроить подключение DPIUI2 к QoE Stor. См. раздел Настройка подключения к QoE Stor