Table of Contents

Конфигурация IPFIX ресиверов

 Конфигурация в GUI

IPFIX ресиверы принимают статистику от DPI:

- Clickstream, Meta, DNS
- Full NetFlow
- GTP
- NAT

Настройка IPFIX ресиверов через файл .env: `/var/qoestor/backend/.env`

Под каждый поток настраивается отдельный ресивер.

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_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

IPFIX_DNSFLOW_PORT_TYPE[0]=tcp
IPFIX_DNSFLOW_PORT[0]=1504
#IPFIX_DNSFLOW_ROTATE_MINUTES[0]=10
#IPFIX_DNSFLOW_ROTATE_DELAY_SECONDS[0]=0
#IPFIX_DNSFLOW_FW_MAX_QUEUE_SIZE[0]=10
#IPFIX_DNSFLOW_DUMP_INSERT_PROCESSES[0]=0
#IPFIX_DNSFLOW_DPI_ID[0]=30
#IPFIX_DNSFLOW_BALANCER_SUB_PROTO[0]=tcp

#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.

Лучше использовать tcp, т.к для udp могут теряться пакеты при превышении MTU.

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 выполнить

```
fastor-restart
```

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 CKAT 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 ресиверов

Перезапуск всех ресиверов можно выполнить командой

```
fastor-restart
```

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

```
fastor-db-stop
```

- Запуск

```
fastor-db-restart
```