

Table of Contents

IPFIX receiver configuration	3
---	----------

IPFIX receiver configuration



Configuration in GUI

IPFIX receivers accept [statistics from DPI](#):

- [Clickstream, Meta, DNS](#)
- [Full NetFlow](#)
- [GTP](#)
- [NAT](#)

IPFIX receivers are configured through the .env file: `/var/qoestor/backend/.env`

A separate receiver is configured for each stream.

A standard configuration looks as follows:

```
#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 dicts 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

```

In this configuration, fullflow and clickstream receivers are started on UDP sockets 1500 and 1501 respectively. The «0» index means data is received from DPI number 0.



It is better to use TCP, as UDP may lose packets when MTU is exceeded.

Parameter list

- IPFIX_FULLFLOW_PORT_TYPE[i] and IPFIX_CLICKSTREAM_PORT_TYPE[i] define the traffic type received on the port: tcp or udp. TCP is recommended.
- IPFIX_FULLFLOW_PORT[i] and IPFIX_CLICKSTREAM_PORT[i] define the port number.
- TRAFFIC_DIR_DEF_MODE and SUBSCRIBER_FILTER_MODE define subscriber filtering mode according to the asnum_local_dic and subnets_local_dic directories. Values TRAFFIC_DIR_DEF_MODE=0 and SUBSCRIBER_FILTER_MODE=0 mean that traffic direction and subscriber filtering are not required.
- SUBSCRIBER_EXCLUDE_MODE defines subscriber exclusion mode according to the asnum_exclude_dic and subnets_exclude_dic directories. Value

SUBSCRIBER_EXCLUDE_MODE=0 means filtering is not required.

- IPFIX_FULLFLOW_EXPORT[i] and IPFIX_CLICKSTREAM_EXPORT[i] allow configuring export to external receivers. Format: ip/port/proto[,ip/port/proto].
- IPFIX_FULLFLOW_ROTATE_MINUTES[i] and IPFIX_CLICKSTREAM_ROTATE_MINUTES[i] allow configuring dump rotation and DB writing intervals. Default: 10 minutes for fullflow and 12 minutes for clickstream.
- IPFIX_FULLFLOW_ROTATE_DELAY_SECONDS[i] and IPFIX_CLICKSTREAM_ROTATE_DELAY_SECONDS[i] allow configuring insertion delay in seconds. Default: 0 seconds for fullflow, 400 seconds for clickstream. The clickstream delay relative to fullflow ensures log correlation for enriched reports.
- IPFIX_FULLFLOW_FW_MAX_QUEUE_SIZE[i] and IPFIX_CLICKSTREAM_FW_MAX_QUEUE_SIZE[i] define maximum receiver queue size. It is recommended not to change these values.



If the configuration has changed, run

```
fastor-restart
```

Example configuration for receiving from multiple 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
```

Example configuration for subscriber identification by CIDR

This configuration is relevant when the SSG DPI is installed on a mirror.

```
TRAFFIC_DIR_DEF_MODE=2
SUBSCRIBER_FILTER_MODE=2
```

Do not forget to configure the subnets_local_dic directory for this example!

Example configuration for export to external receivers

```
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
```

Restarting receivers

All receivers can be restarted with the command

```
fastor-restart
```

To restart receivers individually, restart the respective services, for example:

- For CentOS 7

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

- For CentOS 6

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

Stopping receivers

- For CentOS 7

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

- For CentOS 6

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

Stopping and starting the clickhouse database

- Stop

```
fastor-db-stop
```

- Start

```
fastor-db-restart
```