

# Table of Contents

<b>Searching for Flood Sources in the Operator's Network</b> .....	3
<b>1. Configuring statistics export from SSG</b> .....	3
<b>2. Searching for a flood source (BotNet)</b> .....	3
Searching for subscribers with a high number of flows per second .....	3
Searching for hosts with a high number of flows per second .....	5
<b>3. Blocking IPs by assigning them to an autonomous system</b> .....	6
Creating a local AS (example for IPv4) .....	6
Assigning a drop rule to the local AS .....	6



# Searching for Flood Sources in the Operator's Network

## 1. Configuring statistics export from SSG

The following parameter values must be set in the configuration file `/etc/dpi/fastdpi.conf`:

```
netflow=12
netflow_dev=vlan200
netflow_timeout=10
netflow_rate_limit=900
netflow_full_collector=10.0.0.0:1500
netflow_passive_timeout=5
netflow_active_timeout=20
netflow_full_collector_type=2
ipfix_reserved=1
```

where:

- `netflow=12` - statistics collection and export:  $8 + 4 = \text{fullnetflow} + \text{billnetflow}$  (accounting).
- `netflow_dev=vlan200` - where `vlan200` is the name of the interface from which statistics will be exported.
- `netflow_timeout=10` - export interval in seconds.
- `netflow_rate_limit=900` - IPFIX rate limit.
- `netflow_full_collector=10.0.0.0:1500` - statistics collector address - specify the correct QoE IP.
- `netflow_passive_timeout=5` - inactivity timeout for a session. If no activity is detected during this period, the session is considered finished and its information is exported.
- `netflow_active_timeout=20` - interval for reporting long sessions (i.e., long sessions are split into fragments of this duration).
- `netflow_full_collector_type=2` - export IPFIX to a TCP collector.
- `ipfix_reserved=1` - reserves the required memory to allow enabling/changing IPFIX/Netflow parameters.

After modifying the parameters, restart the service:

```
service fastdpi restart
```

## 2. Searching for a flood source (BotNet)

### Searching for subscribers with a high number of flows per second

1. Open the QoE Analytics report → Raw Full Netflow → Attack detection → Top subscribers → By flow:

QoE analytics > Raw full netflow

Period: 11/14/2025 11:02 - 11/14/2025 11:17 For all DPI devices 10 minutes

Top subscribers by flow

Subscriber	Login	Sessions	Flow	Flow from subscribers	Flow to subscribers	Flow volume	Flow volume from	Flow volume to
142.251.15.100		1	7 Kpkts/s	7 Kpkts/s	0 Pkts/s	7 Pkts	7 Pkts	0 Pkts
10.97.41.59	54955	2,131	6.9 Kpkts/s	6.9 Kpkts/s	0 Pkts/s	6.8 Mppts	6.8 Mppts	0 Pkts
10.97.73.153	51140	2,054	6.6 Kpkts/s	6.6 Kpkts/s	0 Pkts/s	6.5 Mppts	6.5 Mppts	0 Pkts
93.191.15.155		1	6 Kpkts/s	6 Kpkts/s	0 Pkts/s	6 Pkts	6 Pkts	0 Pkts
88.210.36.195		1	5 Kpkts/s	5 Kpkts/s	0 Pkts/s	15 Pkts	15 Pkts	0 Pkts
10.97.65.137	48397	1,002	5 Kpkts/s	5 Kpkts/s	0 Pkts/s	4.9 Mppts	4.9 Mppts	0 Pkts
10.97.366.85	39032	1,373	5 Kpkts/s	5 Kpkts/s	0 Pkts/s	5 Mppts	5 Mppts	0 Pkts
10.97.1.3	30880	4,360	4.2 Kpkts/s	4.2 Kpkts/s	0 Pkts/s	4.2 Mppts	4.2 Mppts	0 Pkts
172.235.182.238		1	4 Kpkts/s	4 Kpkts/s	0 Pkts/s	4 Pkts	4 Pkts	0 Pkts
172.234.171.9		1	4 Kpkts/s	4 Kpkts/s	0 Pkts/s	4 Pkts	4 Pkts	0 Pkts
172.235.245.182		1	4 Kpkts/s	4 Kpkts/s	0 Pkts/s	4 Pkts	4 Pkts	0 Pkts
172.232.205.212		1	3 Kpkts/s	3 Kpkts/s	0 Pkts/s	3 Pkts	3 Pkts	0 Pkts
23.221.236.70		1	3 Kpkts/s	3 Kpkts/s	0 Pkts/s	3 Pkts	3 Pkts	0 Pkts
192.168.1.100		1	3 Kpkts/s	3 Kpkts/s	0 Pkts/s	3 Pkts	3 Pkts	0 Pkts
104.88.206.203		1	3 Kpkts/s	3 Kpkts/s	0 Pkts/s	3 Pkts	3 Pkts	0 Pkts
172.237.126.231		1	3 Kpkts/s	3 Kpkts/s	0 Pkts/s	3 Pkts	3 Pkts	0 Pkts
9,618	9,618							

1-100 of 9618

Version 2.36.65 S

2. Set the time range:

QoE analytics > Raw full netflow

Period: 11/14/2025 11:02 - 11/14/2025 11:17 For all DPI devices 10 minutes

Custom range

Start: 14.11.2025 14:11

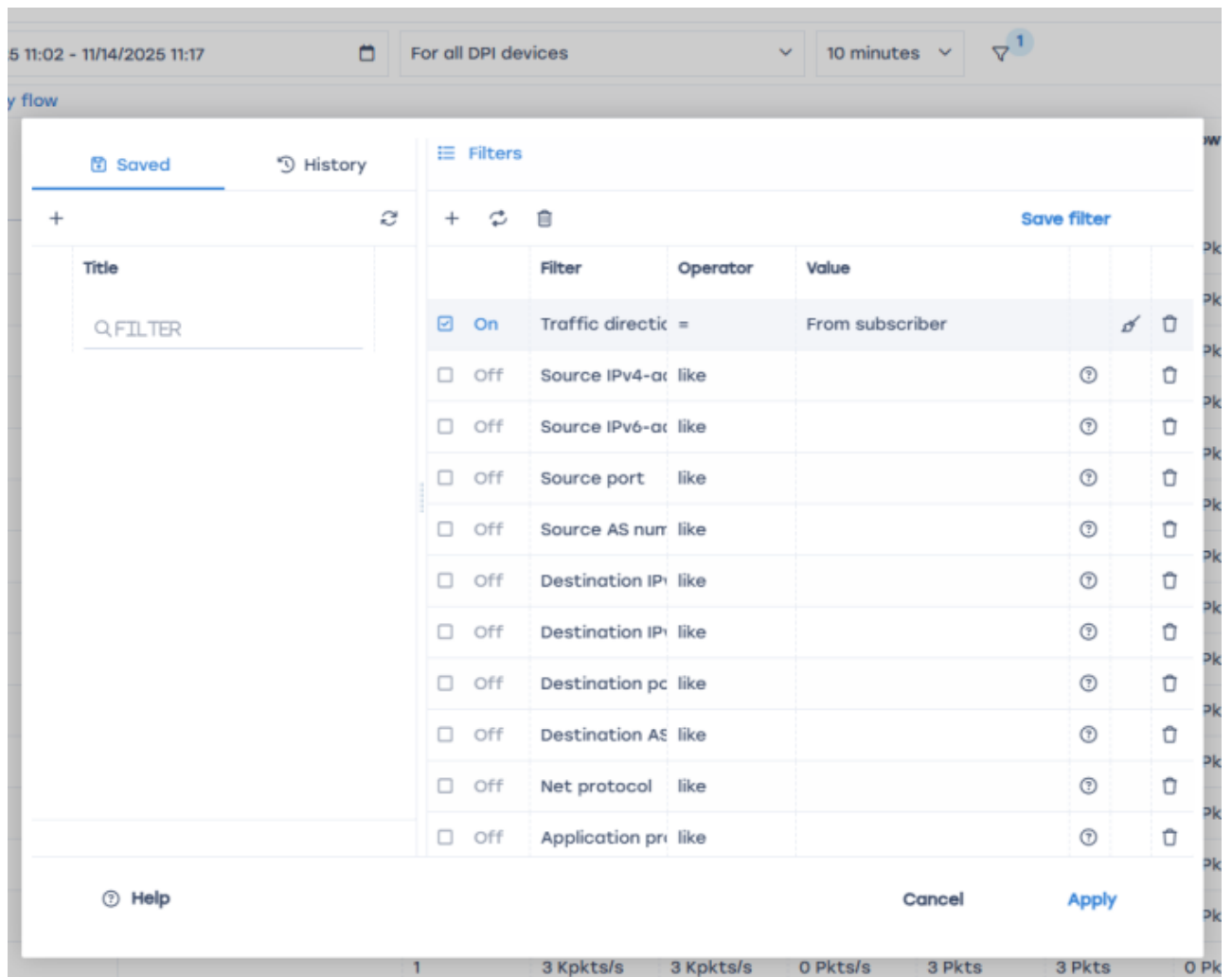
End: 14.11.2025 14:26

Quick ranges

- Last 5 minutes
- Last 15 minutes
- Last 30 minutes
- This hour
- This hour so far
- This 2 hours
- This 2 hours so far
- This 3 hours
- This 3 hours so far
- Last 1 hour
- Last 2 hours
- Last 3 hours
- Last 4 hours
- Last 5 hours
- Last 6 hours
- Last 12 hours
- Last 24 hours
- Last 2 days
- Last 3 days
- Last 4 days
- Last 5 days
- Last 6 days
- Last 7 days
- Last 15 days
- Last 30 days
- Last 90 days
- Last 6 months
- Last 1 year
- Last 2 years
- Last 5 years
- Yesterday
- Day before yesterday
- This day last week
- Previous week
- Previous month
- Previous year
- Today
- Today so far
- This week
- This week so far
- This month
- This month so far
- This year
- This year so far

Cancel Apply

3. Add a traffic direction filter - From subscriber:



4. Click the Flow column for convenient sorting

The detected subscriber source IP addresses must be added to a local AS ([see section 3.1](#))

## Searching for hosts with a high number of flows per second

1. Open the QoE Analytics report → Raw Full Netflow → Attack detection → Top host IP addresses → By flow:

QoE analytics > Raw full netflow

Period: 11/14/2025 11:02 - 11/14/2025 11:17

For all DPI devices

10 minutes

1

Top hosts IPs by flow

Hosts IPs	Host	Sessions	Flow	Flow from subscribers	Flow to subscribers	Flow volume from	Flow volume to	Flow volume to
5.59.131.194	5.59.131.194	18,423	30 Kpkts/s	30 Kpkts/s	0 Pkts/s	30 Mppts	30 Mppts	0 Pkts
108.181.60.75		1	28 Kpkts/s	28 Kpkts/s	0 Pkts/s	28 Pkts	28 Pkts	0 Pkts
89.187.180.24		1	13 Kpkts/s	13 Kpkts/s	0 Pkts/s	13 Pkts	13 Pkts	0 Pkts
92.301.11.172		1	11 Kpkts/s	11 Kpkts/s	0 Pkts/s	11 Pkts	11 Pkts	0 Pkts
172.233.251.92		52	11 Kpkts/s	11 Kpkts/s	0 Pkts/s	505 Pkts	505 Pkts	0 Pkts
163.171.158.12		1	10 Kpkts/s	10 Kpkts/s	0 Pkts/s	10 Pkts	10 Pkts	0 Pkts
108.130.104.143		9	9 Kpkts/s	9 Kpkts/s	0 Pkts/s	9 Pkts	9 Pkts	0 Pkts
34.250.170.239		9	9 Kpkts/s	9 Kpkts/s	0 Pkts/s	9 Pkts	9 Pkts	0 Pkts
142.251.16.100		1	7 Kpkts/s	7 Kpkts/s	0 Pkts/s	7 Pkts	7 Pkts	0 Pkts
92.223.123.57		7	7 Kpkts/s	7 Kpkts/s	0 Pkts/s	7 Pkts	7 Pkts	0 Pkts
199.232.173.189	gst.prod.dl.playstation.net	2	6.5 Kpkts/s	6.5 Kpkts/s	0 Pkts/s	1.8 Mppts	1.8 Mppts	0 Pkts
146.75.117.189	gs2.wv.prod.dl.playstation.net	6	6.5 Kpkts/s	6.5 Kpkts/s	0 Pkts/s	6.2 Mppts	6.2 Mppts	0 Pkts
5.188.121.254		129	6.7 Kpkts/s	6.7 Kpkts/s	0 Pkts/s	6.6 Mppts	6.6 Mppts	0 Pkts
91.105.192.100		10,308	5.5 Kpkts/s	5.5 Kpkts/s	0 Pkts/s	5.5 Mppts	5.5 Mppts	0 Pkts
185.226.54.242	ovu.mycdn.me	50	5.5 Kpkts/s	5.5 Kpkts/s	0 Pkts/s	5.4 Mppts	5.4 Mppts	0 Pkts
31.13.72.52	media-arn2-1.cdn.whatsapp.ne	22,980	4.2 Kpkts/s	4.2 Kpkts/s	0 Pkts/s	4.2 Mppts	4.2 Mppts	0 Pkts
100.000	100.000							

1-100 of 100000

Export 100

Reports

- Row log
- Attacks detection
  - SSH brute force
  - Top application protocols
  - Top application protocols groups
  - Top subscribers
  - Top hosts IPs
  - By traffic
  - By flow
  - By session lifetime
  - By subscribers and hosts
  - Maxi

2. Set the time range.
  3. Add a traffic direction filter – From subscriber.
  4. Click the Flow column for convenient sorting.
- The detected host IP addresses must be added to a local AS ([see section 3.1](#))

## 3. Blocking IPs by assigning them to an autonomous system

### Creating a local AS (example for IPv4)

1. Create a copy of /etc/dpi/aslocal.bin:

```
cp /etc/dpi/aslocal.bin /etc/dpi/aslocal.bin.backup
```

2. Convert aslocal.bin to a TXT file using the bin2as utility:

```
bin2as /etc/dpi/aslocal.bin > /etc/dpi/list.txt
```

If the aslocal.bin file is missing in /etc/dpi/, create it:

```
vi /etc/dpi/list.txt
```

3. Add entries to list.txt in the format (CIDR <space> ASN):

```
10.0.0.1/32 64525
172.16.0.0/12 64525
192.168.0.0/16 64525
```

Where 64525 is the AS that will later need to be blocked.

4. Convert the CIDR-ASN list from TXT to BIN format using the as2bin utility:

```
cat /etc/dpi/list.txt | as2bin /etc/dpi/aslocal.bin
```

5. Reload the service (hot parameter):

```
service fastdpi reload
```



[More details about preparing aslocal lists](#)

### Assigning a drop rule to the local AS

1. Create a copy of the asnum.dscp file:

```
cp /etc/dpi/asnum.dscp /etc/dpi/asnum.dscp.backup
```

2. Convert asnum.dscp to TXT using the dscp2as utility:

```
dscp2as /etc/dpi/asnum.dscp > /etc/dpi/asnum.txt
```

3. Add entries in the format ASN <space> drop to the existing records in asnum.txt:

```
64525 drop
```

4. Convert the TXT file back using the as2dscp utility:

```
cat /etc/dpi/asnum.txt | as2dscp /etc/dpi/asnum.dscp
```

5. Reload the service (hot parameter):

```
service fastdpi reload
```



[More details about DSCP assignment for ASN](#)