

Table of Contents

Searching for Flood Sources in the Operator's Network	3
1. Configuring statistics export from SSG	3
2. Searching for a flood source (BotNet)	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
3. Blocking IPs by assigning them to an autonomous system	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 = fullnetflow + 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

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 Mpks	6.8 Mpks	0 Pkts
10.97.73.153	51140	2,054	6.6 Kpkts/s	6.6 Kpkts/s	0 Pkts/s	6.5 Mpks	6.5 Mpks	0 Pkts
93.391.15.156		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
10.97.6.137	48397	1,002	6 Kpkts/s	5 Kpkts/s	0 Pkts/s	4.9 Mpks	4.9 Mpks	0 Pkts
10.97.166.85	39032	1,373	5 Kpkts/s	5 Kpkts/s	0 Pkts/s	5 Mpks	5 Mpks	0 Pkts
10.97.1.3	30880	4,360	4.2 Kpkts/s	4.2 Kpkts/s	0 Pkts/s	4.2 Mpks	4.2 Mpks	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
172.236.245.182		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						

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	Quick ranges
Start: 14.11.2025 14:11	Last 5 minutes
End: 14.11.2025 14:26	Last 15 minutes

Cancel Apply

3. Add a traffic direction filter – From subscriber:

Filter	Operator	Value
<input checked="" type="checkbox"/> On	Traffic direction	= From subscriber
<input type="checkbox"/> Off	Source IPv4-address	like
<input type="checkbox"/> Off	Source IPv6-address	like
<input type="checkbox"/> Off	Source port	like
<input type="checkbox"/> Off	Source AS number	like
<input type="checkbox"/> Off	Destination IP	like
<input type="checkbox"/> Off	Destination IP	like
<input type="checkbox"/> Off	Destination port	like
<input type="checkbox"/> Off	Destination AS	like
<input type="checkbox"/> Off	Net protocol	like
<input type="checkbox"/> Off	Application protocol	like

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:

Hosts IP	Host	Sessions	Flow	Flow from subscribers	Flow to subscribers	Flow volume	Flow volume from	Flow volume to
5.59.131.194	5.59.131.194	18,423	30 Kpkts/s	30 Kpkts/s	0 Pkts/s	30 Mpks	30 Mpks	0 Pkts
106.161.60.75		1	26 Kpkts/s	28 Kpkts/s	0 Pkts/s	26 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
92.101.11.172		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
108.130.104.343		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
142.251.19.100		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 Mpks	1.8 Mpks	0 Pkts
146.75.117.189	gs2.ww.prod.dl.playstation.net	6	6.5 Kpkts/s	6.5 Kpkts/s	0 Pkts/s	6.2 Mpks	6.2 Mpks	0 Pkts
6.188.121.254		129	6.7 Kpkts/s	6.7 Kpkts/s	0 Pkts/s	5.6 Mpks	5.6 Mpks	0 Pkts
91.105.192.100		10,308	6.5 Kpkts/s	6.5 Kpkts/s	0 Pkts/s	5.5 Mpks	5.5 Mpks	0 Pkts
186.226.54.242	ovu.mycdn.me	50	6.5 Kpkts/s	5.5 Kpkts/s	0 Pkts/s	5.4 Mpks	5.4 Mpks	0 Pkts
313.172.52.100,000	media-omn2-1.cdn.whotsoco.ne	22,980	4.2 Kpkts/s	4.2 Kpkts/s	0 Pkts/s	4.2 Mpks	4.2 Mpks	0 Pkts

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](#)