

# Table of Contents

<b>Configuring DDoS and BotNet Detector Based on QoE</b> .....	3
<b>1. Updating QoE</b> .....	3
<b>2. Updating GUI</b> .....	3
<b>3. Installing the Detector</b> .....	3
<b>4. Configuring the Detector</b> .....	4
<b>5. Trigger Thresholds</b> .....	5
<b>6. Metrics Storage (DDoS Attack Logs)</b> .....	5
<b>7. Attack Analysis</b> .....	6



# Configuring DDoS and BotNet Detector Based on QoE

The detector allows automatic monitoring of incoming traffic, identifying DDoS attacks, and quickly taking measures to protect the network. When a threat is detected, the system can fully isolate the malicious stream or clean the traffic while maintaining service availability for users.

The solution requires SSG version BASE, COMPLETE, or BNG with additional options and is deployed on an existing server with QoE.



[More about tools for DDoS protection and BotNet detection](#)

## 1. Updating QoE

**On the QoE server.**

[Update QoE](#) to the latest version, stopping the receivers beforehand. Before starting receivers, patch ClickHouse:

```
dnf --refresh install clickhouse-patched
```

Start the receivers.

## 2. Updating GUI

**On the GUI server.**

[Update GUI](#) to the latest version. Connect GUI to VAS Cloud if not already connected. Enable the aniddos license option.

In the file `/var/www/html/dpiui2/frontend/env.js` set the option `AppEnv.DDoSAttack_isVisible = 1;`

## 3. Installing the Detector

**On the QoE server.**

Install the mitigator package `fastm_qoe` on all nodes:

```
dnf install fastm_qoe
```

Switch Python version:

```
dnf install -y python39 python39-devel -y
sudo update-alternatives --install /usr/bin/python3 python3
/usr/bin/python3.6 60
sudo update-alternatives --install /usr/bin/python3 python3
/usr/bin/python3.9 70
sudo update-alternatives --config python3
```

Select version 3.9:

```
python3 --version
```

## 4. Configuring the Detector

### On the QoE server.

On all nodes, or on selected ones:

1. Edit the file `/var/fastm_qoe/etc/.env`.  
It should contain the following:

```
ANALYZER=avg-based-z-score
ANALYZER_RULES_KEY=avg-based-z-score-any

IDLE_MODE=1
FORCE_MODE=0
DB_DROP_TABLES=1

FM_ATTACKS_METRICS_BY_SUBS_FILTER="and has_attack = 0"
FM_ATTACKS_METRICS_BY_SUBS_LIMIT=1
FM_ATTACKS_METRICS_BY_SUBS_COLLAPSE=1
FM_ATTACKS_METRICS_BY_SUBS_DAY='day_'
```

2. Update schema:

```
fastm-db-scheme
```

3. Enable metrics collection

Add to file `/var/qoestor/backend/.env` the following:

```
FM_FULLFLOW_HOOK_ENABLE=1
GEO_IP_DIC_AUTOLOAD_ENABLED=1
```

Execute the daily cron:

```
sh /var/qoestor/backend/app_bash/cron_daily.sh
```

Collect metrics for several hours, ideally 24 hours. Then edit `/var/fastm_qoe/etc/.env` again and change 2 parameters:

```
IDLE_MODE=0
DB_DROP_TABLES=0
```

This activates the detector.

## 5. Trigger Thresholds

In the file `/var/fastm_qoe/lib/rules/config.json`, edit the section `avg-based-z-score-any` as follows:

```
"avg-based-z-score-any": {
  "octets": { "th": 100, "weight": 0.1 },
  "octets_dropped": { "th": 1000, "weight": 0.3 },
  "packets": { "th": 100, "weight": 0.3 },
  "packets_dropped": { "th": 1000, "weight": 0.3 },
  "flows": { "th": 100, "weight": 0.4 },
  "sessions": { "th": 100, "weight": 0.4 },
  "duration": { "th": 100, "weight": 0.01 },
  "host_ips": { "th": 100, "weight": 0.3 },
  "protos": { "th": 100, "weight": 0.3 },
  "bits_sec": { "th": 100, "weight": 0.05 },
  "bits_dropped_sec": { "th": 1000, "weight": 0.05 },
  "packets_sec": { "th": 100, "weight": 0.05 },
  "packets_dropped_sec": { "th": 1000, "weight": 0.05 }
},
```

## 6. Metrics Storage (DDoS Attack Logs)

In the GUI web interface, configure storage of raw and aggregated metrics, as well as raw and aggregated attack logs.

In Admin → GUI Configuration → QoE Stor: set DB retention time values as follows:

- `QOESTOR_FM_ATTACKS_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR = 720`
- `QOESTOR_FM_ATTACKS_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS = 30`
- `QOESTOR_FM_METRICS_MAIN_LOG_PARTITIONS_LIFE_TIME_HOUR = 72`
- `QOESTOR_FM_METRICS_AGG_LOG_PARTITIONS_LIFE_TIME_DAYS = 7`

Administrator > GUI configuration

Save The form Editor

Settings

Common

Jobs intervals and periods

QoE Stor: DB (Clickhouse) connection

QoE Stor: Raw log aggregation settings

QoE Stor: DB lifetime settings

QoE Stor: Discs settings

SMTP settings

System

DB (MySQL) connection

Ulr settings: System settings

Ulr settings: Web rules lists

Push notifications settings

SSO authorization settings

Maps settings

VasCloud settings

Cluster settings

Backup settings

Backup auto restoration settings

Telegram settings

QoE Stor: DB lifetime settings

100

GTP LOAD RATE from fullflow logs lifetime in days (GTP\_LOAD\_RATE\_FROM\_FULLFLOW\_LIFE\_TIME\_DAYS)

30 days

UPLINK LOAD RATE from fullflow logs lifetime in days (UPLINK\_LOAD\_RATE\_FROM\_FULLFLOW\_LIFE\_TIME\_DAYS)

30 days

DDoS attack logs lifetime in hours (QOESTOR\_FM\_ATTACKS\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)

720

DDoS attack aggregated logs lifetime in days (QOESTOR\_FM\_ATTACKS\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)

30

DDoS attack metrics logs lifetime in hours (QOESTOR\_FM\_METRICS\_MAIN\_LOG\_PARTITIONS\_LIFE\_TIME\_HOUR)

72

DDoS attack metrics aggregated logs lifetime in days (QOESTOR\_FM\_METRICS\_AGG\_LOG\_PARTITIONS\_LIFE\_TIME\_DAYS)

7

Default page size of QoE query (QUERY\_PAGE\_SIZE)

100

Max page size of QoE query (QUERY\_MAX\_PAGE\_SIZE)

10000

Export files life time in hours (EXPORT\_FILES\_LIFE\_TIME\_HOURS)

24

Limit lines in export file (LIMIT\_LINES\_IN\_EXPORT\_FILE)

1000000

## 7. Attack Analysis

Detected attacks can be examined in the DDoS attack sections in QoE Analytics.

1. Start with the "TOP Attacks" section for the last 24 hours.  
Sort attacks by number of sessions and note a few IPs with the highest session count.

Период

13.02.2026 10:48 - 13.02.2026 22:00 📅

По всем DPI устройствам ▾

10 минут ▾

☰ **Топ атак (DDoS атаки)**

IP-адрес цели	Количество атак	Количество типов атак	Сессии ▾	Средняя продолжительность	Скорость трафика	Скорость потока
<input type="text" value="Фильтр"/>		→				
10.23.18.203	1	1	1312070	13.1 с	2.4 Мбит/с	291 Пак/с
10.3.4.10	1	1	776707	15.3 с	2.3 Мбит/с	1.2 Кпак/с
10.23.60.41	1	1	676630	14.2 с	2 Мбит/с	477 Пак/с
10.23.43.85	1	1	540879	11.5 с	456.7 Кбит/с	67 Пак/с
10.23.29.21	1	1	396293	13.5 с	735.8 Кбит/с	98 Пак/с
10.253.21.104	1	1	278265	25.7 с	535.1 Кбит/с	384 Пак/с
10.9.216.221	1	1	155229	15.3 с	2.4 Мбит/с	773 Пак/с
10.208.172.214	1	1	133678	1.3 с	80.3 Кбит/с	21 Пак/с
10.25.253.17	1	1	72537	2 с	1 Мбит/с	393 Пак/с
10.208.23.196	1	1	56129	8.5 с	1.3 Мбит/с	153 Пак/с
10.253.19.62	1	1	54206	914 мс	175 Кбит/с	63 Пак/с
10.24.167.166	1	1	40898	8.4 с	448 Кбит/с	158 Пак/с
10.8.102.76	1	1	37255	2.6 с	600.8 Кбит/с	187 Пак/с
10.25.233.33	1	1	36759	1.1 с	601.2 Кбит/с	464 Пак/с

2. Check the "TOP Attacks by Protocols" section  
Also sort by session count. Note these protocols.
3. Check the "TOP Attacking IP Addresses" section, note a few IPs with the highest session count

Период 13.02.2026 10:48 - 13.02.2026 22:48 По всем DPI устройствам

Топ атакующих IP-адресов (DDoS атаки)

<input checked="" type="checkbox"/>	IP-адрес атакующего	Код страны	Регион	Город	Устройство	Количество типов атак	Сессии	Средняя продолжительность
	🔍 Фильтр	🔍 Фильтр	🔍 Фильтр	🔍 Фильтр				
<input checked="" type="checkbox"/>	179.6.109.0	PE	Ica	San Juan de P		1	278020	26.1 с
<input checked="" type="checkbox"/>	45.136.204.43	RU	Moscow	Moscow		1	153043	13.5 с
<input checked="" type="checkbox"/>	46.174.51.77	RU	Moscow	Moscow		1	138659	14.3 с
<input checked="" type="checkbox"/>	62.122.214.86	RU	Moscow	Moscow		1	123687	13.3 с
<input checked="" type="checkbox"/>	37.230.137.82	RU	Moscow	Moscow		1	123364	12.9 с
<input checked="" type="checkbox"/>	37.230.137.70	RU	Moscow	Moscow		1	83380	14.6 с
<input checked="" type="checkbox"/>	46.174.50.12	RU	Moscow	Moscow		1	73829	13.1 с
<input checked="" type="checkbox"/>	45.136.205.47	RU	Moscow	Moscow		1	72742	13.4 с
<input checked="" type="checkbox"/>	62.122.214.239	RU	Moscow	Moscow		1	72362	12.4 с
<input checked="" type="checkbox"/>	181.176.44.91	PE	Loreto	Yurimaguas		1	71875	786.3 мс
<input checked="" type="checkbox"/>	62.122.215.229	RU	Moscow	Moscow		1	71415	15.5 с
<input checked="" type="checkbox"/>	148.227.93.94	EC	Pichincha	Quito		1	69112	1 с
<input checked="" type="checkbox"/>	190.63.182.86	EC	Guayas	Tenguel		1	64421	1.2 с
<input checked="" type="checkbox"/>	37.230.210.146	RU	Moscow	Moscow		1	60088	9.8 с

4. Analyze the Attack Log with a filter by previously selected subscribers and protocol. You can extract attack details and make additional conclusions to take appropriate actions. For example, in the screenshot below it is clearly visible that there is port scanning on the same address using the UDP protocol. In this case, it is sufficient to assign a drop policy for the application protocol `udp unknown` to the attacking subscriber profile using session policing (service 18).

This means that for the selected subscriber, all traffic matching this protocol will be completely blocked, i.e., both UDP flood and legitimate UDP traffic identified by DPI as `udp unknown`.



More details about session policing configuration: [Policing by session and overriding traffic classes](#)

Состояние подлинки: **ОСТАЛОСЬ 18 ДНЕЙ**

Период: 12.02.2026 23:15 - 13.02.2026 23:15

По всем DPI устройствам

10 минут

2

🔄 🗑️ 📄

Сырой лог DDoS атак

Вой точка	Прикладной протокол	Группа	АС источника	IP-адрес атакующего	Порты атакующего	IP-адрес цели	Целевой порт	Логин абонента	Дельта пакетов	Отброшено байты
Фильтр	Фильтр		Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр	Фильтр
17	udp unknown	Неизвестно	65535	38.43.130.175	61278, 61616, 7417, 35174, 36464, 19988, 15039, 63451, 29674, 64210, 5485, 11732, 64323, 49437, 31	10.23.36.121	39368		289932	0
17	udp unknown	Неизвестно	65535	38.43.130.175	36298, 20685, 56667, 48295, 39652, 16227, 54408, 59065, 18084, 7122, 47621, 49975, 47972, 590	10.23.36.121	39368		286047	0
17	udp unknown	Неизвестно	65535	192.168.1.226	62500	10.23.36.121	39368		777	0
17	udp unknown	Неизвестно	65535	38.43.130.175	5291, 20685, 48295, 10978, 7951, 25163, 20362, 33961, 61686, 25980, 27988, 55845, 35368, 13483	10.23.36.121	56431		290598	0
17	udp unknown	Неизвестно	65535	38.43.130.175	51600, 12022, 47786, 40336, 63869, 14384, 22836, 35174, 58805, 47866, 25860, 32116, 58255, 575	10.23.36.121	56431		283383	0
17	udp unknown	Неизвестно	65535	192.168.1.226	64703	10.23.36.121	56431	64703	777	0
17	udp unknown	Неизвестно	65535	38.43.130.175	32100, 9171, 49799, 41168, 54408, 22415, 8845, 27983, 64809, 24923, 47407, 60845, 39494, 51720	10.23.36.121	49133		282606	0
17	udp unknown	Неизвестно	65535	38.43.130.175	38750, 15432, 43812, 23633, 22836, 35174, 55018, 29737, 15335, 43149, 29908, 5485, 32602, 5717	10.23.36.121	49133		290154	0
17	udp unknown	Неизвестно	65535	192.168.1.226	49420	10.23.36.121	49133		777	0
17	udp unknown	Неизвестно	65535	38.43.130.175	41801, 43812, 6772, 30893, 50625, 29737, 40896, 49437, 48713, 14684, 42081, 62476, 35003, 6305	10.23.36.121	32889		288267	0
17	udp unknown	Неизвестно	65535	38.43.130.175	31417, 56667, 49799, 49418, 37870, 58437, 55850, 49102, 57399, 58803, 25351, 17836, 44354, 5205	10.23.36.121	32889		289155	0
17	udp unknown	Неизвестно	65535	192.168.1.226	62954	10.23.36.121	32889		777	0
17	udp unknown	Неизвестно	65535	38.43.130.175	7417, 32676, 15335, 24654, 15039, 60803, 47753, 20833, 29071, 6574, 25918, 11748, 24856, 49307	10.23.36.121	43541		284826	0
17	udp unknown	Неизвестно	65535	38.43.130.175	35455, 20685, 30315, 55785, 58632, 16227, 64948, 7951, 22200, 16111, 62181, 7342, 33464, 47972	10.23.36.121	43541		289821	0
17	udp unknown	Неизвестно	65535	38.43.130.175	37842, 43755, 43282, 15432, 23633, 63017, 20622, 49604, 28322, 47469, 16727, 29071, 13636, 566	10.23.36.121	64525		246309	0

1-100 of 834

<< < 1 2 3 4 5 > >>

🔄 🗑️ 📄 Экспорт 100 ↓

