Содержание

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:

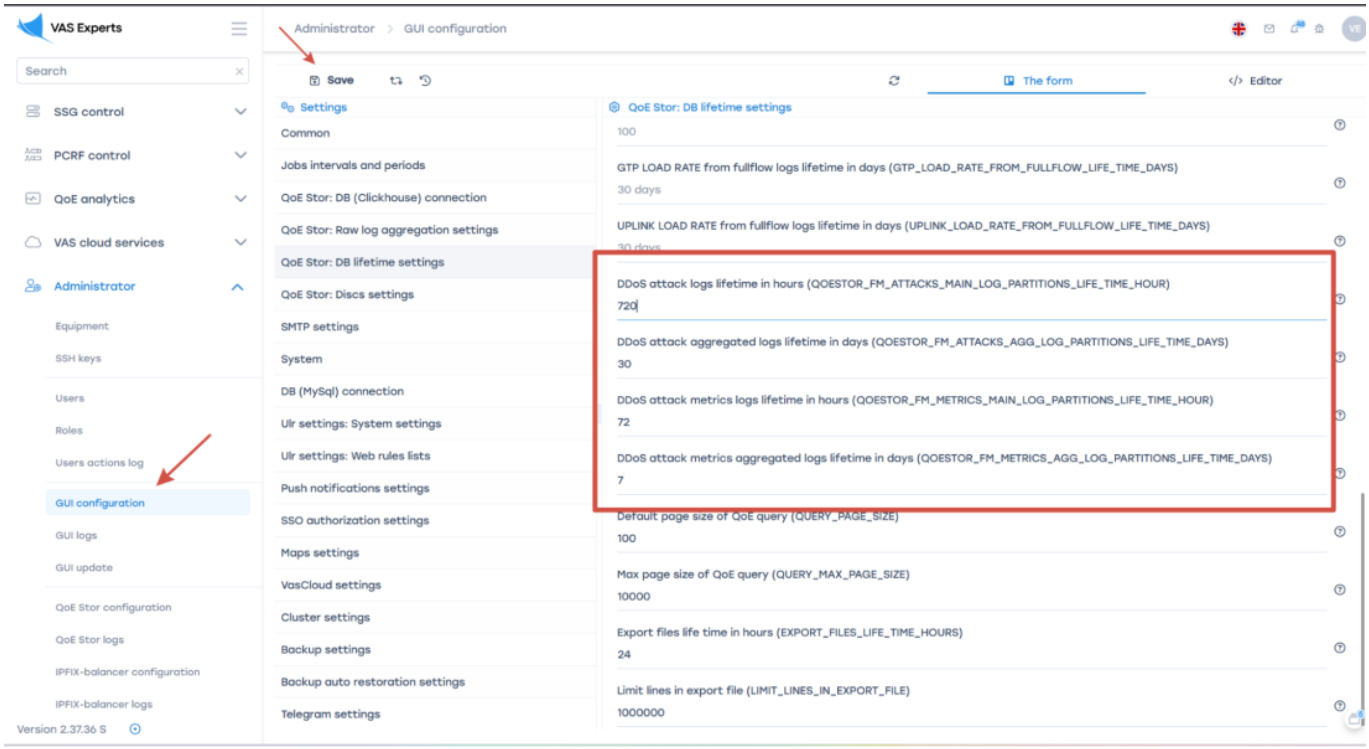
```
"avg-based-z-score-any": {
        "octets": { "th": 100, "weight": 0.1 },
        "octets_dropped": { "th": 1000, "weight": 0.3 },
        "packets": { "th": 100, "weight": 0.3 },
        "packets_dropped": { "th": 1000, "weight": 0.3 },
        "flows": { "th": 100, "weight": 0.4 },
        "sessions": { "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`



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.

Period 04/06/2026 11:21 - 04/06/2026 11:21 | For all DPI devices | 10 minutes

Top attacks (DDoS attacks)

Target IP address	Number of attacks	Number of attack	Sessions	Average duration	Traffic speed	flow speed
10.24.155.167	1	1	12076528	8.4 s	10.6 Mbit/s	1.1 Kpkts/s
10.29.65.249	1	1	4939850	13.9 s	4.9 Mbit/s	872 Pkts/s
10.21.143.162	1	1	4759639	13.3 s	2.3 Mbit/s	392 Pkts/s
10.17.140.164	1	1	2005908	20.6 s	2.2 Mbit/s	234 Pkts/s
10.29.240.241	1	1	1265823	5.4 s	523.2 Kbit/s	55 Pkts/s
10.29.102.74	1	1	1063588	9.1 s	1.2 Mbit/s	144 Pkts/s
10.22.61.219	1	1	640078	7 s	178.1 Kbit/s	31 Pkts/s
10.248.116.80	1	1	565021	14.6 s	617.6 Kbit/s	106 Pkts/s
10.8.125.162	1	1	559637	965 ms	95.3 Kbit/s	27 Pkts/s
10.29.76.96	1	1	333443	16.9 s	130.5 Kbit/s	16 Pkts/s
10.138.20.57	1	1	314470	26.3 s	551.8 Kbit/s	64 Pkts/s
10.25.200.147	1	1	287159	16.3 s	473.1 Kbit/s	55 Pkts/s
10.20.218.178	1	1	266081	15 s	82.7 Kbit/s	27 Pkts/s
10.17.88.12	1	1	224360	10.5 s	794.3 Kbit/s	103 Pkts/s

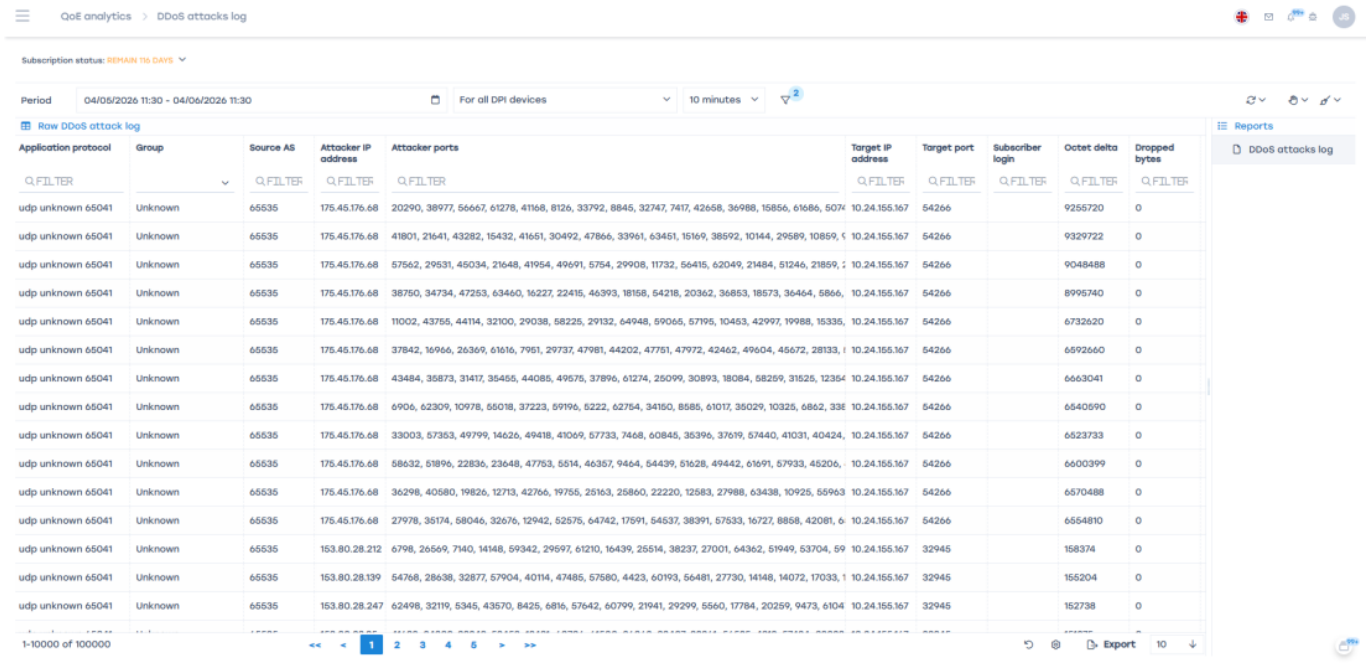
2. Check the "TOP Attacks by Protocols" section
   Also sort by session count. Note these protocols.
3. Check the "TOP Attacking IP Addresses" section, note a few IPs with the highest session count

Attacker IP address	Country code	State	City	Sessions	Average duration
175.45.176.68	US	California	Los Angeles	648894	3.8 s
87.76.218.2	NL	Overijssel	Hengevelde	365396	10.2 s
103.7.141.197	CN	Hubei	Shiyan (Maoji	348483	19.3 s
87.98.244.172	DE	Saarland	Saarbrucken	305586	29.8 s
181.214.214.24	IL	Haifa	Giv'at Nili	273252	18.3 s
82.167.183.26	SA	Riyadh Regior	Riyadh	253765	17.1 s
31.56.144.4	US	Virginia	Reston	209256	8.9 s
37.202.197.131	DE	Hesse	Frankfurt am	174740	19.8 s
101.98.88.216	NZ	Auckland	Auckland (Au	168953	16.3 s
156.246.66.20	HK	Kowloon	Hong Kong	139354	14.4 s
181.176.42.160	PE	Cajamarca D	Catilluc	129449	2.6 s
156.246.66.4	HK	Kowloon	Hong Kong	112427	18.9 s
45.138.202.181	IT	Tuscany	Scarperia e S	97502	13.8 s
200.40.36.1	UY	Montevideo D	Montevideo	92730	4.4 s

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


QoE analytics > DDoS attacks log
Subscription status: REMAIN 116 DAYS
Period
04/05/2026 11:30 - 04/06/2026 11:30
For all DPI devices
10 minutes
Raw DDoS attack log
Reports
DDoS attacks log
Application protocol
Group
Source AS
Attacker IP address
Attacker ports
Target IP address
Target port
Subscriber login
Octet delta
Dropped bytes
FILTER
udp unknown 65041 Unknown 65535 175.45.176.68 20290, 38977, 56667, 61278, 41168, 8126, 33792, 8845, 32747, 7417, 42658, 36988, 15856, 61686, 507 10.24.155.167 54266 9255720 0
udp unknown 65041 Unknown 65535 175.45.176.68 41801, 21641, 43282, 15432, 41651, 30492, 47866, 33961, 63451, 15169, 38592, 10144, 29589, 10859, 1 10.24.155.167 54266 9329722 0
udp unknown 65041 Unknown 65535 175.45.176.68 57562, 29531, 45034, 21648, 41954, 49691, 5754, 29908, 11732, 56415, 62049, 21484, 51246, 21859, 2 10.24.155.167 54266 9048488 0
udp unknown 65041 Unknown 65535 175.45.176.68 38750, 34734, 47253, 63460, 16227, 22415, 46393, 18158, 54218, 20362, 36853, 18573, 36464, 5866, 10.24.155.167 54266 8995740 0
udp unknown 65041 Unknown 65535 175.45.176.68 11002, 43755, 44114, 32100, 29038, 58225, 29132, 64948, 59065, 57195, 10453, 42997, 19988, 15335, 10.24.155.167 54266 6732620 0
udp unknown 65041 Unknown 65535 175.45.176.68 37842, 16966, 26369, 61616, 7951, 29737, 47981, 44202, 47751, 47972, 42462, 49604, 45672, 28133, 1 10.24.155.167 54266 6592660 0
udp unknown 65041 Unknown 65535 175.45.176.68 43484, 35873, 31417, 35455, 44085, 49575, 37896, 61274, 25099, 30893, 18084, 58259, 31525, 12354 10.24.155.167 54266 6663041 0
udp unknown 65041 Unknown 65535 175.45.176.68 6906, 62309, 10978, 55018, 37223, 59196, 5222, 62754, 34150, 8585, 61017, 35029, 10325, 6862, 338 10.24.155.167 54266 6540590 0
udp unknown 65041 Unknown 65535 175.45.176.68 33003, 57353, 49799, 14626, 49418, 41069, 57733, 7468, 60845, 35396, 37619, 57440, 41031, 40424, 10.24.155.167 54266 6523733 0
udp unknown 65041 Unknown 65535 175.45.176.68 58632, 51896, 22836, 23648, 47753, 5514, 46357, 9464, 54439, 51628, 49442, 61691, 57933, 45206, 10.24.155.167 54266 6600399 0
udp unknown 65041 Unknown 65535 175.45.176.68 36298, 40580, 19826, 12713, 42766, 19755, 25163, 25860, 22220, 12583, 27988, 63438, 10925, 55963 10.24.155.167 54266 6570488 0
udp unknown 65041 Unknown 65535 175.45.176.68 27978, 35174, 58046, 32676, 12942, 52575, 64742, 17591, 54537, 38391, 57533, 16727, 8858, 42081, 6 10.24.155.167 54266 6554810 0
udp unknown 65041 Unknown 65535 153.80.28.212 6798, 26569, 7140, 14148, 59342, 29597, 61210, 16439, 25514, 38237, 27001, 64362, 51949, 53704, 59 10.24.155.167 32945 158374 0
udp unknown 65041 Unknown 65535 153.80.28.139 54768, 28638, 32877, 57904, 40114, 47485, 57580, 4423, 60193, 56481, 27730, 14148, 14072, 17033, 1 10.24.155.167 32945 155204 0
udp unknown 65041 Unknown 65535 153.80.28.247 62498, 32119, 5345, 43570, 8425, 6816, 57642, 60799, 21941, 29299, 5560, 17784, 20259, 9473, 6104 10.24.155.167 32945 152738 0
1-10000 of 100000
<< < 1 2 3 4 5 > >>
Export
10