

Содержание

Настройка детектора DDoS и BotNet на базе QoE	3
1. Обновление QoE	3
2. Обновление GUI	3
3. Установка детектора	4
4. Настройка детектора	4
5. Пороги срабатывания	5
6. Хранение метрик (логи DDoS атак)	6
7. Анализ атак	7

Настройка детектора DDoS и BotNet на базе QoE

Детектор позволяет автоматически контролировать исходящий и входящий трафик, выявлять DDoS-атаки и оперативно принимать меры для защиты сети. Определять абонентов участников BotNet. При обнаружении угрозы система может полностью изолировать вредоносный поток или очистить трафик, сохранив доступность сервисов для пользователей. Решение требует:

- SKAT версии BASE, COMPLETE или BRAS с дополнительными опциями
- QoE с опцией Обнаружение и очистка трафика (blackhole and flowspec) от BotNet и DDoS-атак (опция antiddos)
- разворачивается на существующем сервере с QoE



[Подробнее об инструментах для защиты от DDoS и выявления BotNet](#)

1. Обновление QoE

На сервере QoE.

[Обновить QoE](#) до последней версии, предварительно остановив ресиверы. Перед запуском ресиверов пропатчить ClickHouse:

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

Установить период ротации на ресиверах – 1 минута.

Запустить ресиверы.

2. Обновление GUI

На сервере GUI.

[Обновить GUI](#) до последней версии. Подключить GUI к VAS Cloud, если еще не подключен, подключать **обязательно через API-токен**. [Настройка авторизации](#). Запросить опцию лицензии antiddos, если она еще не выдана.

В файле /var/www/html/dpiui2/frontend/env.js прописать опцию
AppEnv.DDoSAttack_isVisible = 1;

3. Установка детектора

На сервере QoE. Установить пакет митигатора fastm_qoe на все узлы:

1. Перед установкой переключить версию Python:

```
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
```

2. Выбрать версию Python 3.9:

```
python3 --version
```

3. Установить fastm_qoe:

```
dnf install fastm_qoe
```

4. Настройка детектора

На сервере QoE.

На всех узлах, либо на выбранных.

1. Отредактировать файл /var/fastm_qoe/etc/.env.
В нем должно быть следующее содержимое:

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

IDLE_MODE=1
FORCE_MODE=0
DB_DRÖP_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. Обновить схему:

```
fastm-db-scheme
clickhouse-client -n --query="system reload function has_attack_func"
clickhouse-client -n --query="system reload dictionary
fm_attacks_metrics_by_sub_dic"
```

3. Включить сбор метрик

Для этого в файле `/var/qoestor/backend/.env` добавить

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

Выполнить дневной крон:

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



Собирать метрики в течение 24 часов. После этого снова отредактировать файл `/var/fastm_qoe/etc/.env`, изменить 2 параметра:

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

Это активирует детектор.

4. Обновить словари:

```
clickhouse-client -n --query="system reload function has_attack_func"
clickhouse-client -n --query="system reload dictionary
fm_attacks_metrics_by_subs_dic"
```

5. Пороги срабатывания

В файле `/var/fastm_qoe/lib/rules/config.json` отредактировать раздел `avg-based-z-score-any` следующим образом:

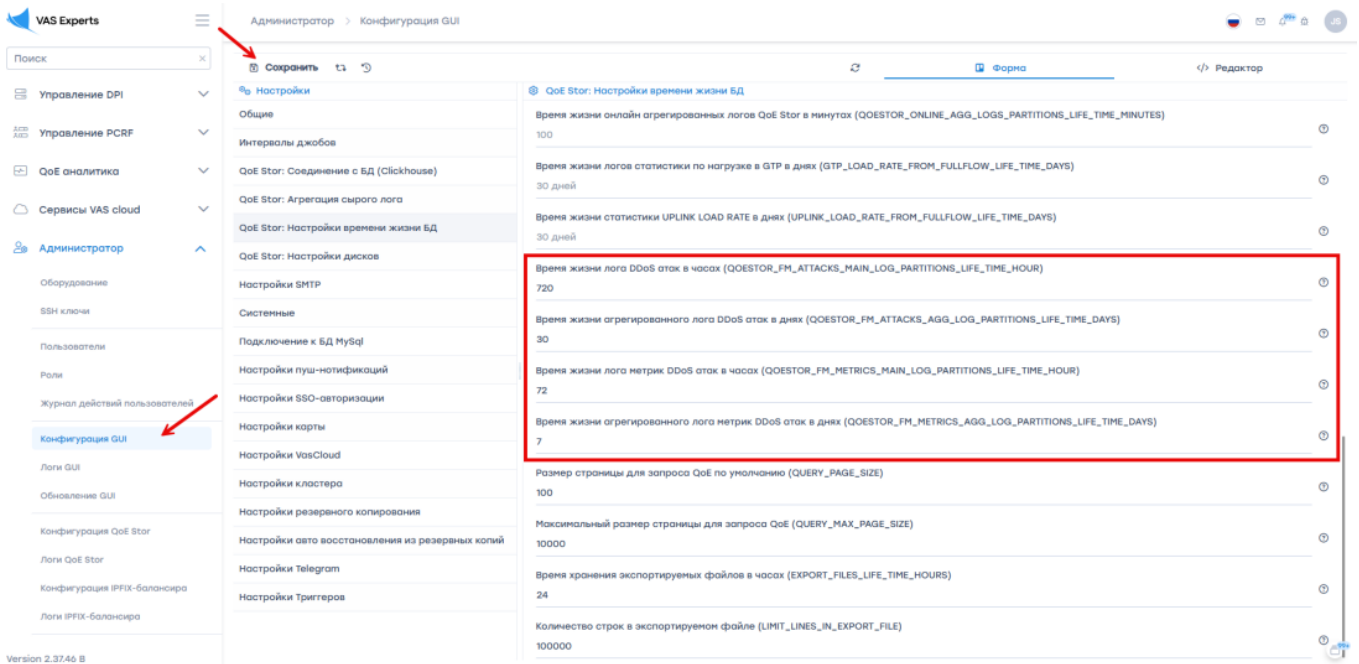
```
"avg-based-z-score-any": {
  "octets": { "th": 100, "weight": 0.1 },
  "octets_dropped": { "th": 1000, "weight": 0.3 },
  "packets": { "th": 100, "weight": 0.3 },
  "packets_dropped": { "th": 1000, "weight": 0.3 },
  "flows": { "th": 100, "weight": 0.4 },
  "sessions": { "th": 100, "weight": 0.4 },
  "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. Хранение метрик (логи DDoS атак)

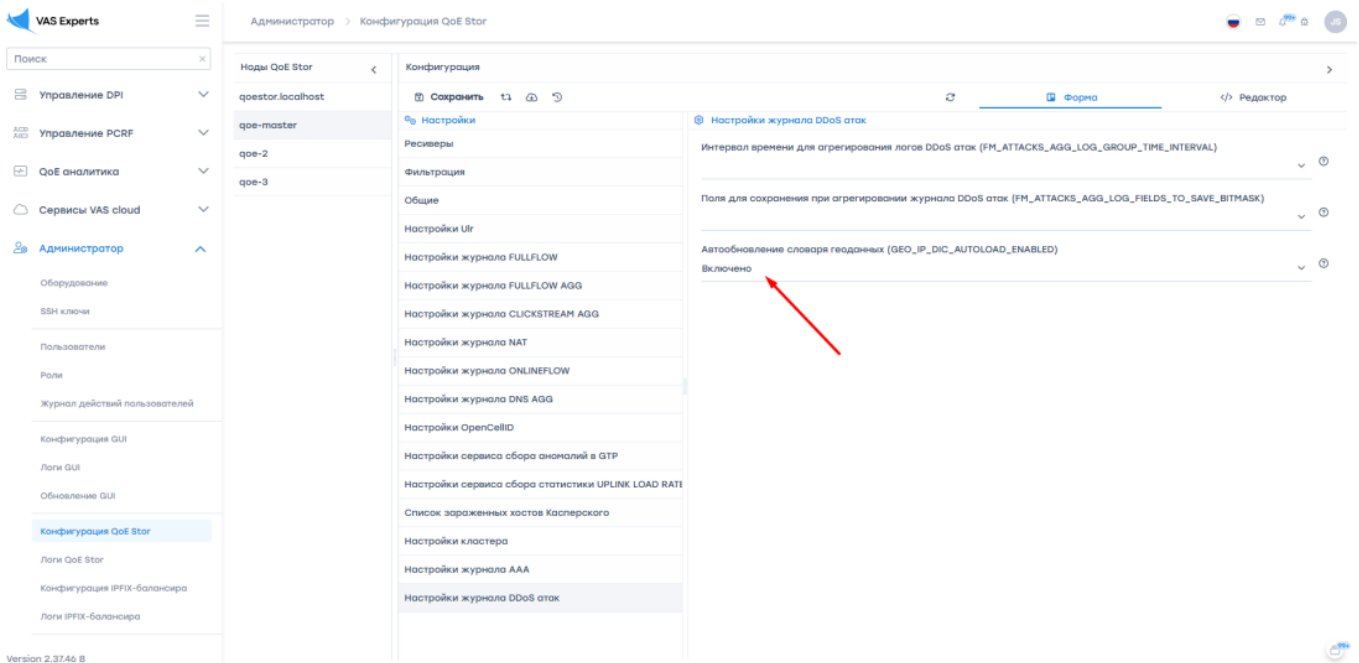
В веб-интерфейсе GUI настроить хранение сырых и агрегированных метрик, а также хранение сырого и агрегированного лога атак.

В разделе Администратор → Конфигурация GUI → QoE Stor: Настройки времени жизни БД задать следующие значения параметрам:

- 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



Для корректного отображения гео-отчетов DDoS-атак необходимо включить параметр GEO_IP_DIC_AUTOLOAD_ENABLED:



7. Анализ атак

Обнаруженные атаки можно изучить в разделах DDoS атаки в QoE Аналитике.

1. Начните с раздела "ТОП атак" за период 24 часа.
Отсортируйте атаки по количеству сессий, запишите себе несколько IP с наибольшим количеством сессий.

Состояние подписки: **ОСТАЛОСЬ 15 ДНЕЙ** ▾

Период	13.02.2026 10:48 - 13.02.2026 22	По всем DPI устройствам	10 минут			
Топ атак (DDoS атаки)						
IP-адрес цели	Количество атак	Количество типов атак	Сессии	Средняя продолжитель	Скорость трафика	Скорость потока
🔍 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. Посмотрите раздел "ТОП атак по протоколам"
Также отсортируйте по количеству сессий. Запишите себе эти протоколы
3. Посмотрите раздел "ТОП атакующих IP-адресов", запишите себе несколько IP с наибольшим количеством сессий

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. Проанализируйте Лог атак с фильтром по выбранным ранее абонентам и протоколу. Там можно почерпнуть детали атаки и сделать дополнительные выводы, чтобы принимать какие-либо решения. Например, на скриншоте ниже явно видно, что идет перебор портов на одном и том же адресе по UDP протоколу. В этом случае достаточно назначить на профиль атакующего абонента политику drop для прикладного протокола udp unknown через сессионный полисинг (18 услуга).

Это означает что для выбранного абонента будет полностью заблокирован трафик попадающий в данный протокол, т.е. как UDP flood, так и легитимный UDP трафик определенный на DPI как udp unknown.



Подробнее о настройке сессионного полисинга: [Полисинг по сессии и перераспределение классов трафика](#)

