Содержание

Настройка детектора DDoS на базе QoE

1. Обновление QoE

На сервере QoE.

Обновить QoE до последней версий как положено с остановкой ресиверов. Перед запуском ресиверов пропатчить KX

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

Запустить ресиверы.

2. Обновление GUI

На сервере GUI.

Обновить GUI до последней версии. Подключить GUI к VAS Cloud, если еще не подключен. Выдать опцию лицензии aniddos. 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 в все узлы:

```
dnf install fastm_qoe
```

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
```

Выбрать версию 3.9:

```
python3 --version
```

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_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. Обновить схему:

   ```
   fastm-db-scheme
   ```

3. Включить сбор метрик
   Для этого в файле `/var/qoestor/backend/.env` добавить
   `FM_FULLFLOW_HOOK_ENABLE=1`
   Собирать метрики несколько часов, лучше сутки. После отредактировать файл
   `/var/fastm_qoe/etc/.env` снова и изменить 2 параметра:

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

   Это активирует детектор.

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 агрегированно лога атак.

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