Содержание

Настройка детектора DDoS и BotNet на базе QoE

1. Обновление QoE

На сервере QoE.

Обновить QoE до последней версии, предварительно остановив ресиверы. Перед запуском ресиверов пропатчить ClickHouse:

```
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 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 },
```

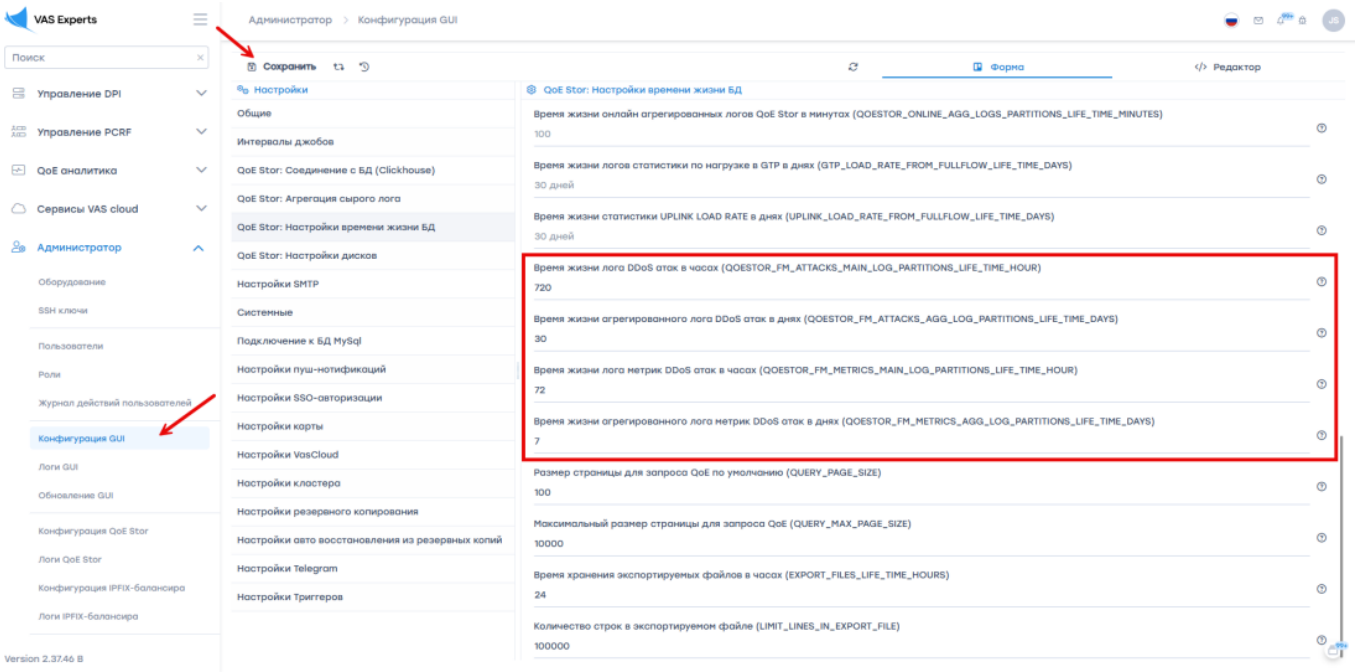
```
        "packets_dropped": { "th": 1000, "weight": 0.3 },
        "flows": { "th": 100, "weight": 0.4 },
        "sessions": { "th": 100, "weight": 0.4 },
        "duration": { "th": 100, "weight": 0.01 },
        "host_ips": { "th": 100, "weight": 0.3 },
        "protos": { "th": 100, "weight": 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 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

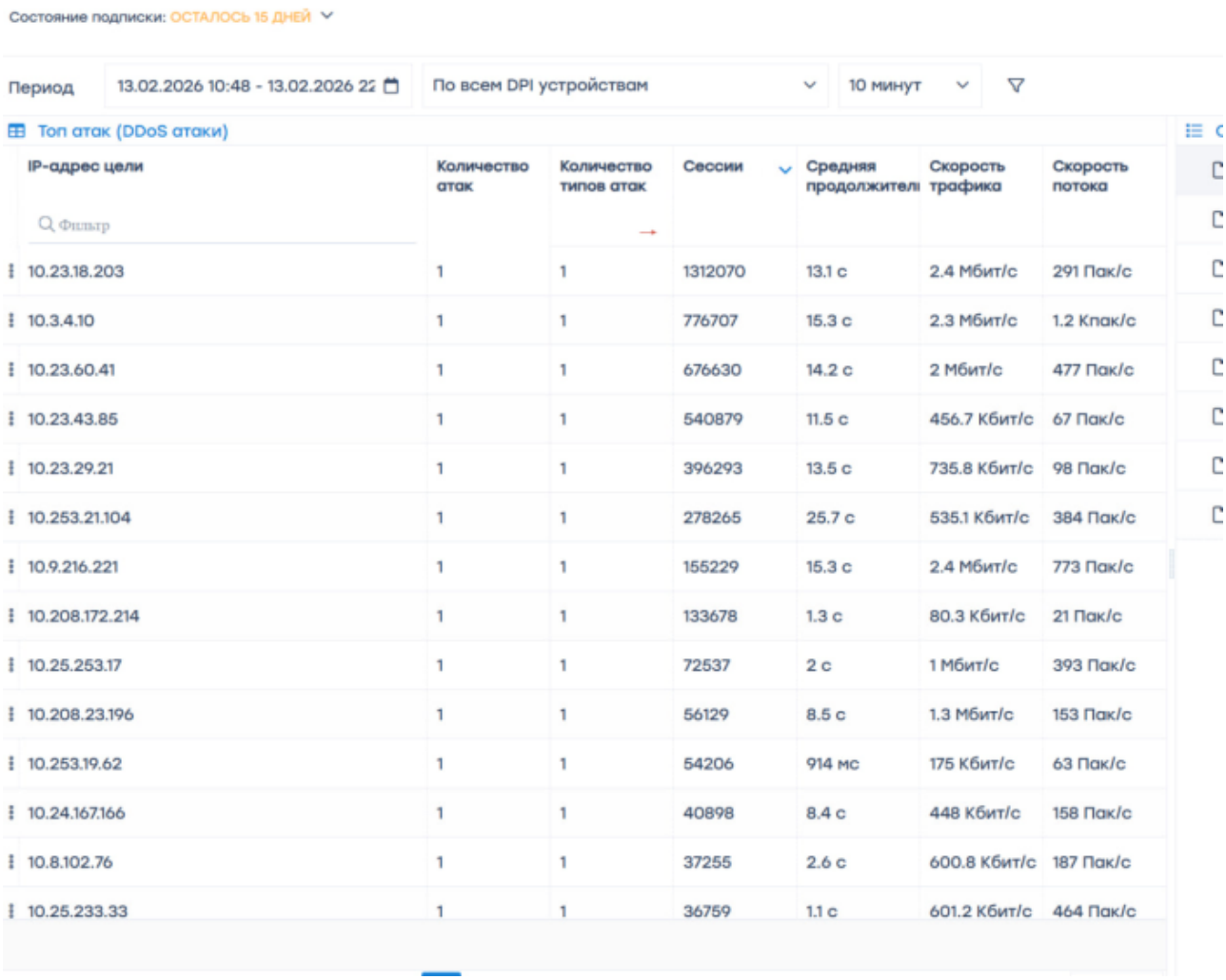


7. Анализ атак

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

1. Начните с раздела "ТОП атак" за период 24 часа.

Отсортируйте атаки по количеству сессий, запишите себе несколько IP с наибольшим количеством сессий.

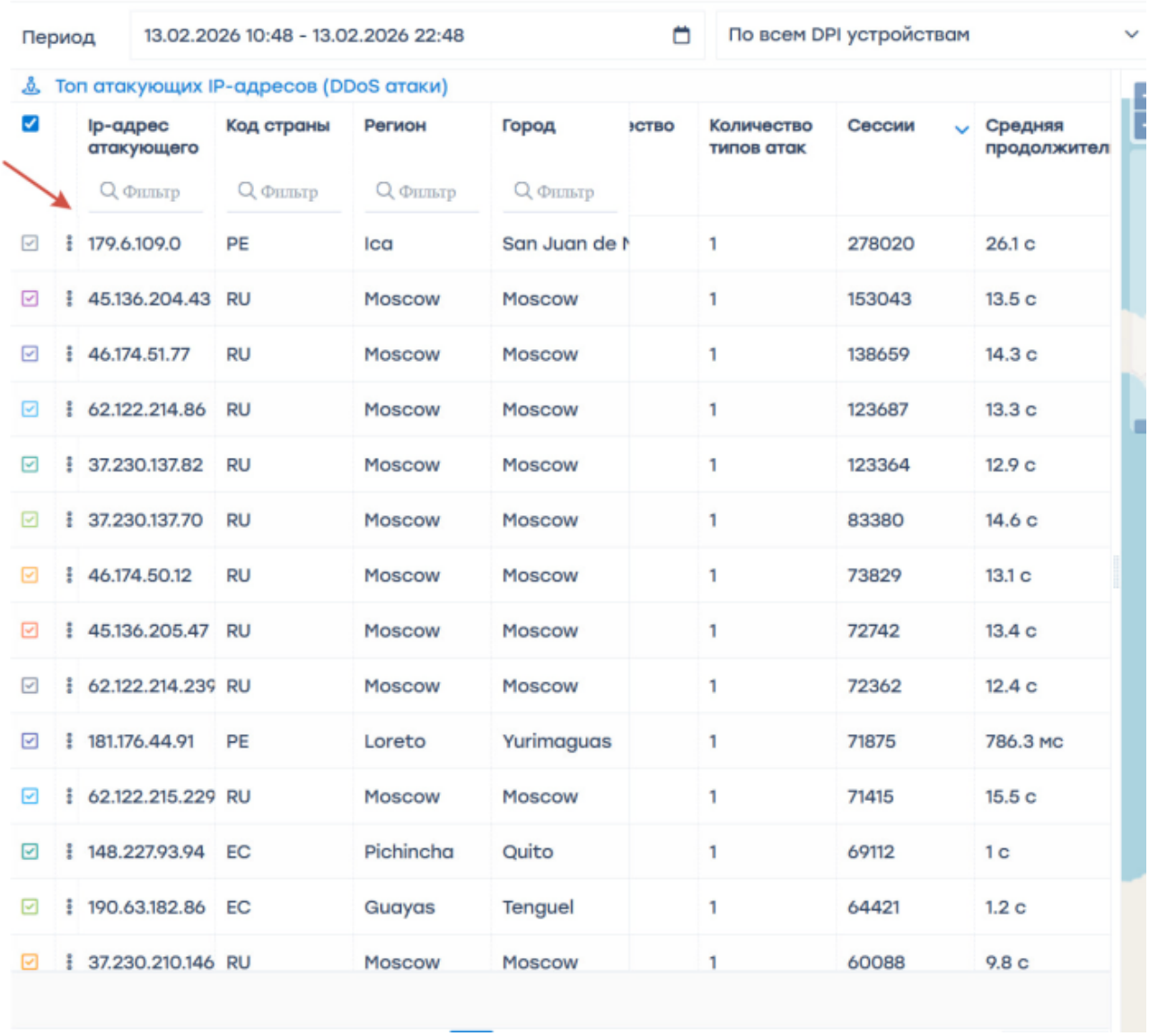

Состояние подписки: ОСТАЛОСЬ 15 ДНЕЙ

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 продолжители	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

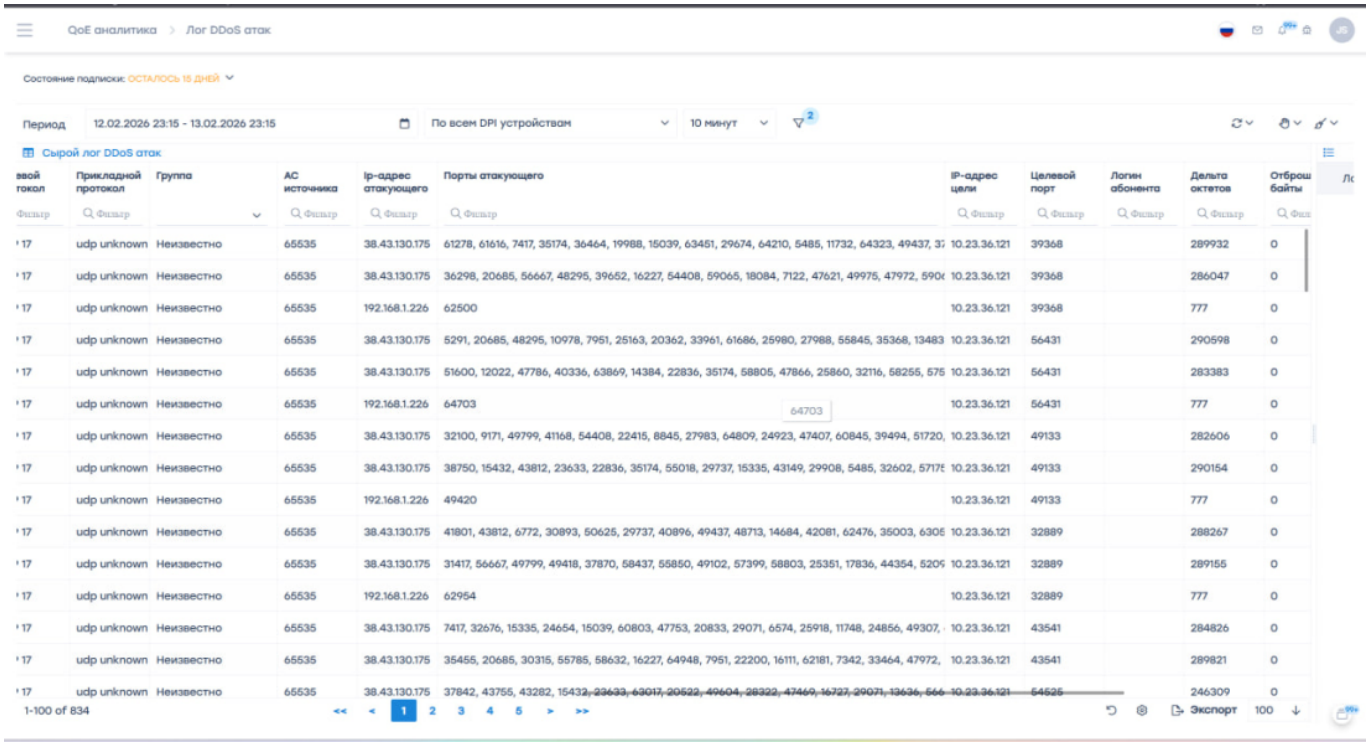
2. Посмотрите раздел "ТОП атак по протоколам"
   Также отсортируйте по количеству сессий. Запишите себе эти протоколы
3. Посмотрите раздел "ТОП атакующих IP-адресов", запишите себе несколько IP с наибольшим количеством сессий



Ip-адрес атакующего	Код страны	Регион	Город	...ство	Количество типов атак	Сессии	Средняя продолжител
Фильтр	Фильтр	Фильтр	Фильтр				
179.6.109.0	PE	Ica	San Juan de M		1	278020	26.1 с
45.136.204.43	RU	Moscow	Moscow		1	153043	13.5 с
46.174.51.77	RU	Moscow	Moscow		1	138659	14.3 с
62.122.214.86	RU	Moscow	Moscow		1	123687	13.3 с
37.230.137.82	RU	Moscow	Moscow		1	123364	12.9 с
37.230.137.70	RU	Moscow	Moscow		1	83380	14.6 с
46.174.50.12	RU	Moscow	Moscow		1	73829	13.1 с
45.136.205.47	RU	Moscow	Moscow		1	72742	13.4 с
62.122.214.239	RU	Moscow	Moscow		1	72362	12.4 с
181.176.44.91	PE	Loreto	Yurimaguas		1	71875	786.3 мс
62.122.215.229	RU	Moscow	Moscow		1	71415	15.5 с
148.227.93.94	EC	Pichincha	Quito		1	69112	1 с
190.63.182.86	EC	Guayas	Tenguel		1	64421	1.2 с
37.230.210.146	RU	Moscow	Moscow		1	60088	9.8 с

4. Посмотрите Лог атак
   С фильтром по выбранным ранее абонентам и протоколу.
   Там можно почерпнуть детали атаки и сделать доп. выводы, чтобы принимать какие-либо решения.
   Например, на скрине ниже явно видно, что идет перебор портов на одном и том же адресе по UDP протоколу. В данном случае достаточно поместить IP атакующего в отдельную АС и сделать ее drop.

Блокировка АС подробно описана в сценарии Блокировка IP с помещением в автономную систему


QoE аналитика
Лог DDoS атак
Состояние подписки: ОСТАЛОСЬ 15 ДНЕЙ
Период
12.02.2026 23:15 - 13.02.2026 23:15
По всем DPI устройствам
10 минут
Сырой лог DDoS атак
Прикладной протокол
Группа
AC источника
Ip-адрес атакующего
Порты атакующего
IP-адрес цели
Целевой порт
Логин абонента
Дельта октетов
udp unknown Неизвестно 65535 38.43.130.175 61278, 61616, 7417, 35174, 36464, 19988, 15039, 63451, 29674, 64210, 5485, 11732, 64323, 49437, 3 10.23.36.121 39368 289932 0
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
udp unknown Неизвестно 65535 192.168.1.226 62500 10.23.36.121 39368 777 0
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
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
udp unknown Неизвестно 65535 192.168.1.226 64703 10.23.36.121 56431 777 0
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
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
udp unknown Неизвестно 65535 192.168.1.226 49420 10.23.36.121 49133 777 0
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
udp unknown Неизвестно 65535 38.43.130.175 31417, 56667, 49799, 49418, 37870, 58437, 55850, 49102, 57399, 58803, 25351, 17836, 44354, 5209 10.23.36.121 32889 289155 0
udp unknown Неизвестно 65535 192.168.1.226 62954 10.23.36.121 32889 777 0
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
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
udp unknown Неизвестно 65535 38.43.130.175 37842, 43755, 43282, 15432, 23633, 63017, 20522, 49604, 28322, 47469, 16727, 29071, 13636, 566 10.23.36.121 54525 246309 0
1-100 of 834
Экспорт
100