Содержание

Поиск источников Flood в сети оператора

1. Настройка отправки статистики со СКАТ

Необходимо выставить в файле конфигурации `/etc/dpi/fastdpi.conf` следующие значения параметров:

```
netflow=12
netflow_dev=vlan200
netflow_timeout=10
netflow_rate_limit=900
netflow_full_collector=10.0.0.0:1500
netflow_passive_timeout=5
netflow_active_timeout=20
netflow_full_collector_type=2
ipfix_reserved=1
```

где:

- `netflow=12` – сбор и экспорт статистики: 8 + 4 = fullnetflow + billnetflow (accounting).
- `netflow_dev=vlan200` – где `vlan200` – название интерфейса, с которого будет отправляться статистика.
- `netflow_timeout=10` – период отправки в секундах.
- `netflow_rate_limit=900'` – ограничение потока IPFIX.
- `netflow_full_collector=10.0.0.0:1500` – адрес коллектора со статистикой – указать корректный IP QoE.
- `netflow_passive_timeout=5` – время ожидания активности в сессии после которого, если не было активности, сессия считается завершенной и происходит передача по ней информации.
- `netflow_active_timeout=20` – время, через которое сообщается информация по длинным сессиям (т.е. фактически длинные сессии разбиваются на фрагменты данной продолжительности).
- `netflow_full_collector_type=2` – экспорт IPFIX на TCP коллектор.
- `ipfix_reserved=1` – позволяет зарезервировать необходимую память для возможности включения/изменения параметров IPFIX/Netflow.

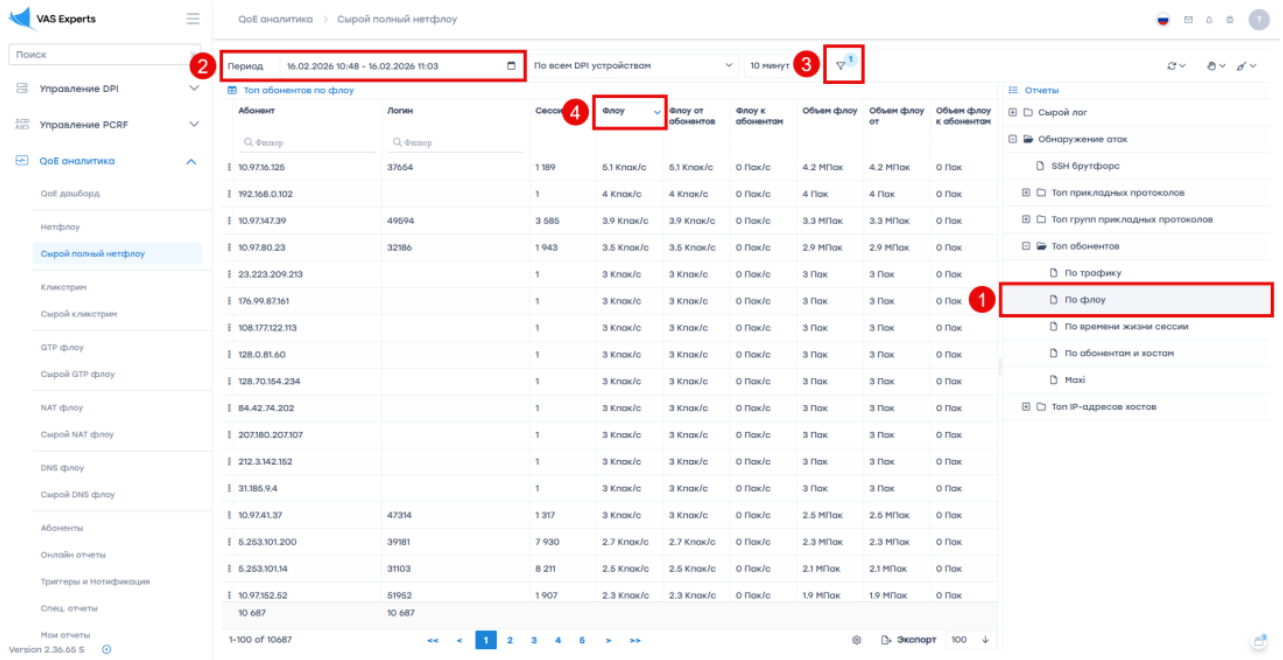
После изменения параметров потребуется рестарт сервиса:

```
service fastdpi restart
```

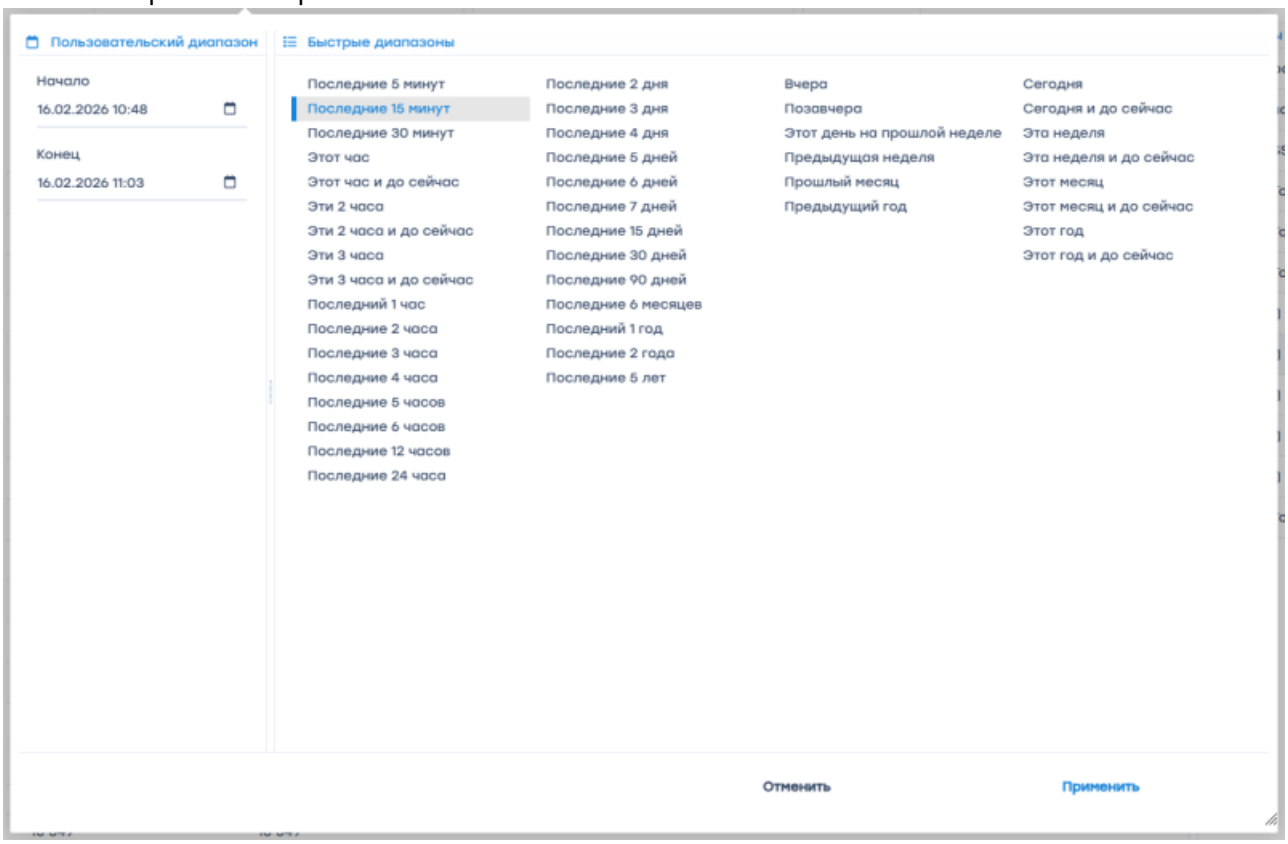
2. Поиск источника Flood (BotNet)

Поиск абонентов с высоким количеством flow в секунду

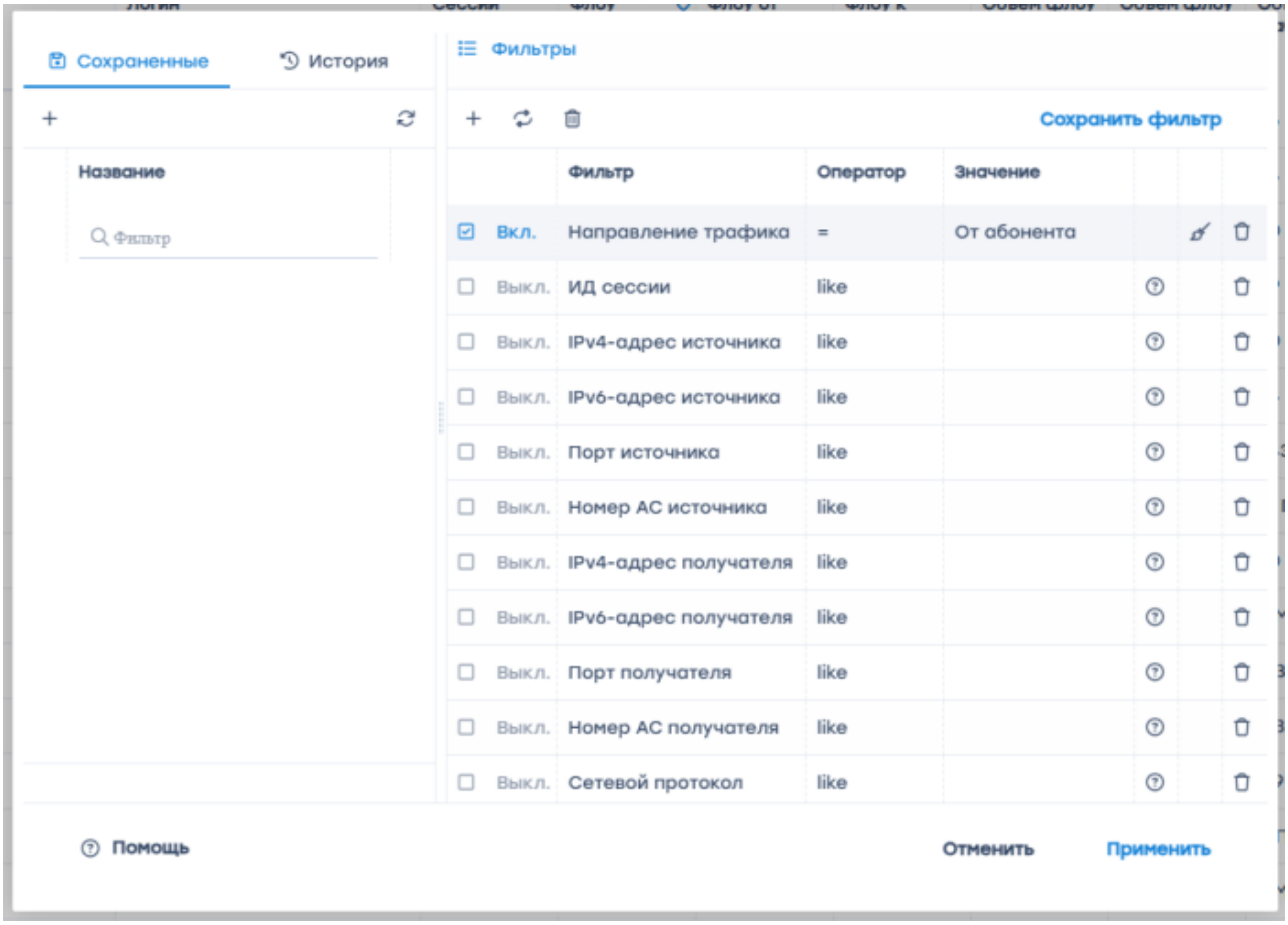
1. Откройте отчет QoE аналитика → Сырой полный нетфлоу → Обнаружение атак → Топ абонентов → По флоу:



2. Укажите временные рамки:



3. Добавьте фильтр по направлению трафика – От абонента:



4. Нажмите на колонку Flow для более удобной сортировки

   Найденные IP абонентов источников flood необходимо добавить в локальную AS (см. раздел 3.1)