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.

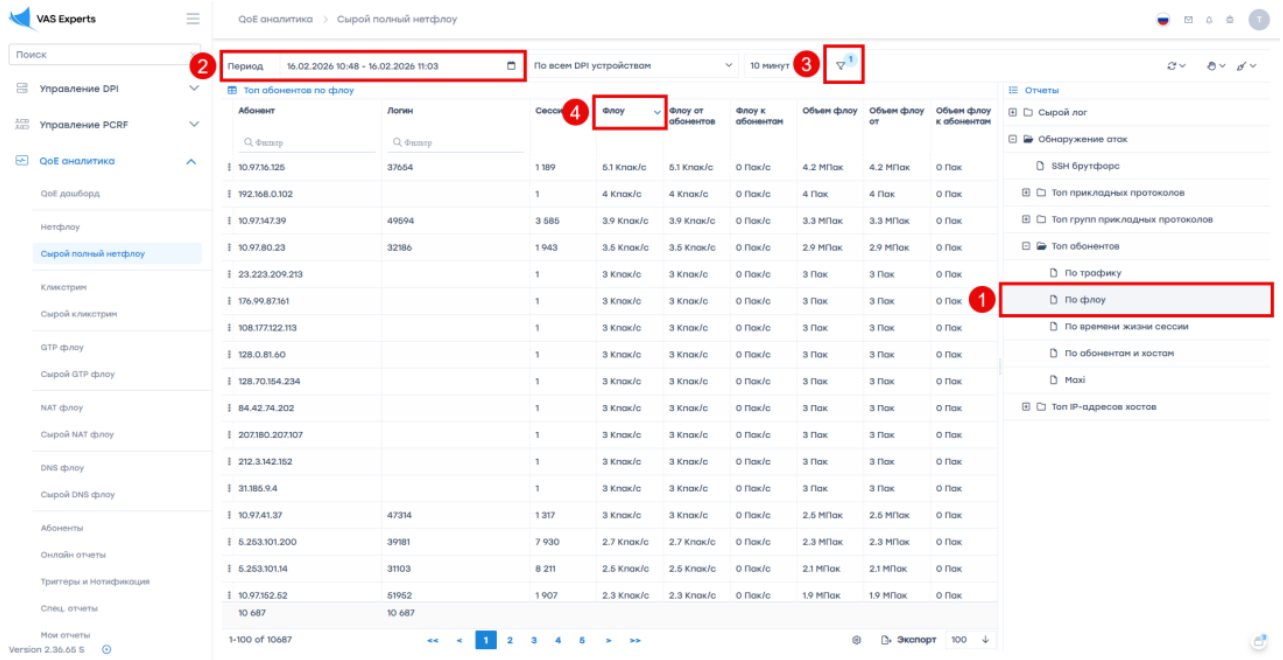
После изменения параметров потребуется рестарт сервиса:

```
service fastdpi restart
```

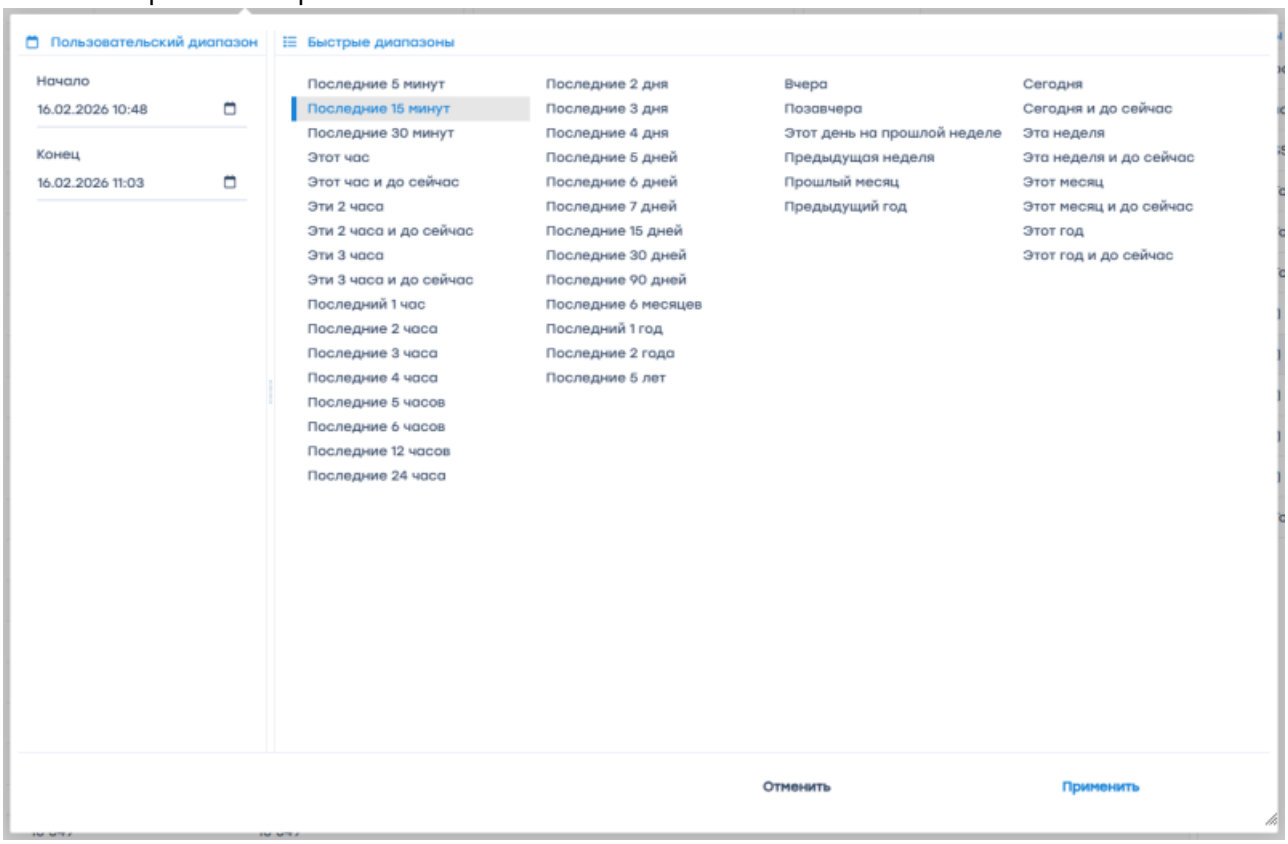
2. Поиск источника Flood (BotNet)

Поиск абонентов с высоким количеством flow в секунду

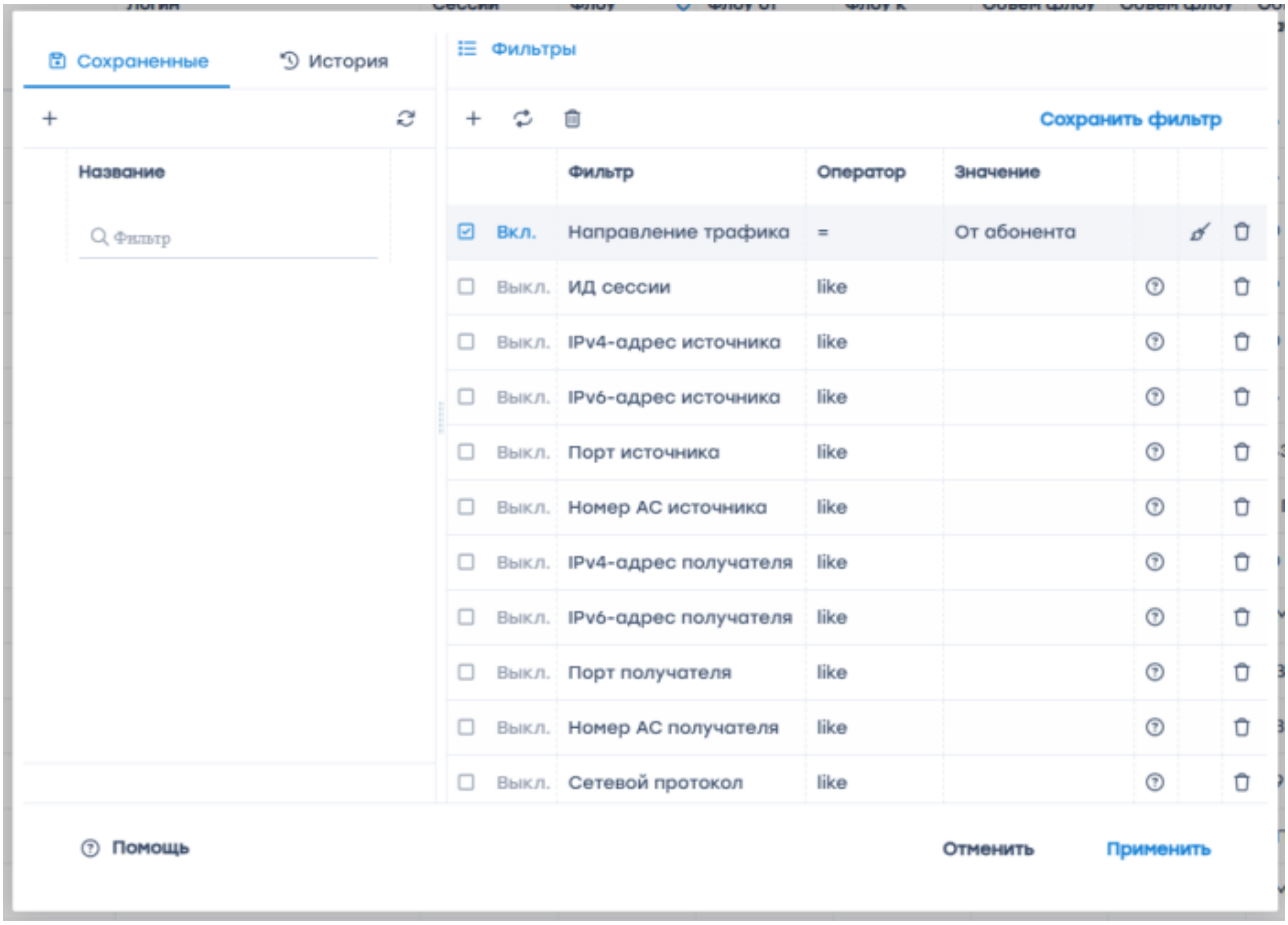
1. Откройте отчет QoE аналитика → Сырой полный нетфлоу → Обнаружение атак → Топ абонентов → По флоу:



2. Укажите временные рамки:



3. Добавьте фильтр по направлению трафика – От абонента:

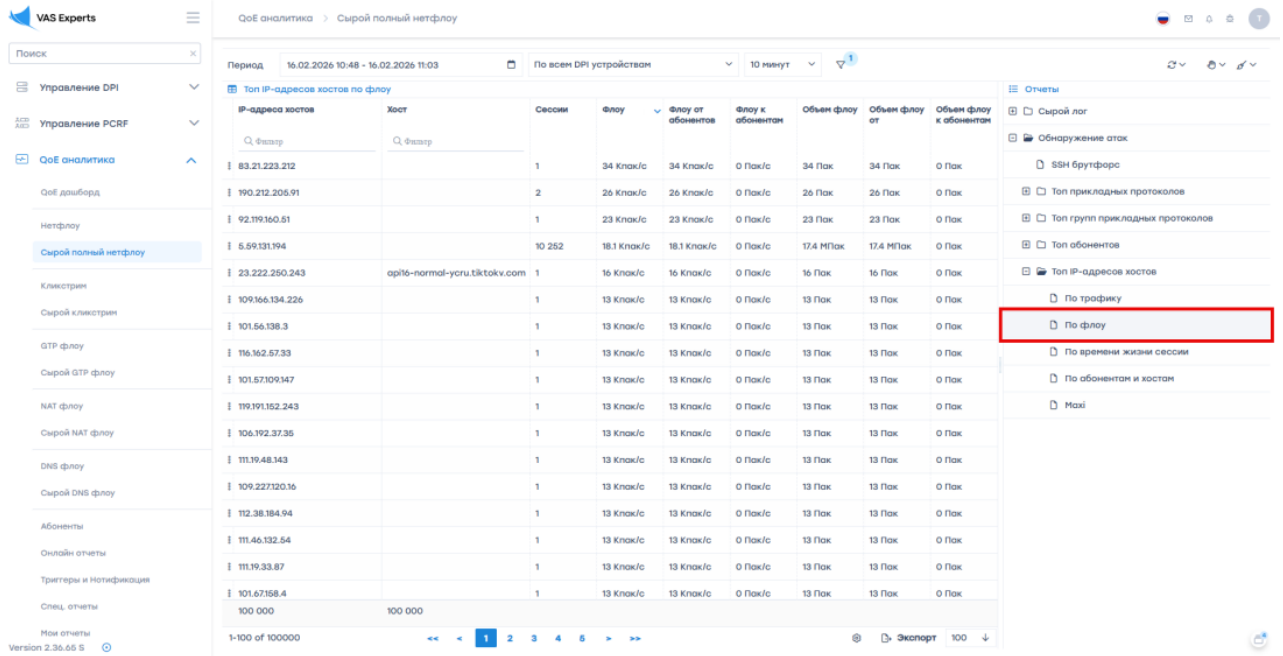


4. Нажмите на колонку Flow для более удобной сортировки

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

Поиск хостов с высоким количеством flow в секунду

1. Откройте отчет QoE аналитика → Сырой полный нетфлоу → Обнаружение атак → Топ IP-адресов хостов → 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 хостов необходимо добавить в локальную AS (см. раздел 3.1)

3. Блокировка IP с помещением в автономную систему

Создание локальной AS (пример для IPv4)

1. Создайте копию /etc/dpi/aslocal.bin:

```
cp /etc/dpi/aslocal.bin /etc/dpi/aslocal.bin.backup
```

2. Сконвертировать aslocal.bin в TXT файл утилитой bin2as

```
bin2as /etc/dpi/aslocal.bin > /etc/dpi/list.txt
```

   Либо если файл aslocal.bin отсутствует в /etc/dpi/, создайте:

```
vi /etc/dpi/list.txt
```

3. Добавить в list.txt записи вида (CIDR <пробел> номер_AS):

```
10.0.0.1/32 64525
172.16.0.0/12 64525
192.168.0.0/16 64525
```

   Где 64525 - AS которую в дальнейшем будет необходимо заблокировать

4. Сконвертировать список CIDR-ASN из TXT в BIN при помощи утилиты as2bin:

```
cat /etc/dpi/list.txt | as2bin /etc/dpi/aslocal.bin
```

5. Выполнить релоад сервиса (горячий параметр):

```
service fastdpi reload
```

Подробнее о подготовке списков aslocal

Назначение правила drop для локальной AS

1. Создайте копию файла asnum.dscp:

```
cp /etc/dpi/asnum.dscp /etc/dpi/asnum.dscp.backup
```

2. Сконвертировать asnum.dscp в TXT утилитой dscp2as:

```
dscp2as /etc/dpi/asnum.dscp > /etc/dpi/asnum.txt
```

3. Добавить в файл asnum.txt записи вида номер_AS <пробел> drop к уже существующим записям:

```
64525 drop
```

4. Сконвертировать TXT в формат утилитой as2dscp:

```
cat /etc/dpi/asnum.txt | as2dscp /etc/dpi/asnum.dscp
```

5. Выполнить релоад сервиса (горячий параметр):

```
service fastdpi reload
```

Подробнее о назначении DSCP для ASN