

Содержание

Поиск источников Flood в сети оператора	3
1. Настройка отправки статистики со СКАТ	3
2. Поиск источника Flood (BotNet)	3
Поиск абонентов с высоким количеством flow в секунду	3
Поиск хостов с высоким количеством flow в секунду	5
3. Блокировка IP с помещением в автономную систему	6
Создание локальной AS (пример для IPv4)	6
Назначение правила drop для локальной AS	6

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: $8 + 4 = \text{fullnetflow} + \text{billnetflow (accounting)}$.
- `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:

Вас Experts

QoE аналитика > Сырой полный нетфлоу

Период: 16.02.2026 10:48 - 16.02.2026 11:03

По всем DPI устройствам

10 минут

Топ абонентов по флоу

Абонент	Логин	Сессии	Флоу	Флоу от абонента	Флоу к абоненту	Объем флоу от	Объем флоу к	Объем флоу к абоненту
10.9736.125	37654	1 189	6.1 Кбайт/с	6.1 Кбайт/с	0 Паков	4.2 МПаков	4.2 МПаков	0 Паков
192.168.0.102		1	4 Кбайт/с	4 Кбайт/с	0 Паков	4 Паков	4 Паков	0 Паков
10.97347.39	49694	3 585	3.9 Кбайт/с	3.9 Кбайт/с	0 Паков	3.3 МПаков	3.3 МПаков	0 Паков
10.97.80.23	32186	1 943	3.5 Кбайт/с	3.5 Кбайт/с	0 Паков	2.9 МПаков	2.9 МПаков	0 Паков
23.223.209.213		1	3 Кбайт/с	3 Кбайт/с	0 Паков	3 Паков	3 Паков	0 Паков
176.99.87.161		1	3 Кбайт/с	3 Кбайт/с	0 Паков	3 Паков	3 Паков	0 Паков
108.177.122.113		1	3 Кбайт/с	3 Кбайт/с	0 Паков	3 Паков	3 Паков	0 Паков
128.0.81.60		1	3 Кбайт/с	3 Кбайт/с	0 Паков	3 Паков	3 Паков	0 Паков
128.70.164.234		1	3 Кбайт/с	3 Кбайт/с	0 Паков	3 Паков	3 Паков	0 Паков
84.42.74.202		1	3 Кбайт/с	3 Кбайт/с	0 Паков	3 Паков	3 Паков	0 Паков
207180.207307		1	3 Кбайт/с	3 Кбайт/с	0 Паков	3 Паков	3 Паков	0 Паков
212.3.142.162		1	3 Кбайт/с	3 Кбайт/с	0 Паков	3 Паков	3 Паков	0 Паков
31.185.9.4		1	3 Кбайт/с	3 Кбайт/с	0 Паков	3 Паков	3 Паков	0 Паков
10.9741.37	47314	1 317	3 Кбайт/с	3 Кбайт/с	0 Паков	2.5 МПаков	2.5 МПаков	0 Паков
6.253.101.200	39181	7 930	2.7 Кбайт/с	2.7 Кбайт/с	0 Паков	2.3 МПаков	2.3 МПаков	0 Паков
6.253.101.14	31103	8 211	2.6 Кбайт/с	2.6 Кбайт/с	0 Паков	2.1 МПаков	2.1 МПаков	0 Паков
10.97152.52	51952	1 907	2.3 Кбайт/с	2.3 Кбайт/с	0 Паков	1.9 МПаков	1.9 МПаков	0 Паков
10.687	10 687							

1-100 of 10687

Быстрые диапазоны

Пользовательский диапазон

Начало: 16.02.2026 10:48

Конец: 16.02.2026 11:03

Быстрые диапазоны:

- Последние 5 минут
- Последние 15 минут
- Последние 30 минут
- Этот час
- Этот час и до сейчас
- Эти 2 часа
- Эти 2 часа и до сейчас
- Эти 3 часа
- Эти 3 часа и до сейчас
- Последний 1 час
- Последние 2 часа
- Последние 3 часа
- Последние 4 часа
- Последние 5 часов
- Последние 6 часов
- Последние 12 часов
- Последние 24 часа
- Последние 2 дня
- Последние 3 дня
- Последние 4 дня
- Последние 5 дней
- Последние 6 дней
- Последние 7 дней
- Последние 15 дней
- Последние 30 дней
- Последние 90 дней
- Последние 6 месяцев
- Последний 1 год
- Последние 2 года
- Последние 5 лет
- Вчера
- Позавчера
- Этот день на прошлой неделе
- Предыдущая неделя
- Прошлый месяц
- Предыдущий год
- Сегодня
- Сегодня и до сейчас
- Эта неделя
- Эта неделя и до сейчас
- Этот месяц
- Этот месяц и до сейчас
- Этот год
- Этот год и до сейчас

Отменить Применить

2. Укажите временные рамки:

Пользовательский диапазон

Быстрые диапазоны

Начало: 16.02.2026 10:48

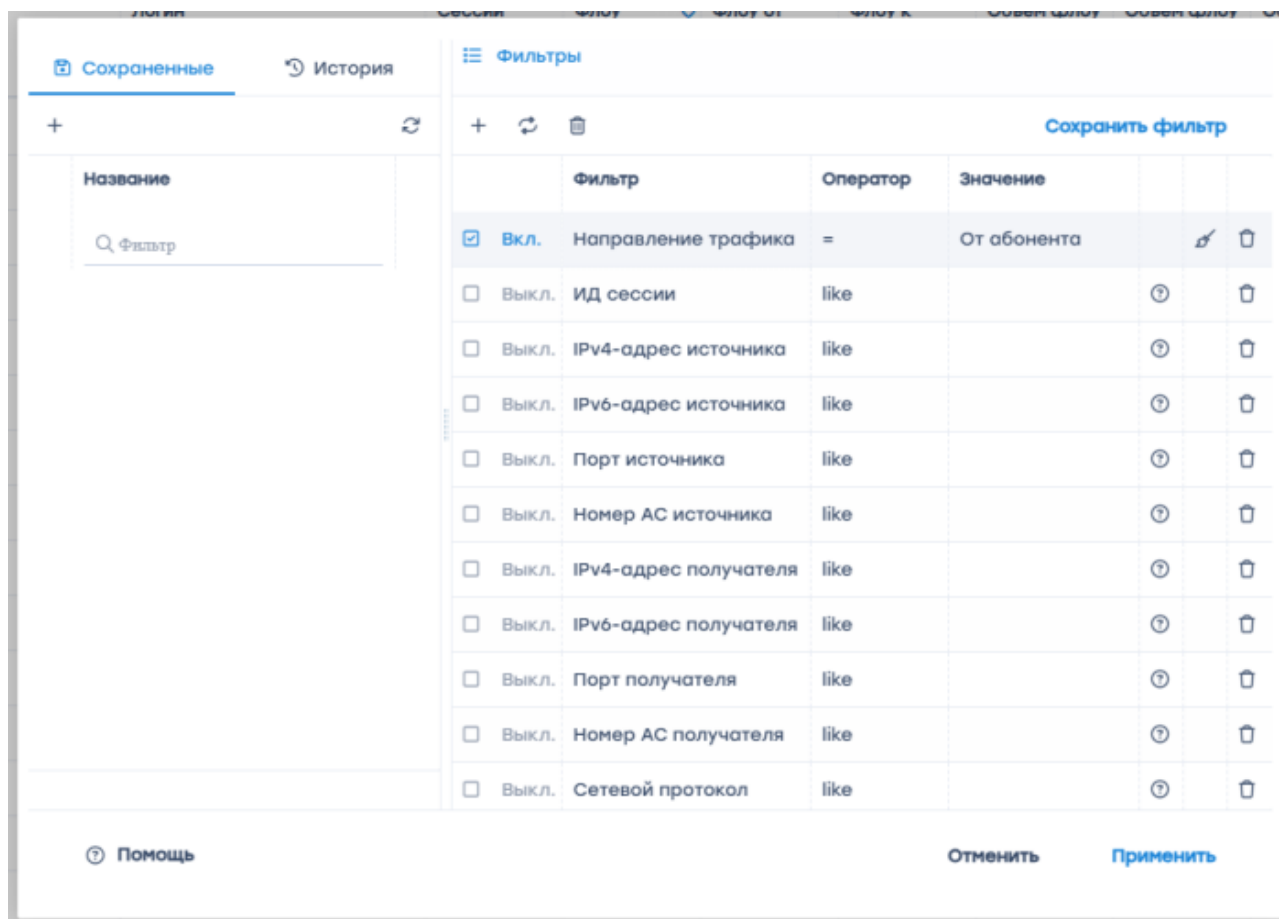
Конец: 16.02.2026 11:03

Быстрые диапазоны:

- Последние 5 минут
- Последние 15 минут
- Последние 30 минут
- Этот час
- Этот час и до сейчас
- Эти 2 часа
- Эти 2 часа и до сейчас
- Эти 3 часа
- Эти 3 часа и до сейчас
- Последний 1 час
- Последние 2 часа
- Последние 3 часа
- Последние 4 часа
- Последние 5 часов
- Последние 6 часов
- Последние 12 часов
- Последние 24 часа
- Последние 2 дня
- Последние 3 дня
- Последние 4 дня
- Последние 5 дней
- Последние 6 дней
- Последние 7 дней
- Последние 15 дней
- Последние 30 дней
- Последние 90 дней
- Последние 6 месяцев
- Последний 1 год
- Последние 2 года
- Последние 5 лет
- Вчера
- Позавчера
- Этот день на прошлой неделе
- Предыдущая неделя
- Прошлый месяц
- Предыдущий год
- Сегодня
- Сегодня и до сейчас
- Эта неделя
- Эта неделя и до сейчас
- Этот месяц
- Этот месяц и до сейчас
- Этот год
- Этот год и до сейчас

Отменить Применить

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 нетфлю → Обнаружение атак → Топ IP-адресов хостов → По флоу:

QoE аналитика > Сырой полный нетфлю

Период: 16.02.2026 10:48 - 16.02.2026 11:03 | По всем DPI устройствам | 10 минут

IP-адреса хостов	Хост	Сессии	Флоу	Флоу от абонентов	Флоу к абонентам	Объем флоу от	Объем флоу к абонентам
83.21.223.212		1	34 Кбайт/с	34 Кбайт/с	0 Паков/с	34 Паков	0 Паков
190.212.205.91		2	26 Кбайт/с	26 Кбайт/с	0 Паков/с	26 Паков	0 Паков
92.199.160.51		1	23 Кбайт/с	23 Кбайт/с	0 Паков/с	23 Паков	0 Паков
5.59.131.194		10 252	18.1 Кбайт/с	18.1 Кбайт/с	0 Паков/с	17.4 МПаков	0 Паков
23.222.250.243	api6-normal-ycru.tiktokv.com	1	16 Кбайт/с	16 Кбайт/с	0 Паков/с	16 Паков	0 Паков
109.166.134.226		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
101.56.138.3		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
116.162.57.33		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
101.57.109.147		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
119.191.152.243		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
106.192.37.35		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
111.19.48.143		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
109.227.120.16		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
112.38.184.94		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
111.46.132.54		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
111.19.33.87		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
101.67.158.4		1	13 Кбайт/с	13 Кбайт/с	0 Паков/с	13 Паков	0 Паков
100 000	100 000						

1-100 of 100000

Варианты отчета: Сырой лог, Обнаружение атак, SBN брутфорс, Топ прикладных протоколов, Топ групп прикладных протоколов, Топ абонентов, Топ IP-адресов хостов, По трафику, **По флоу**, По времени жизни сессии, По абонентам и хостам, Max

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](#)