

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 нетфлору → Обнаружение атак → Топ абонентов → По флору:

Вас Experts

QoS аналитика > Сырой полный нетфлю

Поиск

Период: 16.02.2026 10:48 - 16.02.2026 11:03

По всем DPI устройствам

10 минут

Управление DPI

Управление PCRF

QoS аналитика

QoS дашборд

Нетфлю

Сырой полный нетфлю

Клиентские

Сырой клиентские

GTP флюу

Сырой GTP флюу

NAT флюу

Сырой NAT флюу

DNS флюу

Сырой DNS флюу

Абоненты

Онлайн отчеты

Триггеры и нотификации

Спец. отчеты

Мои отчеты

Version 2.36.66 S

Абонент	Логин	Сессии	Флюу	Флюу от абонентов	Флюу к абонентам	Объем флюу	Объем флюу от	Объем флюу к абонентам
192.168.0.102		1	4 Кбайт/с	4 Кбайт/с	0 Пак/с	4 Пак	4 Пак	0 Пак
10.97347.39	49694	3 585	3.9 Кбайт/с	3.9 Кбайт/с	0 Пак/с	3.3 МПак	3.3 МПак	0 Пак
10.97.80.23	32186	1 943	3.5 Кбайт/с	3.5 Кбайт/с	0 Пак/с	2.9 МПак	2.9 МПак	0 Пак
23.223.209.213		1	3 Кбайт/с	3 Кбайт/с	0 Пак/с	3 Пак	3 Пак	0 Пак
176.99.87.161		1	3 Кбайт/с	3 Кбайт/с	0 Пак/с	3 Пак	3 Пак	0 Пак
108.177.122.113		1	3 Кбайт/с	3 Кбайт/с	0 Пак/с	3 Пак	3 Пак	0 Пак
128.0.81.60		1	3 Кбайт/с	3 Кбайт/с	0 Пак/с	3 Пак	3 Пак	0 Пак
128.70.164.234		1	3 Кбайт/с	3 Кбайт/с	0 Пак/с	3 Пак	3 Пак	0 Пак
84.42.74.202		1	3 Кбайт/с	3 Кбайт/с	0 Пак/с	3 Пак	3 Пак	0 Пак
207180.207107		1	3 Кбайт/с	3 Кбайт/с	0 Пак/с	3 Пак	3 Пак	0 Пак
212.3.142.152		1	3 Кбайт/с	3 Кбайт/с	0 Пак/с	3 Пак	3 Пак	0 Пак
31385.94		1	3 Кбайт/с	3 Кбайт/с	0 Пак/с	3 Пак	3 Пак	0 Пак
10.9741.37	47314	1 317	3 Кбайт/с	3 Кбайт/с	0 Пак/с	2.5 МПак	2.5 МПак	0 Пак
5.253.101.200	39181	7 930	2.7 Кбайт/с	2.7 Кбайт/с	0 Пак/с	2.3 МПак	2.3 МПак	0 Пак
5.253.101.14	31103	8 211	2.5 Кбайт/с	2.5 Кбайт/с	0 Пак/с	2.1 МПак	2.1 МПак	0 Пак
10.97152.52	51952	1 907	2.3 Кбайт/с	2.3 Кбайт/с	0 Пак/с	1.9 МПак	1.9 МПак	0 Пак
10.687	10 687							

1-100 of 10687

Экспорт 100 ↓

Отчеты

- Сырой лог
- Обнаружение атак
- SSH брутфорс
- Топ прикладных протоколов
- Топ групп прикладных протоколов
- Топ абонентов
- По трафику
- По флюу**
- По времени жизни сессии
- По абонентам и хостам
- Max
- Топ IP-адресов хостов

2. Укажите временные рамки:

Пользовательский диапазон

Быстрые диапазоны

Начало

16.02.2026 10:48

Конец

16.02.2026 11:03

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 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

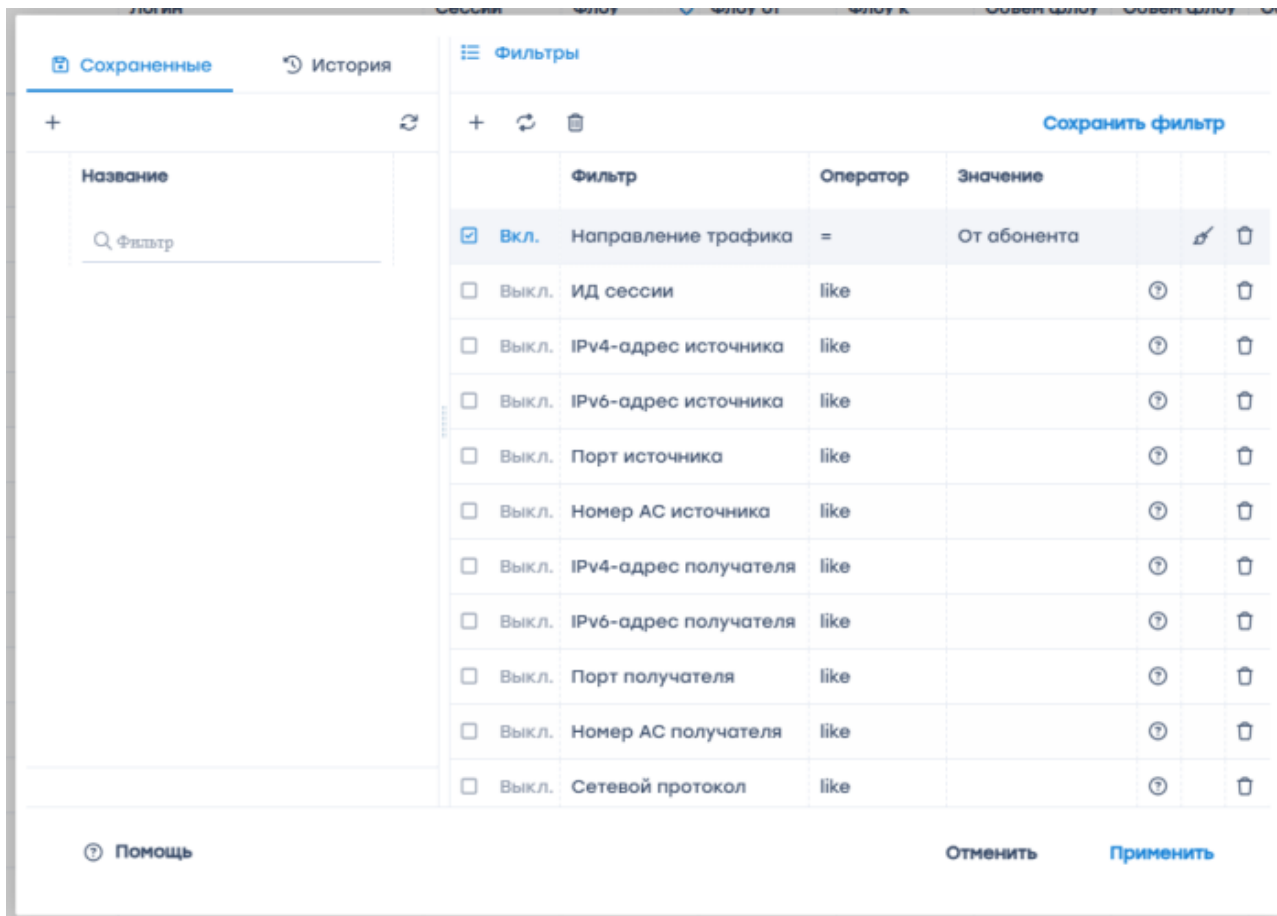
Этот год

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:

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 Кпак/с	34 Кпак/с	0 Пак/с	34 Пак	34 Пак
190.212.205.91		2	26 Кпак/с	26 Кпак/с	0 Пак/с	26 Пак	26 Пак
92.199.160.51		1	23 Кпак/с	23 Кпак/с	0 Пак/с	23 Пак	23 Пак
5.59.131.194		10 252	18.1 Кпак/с	18.1 Кпак/с	0 Пак/с	17.4 МПак	17.4 МПак
23.222.250.243	ap16-normal-ycru.tktokv.com	1	16 Кпак/с	16 Кпак/с	0 Пак/с	16 Пак	16 Пак
109.166.134.226		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
101.56.138.3		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
116.162.57.33		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
101.57109.147		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
119.191.152.243		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
106.192.37.35		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
111.19.48.143		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
109.227120.16		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
112.38.184.94		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
111.46.132.54		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
111.19.33.87		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
101.67158.4		1	13 Кпак/с	13 Кпак/с	0 Пак/с	13 Пак	13 Пак
100 000						100 000	100 000

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](#)