

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 = 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:

Фильтр	Оператор	Значение
Вкл. Направление трафика	=	От абонента
Выкл. ИД сессии	like	
Выкл. IPv4-адрес источника	like	
Выкл. IPv6-адрес источника	like	
Выкл. Порт источника	like	
Выкл. Номер АС источника	like	
Выкл. IPv4-адрес получателя	like	
Выкл. IPv6-адрес получателя	like	
Выкл. Порт получателя	like	
Выкл. Номер АС получателя	like	
Выкл. Сетевой протокол	like	

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:

IP-адреса хостов	Хост	Сессии	Флоу	Флоу от абонентов	Флоу к абонентам	Объем флоу	Объем флоу от	Объем флоу к абонентам
83.21.223.212		1	34 Клак/с	34 Клак/с	0 Пак/с	34 Пак	34 Пак	0 Пак
190.212.206.91		2	26 Клак/с	26 Клак/с	0 Пак/с	26 Пак	26 Пак	0 Пак
92.119.160.51		1	23 Клак/с	23 Клак/с	0 Пак/с	23 Пак	23 Пак	0 Пак
5.59.131.194		10 252	18.1 Клак/с	18.1 Клак/с	0 Пак/с	17.4 МПак	17.4 МПак	0 Пак
23.222.250.243	orpt-normal-ycru.tiktokv.com	1	16 Клак/с	16 Клак/с	0 Пак/с	16 Пак	16 Пак	0 Пак
109.166.134.226		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
101.56.138.3		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
116.162.57.33		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
101.57.109.147		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
119.191.152.243		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
106.192.37.38		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
111.19.48.143		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
109.227.120.16		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
112.38.184.94		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
111.46.132.54		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
111.19.33.87		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
101.67.158.4		1	13 Клак/с	13 Клак/с	0 Пак/с	13 Пак	13 Пак	0 Пак
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](#)