# **Table of Contents**

Расширенные возможности	3
Построение графиков	3
Построение отчетов	4
Построение отчетов по IP	5

# Расширенные возможности

NFSEN дополнен возможностями построения графиков и отчетов с учетом имен автономных систем и названий протоколов.

- 1. Построение графиков
- 2. Построение отчетов
- 3. Построение отчетов по ІР

## Построение графиков

Перед построением графика убедитесь, что накопилась статистика хотя бы за одни сутки.

Для вашего удобства мы создали скрипты, которые автоматически вычисляют топ N протоколов (или направлений - автономных систем) и создают профиль, в котором каждый из них выделен своим цветом.

Запуск скрипта для построения профиля с топом протоколов

```
/usr/local/nfsen/bin/create_top_protocols --consumers 8 --divide-up-down --
profile-name top_8_protocols
```

где consumers 8 - число отображаемых на графике протоколов (максимум 10) divide-up-down - означает, что входящий и исходящий трафик будут отображаться на графике раздельно относительно нулевой оси profile-name top\_8\_protocols - имя создаваемого профиля<sup>1)</sup>

В результате работы скрипта будет создан профиль top\_8\_protocols, в котором в графиках топ 8 протоколов по объему будут выделены разным цветом:

#### ×

Протоколы, не вошедшие в топ, на графике будут объединены в others под общим цветом На данном профиле удобно строить отчеты по протоколам, как указано в разделе Построение отчетов

Кроме того на графиках можно оставить только интересующие нас протоколы, убрав галочки напротив "лишних" протоколов в разделе Statistics (расположенном под графиками). Пример: на графике оставлены только торренты

#### ×

Аналогично, для построения профиля с топом направлений запускаем скрипт:

/usr/local/nfsen/bin/create\_top\_directions --consumers 10 --divide-up-down -profile-name top\_10\_directions

В результате будет создан профиль top\_10\_directions, в котором можно, например, наглядно наблюдать разницу в объемах трафика на сервисы GOOGLE и BKOHTAKTE

## Построение отчетов

Выберите профиль live (профиль выбирается в правом верхнем углу) или, если вы ранее создали отдельный профиль с топом направлений, как указано в разделе Построение графиков, то выберите его.

Для создания отчета по автономным системам нажмите закладку Details в самой верхней строке и выберите на графике требуемый период (Time Window) или передвиньте ползунок на исследуемый момент времени (Single Timeslot)

Теперь в разделе Options (под Netflow Processing) выберите тип желаемого отчета:

#### Netflow Processing

Source:	Filter:		<b>Options:</b>	
protocols		*	ws 💿 Stat TopN	
directions			Top:	10 🔻
			Stat:	Any AS Name  v order by bytes  v
		-	Limit:	■ Packets ▼ > ▼ 0 - ▼
All Sources	and none -		Output:	/ IPv6 long
				Clear Form process

где Stat TopN - список из топовых направлений

Тор: 10 - количество элементов в топе

Stat: Any AS Name/SRC AS Name или DST AS Name - учитывать весь трафик или только в одном из направлений

Order By: bytes - топ считать по объему данных

и нажмите кнопку Process.

Для профиля live необходимо также отметить только Source: directions

#### В результате будет подготовлен отчет по топовым направлениям передачи данных

#### **Processing Result**

Top 10 AS Name ordered by bytes:											
Date first seen	Duration Prot	AS Name	Flo	ws (%)	Packet	ts(%)	Byt	es(%)	pps	bps	bpp
2013-11-13 08:49:00.583	300.221 any	202002	10(	0.0)	16.0 M( 5	50.6)	12.9 G(	50.3)	53368	342.8 M	802
2013-11-13 08:49:00.583	300.221 any	VKONTAKTE-SPB-AS	10(	0.0)	1.4 M(	4.5)	1.5 G(	5.7)	4799	39.1 M	1019
2013-11-13 08:49:00.583	300.221 any	RETN-AS	10(	0.0)	797176(	2.5)	824.6 M(	3.2)	2655	22.0 M	1034
2013-11-13 08:49:00.583	300.220 any	GOOGLE	10(	0.0)	504978 (	1.6)	459.0 M(	1.8)	1682	12.2 M	908
2013-11-13 08:49:00.583	300.221 any	RUTUBE-AS	10(	0.0)	302192(	1.0)	334.4 M(	1.3)	1006	8.9 M	1106
2013-11-13 08:49:00.583	300.221 any	UKRTELNET	10(	0.0)	309298 (	1.0)	276.0 M(	1.1)	1030	7.4 M	892
2013-11-13 08:49:00.583	300.221 any	NCNET-AS	10(	0.0)	267044(	0.8)	268.3 M(	1.0)	889	7.1 M	1004
2013-11-13 08:49:00.583	300.220 any	SIBIRTELECOM-AS	10(	0.0)	309878 (	1.0)	238.0 M(	0.9)	1032	6.3 M	768
2013-11-13 08:49:00.583	300.221 any	CORBINA-AS	10(	0.0)	350953 (	1.1)	230.6 M(	0.9)	1168	6.1 M	657
2013-11-13 08:50:00.626	180.136 any	TVIGO	6(	0.0)	202119(	0.6)	211.6 M(	0.8)	1122	9.4 M	1046

Summary: total flows: 43750, total bytes: 25.6 G, total packets: 31.7 M, avg bps: 681.2 M, avg pps: 105482, avg bpp: 807

Аналогично при выборе Source: protocols или отдельного профиля с топом протоколов можно стоить отчеты по протоколам в обеих или одном из направлений DPI Protocol/IN DPI Protocol/OUT DPI Protocol

×

#### **Options:**

C List Flow	ws 🔘 Stat TopN	
Top:	10 🔻	
Stat:	OUT DPI Protocol 👻 order by	oytes 🔻
Limit:	Packets  V >  V 0	- •
Output:	/ IPv6 long	

Clear Form process

#### **Processing Result**

Top 10 OUT DPI Proto ord	iered by bytes:							
Date first seen	Duration Proto	OUT DPI Proto	Flows (	<li>Packets (%)</li>	Bytes (%)	pps	bps	bpp
2013-11-13 08:44:00.355	300.225 any	MPEG	5( 0.	0) 1.8 M( 10.8)	2.7 G( 20.4)	5924	73.0 M	1540
2013-11-13 08:44:00.356	300.225 any	http	5( 0.	0) 1.3 M( 7.9)	1.8 G( 13.3)	4316	47.5 M	1375
2013-11-13 08:44:00.355	300.225 any	Bittorrent	5( 0.	0) 3.1 M(18.8)	1.4 G( 10.7)	10330	38.1 M	461
2013-11-13 08:44:00.355	300.225 any	Flash	5( 0.	0) 465697( 2.8)	702.9 M( 5.2)	1551	18.7 M	1509
2013-11-13 08:44:00.356	300.225 any	https	5( 0.	0) 203621( 1.2)	190.7 M( 1.4)	678	5.1 M	936
2013-11-13 08:44:00.355	300.225 any	UDP Unknown	5( 0.	0) 511952( 3.1)	150.9 M( 1.1)	1705	4.0 M	294
2013-11-13 08:44:00.355	300.225 any	TCP Unknown	5( 0.	0) 682412( 4.1)	120.2 M( 0.9)	2273	3.2 M	176
2013-11-13 08:44:00.355	300.225 any	Skype	5( 0.	0) 133930( 0.8)	55.3 M( 0.4)	446	1.5 M	412
2013-11-13 08:44:00.355	300.225 any	H323	5( 0.	0) 88163( 0.5)	32.4 M( 0.2)	293	862254	367
2013-11-13 08:44:00.355	300.225 any	RTP	5( 0.	0) 65129( 0.4)	27.6 M( 0.2)	216	736441	424

Summary: total flows: 15047, total bytes: 13.4 G, total packets: 16.5 M, avg bps: 357.3 M, avg pps: 54823, avg bpp: 814

### Построение отчетов по IP

1. Добавить новый приемник данных в конфигурацию nfsen

```
vi /usr/local/nfsen/etc/nfsen.conf
%sources = (
'protocols' => { 'port' => '9997', 'col' => '#00ff00', 'type' => 'netflow'
},
'directions' => { 'port' => '9998', 'col' => '#ffff00', 'type' => 'netflow'
},
'full' => { 'port' => '9999', 'col' => '#114422', 'type' => 'netflow' }
);
```

2. активировать изменения в конфигурации

/usr/local/nfsen/bin/nfsen reconfig

3. разрешить прием udp на порт 9999 в iptables

```
vi /etc/sysconfig/iptables
-A INPUT -m state --state NEW -m udp -p udp --dport 9999 -j ACCEPT
service iptables restart
```

4. Активировать на dpi отправку полного netflow на созданный коллектор (в дополнении к коллекторам протоколов и направлений)

vi /etc/dpi/fastdpi.conf

```
netflow=11
netflow_full_collector=127.0.0.1:9999
netflow_passive_timeout=20
netflow_active_timeout=60
service fastdpi restart
```

nfsen не лучший инструмент для исследования полного netflow но позволяет строить простые отчеты (раздел на страничке Netflow Processing, например, top по ip)

В полном netflow по умолчанию передается оригинальный номер порта, поэтому отчет по протоколам не работает. Чтобы активировать кодирование в номере порта информации о протоколе нужно активировать настройку netflow\_full\_port\_swap=1

1)

профиль выбирается в правом верхнем углу экрана NFSEN, если не удается выбрать только что созданный профиль выберите закладку Stat в верхней строке