Traffic Flow

Получете пълна представа за трафика във вашата мрежа

MikroTik Net Camp 2016

Цигов Чарк

Петър Димитров

За мен:

- Име: Петър Димитров
- Опит в областта на компютърните мрежи: от 2002 г.
- Опит с MikroTik: от 2005 г.
- MikroTik Trainer: от 2013 г.
- Предлагани MikroTik обучения:

MTCNA, MTCWE, MTCRE, MTCTCE, MTCUME, MTCINE

Traffic Flow

- Това е система, проследяваща "потоци" от пакети, преминаващи през рутера, осигуряваща статистическа информация за различните потоци
- Полезен изтрумент както за наблюдение и статистика в мрежата, така и за диагностика на проблеми и анализ на цялостното състояние на мрежата

Traffic Flow

- Информационен "поток" са всички пакети, които имат еднакви атрибути:
  - Source address
  - Destination address
  - Source port
  - Destination port
  - Протокол
  - Други

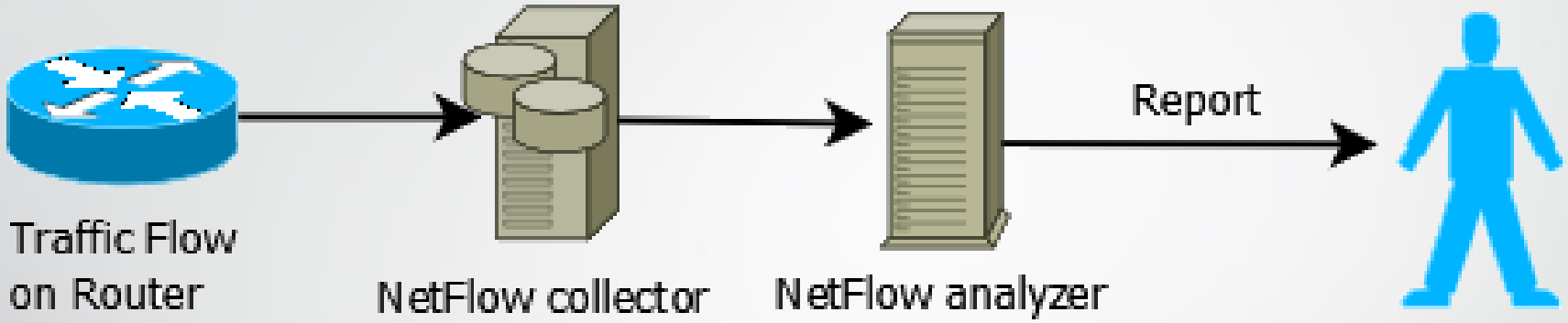
Traffic Flow

- С помощта на Traffic Flow можете да
  - Установявате наличието на неоторизиран трафик/мрежови атаки
  - Анализирате използваните от различните приложения ресурси/планирате своевременно и адекватно нужните техника и услуги
  - Наблюдавате ефекта от пускане на нови приложения, услуги или преконфигуриране на мрежата

Traffic Flow

- MikroTik Traffic-Flow е съвместим със Cisco NetFlow, поддържат се NetFlow формати версия 1, 5 и 9
- Traffic-Flow се случва в края на вериги input, output и forward, т.е. няма да бъде анализиран трафик, който се филтрира или не може да се маршрутизира
- Информацията от Traffic-Flow обикновено се събира и анализира с външни средства

NetFlow collector/analyzer



- Съществуват множество платени и безплатни продукти, работещи като NetFlow Collector и/или NetFlow Analyzer
- Ще разгледаме ntopng (http://www.ntop.org/)

Инсталация на ntopng

- ntopng може да се инсталира на различни платформи (linux, windows), ще разгледаме примерна инсталация на debian

- За да инстралираме ntopng:

```
wget http://apt.ntop.org/jessie/all/apt-ntop.deb
dpkg -i apt-ntop.deb
apt-get update
apt-get install nprobe ntopng ntopng-data
```

Стартиране на ntopng

- Стартираме nprobe като collector

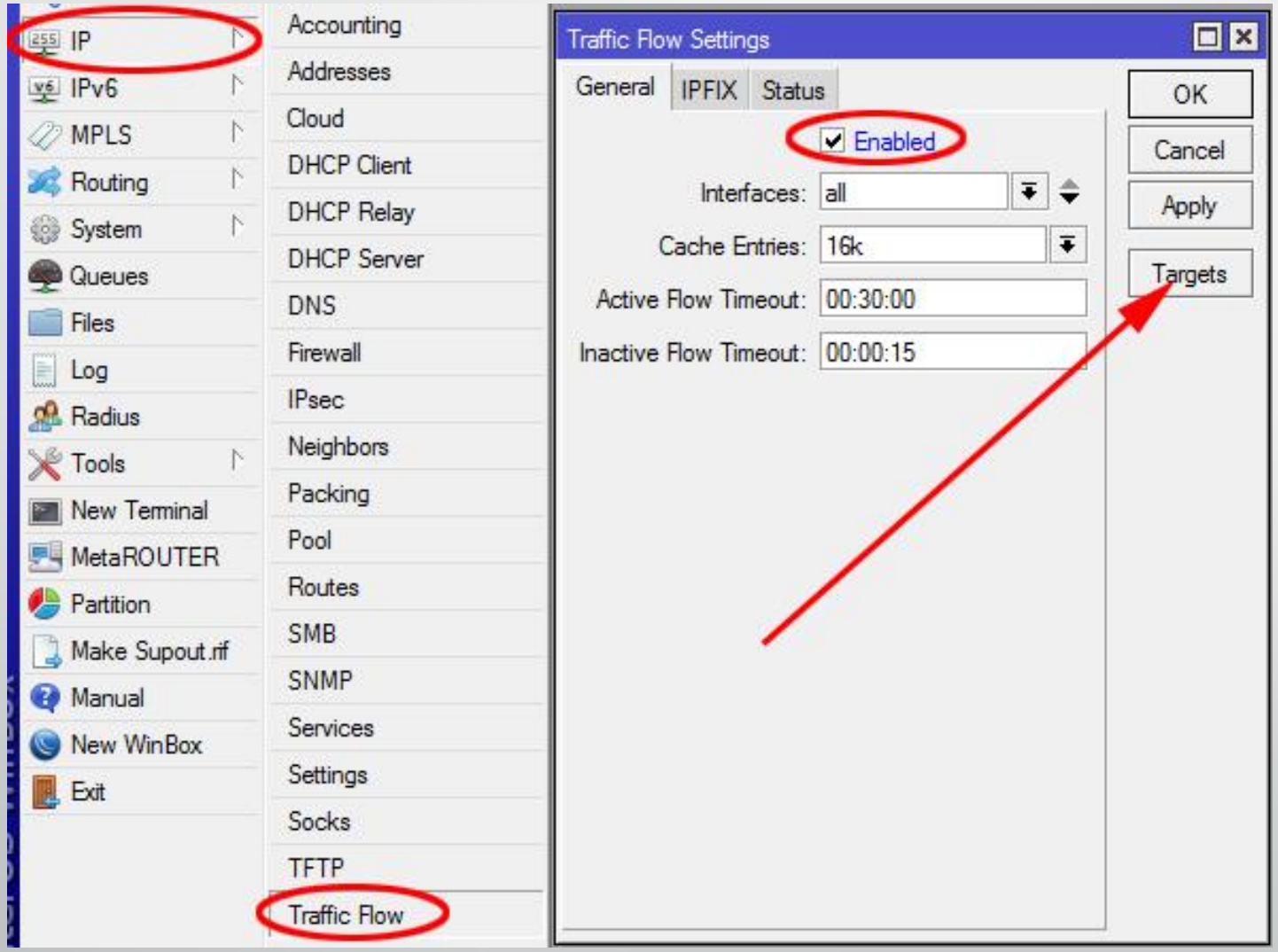
```
nprobe --zmq "tcp://*:5556" -G -i none -n none --collector-port 2055
```

- Стартираме ntopng

```
ntopng -i "tcp://127.0.0.1:5556" -e
```

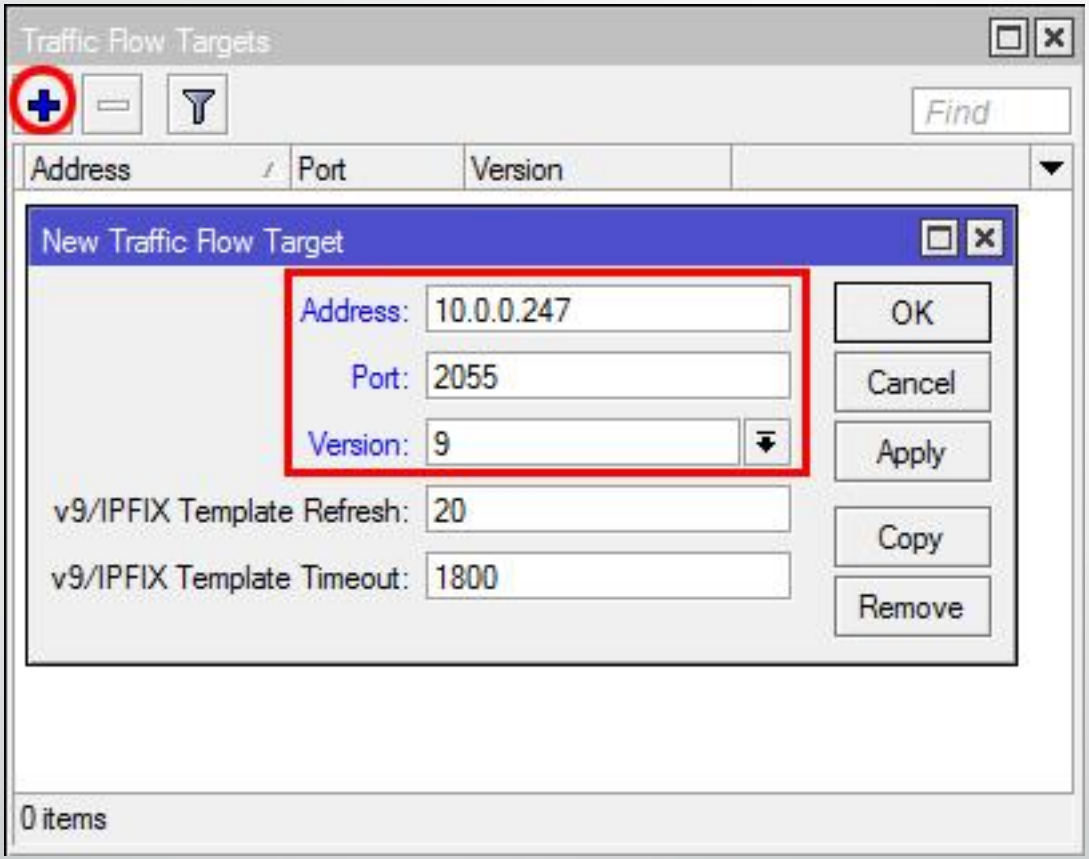
- Уеб достъп през http://<IP адрес>:3000
- Потребител/парола: admin/admin

Конфигуриране на Traffic Flow

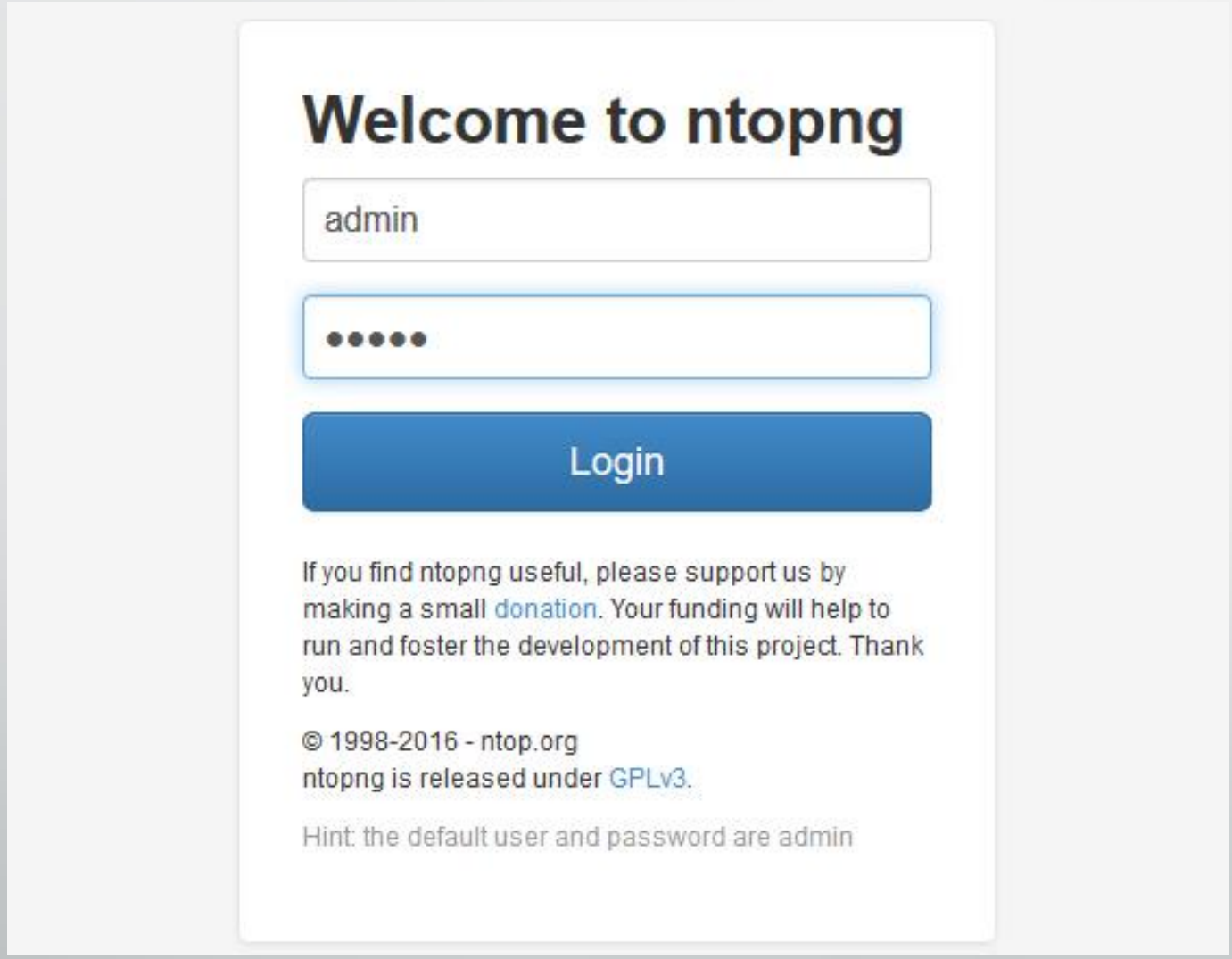


Traffic Flow, Петър Димитров

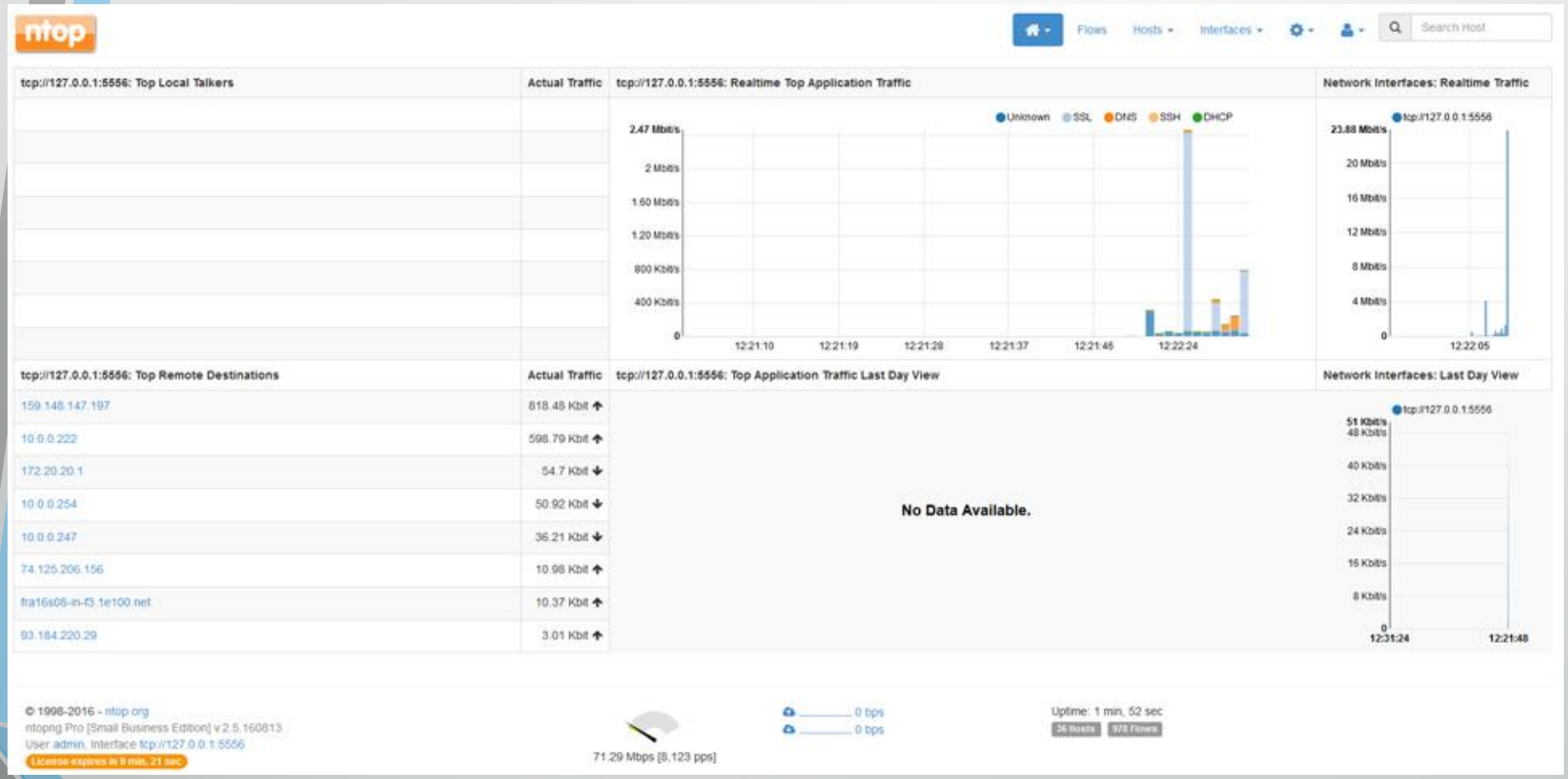
Конфигуриране на Traffic Flow



ntopng login

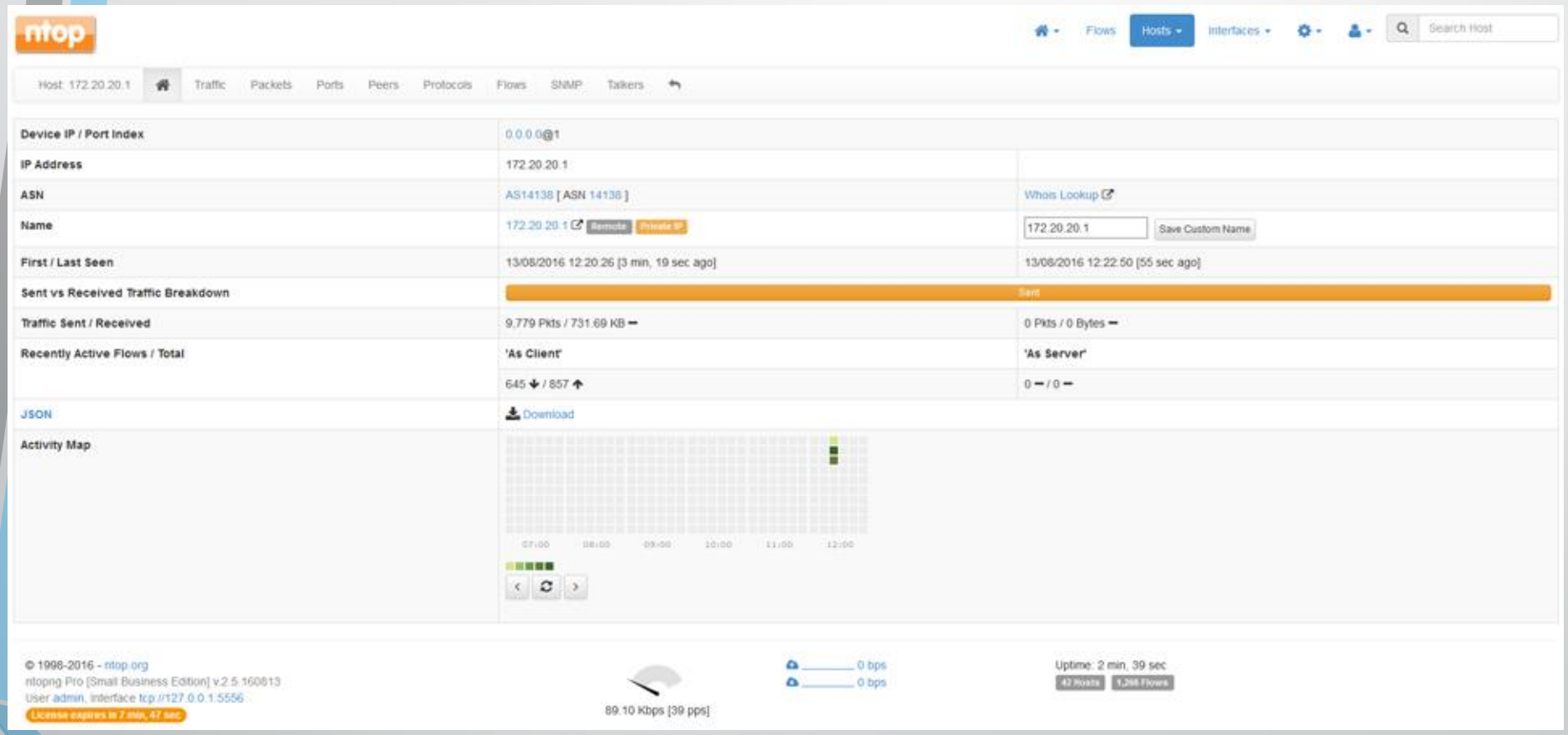


ntopng dashboard 1



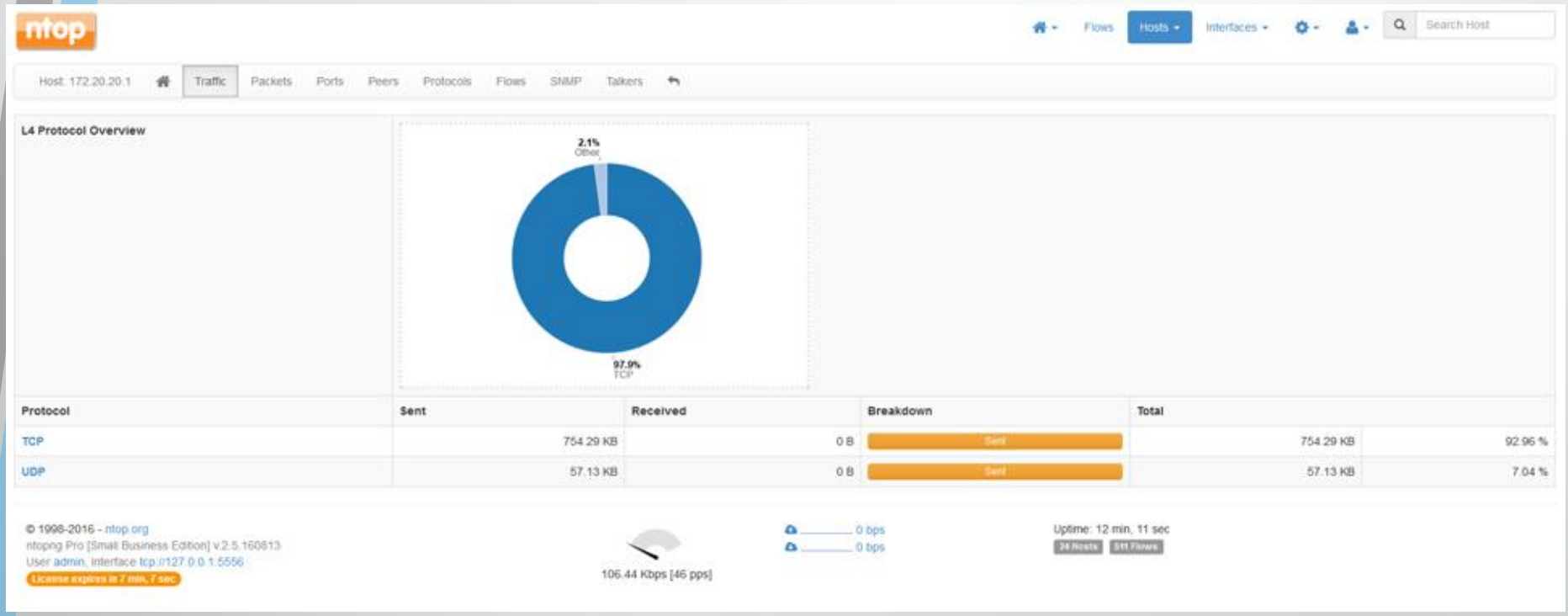
Traffic Flow, Петър Димитров

ntopng host



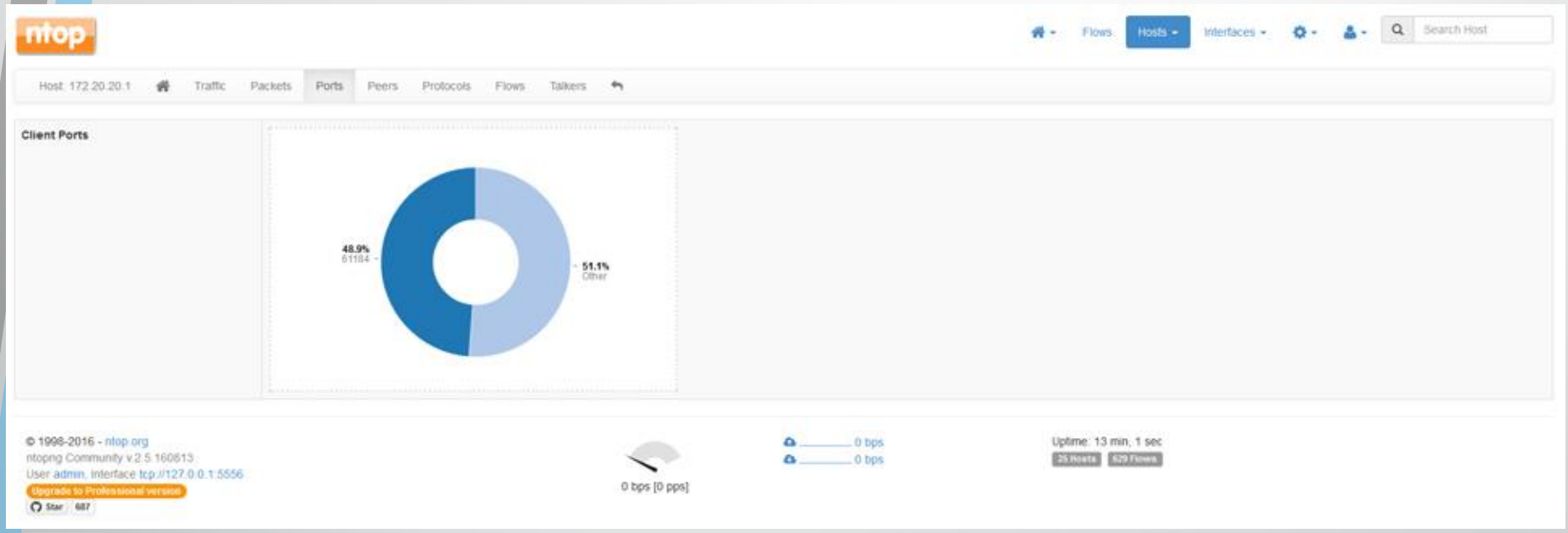
Traffic Flow, Петър Димитров

ntopng host L4 protocols



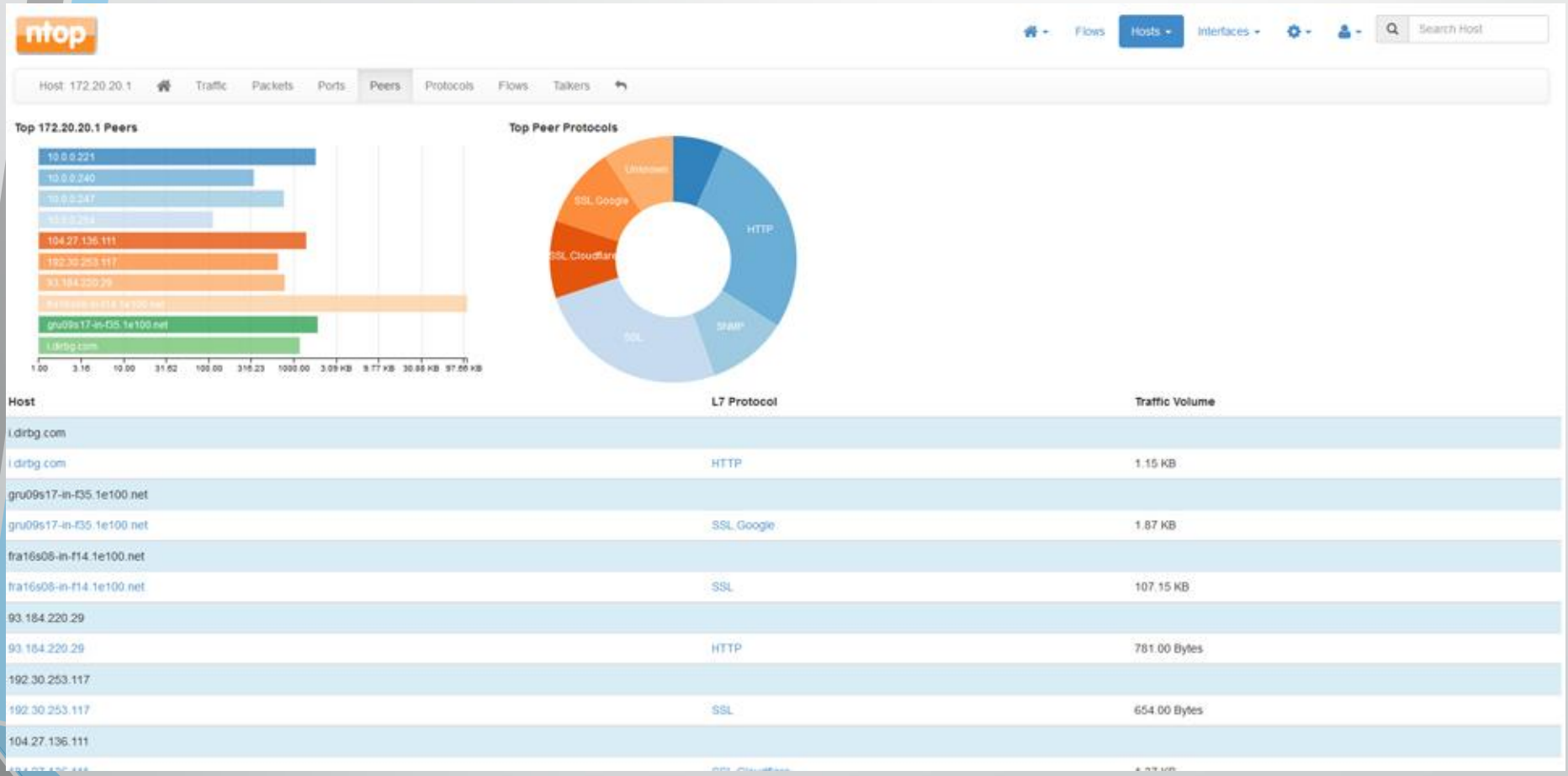
Traffic Flow, Петър Димитров

ntopng host ports



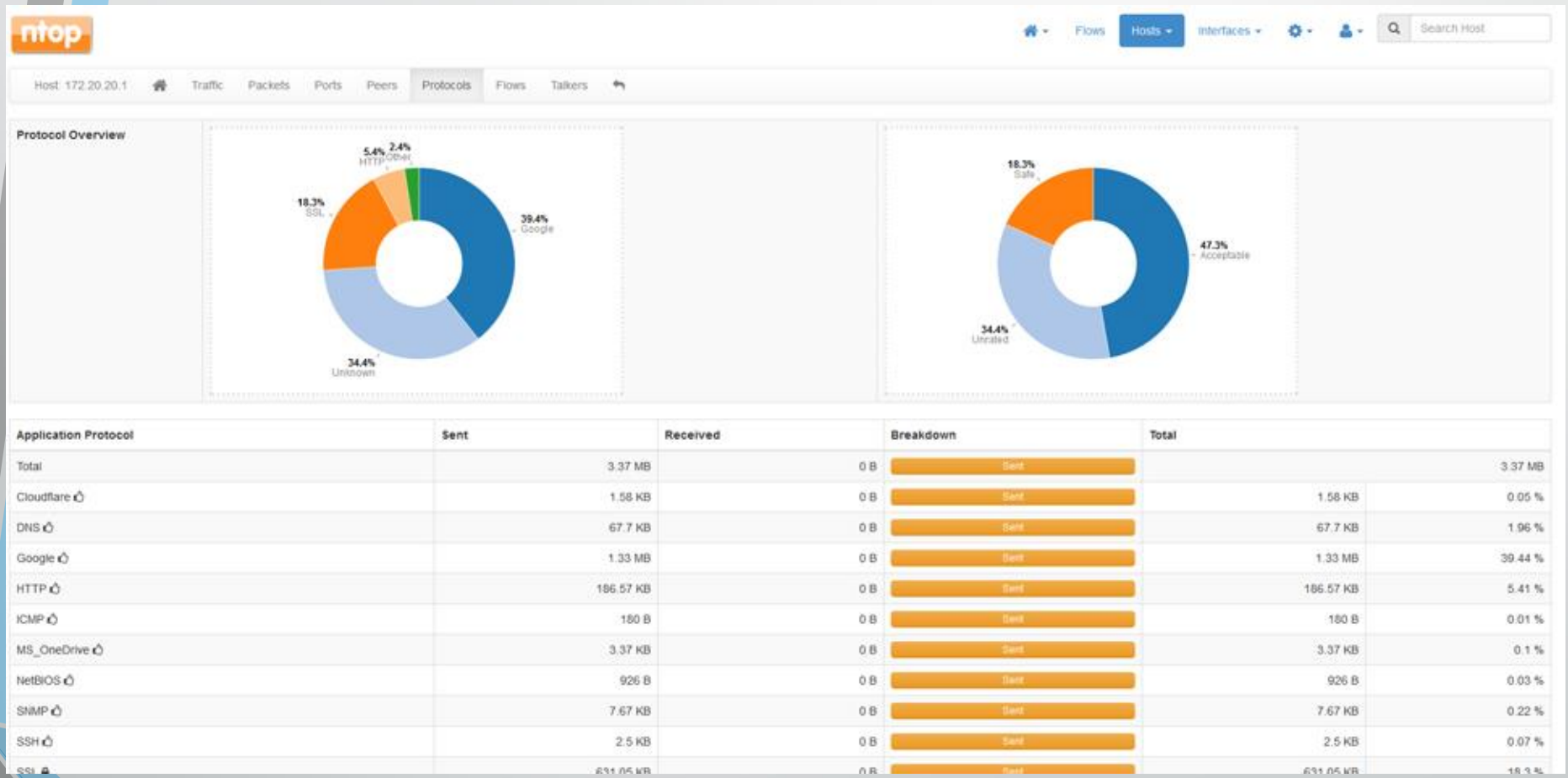
Traffic Flow, Петър Димитров

ntopng host peers



Traffic Flow, Петър Димитров

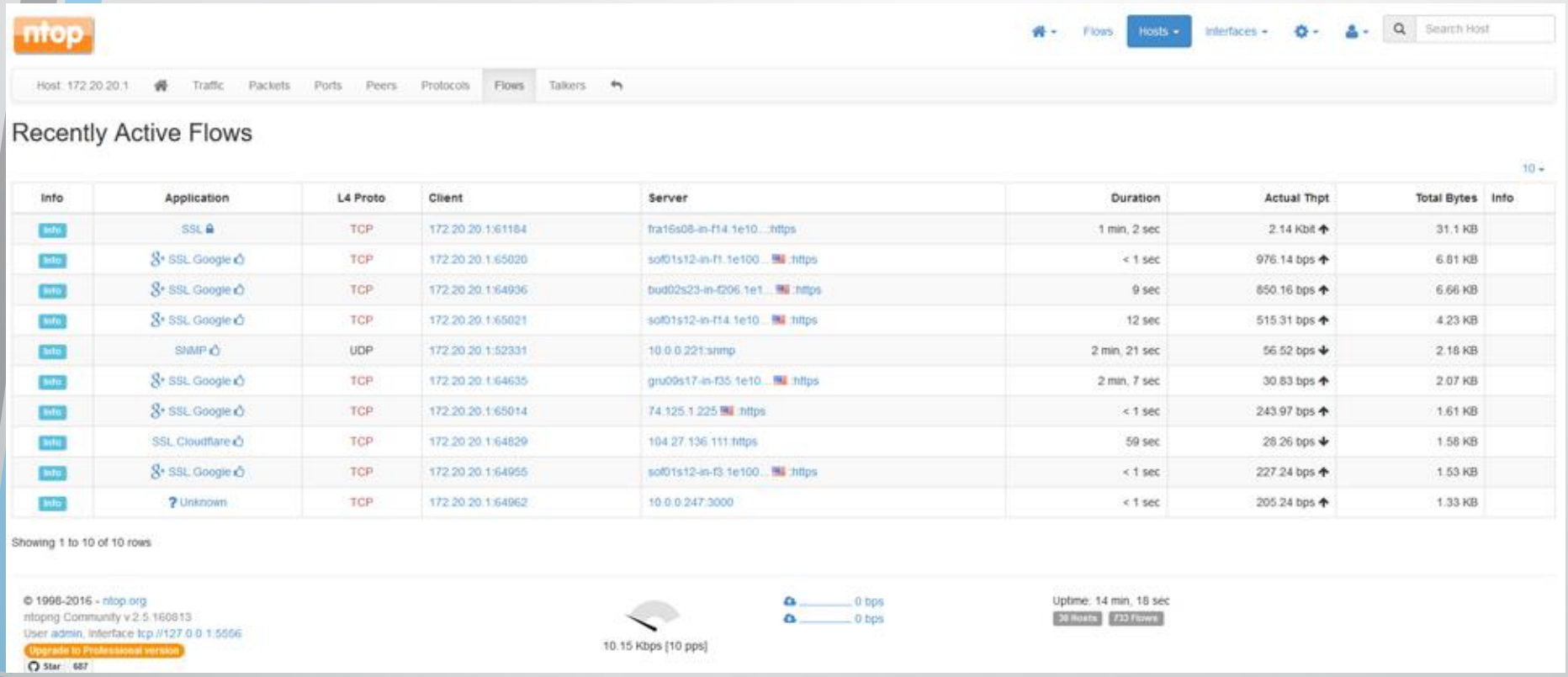
ntopng host protocols



Application Protocol	Sent	Received	Breakdown	Total	
Total	3.37 MB	0 B	Sent		3.37 MB
Cloudflare	1.58 KB	0 B	Sent	1.58 KB	0.05 %
DNS	67.7 KB	0 B	Sent	67.7 KB	1.96 %
Google	1.33 MB	0 B	Sent	1.33 MB	39.44 %
HTTP	186.57 KB	0 B	Sent	186.57 KB	5.41 %
ICMP	180 B	0 B	Sent	180 B	0.01 %
MS_OneDrive	3.37 KB	0 B	Sent	3.37 KB	0.1 %
NetBIOS	926 B	0 B	Sent	926 B	0.03 %
SNMP	7.67 KB	0 B	Sent	7.67 KB	0.22 %
SSH	2.5 KB	0 B	Sent	2.5 KB	0.07 %
SSL	631.05 KB	0 B	Sent	631.05 KB	18.3 %

Traffic Flow, Петър Димитров

ntopng host flows

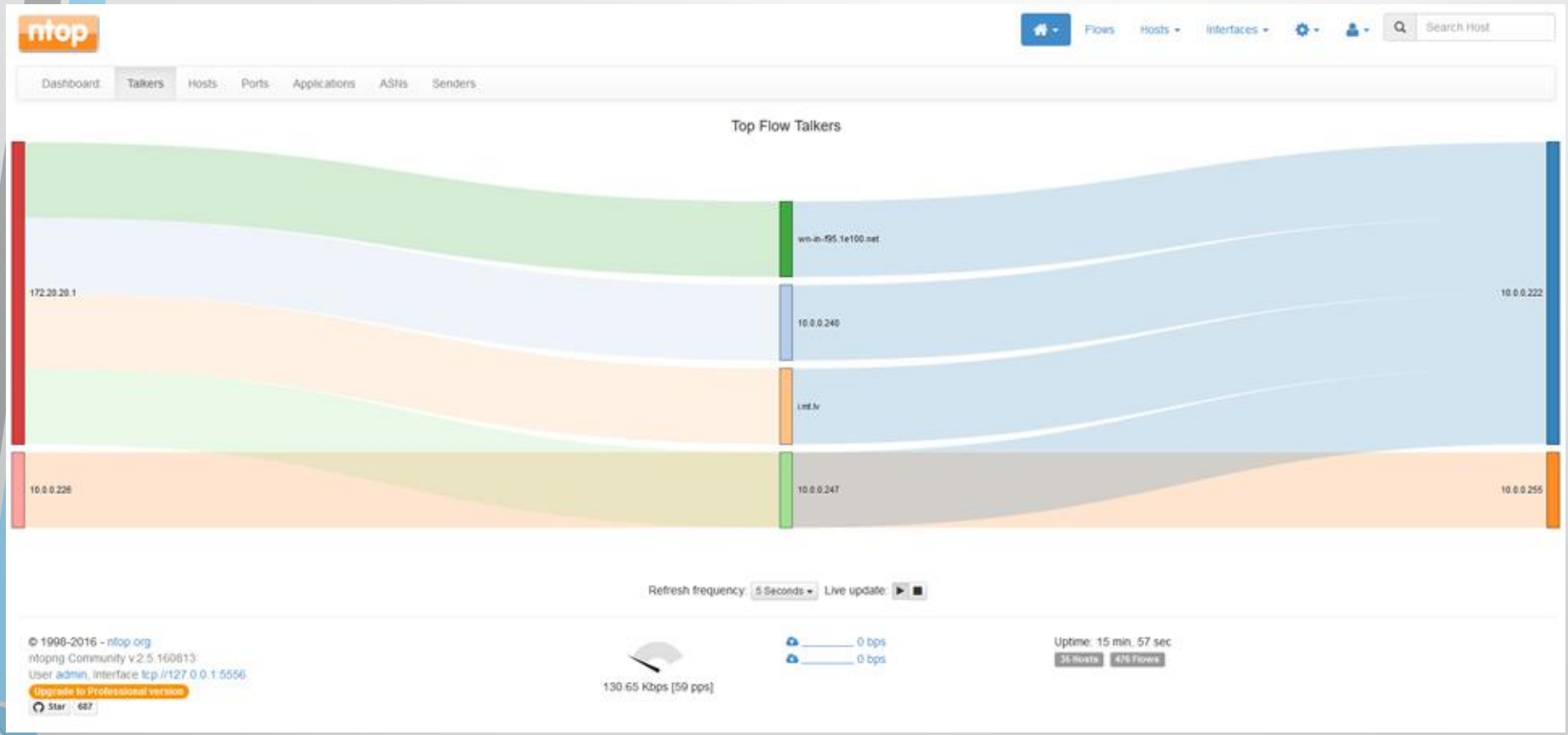


Traffic Flow, Петър Димитров

ntopng host talkers

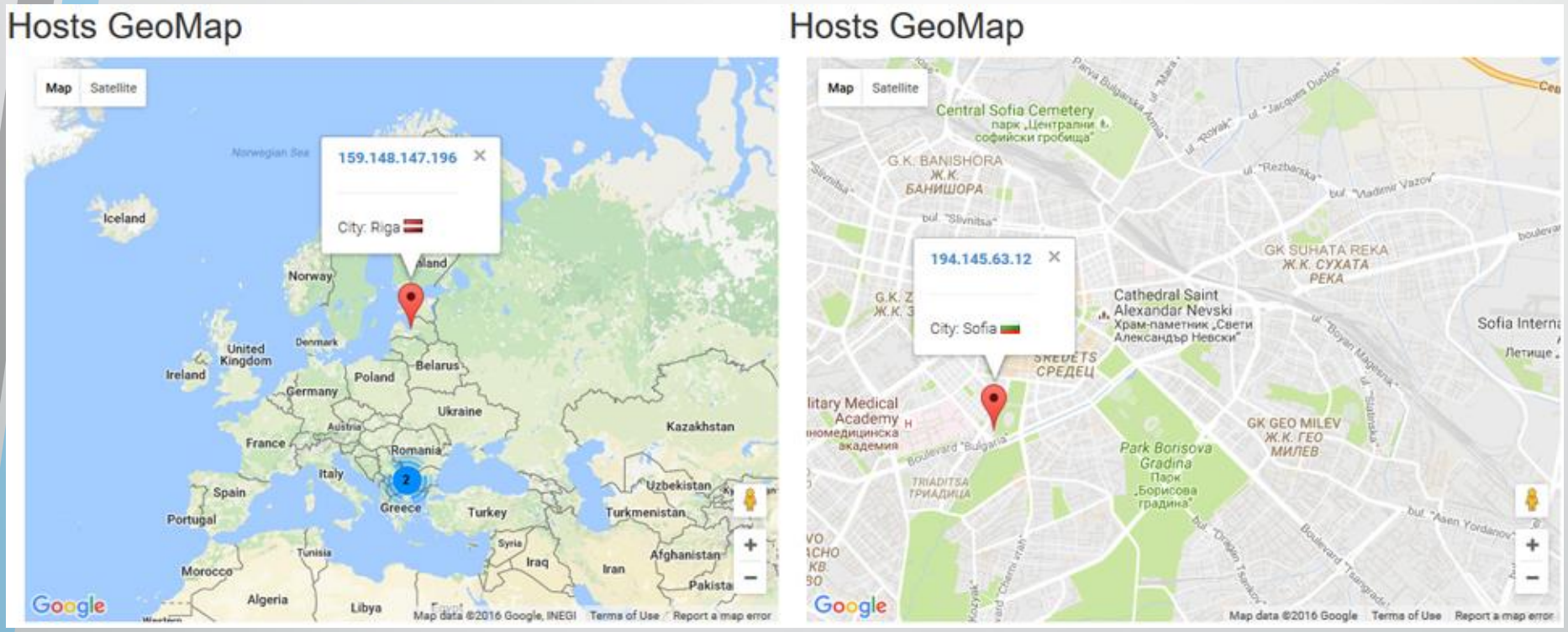
Traffic Flow, Петър Димитров

ntopng dashboard top talkers



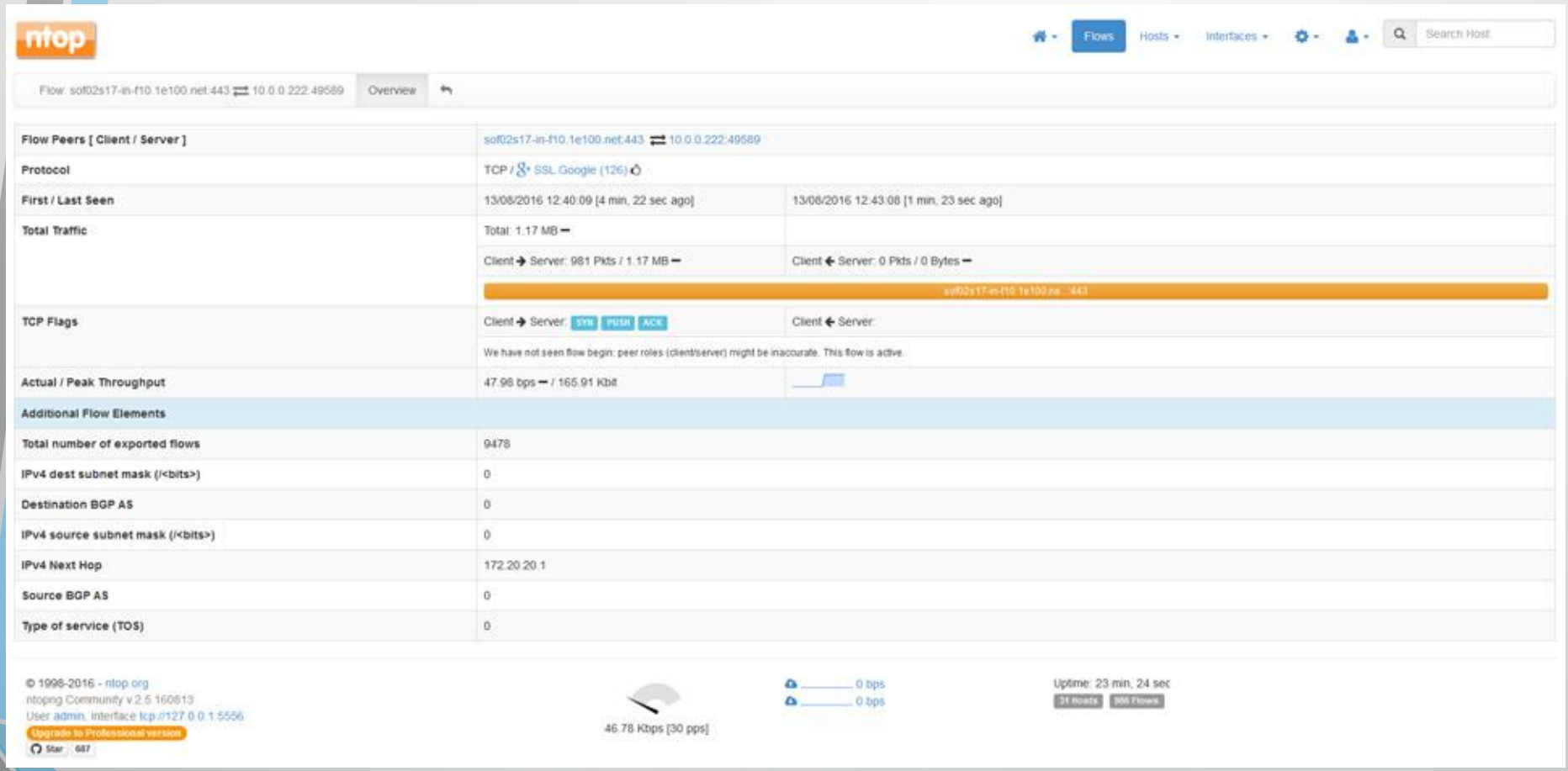
Traffic Flow, Петър Димитров

ntopng host GeoMap



Traffic Flow, Петър Димитров

ntopng flow

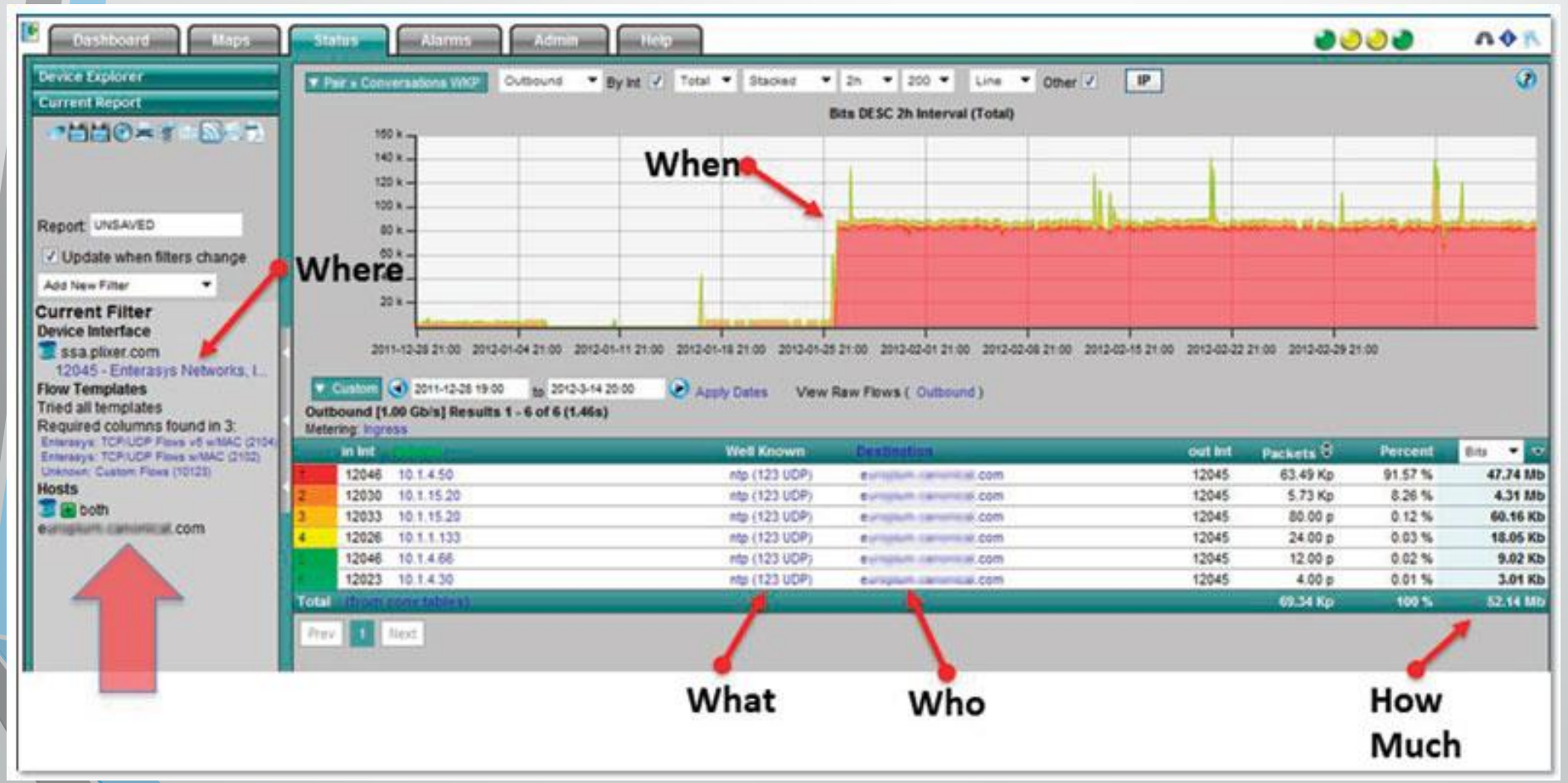


Traffic Flow, Петър Димитров

Да го направим!

Traffic Flow, Петър Димитров

Благодаря за вниманието!



Traffic Flow, Петър Димитров