



Traffic Flow

Получете пълна представа за трафика във
вашата мрежа

MikroTik Net Camp 2016

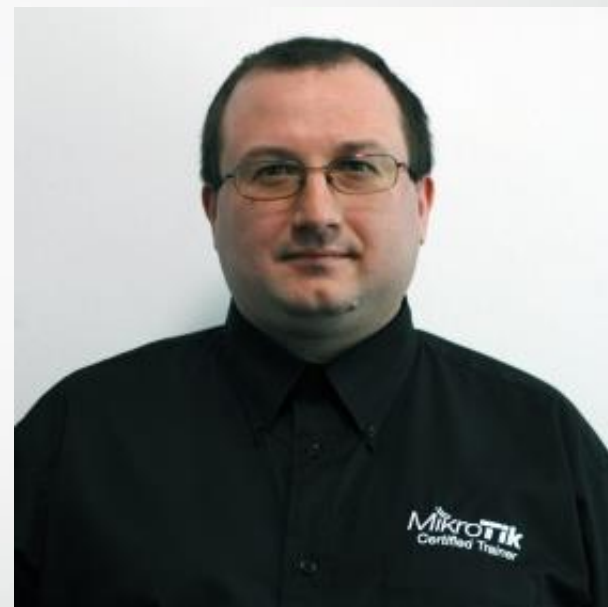
Цигов Чарк

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:

МТСНА, МТСВЕ, МТСРЕ, МТСТСЕ, МТСУМЕ, МТСИНЕ



Traffic Flow, Петър Димитров

Traffic Flow

- ❖ Това е система, проследяваща "потоци" от пакети, преминаващи през рутера, осигуряваща статистическа информация за различните потоци
- ❖ Полезен инструмент 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

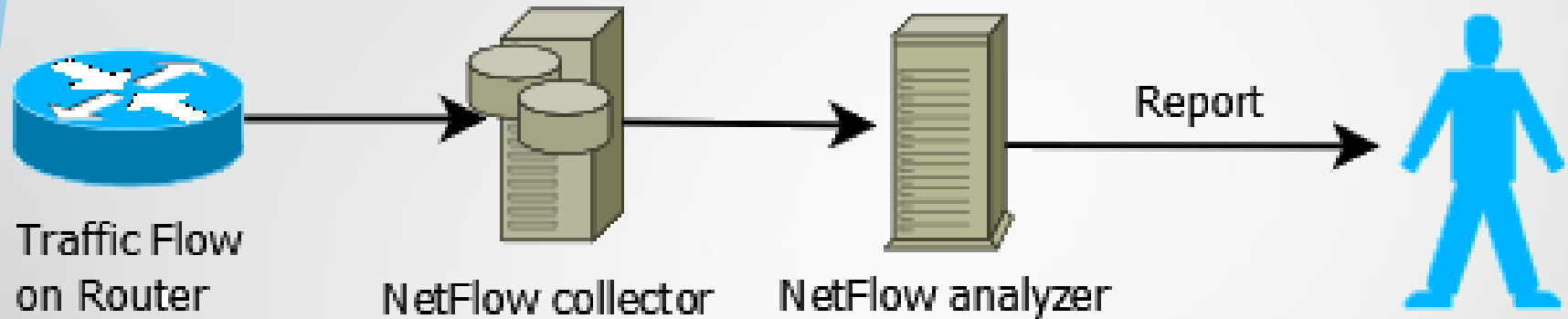
Traffic Flow

- ❖ 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 инсталираме 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`

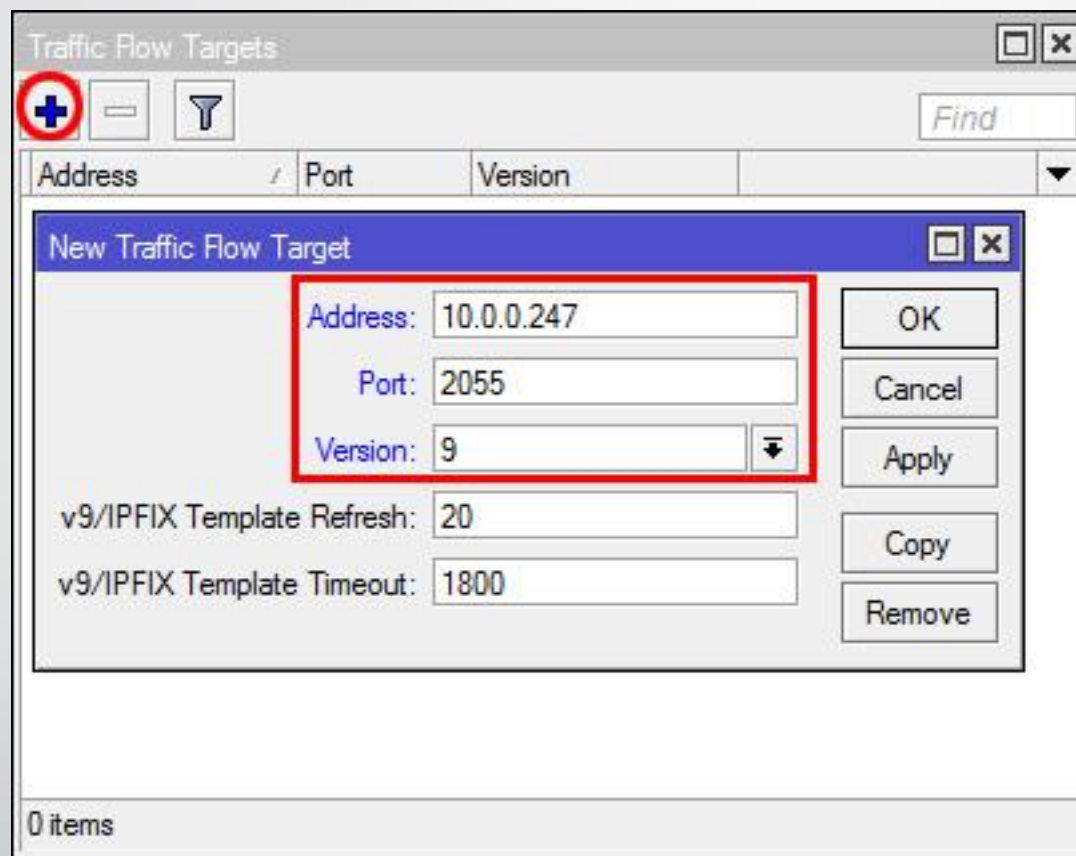
- ❖ Потребител/парола: `admin/admin`

Конфигуриране на Traffic Flow

The image shows a screenshot of the Mikrotik WinBox interface. On the left, the 'IP' menu item is circled in red. Below it, the 'Traffic Flow' menu item is also circled in red. On the right, the 'Traffic Flow Settings' dialog box is open, showing the 'Status' tab. The 'Enabled' checkbox is checked and circled in red. A red arrow points from the 'Enabled' checkbox to the 'Targets' button. The 'Targets' button is also circled in red. The 'Status' tab shows the following settings: 'Interfaces: all', 'Cache Entries: 16k', 'Active Flow Timeout: 00:30:00', and 'Inactive Flow Timeout: 00:00:15'. The 'Status' tab is selected, and the 'Enabled' checkbox is checked. The 'Targets' button is highlighted with a red arrow.

Traffic Flow, Петър Димитров

Конфигуриране на Traffic Flow



Traffic Flow, Петър Димитров

ntopng login

Welcome to ntopng

Login

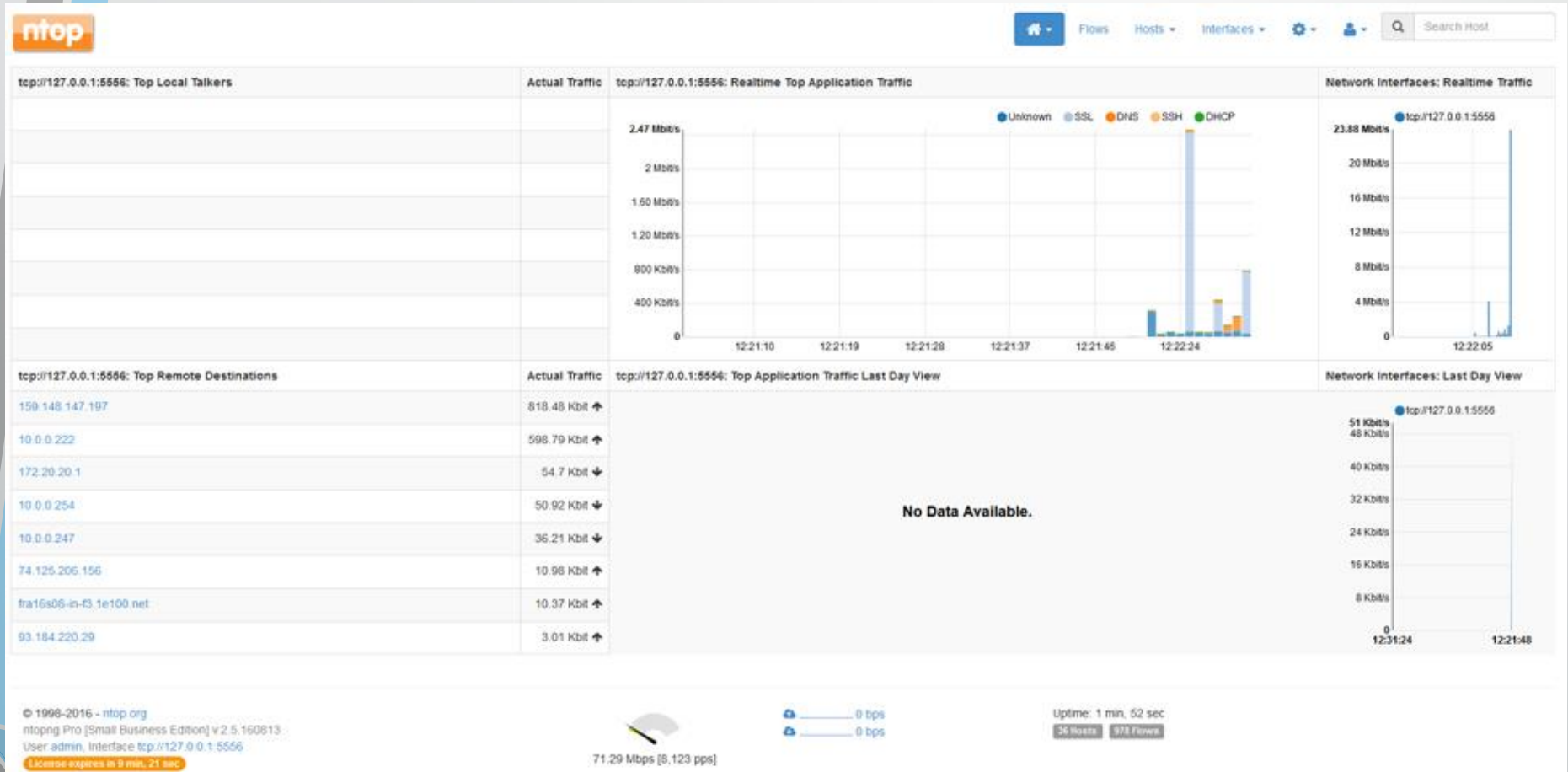
If you find ntopng useful, please support us by making a small [donation](#). Your funding will help to run and foster the development of this project. Thank you.

© 1998-2016 - ntop.org
ntopng is released under [GPLv3](#).

Hint: the default user and password are admin

Traffic Flow, Петър Димитров

ntopng dashboard 1



Traffic Flow, Петър Димитров

ntopng host

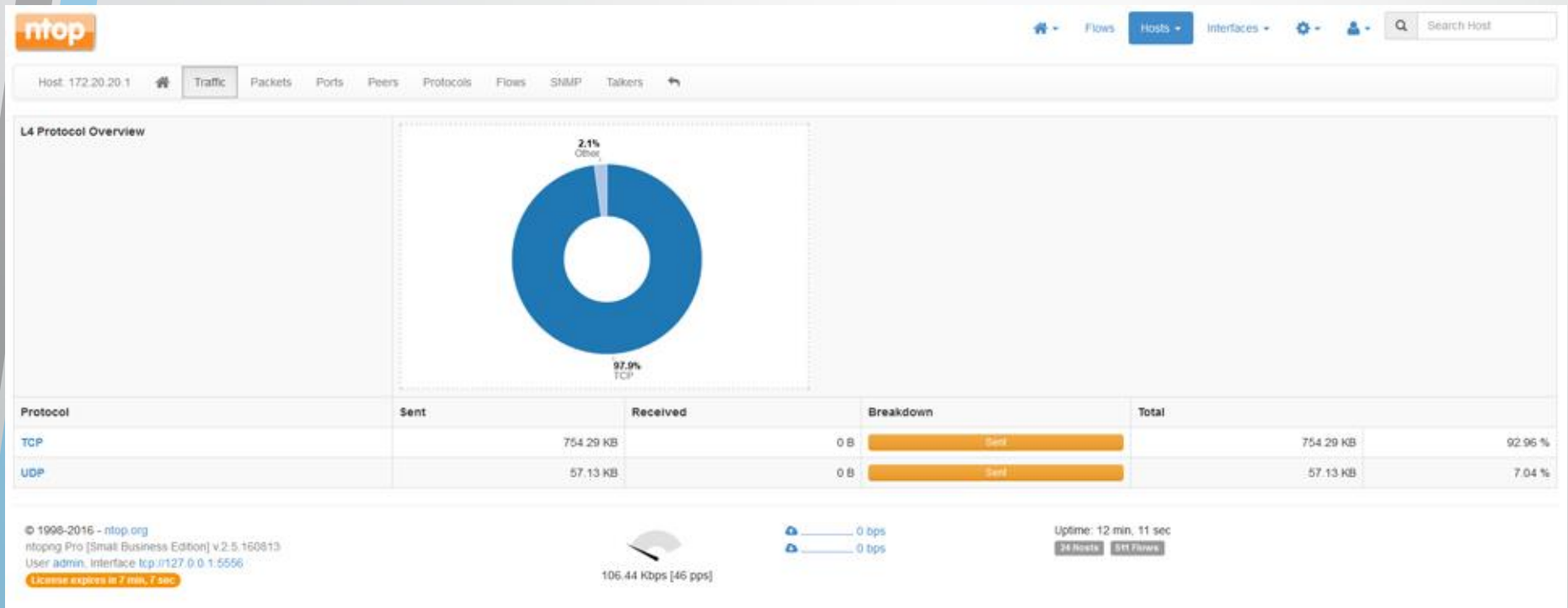
The screenshot displays the ntopng web interface for a specific host. The top navigation bar includes the ntop logo, a search bar, and menu items for Flows, Hosts, Interfaces, Settings, and Users. Below this, a secondary navigation bar shows tabs for Traffic, Packets, Ports, Peers, Protocols, Flows, SNMP, and Talkers. The main content area is divided into several sections:

- Device IP / Port Index:** 0.0.0.0@1
- IP Address:** 172.20.20.1
- ASN:** AS14138 [ASN 14138] with a Whois Lookup link.
- Name:** 172.20.20.1 with a Save Custom Name button.
- First / Last Seen:** 13/08/2016 12:20:26 [3 min, 19 sec ago] and 13/08/2016 12:22:50 [55 sec ago].
- Sent vs Received Traffic Breakdown:** A horizontal bar chart showing a large orange segment for 'Sent' traffic.
- Traffic Sent / Received:** 9,779 Pkts / 731.69 KB and 0 Pkts / 0 Bytes.
- Recently Active Flows / Total:** 'As Client' (645 ↓ / 857 ↑) and 'As Server' (0 ← / 0 →).
- JSON:** A Download button.
- Activity Map:** A grid-based heatmap showing activity over time from 07:00 to 12:00.

At the bottom of the interface, there is a footer with copyright information (© 1998-2016 - ntop.org), version details (ntopng Pro [Small Business Edition] v.2.5.160813), user information (User admin, Interface tcp://127.0.0.1:5556), and a license expiration notice (License expires in 7 min, 47 sec). On the right side of the footer, there are status indicators: a fan icon for CPU usage (89.10 Kbps [39 pps]), network status (0 bps), and system uptime (Uptime: 2 min, 39 sec) with a summary box showing 42 Hosts and 1,268 Flows.

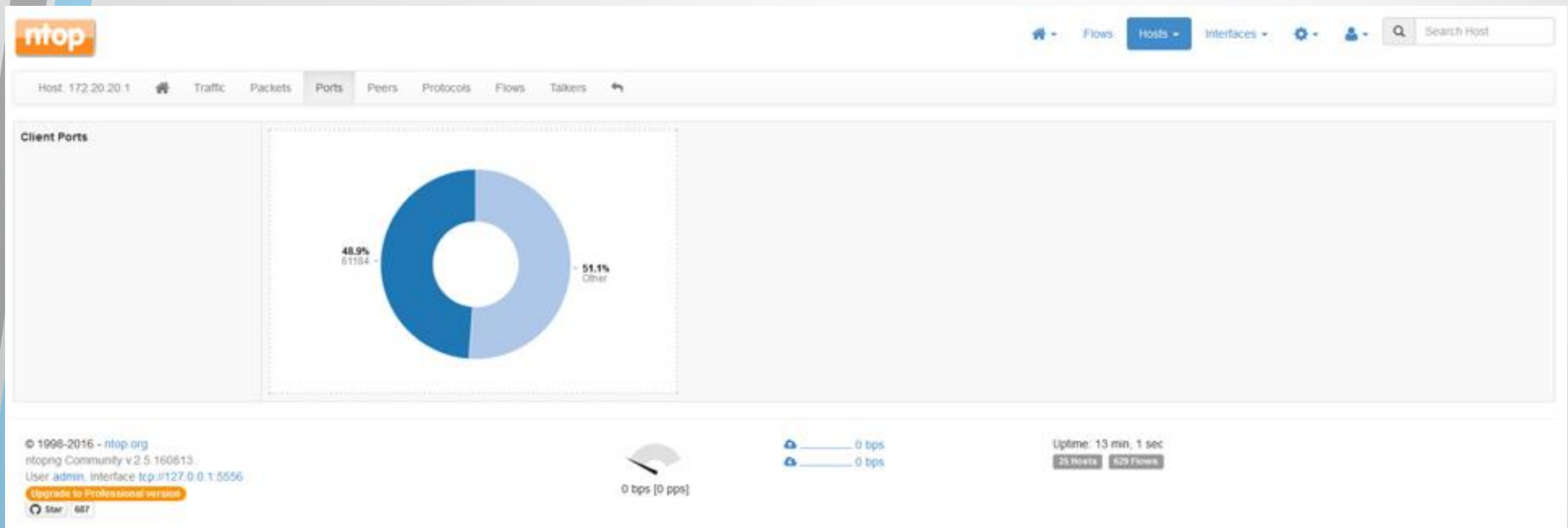
Traffic Flow, Петър Димитров

ntopng host L4 protocols



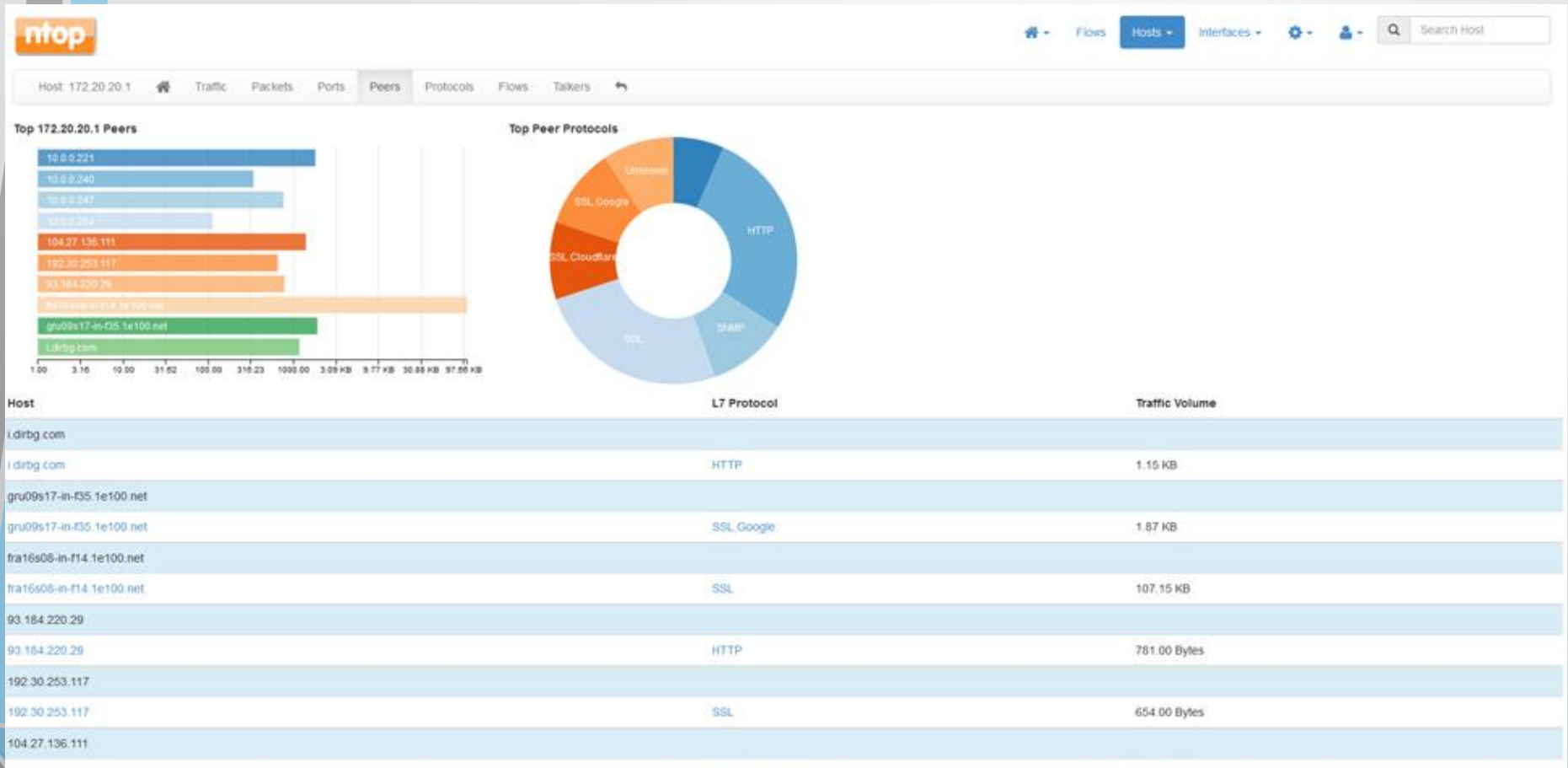
Traffic Flow, Петър Димитров

ntopng host ports



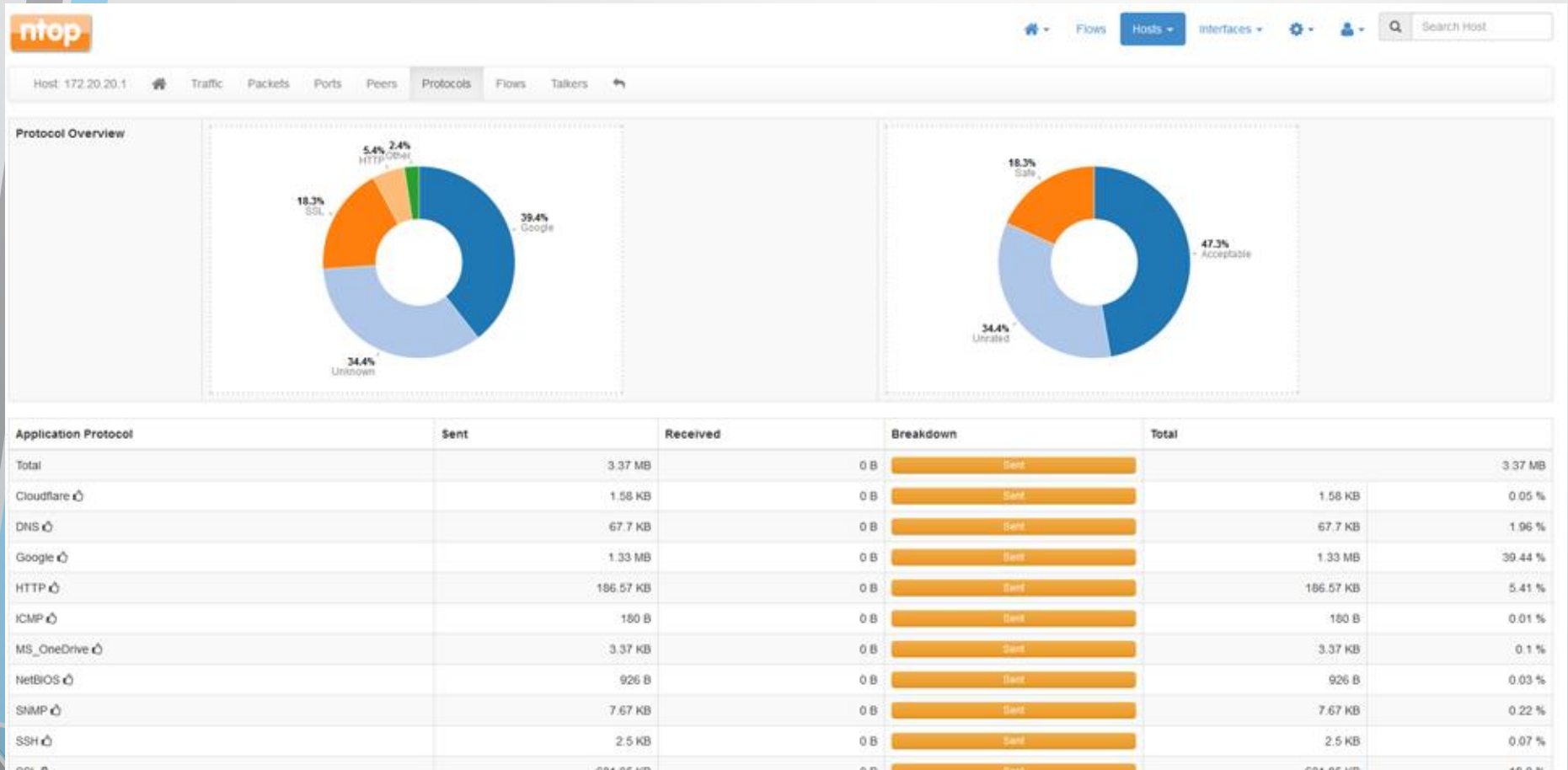
Traffic Flow, Петър Димитров

ntopng host peers



Traffic Flow, Петър Димитров

ntopng host protocols



Traffic Flow, Петър Димитров

ntopng host flows

ntopng

Host: 172.20.20.1

Flows | Hosts | Interfaces

Host: 172.20.20.1 Traffic Packets Ports Peers Protocols **Flows** Talkers

Recently Active Flows

Info	Application	L4 Proto	Client	Server	Duration	Actual Thpt	Total Bytes	Info
Info	SSL	TCP	172.20.20.1:61184	fra15s08-in-f14.1e10...:https	1 min, 2 sec	2.14 KB/s ↑	31.1 KB	
Info	SSL Google	TCP	172.20.20.1:65020	sof01s12-in-f1.1e100...:https	< 1 sec	976.14 bps ↑	6.81 KB	
Info	SSL Google	TCP	172.20.20.1:64936	bud02s23-in-f206.1e1...:https	9 sec	650.16 bps ↑	6.66 KB	
Info	SSL Google	TCP	172.20.20.1:65021	sof01s12-in-f14.1e10...:https	12 sec	515.31 bps ↑	4.23 KB	
Info	SNMP	UDP	172.20.20.1:52331	10.0.0.221:snmp	2 min, 21 sec	56.52 bps ↓	2.16 KB	
Info	SSL Google	TCP	172.20.20.1:64635	gru00s17-in-f35.1e10...:https	2 min, 7 sec	30.83 bps ↑	2.07 KB	
Info	SSL Google	TCP	172.20.20.1:65014	74.125.1.225:https	< 1 sec	243.97 bps ↑	1.61 KB	
Info	SSL Cloudflare	TCP	172.20.20.1:64829	104.27.136.111:https	59 sec	28.26 bps ↓	1.58 KB	
Info	SSL Google	TCP	172.20.20.1:64955	sof01s12-in-f3.1e100...:https	< 1 sec	227.24 bps ↑	1.53 KB	
Info	Unknown	TCP	172.20.20.1:64962	10.0.0.247:3000	< 1 sec	205.24 bps ↑	1.33 KB	

Showing 1 to 10 of 10 rows

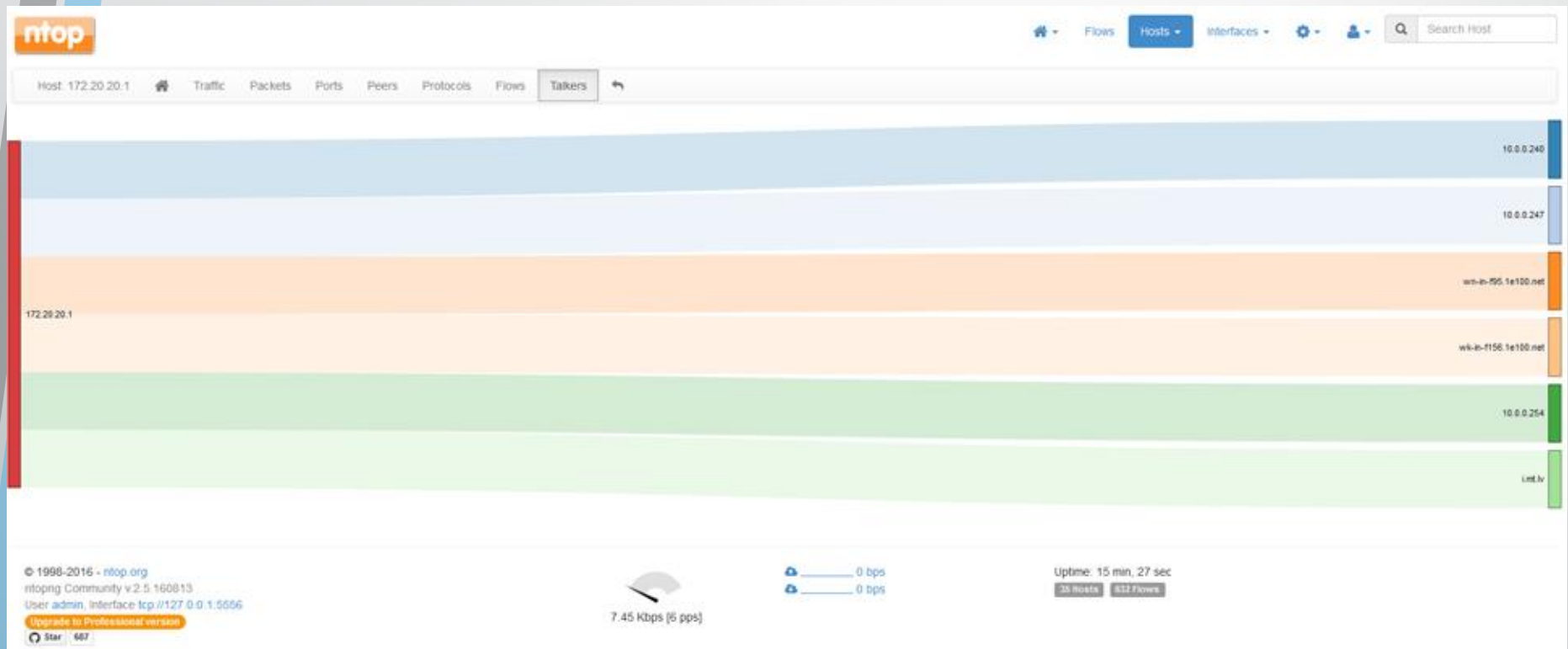
© 1998-2015 - ntop.org
ntopng Community v 2.5.160813
User admin, interface tcp://127.0.0.1:5556
[Upgrade to Professional version](#)
Star 687

10.15 Kbps [10 pps]

Uptime: 14 min, 18 sec
38 Hosts, 733 Flows

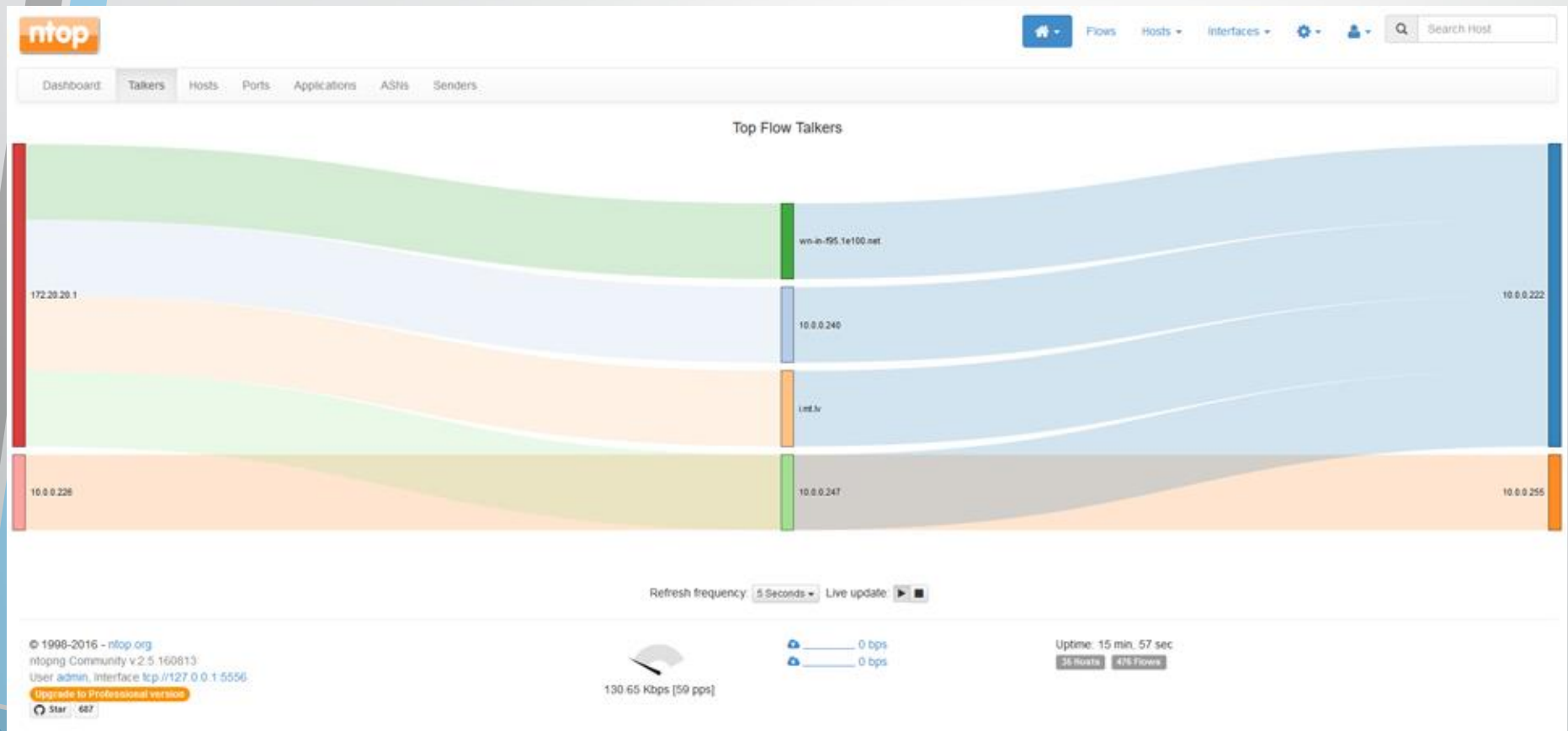
Traffic Flow, Петър Димитров

ntopng host talkers



Traffic Flow, Петър Димитров

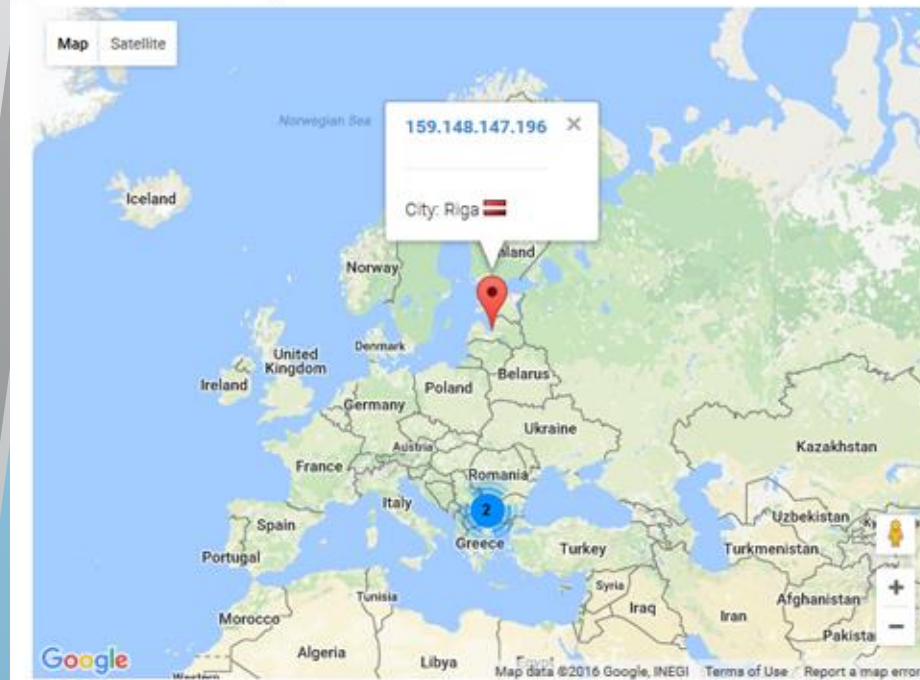
ntopng dashboard top talkers



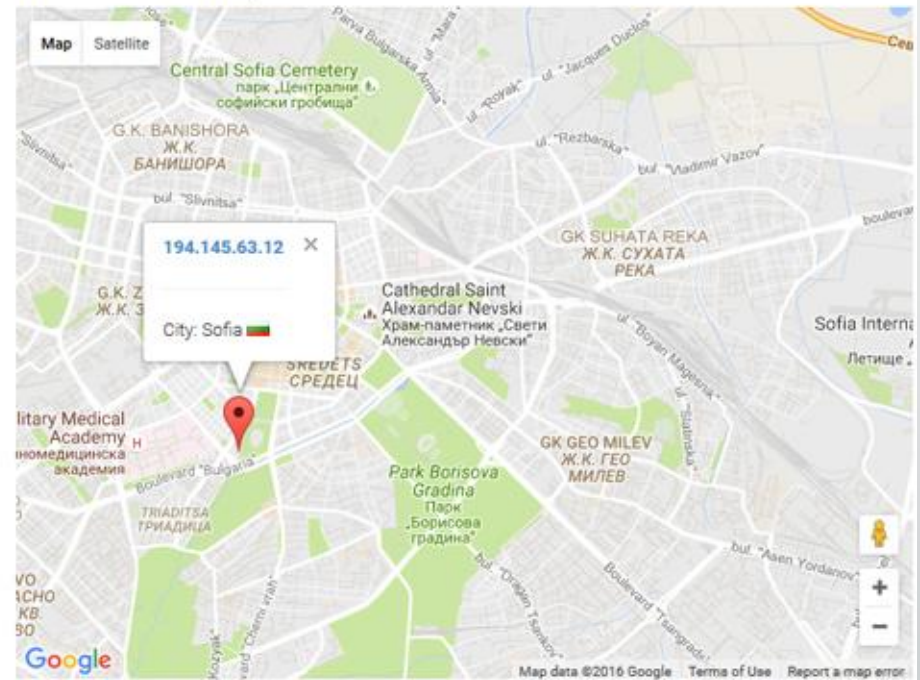
Traffic Flow, Петър Димитров

ntopng host GeoMap

Hosts GeoMap



Hosts GeoMap



Traffic Flow, Петър Димитров

ntopng flow

The screenshot displays the ntopng interface for monitoring a specific flow. The flow is identified as 'Flow: soft02s17-in-f10.1e100.net.443' with IP addresses '10.0.0.222' and '49589'. The protocol is 'TCP / SSL Google (126)'. The flow is active, with a total traffic of 1.17 MB. The client-to-server direction shows 981 packets and 1.17 MB of traffic, while the server-to-client direction shows 0 packets and 0 bytes. The TCP flags are SYN, PUSH, and ACK. The actual throughput is 47.98 bps, and the peak throughput is 165.91 Kbit. The interface also shows additional flow elements such as the total number of exported flows (9478), IPv4 destination subnet mask (0), destination BGP AS (0), IPv4 source subnet mask (0), IPv4 next hop (172.20.20.1), source BGP AS (0), and type of service (TOS) (0). The interface includes a search bar, navigation tabs for Flows, Hosts, and Interfaces, and a status bar at the bottom showing uptime (23 min, 24 sec) and current traffic (46.78 Kbps [30 pps]).

Flow Peers [Client / Server]	soft02s17-in-f10.1e100.net.443 10.0.0.222:49589	
Protocol	TCP / SSL Google (126)	
First / Last Seen	13/08/2016 12:40:09 [4 min, 22 sec ago]	13/08/2016 12:43:08 [1 min, 23 sec ago]
Total Traffic	Total: 1.17 MB	
	Client → Server: 981 Pkts / 1.17 MB	Client ← Server: 0 Pkts / 0 Bytes
TCP Flags	Client → Server: SYN PUSH ACK	Client ← Server:
Actual / Peak Throughput	47.98 bps / 165.91 Kbit	
Additional Flow Elements		
Total number of exported flows	9478	
IPv4 dest subnet mask (<bits>)	0	
Destination BGP AS	0	
IPv4 source subnet mask (<bits>)	0	
IPv4 Next Hop	172.20.20.1	
Source BGP AS	0	
Type of service (TOS)	0	

© 1998-2016 - ntop.org
ntopng Community v 2.5.160813
User admin, interface lcp://127.0.0.1:5556
Upgrade to Professional version
Star 687

46.78 Kbps [30 pps]

Uptime: 23 min, 24 sec
31 Hosts 188 Flows

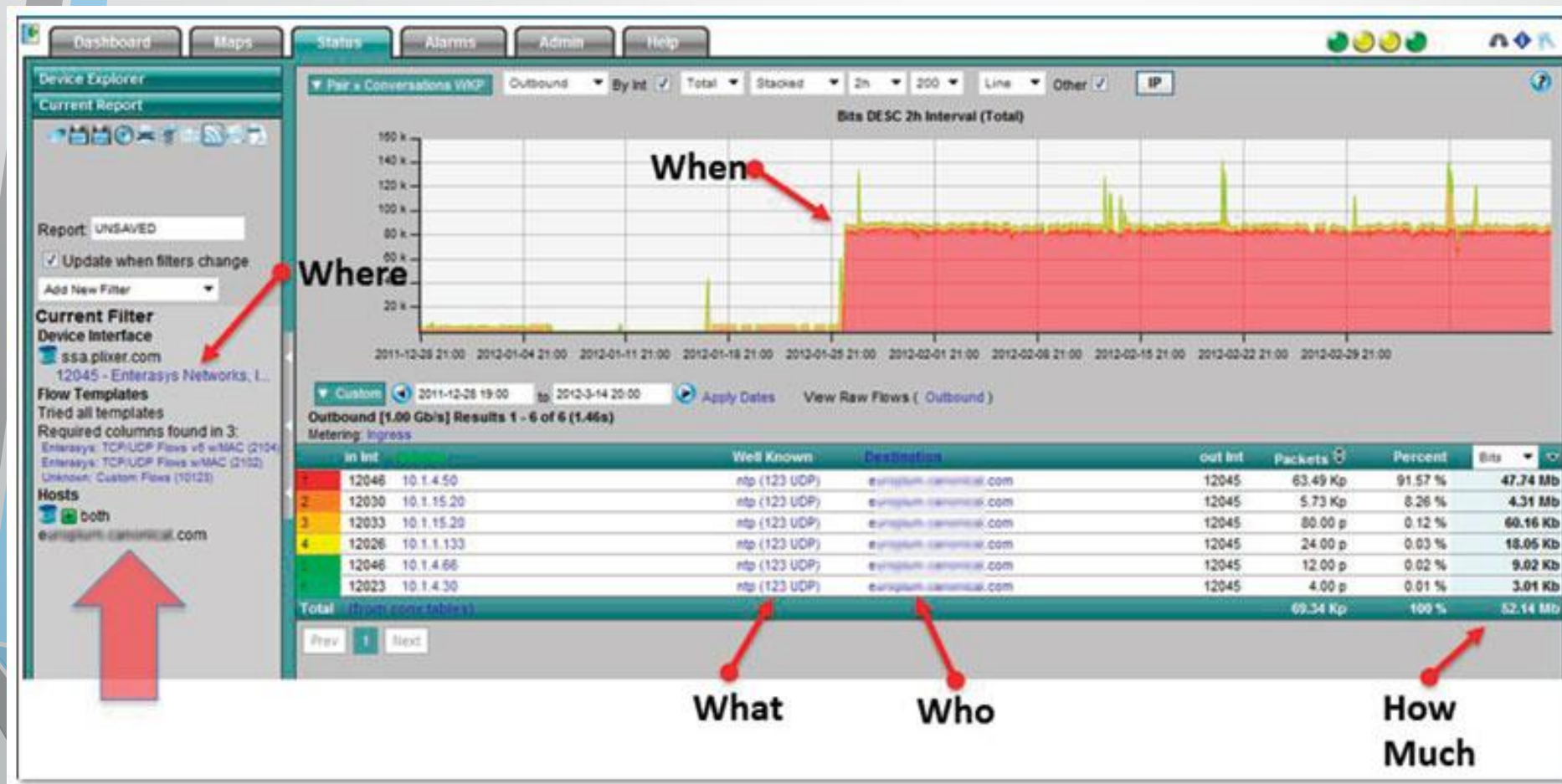
Traffic Flow, Петър Димитров



Да го направим!

Traffic Flow, Петър Димитров

Благодаря за вниманието!



Traffic Flow, Петър Димитров