Network Management & Monitoring

NfSen

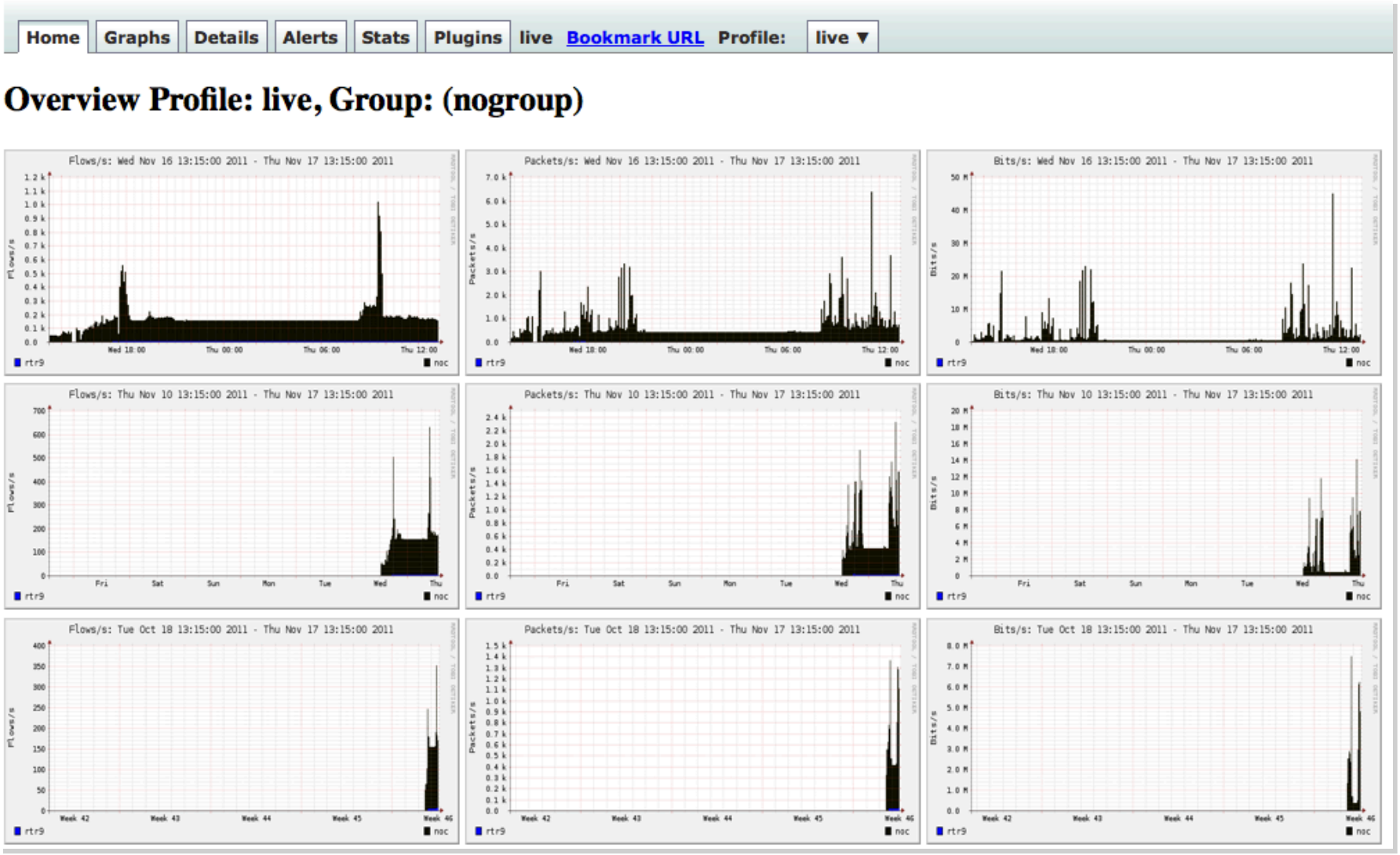
What is NfSen

- Is a graphical (Web Based) front end to NfDump
- NfDump tools collect and process netflow data on the command line
- NfSen allows you to:
  - Easily navigate through the netflow data.
  - Process the netflow data within the specified time span.
  - Create history as well as continuous profiles.
  - Set alerts, based on various conditions.
  - Write your own plugins to process netflow data on a regular interval.

NfSen structure

- Configuration file - nfsen.conf
- NfDump files – Netflow files containing collected flows stored in ‘profiles-data’ directory
  - NB: It is possible for other programs to read NFdump files but don’t store them for too long as they can fill up your drive
- Actual graphs – stored in ‘profiles-stat’ directory

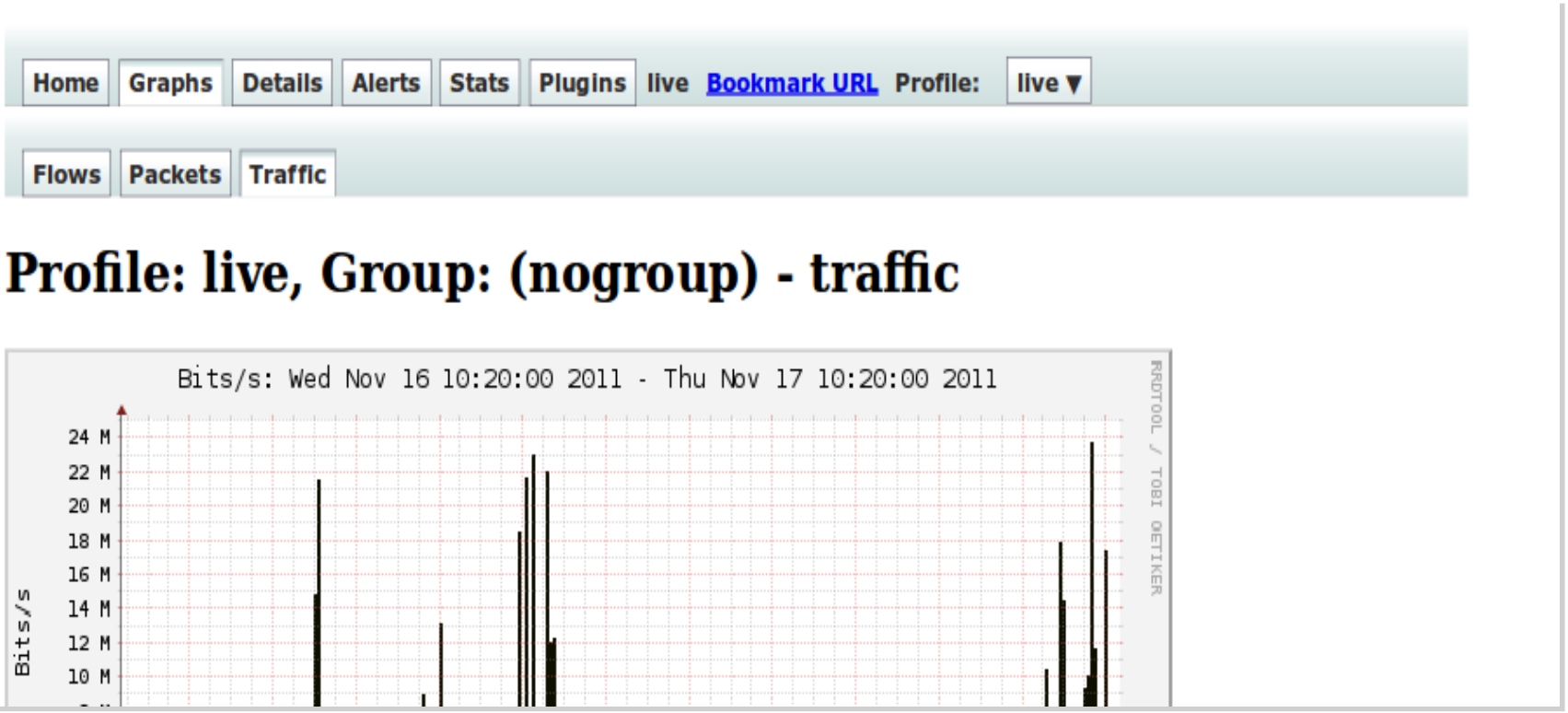
NfSen Home Screen



Graphs Tab

Graphs of flows, packets and traffic based on interface with netflow activated

NB: What is seen under Traffic should closely match what is under Cacti for the same interface



Details Page

- Most interesting page
- Can view present flow information or stored flow information
- Can view detailed Netflow information such as
  - AS Numbers (more useful if you have full routing table exported on your router)
  - Src hosts/ports, destination hosts and ports
  - Unidirectional or Bi-directional flows
  - Flows on specific interfaces
  - Protocols and TOS


Home
Graphs
Details
Alerts
Stats
Plugins
live
Bookmark URL
Profile:
live
Profile: live
TCP
UDP
ICMP
other
Wed Nov 16 22:25:00 2011 Bits/s any protocol
Bits/s any protocol
Wed 12:00
Wed 18:00
Thu 00:00
Thu 06:00
rtr9
noc
ProfileInfo:
Type: live
Max: unlimited
Exp: never
Start: Nov 16 2011 - 12:10 UTC
End: Nov 17 2011 - 10:25 UTC
tstart 2011-11-16-22-25
tend 2011-11-16-22-25
Packets
Flows
Select
Single Timeslot
Display:
1 day
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot Nov 16 2011 - 22:25
Channel:
Flows:
Packets:
Traffic:
all:
tcp:
udp:
icmp:
other:
noc
149.1 /s
29.3 /s
50.6 /s
69.2 /s
0 /s
393.2 /s
222.7 /s
52.2 /s
118.3 /s
0 /s
348.3 kb/s
226.4 kb/s
41.0 kb/s
80.9 kb/s
0 b/s
rtr9
5.1 /s
1.7 /s
3.0 /s
0.4 /s
0 /s
17.5 /s
8.6 /s
3.0 /s
6.0 /s
0 /s
13.7 kb/s
7.4 kb/s
2.2 kb/s
4.1 kb/s
0 b/s
All
None
Display:
Sum
Rate
Netflow Processing
Source:
Filter:
Options:
noc
rtr9
All Sources
List Flows
Stat TopN
Top:
10
Stat:
Any IP Address
order by
flows
Limit:
Packets
>
0
Output:
/ IPv6 long
and
<none>
Clear Form
process
Netflow traffic graphs organized by Protocol
Time period for flows being observed
Graph of Netflow traffic for all Protocols
Routers being monitored
Extended Netflow processing options

Alerts and Stats

Alerts Page

- Can create alerts based on set thresholds eg, increase or decrease of traffic
- Emails can be sent once alarm is triggered

Stats page

- Can create graphs based on specific information
  - ASNs,
  - Host/Destination IPs/Ports
  - In/Out interfaces
  - Among others

Plugins

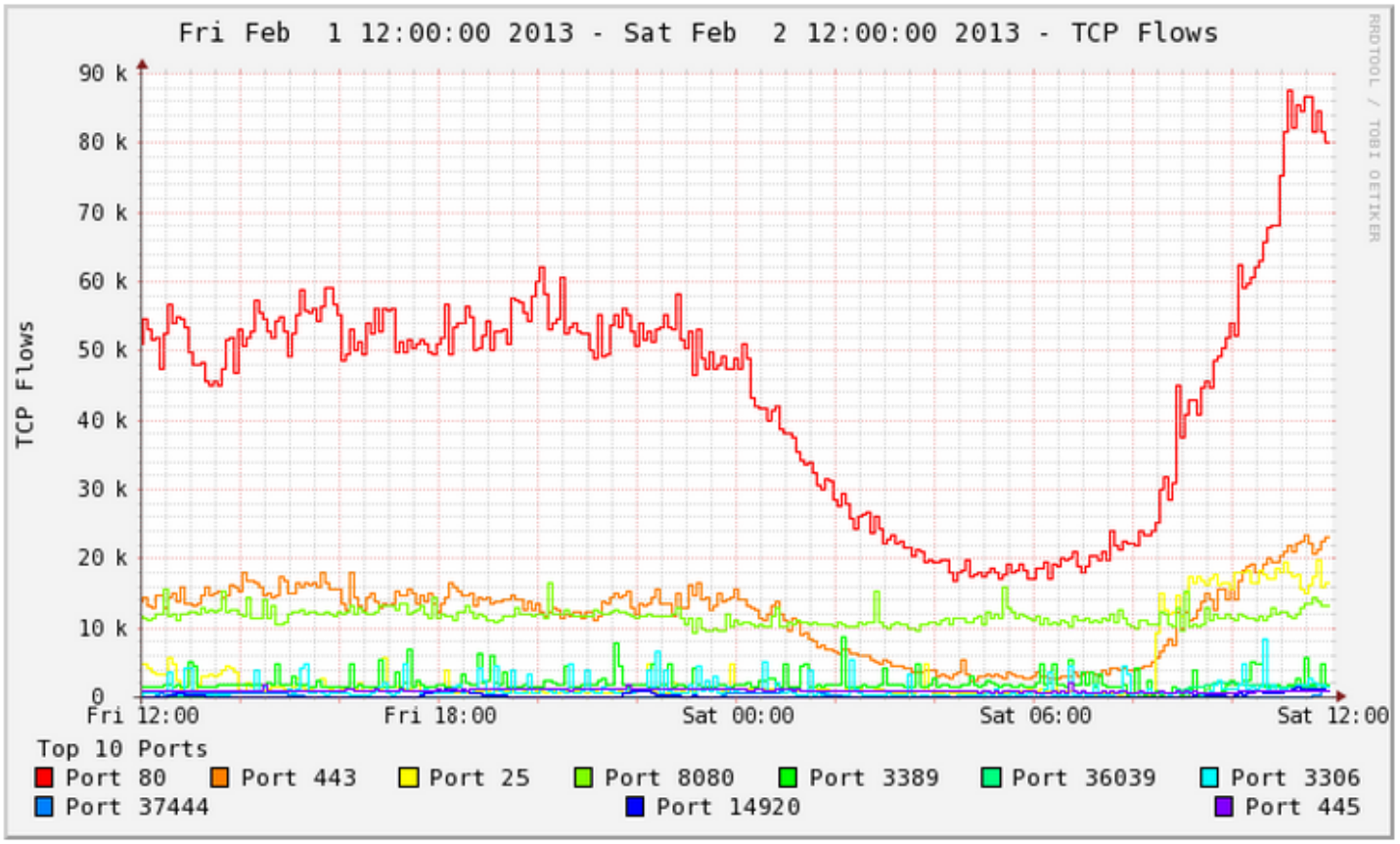
Several plugins available:

- **Portracker** tracks the top 10 most active ports and displays a graph
- **Surfmap** displays country based traffic based on a Geo-Locator

More plugins available here
http://sourceforge.net/apps/trac/nfsen-plugins/

PortTracker

TCP Packets | TCP Bytes | UDP Flows | UDP Packets | UDP Bytes



Show Top 10 Ports

now 24 hours

Track Ports:

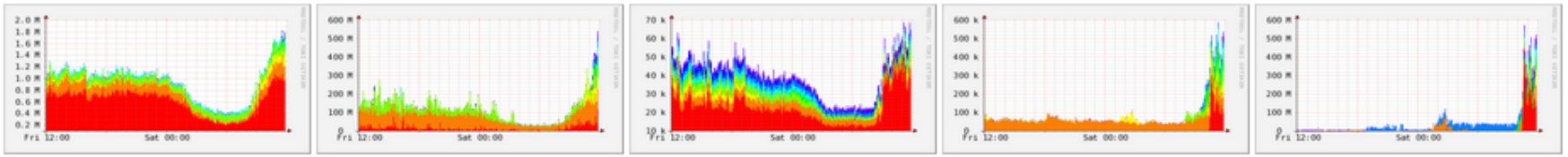
Add Delete

Skip Ports:

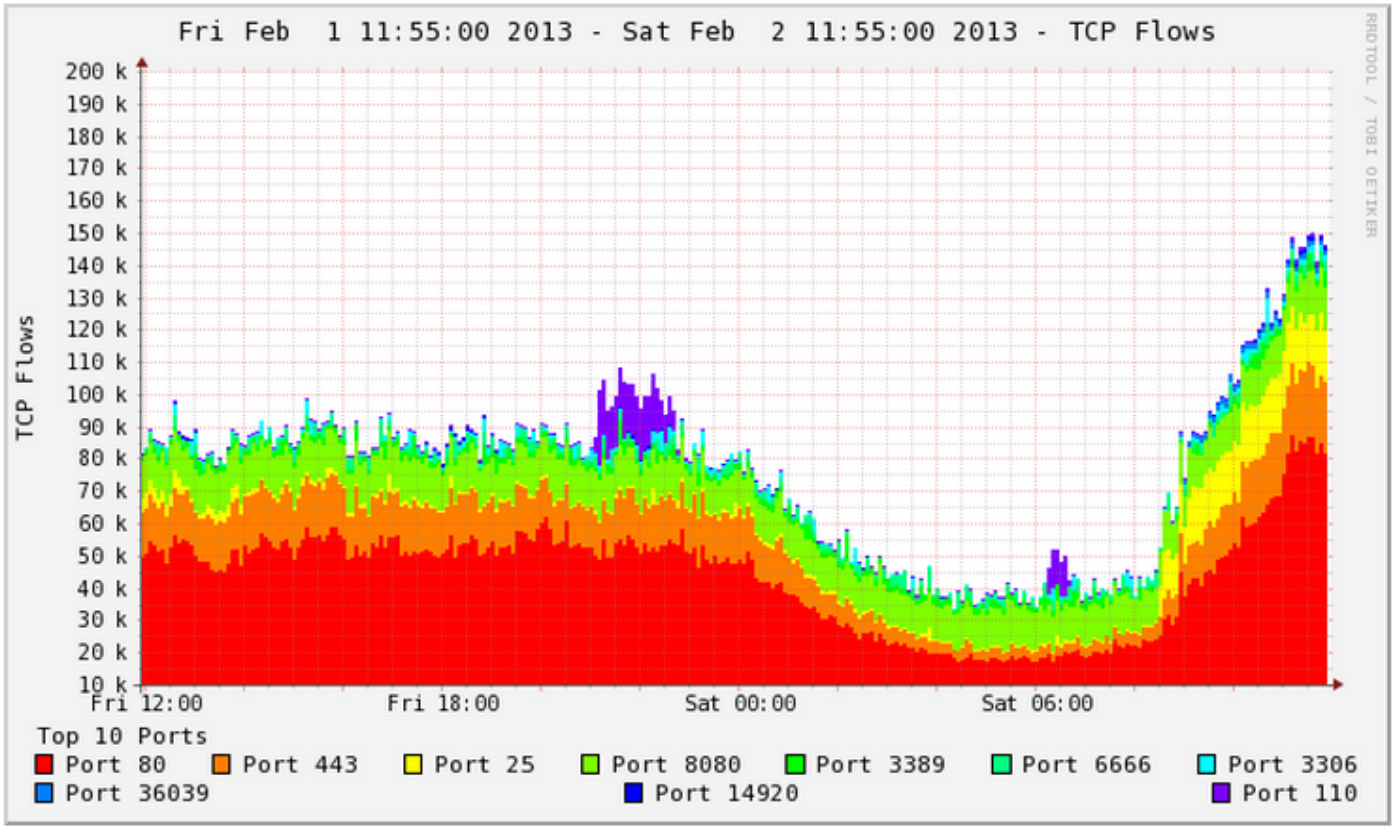
Add Delete

PortTracker

TCP Packets | TCP Bytes | UDP Flows | UDP Packets | UDP Bytes



Show Top 10 Ports



◉ now ○ 24 hours

Track Ports:

Add Delete

Skip Ports:

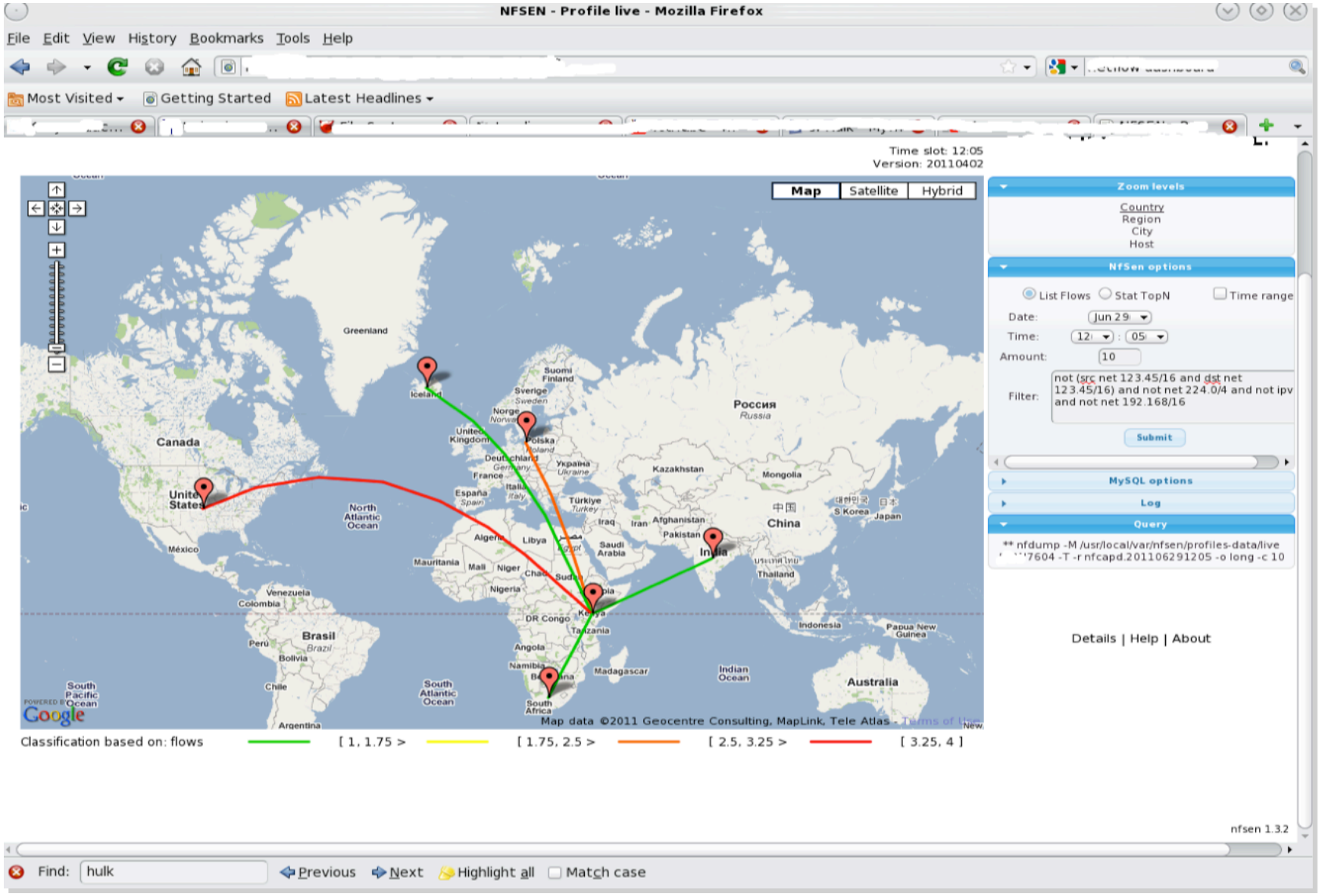
Add Delete

PortTracker

TOP TEN PORTS STATISTICS

	TCP						UDP					
	Flows		Packets		Bytes		Flows		Packets		Bytes	
Rank	Port	Count	Port	Count	Port	Count	Port	Count	Port	Count	Port	Count
1	80	39029	80	570630	80	111021671	53	116671	53	150335	12610	142186426
2	445	27833	25	83140	40936	88004359	6881	2388	12610	99433	28712	101344390
3	135	24572	40936	66203	25	52612168	39792	2276	28712	70901	40493	93146942
4	25	7881	445	53175	55893	43525223	15507	1904	40493	65155	46886	27824516
5	23	6761	135	49066	46395	39079355	43040	1611	15699	46682	57563	26436088
6	3128	4786	55893	37615	2889	30261886	60928	1588	1416	40540	62390	25767022
7	443	2999	46395	35068	1317	24692504	51012	1573	57563	37794	54505	25550351
8	22	2517	22	27489	49674	23472247	61295	1447	34018	37747	55893	23548341
9	9415	1275	443	26468	54311	23342821	5060	1309	21694	24942	40633	22940400
10	**8080**	**1081**	**21651**	**25614**	**44879**	**23306526**	**49665**	**1225**	**46886**	**19468**	**40403**	**19544859**

SurfMap


NFSEN - Profile live - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Most Visited
Getting Started
Latest Headlines
Time slot: 12:05
Version: 20110402
Map
Satellite
Hybrid
Zoom levels
Country
Region
City
Host
NfSen options
List Flows
Stat TopN
Time range
Date:
Jun 29
Time:
Amount:
10
Filter:
not (src net 123.45/16 and dst net 123.45/16) and not net 224.0/4 and not ipv and not net 192.168/16
Submit
MySQL options
Log
Query
** nfdump -M /usr/local/var/nfsen/profiles-data/live
'''7604 -T -r nfcapd.201106291205 -o long -c 10
Details | Help | About
nfsen 1.3.2
Map data ©2011 Geocentre Consulting, MapLink, Tele Atlas
Classification based on: flows
[1, 1.75 >
[1.75, 2.5 >
[2.5, 3.25 >
[3.25, 4]
Find:
hulk
Previous
Next
Highlight all
Match case

When to use NfSen

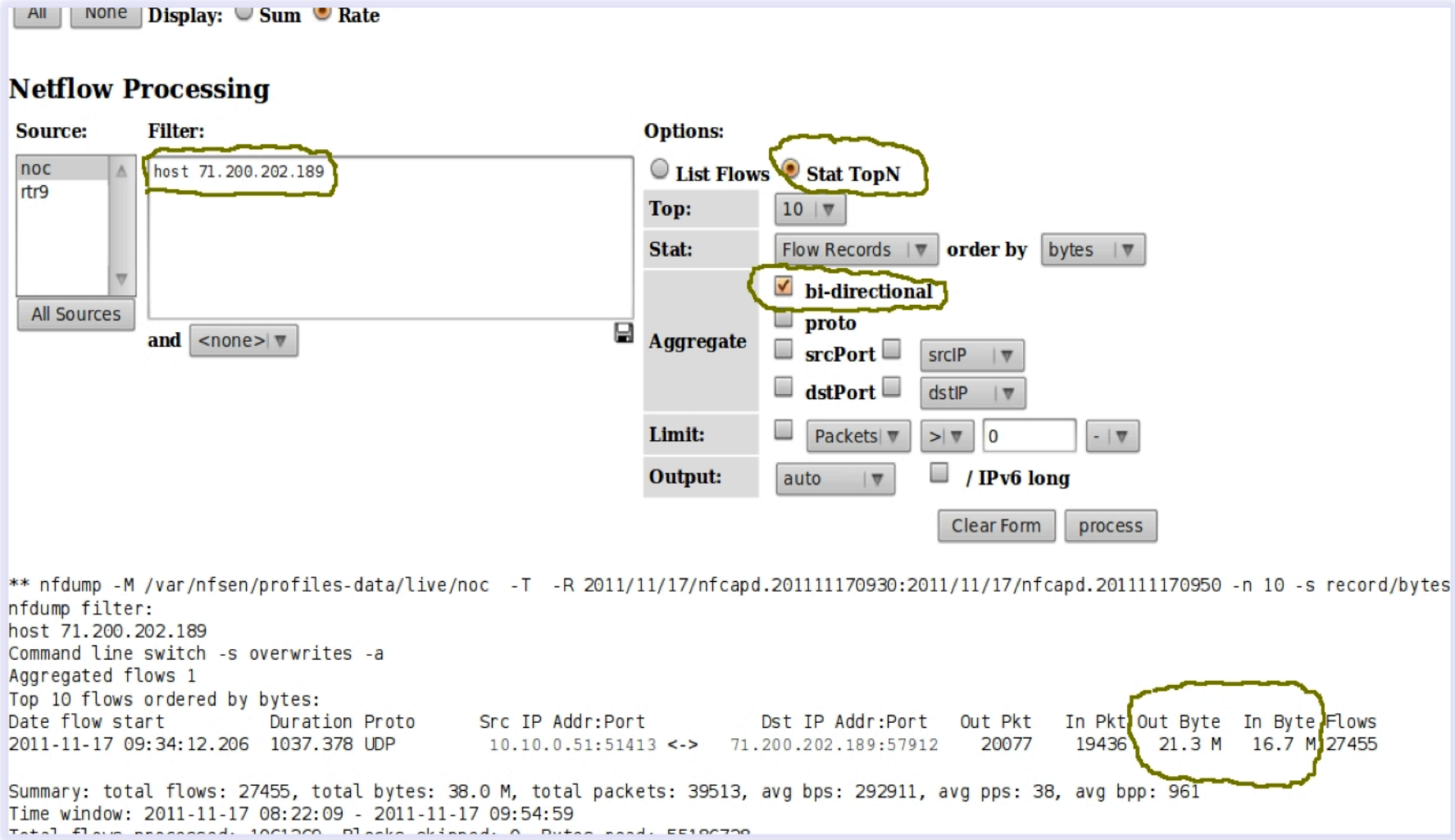
- Can be used for:
  - Forensic work: which hosts were active at a specific time
  - Viewing src/dst AS traffic, src/dst port/IP traffic among many other options
  - Identifying most active IPs or Protocols
- It is a tool to complement Cacti so that you can have more detailed info regarding the traffic
- With this information, you can make an informed decision eg:
  - You have a high amount of SMTP traffic, some machines could be sending out spam
  - 80% of your traffic is to ASN X. Perhaps its wise to connect directly with that network and save costs

Bidirectional vs Unidirectional traffic as seen via NfSen

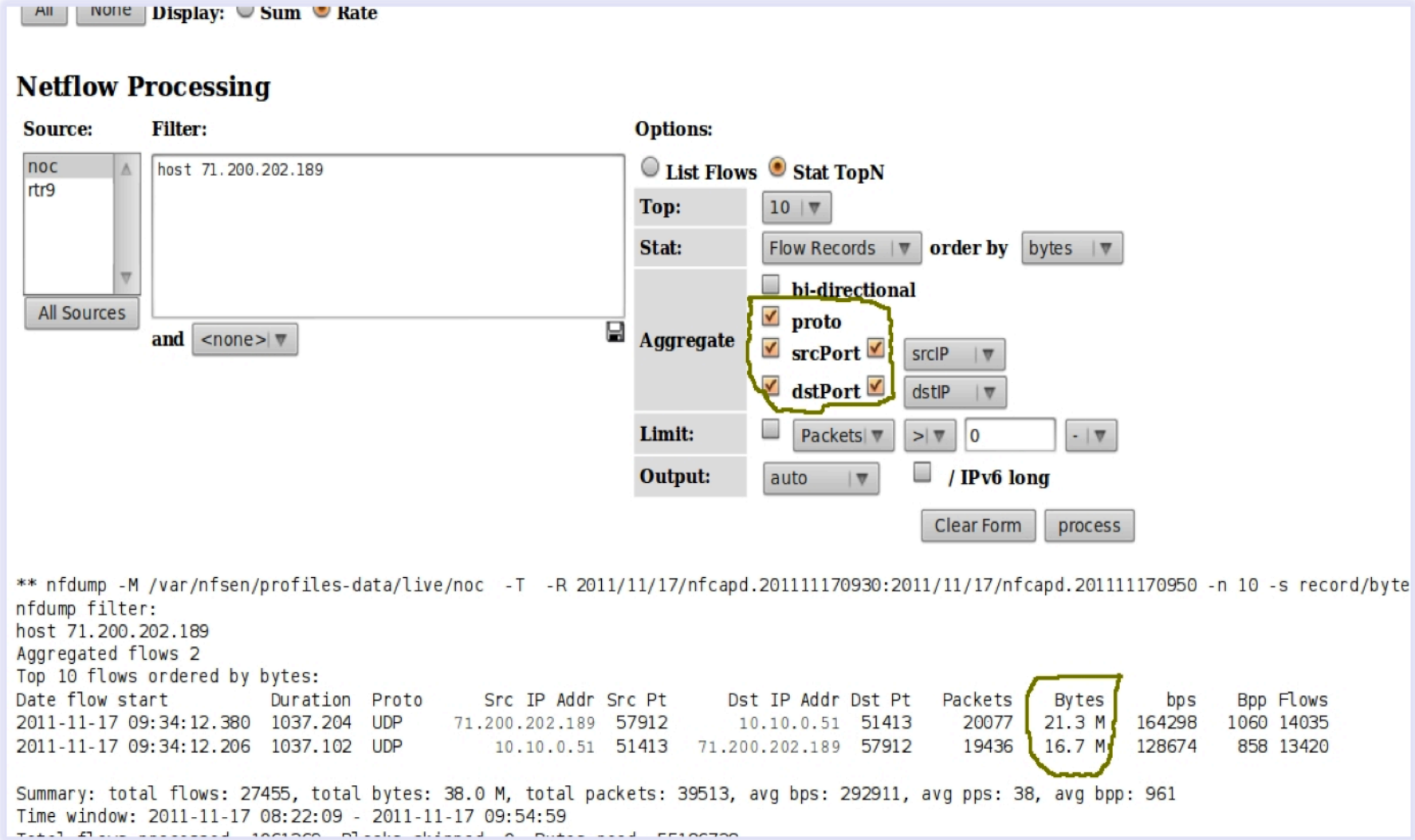
Unidirectional and Bidirectional

- Unidirectional shows flows from host A to B and then host B to host A
- Bidirectional shows flows between Host A and B combined
- Can be used with any of the other filters (src port, src host plus many more)
- List of filters can be found here:
  - http://nfsen.sourceforge.net/#mozTocId652064

Bidirectional



Unidirectional



References

NfSen

http://nfsen.sourceforge.net

NfDump

http://nfdump.sourceforge.net/

Exercises