



Network Management & Monitoring

NfSen



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license
(<http://creativecommons.org/licenses/by-nc/3.0/>)

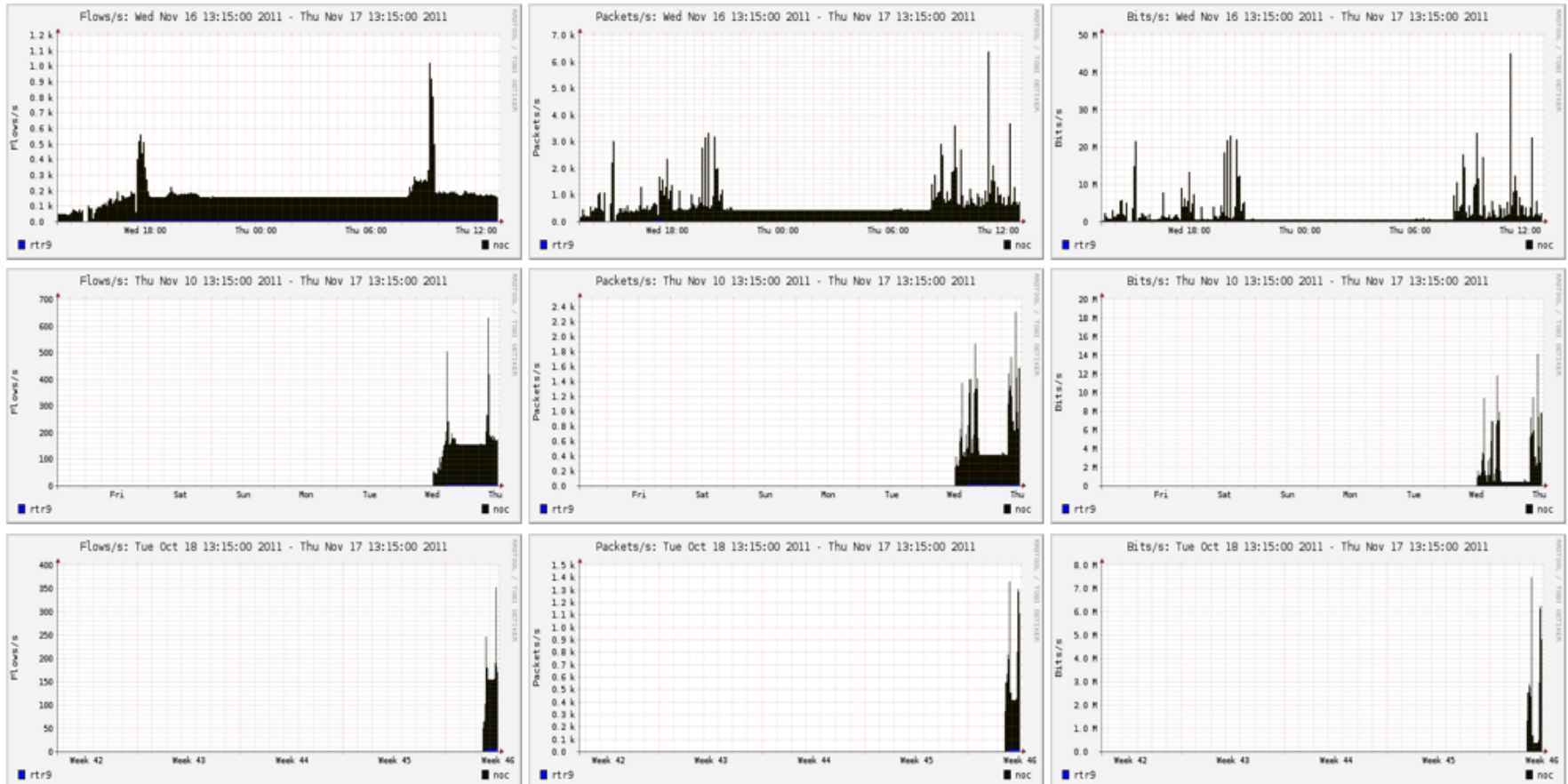
What is NfSen

- Is a graphical 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 Home Screen

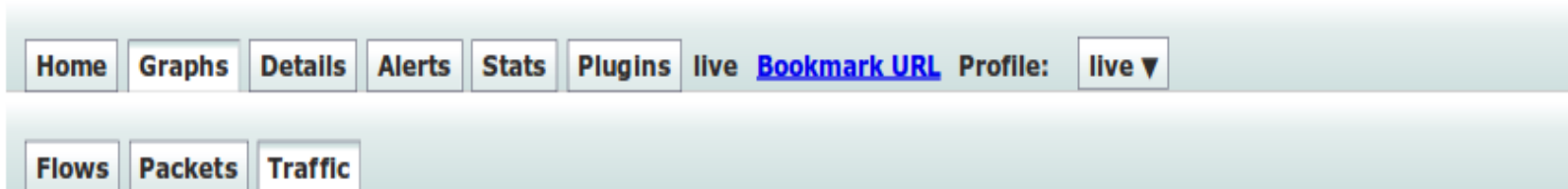
Home Graphs Details Alerts Stats Plugins live [Bookmark URL](#) Profile: live ▼

Overview Profile: live, Group: (nogroup)

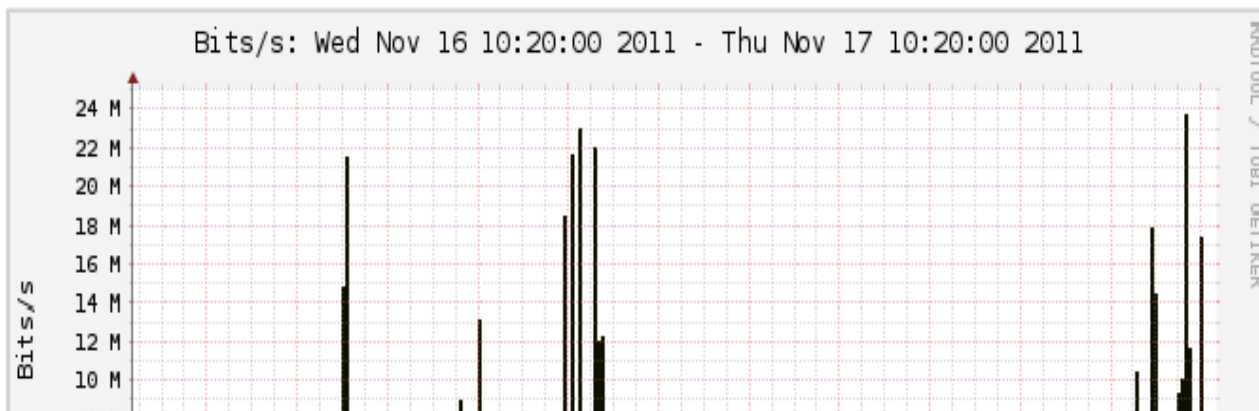


Graphs Tab

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



Profile: live, Group: (nogroup) - traffic

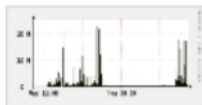


Details Page

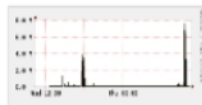
- Most interesting page
- Can view present flow information or stored flow information
- Can view detailed netflow information such as
 - AS Numbers (more useful if you have full routing table exported on your router)
 - Src hosts/ports, destination hosts and ports
 - Unidirectional or Bi-directional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

Profile: live

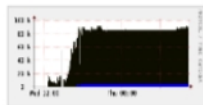
TCP



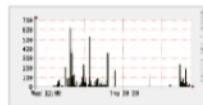
UDP



ICMP



other



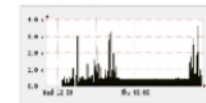
Profileinfo:

Type: live
Max: unlimited
Exp: never
Start: Nov 16 2011 - 12:10 UTC
End: Nov 17 2011 - 10:25 UTC

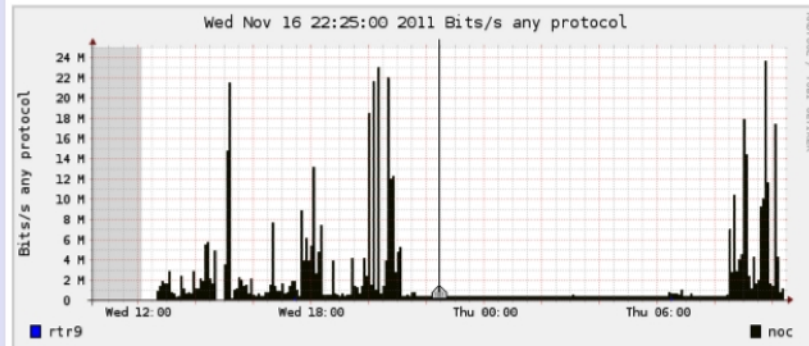
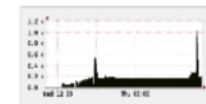
t_start 2011-11-16-22-25

t_end 2011-11-16-22-25

Packets



Flows



Select Display:

☒ Lin Scale ☒ Stacked Graph
☐ Log Scale ☐ Line Graph

Statistics timeslot Nov 16 2011 - 22:25

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
<input checked="" type="checkbox"/> 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
<input checked="" type="checkbox"/> 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

Display: ☐ Sum ☒ Rate

Netflow Processing

Source:

noc
rtr9

Filter:

and

Options:

☐ List Flows ☒ Stat TopN

Top:

Stat: order by

Limit: ☐ Packets

Output: ☐ / IPv6 long

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

History/Past Flows

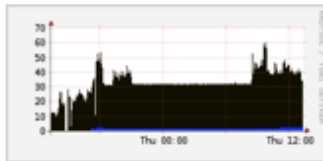
- Can be used for forensic work
- Displays flow transactions based on specific time, time selected by working with time window graph
- Can view unidirectional or bidirectional flows
- Can sort by top flows, src AS, dst port among many other options

Time Window

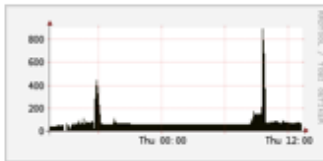
[Home](#)[Graphs](#)[Details](#)[Alerts](#)[Stats](#)[Plugins](#)[live](#)[Bookmark URL](#)[Profile:](#)[live ▼](#)

Profile: live

TCP



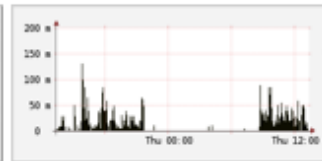
UDP



ICMP



other



Profileinfo:

Type: live

Max: unlimited

Exp: never

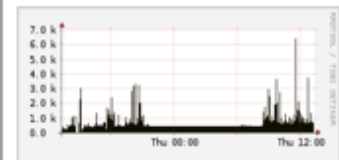
Start: Nov 16 2011 - 12:10 UTC

End: Nov 17 2011 - 13:20 UTC

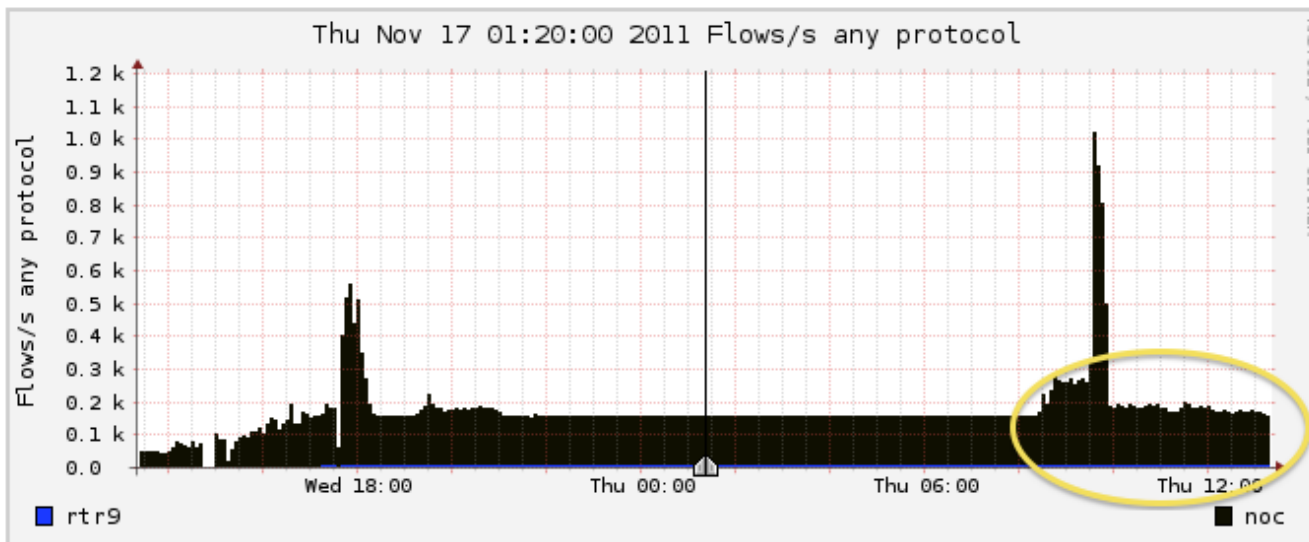
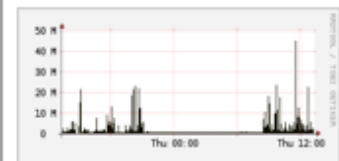
t_start 2011-11-17-01-20

t_end 2011-11-17-01-20

Packets



Traffic



Select Time Window

Display: 1 day

☒ Lin Scale ☒ Stacked Graph

☐ Log Scale ☐ Line Graph

Bidirectional vs Unidirectional

Bidirectional

All None Display: ☐ Sum ☒ Rate

Netflow Processing

Source:

noc
rtr9
All Sources

Filter:

host 71.200.202.189

and <none>

Options:

☐ List Flows

☒ Stat TopN

Top:

10

Stat:

Flow Records

order by

bytes

☒ bi-directional

Aggregate

☐ proto

☐ srcPort

srcIP

☐ dstPort

dstIP

Limit:

☐ Packets

> 0

Output:

auto

☐ / IPv6 long

Clear Form

process

```
** nfdump -M /var/nfsen/profiles-data/live/noc -T -R 2011/11/17/nfcapd.201111170930:2011/11/17/nfcapd.201111170950 -n 10 -s record/bytes
```

```
nfdump filter:
```

```
host 71.200.202.189
```

```
Command line switch -s overwrites -a
```

```
Aggregated flows 1
```

```
Top 10 flows ordered by bytes:
```

Date flow start	Duration	Proto	Src IP Addr:Port	Dst IP Addr:Port	Out Pkt	In Pkt	Out Byte	In Byte	Flows
2011-11-17 09:34:12.206	1037.378	UDP	10.10.0.51:51413 <->	71.200.202.189:57912	20077	19436	21.3 M	16.7 M	27455

```
Summary: total flows: 27455, total bytes: 38.0 M, total packets: 39513, avg bps: 292911, avg pps: 38, avg bpp: 961
```

```
Time window: 2011-11-17 08:22:09 - 2011-11-17 09:54:59
```

```
Total flows processed: 1061360, Blocks skipped: 0, Bytes read: 55186738
```

Unidirectional

All None Display: ☐ Sum ☒ Rate

Netflow Processing

Source:
noc
rtr9
All Sources

Filter:
host 71.200.202.189
and <none>

Options:
☐ List Flows ☒ Stat TopN
Top: 10
Stat: Flow Records order by bytes
☐ bi-directional
Aggregate ☒ proto ☒ srcPort ☒ dstPort
Limit: ☐ Packets > 0
Output: auto ☐ / IPv6 long
Clear Form process

```
** nfdump -M /var/nfsen/profiles-data/live/noc -T -R 2011/11/17/nfcapd.201111170930:2011/11/17/nfcapd.201111170950 -n 10 -s record/byte
nfdump filter:
host 71.200.202.189
Aggregated flows 2
Top 10 flows ordered by bytes:
Date flow start      Duration  Proto    Src IP Addr Src Pt    Dst IP Addr Dst Pt    Packets  Bytes    bps    Bpp Flows
2011-11-17 09:34:12.380 1037.204  UDP      71.200.202.189 57912    10.10.0.51 51413    20077    21.3 M    164298 1060 14035
2011-11-17 09:34:12.206 1037.102  UDP      10.10.0.51 51413    71.200.202.189 57912    19436    16.7 M    128674 858 13420

Summary: total flows: 27455, total bytes: 38.0 M, total packets: 39513, avg bps: 292911, avg pps: 38, avg bpp: 961
Time window: 2011-11-17 08:22:09 - 2011-11-17 09:54:59
Total flows processed: 1061260, flows skipped: 0, bytes read: 55186700
```

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>

Graphing Specific Traffic Flows

Creating Stats

- Click on live on the top left and select new profile
- Enter a name for the profile and additionally create a new group
- Select individual channels and shadow profile.
 - Individual channel – can create channels with own filters
 - Shadow profile – save hard disk space by not creating new data but instead analyses already collected data

Profile:	<input type="text" value="Troublesome_User"/>	?
Group:	<div><div>New group ... ▼</div><div>Hosts</div></div>	?
Description:	<div></div>	
Start:	<div><input type="text"/><div>Format: yyyy-mm-dd-HH-MM</div></div>	?
End:	<div><input type="text"/><div>Format: yyyy-mm-dd-HH-MM</div></div>	?
Max. Size:	<input type="text" value="0"/>	?
Expire:	<input type="text" value="never"/>	?
Channels:	<div><div><input type="radio"/> 1:1 channels from profile live</div><div><input checked="" type="radio"/> individual channels</div></div>	?
Type:	<div><div><input type="radio"/> Real Profile</div><div><input checked="" type="radio"/> Shadow Profile</div></div>	?
<div><div>Cancel</div><div>Create Profile</div></div>		

- When done click on 'Create Profile' at the bottom
- You will see a message “new profile created”
- Then click on the plus sign at the bottom to begin adding channels

Add a Channel

Home Graphs Details Alerts Stats Plugins continuous / shadow [Bookmark URL](#) Pr

Channel name		<input type="text" value="User1"/>	
Colour:	Enter new value	<input type="text" value="#abcdef"/> or	
		<input type="button" value="Select a colour from"/> ▼	
Sign:	<input type="button" value="+"/> ▼	Order:	<input type="button" value="1"/> ▼
Filter:	<input type="text" value="host 10.10.0.51"/>		
Sources:	Available Sources		Selected Sources
	<div><div>rtr9</div><div></div></div>		<div><div>noc</div><div></div></div>
		<input type="button" value=" <<"/>	<input type="button" value=" >>"/>
<input type="button" value="Cancel"/>		<input type="button" value="Add Channel"/>	


Add a second channel and start to accept


Last Update: 2011-11-17-11-03


Size: 0 B

Max. Size: unlimited

Expire: never

Status: new 

▼ Channel List: 

▼ User1 

Colour: #abcdef Sign: + Order: 1

Filter: host 10.10.0.51

Sources: noc

Home Graphs Details Alerts Stats Plugins continuous / shadow !

Channel name User2

Colour: Enter new value #FF0000 or Select a colour from ▼

Sign: + | ▼ Order: 2 | ▼

Filter: dst host 10.10.0.139

Sources:

Available Sources: rtr9

Selected Sources: noc

<< >>

Cancel Add Channel


Filters

- Select a different color for the second channel so that the graphs can be distinguished
- Note that the two filters are different
 - The first filter will capture any flows pertaining to host 10.10.0.51
 - The second filter will only capture flows where host 10.10.0.139 is the DESTINATION host
- More attributes can be added here like src AS, dst AS, src ports etc based on the NFSEN filter syntax

Activate the profile

Start:	2011-11-17-11-10
End:	2011-11-17-11-10
Last Update:	2011-11-17-11-05
Size:	0 B
Max. Size:	unlimited
Expire:	never
Status:	new

▼ Channel List: +

▼ User2 

Colour:	#FF0000	Sign:	+	Order:	2
---------	---------	-------	---	--------	---

Filter: dst host 10.10.0.139

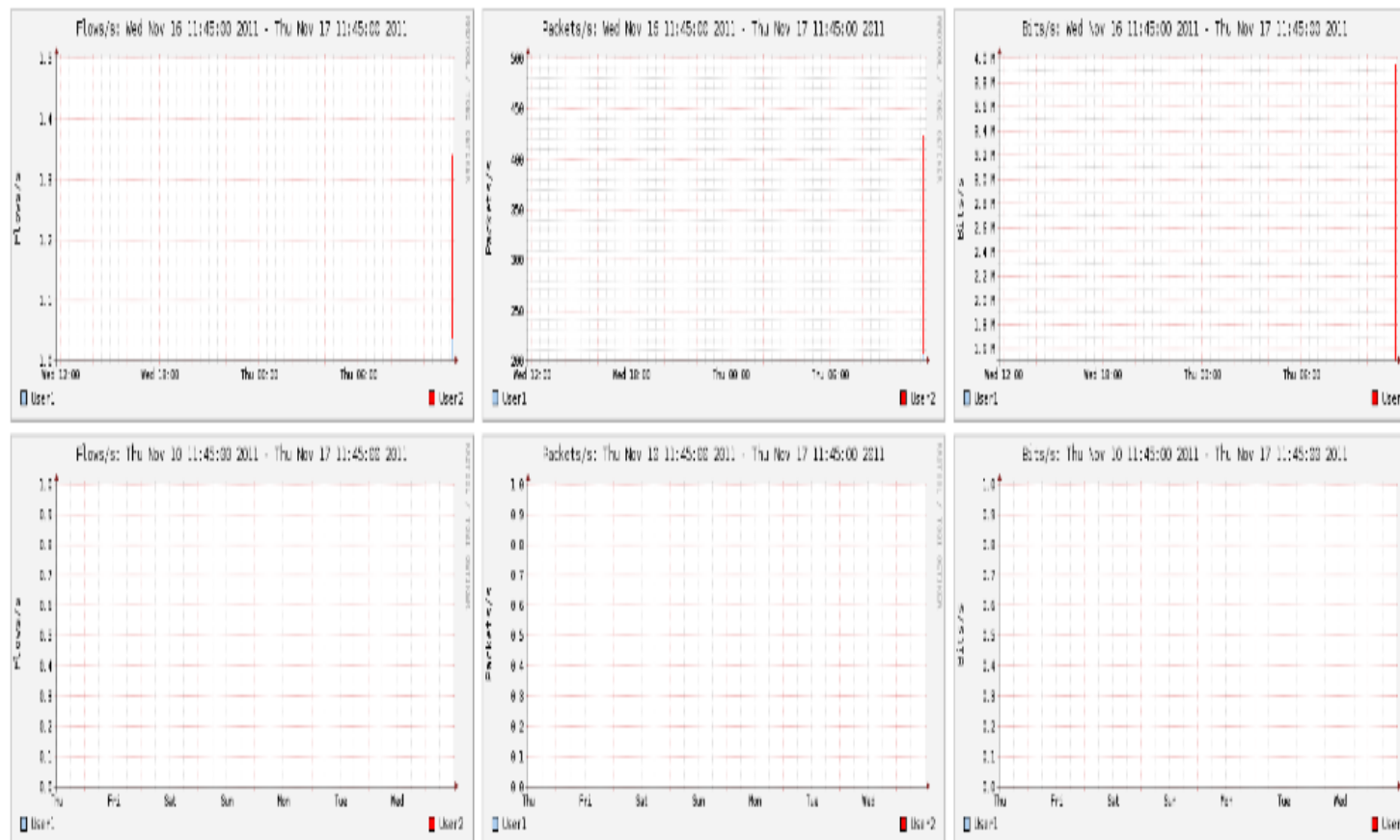
- Click the green tick to activate your new profile.
- It will display some data after a few minutes
- Click on Live then select the group you created and you will see your profile

[Home](#)[Graphs](#)[Details](#)[Alerts](#)[Stats](#)[Plugins](#)[continuous / shadow](#)[Bookmark URL](#)

Profile:

Troublesome_User ▼

Overview Profile: Troublesome_User, Group Hosts



Details Page of New Profile

Only information on the channels is shown
in new profile

Clear Form process

```
** nfdump -M /var/nfsen/profiles-data/live/noc -T -r 2011/11/17/nfcapd.201111171145 -n 100 -s record/bytes -A proto,srcip,srcport,dstip,dstport
nfdump filter:
(( ident noc) and (
dst host 10.10.0.139
)
or
( ident noc) and (
host 10.10.0.51
))
Aggregated flows 368
```

Top 100 flows ordered by bytes:

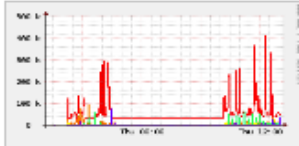
Date flow start	Duration	Proto	Src IP Addr	Src Pt	Dst IP Addr	Dst Pt	Packets	Bytes	bps	Bpp	Flows
2011-11-17 11:26:53.320	1267.891	TCP	88.221.216.85	1935	10.10.0.139	2708	60660	86.0 M	542683	1417	1
2011-11-17 11:40:59.711	358.735	TCP	208.117.245.85	80	10.10.0.51	54280	36427	51.5 M	1.1 M	1413	1
2011-11-17 11:47:53.862	39.907	TCP	92.122.49.172	1935	10.10.0.139	2809	3931	5.5 M	1.1 M	1407	1
2011-11-17 11:45:07.917	14.783	TCP	92.52.113.98	80	10.10.0.51	54342	937	1.3 M	714811	1409	1
2011-11-17 11:40:59.711	358.735	TCP	10.10.0.51	54280	208.117.245.85	80	20555	1.1 M	24251	52	1
2011-11-17 11:48:08.300	43.260	TCP	74.125.230.72	80	10.10.0.51	54417	320	415126	76768	1297	1
2011-11-17 11:48:28.045	22.127	TCP	74.125.230.72	80	10.10.0.51	54456	192	251166	90808	1308	1
2011-11-17 11:48:08.438	43.062	TCP	74.125.230.72	80	10.10.0.51	54422	190	242861	45118	1278	1
2011-11-17 11:45:28.792	11.086	TCP	92.52.113.98	80	10.10.0.51	54367	168	223214	161078	1328	2
2011-11-17 11:45:28.660	2.481	TCP	92.52.113.98	80	10.10.0.51	54366	133	180549	582181	1357	1
2011-11-17 11:48:08.302	21.538	TCP	74.125.230.72	80	10.10.0.51	54418	89	110256	40953	1238	1
2011-11-17 11:45:34.394	117.259	TCP	173.194.67.120	80	10.10.0.51	54374	71	89405	6099	1259	1

PortTracker

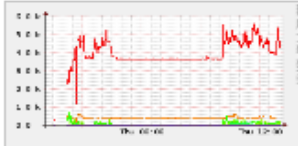
PortTracker

Port Tracker

TCP Packets



TCP Flows



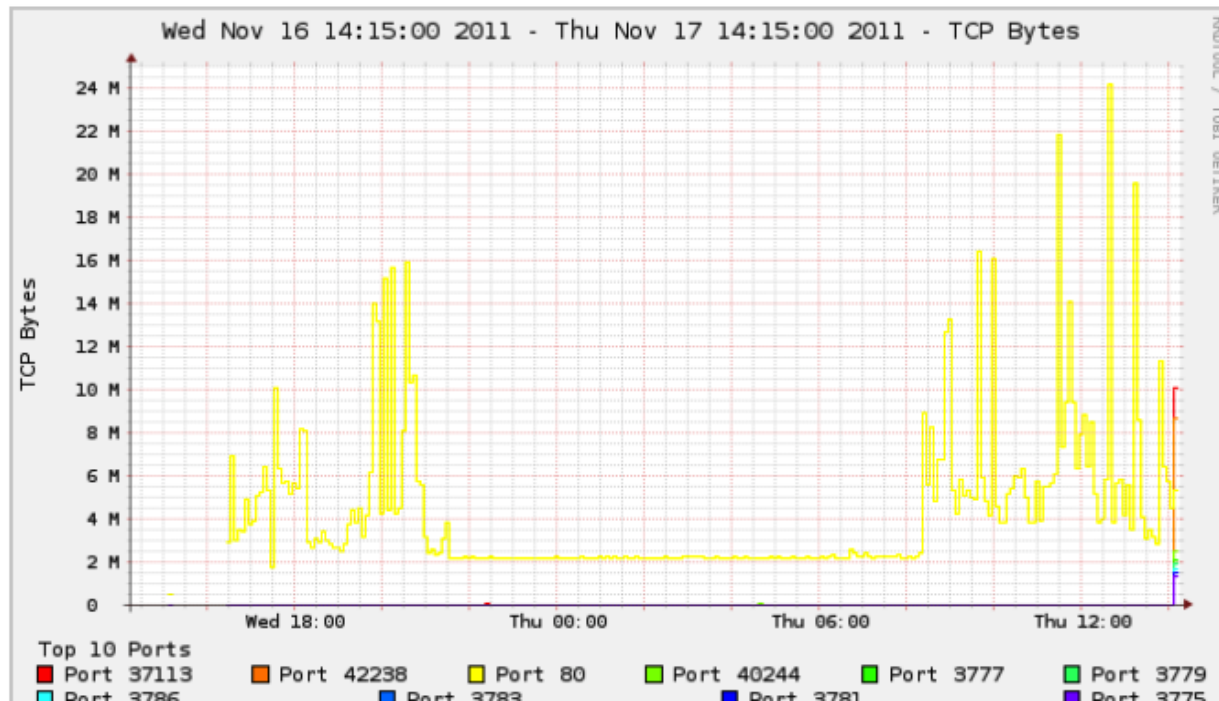
UDP Flows



UDP Packets



UDP Bytes



Show Top Ports

☒ now ☐ 24 hours

Track Ports:

Add

Delete

Skip Ports:

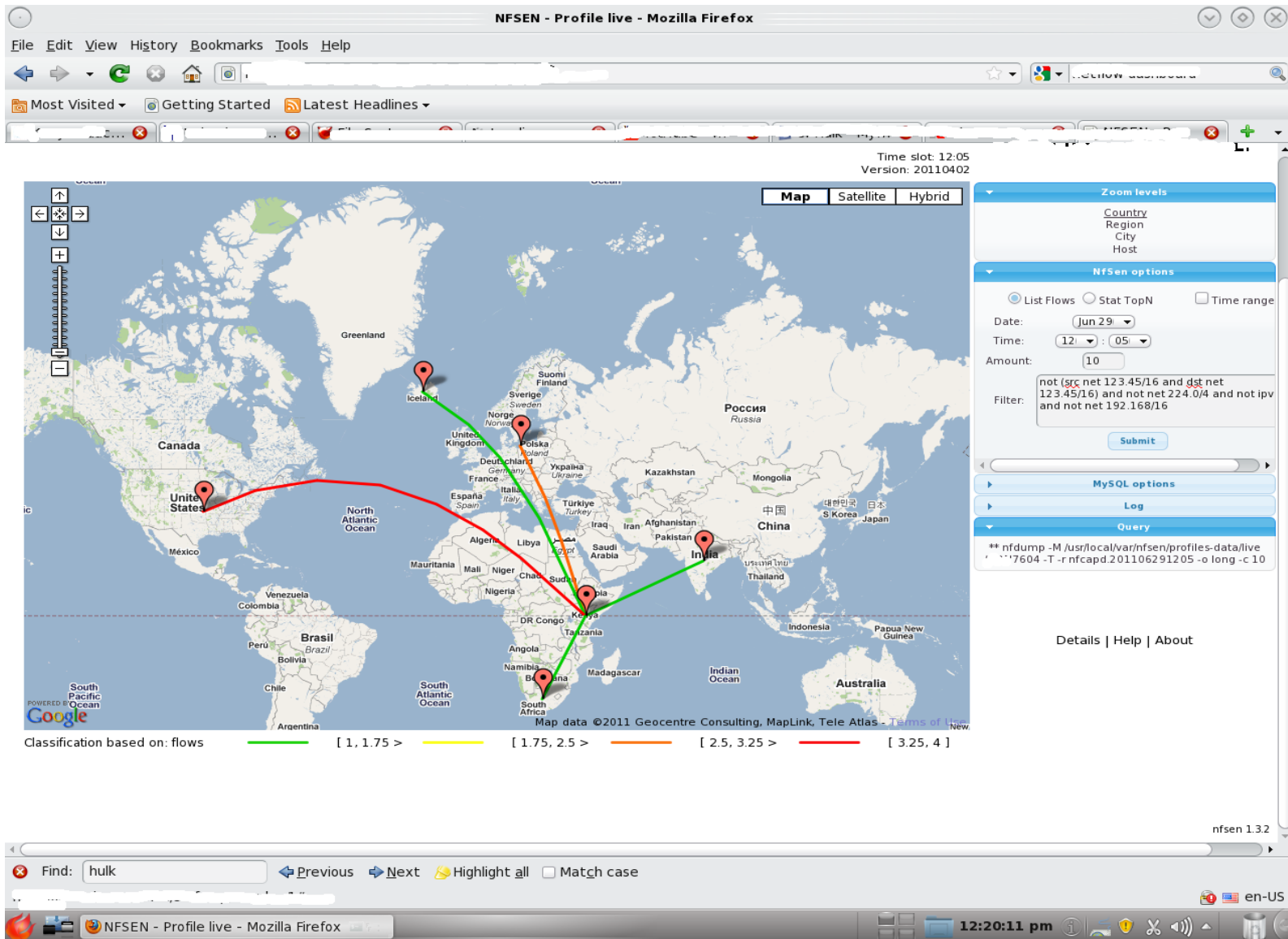
Add

Delete

Plugins

- Several plugins available
- Porttracker 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/>

SurfMap



References

NFSEN

<http://nfsen.sourceforge.net>

NFDUMP

<http://nfdump.sourceforge.net/>