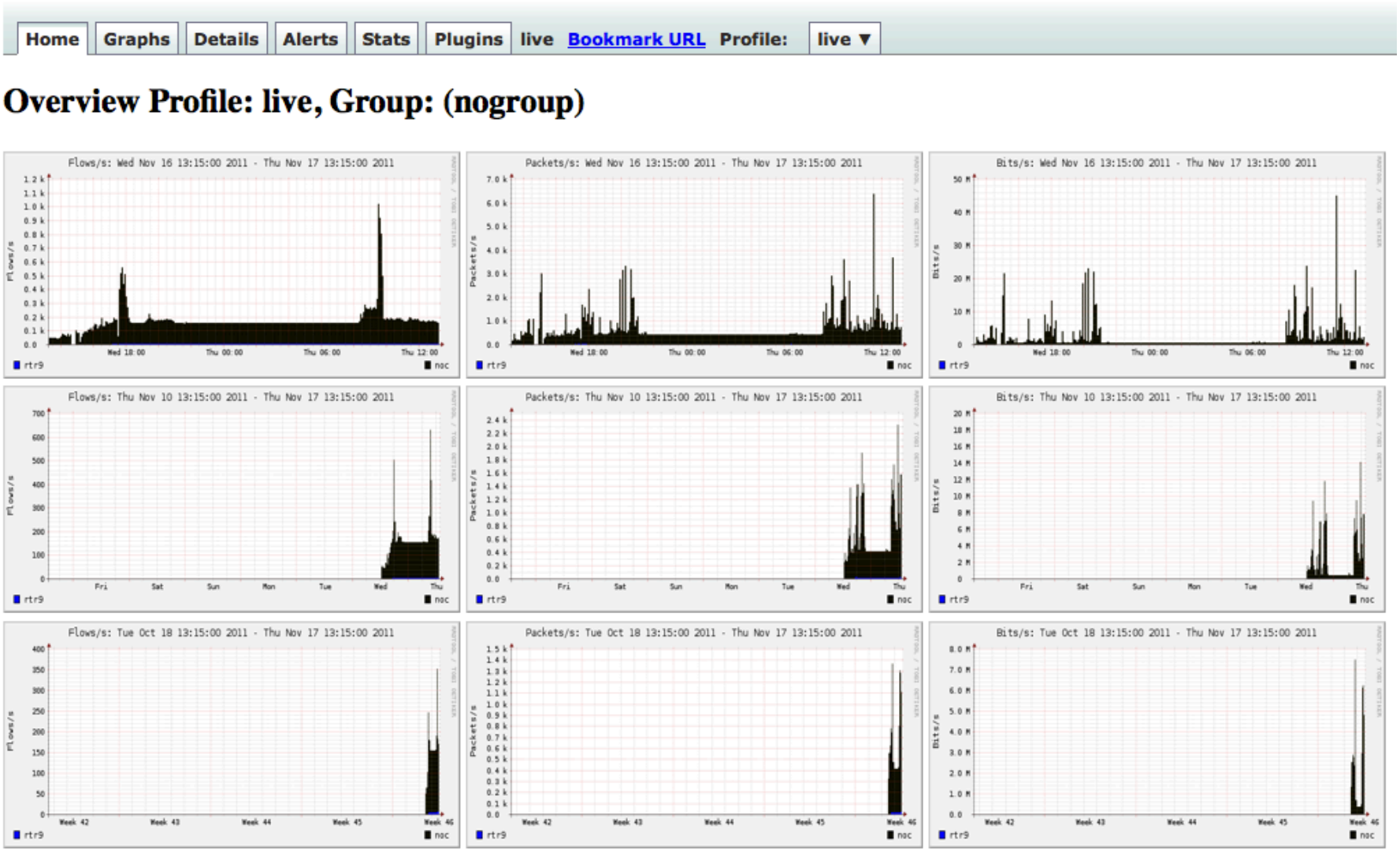

# Network Management & Monitoring

## NfSen

# 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.

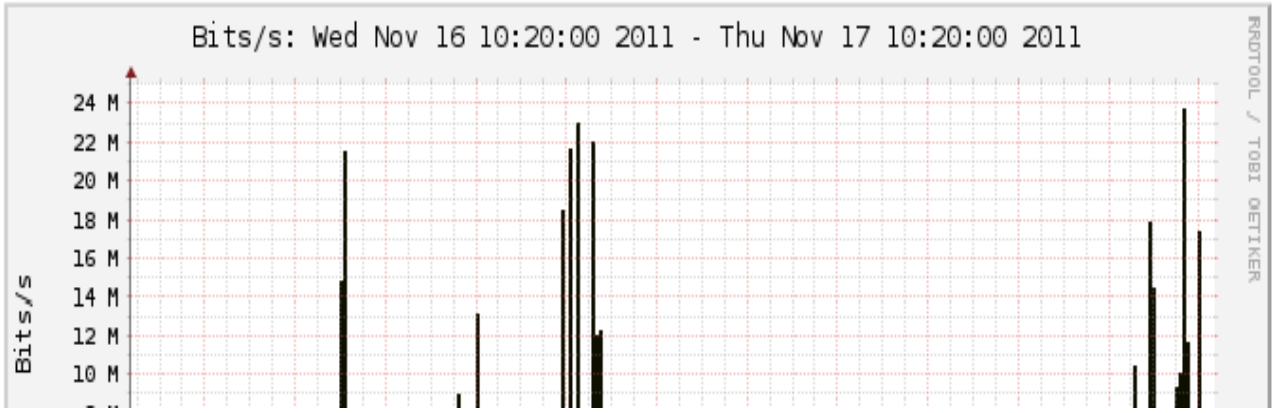
# NfSen Home Screen



# Graphs Tab

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


**Profile: live, Group: (nogroup) - traffic**



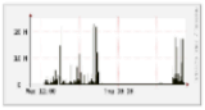
# Details Page

- 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

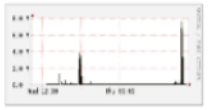
Home | Graphs | Details | Alerts | Stats | Plugins | live | Bookmark URL | Profile: | live ▼

## Profile: live

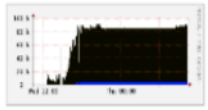
**TCP**



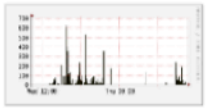
**UDP**



**ICMP**

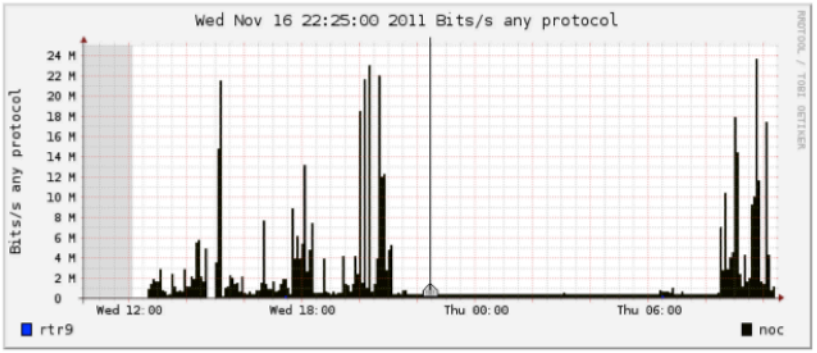


**other**



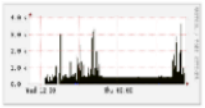
**Profileinfo:**

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

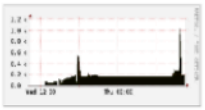



$t_{start}$ **2011-11-16-22-25**
$t_{end}$ **2011-11-16-22-25**

**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: | all: | tcp: | udp: | icmp: | other: | 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:**

noc
rtr9

All Sources

**Filter:**

**and** <none> ▼

**Options:**

○ List Flows ◉ Stat TopN

**Top:** 10 ▼

**Stat:** Any IP Address ▼ **order by** flows ▼

**Limit:** ☐ Packets ▼ >| ▼ 0 - ▼

**Output:** ☐ / IPv6 long

Clear Form | process

# 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

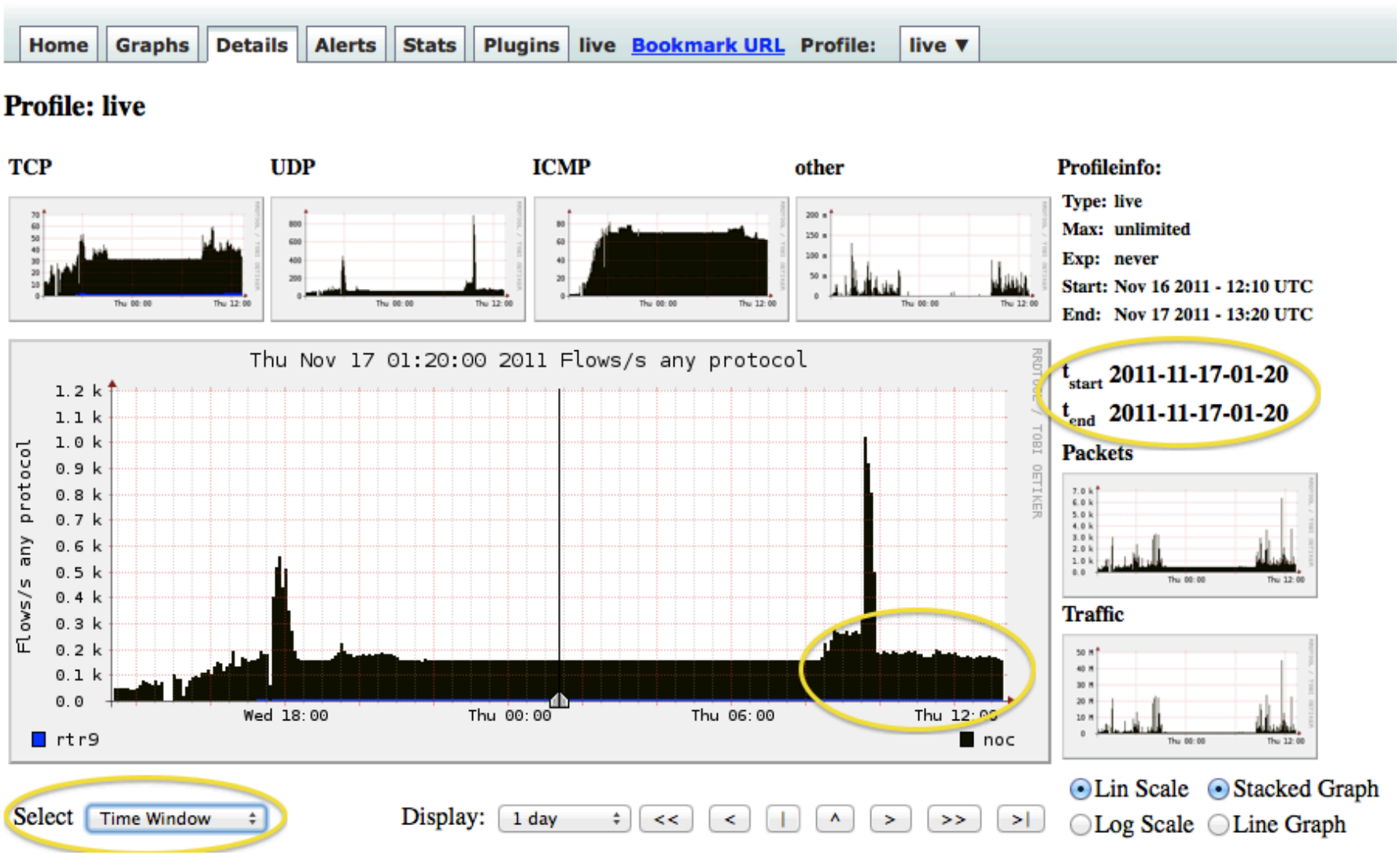
## Stats page

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

# History/Past Flows

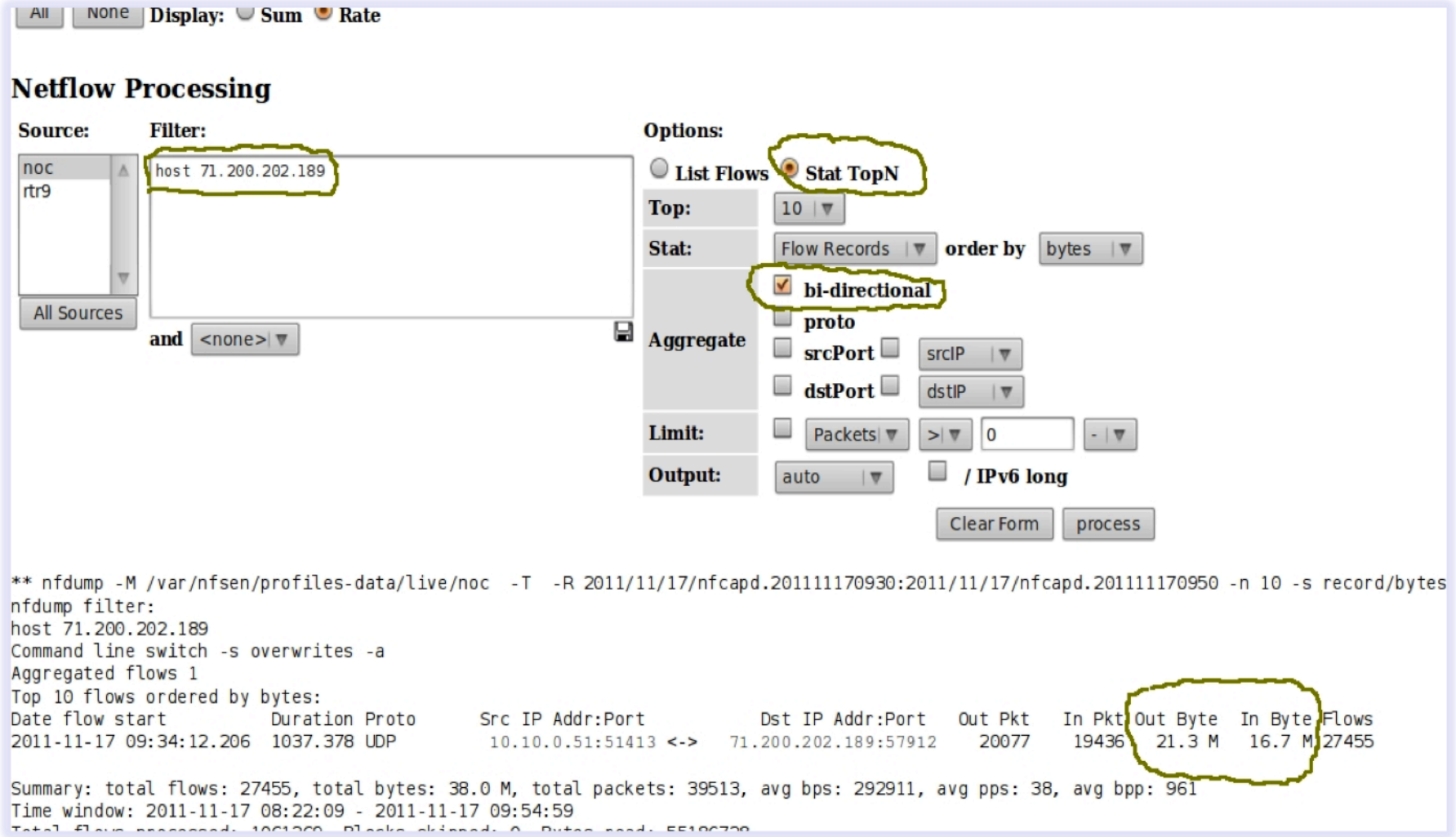
- Can be used for forensic work
- Displays flow transactions based on specific time, time selected by working with time window graph
- Can view unidirectional or bidirectional flows
- Can sort by top flows, src AS, dst port among many other options

# Time Window

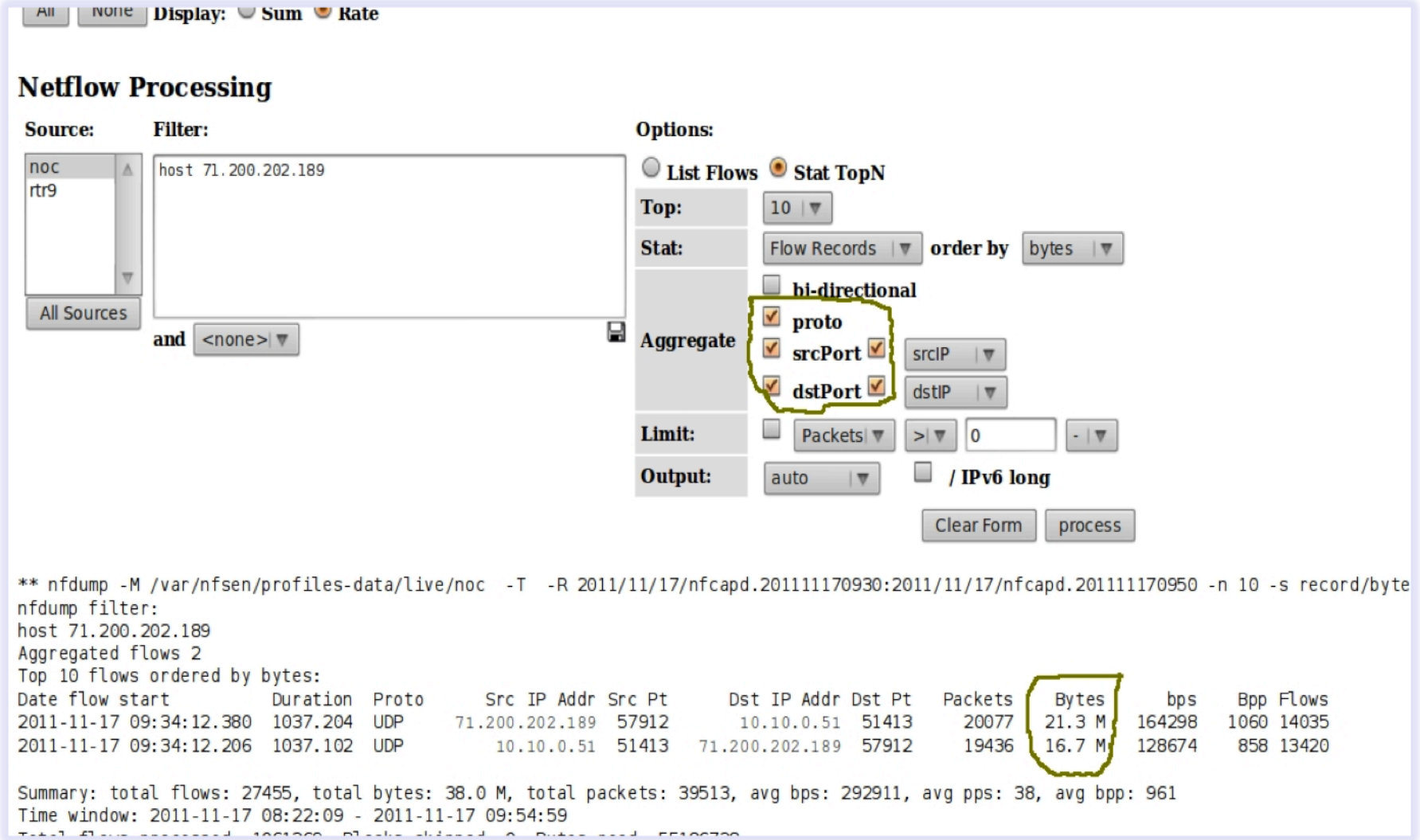

Home
Graphs
Details
Alerts
Stats
Plugins
live
Bookmark URL
Profile:
live ▼
Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Type: live
Max: unlimited
Exp: never
Start: Nov 16 2011 - 12:10 UTC
End: Nov 17 2011 - 13:20 UTC
Thu Nov 17 01:20:00 2011 Flows/s any protocol
Flows/s any protocol
1.2 k
1.1 k
1.0 k
0.9 k
0.8 k
0.7 k
0.6 k
0.5 k
0.4 k
0.3 k
0.2 k
0.1 k
0.0
Wed 18:00
Thu 00:00
Thu 06:00
Thu 12:00
rtr9
noc
RRDTOOL / TOBI OETIKER
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



# Unidirectional



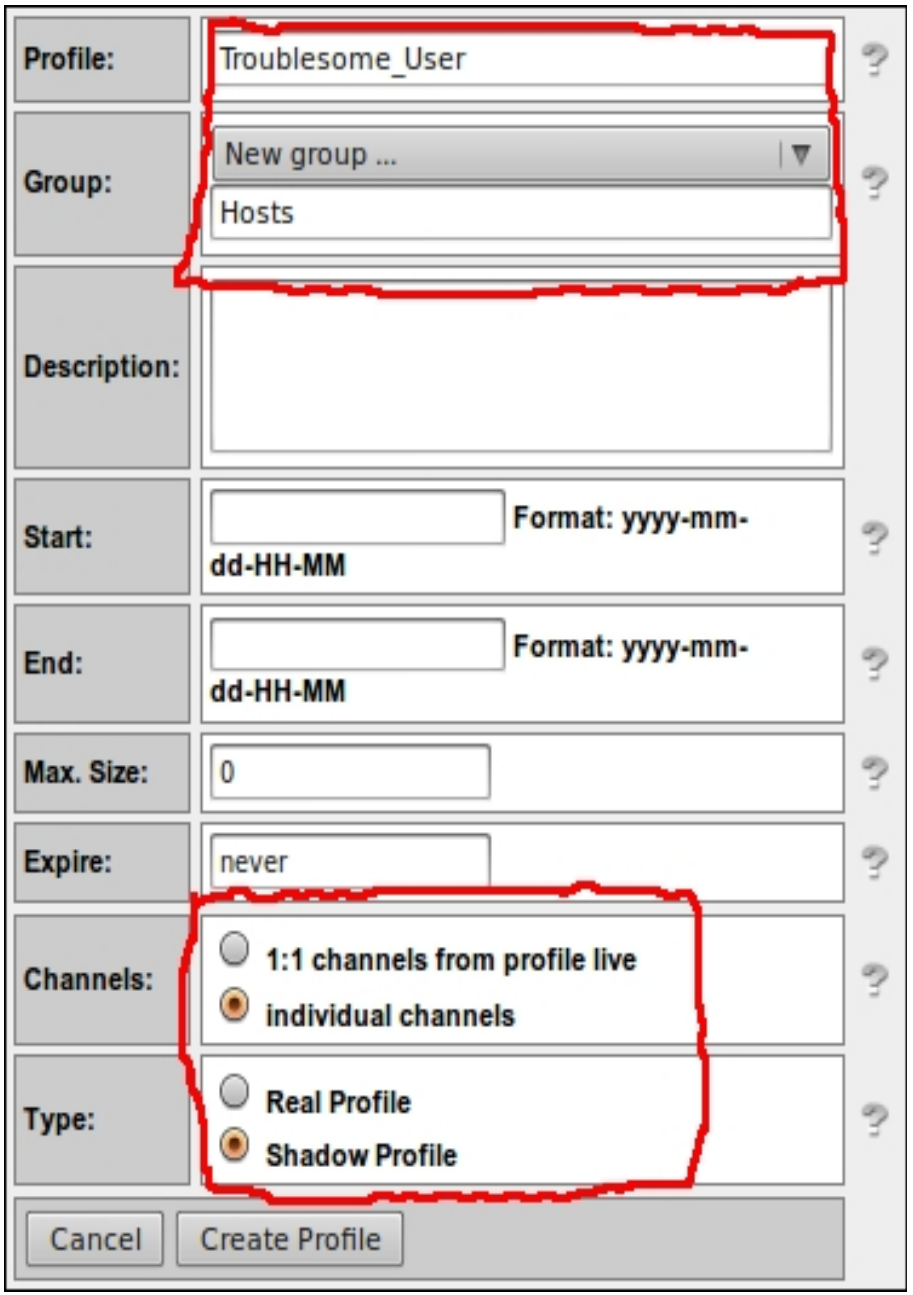
# Unidirectional and Bidirectional

- 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

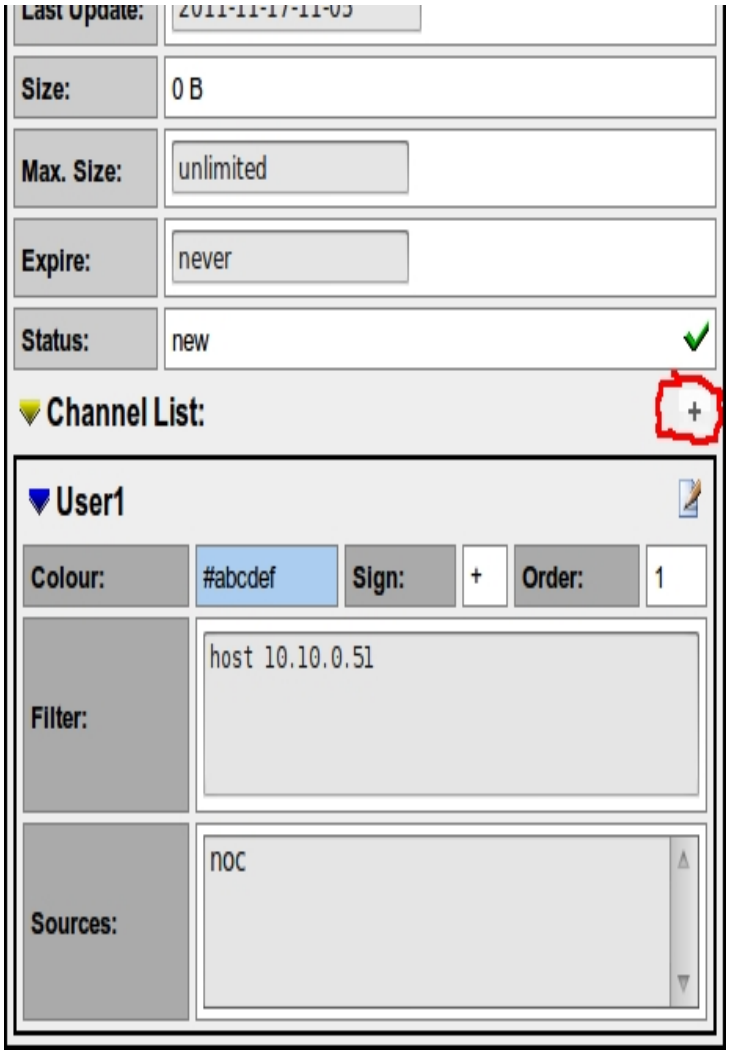
- Click on live on the top left and select new profile
- Enter a name for the profile and additionally create a new group
- Select individual channels and shadow profile.
  - Individual channel – can create channels with own filters
  - Shadow profile – save hard disk space by not creating new data but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

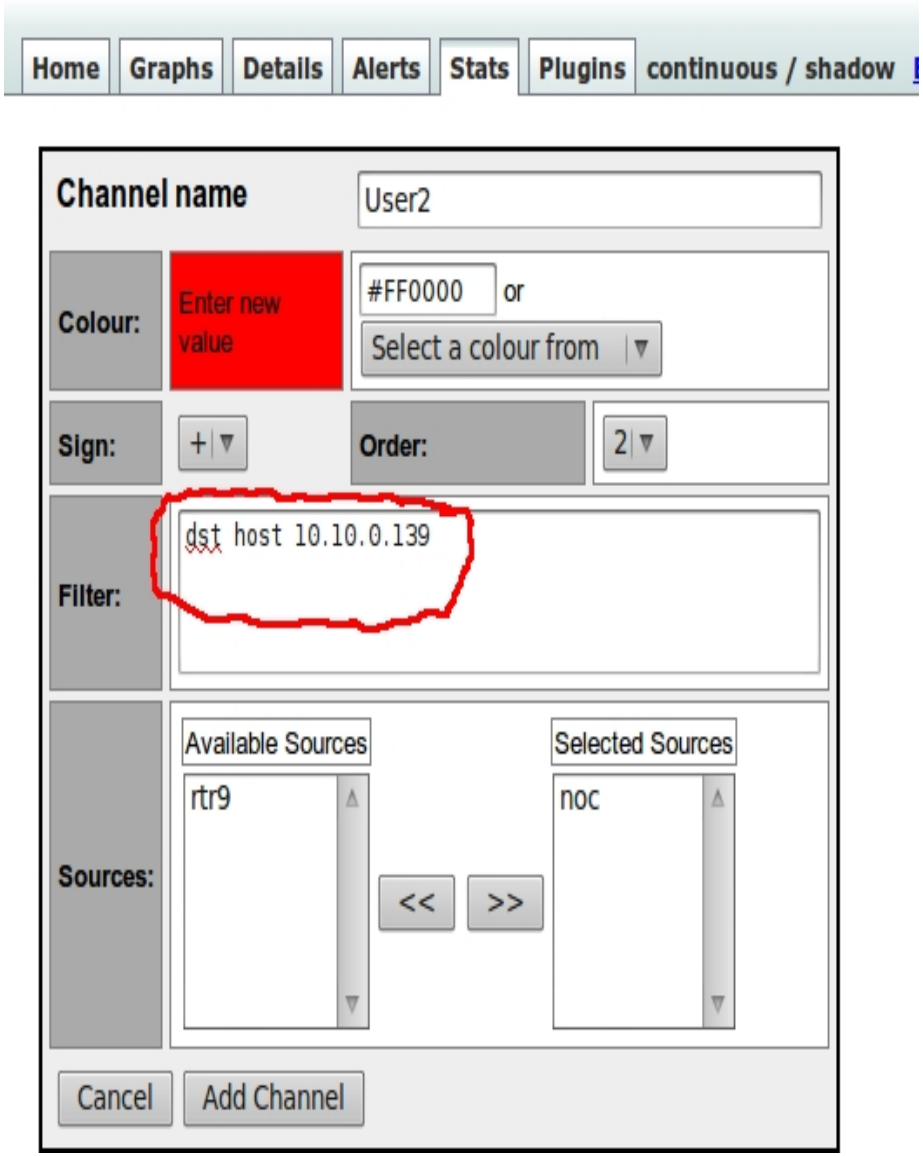



- When done click on 'Create Profile' at the bottom
- You will see a message “new profile created”
- Then click on the plus sign at the bottom to begin adding channels

# Add a Channel

# Add a second channel and start to accept

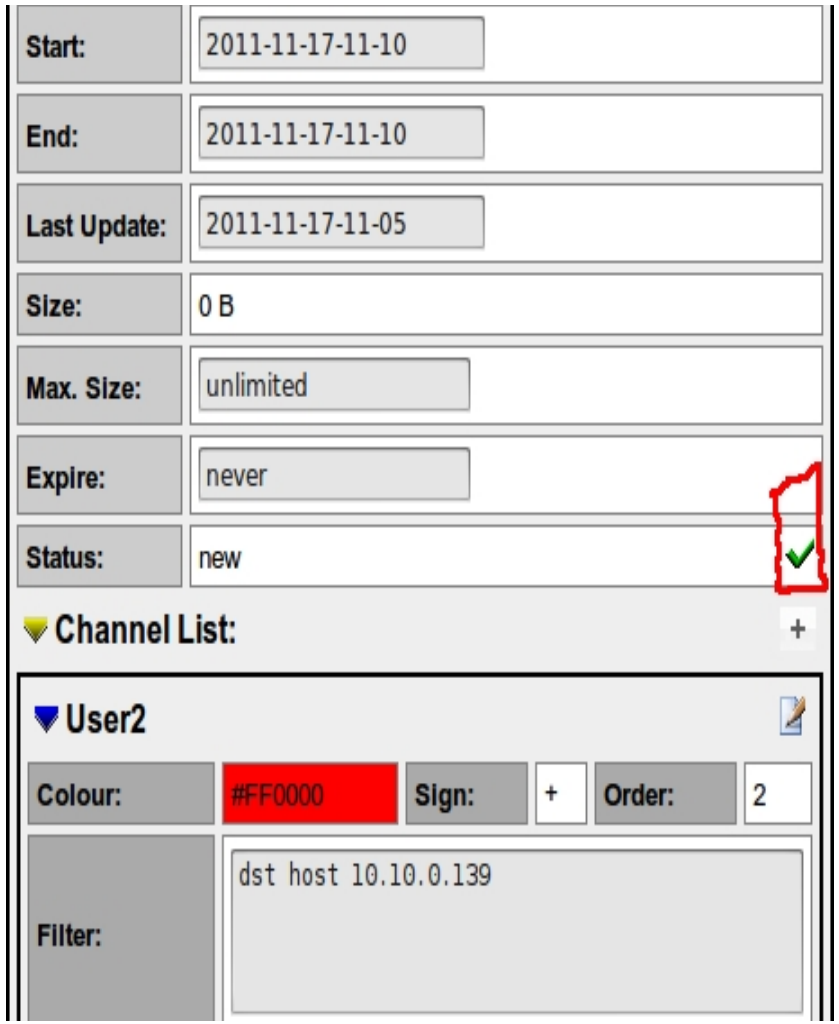


# Filters

- 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

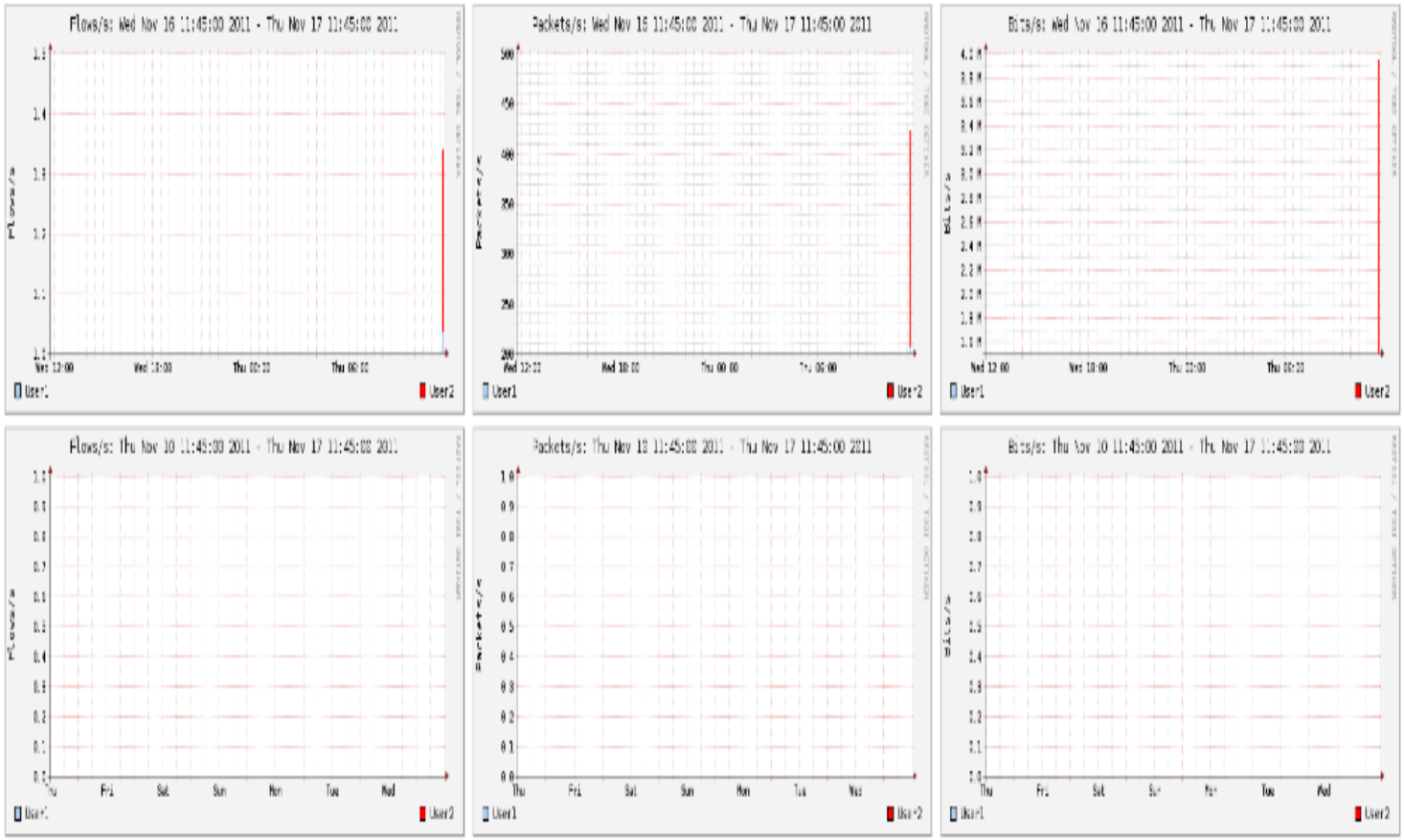
# Activate the profile




- 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:
```

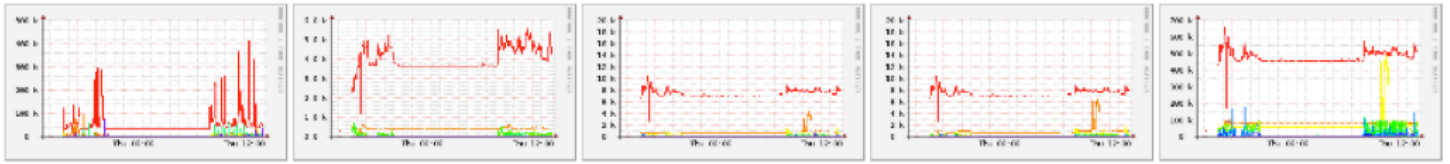
| Date flow start | Duration | Proto | Src IP Addr | Src Pt | Dst IP Addr | Dst Pt | Packets | Bytes | bps | Bpp | Flows |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 2011-11-17 11:26:53.320 | 1267.891 | TCP | 88.221.216.85 | 1935 | 10.10.0.139 | 2708 | 60660 | 86.0 M | 542683 | 1417 | 1 |
| 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 |

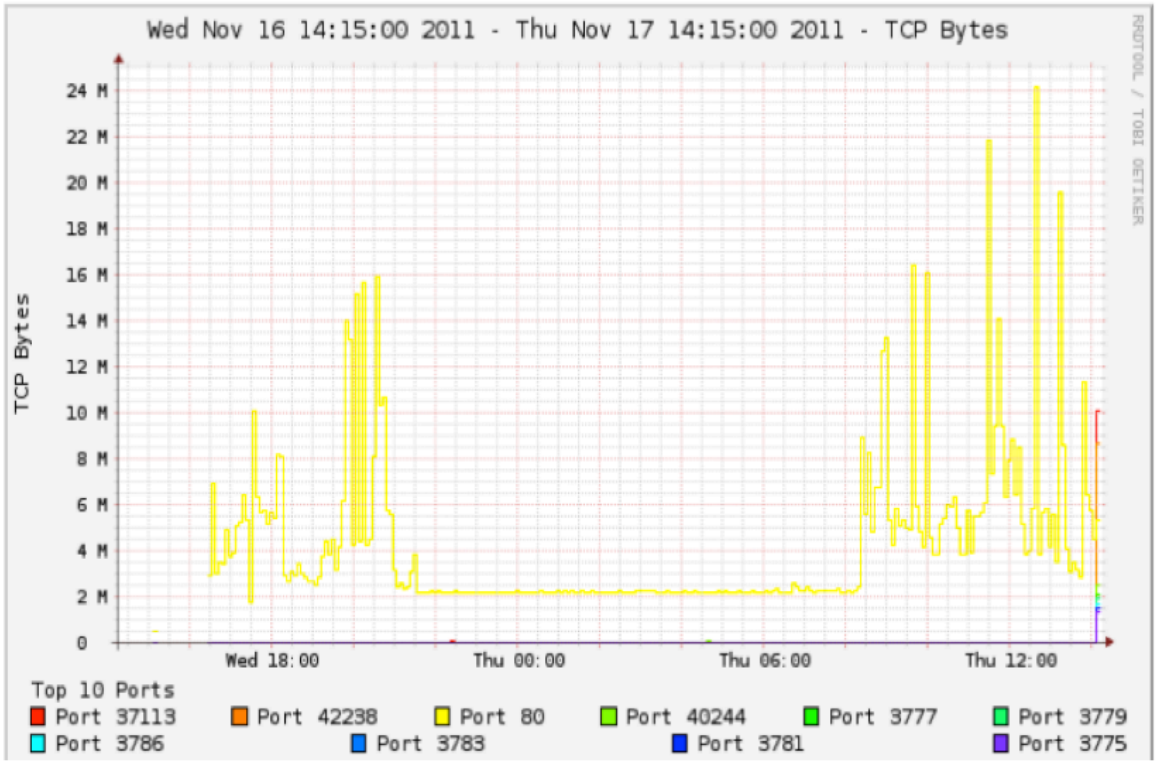
# PortTracker

PortTracker

## Port Tracker

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






Show Top 10 Ports

now | 24 hours

Track Ports:

Add | Delete

Skip Ports:

Add | Delete

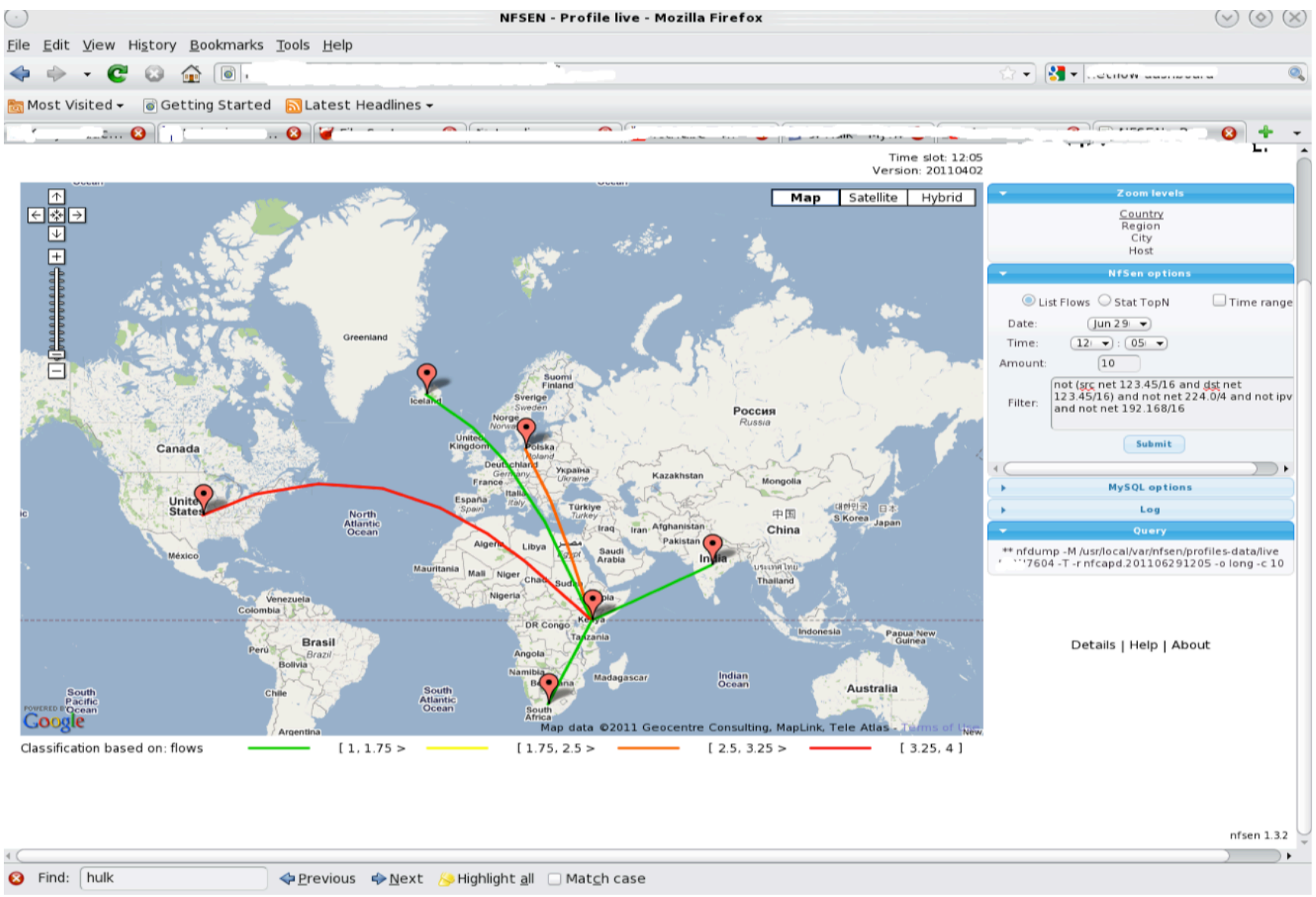
# Plugins

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/

# 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:
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
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

# References

NFSEN

http://nfsen.sourceforge.net

NFDUMP

http://nfdump.sourceforge.net/