



# 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 (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.

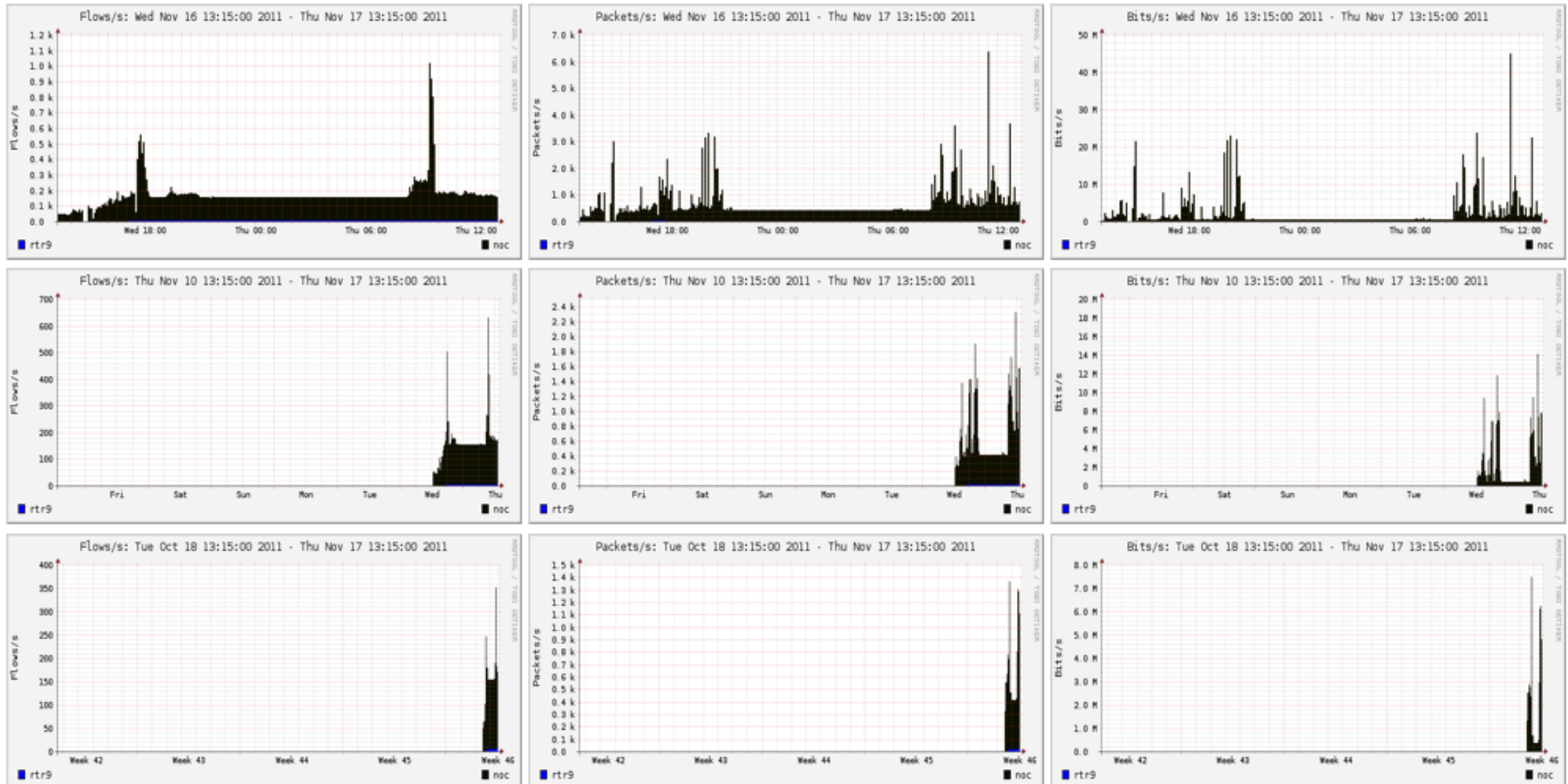
# NfSen structure

- 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

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

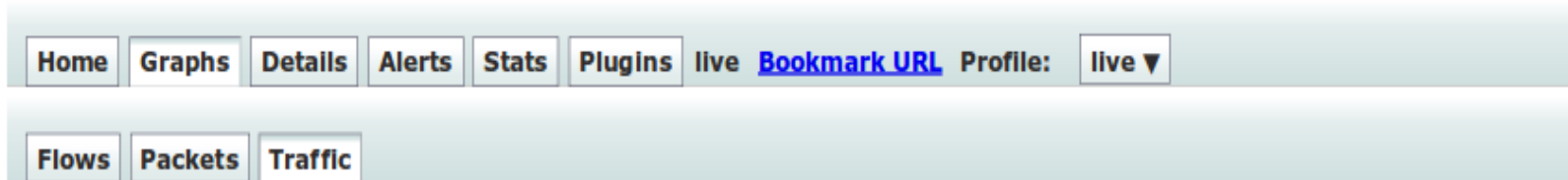
## Overview Profile: live, Group: (nogroup)



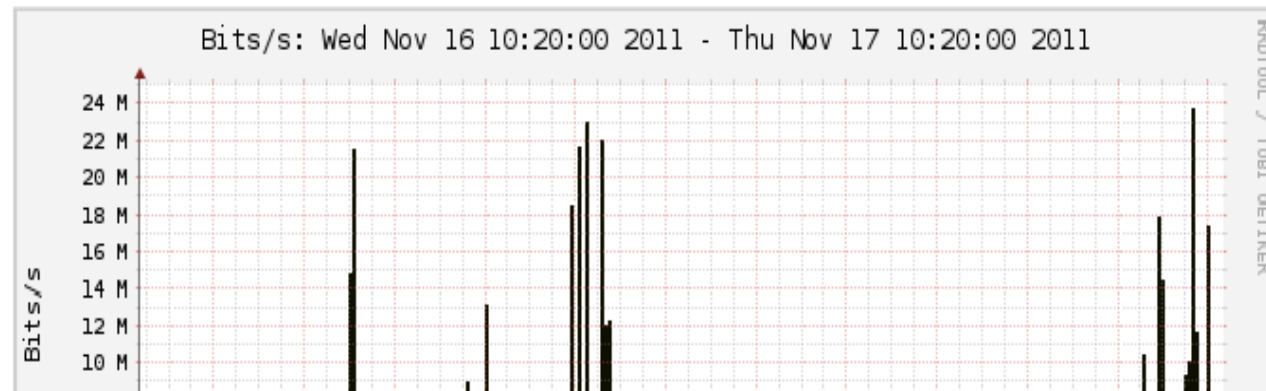
# Graphs Tab

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

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



**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



# 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:

- **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/>

# PortTracker

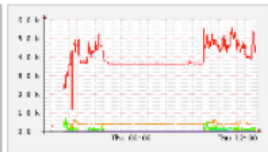
PortTracker

## Port Tracker

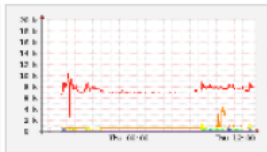
TCP Packets



TCP Flows



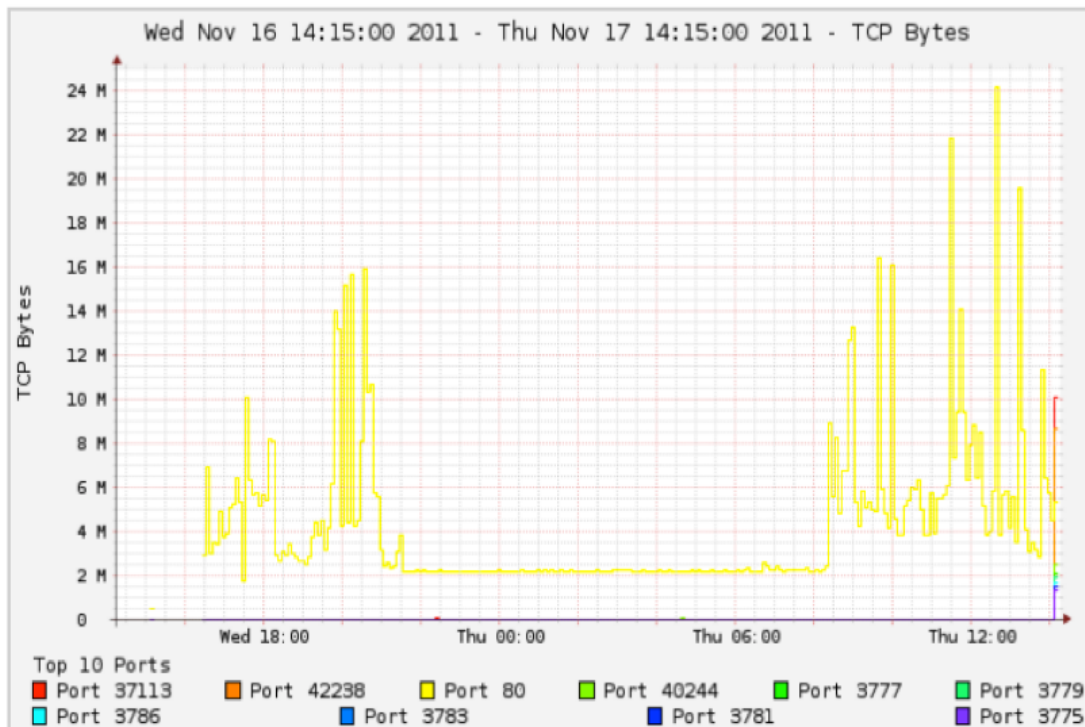
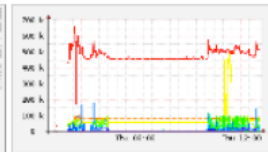
UDP Flows



UDP Packets



UDP Bytes



Show Top 10 Ports

☒ now ☐ 24 hours

Track Ports:

Add

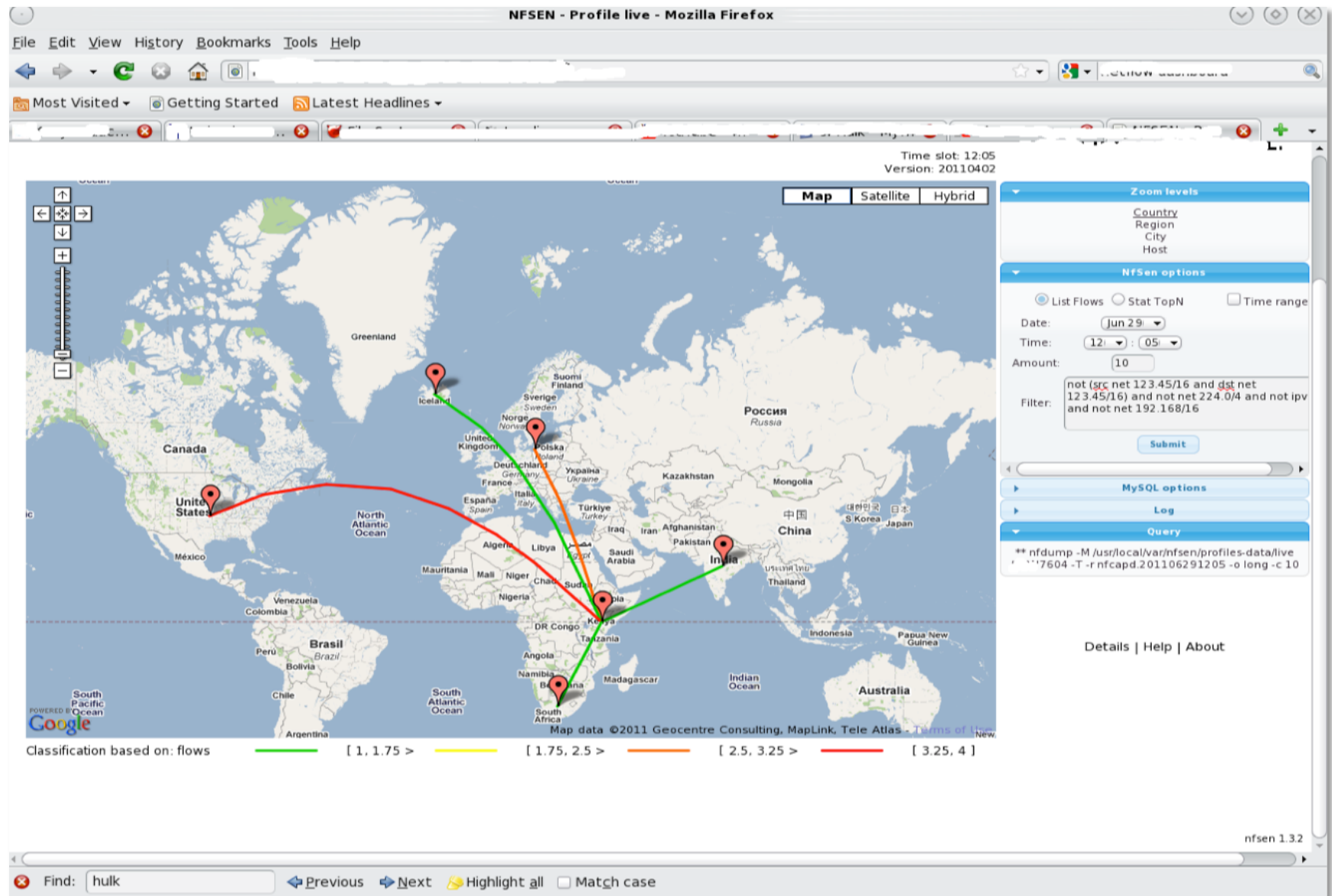
Delete

Skip Ports:

Add

Delete

# SurfMap



# 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

All None Display: ☐ Sum ☒ Rate

## Netflow Processing

Source: noc  
rtr9

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/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

srcIP

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/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
```

# References

NfSen

<http://nfsen.sourceforge.net>

NfDump

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

# Exercises