



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.

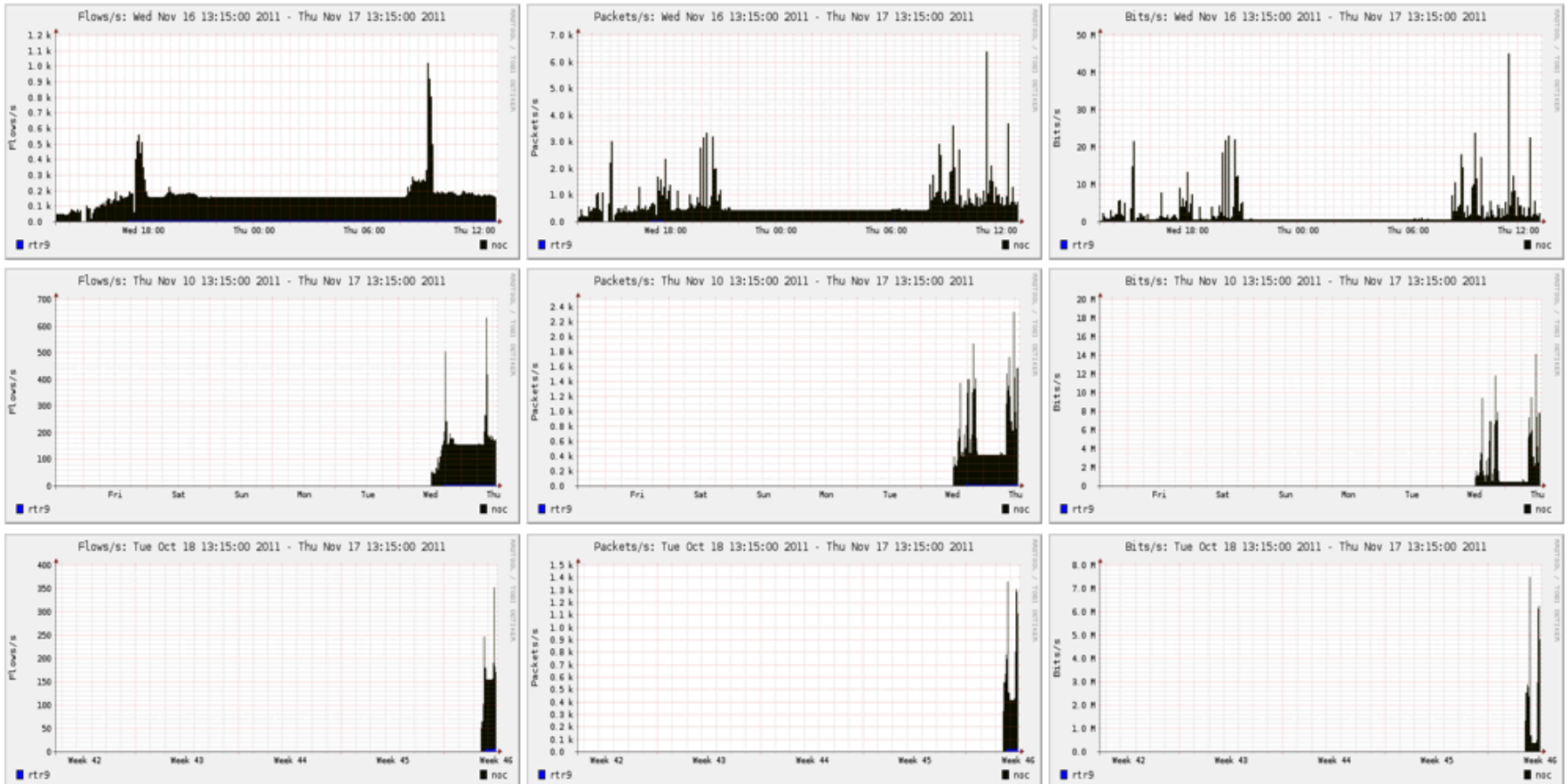
NfSen structure

- 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

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

Overview Profile: live, Group: (nogroup)



Graphs Tab

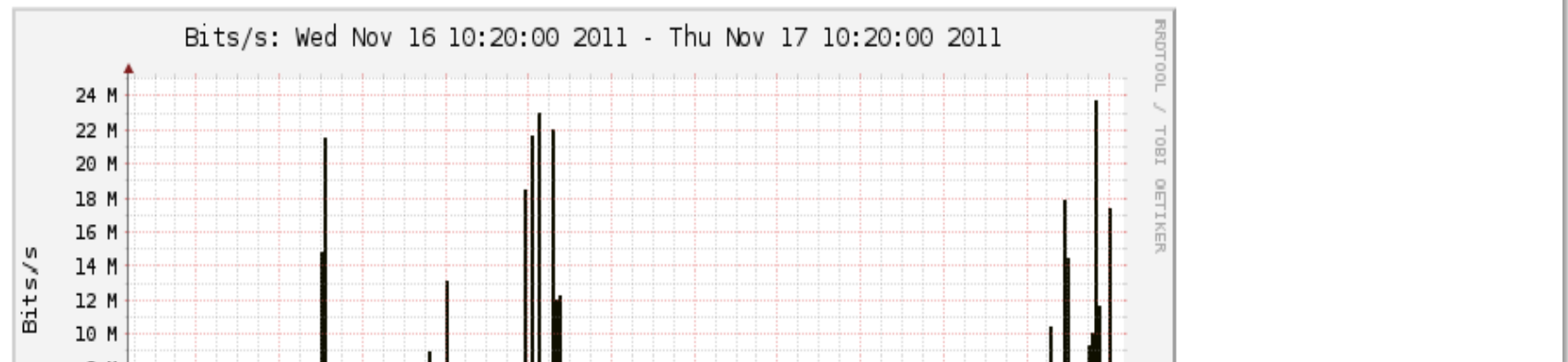
Graphs of flows, packets and traffic based on interface with netflow activated

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

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

Flows Packets Traffic

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

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

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

Netflow traffic graphs organized by Protocol

Graph of Netflow traffic for all Protocols

Time period for flows being observed

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:

- **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

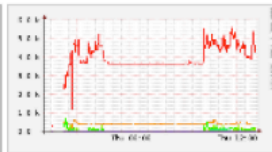
PortTracker

Port Tracker

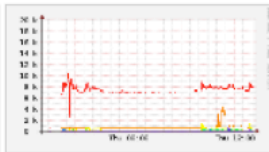
TCP Packets



TCP Flows



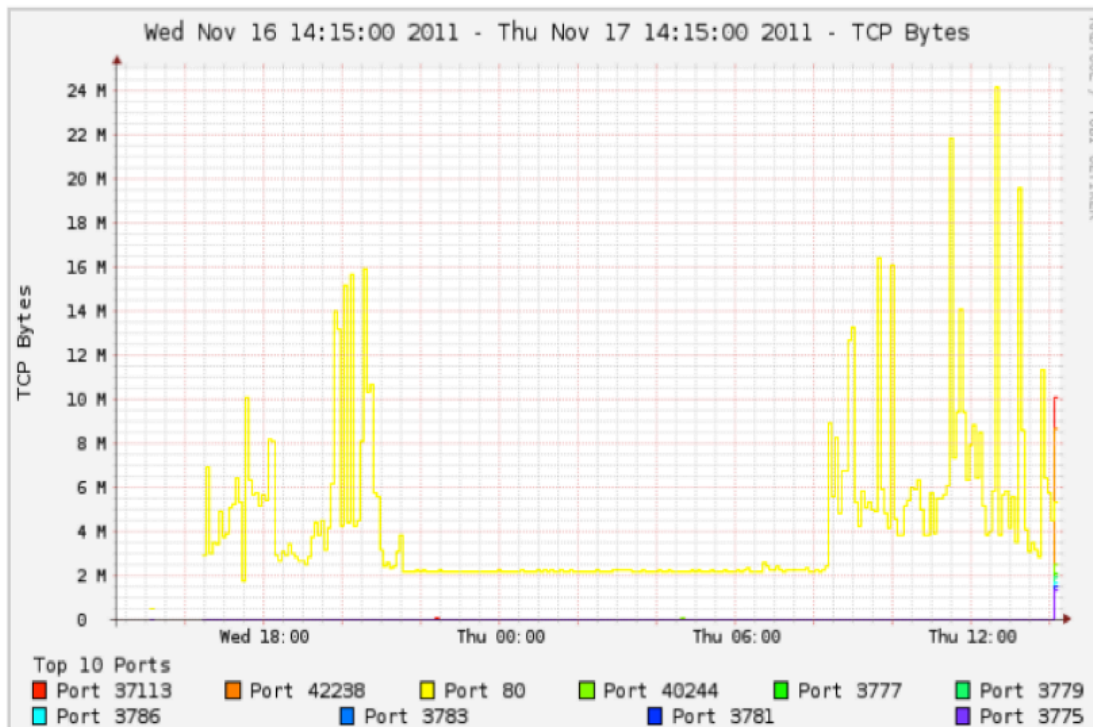
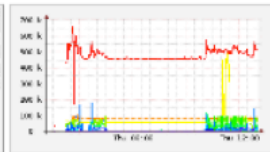
UDP Flows



UDP Packets



UDP Bytes



Show Top Ports

now 24 hours

Track Ports:

Add

Delete

Skip Ports:

Add

Delete

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: 12:05
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

Classification based on: flows
[1, 1.75 >] [1.75, 2.5 >] [2.5, 3.25 >] [3.25, 4]

nfsen 1.3.2

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

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: 1061200, Blocks skipped: 0, Bytes read: 55106720
```

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: 1001260, flows skipped: 0, bytes read: 55106700
```


References

NfSen

<http://nfsen.sourceforge.net>

NfDump

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

Exercises