NfSen

Network Startup Resource Center

www.ws.nsrc.org

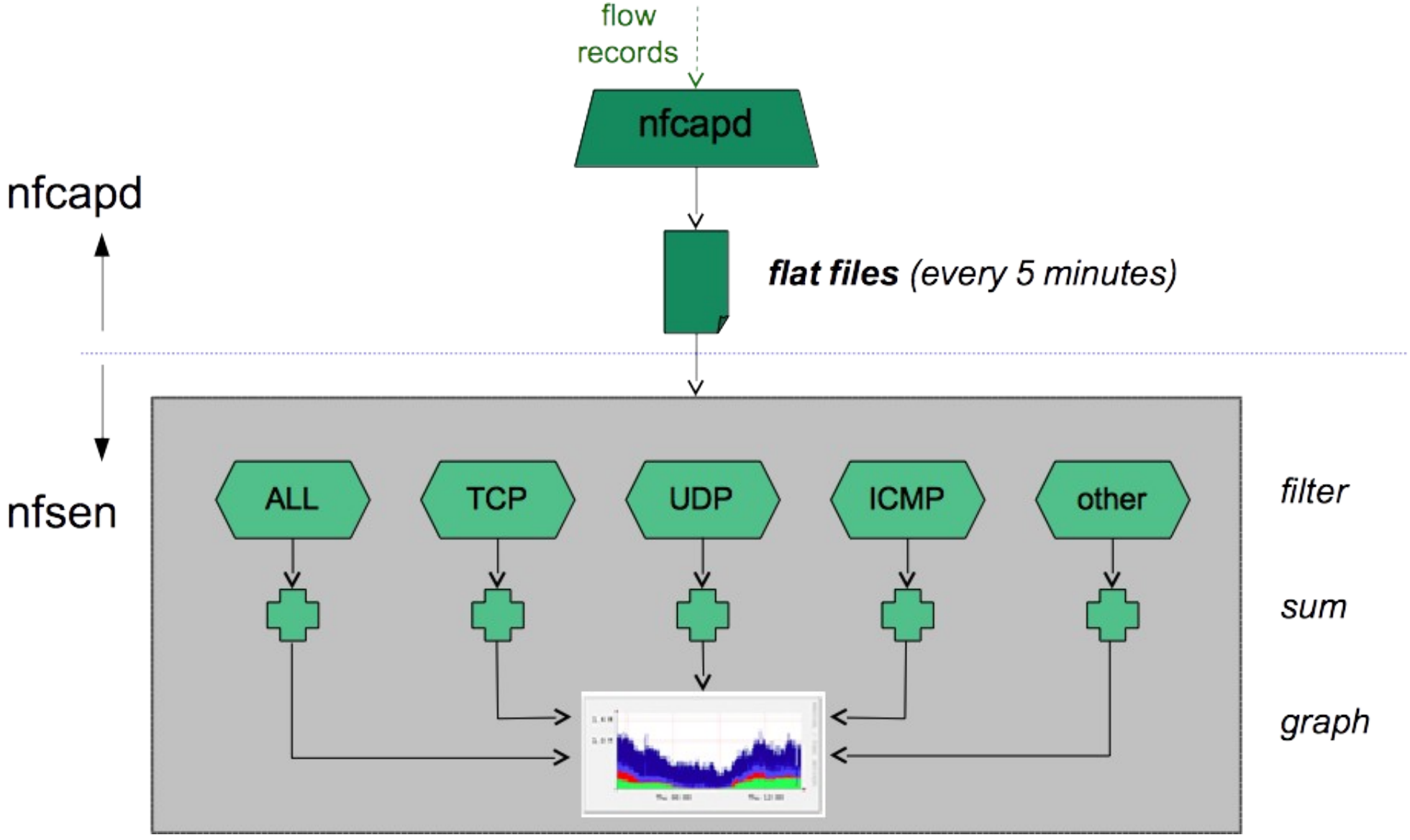
What is NfSen

- Companion to NfDump tools
- NfDump tools collect netflow data and store them in files
- Processing netflow data with NfDump tools can only be done on the command line
- NfSen is a graphical (Web Based) front end to NfDump
- Creates RRD graphs based on stored data
- Plugins extend the functionality of base (e.g. PortTracker and SURFmap)

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 architecture



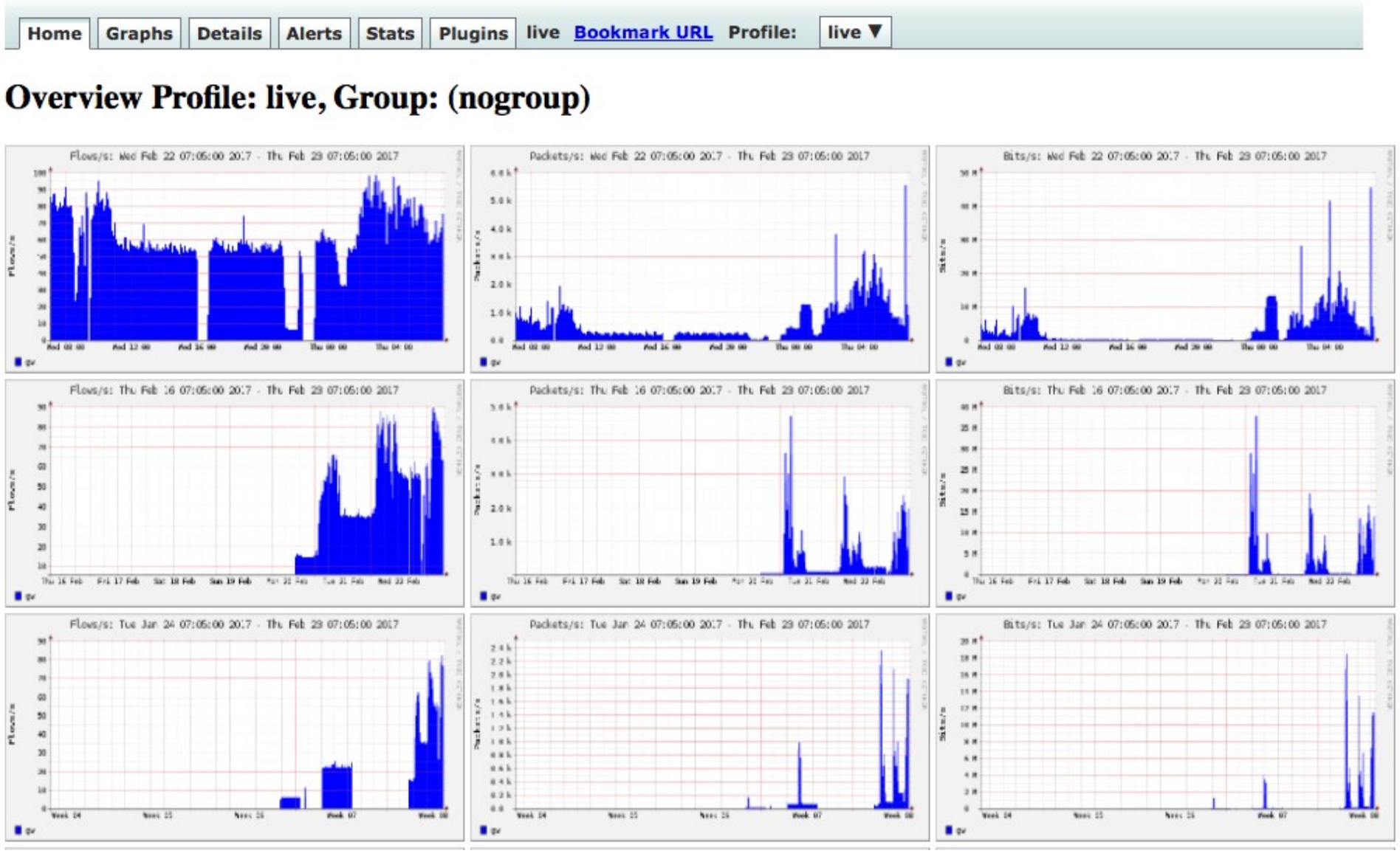
NfSen: Points to note

- Every 5 minutes *nfcapd* starts a new file, and *nfsen* processes the previous one
- Hence each graph point covers 5 minutes
- The graph shows you the total of selected traffic in that 5-minute period
- To get more detailed information on the individual flows in that period, *nfsen* lets you drill down using *nfdump* in the back end

NfSen structure

- Configuration file - `nfsen.conf`
- NfDump files – Netflow files containing collected flows stored in the directory: `/var/nfsen/profiles-data`
  - Note: 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 the directory: `/var/nfsen/profiles-stat`

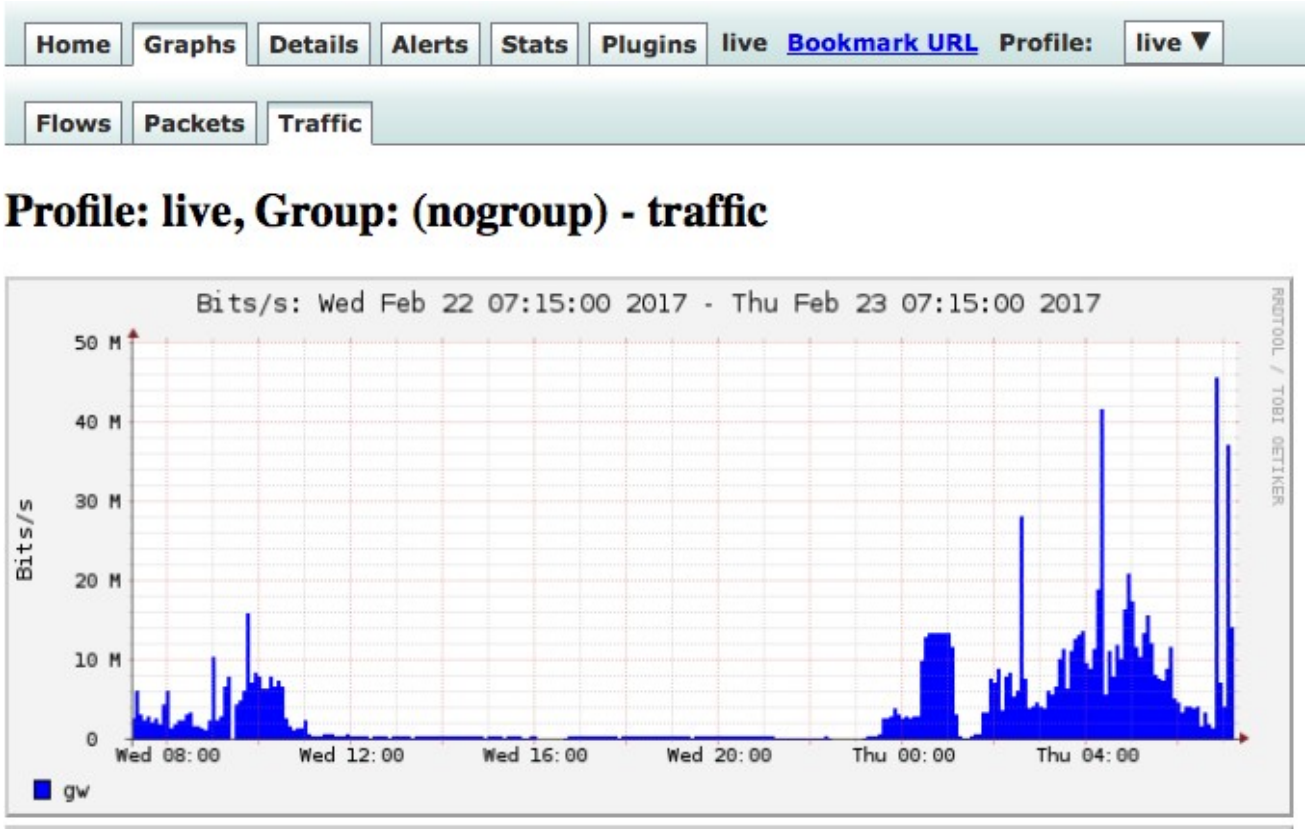
NfSen home screen



Graphs tabs

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

Note: What is seen under Traffic should closely match what your NMS shows 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

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

Profiles and Channels

- A *channel* is a type of traffic of interest
  - Total HTTP, HTTPS, SMTP traffic (etc)
  - Traffic to and from the Science department
- A *profile* is a collection of channels which can be shown together in a graph
  - v4 TCP, v6 TCP, v4 UDP, v6 UDP, Other
- You can create your own profiles and channels, and hence graphs.
- Use *filters* to define a channel
  - Filter out the flow data you are interested in from the data files that contain all the flows

Filters

- A *filter* is a collection of *expressions*
  - `expr1, expr2 **and** expr3, expr4 **or** expr5, **not** expr6, ( expr7 ), **not** ( expr8 )`
- Each *expression* can specify things like
  - IP version: `inet, ipv4, inet6, ipv6`
  - Protocol: `{proto} tcp, udp, icmp, gre, …`
  - IP Address:
    `[src|dst] ip 10.10.10.1`
    `[src|dst] ip in <addr1> <addr2> <addr3>`

Filters (2)

- IP Network: `[src|dst] net 172.16/16`
- Port: `[src|dst] port 80`
  `[src|dst] port > 1024`
- TCP Flags: `flags S`
  `flags S and not flags AFPRU`
- TOS: `tos 8`

Filters (3)

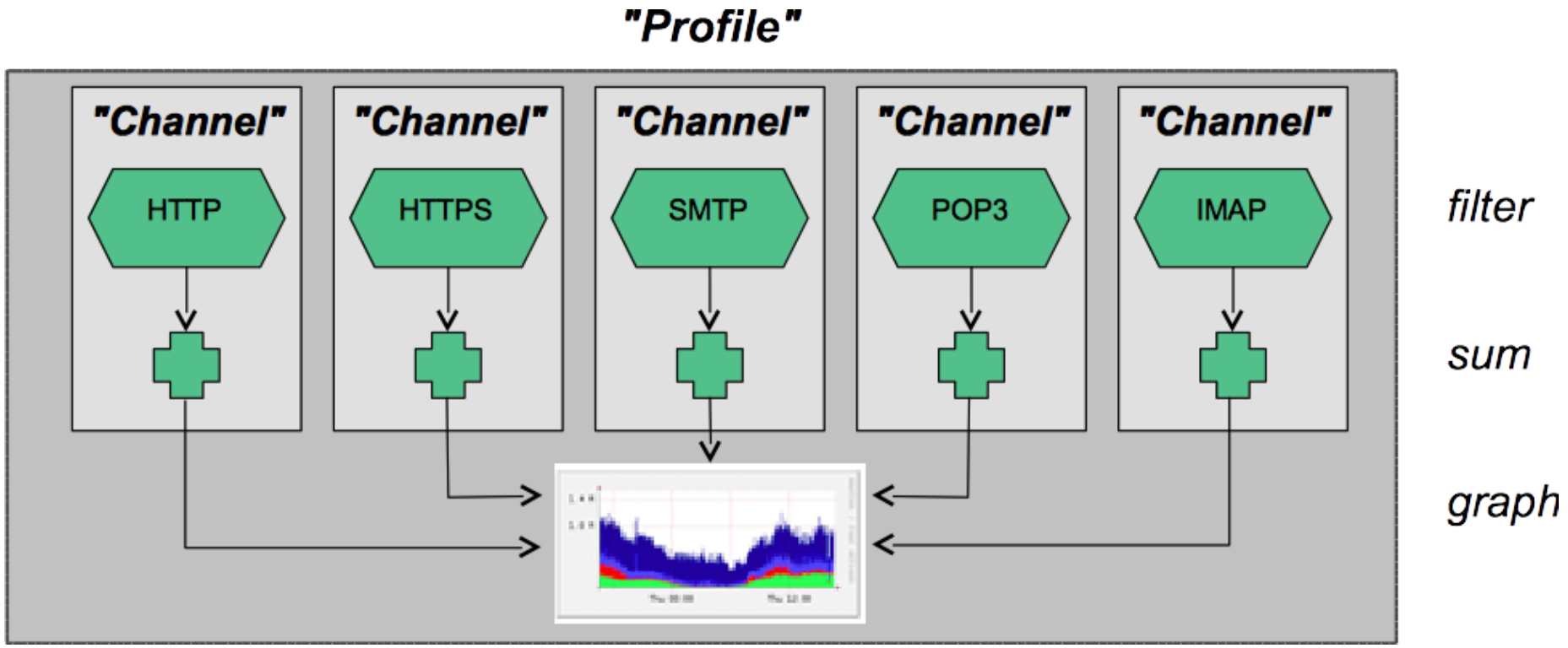
- Bytes: `bytes > 1024`
  `bytes = 64`
- Packets per second: `pps > 10`
- Bits per second: `bps > 10m`
- Bits per packet: `bpp > 15`
- Duration of flow: `duration > 36000000`
- AS Number: `[src|dst] 23456`
- All numbers can have scaling factors:
  `k, m, g, t` with 1024 as factor

Example filters

- `proto tcp and ( port 80 or port 443)`
- `proto tcp and ( src ip 172.16.17.18 or dst ip 172.16.17.19)`
- `proto tcp and ( net 172.16/16 and src port > 1024 and dst port 80 ) and bytes > 2048`
- `ipv6 and proto tcp and ( port 80 or port 443)`

Profiles and Channels

A *profile* is a collection of *channels* graphed together



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

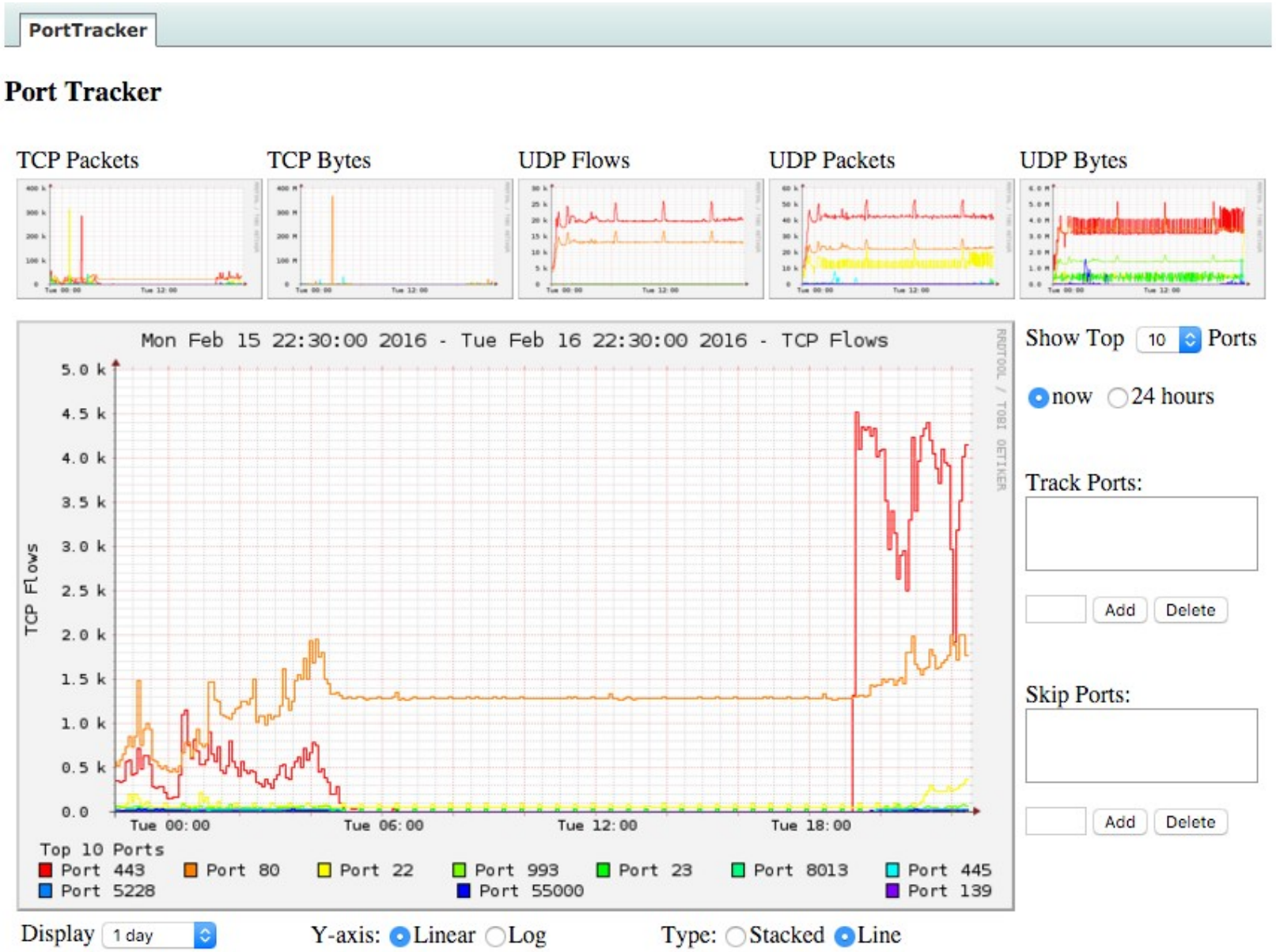
Plugins

Several plugins available:

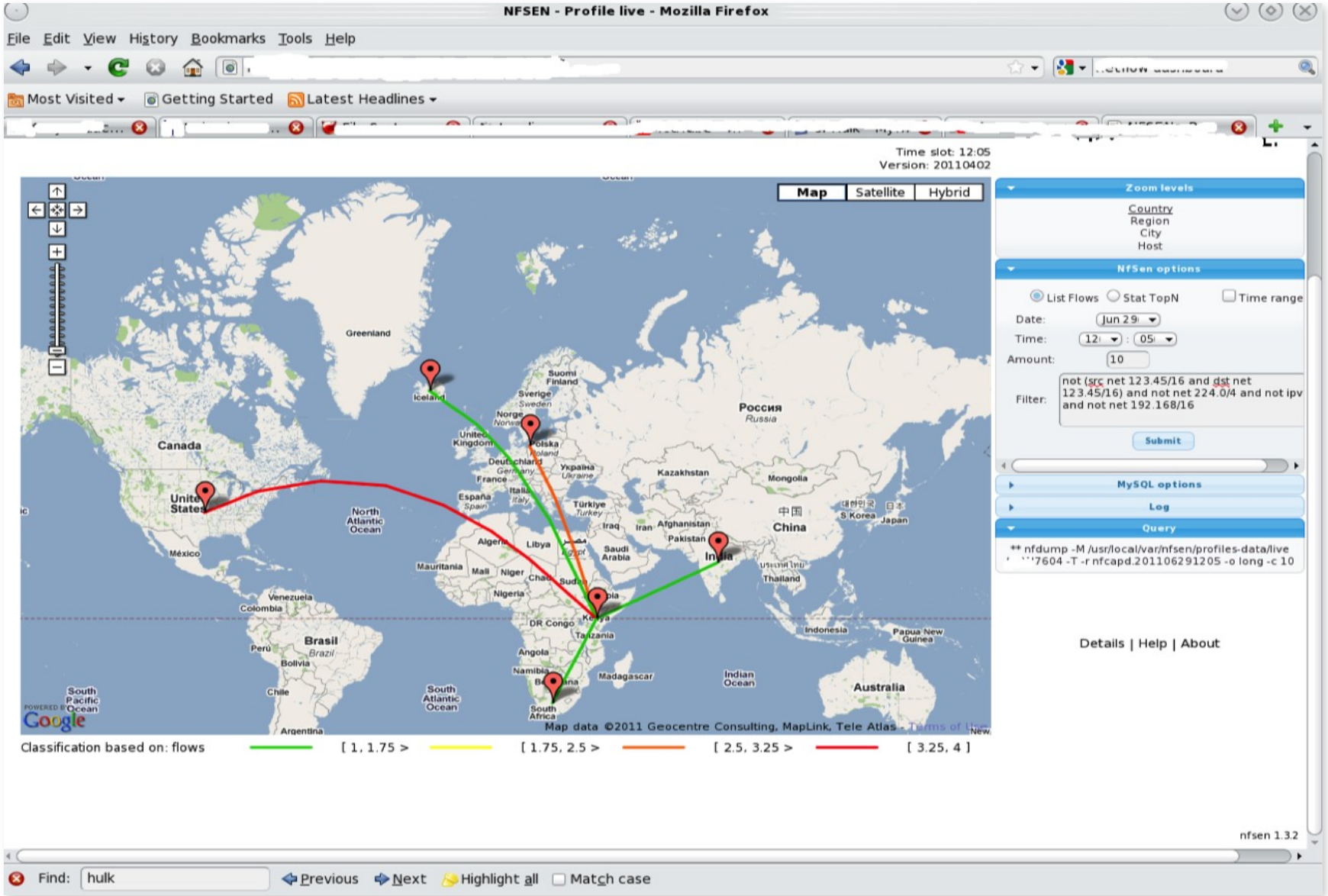
- PortTracker tracks the top 10 most active ports and displays a graph
- SURFmap displays country-based traffic based on a Geo-Locator

- More plugins available here `http://sourceforge.net/projects/nfsen-plugins/`

Plugins: PortTracker



Plugins: 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 your NMS 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

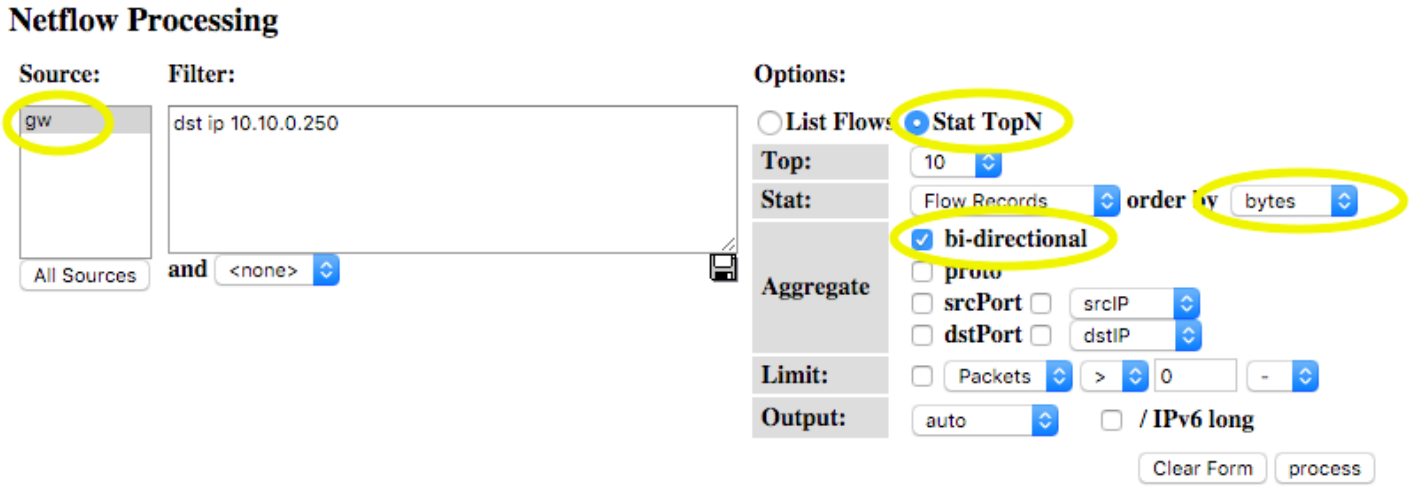
Bidirectional vs Unidirectional traffic as seen via NfSen

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 (*Detail*s tab)

You need to select either a *Singe Timeslot* or *Time Window*



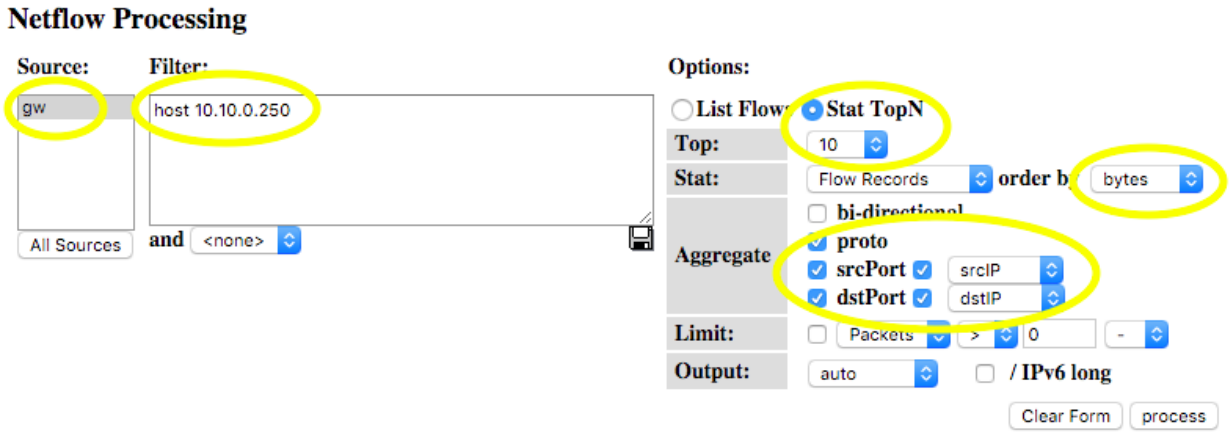

```
** nfdump -M /var/nfsen/profiles-data/live/gw  -T  -R 2016/02/15/nfcapd.201602152245:2016/02/16/nfcapd.201602161935 -n 10 -s record/bytes
nfdump filter:
dst ip 10.10.0.250
Command line switch -s overwrites -a

Aggregated flows 631392
Top 10 flows ordered by bytes:
Date first seen          Duration Proto      Src IP Addr:Port           Dst IP Addr:Port   Out Pkt   In Pkt Out Byte   In Byte Flows
2016-02-15 22:40:08.628 75342.352 UDP        10.10.0.241:40311 <->      10.10.0.250:9991        0    3.1 M        0  872.7 M  1080
2016-02-15 22:40:12.387 75365.281 UDP        10.10.0.225:58565 <->      10.10.0.250:9001        0   104774        0  124.4 M   890
2016-02-15 22:40:06.525 75326.616 UDP        10.10.0.225:52808 <->      10.10.0.250:9996        0    76175        0  111.4 M   875
```

Note the protocol

These ports are your clue!

Unidirectional (*Detail*s tab)




```
** nfdump -M /var/nfsen/profiles-data/live/gw  -T  -R 2016/02/15/nfcapd.201602152245:2016/02/16/nfcapd.201602161935 -n 10 -s record/bytes
nfdump filter:
host 10.10.0.250
Aggregated flows 1265694
Top 10 flows ordered by bytes:
Date first seen          Duration  Proto      Src IP Addr Src Pt      Dst IP Addr Dst Pt   Packets     Bytes       bps     Bpp Flows
2016-02-15 22:40:08.628 75342.35  UDP        10.10.0.241   40311      10.10.0.250   9991     3.1 M  872.7 M     92668     282  1080
2016-02-15 22:40:12.387 75365.28  UDP        10.10.0.225   58565      10.10.0.250   9001     104774  124.4 M     13209    1187   890
2016-02-15 22:40:06.525 75326.61  UDP        10.10.0.225   52808      10.10.0.250   9996     76175   111.4 M     11831    1462   875
2016-02-15 22:40:06.529 75375.46  ICMP       10.10.0.250       0      10.10.0.225    0.0     39724   18.4 M      1951     462   937
2016-02-16 03:44:41.037     1.18  TCP        10.10.0.250      80      10.10.0.35   39621     3070    4.6 M    31.0 M    1496     1
2016-02-15 22:40:21.929 75469.614 ICMP       10.10.0.250       0       10.10.1.3    0.0     12090   1.0 M       107      84   322
2016-02-15 22:40:21.782 75399.793 ICMP       10.10.0.250       0      10.10.5.17    0.0     12086   1.0 M       107      84   321
2016-02-15 22:40:23.207 75408.871 ICMP       10.10.0.250       0      10.10.5.19    0.0     12084   1.0 M       107      84   325
2016-02-15 22:40:23.531 75408.019 ICMP       10.10.0.250       0       10.10.1.2    0.0     12082   1.0 M       107      84   306
2016-02-15 22:40:25.393 75388.616 ICMP       10.10.0.250       0       10.10.1.1    0.0     12080   1.0 M       107      84   314
Summary: total flows: 3187046, total bytes: 4428808141, total packets: 15754144, avg bps: 469115, avg pps: 208, avg bpp: 281
Time window: 2016-02-15 22:40:04 - 2016-02-16 19:39:43
Total flows processed: 17563909, Blocks skipped: 0, Bytes read: 1124162856
Sys: 2.824s flows/second: 6219514.5  Wall: 3.575s flows/second: 4912349.5
```

References

NfSen

http://nfsen.sourceforge.net

NfDump

http://nfdump.sourceforge.net/

This is a good read to better understand NfSen, NfDump and nfcapd.

Questions

?

Exercises