Network Monitoring, Management and Automation

NfSen

Netflow Sensor

npNOG 5

Dec 8 - 12, 2019

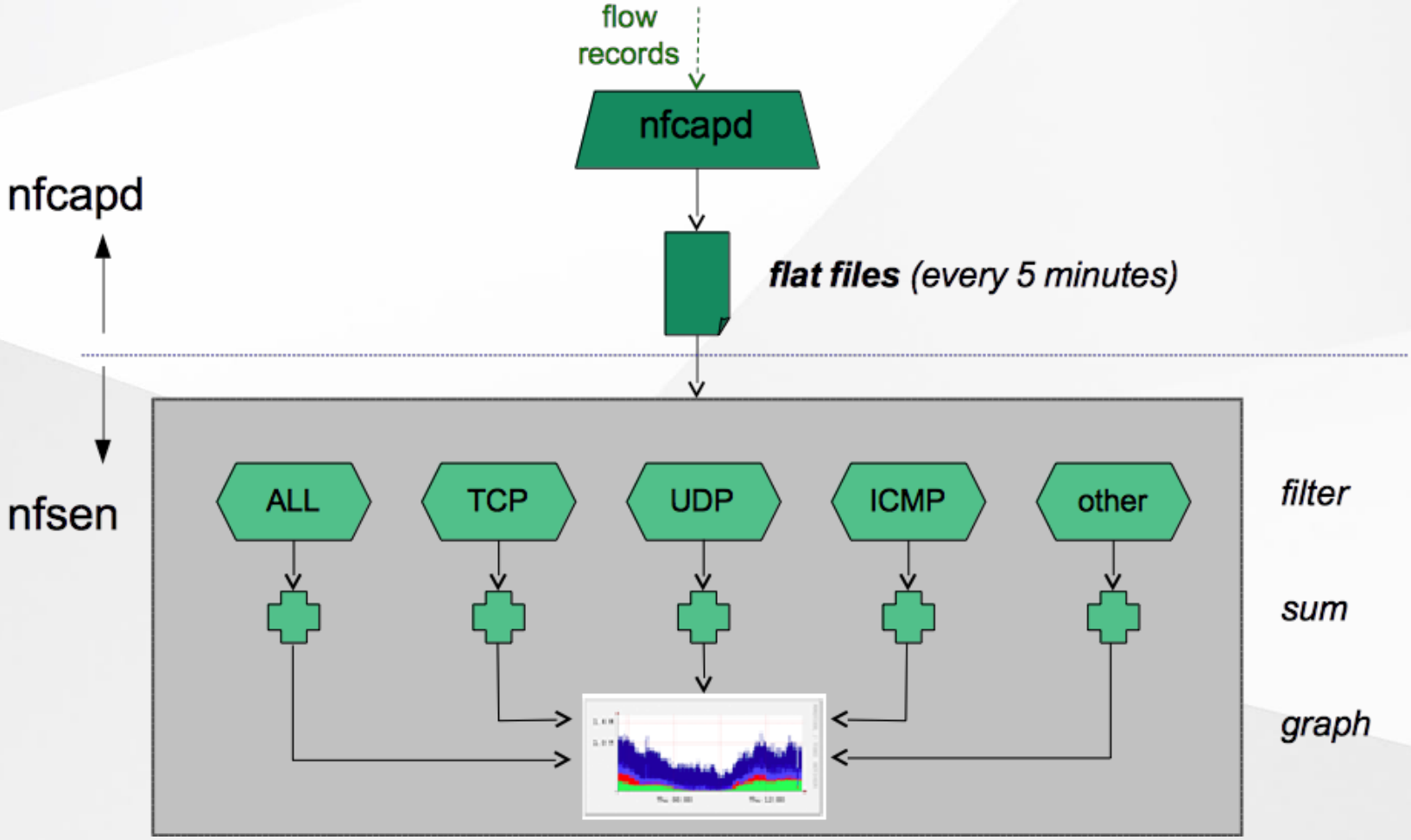
What is NfSen

- 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)

What can you do with NfSen

- 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



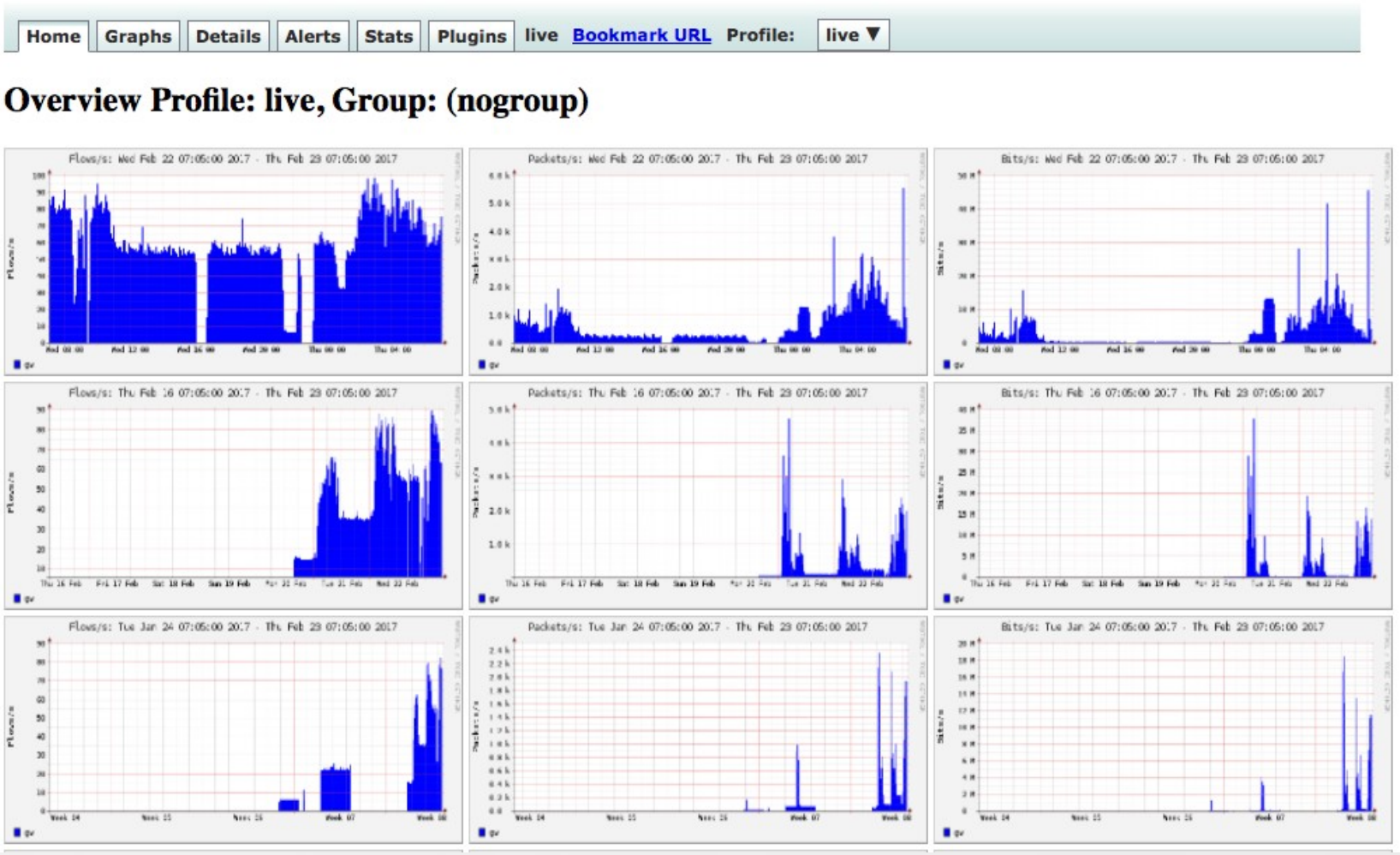
NfSen: Points to note

- 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***

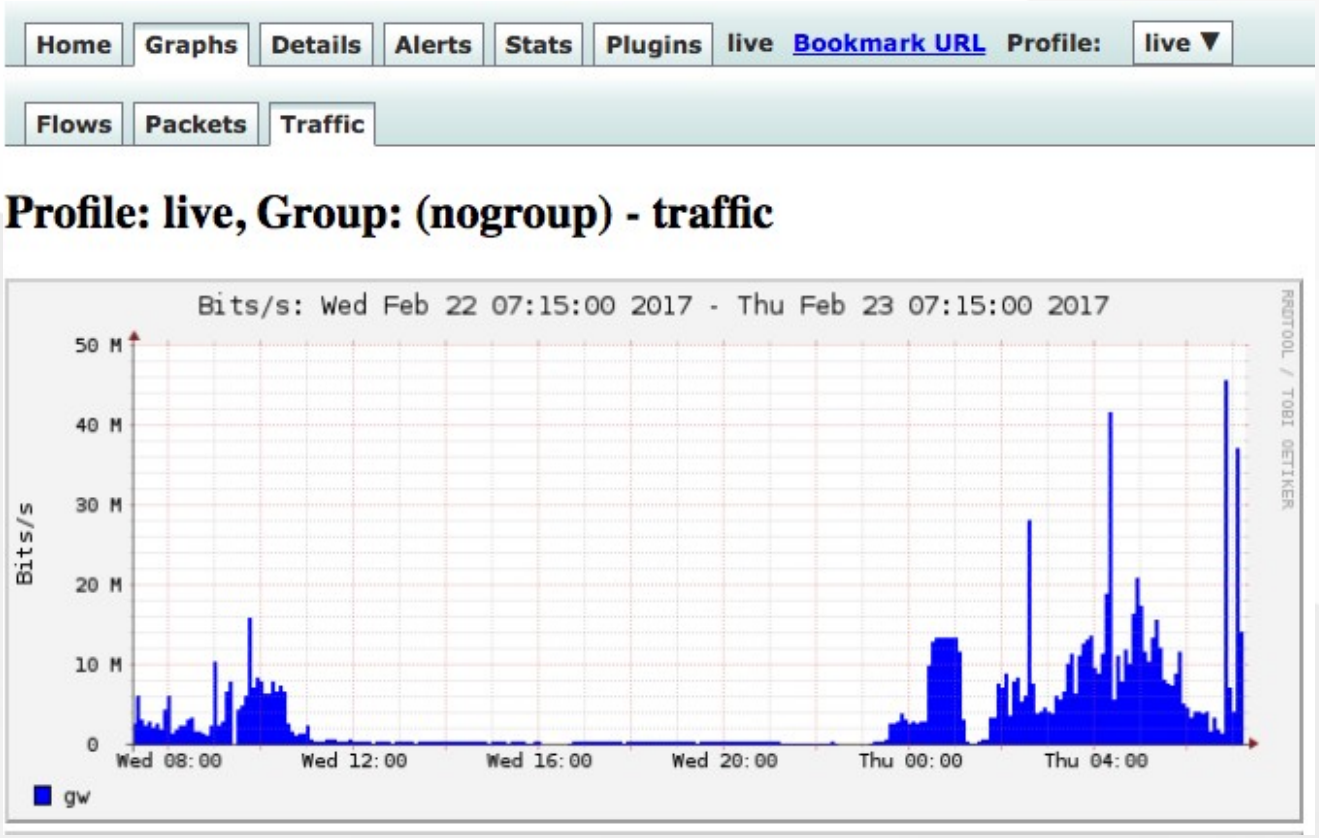
NfSen Home Screen



Graphs Tab

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

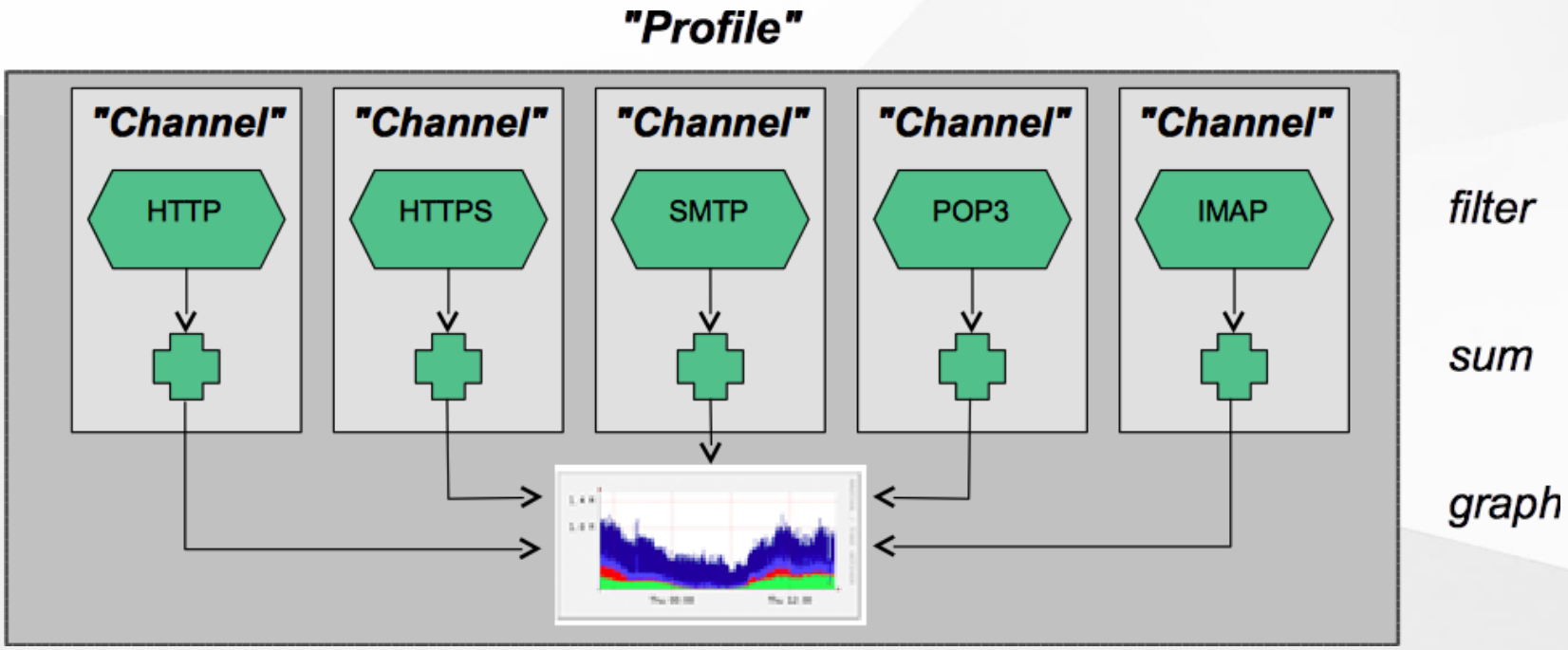
Details Page (Contd.)

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

Profiles and Channels (Contd.)

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



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>
  - **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 (contd.)

- **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)

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

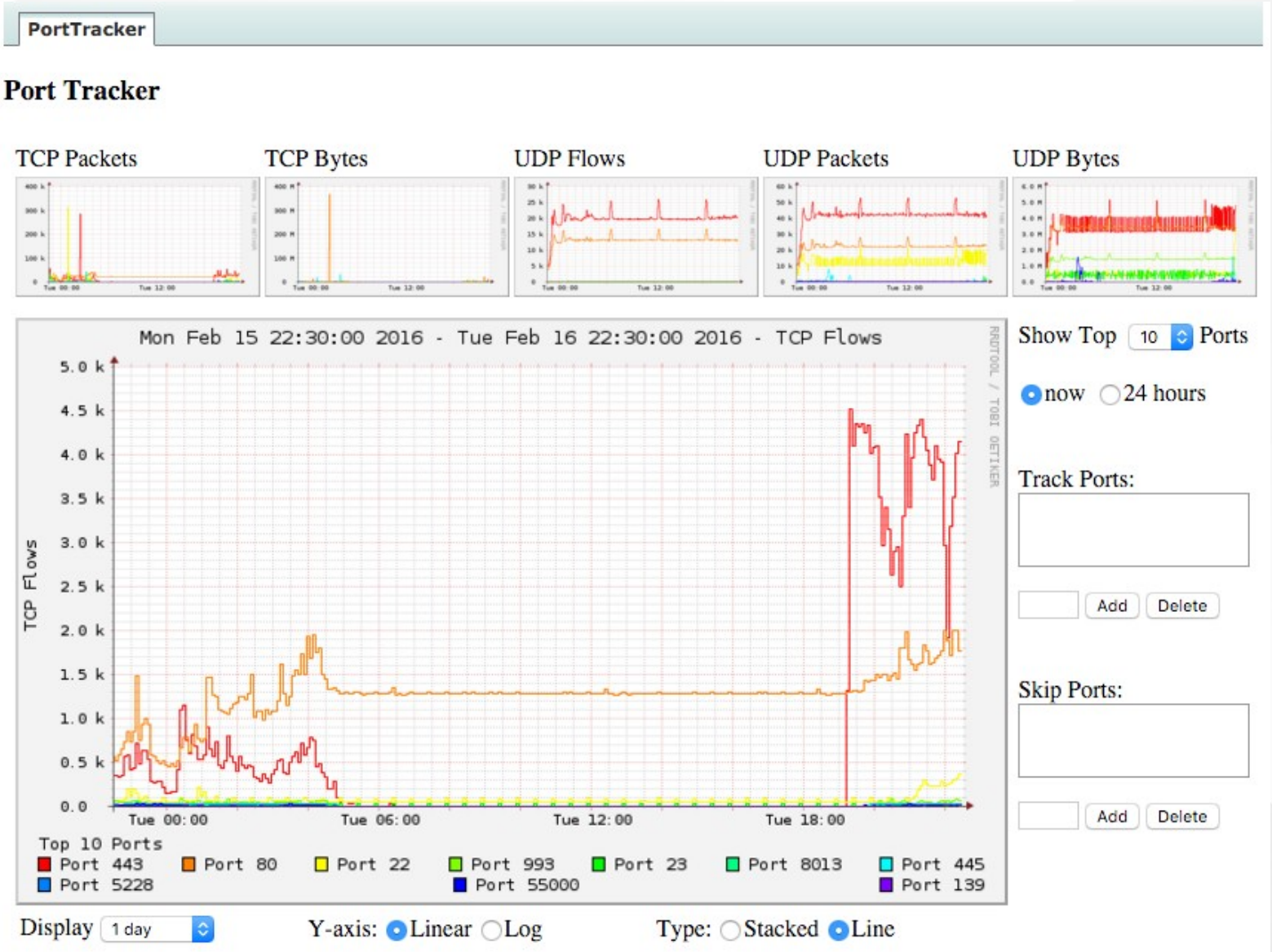
Plugins

Several plugins available:

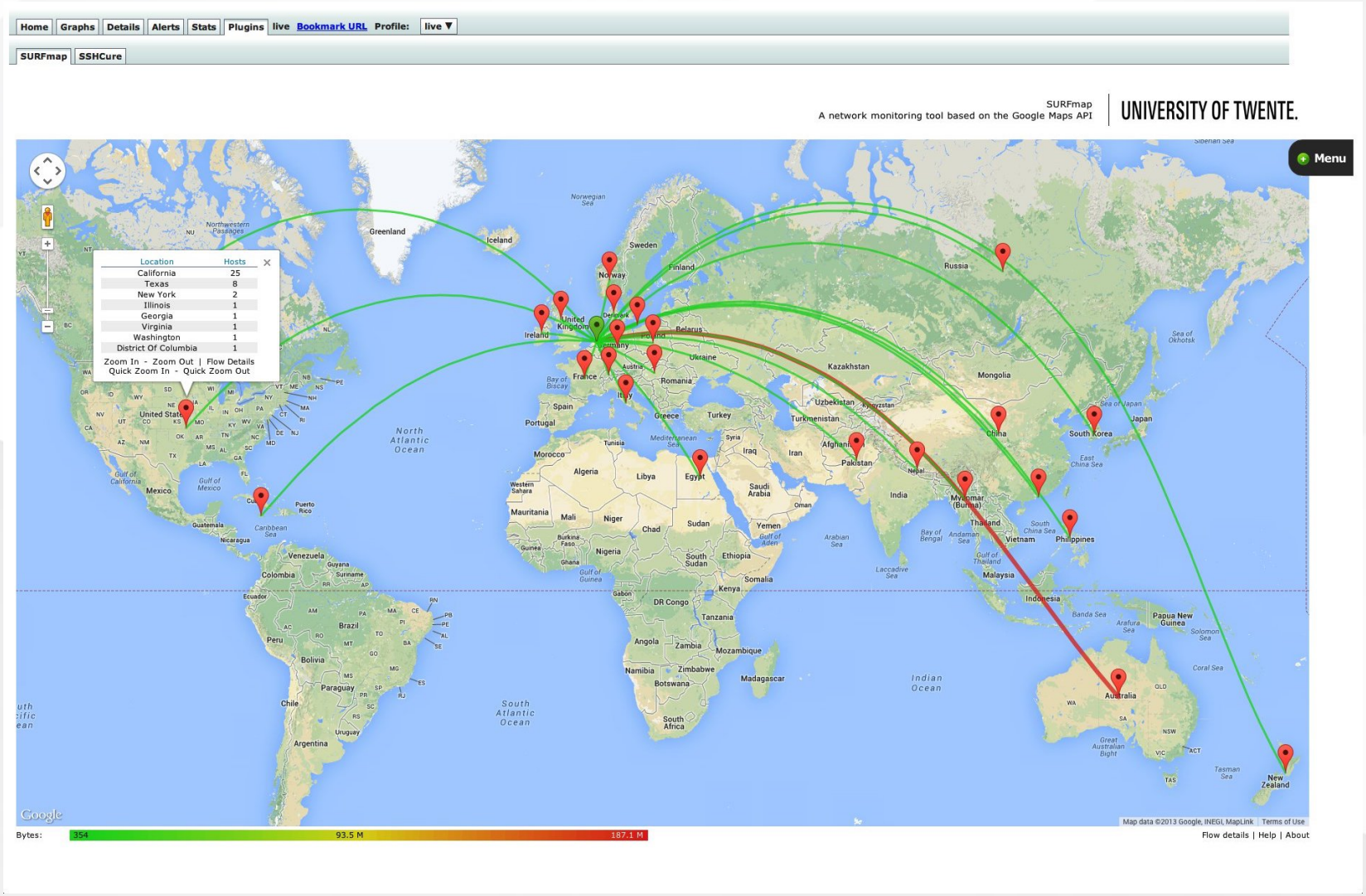
- **PortTracker** tracks the top 10 most active ports and displays a graph
- **SURFmap** displays country based traffic based on a Geo-Locator

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

Plugin: Porttracker



Plugin: 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

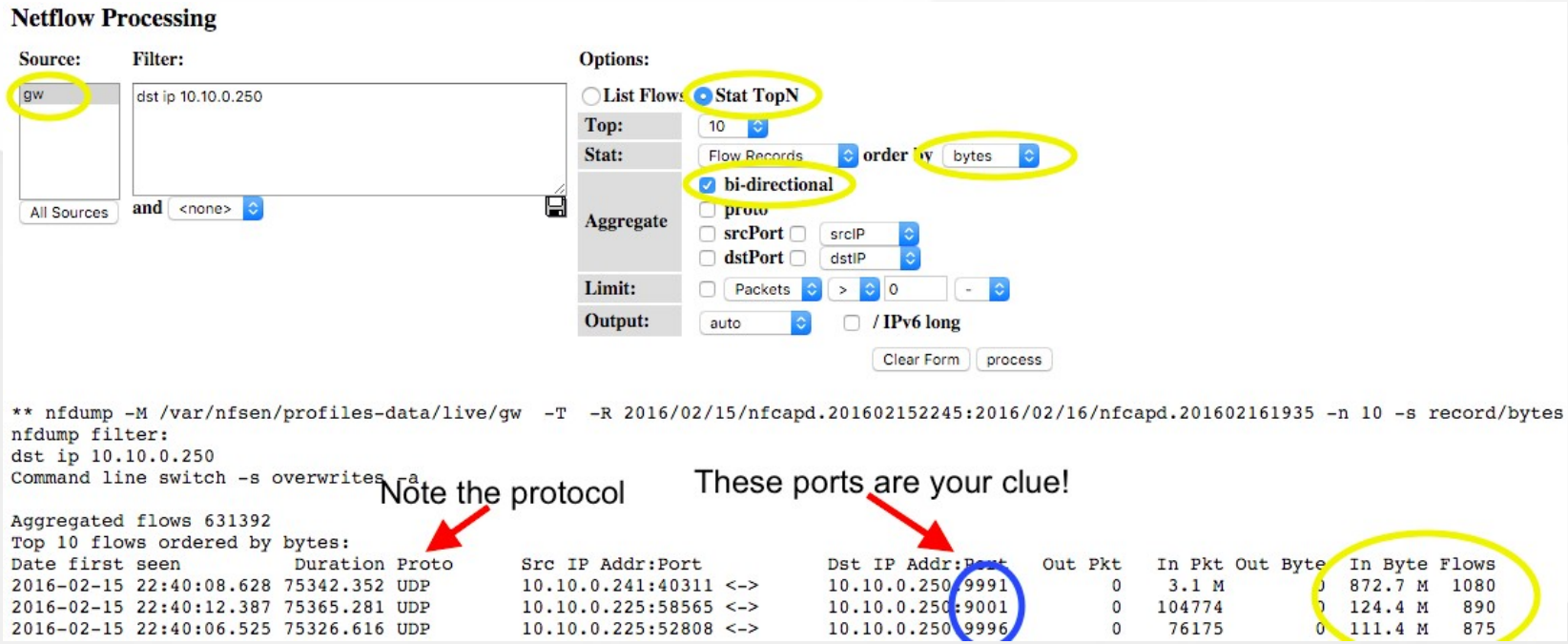
Bidirectional vs Unidirectional traffic as seen via NfSen

Unidirectional and Bidirectional

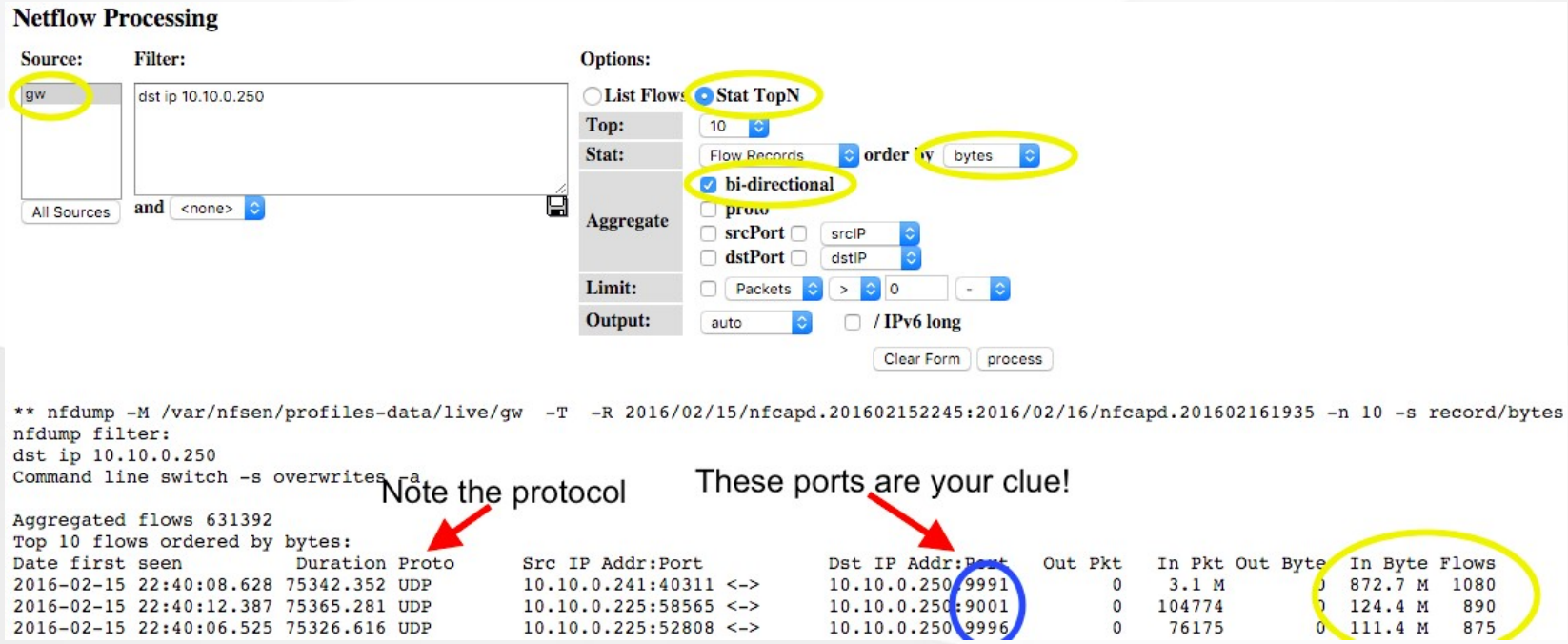
- Unidirectional shows flows from host A to B and then host B to host A
- Bidirectional shows flows between Host A and B combined
- Can be used with any of the other filters (src port, src host plus many more)
- List of filters can be found here: http://nfsen.sourceforge.net/#mozTocId652064

Bidirectional (Details tab)

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



Unidirectional (Details tab)



References

NfSen

http://nfsen.sourceforge.net

NfDump

http://nfdump.sourceforge.net/