



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

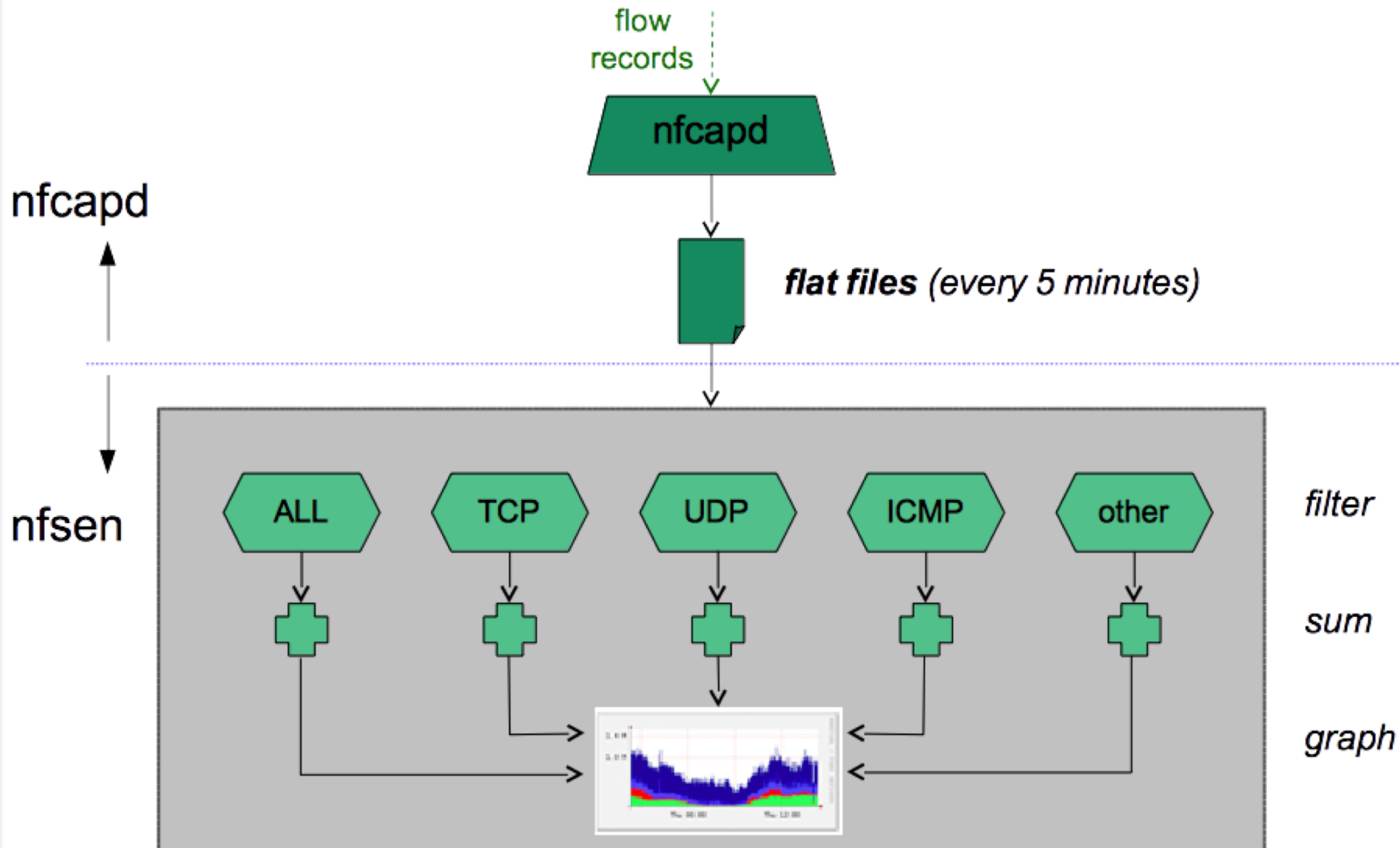
- Companion to NfDump tools
- NfDump tools collect netflow data and store them in files
- Processing netflow data with NfDump tools can only be done on the command line
- NfSen is a graphical (Web Based) front end to NfDump
- Creates RRD graphs based on stored data
- Plugins extend the functionality 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 - `nfсен.conf`
- NfDump files – Netflow files containing collected flows stored in the directory:
`/var/nfсен/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/nfсен/profiles-stat`

NfSen Home Screen

[Home](#)[Graphs](#)[Details](#)[Alerts](#)[Stats](#)[Plugins](#)

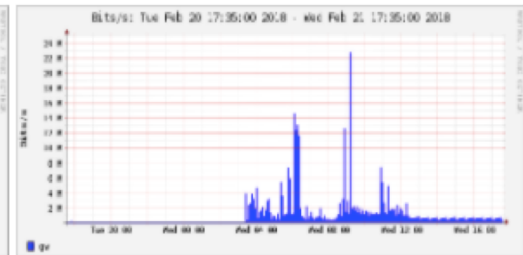
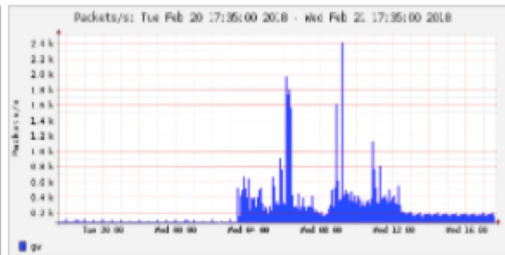
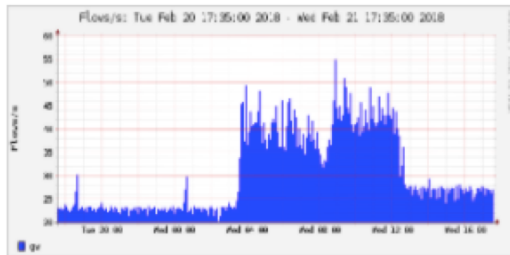
live

[Bookmark URL](#)

Profile:

live ▼

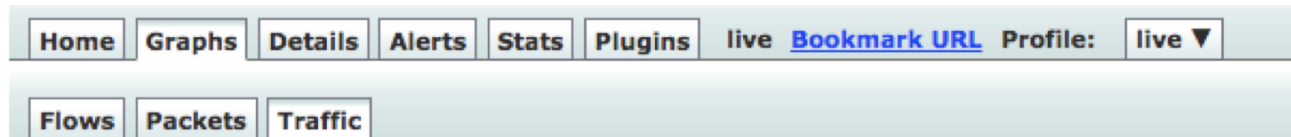
Overview Profile: live, Group: (nogroup)



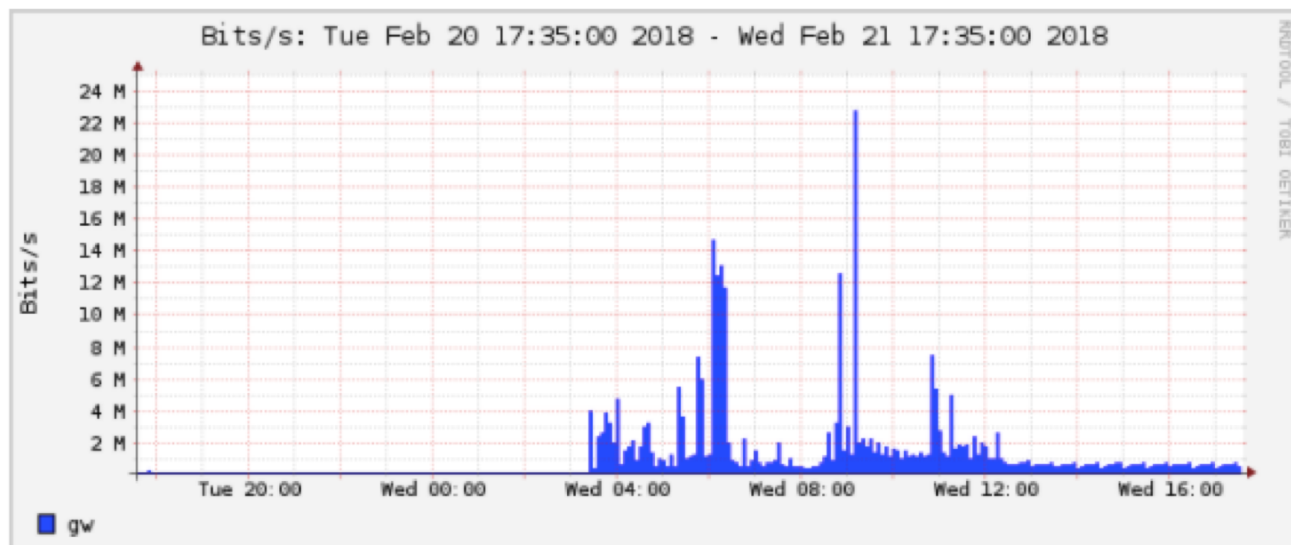
Graphs Tab

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

Note: What is seen under Traffic should closely match what your NMS shows for the same interface



Profile: live, Group: (nogroup) - traffic



Details Page

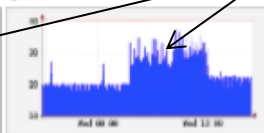
- Most interesting page
- Can view present flow information or stored flow information
- Can view detailed NetFlow information such as
 - AS Numbers (more useful if you have full routing table exported on your router)
 - Src hosts/ports, destination hosts and ports
 - Unidirectional or Bi-directional flows
 - Flows on specific interfaces
 - Protocols and TOS

Profile: live

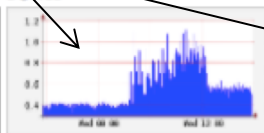
TCP



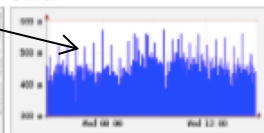
UDP



ICMP

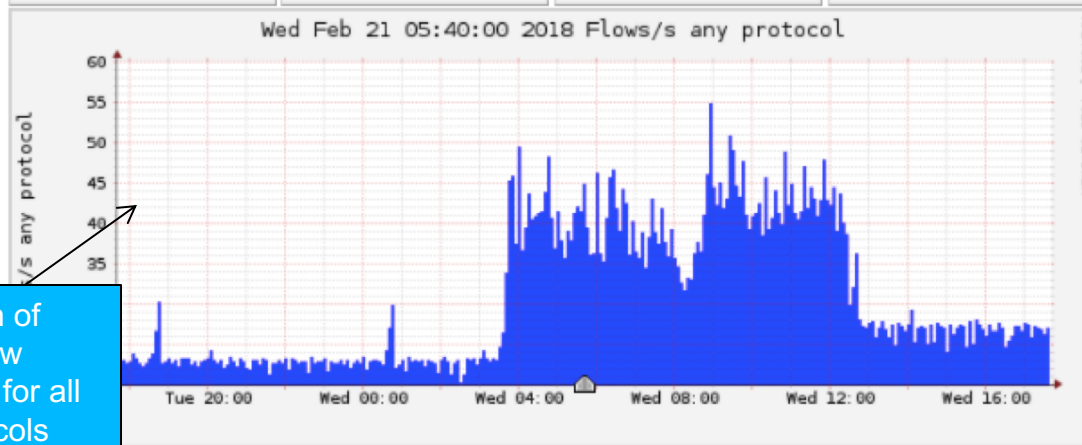


other



Netflow traffic graphs organized by Protocol

Type: live
Max: unlimited
Exp: never
Start: Oct 07 2017 - 12:25 UTC
End: Feb 21 2018 - 17:40 UTC



t_start 2018-02-21-05-40

t_end 2018-02-21-05-40

Packets



Traffic



Time period for flows being observed

Graph of Netflow traffic for all Protocols

Select Single Timeslot

Display: 1 day << < | ^ > >> >|

Lin Scale Stacked Graph
Log Scale Line Graph

Statistics timeslot Feb 21 2018 - 05:40

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
<input checked="" type="checkbox"/> gw	44.9 /s	11.9 /s	31.8 /s	0.7 /s	0.5 /s	345.6 /s	256.6 /s	79.5 /s	5.6 /s	3.8 /s	1.2 Mb/s	1.1 Mb/s	107.8 kb/s	4.3 kb/s	2.3 kb/s
TOTAL	44.9 /s	11.9 /s	31.8 /s	0.7 /s	0.5 /s	345.6 /s	256.6 /s	79.5 /s	5.6 /s	3.8 /s	1.2 Mb/s	1.1 Mb/s	107.8 kb/s	4.3 kb/s	2.3 kb/s

Routers being monitored

Display: Sum Rate

Processing

Source:

gw

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

Extended Netflow processing options

Clear Form process

Profiles and Channels

- **channel** is a type of traffic of interest
 - Total HTTP, HTTPS, SMTP traffic (etc)
 - Traffic to and from the Science department
- **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 100.68.4.130`
`[src|dst] ip in <addr1> <addr2>`
`<addr3>`

Filters (ctd)

- **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 (ctd)

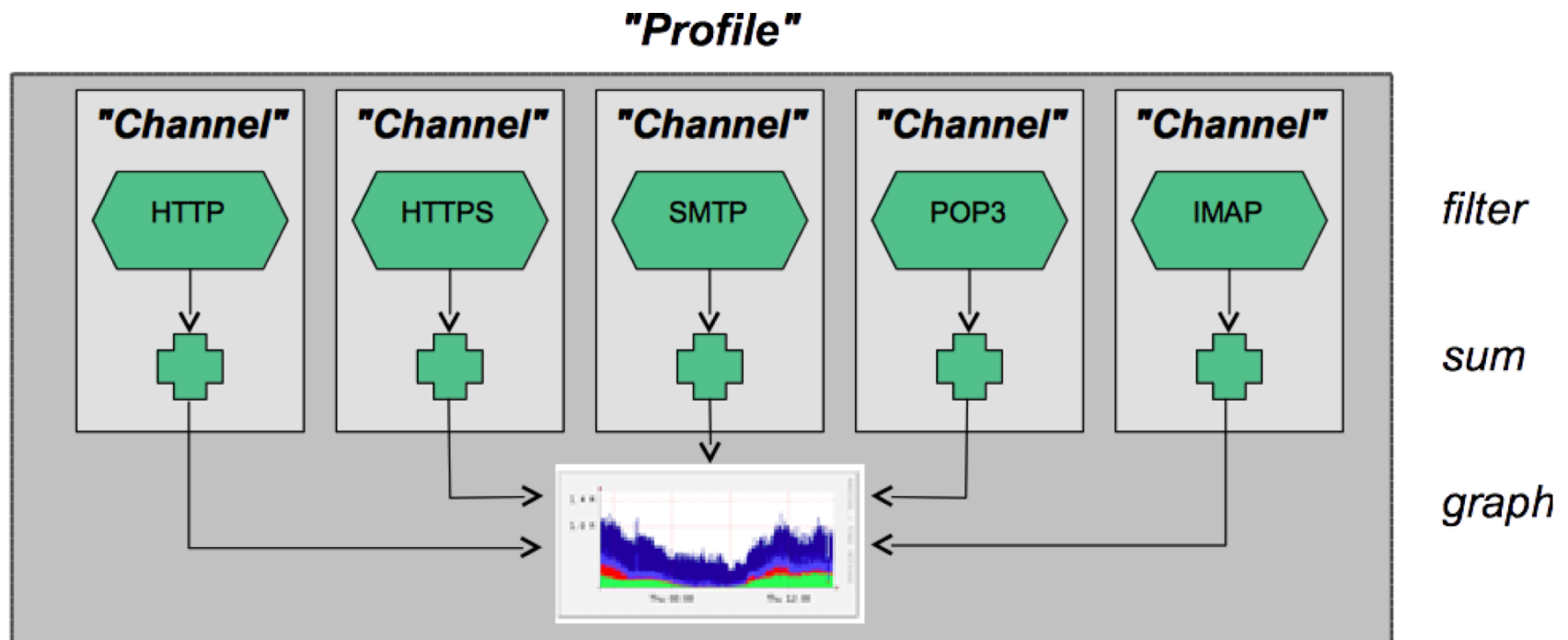
- Bytes: `bytes > 1024`
`bytes = 64`
- Packets per second: `pps > 10`
- Bits per second: `bps > 10m`
- Bits per packet: `bpp > 15`
- Duration of flow: `duration > 360000000`
- AS Number: `[src|dst] 23456`
- All numbers can have scaling factors:
`k, m, g, t` with 1024 as factor

Example filters

- `proto tcp and (port 80 or port 443)`
- `proto tcp and (src ip 172.21.10.2 or dst ip 172.21.20.2)`
- `proto tcp and (net 172.21.10/24 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 at:

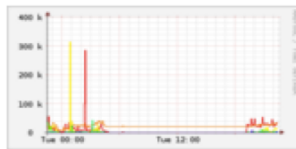
<http://sourceforge.net/projects/nfsen-plugins/>

PortTracker

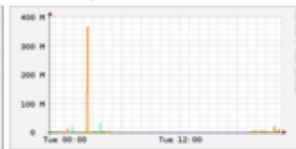
PortTracker

Port Tracker

TCP Packets



TCP Bytes



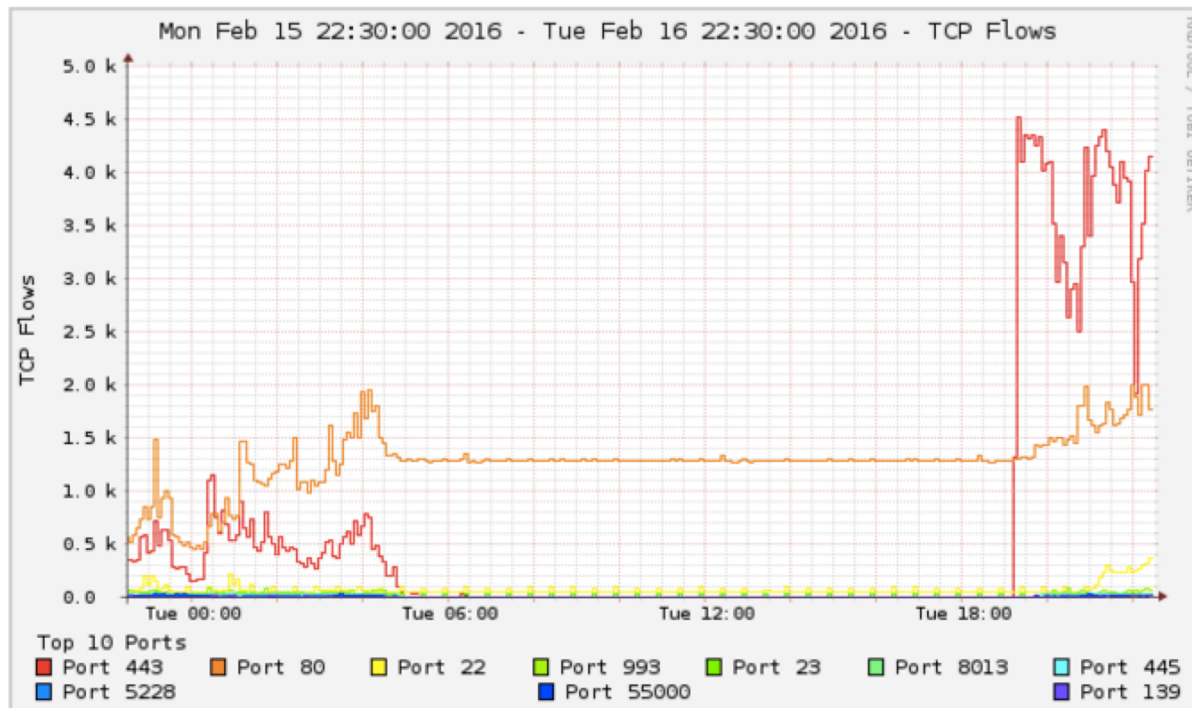
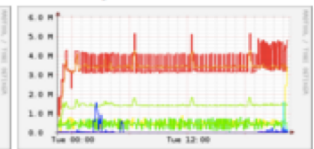
UDP Flows



UDP Packets



UDP Bytes



Show Top 10 Ports

☒ now ☐ 24 hours

Track Ports:

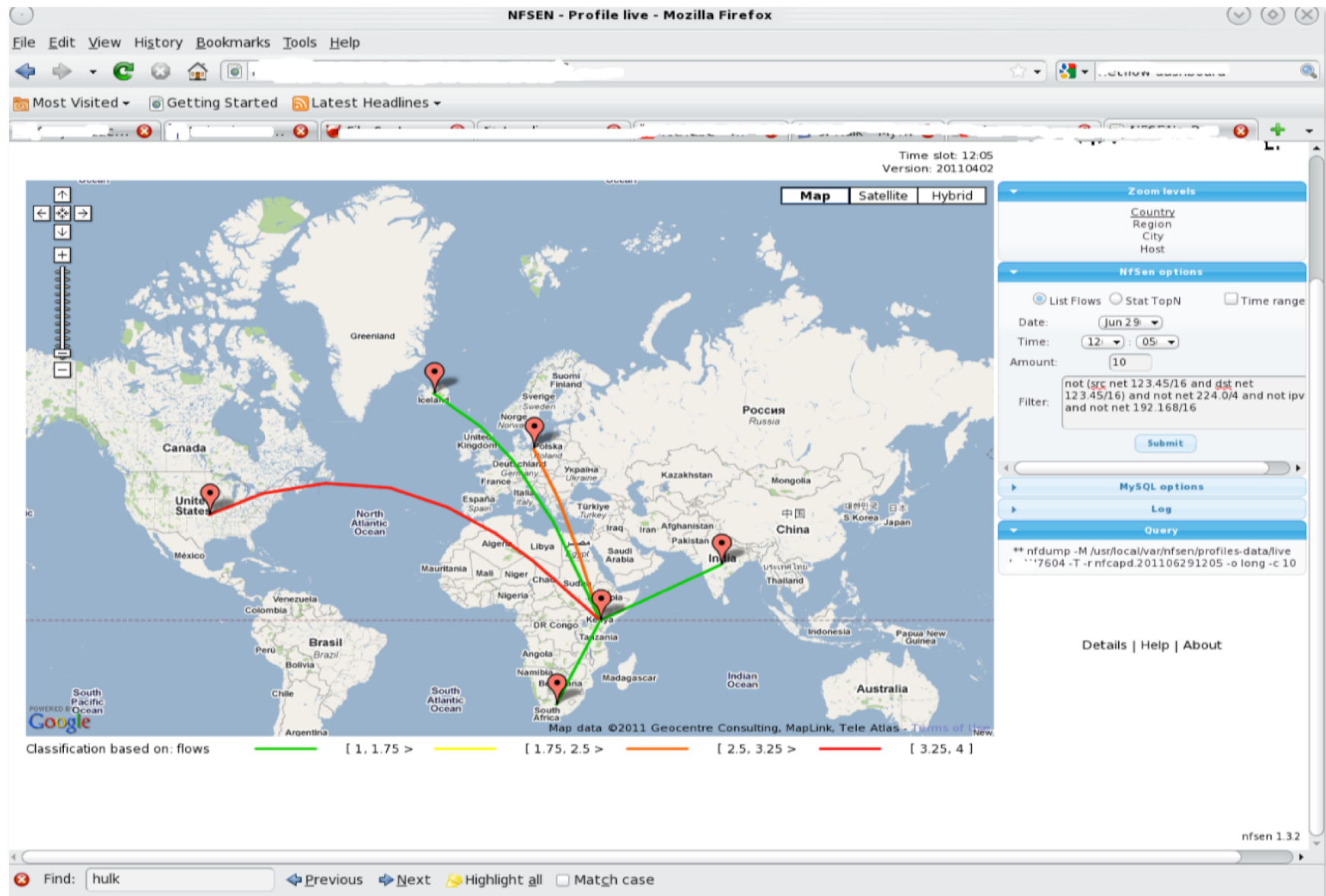
Skip Ports:

Display 1 day

Y-axis: ☒ Linear ☐ Log

Type: ☐ Stacked ☒ Line

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*

Netflow Processing

Source: gw

Filter: dst ip 100.68.100.250

Options:

- ☐ List Flows
- ☒ Stat TopN

Top: 10

Stat: Flow Records

order by: bytes

☒ bi-directional

☐ proto

☐ srcPort

☐ dstPort

Limit: Packets

Output: auto

☐ / IPv6 long

```
** nfdump -M /var/nfsen/profiles-data/live/gw -T -R 2018/02/21/nfcapd.201802210335:2018/02/21/nfcapd.201802211225 -n 10 -s record/bytes -B
nfdump filter:
dst ip 100.68.100.250
Command line switch -s overwrites -a
```

Note the protocol

The ports are your clue!

Aggregated flows 99398

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
2018-02-21 03:34:52.092	31928.580	UDP	100.68.100.254:35496	100.68.100.250:9996	0	105902	0	49.6 M	105
2018-02-21 03:32:12.840	32109.068	UDP	100.68.100.254:36576	100.68.100.250:9996	0	47328	0	23.3 M	104
2018-02-21 09:56:43.799	4.108	TCP	100.64.2.2:49476	100.68.100.250:22	0	994	0	1.4 M	2
2018-02-21 09:57:42.079	3.435	TCP	100.64.2.2:49484	100.68.100.250:22	0	376	0	466586	2

Unidirectional (*Details* tab)

Netflow Processing

Source: gw Filter: host 100.68.100.250

All Sources and <none>

Options:

☐ List Flow ☒ Stat Top

Top: 10

Stat: Flow records order by bytes

☐ bi-directional

Aggregate

☒ proto

☒ srcPort ☒ dstPort

Limit: Packets

Output: auto / IPv6 long

Clear Form process

```
** nfdump -M /var/nfsen/profiles-data/live/gw -T -R 2018/02/21/nfcapd.201802210330:2018/02/21/nfcapd.201802211240 -n 10 -s record/bytes -A proto,srcip,srcport,dstip,dstport
nfdump filter:
host 100.68.100.250
Aggregated flows 214568
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
2018-02-21 03:29:49.836 33135.809 UDP      100.68.100.254 35496    100.68.100.250 9096     110030    51.5 M   12435  468   109
2018-02-21 03:27:01.420 33377.576 UDP      100.68.100.254 16576    100.68.100.250 9996     47794    23.5 M   5627   491   108
2018-02-21 09:56:43.799 4.108     TCP      100.64.2.2    19476    100.68.100.250 22       994       1.4 M    2.7 M   1391   2
2018-02-21 06:21:25.520 59.925    TCP      100.68.100.250 80        100.64.2.2    64319    168       695652   92869   4140   2
2018-02-21 03:27:50.353 33308.646 ICMP     100.68.100.250 0         100.68.6.1    0        7206     605304   145     84   104
2018-02-21 09:57:42.079 3.435     TCP      100.64.2.2    49484    100.68.100.250 22       376       466586   1.1 M   1240   2
2018-02-21 03:27:23.045 33041.950 ICMP     100.68.100.250 0         100.68.1.1    0        5552     466368   112     84   107
2018-02-21 03:27:13.254 33051.972 ICMP     100.68.100.250 0         100.68.1.1    0        5344     448896   108     84   107
2018-02-21 03:27:33.038 33031.345 ICMP     100.68.100.250 0         100.68.4.1    0        5336     448224   108     84   107
2018-02-21 03:27:23.046 33041.307 ICMP     100.68.100.250 0         100.68.2.1    0        5322     447048   108     84   107
Summary: total flows: 265760, total bytes: 320009429, total packets: 1519967, avg bps: 76226, avg pps: 45, avg bpp: 210
Time window: 2018-02-21 03:24:01 - 2018-02-21 12:44:52
Total flows processed: 1349168, Blocks skipped: 0, Bytes read: 98026892
Sys: 0.548s flows/second: 2461985.4 Wall: 0.763s flows/second: 1766828.6
```

References

NfSen

<http://nfsen.sourceforge.net>

NfDump

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

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

Exercises