

Network Monitoring and Management

NfSen

Netflow Sensor

INNOG 6

March 22 - 25, 2023



This material is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>)

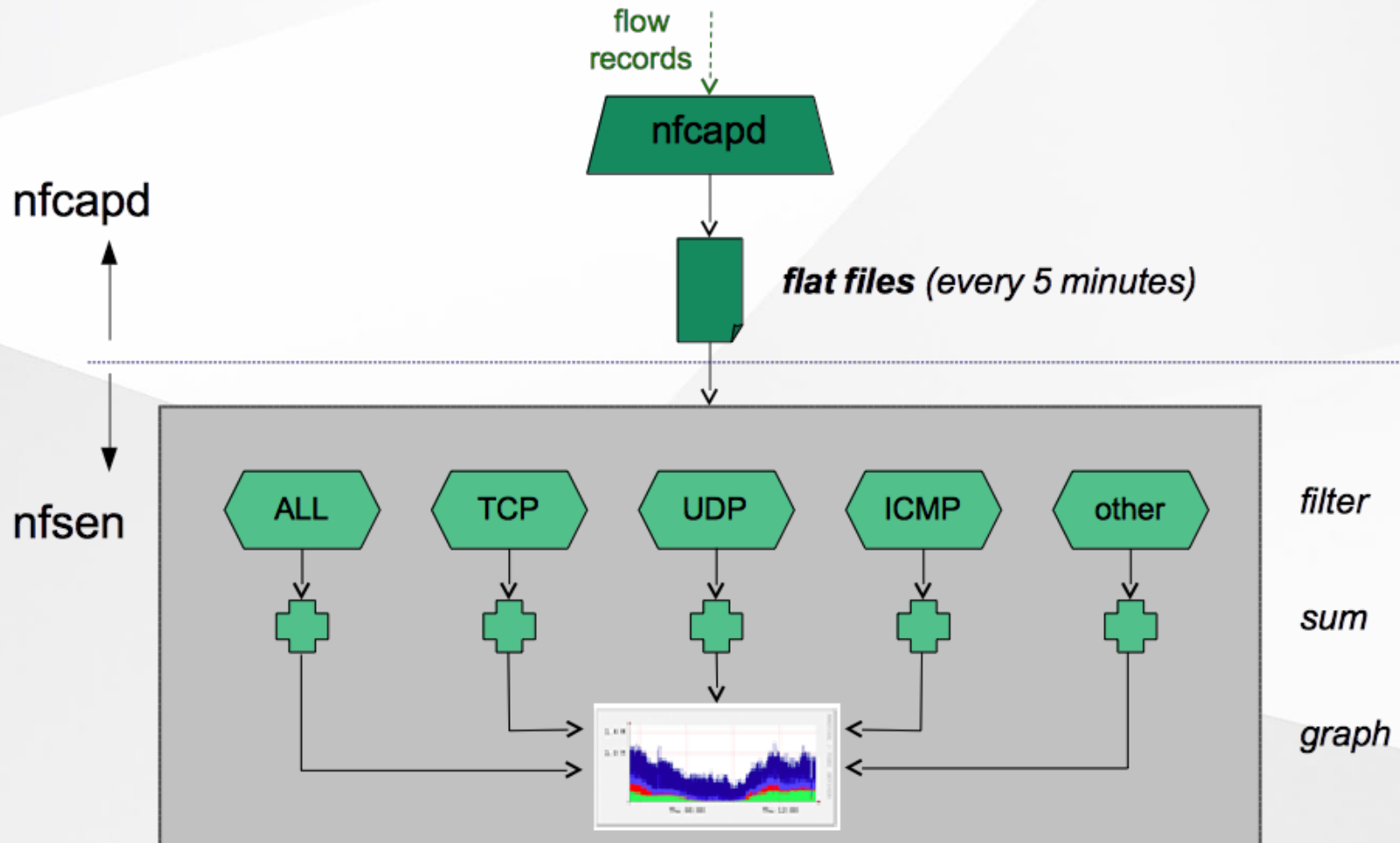
What is NfSen

- 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



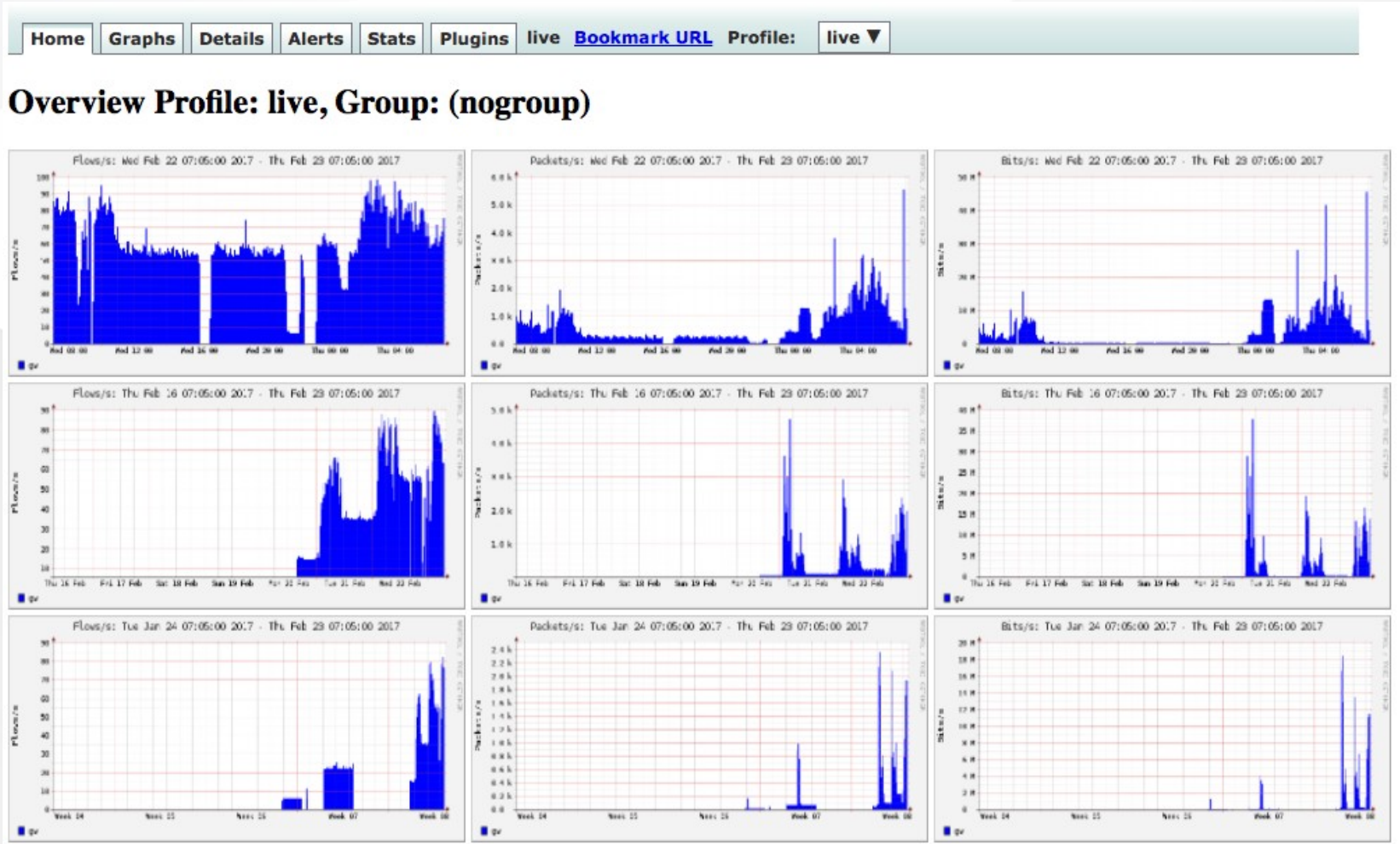
NfSen: Points to note

- 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 - ***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



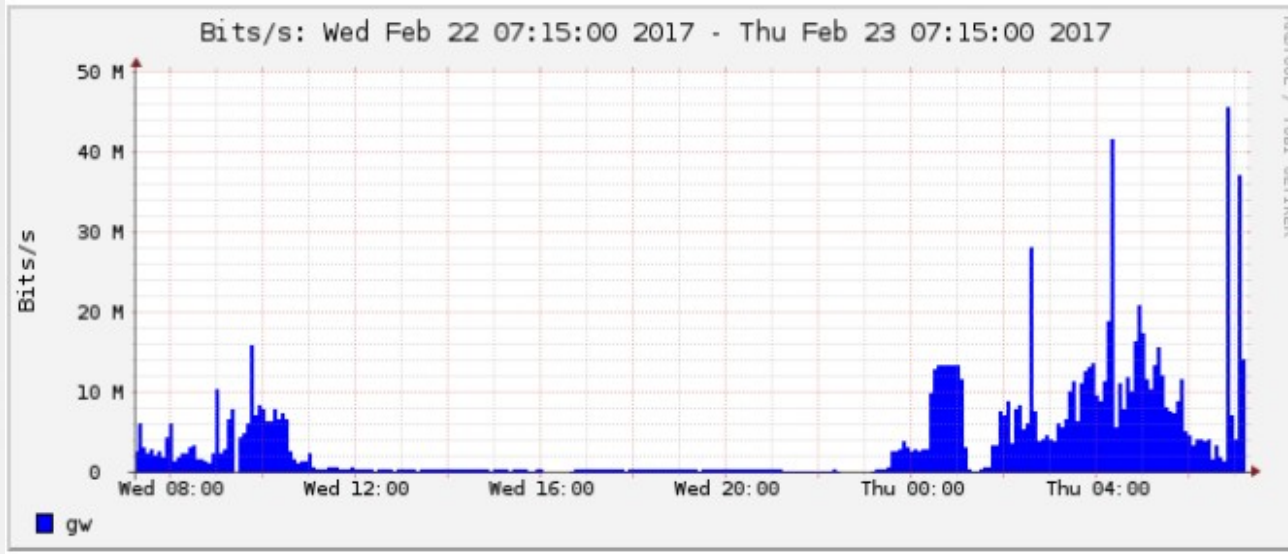
Graphs Tab

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



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

Details Page (Contd.)

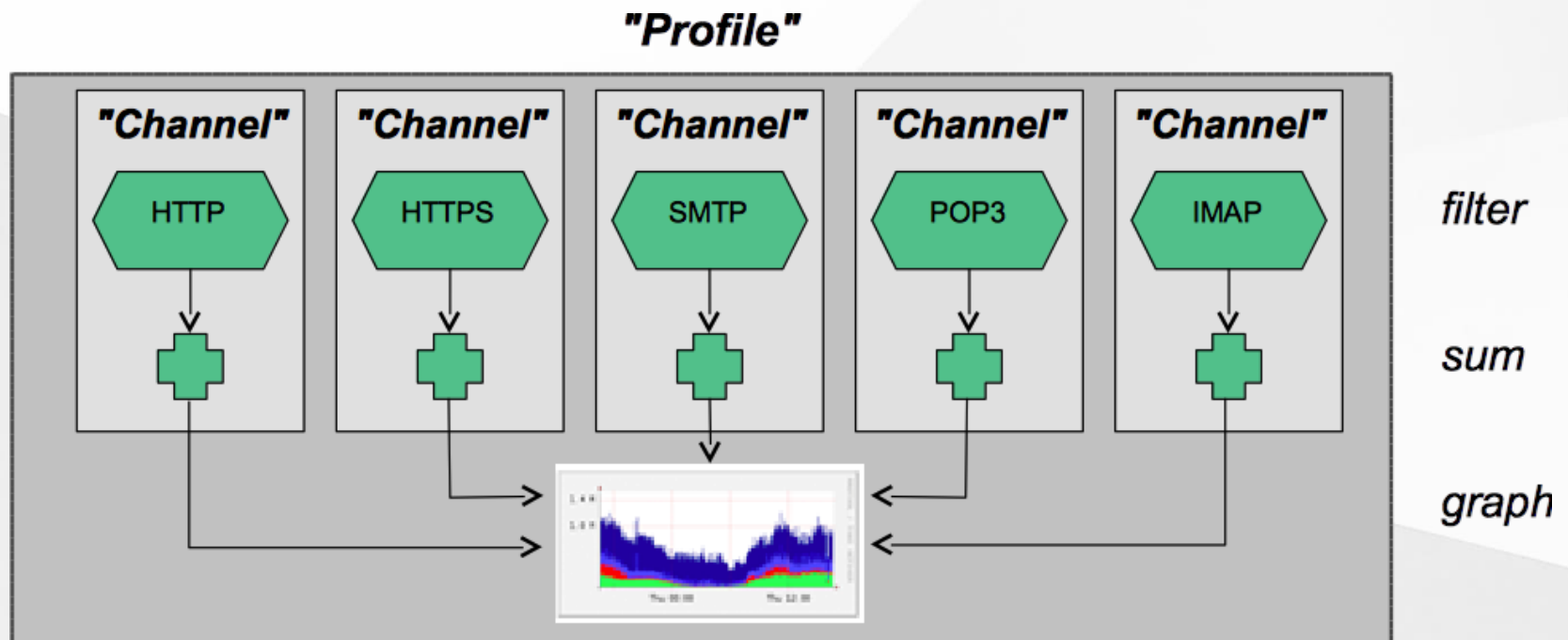


Profiles and Channels

- 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 > 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 172.16.17.18 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

PortTracker

Port Tracker

TCP Packets



TCP Bytes



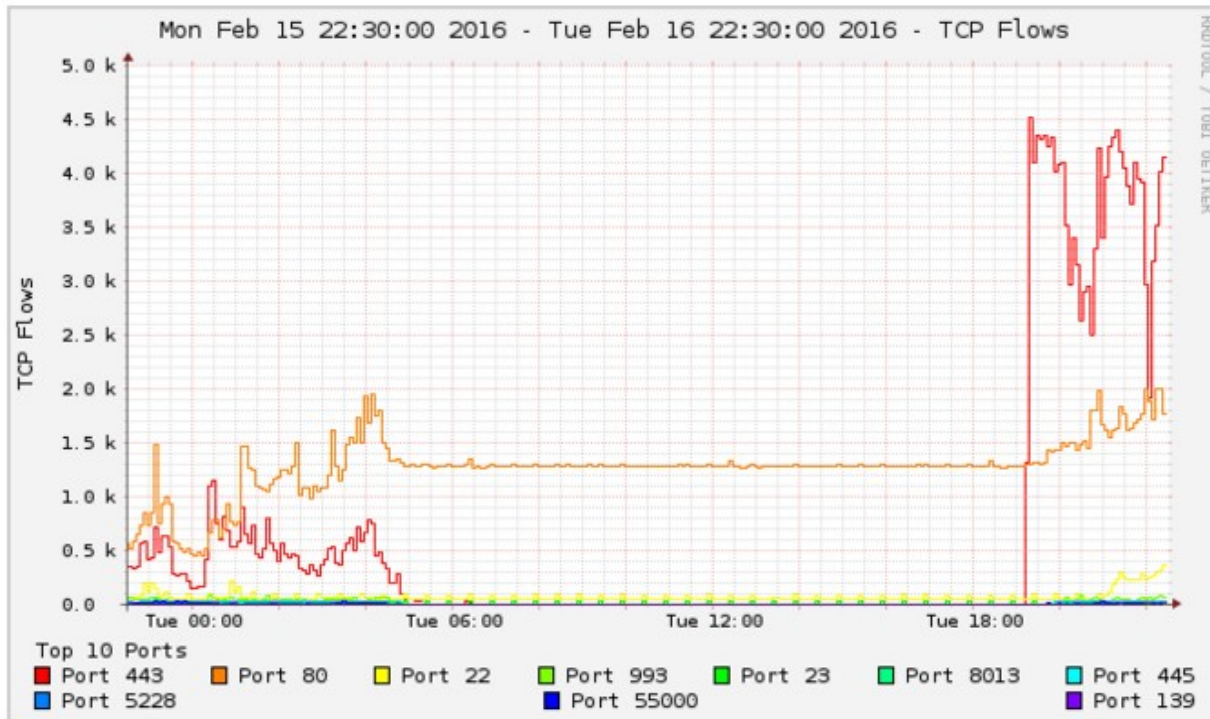
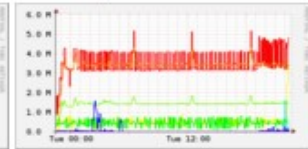
UDP Flows



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

Plugin: SURFmap

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

SURFmap SSHCure

SURFmap
A network monitoring tool based on the Google Maps API

UNIVERSITY OF TWENTE.



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 10.10.0.250

Options:

- ☐ List Flows ☒ Stat TopN
- Top: 10
- Stat: Flow Records order by bytes
- ☒ bi-directional
- ☐ proto
- ☐ srcPort srcIP
- ☐ dstPort dstIP
- Limit: Packets > 0
- Output: auto / IPv6 long

Clear Form process

```
** 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
```

Note the protocol

These ports are your clue!

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

Unidirectional (Details tab)

Netflow Processing

Source: gw **Filter:** dst ip 10.10.0.250

Options:

- ☐ List Flows ☒ Stat TopN
- Top:** 10
- Stat:** Flow Records **order by:** bytes
- ☒ bi-directional
- ☐ proto
- ☐ srcPort ☐ srcIP
- ☐ dstPort ☐ dstIP
- Limit:** ☐ Packets ☐ > 0 ☐ -
- Output:** auto ☐ / IPv6 long

Clear Form process

```
** 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!

References

NfSen

<http://nfsen.sourceforge.net>

NfDump

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

