Using NfSen

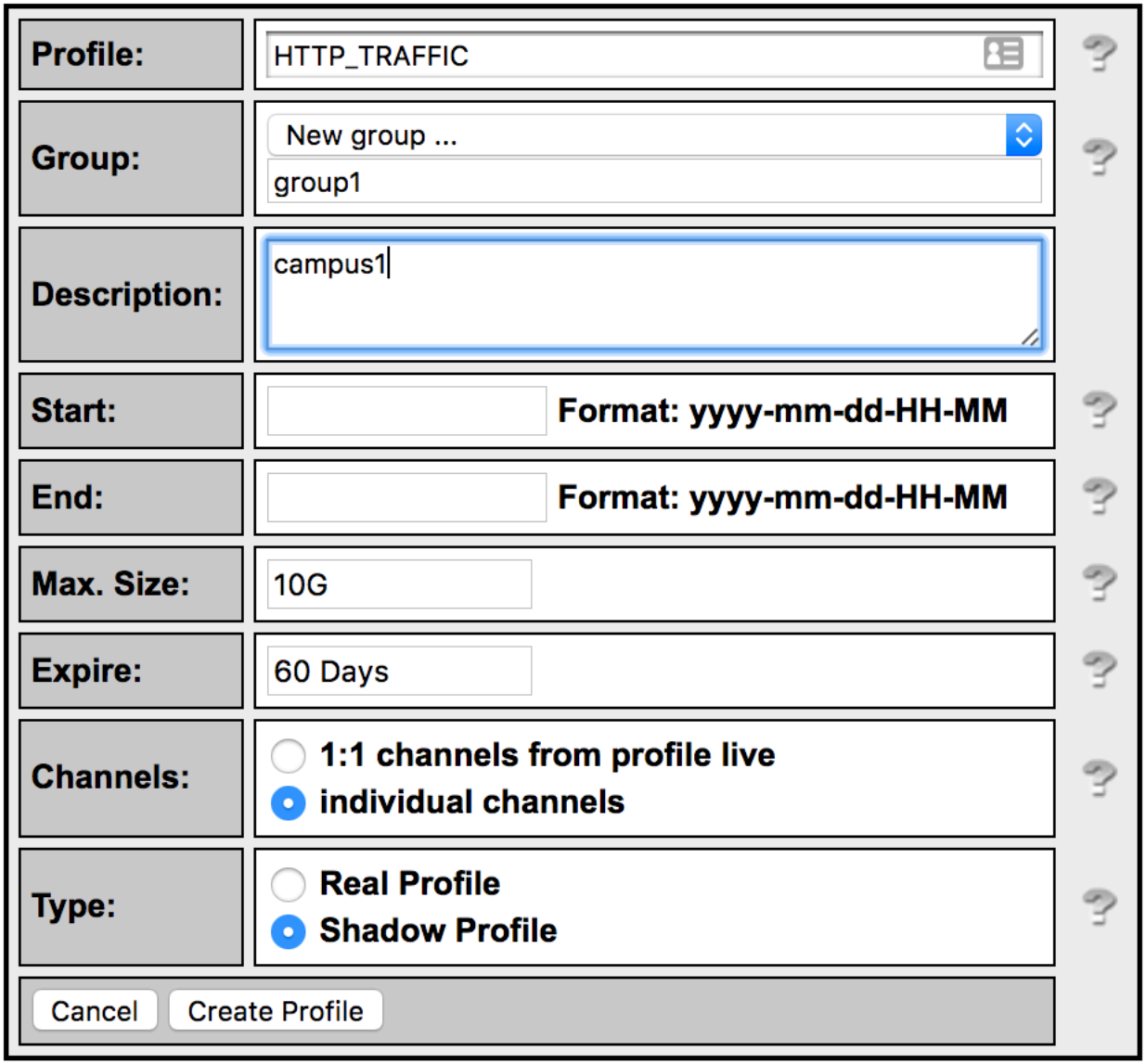
What we will do

1. Your router should be sending flows to each DB server in your group from bdr1 router
2. Ensure NfSen is running by browsing on the page and ensuring you can see the graphs with no errors indicated
3. We will now see what type of traffic is passing through your group's router

Create a Stat to graph specific traffic

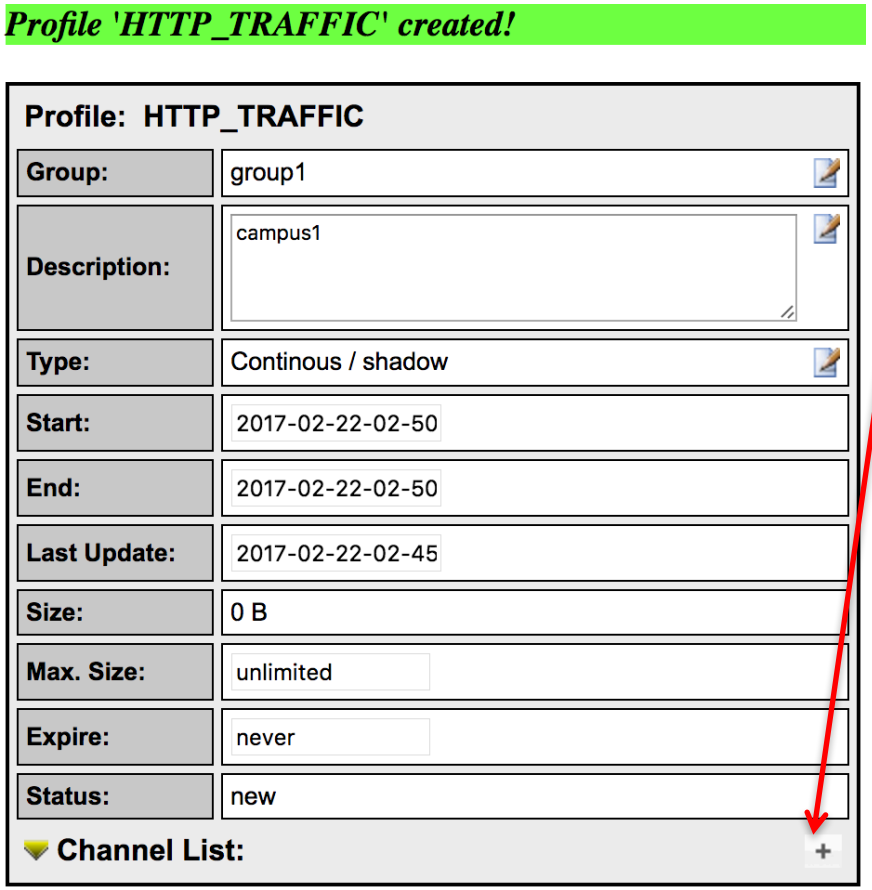
- Open the NFSEN page and click on ‘live’ on the top right of the page and select “New Profile …”
  - *You may need to select several times as NfSen is picky.*
- Enter the name ‘HTTP_TRAFFIC’ for the profile name and additionally create a new group called “groupX” where X is your group number
- Select individual channels and shadow profile.
  - Individual channel – can create channels with own filters
  - Shadow profile – save hard disk space by not creating new data but instead analyses already collected data

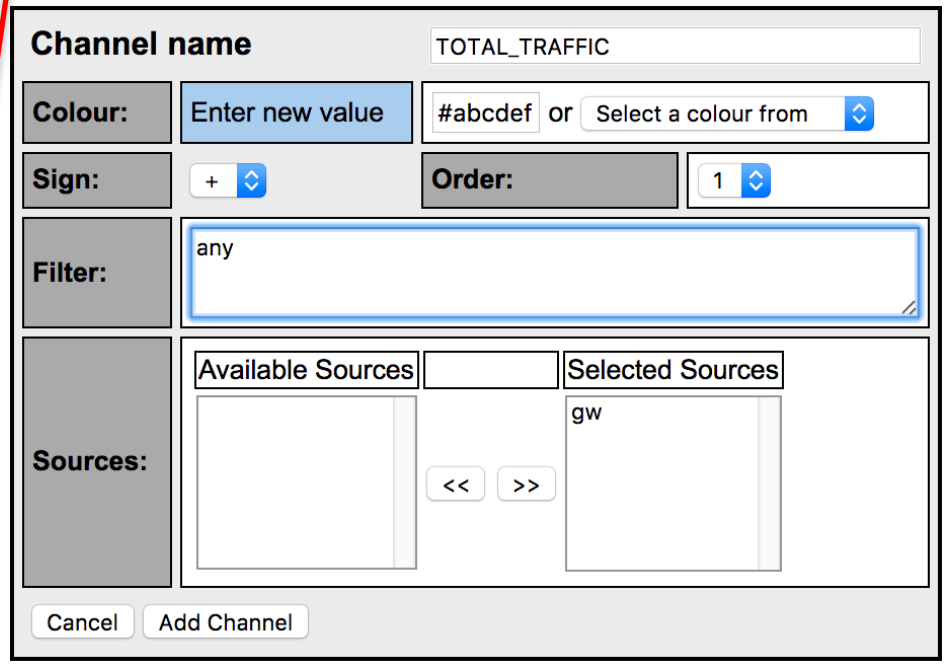
➔ **See next page for an example image…**

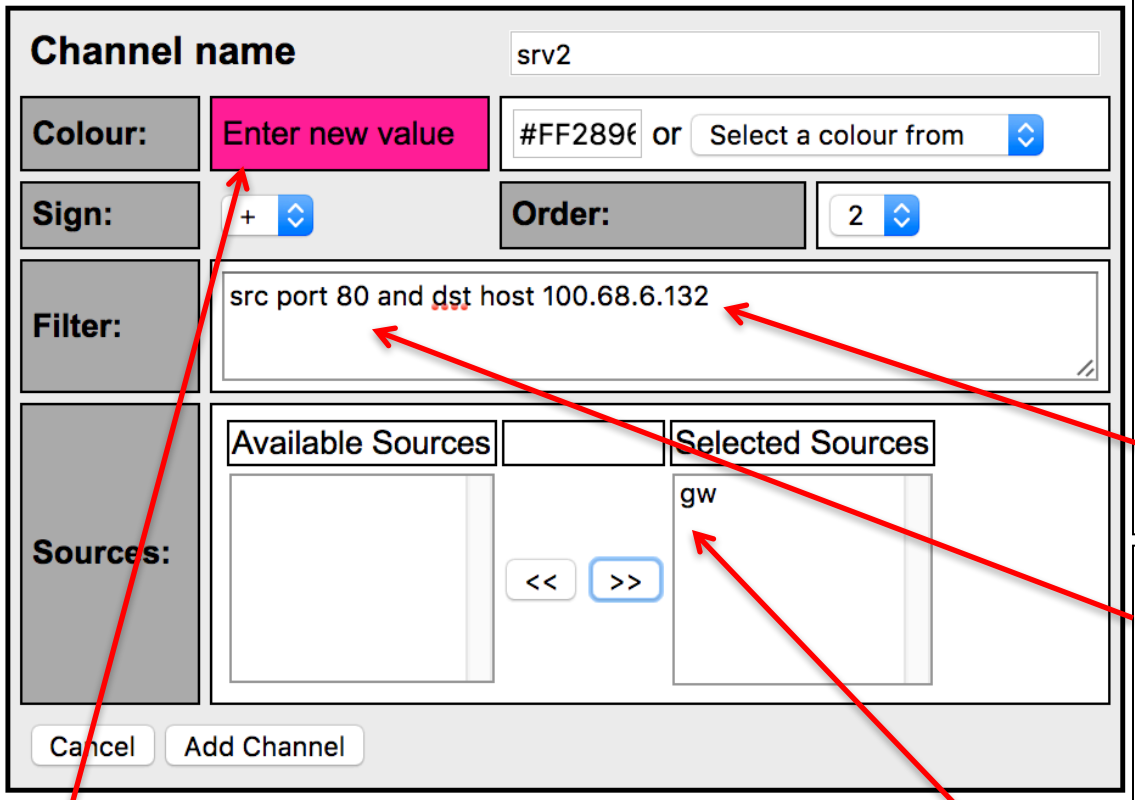


Click “Create Profile” at the bottom of the menu.

Click on the plus (+) sign next to ‘Channel List’ at the bottom of the page then fill the next page as below and click on ‘Add Channel’ at the bottom.
The filter “any” means ALL traffic. Select your sources in “Available Sources” and press the “>>” to add them to “Selected Sources.” Click on “Add Channel”







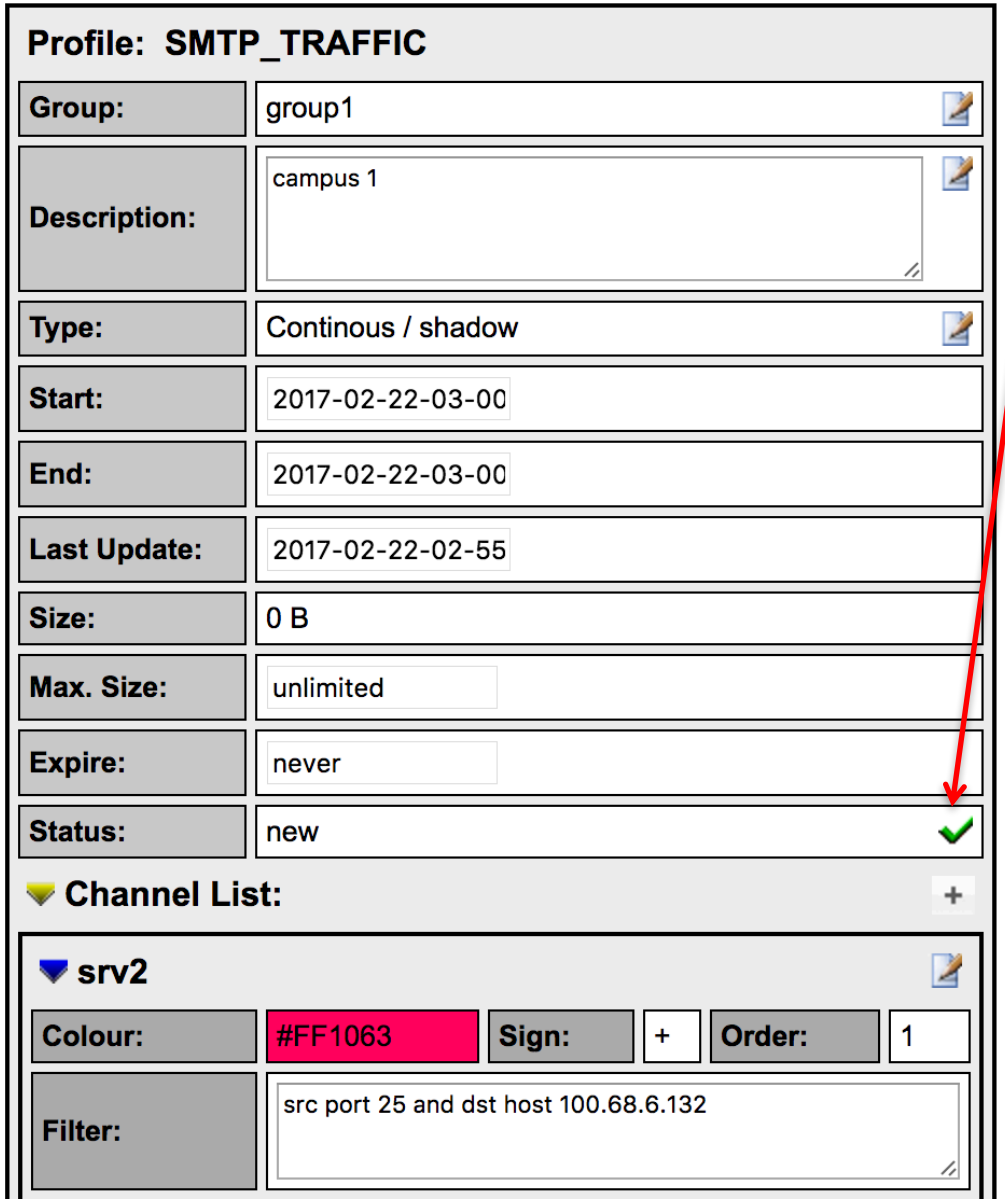
Add another channel by clicking the plus sign as before next to 'Channel List'. Fill the details as shown on the left. Replace srvX with the server number in your campus that is not yours. Also, replace the IP address in the Filter to match the IP of the SRV in question. i.e
100.68.6(campus6).131(srv1)
100.68.6(campus6).132(srv2)

With this, we will track how much HTTP traffic is going to that PC. That is how much is actually being downloaded. In a HTTP download, source traffic is from port 80 always

Ensure you change the color. You can use the color picker or enter the value shown in this example

Select your group's routers as the source then click add channel. This will be the netflow exported from bdr1.campusY

Activate the profile



- Click the green tick to activate your new profile.
- Click on Live then select the group you created and “HTTP_TRAFFIC” you will see your profile. Then click on the “Home” menu item on the upper left of the NfSen screen.

Download HTTP data to srvY

Log in on srvY in your group and use the `wget` command to simulate an HTTP download.

```
ssh sysadm@srvY.campusY.ws.nsrc.org
$ cd /tmp
$ wget http://www.ws.nsrc.org/downloads/BigFile
```

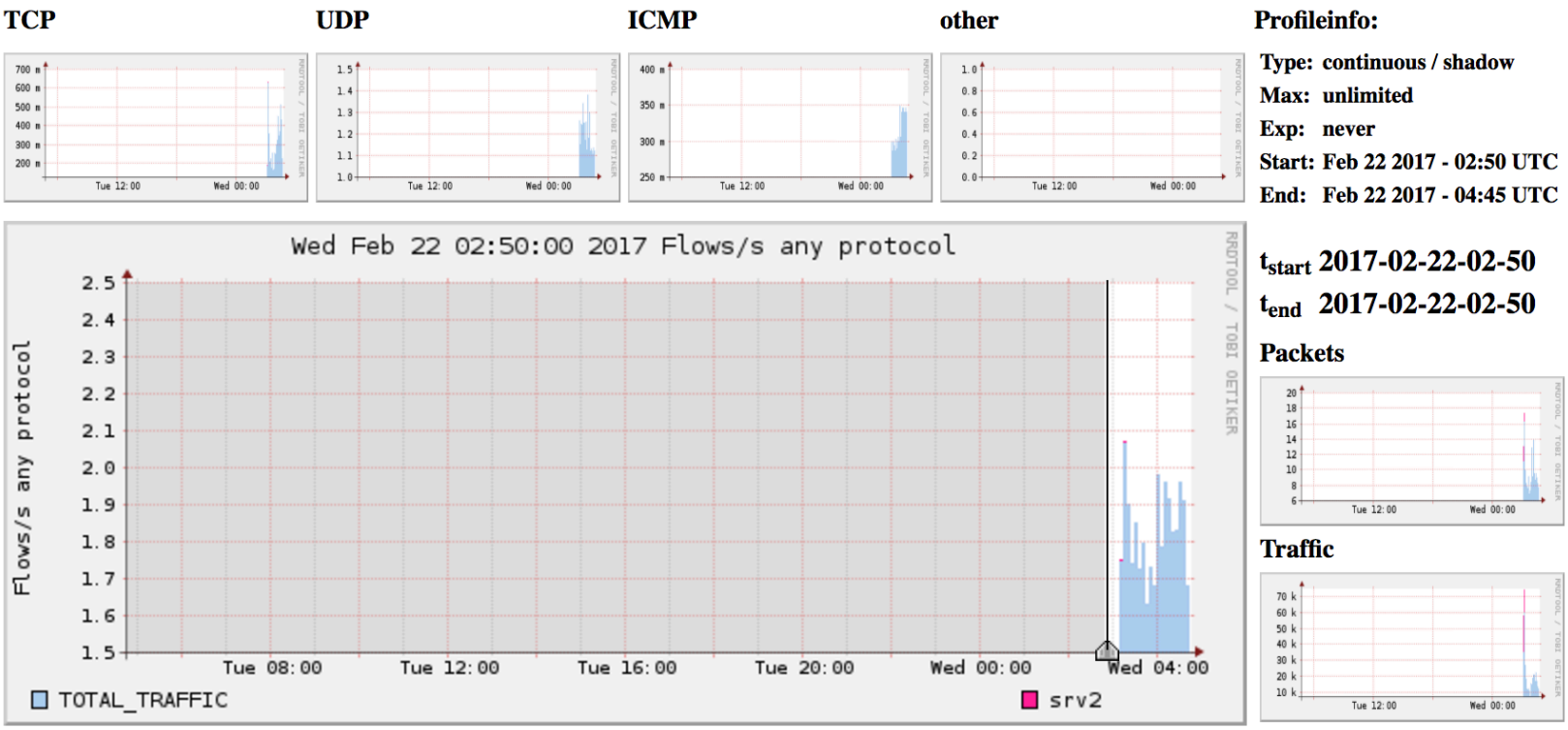
Once the download completes you can delete the file:

```
$ rm /tmp/BigFile
$ exit
```

(to log off from srvY.campusY)

See the traffic

Your graph will take up to 15 min to update. Go to Graphs then Traffic. Then go to details and select ‘Line Graph’ at bottom

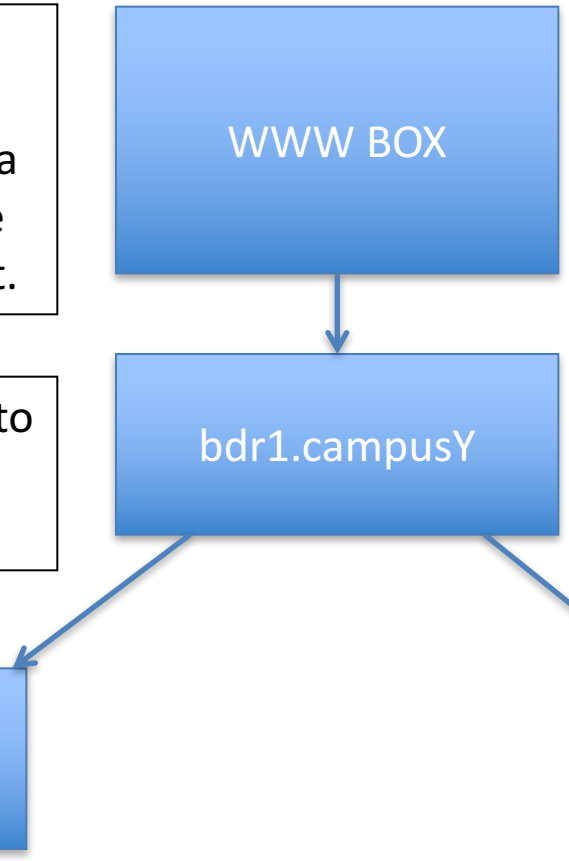


This is a graph of the total traffic passing through the router bdr1.campusX **<u>vs the HTTP downloads that srvY.campusY is making</u>**

Stop! What's happening here?

The NOC (www.ws.nsrc.org) box is running a HTTP server. In a real network this could be any server on the Internet.

Router is exporting flows to the NFSEN Server and NFSEN graphs



SrvY is downloading a file over HTTP via bdr1.campusX and is the destination host aka 'dst host'

We have told NFSEN to graph traffic where the source port is 80 and the destination host is 100.68.X.Y. You can do the same thing back in your networks and additionally graph a specific web server with 'src host a.b.c.d' eg FaceBook's IP

See an FTP download from the NOC

- Perform the exact same steps from slide number 5 but this time, change 'HTTP_TRAFFIC' to 'FTP_TRAFFIC'
- The FTP could randomize the ports so it may not be source port 20. We do know that it will be a port greater than 1024 so the filter should read:
  `src port > 1024 and dst host 100.68.X.Y`
- Make sure to select the correct source from Available Sources.
- Now download the large file from the www box via ftp to srvY.campusY.ws.nsrc.org.
- **➔ See next slide for instructions…**

Download FTP data to srvY

Log in on srvY and use the `ftp` command to generate FTP traffic from the noc to pcY.

```
ssh sysadm@srvY.campusY.ws.nsrc.org
$ sudo apt-get install ftp
$ ftp www.ws.nsrc.org
   Name (www.ws.nsrc.org): test
   331 User test OK. Password required
   Password: nsrc+ws
   ftp> get BigFile
   ftp> quit
$ rm /tmp/BigFile
```

(long time to download)

Your graph will take up to 15min to update. Go to Graphs then Traffic. Then go to details and select 'Line Graph' at bottom to see the results.

Part 2

Graph a specific interface on the router

Use the *snmpwalk* command on your PC to determine the ifIndex number of an interface that you want to graph:

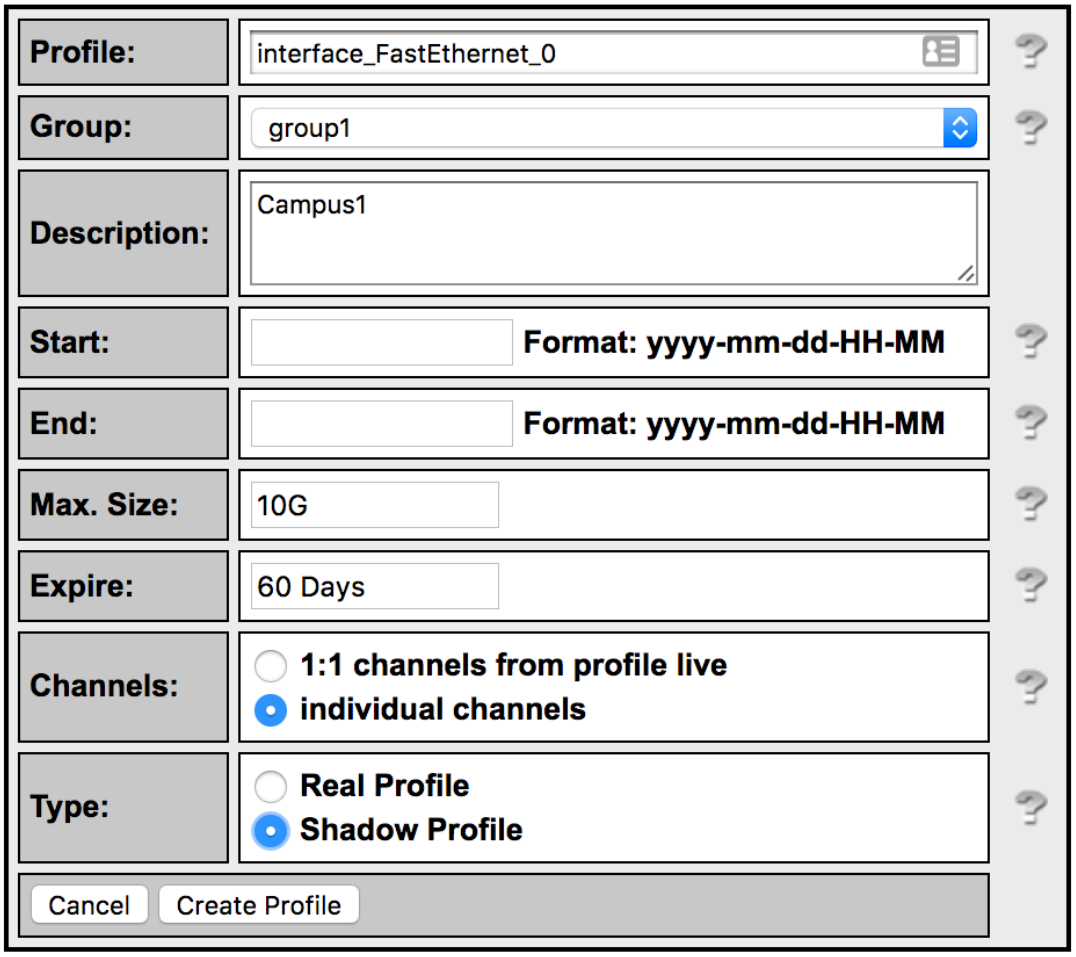
```
$ snmpwalk -v2c -c NetManage bdrX.campusX.ws.nsrc.org
ifDescr

    IF-MIB::ifDescr.1 = STRING: FastEthernet0/0
    IF-MIB::ifDescr.2 = STRING: FastEthernet0/1
    IF-MIB::ifDescr.3 = STRING: Null0
    IF-MIB::ifDescr.4 = STRING: Loopback0
    IF-MIB::ifDescr.5 = STRING: Loopback5
```

This means that interface F0/0 has been assigned index number 1. We can now use NFSEN to graph traffic for this specific interface

- This interface must have 'ip flow egress' or ingress enabled
- With 'snmp ifindex persist' the index number is maintained

Add the interface on NfSen

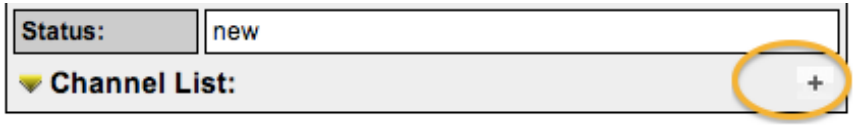


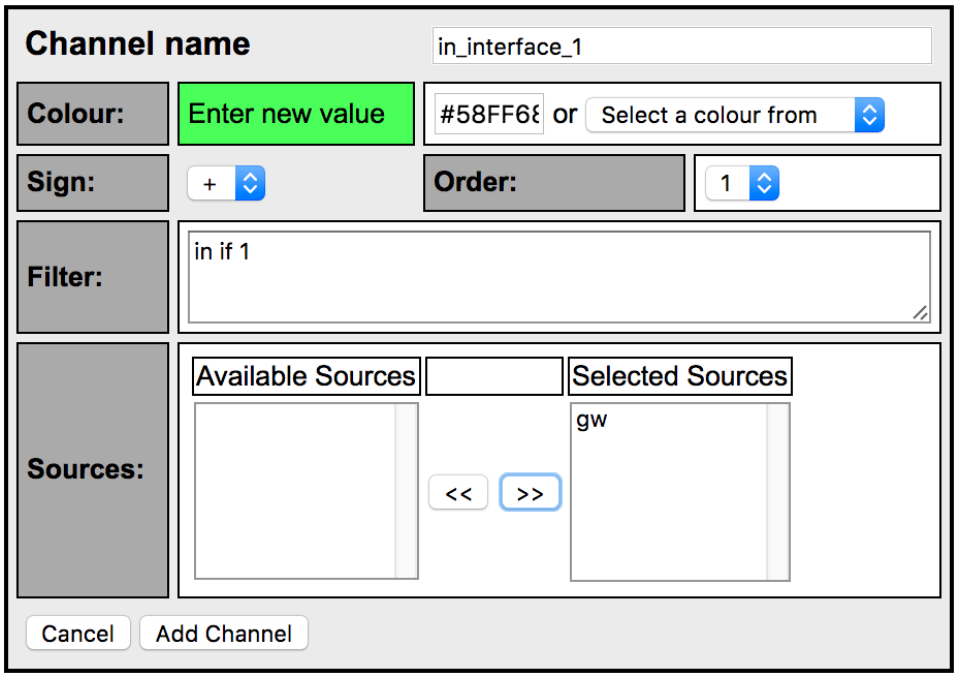
Click on Live and select “New Profile…”

Give the Profile a suitable name and add it to the same Group you created earlier

Choose individual channels and Shadow profile as before and click on “Create Profile”.

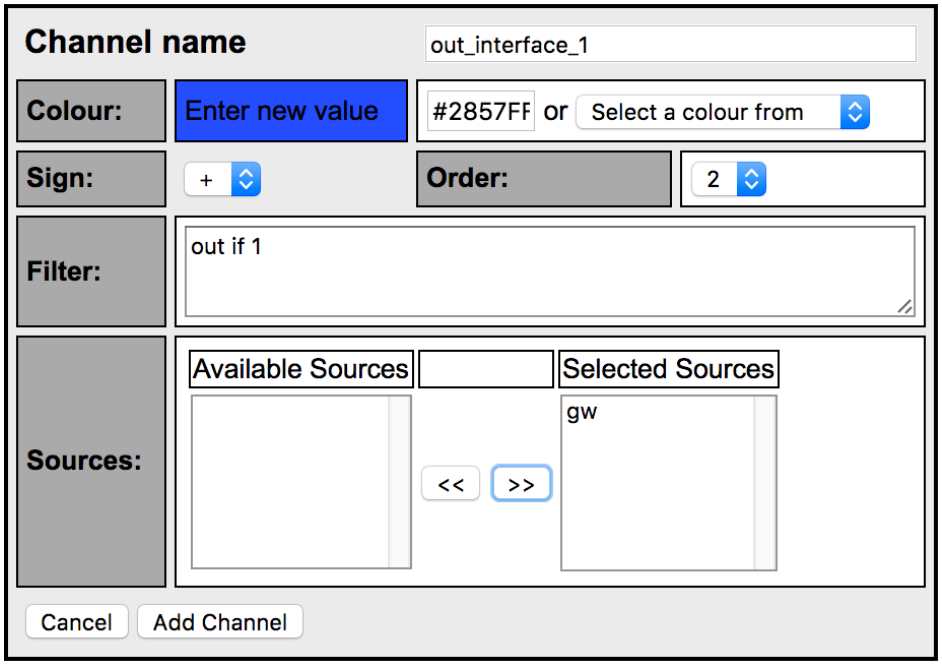
Then on the following screen click on the plus sign next to Channel list



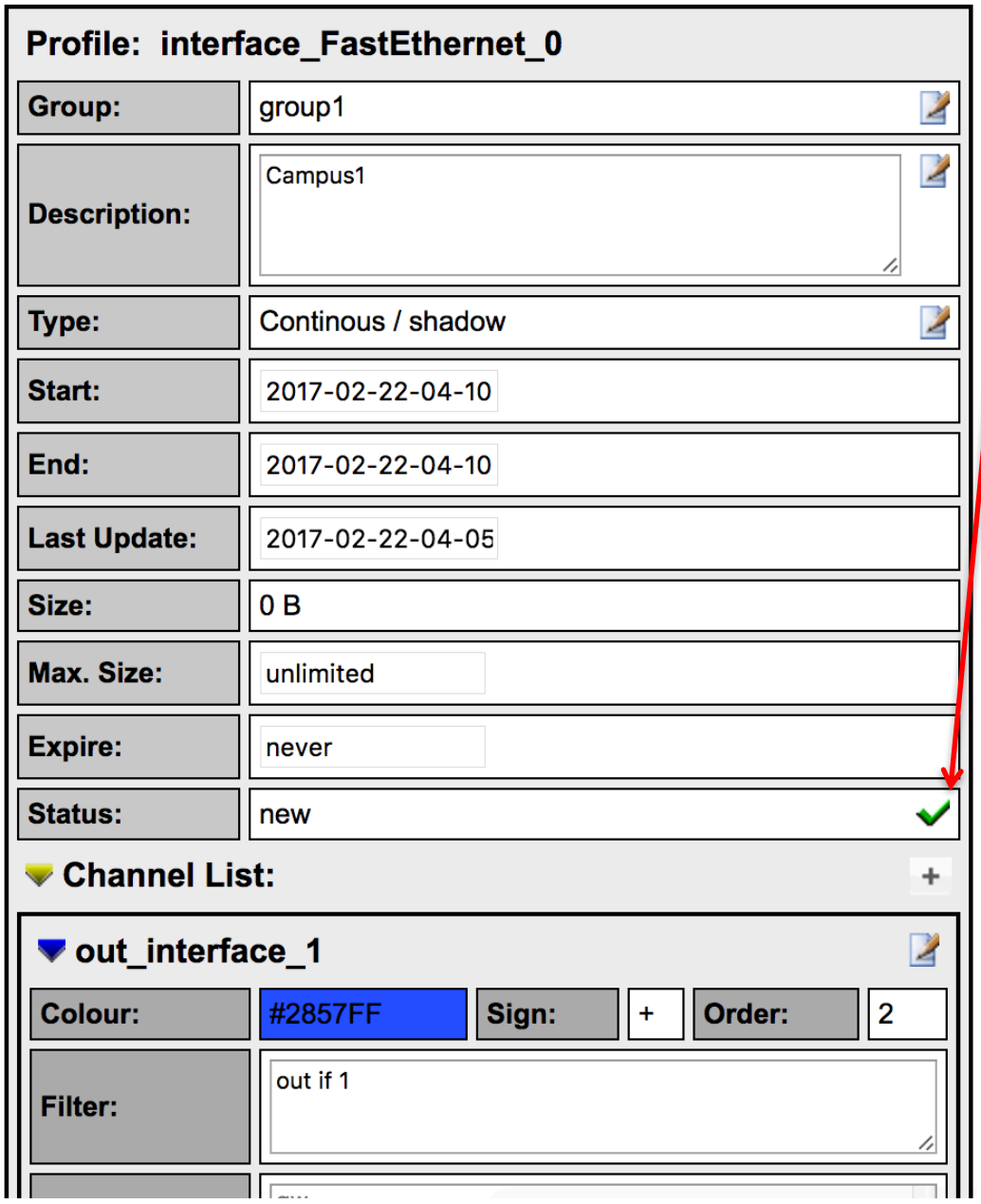


This means graph all traffic passing INTO interface 1. Click “Add Channel” and click plus to add a second channel.

NOTE: Interface “1” refers to the index number that was referring to interface “FastEthernet 0/0” on rtrX.



This means graph all traffic LEAVING/GOING OUT OF interface 1. Click “Add Channel” then activate the filter on the next screen by clickingon the green check.

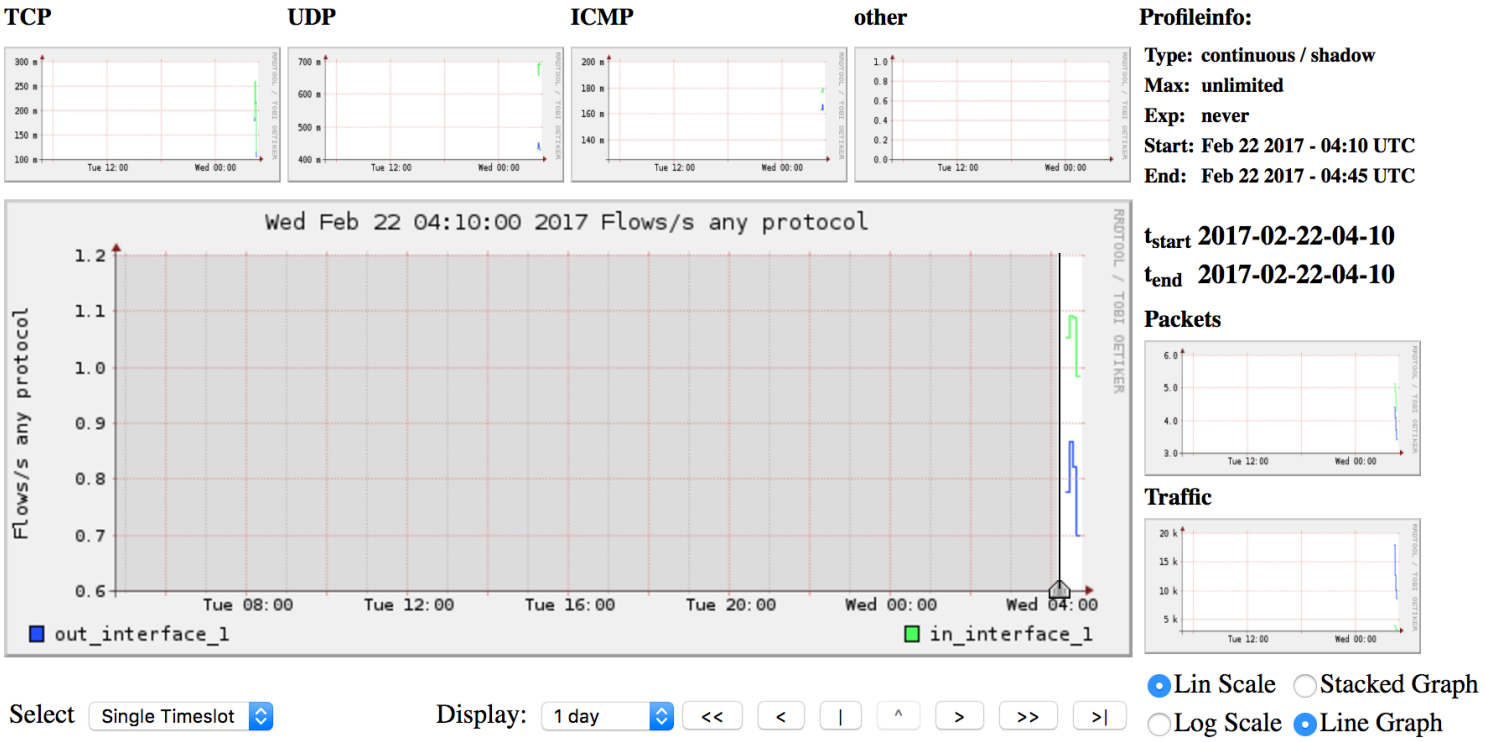


Click on the green color tick to enable it.

Give the graph time to generate. Compare the graph with Cacti's graph

See the traffic

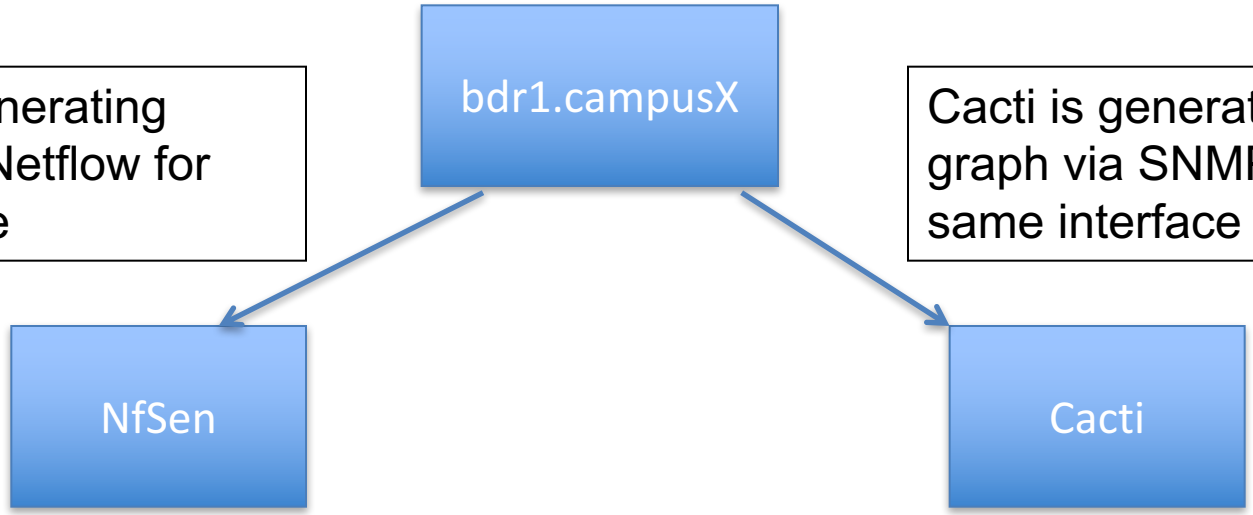
Your graph will take up to 15 min to update. Go to Graphs then Traffic. Then go to details and select ‘Line Graph’ at bottom



This is a graph of the total traffic passing through the router bdr1.campusX on interface FastEthernet 0/0.

Stop! What's happening here?

NfSen is generating graphs via Netflow for the interface



Cacti is generating the graph via SNMP for the same interface

With NfSen, we can use the Netflow features to extract more data like which IP Addresses are active, what are the highest ports in use by bytes, what are the AS Numbers coming/leaving our network and so much more!

Stop! What's happening here?

NfSen is generating graphs via Netflow for the interface

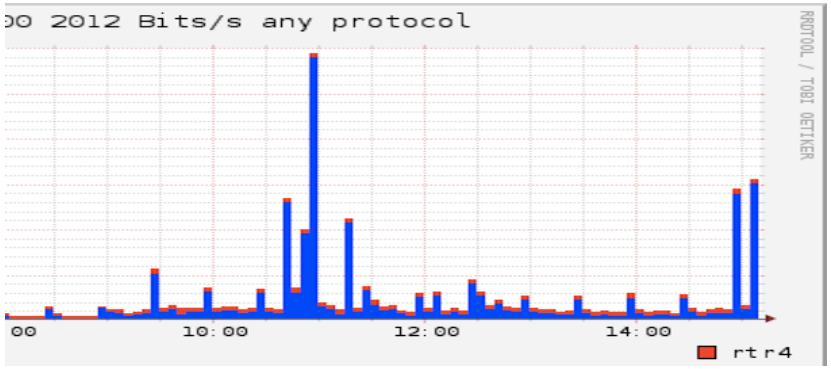
bdr1.campuX

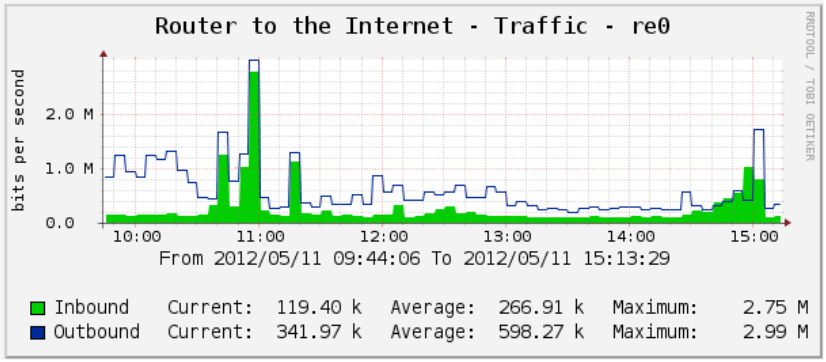
Cacti is generating the graph via SNMP for the same interface

NFSEN

Cacti

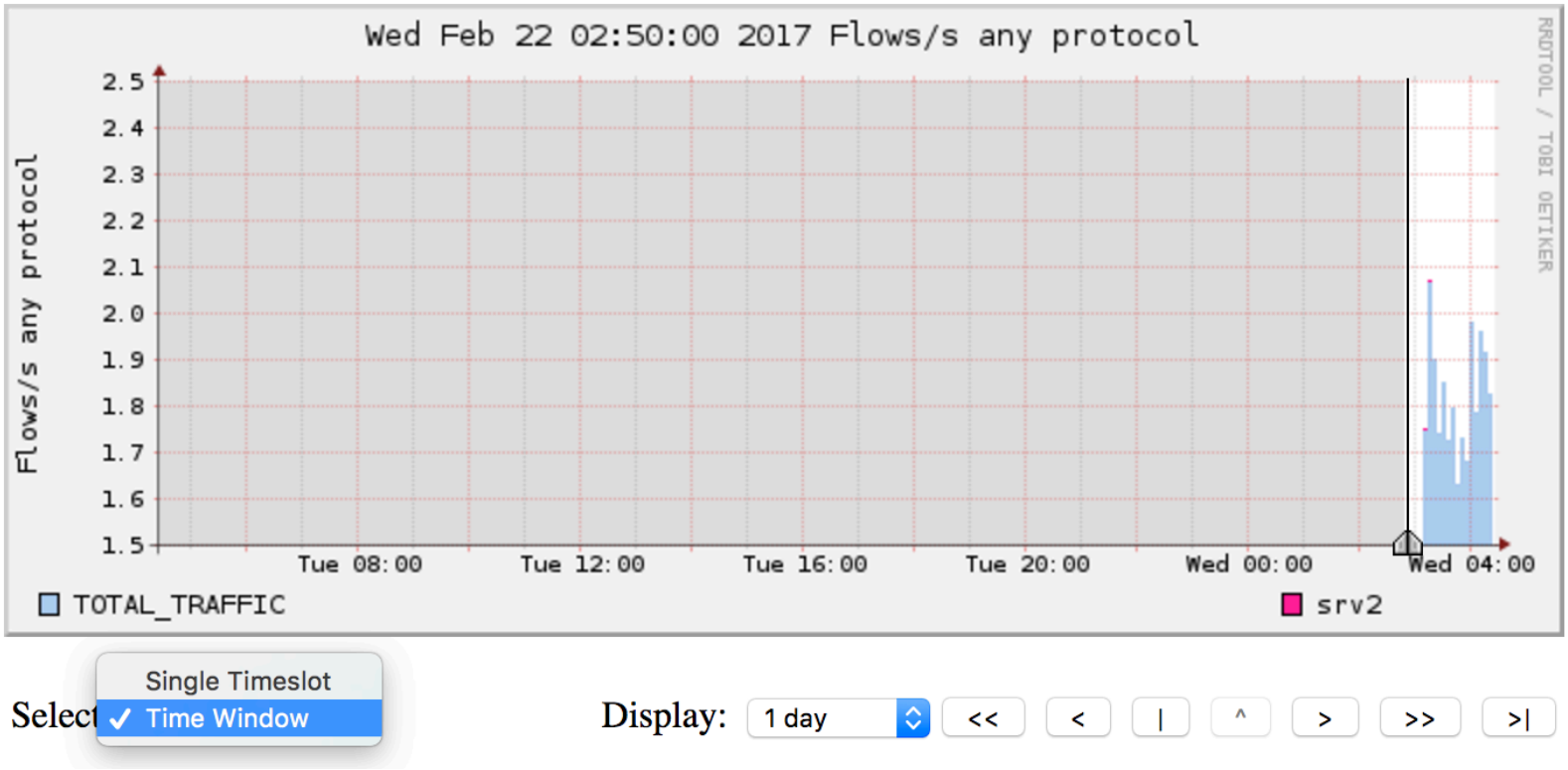
If you are measuring the same interface with both Cacti and NfSen, then you should obtain similar graphs when comparing the bits/s



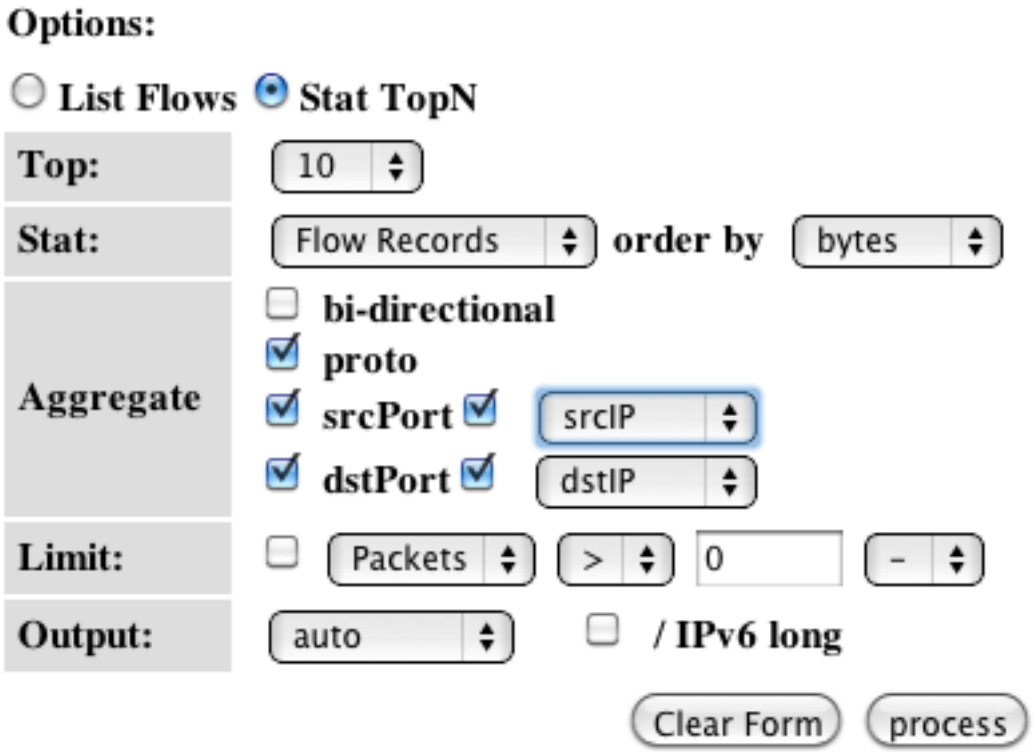


Part 3

Extended Netflow processing

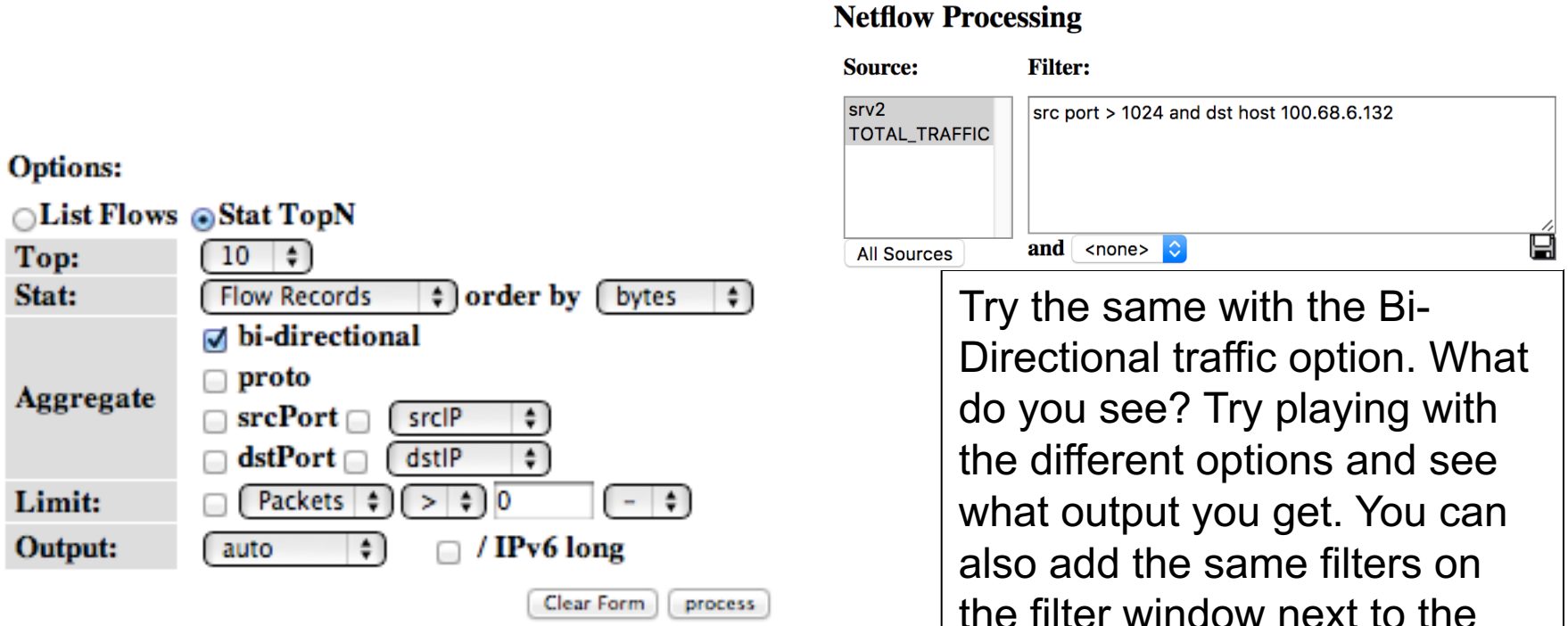


Go to Profile, select the group you created then select ‘HTTP_TRAFFIC’. Then go to the ‘Details’ tab and select ‘Time Window’ instead of ‘Time Slot’ beneath the graph. Choose a part of the graph with activity as above.



Select the options as on the left. This means, select the Top 10 Flows, Order them by bytes from the highest to the lowest and display information of the source and destination ports and IPs. Then select 'Process'. Analyze the output you get which will look like the below screen.

```
Aggregated flows 450
Top 10 flows ordered by flows:
Date first seen          Duration  Proto Src Pt Dst Pt   Packets    Bytes      bps    Bpp Flows
2017-02-22 02:49:48.312   292.508  ICMP        0    0.0       410    34440      941     84    49
2017-02-22 02:49:48.344   292.488  ICMP        0    0.0       365    30660      838     84    43
2017-02-22 02:52:41.864    31.332  TCP     50959     80         7      878      224    125     3
2017-02-22 02:52:41.864    31.328  TCP     50958     80         6      813      207    135     3
2017-02-22 02:49:56.228   282.976  UDP       123    123         6      456       12     76     3
2017-02-22 02:52:41.944    31.356  TCP        80  50958         5     1263      322    252     3
2017-02-22 02:52:42.008    31.312  TCP        80  50959         7     4318     1103    616     3
2017-02-22 02:52:28.276    13.040  TCP     50952     80        53     5516     3384    104     2
2017-02-22 02:53:13.204     7.412  TCP     50966     80        11     1796     1938    163     2
2017-02-22 02:53:13.360     7.272  TCP        80  50966        11     7685     8454    698     2
Summary: total flows: 578, total bytes: 975462, total packets: 2949, avg bps: 26495, avg pps: 10, avg bpp: 330
Time window: 2017-02-22 02:49:48 - 2017-02-22 02:54:42
Total flows processed: 578, Blocks skipped: 0, Bytes read: 39408
Sys: 0.956s flows/second: 604.6      Wall: 0.959s flows/second: 602.2
```



Try the same with the Bi-Directional traffic option. What do you see? Try playing with the different options and see what output you get. You can also add the same filters on the filter window next to the Options.

Try the following filters:

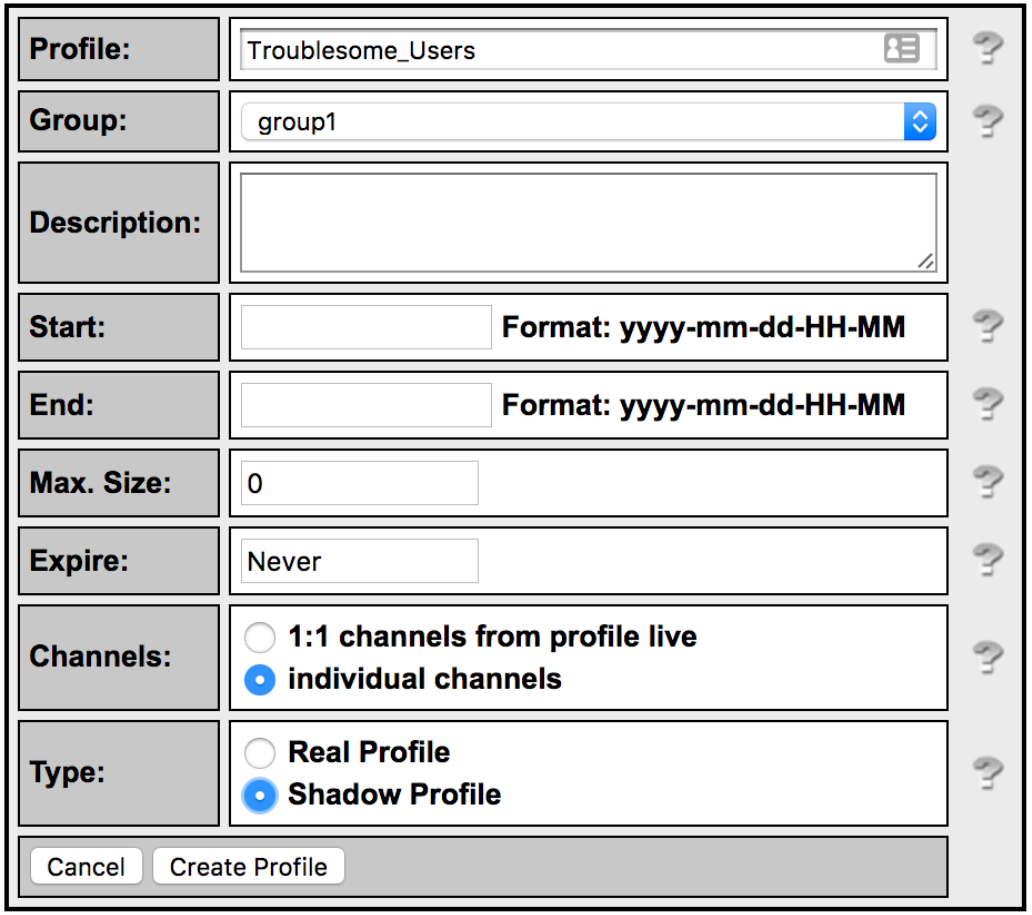
src host 100.68.X.Y – meaning look for flows for this host
src port 22 – meaning flows where the source port is 22
src port 22 or src port 80 – meaning flows of either port 22 or 80
src port 80 and in if 1 – meaning flows of src port 80 that passed via interface 1
dst net 100.64.0.0/10 – meaning all flows where the destination network is 100.64.0.0/10
src port > 5000 – meaning all flows where the source port is greater than 5000

Many more filters you could use

- If you want to see AS Number traffic for Google's AS 15169
  - `src as 15169`
- You can do the same for anyone's AS but your router should have the routing table installed and have *'ip flow-export version 9 origin-as'* configured
- You can then graph each of them using a Stat as in the earlier exercise
- More filters here: http://nfsen.sourceforge.net/#mozTocId652064

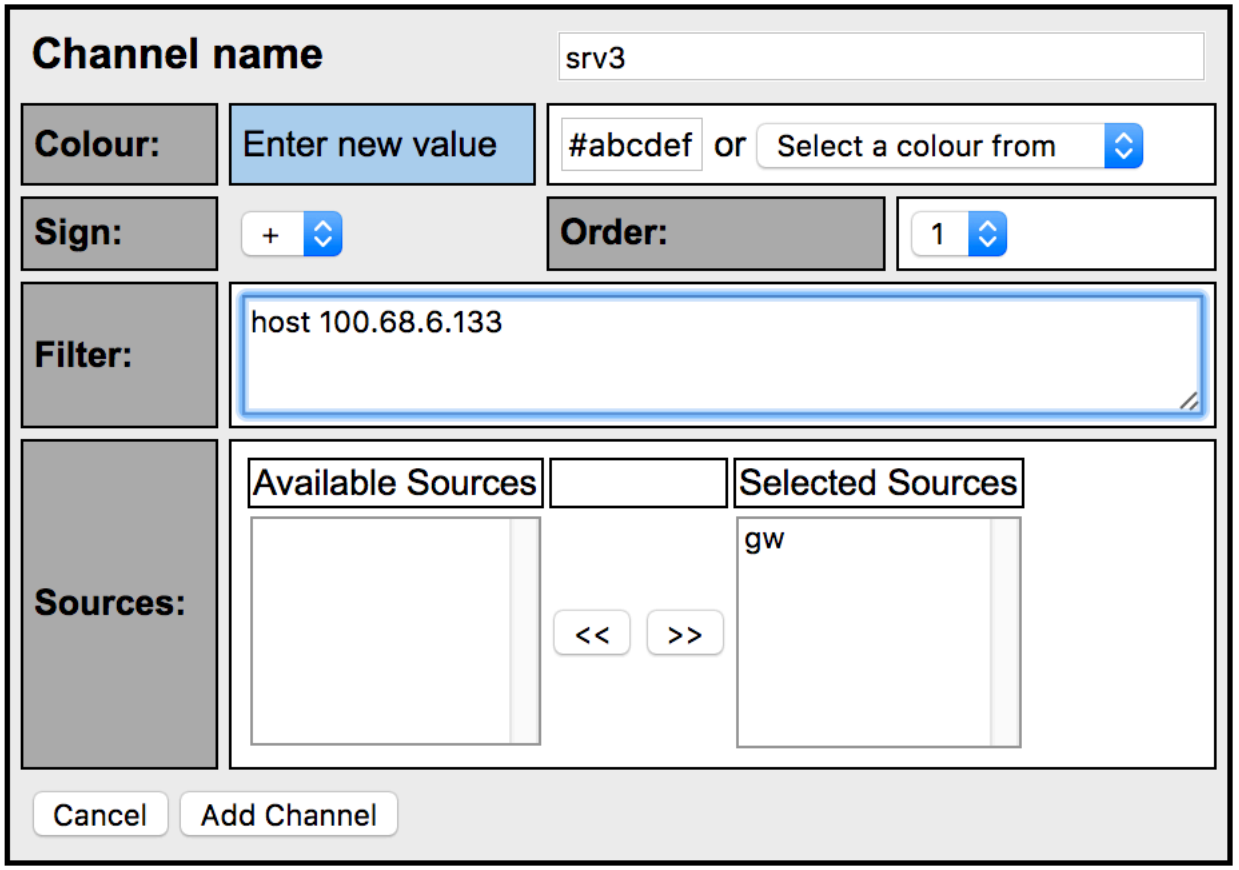
ADDITIONAL/OPTIONAL

Monitor a specific host



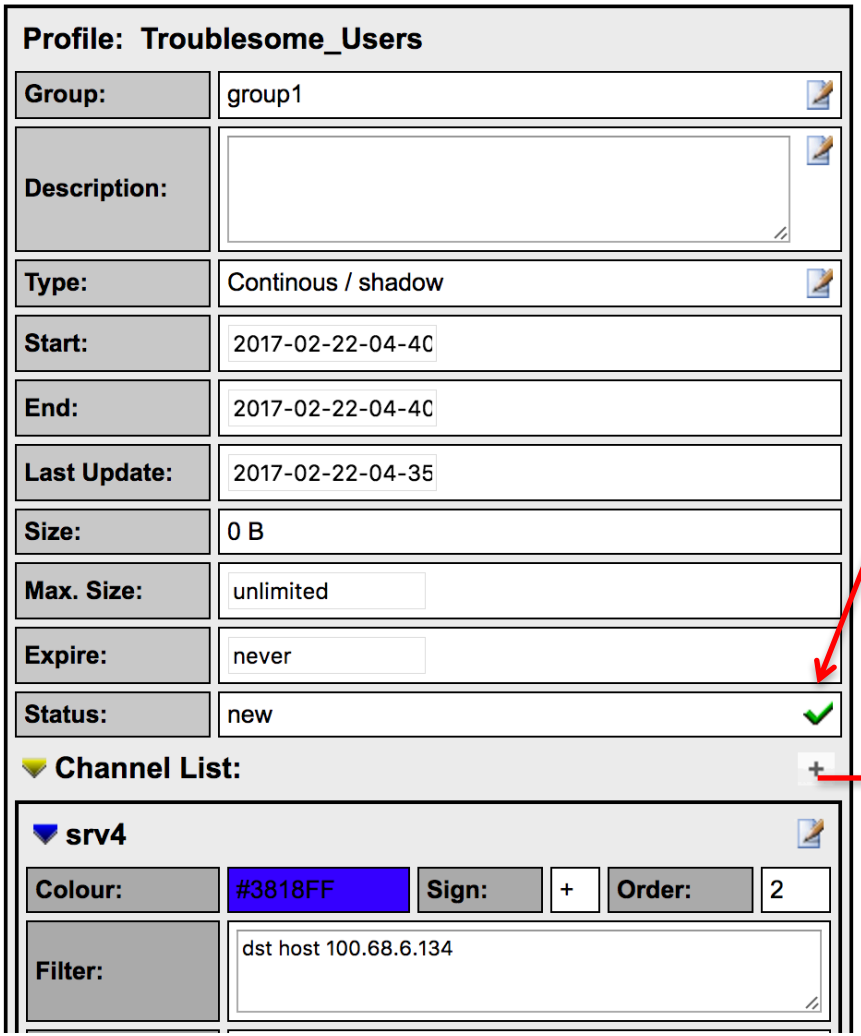
- On the “Profile” menu in NfSen select “New Profile…”
- When done click on “Create Profile” at the bottom
- You will see a message “new profile created”
- Then click on the plus sign at the bottom to begin adding channels

Monitor a Specific IP

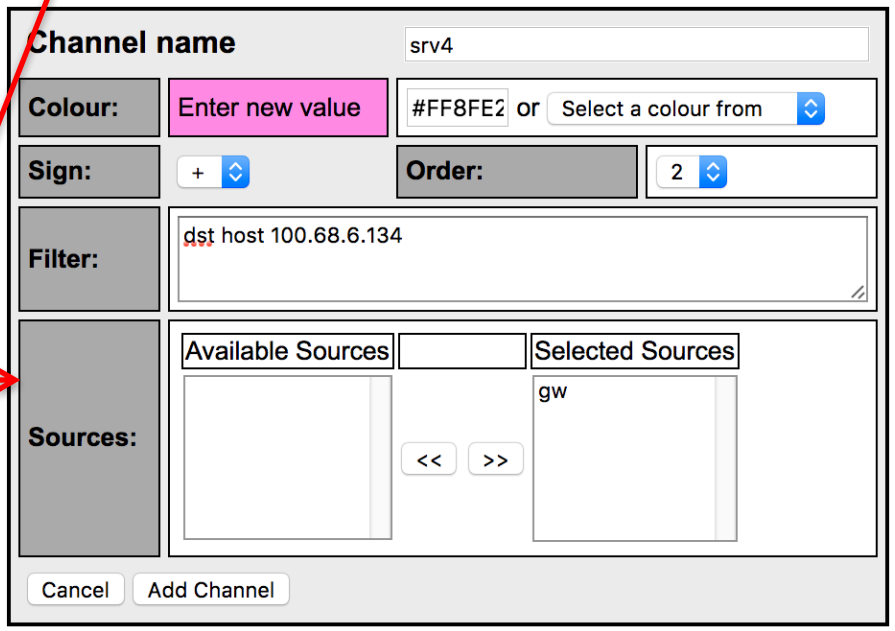


Replace 100.68.x.y with the IP of your virtual machine.

Add a second channel and start to accept



Click on “Add Channel” and then click the green check mark to activate the Troublesome_User”.



Filters

- Select a different color for the second channel so that the graphs can be distinguished
- Note that the two filters are different
  - The first filter will capture any flows pertaining to host one pc
  - The second filter will only capture flows where the host the second pc is the DESTINATION host.
  - To generate traffic to see on graph details for this profile try transferring files from the first host to the second host.
- More attributes can be added here like src AS, dst AS, src ports etc based on the NfSen filter syntax

See trends over time

Overview Profile: Troublesome_User, Group Hosts