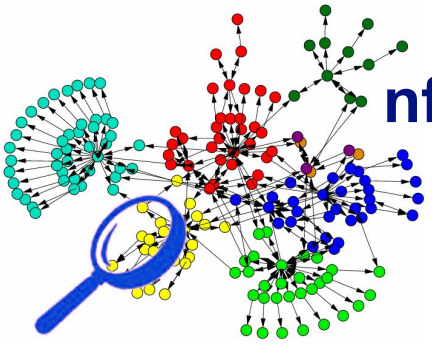
SWITCH

The Swiss Education & Research Network



nfdump and NfSen

SWINOG-12
May 4th 2006, Bern
Peter Haag

SWITCH cert

2006 © SWITCH

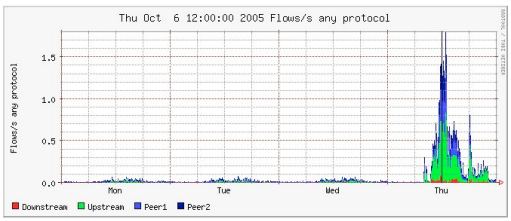
nfdump and NfSen

SWITCH
The Swiss Education & Research Network

Some operational questions, popping up now and then:

- **Do you see this peek on port 445 as well ?**
- **What caused this peek on your network graph ?**
- **How did SoberR spread in your network ?**
- **Do we have any traffic pattern of this incident ?**
- **Which host/subnet consumes most of your bandwidth ?**
- **Which are the top talkers in your network ?**
- **…**

Sober.R

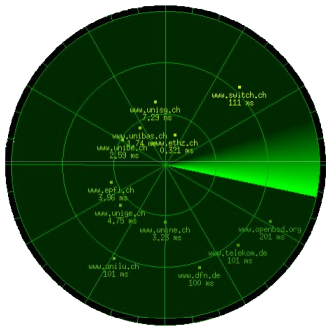


How to find answers for all these questions?

Netflow turnes out to be a good Data Source - although not the only one - for all kind of information and/or events to look at.

.. in discussions with other teams:

- "Watch your flows for …"
- "I've seen a lot of … in our flows …"
- "Host are infected, when you see flows to …"



What is NetFlow?

NetFlow is a traffic monitoring technology developed by Cisco Networks. Flows are unidirectional and contain connection related data such as:

- Source and destination IP address.
- Source and destination port.
- Source and destination AS.
- Level3 protocol, ToS byte, TCP flags.
- Logical input and output interfaces.
- Bytes and packet counters.

Example:

```
2006-03-30 00:47:33.728 54.971   TCP  172.16.71.66:13599 -> 192.168.10.34:80  .A..SF  215 9890
```

Netflow records never contain any user data!

SWITCH
The Swiss Education & Research Network

How to get netflow data and how to look at them?

Routers do provide netflow data …

but …

```
Router# show ip cache flow
```

… seems not to be the solution for every task.

⇒ Tools to collect and look at the netflow data

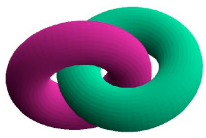
nfdump and NfSen

SWITCH
The Swiss Education & Research Network

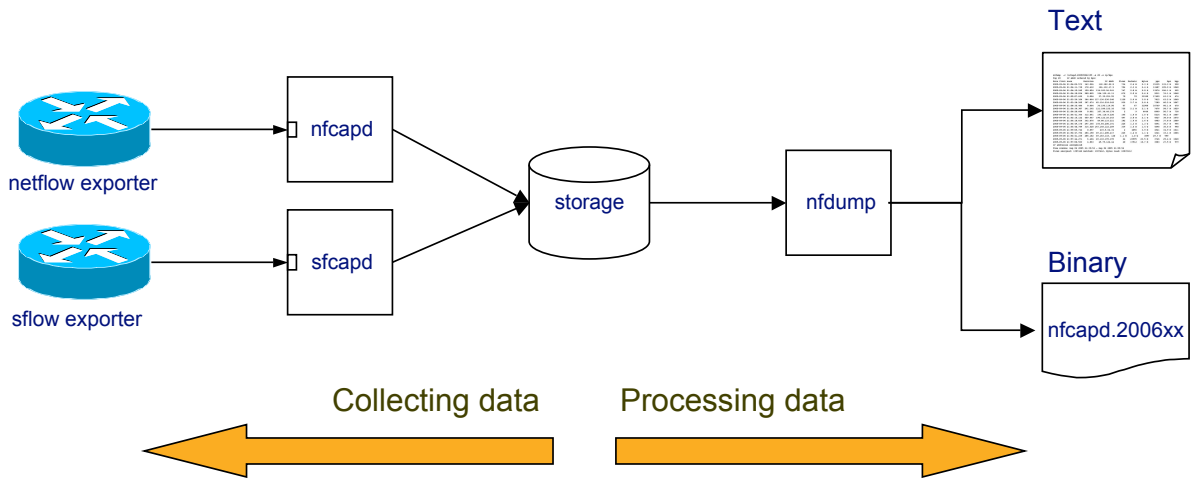
nfdump and NfSen:

NfSen:
- Web based frontend
- Display flows
- Framework to automate tasks

nfdump:
- Collect and store flows
- Process flows on command line



nfdump overview :



nfdump features:

- CMD line based tool comparable to tcpdump.
- Written in C ⇒ fast.
- Stores netflow data in time sliced files.
- Supports netflow format v5,v7 and v9.
- All processing options support IPv4 and IPv6.
- Powerful pcap like filter syntax:
  (proto tcp and dst net 172.16/16 and src port > 1024 and bytes < 600)
  or (bps > 1k and …
- Flexible flow aggregation.
- Efficient filter engine: > 6 Mio flows/s on 3GHz Intel.
- Lots of fast Top N statistics.
- Anonymizing of IP addresses. (Crypto-Pan)
- User defined output formats.

Example:

List the first 20 tcp flows:

```
forth% nfdump -r /data/rz/nfcapd.200603300150 -K 123.. -c 20 'proto tcp'
Date flow start          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Flags  Packets    Bytes
2006-03-30 00:43:40.569    82.880 TCP     130.20.234.125:58035 ->      200.66.27.5:61486 .AP...      673   199208
2006-03-30 00:43:40.569    82.880 TCP        200.66.27.5:61486 ->   130.20.234.125:58035 .A....      421    19674
2006-03-30 00:44:00.082    63.113 TCP     130.20.234.125:55697 ->      159.93.88.3:60454 .AP...      814    1.1 M
2006-03-30 00:44:00.082    63.113 TCP        159.93.88.3:60454 ->   130.20.234.125:55697 .A....      498    25896
2006-03-30 00:45:02.647     0.431 TCP     193.246.238.35:80    ->    192.254.4.182:56547 .A....        1     1500
2006-03-30 00:45:02.647     0.431 TCP      192.254.4.182:56547 ->   193.246.238.35:80    .A....        3      156
2006-03-30 00:45:02.813     0.000 TCP     130.20.234.124:59112 ->   194.50.123.176:45458 .A...F        1       52
2006-03-30 00:45:02.913     0.000 TCP      192.254.4.167:58659 ->     49.20.115.83:80    .A...F        1       52
2006-03-30 00:45:02.913     0.000 TCP     129.66.105.181:11248 ->    192.254.4.183:80    ....S.        1       46
2006-03-30 00:45:02.913     0.000 TCP      192.254.4.183:80    ->   129.66.105.181:11248 .A..S.        1       46
2006-03-30 00:45:02.879     0.000 TCP     129.66.105.181:11247 ->    192.254.4.183:80    .AP...        1      515
2006-03-30 00:45:02.879     0.000 TCP      192.254.4.183:80    ->   129.66.105.181:11247 .A....        1       46
2006-03-30 00:45:02.913     0.355 TCP     214.203.35.177:19027 ->   130.20.234.125:80    .A....        3      156
2006-03-30 01:40:02.347   300.572 TCP   dffe:e6..:199:fd.119   -> dc7e:18..:fe99:2.35541 .AP...      811    66835
2006-03-30 01:40:02.347   300.572 TCP   dc7e:18..:fe99:2.35541 -> dffe:e6..:199:fd.119   .AP.S.     4850    6.9 M
2006-03-30 00:45:02.895     0.000 TCP      192.254.4.183:80    ->  192.254.179.207:56323 .AP...        1      129
2006-03-30 00:45:02.978     0.000 TCP     194.50.123.176:45465 ->   130.20.234.124:55652 ....S.        1       60
2006-03-30 00:45:03.013     0.000 TCP     130.20.234.125:21    ->    50.242.99.240:61288 .A..S.        1       48
2006-03-30 00:45:03.009     0.000 TCP       156.32.82.45:35110 ->   130.20.234.124:25    ....S.        1       60
2006-03-30 00:45:03.041     0.000 TCP     130.20.234.125:80    ->   130.219.188.88:57168 .A....        1       52
IP addresses anonymized
Time window: 2006-03-30 00:40:02 - 2006-03-30 01:49:10
Total flows: 15970 matched: 20, skipped: 0, Bytes read: 838972
Sys: 0.007s flows/second: 2044290.8  Wall: 0.004s flows/second: 3391378.2
```


Example:

Show the top 15 IP addresses consuming most bandwidth:

```
forth% nfdump -r /data/rz/nfcapd.200603300150 -K 123… -n 20 -s ip/bps
Top 15     IP Addr ordered by bps:
Date first seen          Duration Proto          IP Addr    Flows  Packets    Bytes      pps      bps   bpp
2006-03-30 00:47:39.999     0.001 TCP      64.132.143.51        2       19    18004    18999  137.4 M   947
2006-03-30 00:45:00.737     0.001 TCP     194.64.105.184        2       20    13600    20000  103.8 M   680
2006-03-30 00:49:16.016     0.001 TCP       163.3.33.241        2        9    12046     9000   91.9 M  1338
2006-03-30 00:49:52.902     0.001 TCP      92.37.170.104        2       10     9208    10000   70.3 M   920
2006-03-30 00:45:06.853     0.001 TCP     214.214.200.81        2        6     6931     6000   52.9 M  1155
2006-03-30 00:46:32.363     0.001 TCP       68.142.57.84        2       10     6720    10000   51.3 M   672
2006-03-30 00:46:30.764     0.001 TCP     151.80.146.115        2        7     6680     7000   51.0 M   954
2006-03-30 00:48:36.966     0.001 TCP       129.4.38.113        2        8     6184     8000   47.2 M   773
2006-03-30 00:49:31.903     0.001 TCP     33.135.213.117        2        6     6104     6000   46.6 M  1017
2006-03-30 01:42:48.834     0.001 TCP      90.38.160.152        2        8     5941     8000   45.3 M   742
2006-03-30 00:48:02.473     0.001 TCP     131.144.55.170        2        6     5608     6000   42.8 M   934
2006-03-30 00:49:29.424     0.001 TCP      24.11.195.220        2        4     4880     4000   37.2 M  1220
2006-03-30 00:48:53.293     0.001 TCP       88.53.69.175        2        6     4721     6000   36.0 M   786
2006-03-30 00:45:41.780     0.001 TCP         49.30.8.60        2        6     3822     6000   29.2 M   637
2006-03-30 01:42:51.618     0.002 TCP      220.24.222.74        2       10     7605     5000   29.0 M   760

IP addresses anonymized
Time window: 2006-03-30 00:40:02 - 2006-03-30 01:49:58
Total flows: 19224 matched: 19224, skipped: 0, Bytes read: 1009920
Sys: 0.046s flows/second: 410112.0   Wall: 0.009s flows/second: 2022089.0
```

Example:

Show port scanning candidates:

```
forth% nfdump -r /data/rz/nfcapd.200603300150 -K 123… -A srcip,dstport -s record/packets 'not proto icmp and bytes < 100
    and bpp < 100 and packets < 5 and not port 80 and not port 53 and not port 110 and not port 123'
Aggregated flows 72506
Top 10 flows ordered by packets:
Date flow start          Duration Proto      Src IP Addr:Port        Dst IP Addr:Port   Packets    Bytes      bps Flows
2006-03-30 01:49:23.800   243.842 TCP      83.130.48.231:0     ->       0.0.0.0:4899    142172    6.5 M   223891 71151
2006-03-30 01:50:48.603   236.035 TCP      165.17.105.18:0     ->       0.0.0.0:5900     34452    1.6 M    56049 17232
2006-03-30 01:52:30.169   143.944 TCP    117.128.149.163:0     ->       0.0.0.0:41523     9982   479136    26629  5143
2006-03-30 01:49:22.650   303.173 TCP    221.200.120.170:0     ->       0.0.0.0:1433      4638   222624     5874  2319
2006-03-30 01:49:53.945   299.401 TCP     211.135.150.43:0     ->       0.0.0.0:135       3273   157104     4197  3273
2006-03-30 01:49:27.196   194.565 TCP     201.143.63.114:0     ->       0.0.0.0:139       1845    88560     3641  1613
2006-03-30 01:52:05.471    96.768 TCP     198.246.113.17:0     ->       0.0.0.0:445       1678    80544     6658   954
2006-03-30 01:49:54.012   300.038 UDP      210.117.33.36:0     ->       0.0.0.0:137       1471   114738     3059  1471
2006-03-30 01:49:22.970   328.838 TCP     164.88.206.114:0     ->       0.0.0.0:135       1432    68736     1672  1077
2006-03-30 01:53:00.822   112.524 TCP     24.169.235.184:0     ->       0.0.0.0:135       1254    60192     4279  1254

IP addresses anonymized
Time window: 2006-03-30 01:34:53 - 2006-03-30 01:54:57
Total flows: 1178835 matched: 245494, skipped: 0, Bytes read: 57559680
Sys: 0.634s flows/second: 1856716.7  Wall: 0.632s flows/second: 1862657.6
```


Example:

Show the top 15 /24 subnets exchanging most traffic:

```
forth% nfdump -r /data/rz/nfcapd.200603300150 -K 123… -n 15 -A srcip4/24,dstip4/24 -s record/bytes
Aggregated flows 7525
Top 15 flows ordered by bytes:
Date flow start          Duration Proto      Src IP Addr:Port        Dst IP Addr:Port   Packets    Bytes Flows
2006-03-30 00:41:06.140  4102.844 TCP      130.20.234.0:0     ->  130.254.221.0:0        79455   95.1 M    14
2006-03-30 00:42:50.622  4022.361 TCP      130.20.234.0:0     ->   194.90.158.0:0        42179   58.2 M    13
2006-03-30 00:40:51.729  4054.221 TCP      130.20.234.0:0     ->    220.63.34.0:0        39593   56.0 M     6
2006-03-30 01:41:42.025   443.957 TCP      130.20.224.0:0     ->     163.3.42.0:0        30543   43.3 M     7
2006-03-30 00:41:06.140  4102.844 TCP     130.254.221.0:0     ->   130.20.234.0:0        60178   29.1 M    14
2006-03-30 01:39:56.087   600.881 TCP      130.20.234.0:0     ->     194.84.7.0:0        17836   24.9 M     9
2006-03-30 00:44:39.128  3900.855 TCP      130.20.234.0:0     ->   214.124.39.0:0        15912   22.6 M     9
2006-03-30 01:41:01.414   529.568 UDP      130.20.223.0:0     ->   130.20.220.0:0        15549   21.4 M     8
2006-03-30 01:41:03.371   329.612 TCP     194.114.160.0:0     ->   130.20.234.0:0        14126   20.1 M     4
2006-03-30 01:40:12.986   300.997 TCP      130.20.234.0:0     ->  194.168.190.0:0        13101   18.7 M     2
2006-03-30 01:41:24.088   506.896 TCP      130.20.234.0:0     ->     24.50.25.0:0        12433   17.8 M     2
2006-03-30 01:43:04.047   300.870 TCP      165.242.80.0:0     ->   130.20.234.0:0         9966   14.3 M     1
2006-03-30 00:43:47.441  3935.542 TCP      130.20.234.0:0     ->   205.175.61.0:0        10445   13.4 M    15
2006-03-30 00:44:01.619   332.758 TCP      130.20.234.0:0     ->   194.61.253.0:0         8973   12.7 M   101
2006-03-30 01:42:43.123   300.860 TCP      130.20.234.0:0     ->    69.155.45.0:0         7872   11.3 M     1

IP addresses anonymized
Time window: 2006-03-30 00:40:02 - 2006-03-30 01:49:58
Total flows: 19224 matched: 18797, skipped: 0, Bytes read: 1009920
Sys: 0.062s flows/second: 307588.9   Wall: 0.010s flows/second: 1839969.4
```

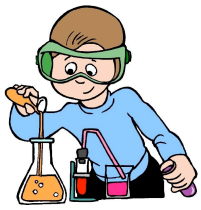
SWITCH
The Swiss Education & Research Network

The art of filter design:

- … depends on your problem you want to look at.
  - Incident Analysis.
  - Host tracking.
  - Port Scanning.
  - Operational issues.
- … depends on your network.

nfump does not do your job, but supports you in doing your job!

Use the power of nfdump's filter syntax!



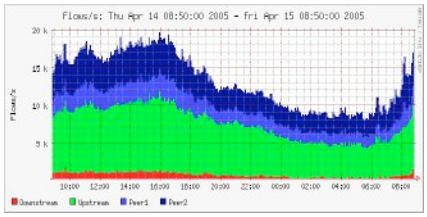
SWITCH
The Swiss Education & Research Network

nfdump is:

- Powerful
- Flexible
- Easy to use
- Fast
- …

but …

… don't we all like pictures?



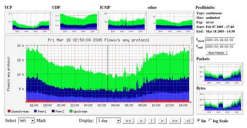
⇒ *NfSen*

nfdump and NfSen

SWITCH
The Swiss Education & Research Network

NfSen features:

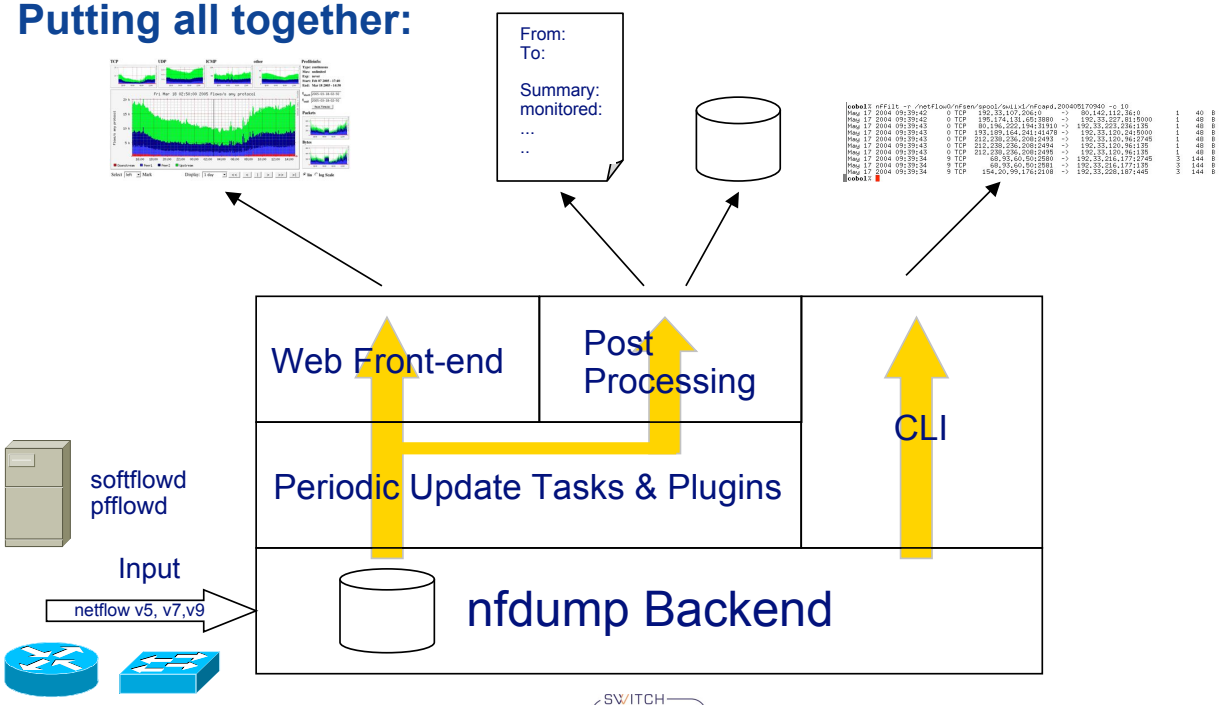
- Use the power of nfdump as backend tool. ⇒ modular design.
- Pictures!
- Drill down from overview to the details down to the specific flows.
- Graph current network situation.
- Graph specific profiles.
  - Track hosts, ports etc. from live data.
  - Profile hosts involved in incidents from history data.
- Analyse a specific time window.
- Web based.
- Automatically post process netflow data for reporting and alerting purpose.
- Flexible extensions using plugins.
- Easy to use.
- Auto - Cleanup. Aging data files: max space, max lifetime.



nfdump and NfSen

SWITCH
The Swiss Education & Research Network

Putting all together:

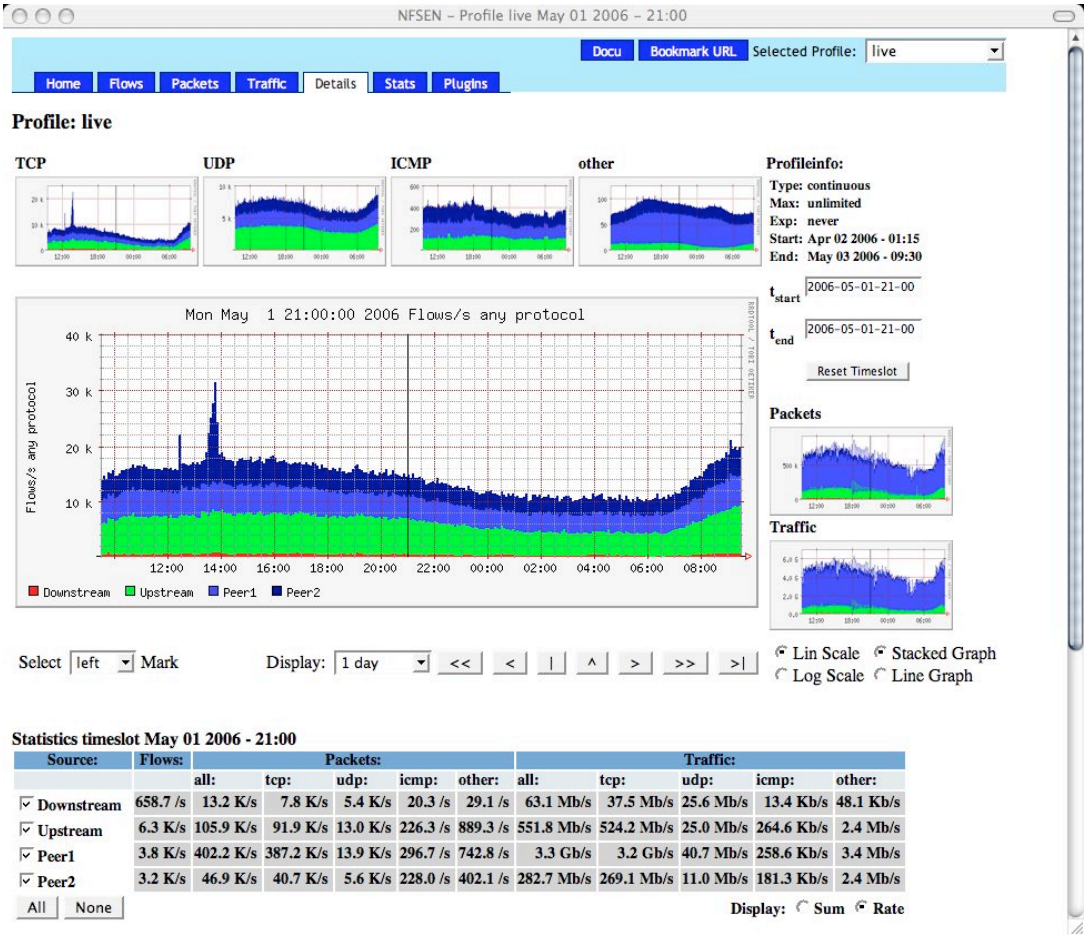


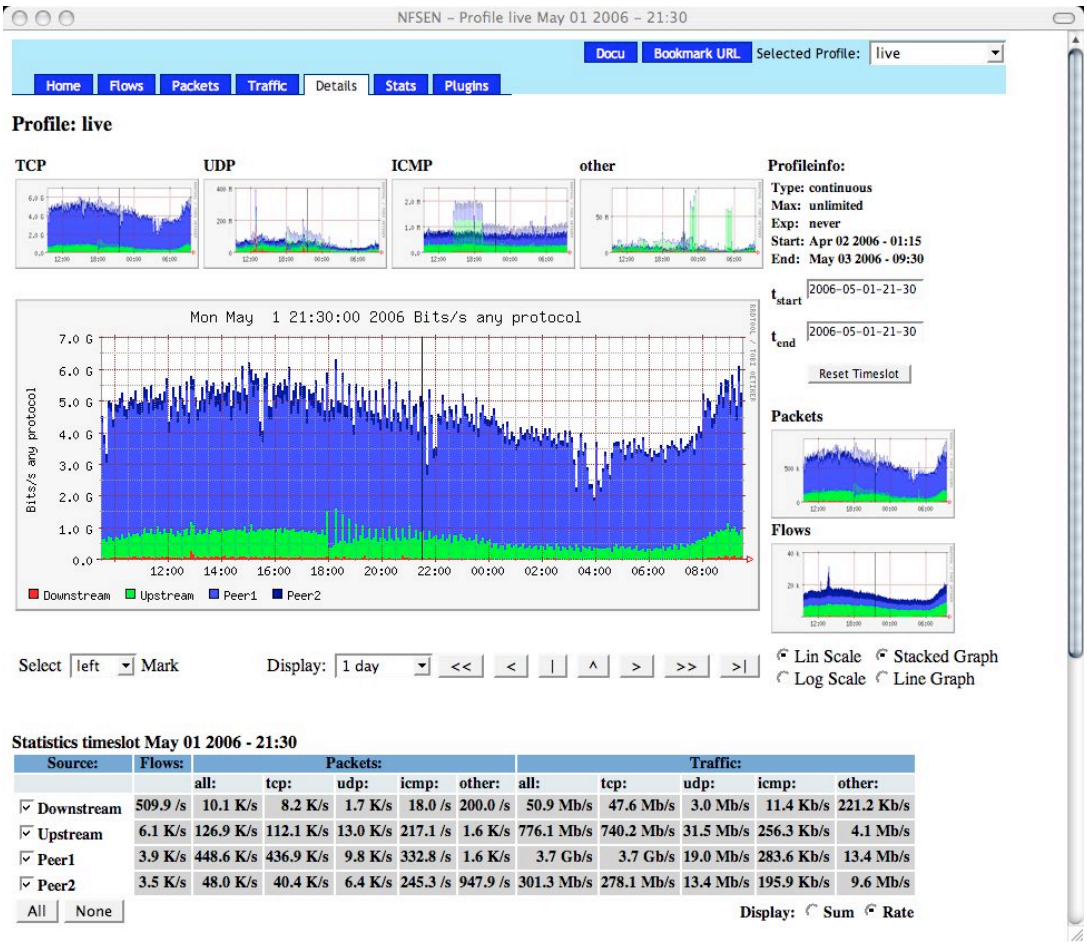
nfdump and NfSen

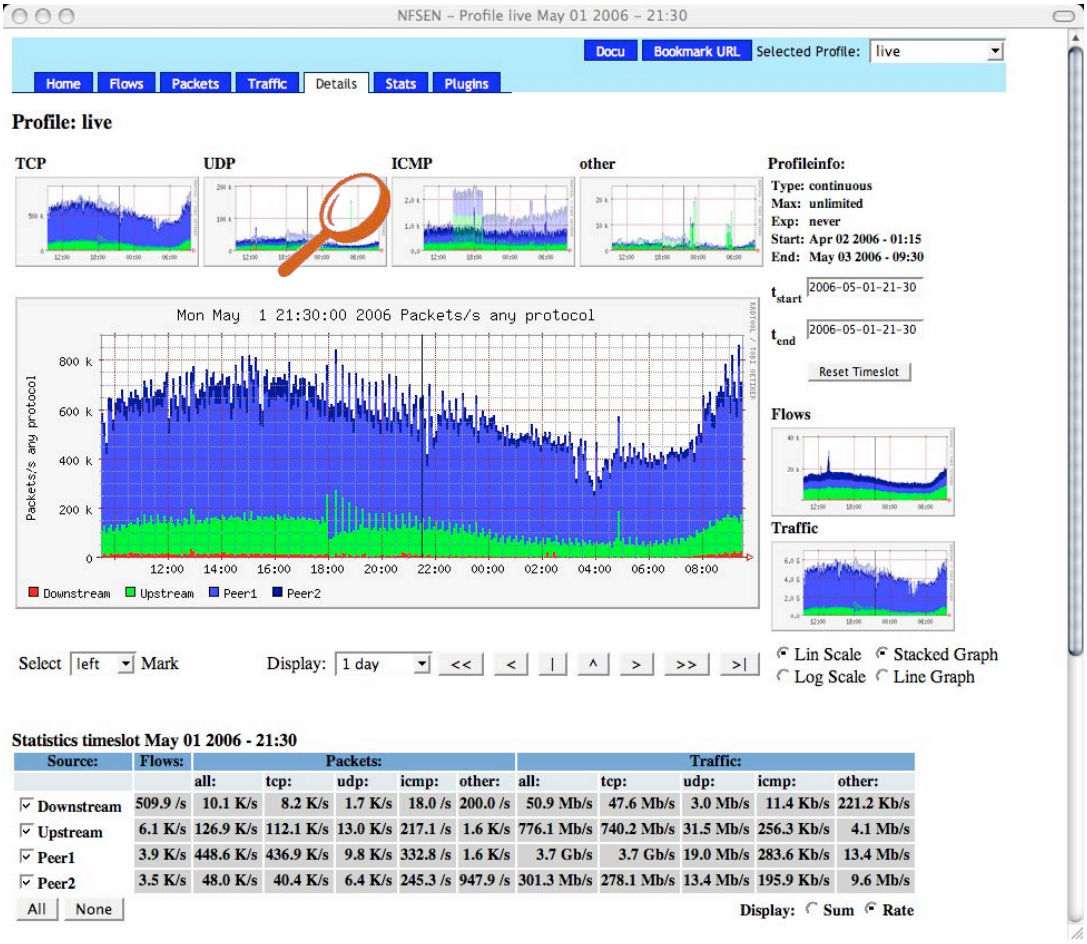
SWITCH
The Swiss Education & Research Network

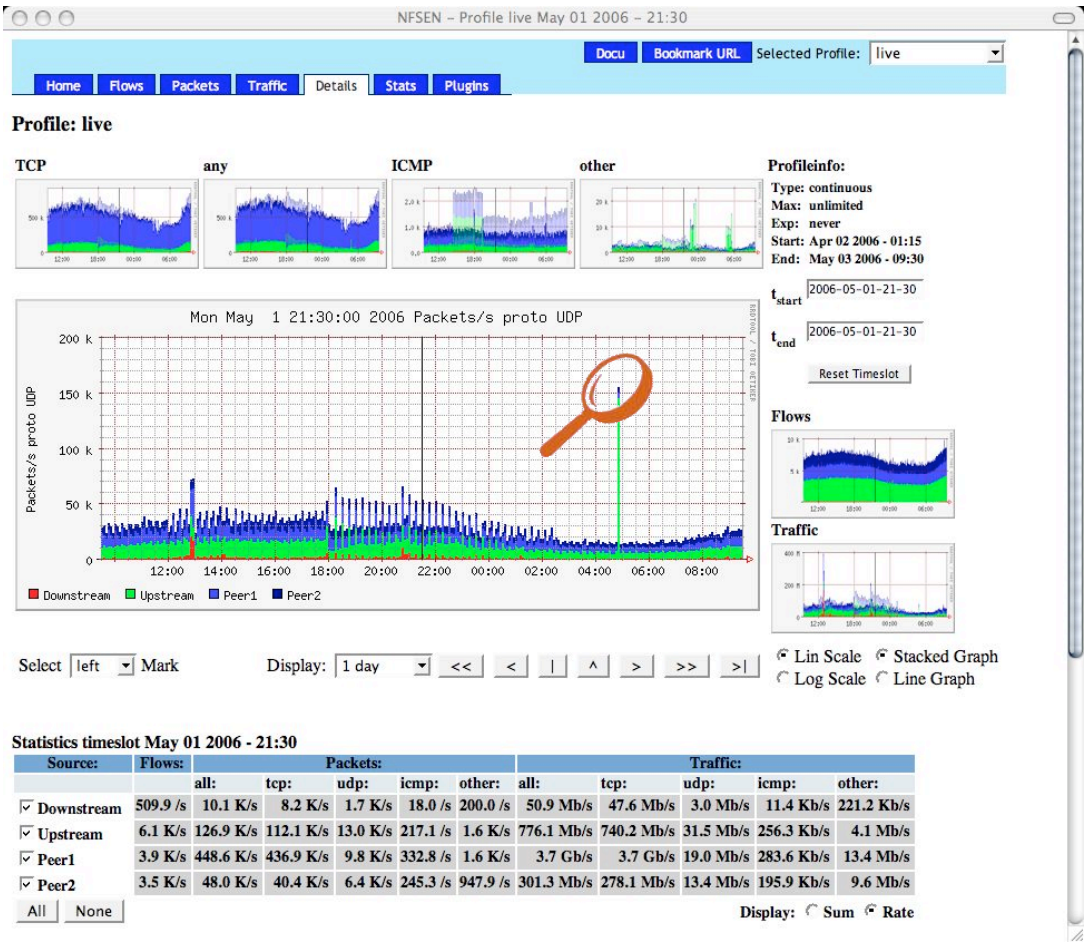
Overview ⇒ Details

Details ⇒ Flows


NFSEN - Profile live May 01 2006 - 21:00
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-05-01-21-00
t end 2006-05-01-21-00
Reset Timeslot
Packets
Traffic
Mon May 1 21:00:00 2006 Flows/s any protocol
Flows/s any protocol
40 k
30 k
20 k
10 k
12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00
Downstream
Upstream
Peer1
Peer2
Select left Mark
Display: 1 day
<< < | ^ > >> >|
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot May 01 2006 - 21:00
Source: Flows: Packets: Traffic:
all: tcp: udp: icmp: other: all: tcp: udp: icmp: other:
Downstream 658.7 /s 13.2 K/s 7.8 K/s 5.4 K/s 20.3 /s 29.1 /s 63.1 Mb/s 37.5 Mb/s 25.6 Mb/s 13.4 Kb/s 48.1 Kb/s
Upstream 6.3 K/s 105.9 K/s 91.9 K/s 13.0 K/s 226.3 /s 889.3 /s 551.8 Mb/s 524.2 Mb/s 25.0 Mb/s 264.6 Kb/s 2.4 Mb/s
Peer1 3.8 K/s 402.2 K/s 387.2 K/s 13.9 K/s 296.7 /s 742.8 /s 3.3 Gb/s 3.2 Gb/s 40.7 Mb/s 258.6 Kb/s 3.4 Mb/s
Peer2 3.2 K/s 46.9 K/s 40.7 K/s 5.6 K/s 228.0 /s 402.1 /s 282.7 Mb/s 269.1 Mb/s 11.0 Mb/s 181.3 Kb/s 2.4 Mb/s
All
None
Display: Sum Rate


NFSEN - Profile live May 01 2006 - 21:30
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-05-01-21-30
t end 2006-05-01-21-30
Reset Timeslot
Packets
Flows
Mon May 1 21:30:00 2006 Bits/s any protocol
Bits/s any protocol
7.0 G
6.0 G
5.0 G
4.0 G
3.0 G
2.0 G
1.0 G
0.0
12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00
Downstream
Upstream
Peer1
Peer2
Select left Mark
Display: 1 day
<< < | ^ > >> >|
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot May 01 2006 - 21:30
Source: Flows: Packets: Traffic:
all: tcp: udp: icmp: other: all: tcp: udp: icmp: other:
Downstream 509.9 /s 10.1 K/s 8.2 K/s 1.7 K/s 18.0 /s 200.0 /s 50.9 Mb/s 47.6 Mb/s 3.0 Mb/s 11.4 Kb/s 221.2 Kb/s
Upstream 6.1 K/s 126.9 K/s 112.1 K/s 13.0 K/s 217.1 /s 1.6 K/s 776.1 Mb/s 740.2 Mb/s 31.5 Mb/s 256.3 Kb/s 4.1 Mb/s
Peer1 3.9 K/s 448.6 K/s 436.9 K/s 9.8 K/s 332.8 /s 1.6 K/s 3.7 Gb/s 3.7 Gb/s 19.0 Mb/s 283.6 Kb/s 13.4 Mb/s
Peer2 3.5 K/s 48.0 K/s 40.4 K/s 6.4 K/s 245.3 /s 947.9 /s 301.3 Mb/s 278.1 Mb/s 13.4 Mb/s 195.9 Kb/s 9.6 Mb/s
All
None
Display: Sum Rate


NFSEN - Profile live May 01 2006 - 21:30
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-05-01-21-30
t end 2006-05-01-21-30
Reset Timeslot
Mon May 1 21:30:00 2006 Packets/s any protocol
Packets/s any protocol
800 k
600 k
400 k
200 k
0
12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00
Downstream
Upstream
Peer1
Peer2
Flows
Traffic
Select left Mark
Display: 1 day
<< < | ^ > >> >|
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot May 01 2006 - 21:30
Source: Flows: Packets: Traffic:
all: tcp: udp: icmp: other: all: tcp: udp: icmp: other:
Downstream 509.9 /s 10.1 K/s 8.2 K/s 1.7 K/s 18.0 /s 200.0 /s 50.9 Mb/s 47.6 Mb/s 3.0 Mb/s 11.4 Kb/s 221.2 Kb/s
Upstream 6.1 K/s 126.9 K/s 112.1 K/s 13.0 K/s 217.1 /s 1.6 K/s 776.1 Mb/s 740.2 Mb/s 31.5 Mb/s 256.3 Kb/s 4.1 Mb/s
Peer1 3.9 K/s 448.6 K/s 436.9 K/s 9.8 K/s 332.8 /s 1.6 K/s 3.7 Gb/s 3.7 Gb/s 19.0 Mb/s 283.6 Kb/s 13.4 Mb/s
Peer2 3.5 K/s 48.0 K/s 40.4 K/s 6.4 K/s 245.3 /s 947.9 /s 301.3 Mb/s 278.1 Mb/s 13.4 Mb/s 195.9 Kb/s 9.6 Mb/s
All
None
Display: Sum Rate


NFSEN - Profile live May 01 2006 - 21:30
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
any
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-05-01-21-30
t end 2006-05-01-21-30
Reset Timeslot
Mon May 1 21:30:00 2006 Packets/s proto UDP
Packets/s proto UDP
200 k
150 k
100 k
50 k
0
12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00
Downstream
Upstream
Peer1
Peer2
Flows
Traffic
Select left Mark
Display: 1 day
<< < | ^ > >> >|
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot May 01 2006 - 21:30
Source: Flows: Packets: Traffic:
all: tcp: udp: icmp: other: all: tcp: udp: icmp: other:
Downstream 509.9 /s 10.1 K/s 8.2 K/s 1.7 K/s 18.0 /s 200.0 /s 50.9 Mb/s 47.6 Mb/s 3.0 Mb/s 11.4 Kb/s 221.2 Kb/s
Upstream 6.1 K/s 126.9 K/s 112.1 K/s 13.0 K/s 217.1 /s 1.6 K/s 776.1 Mb/s 740.2 Mb/s 31.5 Mb/s 256.3 Kb/s 4.1 Mb/s
Peer1 3.9 K/s 448.6 K/s 436.9 K/s 9.8 K/s 332.8 /s 1.6 K/s 3.7 Gb/s 3.7 Gb/s 19.0 Mb/s 283.6 Kb/s 13.4 Mb/s
Peer2 3.5 K/s 48.0 K/s 40.4 K/s 6.4 K/s 245.3 /s 947.9 /s 301.3 Mb/s 278.1 Mb/s 13.4 Mb/s 195.9 Kb/s 9.6 Mb/s
All
None
Display: Sum Rate

NFSEN – Profile live May 02 2006 – 04:55

Docu | Bookmark URL | Selected Profile: live

Home | Flows | Packets | Traffic | Details | Stats | Plugins

Profile: live

TCP | any | ICMP | other

Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30

t_{start} 2006-05-02-04-55
t_{end} 2006-05-02-04-55
Reset Timeslot

Tue May 2 04:55:00 2006 Packets/s proto UDP

Packets/s proto UDP: 200 k, 150 k, 100 k, 50 k, 0

12:00 14:00 16:00 18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00

Downstream | Upstream | Peer1 | Peer2

Flows

Traffic

Select left Mark Display: 1 day << < | ^ > >> >|

Lin Scale | Stacked Graph
Log Scale | Line Graph

Statistics timeslot May 02 2006 - 04:55

Source:	Flows:	Packets:					Traffic:				
		all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
Downstream	506.6 /s	3.3 K/s	2.7 K/s	556.9 /s	13.9 /s	6.7 /s	13.1 Mb/s	12.3 Mb/s	754.6 Kb/s	9.1 Kb/s	14.2 Kb/s
Upstream	4.1 K/s	182.3 K/s	39.3 K/s	142.5 K/s	190.7 /s	299.8 /s	318.6 Mb/s	260.6 Mb/s	57.0 Mb/s	245.7 Kb/s	801.6 Kb/s
Peer1	3.0 K/s	350.6 K/s	344.5 K/s	4.7 K/s	922.7 /s	493.7 /s	3.0 Gb/s	3.0 Gb/s	7.8 Mb/s	516.6 Kb/s	509.7 Kb/s
Peer2	2.4 K/s	22.4 K/s	18.7 K/s	3.2 K/s	183.3 /s	245.5 /s	118.4 Mb/s	112.7 Mb/s	5.3 Mb/s	163.9 Kb/s	252.8 Kb/s

All | None Display: Sum | Rate

NFSEN – Profile live May 02 2006 – 04:55

Peer1	3.0 K/s	350.6 K/s	344.5 K/s	4.7 K/s	922.7 /s	493.7 /s	3.0 Gb/s	3.0 Gb/s	7.8 Mb/s	516.6 Kb/s	509.7 Kb/s
Peer2	2.4 K/s	22.4 K/s	18.7 K/s	3.2 K/s	183.3 /s	245.5 /s	118.4 Mb/s	112.7 Mb/s	5.3 Mb/s	163.9 Kb/s	252.8 Kb/s

All | None Display: Sum | Rate

Netflow Processing

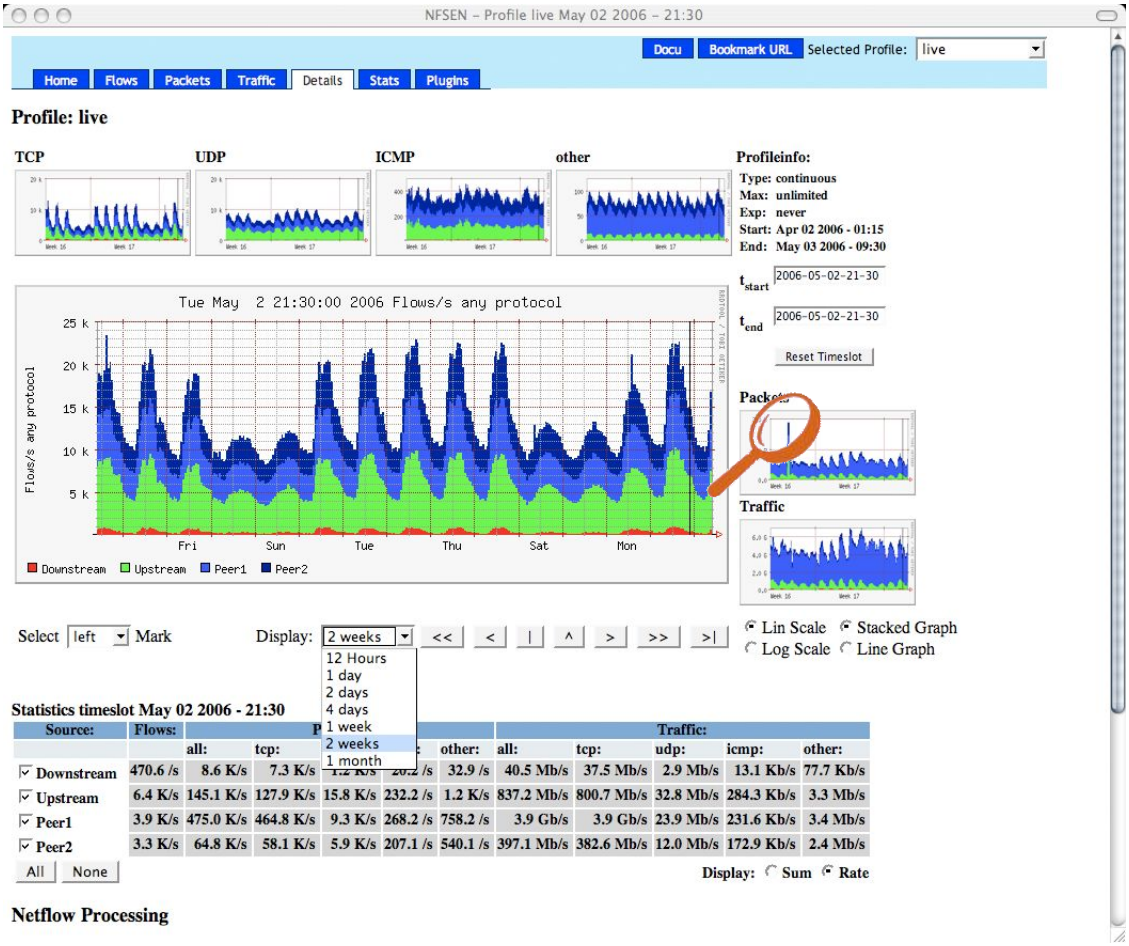
Source: Downstream, Upstream, Peer1, Peer2
All Sources

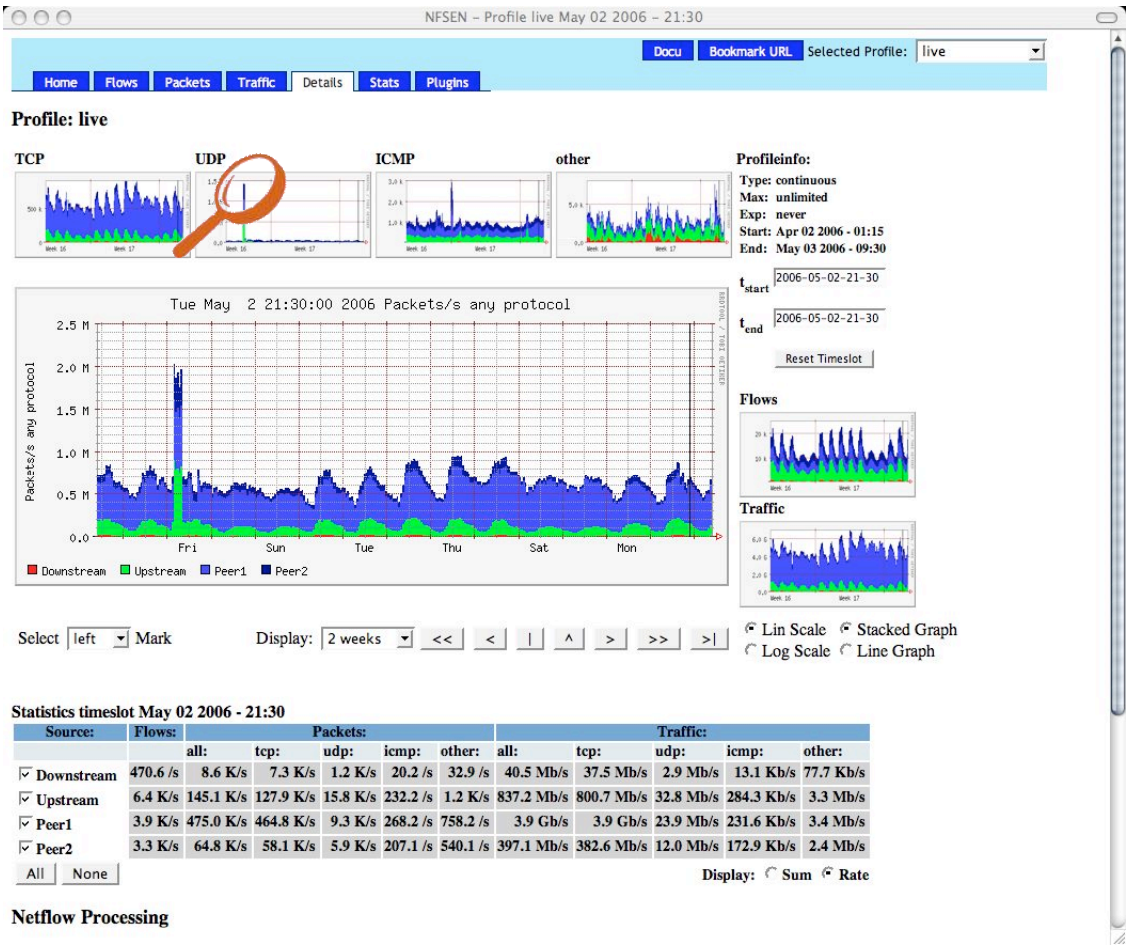
Filter: udp
and <none>

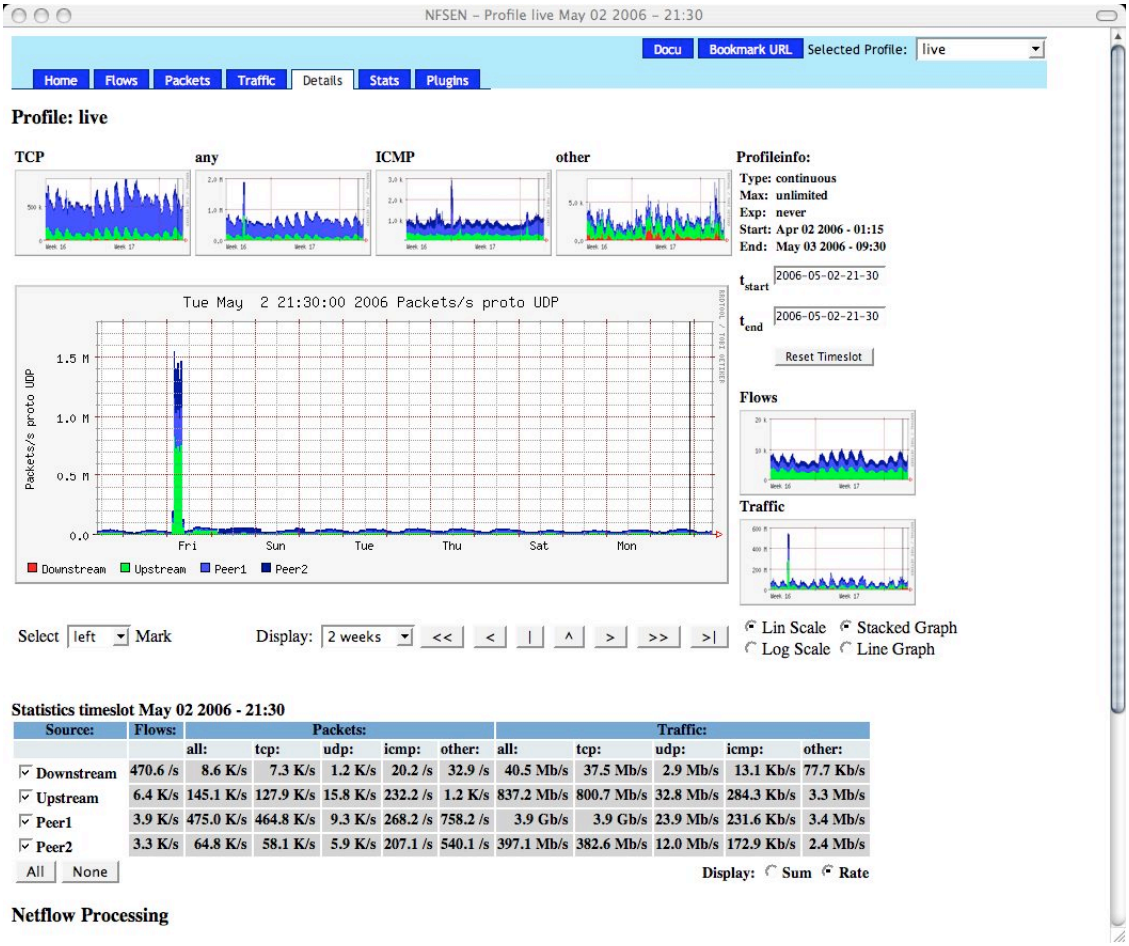
Show:
List: First 10 Flows
aggregated.
time sorted.
long output
process

Stat: Top 20
Limit Packets > 0 -
Flows order by packets
long output
Any IP Addr order by packets
process
Clear Form

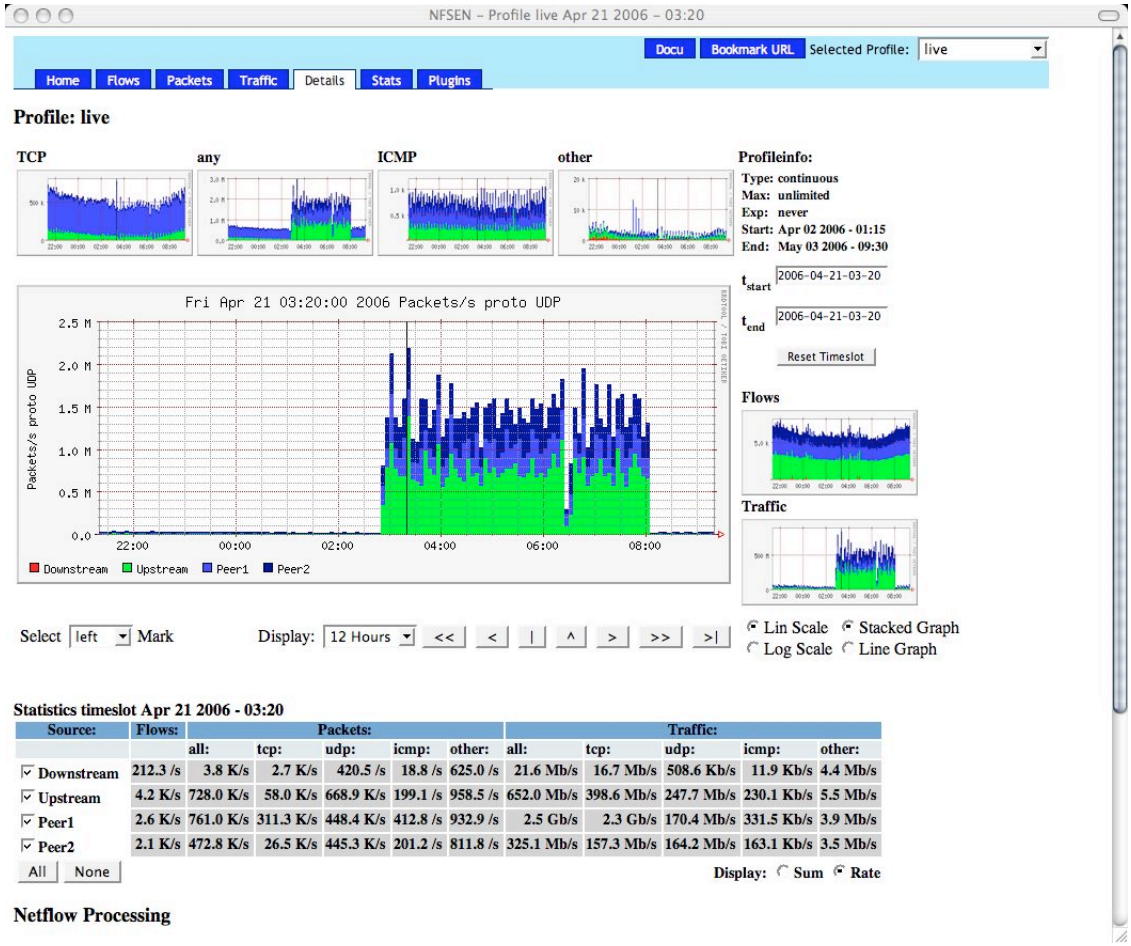
```
/usr/local/bin/nfdump  -r /netflow2/nfsen-devel/profiles/live/Downstream/nfcapd.200605020455 -n 20 -s record/packets -o extended 'udp '

Aggregated flows 23100
Top 20 flows ordered by packets:
Date flow start          Duration Proto    Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes      pps      bps    Bpp Flows
2006-05-02 04:43:47.315  867.356 UDP   254.118.64.166:7001  ->  190.50.223.175:7000  ......   0    31919    4.7 M       36    45282    153     2
2006-05-02 04:43:47.339  867.333 UDP   190.50.223.175:7000  ->  254.118.64.166:7001  ......   0    26147    3.9 M       30    37574    155     2
2006-05-02 04:47:28.256  694.211 UDP   254.118.64.166:7001  ->    247.3.248.90:7000  ......   0    18676    2.8 M       26    34277    159     2
2006-05-02 04:47:28.278  694.188 UDP     247.3.248.90:7000  ->  254.118.64.166:7001  ......   0    16738    1.9 M       24    23112    119     2
2006-05-02 04:39:47.202  924.585 UDP  247.124.101.236:3830  ->  191.181.110.37:3830  ......   0     2245   348041        2     3011    155     1
2006-05-02 04:58:12.827   62.100 UDP   254.118.64.166:7001  -> 252.155.202.149:7000  ......   0     1162   132304       18    17043    113     1
2006-05-02 04:52:03.208  410.139 UDP  193.237.155.232:53    ->      224.8.41.1:39918 ......   0      889   110788        2     2160    124     2
2006-05-02 04:55:12.894   45.145 UDP    191.190.51.17:44808 -> 253.232.92.197:48699 ......   0      874    1.2 M       19   218069   1408     1
2006-05-02 04:42:27.287  926.983 UDP  252.152.144.207:2906  ->   121.88.20.254:8767  ......   0      874    41952        0      362     48     1
2006-05-02 04:40:50.999  927.816 UDP    121.88.20.254:8767  -> 252.152.144.207:2906  ......   0      873    45396        0      391     52     1
2006-05-02 04:58:12.841   62.084 UDP  252.155.202.149:7000  ->  254.118.64.166:7001  ......   0      801   482579       12    62184    602     1
2006-05-02 04:54:26.980  167.576 UDP   252.152.122.19:10000 ->  172.172.21.233:11790 ......   0      787   772832        4    36894    981     1
2006-05-02 04:56:21.369  138.661 UDP   254.118.64.166:7001  ->    247.3.248.58:7000  ......   0      746    91957        5     5305    123     2
2006-05-02 04:47:28.327  657.231 UDP     247.3.248.90:0     ->  254.118.64.166:0     ......   0      709   625704        1     7616    882     2
2006-05-02 04:43:15.919  910.502 UDP    191.190.51.17:8089  -> 247.124.101.237:8089  ......   0      701   248700        0     2185    354     1
2006-05-02 04:43:15.947  910.560 UDP  247.124.101.237:8089  ->   191.190.51.17:8089  ......   0      694   331436        0     2911    477     1
2006-05-02 04:56:21.392  138.636 UDP    247.3.248.58:7000  ->  254.118.64.166:7001  ......   0      493   132606        3     7652    268     2
2006-05-02 04:40:57.494  913.857 UDP   191.181.110.36:3830  -> 247.124.101.237:3830  ......   0      478    70277        0      615    147     1
2006-05-02 04:44:04.603  924.443 UDP    191.190.51.17:5850  -> 247.124.101.236:5850  ......   0      463    62823        0      543    135     1
2006-05-02 04:44:04.598  924.453 UDP  247.124.101.236:5850  ->   191.190.51.17:5850  ......   0      461    42050        0      363     91     1

IP addresses anonymized
Time window: May 02 2006 04:39:43 - May 02 2006 04:59:59
Flows analysed: 151994 matched: 29565, Bytes read: 7431168
Sys: 0.064s flows/second: 2338765.0  Wall: 0.061s flows/second: 2474988.6
```

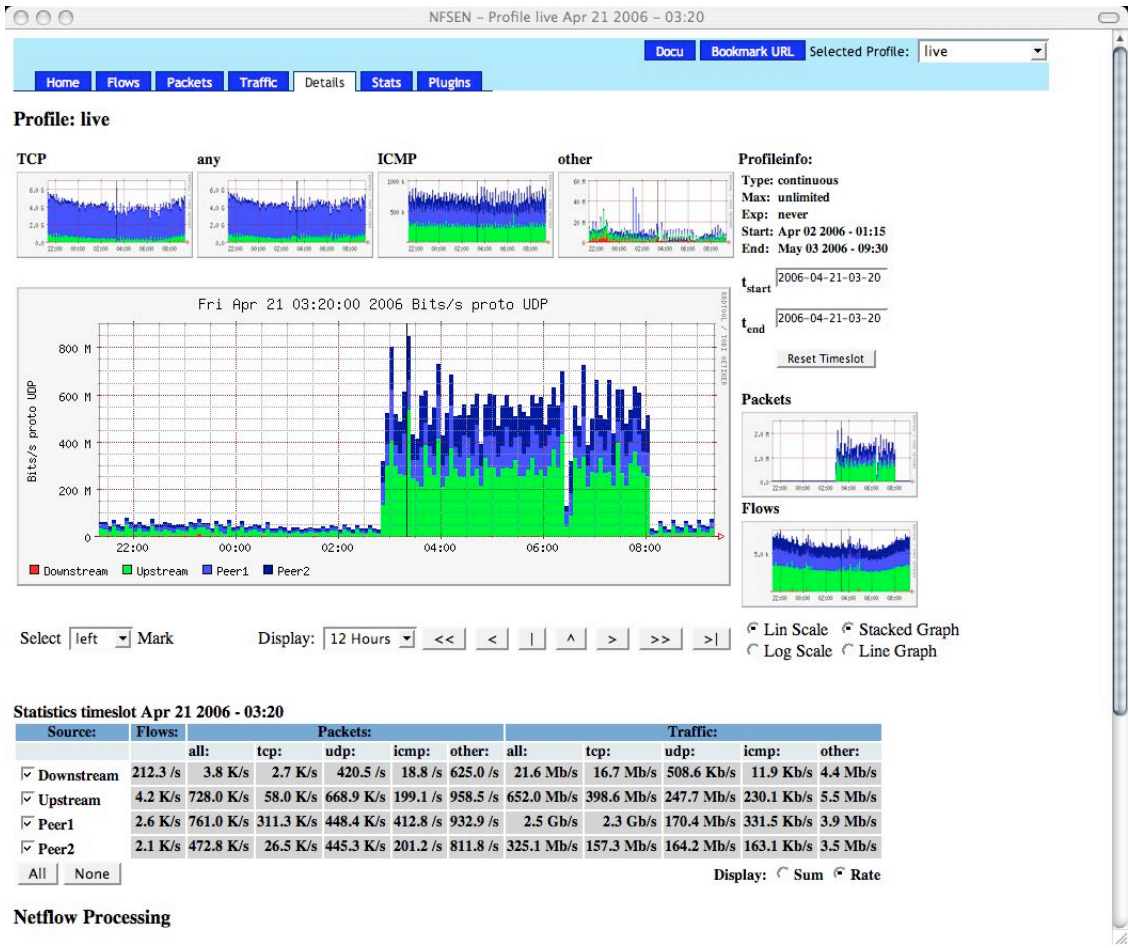

NFSEN - Profile live May 02 2006 - 21:30
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-05-02-21-30
t end 2006-05-02-21-30
Reset Timeslot
Tue May 2 21:30:00 2006 Flows/s any protocol
Flows/s any protocol
25 k
20 k
15 k
10 k
5 k
Fri
Sun
Tue
Thu
Sat
Mon
Downstream
Upstream
Peer1
Peer2
Traffic
Select left Mark
Display: 2 weeks
12 Hours
1 day
2 days
4 days
1 week
2 weeks
1 month
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot May 02 2006 - 21:30
Source:
Flows:
Traffic:
all:
tcp:
other:
udp:
icmp:
Downstream 470.6 /s 8.6 K/s 7.3 K/s 32.9 /s 40.5 Mb/s 37.5 Mb/s 2.9 Mb/s 13.1 Kb/s 77.7 Kb/s
Upstream 6.4 K/s 145.1 K/s 127.9 K/s 15.8 K/s 232.2 /s 1.2 K/s 837.2 Mb/s 800.7 Mb/s 32.8 Mb/s 284.3 Kb/s 3.3 Mb/s
Peer1 3.9 K/s 475.0 K/s 464.8 K/s 9.3 K/s 268.2 /s 758.2 /s 3.9 Gb/s 3.9 Gb/s 23.9 Mb/s 231.6 Kb/s 3.4 Mb/s
Peer2 3.3 K/s 64.8 K/s 58.1 K/s 5.9 K/s 207.1 /s 540.1 /s 397.1 Mb/s 382.6 Mb/s 12.0 Mb/s 172.9 Kb/s 2.4 Mb/s
All
None
Display: Sum Rate
Netflow Processing


NFSEN - Profile live May 02 2006 - 21:30
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-05-02-21-30
t end 2006-05-02-21-30
Reset Timeslot
Tue May 2 21:30:00 2006 Packets/s any protocol
Packets/s any protocol
2.5 M
2.0 M
1.5 M
1.0 M
0.5 M
0.0
Fri
Sun
Tue
Thu
Sat
Mon
Downstream
Upstream
Peer1
Peer2
Flows
Traffic
Select left Mark
Display: 2 weeks
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot May 02 2006 - 21:30
Source:
Flows:
Packets:
Traffic:
all:
tcp:
udp:
icmp:
other:
Downstream 470.6 /s 8.6 K/s 7.3 K/s 1.2 K/s 20.2 /s 32.9 /s 40.5 Mb/s 37.5 Mb/s 2.9 Mb/s 13.1 Kb/s 77.7 Kb/s
Upstream 6.4 K/s 145.1 K/s 127.9 K/s 15.8 K/s 232.2 /s 1.2 K/s 837.2 Mb/s 800.7 Mb/s 32.8 Mb/s 284.3 Kb/s 3.3 Mb/s
Peer1 3.9 K/s 475.0 K/s 464.8 K/s 9.3 K/s 268.2 /s 758.2 /s 3.9 Gb/s 3.9 Gb/s 23.9 Mb/s 231.6 Kb/s 3.4 Mb/s
Peer2 3.3 K/s 64.8 K/s 58.1 K/s 5.9 K/s 207.1 /s 540.1 /s 397.1 Mb/s 382.6 Mb/s 12.0 Mb/s 172.9 Kb/s 2.4 Mb/s
All
None
Display: Sum Rate
Netflow Processing


NFSEN - Profile live May 02 2006 - 21:30
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
any
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-05-02-21-30
t end 2006-05-02-21-30
Reset Timeslot
Tue May 2 21:30:00 2006 Packets/s proto UDP
Packets/s proto UDP
1.5 M
1.0 M
0.5 M
0.0
Fri
Sun
Tue
Thu
Sat
Mon
Downstream
Upstream
Peer1
Peer2
Flows
Traffic
Select left Mark
Display: 2 weeks
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot May 02 2006 - 21:30
Source: Flows: Packets: Traffic:
all: tcp: udp: icmp: other: all: tcp: udp: icmp: other:
Downstream 470.6 /s 8.6 K/s 7.3 K/s 1.2 K/s 20.2 /s 32.9 /s 40.5 Mb/s 37.5 Mb/s 2.9 Mb/s 13.1 Kb/s 77.7 Kb/s
Upstream 6.4 K/s 145.1 K/s 127.9 K/s 15.8 K/s 232.2 /s 1.2 K/s 837.2 Mb/s 800.7 Mb/s 32.8 Mb/s 284.3 Kb/s 3.3 Mb/s
Peer1 3.9 K/s 475.0 K/s 464.8 K/s 9.3 K/s 268.2 /s 758.2 /s 3.9 Gb/s 3.9 Gb/s 23.9 Mb/s 231.6 Kb/s 3.4 Mb/s
Peer2 3.3 K/s 64.8 K/s 58.1 K/s 5.9 K/s 207.1 /s 540.1 /s 397.1 Mb/s 382.6 Mb/s 12.0 Mb/s 172.9 Kb/s 2.4 Mb/s
All
None
Display: Sum Rate
Netflow Processing

NFSEN - Profile live Apr 21 2006 - 06:50
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
any
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-04-21-06-50
t end 2006-04-21-06-50
Reset Timeslot
Fri Apr 21 06:50:00 2006 Packets/s proto UDP
Packets/s proto UDP
1.5 M
1.0 M
0.5 M
0.0
Fri
Sun
Tue
Thu
Sat
Mon
Downstream
Upstream
Peer1
Peer2
Flows
Traffic
Select left Mark
Display: 2 weeks
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot Apr 21 2006 - 06:50
Source: Flows: Packets: Traffic:
all: tcp: udp: icmp: other: all: tcp: udp: icmp: other:
Downstream 220.8 /s 3.0 K/s 2.4 K/s 317.2 /s 16.2 /s 233.5 /s 12.0 Mb/s 10.3 Mb/s 452.0 Kb/s 10.4 Kb/s 1.3 Mb/s
Upstream 3.9 K/s 925.4 K/s 26.7 K/s 898.1 K/s 203.3 /s 305.6 /s 490.3 Mb/s 163.4 Mb/s 325.8 Mb/s 238.6 Kb/s 873.5 Kb/s
Peer1 2.8 K/s 792.3 K/s 346.1 K/s 445.6 K/s 223.4 /s 362.2 /s 3.1 Gb/s 2.9 Gb/s 163.7 Mb/s 210.1 Kb/s 605.3 Kb/s
Peer2 2.2 K/s 575.1 K/s 15.3 K/s 559.6 K/s 172.2 /s 46.0 /s 301.3 Mb/s 100.2 Mb/s 200.9 Mb/s 139.6 Kb/s 52.3 Kb/s
All
None
Display: Sum Rate
Netflow Processing


NFSEN - Profile live Apr 21 2006 - 03:20
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
any
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-04-21-03-20
t end 2006-04-21-03-20
Reset Timeslot
Fri Apr 21 03:20:00 2006 Packets/s proto UDP
Packets/s proto UDP
2.5 M
2.0 M
1.5 M
1.0 M
0.5 M
0.0
22:00
00:00
02:00
04:00
06:00
08:00
Downstream
Upstream
Peer1
Peer2
Flows
Traffic
Select left Mark
Display: 12 Hours
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot Apr 21 2006 - 03:20
Source:
Flows:
Packets:
Traffic:
all:
tcp:
udp:
icmp:
other:
Downstream 212.3 /s 3.8 K/s 2.7 K/s 420.5 /s 18.8 /s 625.0 /s 21.6 Mb/s 16.7 Mb/s 508.6 Kb/s 11.9 Kb/s 4.4 Mb/s
Upstream 4.2 K/s 728.0 K/s 58.0 K/s 668.9 K/s 199.1 /s 958.5 /s 652.0 Mb/s 398.6 Mb/s 247.7 Mb/s 230.1 Kb/s 5.5 Mb/s
Peer1 2.6 K/s 761.0 K/s 311.3 K/s 448.4 K/s 412.8 /s 932.9 /s 2.5 Gb/s 2.3 Gb/s 170.4 Mb/s 331.5 Kb/s 3.9 Mb/s
Peer2 2.1 K/s 472.8 K/s 26.5 K/s 445.3 K/s 201.2 /s 811.8 /s 325.1 Mb/s 157.3 Mb/s 164.2 Mb/s 163.1 Kb/s 3.5 Mb/s
All
None
Display: Sum Rate
Netflow Processing


NFSEN - Profile live Apr 21 2006 - 03:20
Docu
Bookmark URL
Selected Profile: live
Home
Flows
Packets
Traffic
Details
Stats
Plugins
Profile: live
TCP
any
ICMP
other
Profileinfo:
Type: continuous
Max: unlimited
Exp: never
Start: Apr 02 2006 - 01:15
End: May 03 2006 - 09:30
t start 2006-04-21-03-20
t end 2006-04-21-03-20
Reset Timeslot
Fri Apr 21 03:20:00 2006 Bits/s proto UDP
Bits/s proto UDP
800 M
600 M
400 M
200 M
0
22:00
00:00
02:00
04:00
06:00
08:00
Downstream
Upstream
Peer1
Peer2
Packets
Flows
Select left Mark
Display: 12 Hours
Lin Scale
Stacked Graph
Log Scale
Line Graph
Statistics timeslot Apr 21 2006 - 03:20
Source:
Flows:
Packets:
Traffic:
all:
tcp:
udp:
icmp:
other:
Downstream 212.3 /s 3.8 K/s 2.7 K/s 420.5 /s 18.8 /s 625.0 /s 21.6 Mb/s 16.7 Mb/s 508.6 Kb/s 11.9 Kb/s 4.4 Mb/s
Upstream 4.2 K/s 728.0 K/s 58.0 K/s 668.9 K/s 199.1 /s 958.5 /s 652.0 Mb/s 398.6 Mb/s 247.7 Mb/s 230.1 Kb/s 5.5 Mb/s
Peer1 2.6 K/s 761.0 K/s 311.3 K/s 448.4 K/s 412.8 /s 932.9 /s 2.5 Gb/s 2.3 Gb/s 170.4 Mb/s 331.5 Kb/s 3.9 Mb/s
Peer2 2.1 K/s 472.8 K/s 26.5 K/s 445.3 K/s 201.2 /s 811.8 /s 325.1 Mb/s 157.3 Mb/s 164.2 Mb/s 163.1 Kb/s 3.5 Mb/s
All
None
Display: Sum Rate
Netflow Processing

NFSEN – Profile live Apr 21 2006 – 03:20

Statistics timeslot Apr 21 2006 - 03:20

Source:	Flows:	Packets:					Traffic:				
		all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
Downstream	212.3 /s	3.8 K/s	2.7 K/s	420.5 /s	18.8 /s	625.0 /s	21.6 Mb/s	16.7 Mb/s	508.6 Kb/s	11.9 Kb/s	4.4 Mb/s
Upstream	4.2 K/s	728.0 K/s	58.0 K/s	668.9 K/s	199.1 /s	958.5 /s	652.0 Mb/s	398.6 Mb/s	247.7 Mb/s	230.1 Kb/s	5.5 Mb/s
Peer1	2.6 K/s	761.0 K/s	311.3 K/s	448.4 K/s	412.8 /s	932.9 /s	2.5 Gb/s	2.3 Gb/s	170.4 Mb/s	331.5 Kb/s	3.9 Mb/s
Peer2	2.1 K/s	472.8 K/s	26.5 K/s	445.3 K/s	201.2 /s	811.8 /s	325.1 Mb/s	157.3 Mb/s	164.2 Mb/s	163.1 Kb/s	3.5 Mb/s

All None Display: Sum Rate

Netflow Processing

Source: Downstream, Upstream, Peer1, Peer2 — All Sources

Filter: udp — and <none>

Show: List: First 10 Flows; aggregated; time sorted; long output — process

Stat: Top 20; Limit Packets > 0 -; Flows order by bps; long output; Any IP Addr order by bps — process; Clear Form

```
/usr/local/bin/nfdump -M /netflow2/nfsen-devel/profiles/live/Downstream:Upstream:Peer1:Peer2 -r nfcapd.200604210320 -n 20 -s record/bps -o extended 'udp '

Aggregated flows 1090426
Top 20 flows ordered by bps:
Date flow start          Duration Proto    Src IP Addr:Port          Dst IP Addr:Port   Flags Tos  Packets    Bytes      pps      bps    Bpp Flows
2006-04-21 03:17:04.531  456.636 UDP  171.232.166.244:37263 -> 253.163.140.151:53    ......   0  129.4 M    5.8 G   297237  104.3 M     46     4
2006-04-21 03:17:04.638  460.499 UDP   125.46.184.211:47125 -> 253.163.140.151:53    ......   0  129.5 M    5.8 G   294944  103.5 M     46     4
2006-04-21 03:17:30.121  232.128 UDP    171.8.244.170:46294 -> 253.163.140.151:53    ......   0   32.2 M    1.4 G   145543   51.1 M     46     1
2006-04-21 03:17:46.123  236.096 UDP    126.205.7.109:47018 -> 253.163.140.151:53    ......   0   32.5 M    1.5 G   144185   50.6 M     46     1
2006-04-21 03:16:06.152  328.128 UDP    108.44.41.181:43830 -> 253.163.140.151:53    ......   0   32.3 M    1.5 G   103351   36.3 M     46     1
2006-04-21 03:18:26.122  356.224 UDP   109.93.137.123:45444 -> 253.163.140.151:53    ......   0   32.1 M    1.4 G    94434   33.1 M     46     1
2006-04-21 03:12:37.961  552.256 UDP  119.137.230.210:45837 -> 253.163.140.151:53    ......   0   32.0 M    1.4 G    60795   21.3 M     46     1
2006-04-21 03:20:23.378    0.001 UDP    15.238.99.170:53    -> 191.190.255.129:32899 ......   0        6     1878     6000   14.3 M    313     2
2006-04-21 03:20:35.152    0.001 UDP      179.216.88.1:53   ->  252.152.125.20:32769 ......   0        6     1110     6000    8.5 M    185     2
2006-04-21 03:23:22.250    0.001 UDP   106.230.159.83:53    -> 253.227.214.215:35699 ......   0        8     1040     8000    7.9 M    130     2
2006-04-21 03:23:06.113    0.014 UDP    191.52.25.202:53    -> 253.227.214.214:33928 ......  128       24    13512     1714    7.4 M    563     2
2006-04-21 03:23:32.789    0.001 UDP    255.33.98.231:9875  ->   128.122.1.249:9875  .A....   0        2      938     2000    7.2 M    469     2
2006-04-21 03:21:40.809    0.001 UDP  192.160.248.158:59468 ->     242.190.27.9:53    ......   0       12      924    12000    7.0 M     77     2
2006-04-21 03:22:42.954    0.001 UDP  171.217.137.235:52936 -> 252.152.192.248:19672 ......   0        2      888     2000    6.8 M    444     2
2006-04-21 03:23:43.051    0.001 UDP      189.182.72.7:53   ->  254.174.227.32:32780 ......   0        4      828     4000    6.3 M    207     2
2006-04-21 03:24:19.215    0.001 UDP  202.150.215.139:0     -> 252.152.110.103:1025  ......   0        2      826     2000    6.3 M    413     2
2006-04-21 03:24:19.214    0.001 UDP  202.150.215.139:0     -> 252.152.110.106:1025  ......   0        2      826     2000    6.3 M    413     2
2006-04-21 03:24:19.214    0.001 UDP  202.150.215.139:0     ->  252.152.110.62:1026  ......   0        2      826     2000    6.3 M    413     2
2006-04-21 03:24:19.214    0.001 UDP  202.150.215.139:0     ->  252.152.110.37:1025  ......   0        2      826     2000    6.3 M    413     2
2006-04-21 03:24:19.214    0.001 UDP  202.150.215.139:0     ->  252.152.110.46:1026  ......   0        2      826     2000    6.3 M    413     2

IP addresses anonymized
Time window: Apr 21 2006 03:04:53 - Apr 21 2006 03:24:58
Flows analysed: 2819126 matched: 1673043, Bytes read: 137655456
Sys: 2.055s flows/second: 1371379.7  Wall: 2.090s flows/second: 1348602.8
```

nfdump and NfSen

SWITCH
The Swiss Education & Research Network

Profiles:

- A profile is a specific view on the netflow data with nfdump filters applied.
- The profile applies to the graphical as well as to the numerical view.
- Profiles can be created from data in the past. (static)
- Profiles can be created from incoming data (continuous)
- Any views or processing options are available.

nfdump and NfSen

SWITCH
The Swiss Education & Research Network

NFSEN – Profile DNStraffic Overview

Docu | Bookmark URL | Selected Profile: DNStraffic

Home | Flows | Packets | Traffic | Details | Stats | Plugins

Profile:	DNStraffic Name of new profile. The naming follows the directory naming definition.
Description:	All port 53 traffic
Start:	Format: yyyy-mm-dd-HH-MM Start time of new profile. Any time is accepted from **2006-04-02-01-15** (Start of the **live** profile) up to **2006-05-03-11-30**. If left empty, the profile starts from now: **2006-05-03-11-30** (continuous profile).
End:	Format: yyyy-mm-dd-HH-MM End time of new profile. Must be later than start of the profile. Leave empty for a continuous profile.
Sources:	Downstream Upstream Peer1 Peer2
Filter:	port 53 and (tcp or udp)
Max. Size:	0 Maximum size, this profile may grow. Any number is taken as **MB**, unless another scale is specified such as **K, M, G, T** or **KB, MB, GB, TB**. If set to **0**, no size limit applies. Ex. 300, 300M, 2G etc.
Expire:	never Expire time. This specifies the maximum lifetime for this profile. Data files older than this, will be deleted. Any number is taken as **hours** unless another scale is specified such as **d, day, days** and/or **h, hour, hours**. If set to **0** or **never**, no time limit applies. Ex. 72, 72h, 4d 12h, 14days etc.

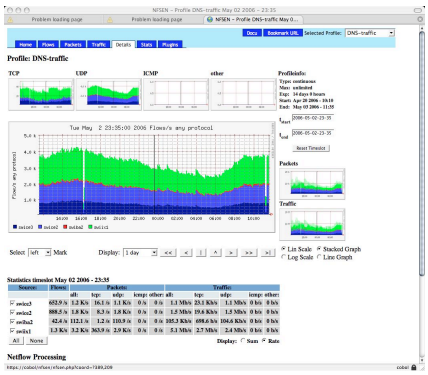
Cancel | Create Profile

nfdump and NfSen

SWITCH
The Swiss Education & Research Network

Profile: ‘port 53 and (tcp or udp):

Overview ⇒ Details



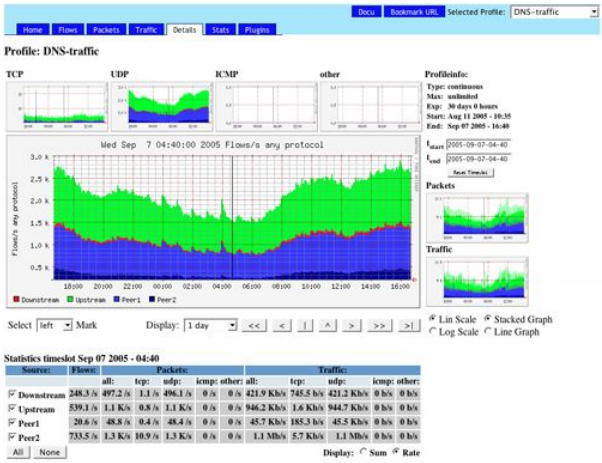
Details ⇒ Flows

nfdump and NfSen

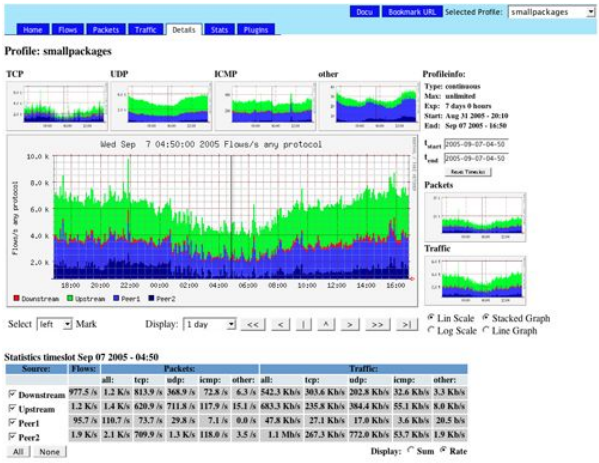
SWITCH
The Swiss Education & Research Network

Example Profiles:

Filter: ‘(udp or tcp) and port 53



Filter: ‘bytes < 100’

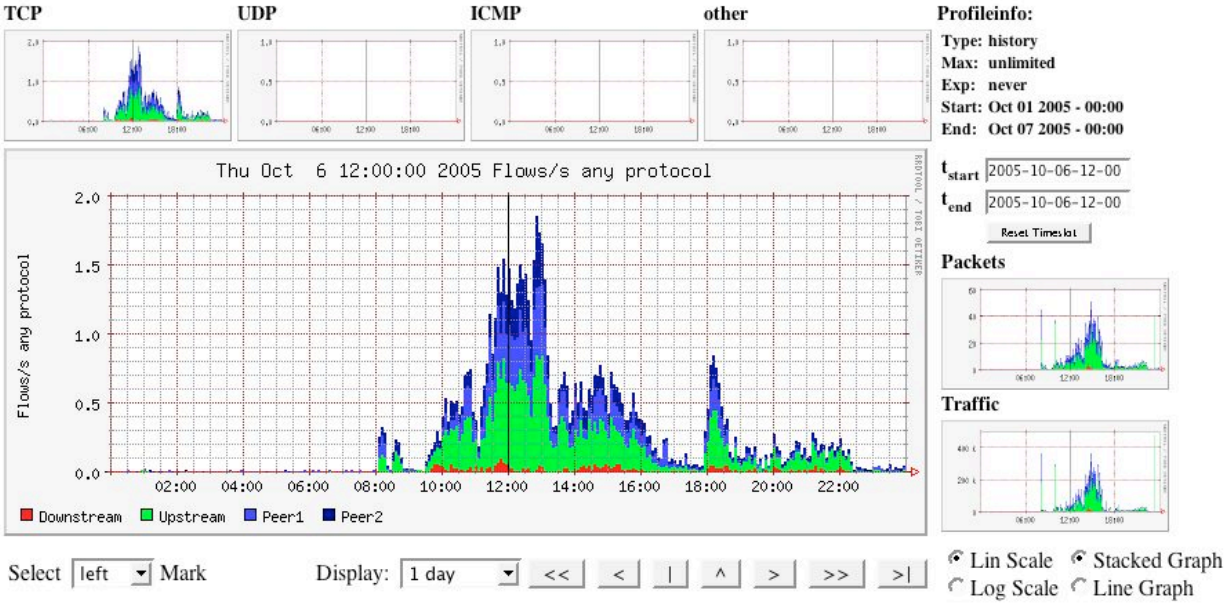


Filters may be as complex as the the filter syntax of nfdump allows.
Example: ‘((src net 172.16/16 and src port > 1024) or dst host 192.168.16.17 and dst port 80) and packets > 1000 and pps > 150’

NfSen/NFDUMP

SWITCH
The Swiss Education & Research Network

SoberR: ‘tcp and dst port 587’



Incident analysis - profile a hacked host:

Plugins - what for?

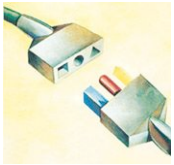
- Monitoring and alerting.
- Track for known botnet masters and send notifications.
- Track for possible scanners or DoS attacks, not necessarily visible in the graph.
- Port Tracking.

Backend Plugins are:

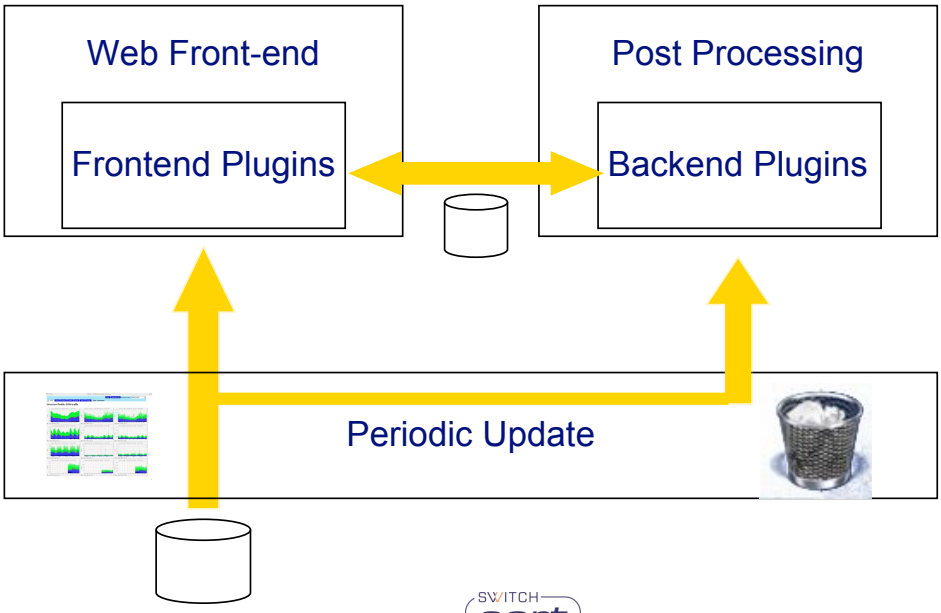
- Simple Perl modules hooked into the NfSen backend.
- Automatically called at regular 5 Min intervals.

Frontend Plugins are:

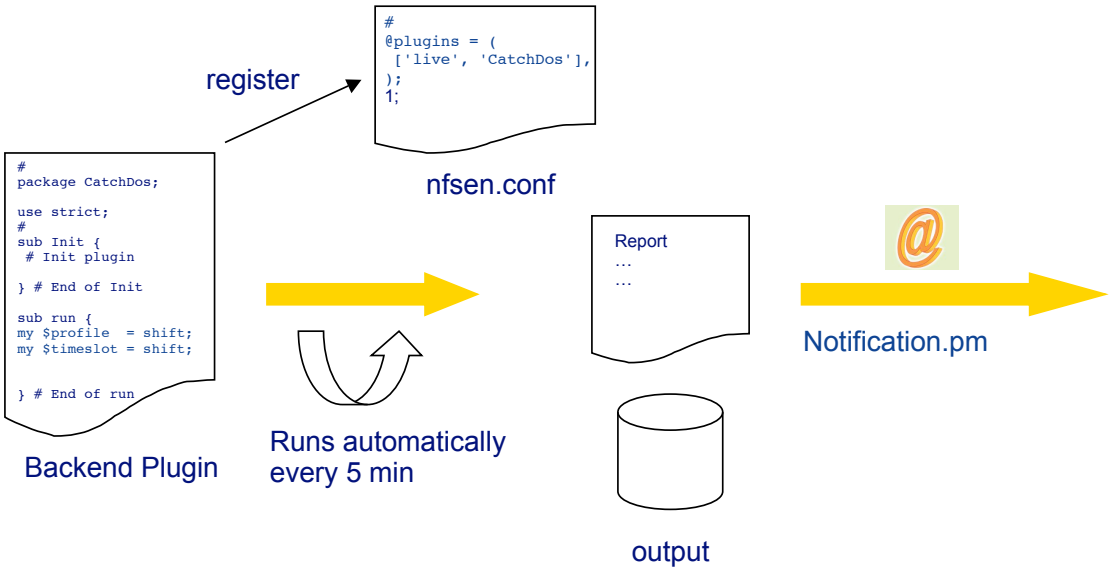
- Simple PHP modules hooked into NfSen frontend.
- Called by selecting the tab.



NfSen Plugins:



Backend Plugins:



Writing Backend Plugins:

- Select a plugin name: **MyPlugin**
- Create a Perl module named **MyPlugin.pm**
- Write your code.
- Try/debug your module offline using $BINDIR/testPlugin:
  ./testPlugin -p MyPlugin -P live -t 200603140800
- Store the file MyPlugin.pm in the directory $BACKEND_PLUGINDIR (e.g. /data/nfsen/plugins)
- Register the plugin in nfsen.conf for the profiles in question:

```
@plugins = ( # profile    # modul
   # [ '*',     'demoplugin' ],
   [ 'live',    'MyPlugin'],
);
```



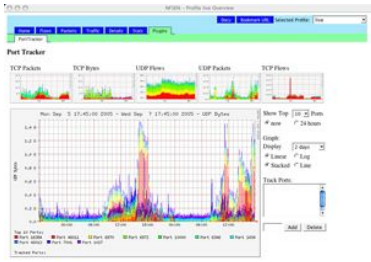
```
#!/usr/bin/perl

package MyPlugin;

use strict;
# Periodic function
# input:  profilename
#         timeslot. Format yyyymmddHHMM e.g. 200503031200
sub run {
     my $profile  = shift;
     my $timeslot = shift;
     # Called at every cycle
     # Your code goes here

}

sub Init {
     # Do module init staff here

     # return 1 on success - module successfully loaded
     # return 0 on failure - module disabled
     return 1;
}

sub BEGIN {
     # Standard BEGIN Perl function - See Perl documentation
     # Called on loading the module
}

sub END {
     # Standard END Perl function - See Perl documentation
     # Called on unloading the module
}

1;
```

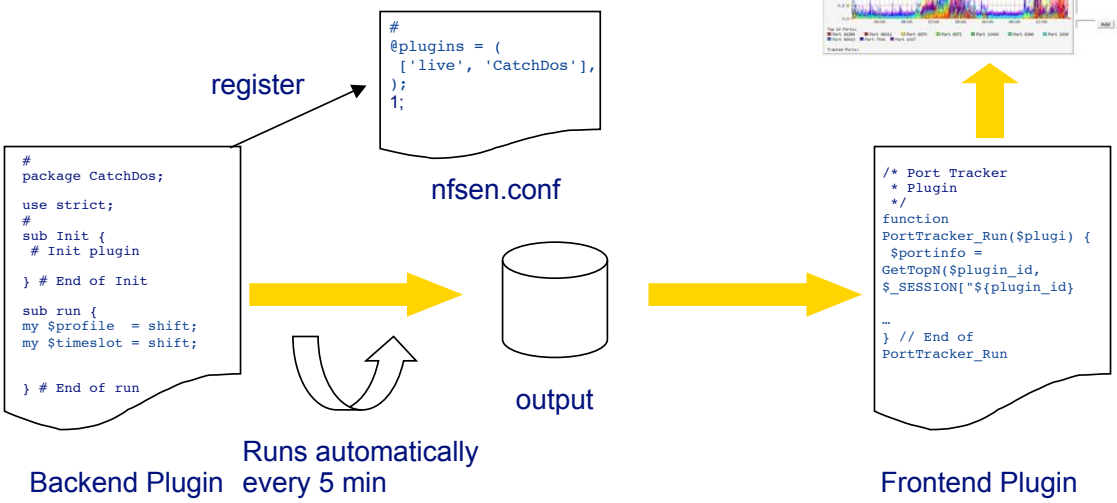
Example Candidates for scanning activities:

```
….
#
#
# Define a nice filter:
# We like to see flows containing more than xxx packets
my $limit = 6000 ;
my $nf_filter = 'duration < 3500 and packets < 3 and bpp < 100 and src as 559';

# Periodic function
#   input:  profilename
#           timeslot. Format yyyymmddHHMM e.g. 200503031200
sub run {
    my $profile  = shift;
    my $timeslot = shift;

    syslog('debug', "CatchScanners run: Profile: $profile, Time: $timeslot");

    my %profileinfo     = NfSen::ReadProfile($profile);
    my $netflow_sources = $profileinfo{'sourcelist'};

    #
    # process all sources of this profile at once
    my @output = `$nfdump -M $PROFILEDATADIR/$profile/$netflow_sources -r nfcapd.$timeslot -a -A srcip,dstport -l
    $limit -f $nf_filter`;

    #
    # Process the output and notify the duty team
…
```

(IP addresses anonymised)

Backend / Frontend Plugins:





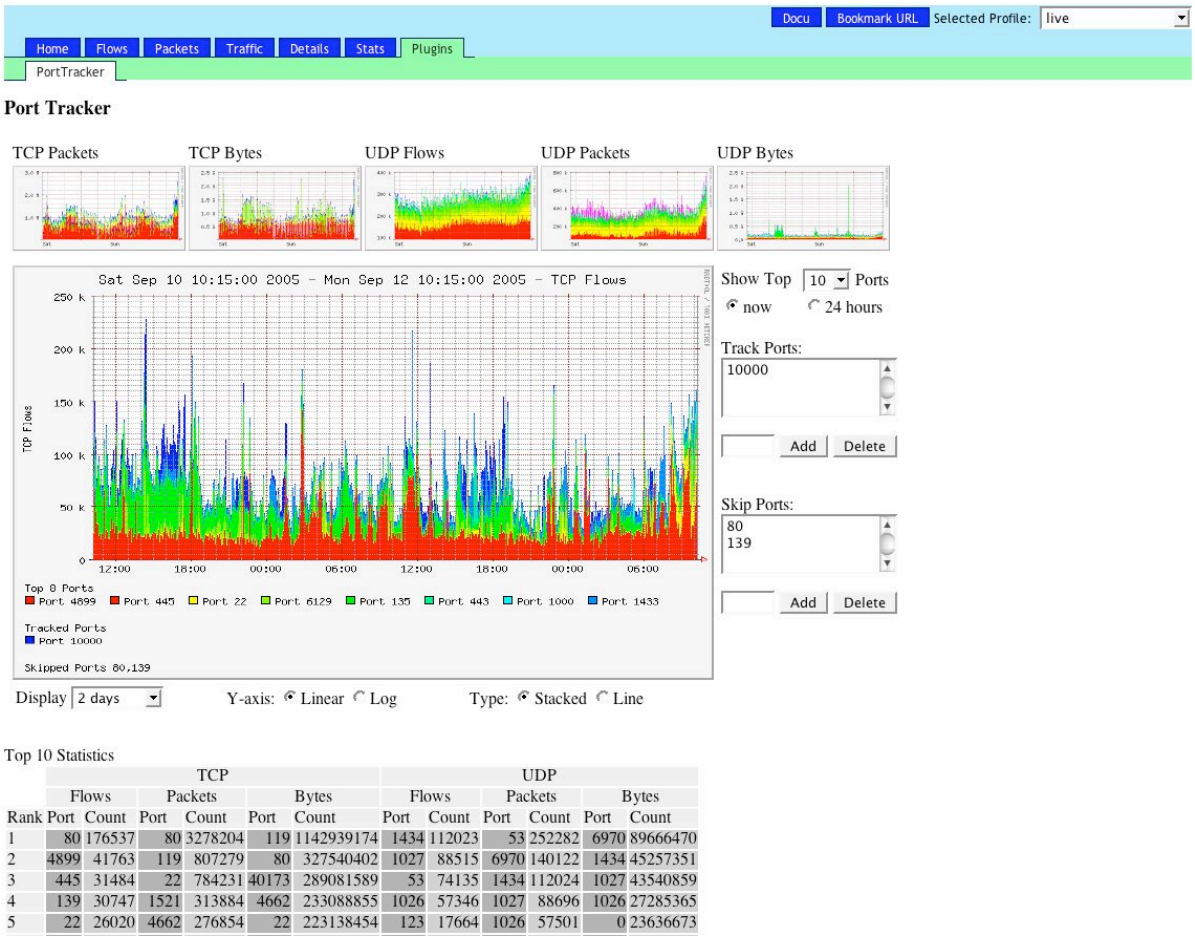
Writing Frontend Plugins:

- Write the Backend plugin: **MyPlugin**
- Create a PHP module named **MyPlugin.php**
- Write your code.
  - Must have 2 well defined functions:

    ```
    function <plugin_name>_ParseInput( $plugin_id )
    function <plugin_name>_Run( $plugin_id )
    ```

  - Have each a unique plugin ID: $plugin_id
  - Run at any time the user selects the plugin.
  - Profile read only information available in $_SESSION['profileinfo']
    example: `$_SESSION['profileinfo']['name']`
- Store the file MyPlugin.php in the directory $FRONTEND_PLUGINDIR (e.g. /var/www/htdocs/nfsen/plugins)
- Reload nfsen-run backgroud process: `$BINDIR/nfsen reload`
- Check correct load of module in syslog file.


```
<?

/*
 * MyPlugin plugin
 */

// Required functions
/*
 * This function is called prior to any output to the web browser and is intended
 * for the plugin to parse possible form data. This function is called only, if this
 * plugin is selected in the plugins tab
 */
function MyPlugin_ParseInput( $plugin_id ) {

    if ( isset($_POST["${plugin_id}_variable"]) ) {

    } else {
        $_SESSION['warning'] = "Warning …";
        $_SESSION['error'] = "Error …";
    }

} // End of MyPlugin_ParseInput


/*
 * This function is called after the header with the navigation bar have been sent to the
 * browser. It's now up to this function what to display.
 * This function is called only, if this plugin is selected in the plugins tab
 */
function MyPlugin_Run( $plugin_id ) {

    $_SESSION["${plugin_id}_variable"] = …

} // End of MyPlugin_Run


?>
```



Top 10 Statistics

	TCP						UDP					
	Flows		Packets		Bytes		Flows		Packets		Bytes	
Rank	Port	Count	Port	Count	Port	Count	Port	Count	Port	Count	Port	Count
1	80	176537	80	3278204	119	1142939174	1434	112023	53	252282	6970	89666470
2	4899	41763	119	807279	80	327540402	1027	88515	6970	140122	1434	45257351
3	445	31484	22	784231	40173	289081589	53	74135	1434	112024	1027	43540859
4	139	30747	1521	313884	4662	233088855	1026	57346	1027	88696	1026	27285365
5	22	26020	4662	276854	22	223138454	123	17664	1026	57501	0	23636673

nfdump and NfSen

SWITCH
The Swiss Education & Research Network

Planned Plugin: Host behaviour based worm detection:

Result of a PhD network security research work in the context of the DDoSVax project at **Swiss Federal Institute of Technology Zurich**:
http://www.tik.ee.ethz.ch/~ddosvax/

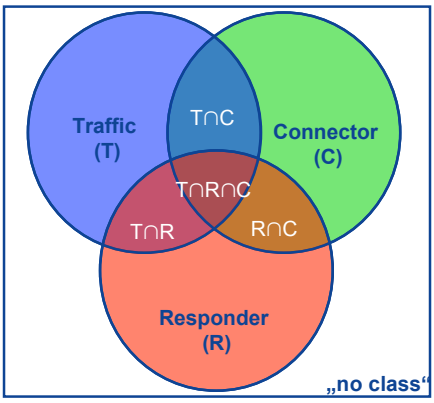
Idea: Infected hosts show a different behaviour and can be put into different classes:

„Traffic“ class:
Worm infected hosts tend to send considerably more traffic than they receive.

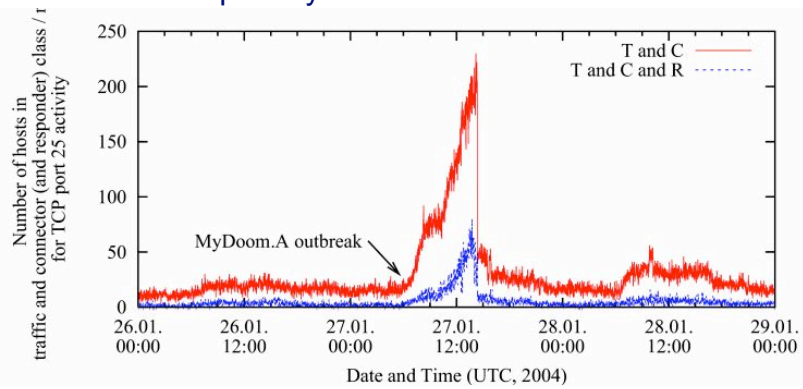
„Responder“ class:
If many more hosts start to answer requests, they probably are victims of a worm.

„Connector“ class:
Worm infected hosts typically open many connections.

DDoS Vax : Host behaviour based worm detection:



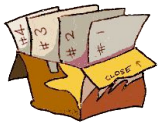
Example: MyDoom.A



Most interesing for worm detection are cardinalities of class combinations.

Figures @ SWITCH:

- Server: 2 x 3GHz 2GB Ram. Debian Linux Kernel 2.6.10
- 3TB (2TB + 1TB) AXUS Disk Raid
- XFS file system.
- Gigabit Ethernet interfaces.
- 5min workload avg. ca. 5%.
- 25GB Netflow data / day.
- About 41 days of netflow data available.



nfdump and NfSen

SWITCH
The Swiss Education & Research Network

Next Steps - Todo list - a lot of work:

NfSen:

- more plugins ..
- Improved profiles.
- Improved interface.
- …

nfdump:

- Related filters: 'Worm Footprint Tracking'

```
first { dst ip <A> dst port 445 bytes > 600 }
then { src ip <A> and dst ip 172.16.17.18 and dst port 80 }
```

- Include more v9/sflow data in capture files.
- Realtime flow processing.
- Nesting direcoriy levels for data organisation
- …

nfdump and NfSen

SWITCH
The Swiss Education & Research Network

Summary:

- Powerful and flexible tools for all sort of netflow tasks.
  - Network monitoring.
  - Incident Handling.
  - All sort of tracking …
- Open Source under BSD License.
- Cmd line tool: nfdump
  - Written in C. Runs on most *nix.
    Tested on Linux Kernel 2.4.* and 2.6.*,
    FreeBSD, OpenBSD, Solaris.
  - Available at http://nfdump.sourceforge.net
- Web based frontend: NfSen
  - Written in PHP and Perl.
  - Extendable using plugins.
  - Available at http://nfsen.sourceforge.net

Thank you for your attention.
Any Questions?