

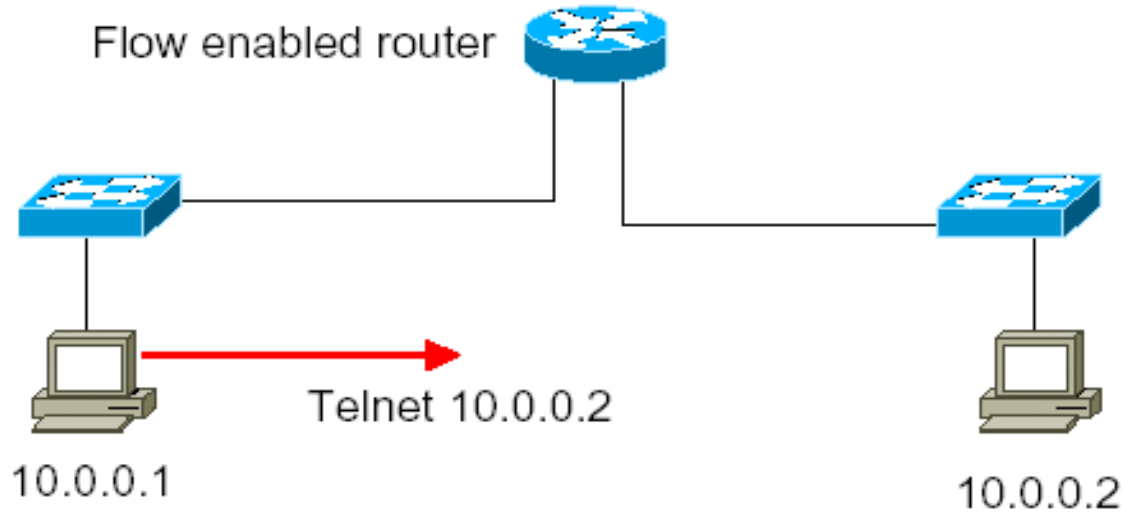
Netflow: Enabling Network Defence

Warren Daly
Network Security Expert
HEAnet

What is Netflow?

- High Performance Switching
- Traffic flow analysis

How does it work?



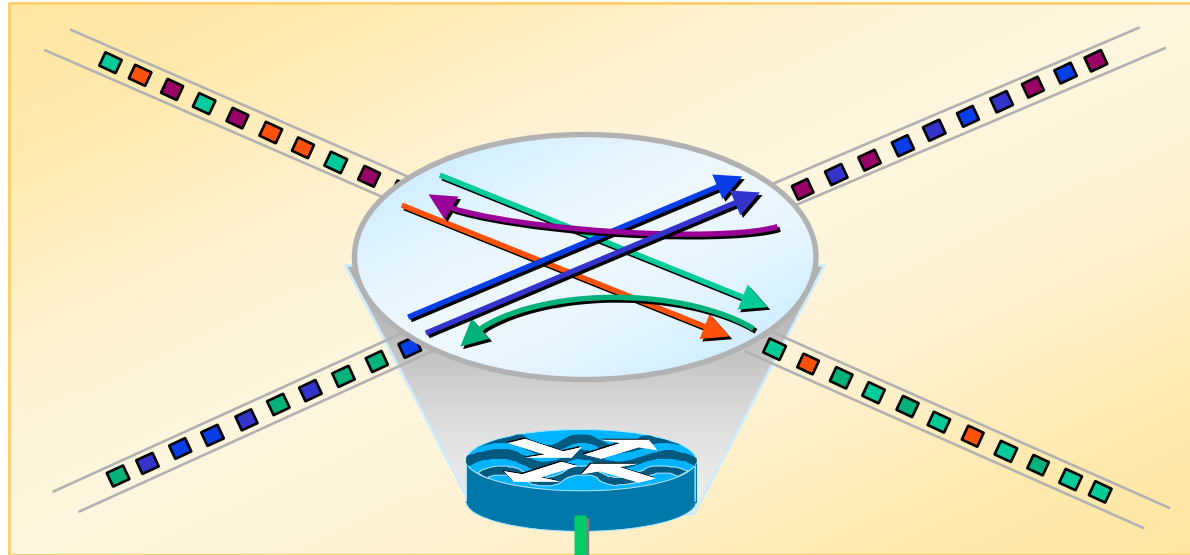
Router creates two flows, one for the client initiating the telnet and one for the server replying to the client.

src IP	dst IP	protocol	src port	dst port
10.0.0.1	10.0.0.2	TCP	1025	23
10.0.0.2	10.0.0.1	TCP	23	1025

Flow Contents

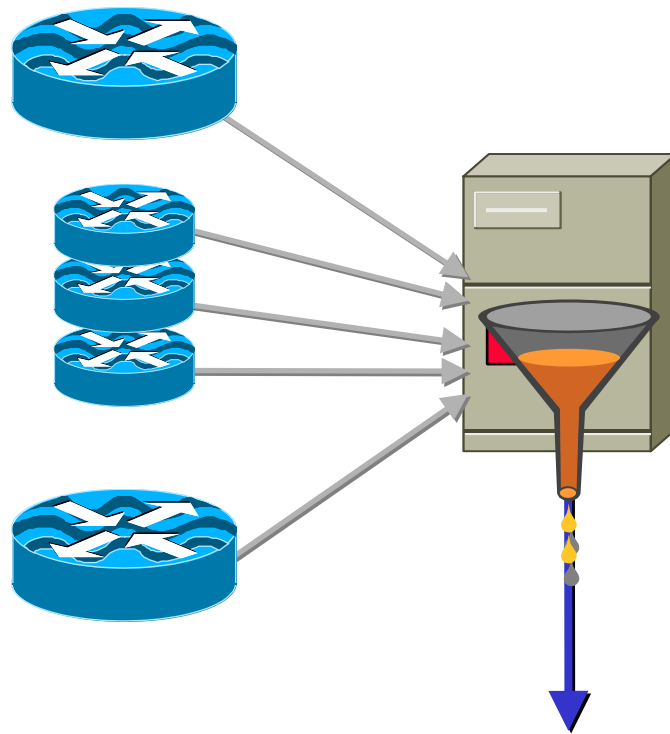
- Start / End time
- Source / Destination Interfaces
- Number of packets / octets
- Source / Destination IP
- Source / Destination PORT
- TCP Flags / QoS
- Source / Destination AS

Netflow Processor



NetFlow Data Exported

Empowers



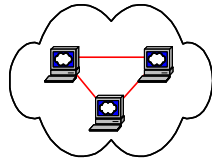
- Rich Data Set
- Data mining
- Imagination

Applications

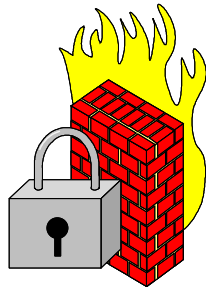
Applications



- Statistics

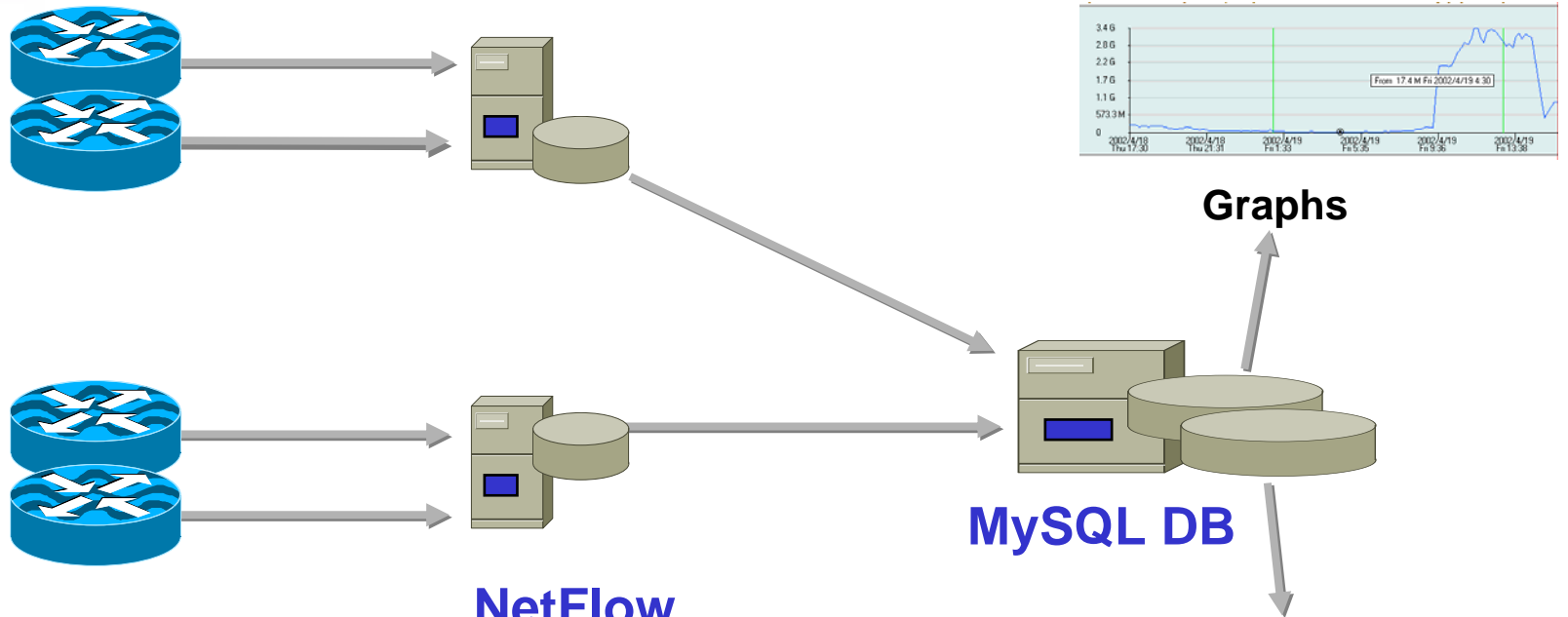


- Network Planning & Debugging



- Security

Infrastructure

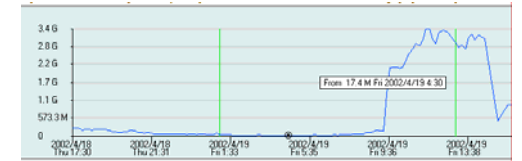


NetFlow Accounting:

- Data Switching
- Data Export
- Data Aggregation

NetFlow Collector

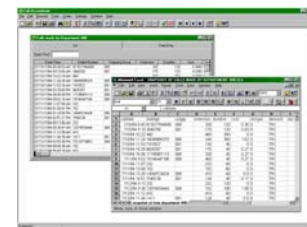
- Data Collection
- Data Filtering
- Data Aggregation
- Data Storage
- File System Management



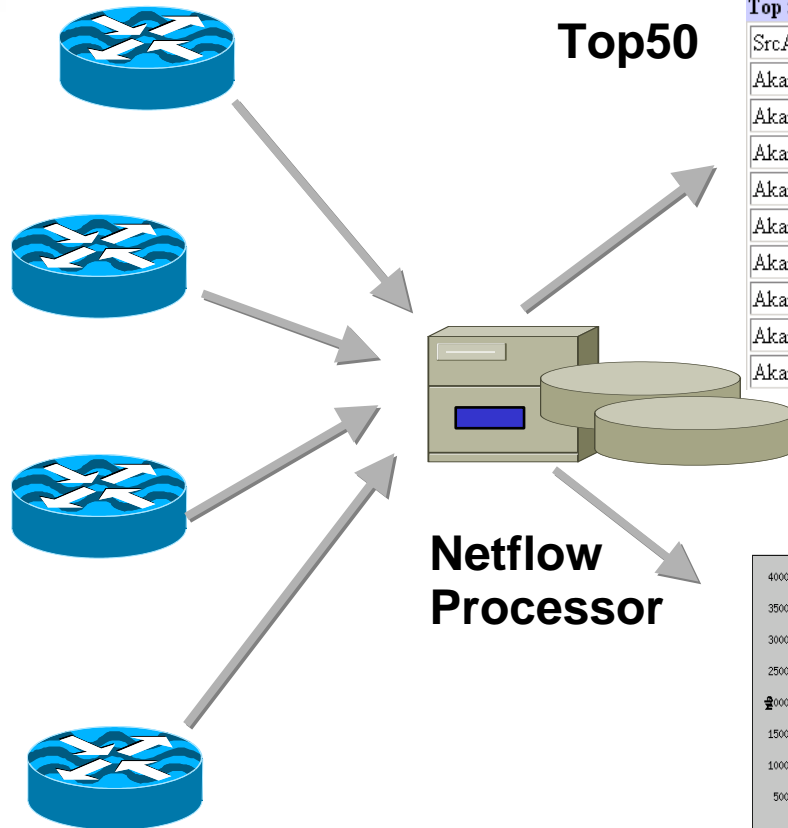
Graphs

MySQL DB

TOP50



Tools



Top50

Top 50 Incoming Traffic Statistics for NUIG - Mon, 4 Nov 2002 23:32:14 +0000 - HEAnet noc@heanet.ie

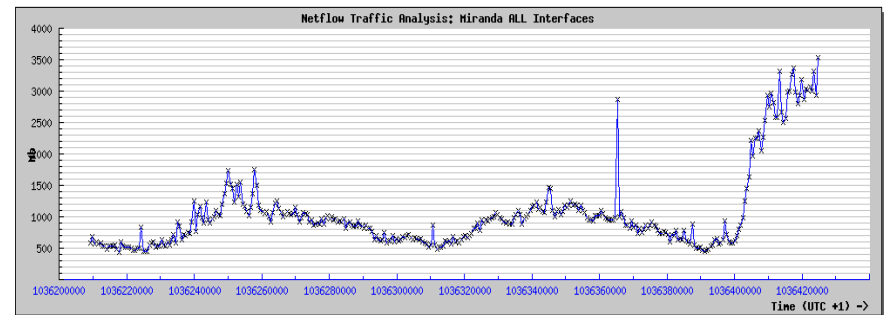
SrcAddr	DstAddr	Dstport	Timestamp	Doctets	
Akamai8.heanet	Castor-a.it.nuigalway.ie	80	Sun Nov 3 18:10	181129869	
Akamai9.heanet	aspen.nuigalway.ie	80	Fri Nov 1 12:40	145676346	
Akamai9.heanet	dspru04.nuigalway.ie	80	Mon Nov 4 9:30	144919507	
Akamai9.heanet	aspen.nuigalway.ie	80	Fri Nov 1 12:50	144562152	
Akamai9.heanet	Castor-b.it.nuigalway.ie	80	Mon Nov 4 13:20	142726667	
Akamai8.heanet	elec205.nuigalway.ie	80	Fri Nov 1 13:30	141539839	
Akamai8.heanet	phystaff07.physics.nuigalway.ie	80	Wed Oct 30 11:50	140177231	
Akamai9.heanet	majko1.nuigalway.ie	80	Fri Nov 1 16:40	140148870	
Akamai8.heanet	phystaff07.physics.nuigalway.ie	80	Wed Oct 30 13:00	135806651	

Netflow Accounting

Netflow Processor

NETFLOW VERSION 0.6

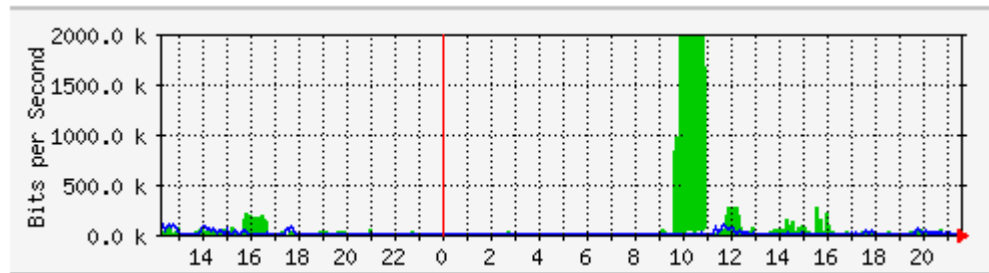
USERID: 1
USERNAME: heanet



Interactive Graphs

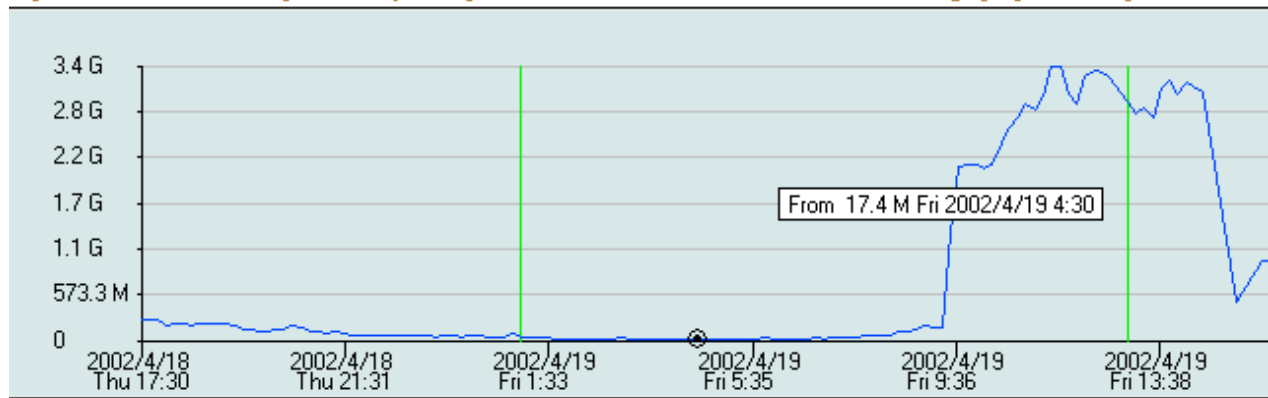
Real Life

- Network is slow



- Logs are gone!
- Netflow to the rescue

Point & Click



143.239.130.150	138.15.108.47	20	Sun Nov 3 20:20	101415440	■
143.239.130.150	138.15.108.47	20	Sun Nov 3 20:30	100315960	■
143.239.130.150	138.15.108.47	20	Sun Nov 3 20:40	93581020	■
143.239.130.150	138.15.108.47	20	Sun Nov 3 20:10	80427504	■
143.239.178.160	141.156.216.45	443	Mon Nov 4 17:20	60366518	■
143.239.130.150	138.15.108.47	20	Sun Nov 3 20:00	53763528	■
143.239.178.160	141.156.216.45	443	Mon Nov 4 17:10	51134400	■
143.239.178.160	141.156.216.45	443	Mon Nov 4 17:00	47997396	■
143.239.178.160	141.156.216.45	443	Mon Nov 4 17:30	36650213	■
143.239.178.160	141.156.216.45	443	Mon Nov 4 16:50	34779078	■

Portmap Scan

Start Pkts	SrcIPAddress	SrcP	DstIPAddress	DstP	P	Fl
0702.10:53:42.50	165.132.86.201	9781	128.146.0.76	111	6	2 1
0702.10:53:42.54	165.132.86.201	9874	128.146.0.7	111	6	2 1
0702.10:53:42.54	165.132.86.201	9982	128.146.0.80	111	6	2 1
0702.10:53:42.54	165.132.86.201	9652	128.146.0.74	111	6	2 1
0702.10:53:42.54	165.132.86.201	9726	128.146.0.75	111	6	2 1
0702.10:53:42.54	165.132.86.201	9855	128.146.0.77	111	6	2 1
0702.10:53:42.58	165.132.86.201	10107	128.146.0.82	111	6	2 1

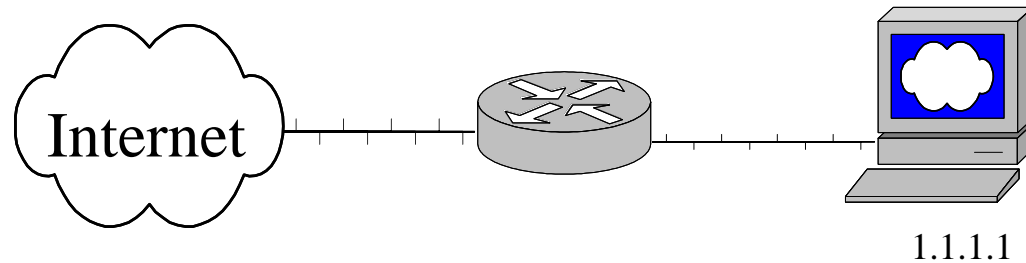
RPC Exploits

Start	SrcIPAddress	SrcP	DstIPAddress	DstP	P	Fl	Pkts
0702.18:56:23.916	130.241.53.23	902	128.146.38.15	32795	6	3	5
0702.18:56:23.924	130.241.53.23	900	128.146.22.19	4138	6	3	5
0702.18:56:23.936	130.241.53.23	893	128.146.9.103	32775	6	3	5
0702.18:56:23.944	130.241.53.23	892	128.146.9.100	32773	6	3	5
0702.18:56:24.196	130.241.53.23	882	128.146.38.187	1027	6	3	5
0702.18:56:24.356	130.241.53.23	901	128.146.39.117	1027	6	3	5

Multihost DOS

Start	SrcIPAddress	SrcP	DstIPAddress	DstP	P	Fl	#P
0703.21:47:11.670	131.142.24.30	514	128.146.97.7	1023	6	3	15
0703.21:47:11.854	131.142.24.30	514	128.146.97.10	1023	6	3	14
0703.21:47:12.198	131.142.24.30	514	128.146.122.244	1023	6	3	14
0703.21:47:12.338	131.142.24.30	514	128.146.132.127	1023	6	3	14
0703.21:47:07.186	130.102.90.105	53982	128.146.97.4	21	6	2	9
0703.21:47:07.470	130.102.90.105	53982	128.146.97.10	21	6	2	12
0703.21:47:07.482	130.102.90.105	53982	128.146.97.7	21	6	2	11

Console Example



- The host 1.1.1.1 is a web server, so web traffic (**TCP-WWW**) is expected.
- This site does not send or receive any UDP based data

Console Example

```
IP packet size distribution (489639251 total packets):
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.000 .992 .000 .003 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .000 .000 .003 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 8913408 bytes
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
----- Flows /Sec /Flow /Pkt /Sec /Flow /Flow
TCP-Telnet 28084 0.0 1 45 0.0 0.1 11.7
TCP-FTP 172835 0.0 1 47 0.0 2.4 13.7
TCP-FTPD 2818 0.0 1 40 0.0 0.2 11.3
TCP-WWW 5551226 1.2 1 53 1.3 0.1 5.0
UDP-NTP 723 0.0 2 40 0.0 9.0 16.8
UDP-TFTP 763 0.0 3 37 0.0 10.2 16.9
UDP-Frag 25 0.0 1 40 0.0 251.4 15.0
UDP-other 169720402 39.5 1 40 46.2 0.6 11.3
ICMP 275131 0.0 10 759 0.6 7.7 14.2
IGMP 36 0.0 1789 1246 0.0 15.2 16.9
IP-other 7 0.0 19 64 0.0 18.9 17.5
Total: 176304332 41.0 2 44 113.9 0.6 11.2
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Hs9/1/0 192.168.2.51 Null 1.1.1.1 11 04A9 0017 614K
Hs9/1/0 192.168.47.72 Null 1.1.1.1 11 05F9 0017 281K
Hs9/1/0 192.168.49.52 Null 1.1.1.1 11 08EA 0017 65K
Hs9/1/0 192.168.32.18 Null 1.1.1.1 11 08EC 0017 1463K
Hs9/1/0 192.168.208.208 Null 1.1.1.1 11 0411 0017 8351K
```

Overview

- Ability to characterize IP data flows
- Enables IP traffic flow analysis without probes
- Efficiently provides the metering base for a key set of applications



Thank you for your time!