



An overview of traffic analysis using NetFlow

Arne Øslebø

UNINETT

Arne.Oslebo@uninett.no



Outline

- What is Netflow?
- Available tools
- Collecting
- Processing
 - Detailed analysis
 - security incidents
 - Long term statistics
 - network trends
 - accounting
- Presentation
 - Stager

- Cisco technology
 - 1996
- IPFIX definition:
 - A set of IP packets passing an observation point in a network during a certain time interval. All packets belonging to a particular flow have a set of common properties.
- Flow Key
 - Each of the properties that are used for defining a flow
- Flow record
 - Measured properties of a flow

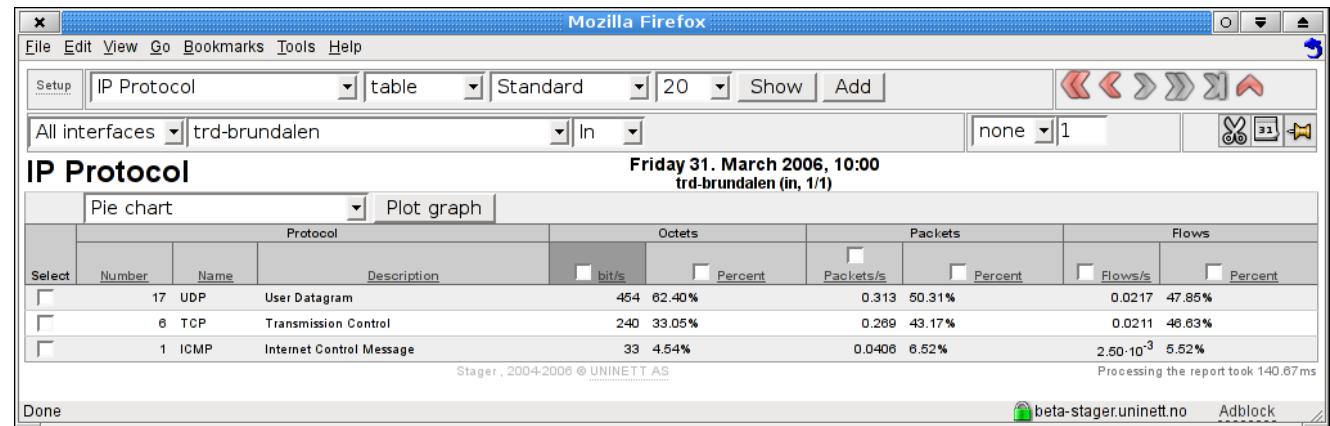
- Flow key:

- Source IP address
- Destination IP address
- Source port
- Destination port
- Layer 3 protocol type
- TOS
- Input interface

- Flow record

- Source and destination IP address
- Next hop router's IP address
- Input and output interface index
- Packets and bytes in the flow
- sysUptime at start and end of flow
- TCP/UDP source and destination port number
- Type of service
- TCP flags
- IP protocol
- Source and destination AS number
- Source and destination address prefix mask bits

- flow-tools
 - Stager
 - FlowViewer
 - FlowScan
 - CUFlow
- nfdump
 - nfsen
 - *Stager*
- flowd
- flamingo
- JKFlow
- <http://www.switch.ch/tf-tant/floma/software.html>



- For example: flow-capture or nfcapd
- Files rotated every n minutes
- Script can be started when file is rotated
- flow-capture supports gzip
 - 2:1 compression ratio
- UNINETT collects:
 - 27 routers, 207 interfaces
 - sampled netflow – 1:100 sampling rate
 - >30GB every day



Process NetFlow – general statistics



<http://www.ist-lobster.org>

- flow-tools
 - flow-cat, flow-filter, flow-nfilter and flow-stat
- nfdump
- src/dst IP, src/dst AS, src/dst port, protocol etc.

```
flow-cat ft-v05.2006-05-12.08* | flow-filter -i1 |
flow-stat -f12 -S2
#
# protocol      flows                octets                packets
#
6                378694              5668763771           8060656
17               541505              352973483            1745931
50               1578                172325976            424695
47               641                 55589150             165236
1                14176              5970023              69637
2                30                 2124                 59
103              28                 1064                 28
41               4                  464                  4
```

- Find traffic to/from specific IP address
- Example is anonymized

```
nfdump -r 2006-05-12.0800.nfdump -o 'fmt:%td
%sa %da %byt' 'ip 166.81.189.132'
```

Duration	Src IP Addr	Dst IP Addr	Bytes
0.952	212.187.175.58	166.81.189.132	552
0.952	166.81.189.132	212.187.175.58	6563
0.180	166.81.189.132	190.88.151.169	468
0.184	190.88.151.169	166.81.189.132	1446
0.524	68.129.203.157	166.81.189.132	536
0.520	166.81.189.132	68.129.203.157	762
1.048	192.127.132.177	166.81.189.132	2569
1.044	166.81.189.132	192.127.132.177	102321



- Who sendt the most traffic to this IP address?

```
nfdump -r 2006-05-12.0800.nfdump -n5 -ssrcip/bytes 'dst ip 166.81.189.132'
```

Top 5 Src IP Addr ordered by bytes:

Duration	Proto	Src IP Addr	Flows	Packets	Bytes
910.083	any	190.88.151.169	152	976	180764
904.953	any	166.81.191.137	14	655	117439
902.915	any	139.65.84.134	172	1413	106792
848.974	any	192.127.132.177	35	1253	92450
876.597	any	166.81.98.117	36	364	56876



Stager

- Long term statistics
- Easy to use web frontend
 - Text based reports and graphs
- Support for different types of network statistics
 - Netflow
 - *SNMP*
 - *Mping*
- Easy to add new reports
 - Templates and plugins
- Access control
 - Observation points and reports

<http://software.uninett.no>



Overview reports



http://www.ist-lobster.org

Mozilla Firefox

File Edit View Go Bookmarks Tools Help

Setup Destination AS overview Octets-percent 20 Show Add hour...

All interfaces vpn-gw.uio.no In none 1

Destination AS

Monday 20. March 2006
All observation points (in)

Pie chart Plot graph

Select	Observation Point	Octets - percent							
		<input type="checkbox"/> NORUnet	<input type="checkbox"/> 0	<input type="checkbox"/> NTNU	<input type="checkbox"/> Universitetet i Bergen	<input type="checkbox"/> Universitetet i Oslo	<input type="checkbox"/> Universitetet i Tromsø	<input type="checkbox"/> Telenor Internet Access, Telenor Networks AS, Norway, (former Telenor Business Solutions, Nextra, Telenor Nextel)	<input type="checkbox"/> NEXTGENTEL Autonomous System, NextGenTel AS, Norway
<input type="checkbox"/>	bergen-haukeland	97.83%	0.17%	0.00%	0.00%	0.00%	0.00%	0.00%	0.00%
<input type="checkbox"/>	teknobyen-kristiansund	88.30%	0.85%	0.00%	0.00%	1.33%	0.00%	1.53%	0.17%
<input type="checkbox"/>	oslo-lillehammer	84.00%	0.37%	0.02%	0.00%	0.13%	0.00%	2.01%	1.34%
<input type="checkbox"/>	oslo-elverum	81.47%	0.80%	0.01%	0.01%	0.20%	0.00%	2.12%	2.36%
<input type="checkbox"/>	teknobyen-narvik	81.16%	0.76%	0.85%	0.00%	0.03%	0.00%	1.82%	2.66%
<input type="checkbox"/>	stolavsp1-stolav32	81.09%	4.65%	0.00%	0.00%	0.01%	0.00%	1.63%	1.43%
<input type="checkbox"/>	bo-notodden	80.70%	7.63%	0.14%	0.00%	0.08%	0.01%	2.66%	1.10%
<input type="checkbox"/>	alesund-volda	80.31%	0.69%	1.73%	0.02%	0.24%	0.01%	2.10%	1.75%
<input type="checkbox"/>	oslo-bo	80.14%	0.34%	0.21%	0.01%	0.12%	0.00%	3.20%	1.60%
<input type="checkbox"/>	trd.trd-ircnett	79.83%	1.24%	0.16%	0.95%	1.28%	0.00%	3.09%	1.29%
<input type="checkbox"/>	tromso-gw.tromsoS-gw	79.01%	3.20%	0.08%	0.02%	0.28%	0.22%	4.08%	1.85%
<input type="checkbox"/>	oslo-gw1.oslo-gw2	78.72%	1.18%	0.04%	0.00%	0.51%	0.00%	2.86%	3.13%
<input type="checkbox"/>	trd-tromso	78.65%	0.97%	0.43%	0.05%	0.18%	0.00%	2.54%	2.10%
<input type="checkbox"/>	alesund-molde	78.47%	1.85%	1.52%	0.02%	0.25%	0.00%	1.93%	2.72%
<input type="checkbox"/>	tromso-uito	78.43%	1.45%	0.44%	0.06%	0.16%	0.00%	2.55%	2.02%
<input type="checkbox"/>	trd-steinkjer	78.22%	1.68%	0.33%	0.00%	0.34%	0.05%	3.30%	2.42%
<input type="checkbox"/>	oslo-kjeller	77.83%	1.33%	0.78%	0.15%	0.78%	0.01%	2.86%	2.77%
<input type="checkbox"/>	oslo-bergen	77.73%	1.74%	0.00%	0.00%	0.62%	0.00%	2.78%	3.52%
<input type="checkbox"/>	oslo-trd	76.89%	2.00%	0.00%	0.00%	0.70%	0.00%	4.19%	0.71%
<input type="checkbox"/>	bergen-bergen3	75.93%	1.79%	0.00%	2.91%	0.53%	0.00%	2.52%	2.29%

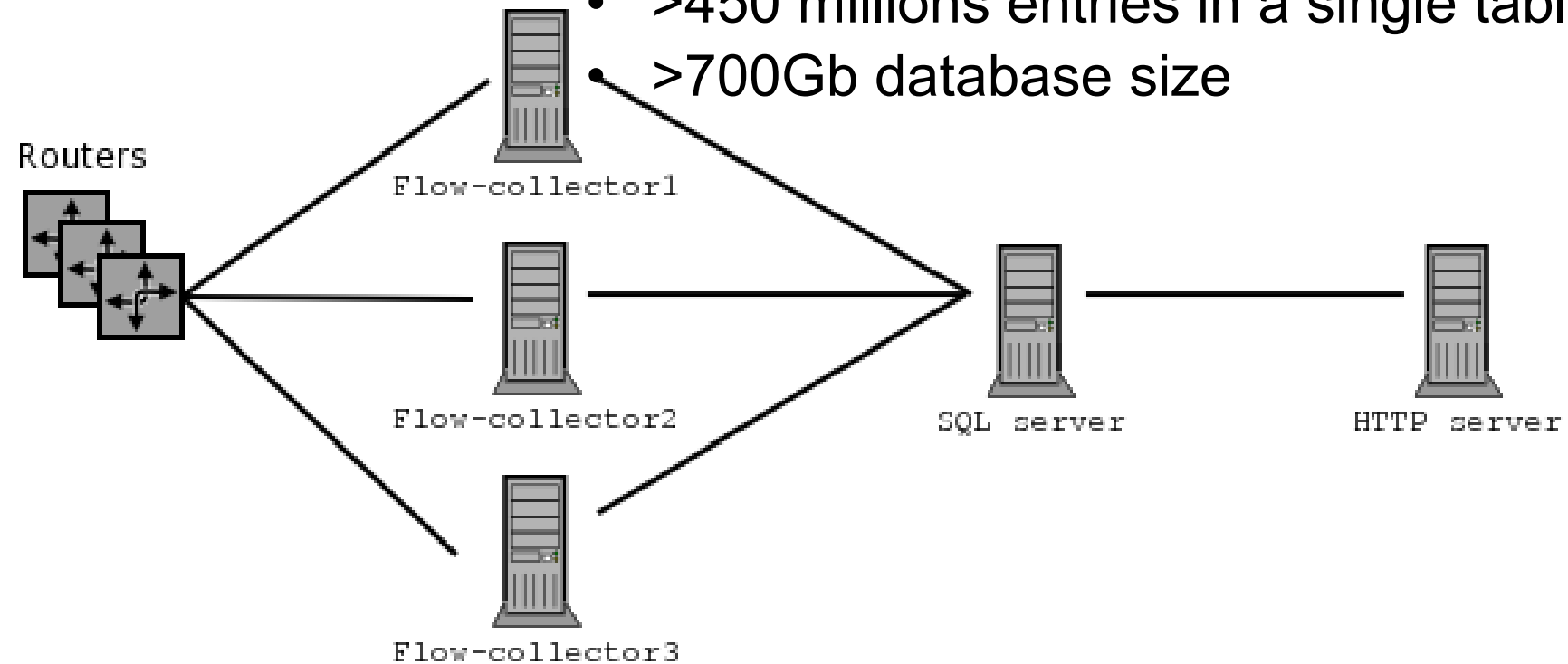
Stager, 2004-2006 © UNINETT AS

Processing the report took 1841.32ms

Done beta-stager.uninett.no Adblock

- Handle database problems
 - Store raw data to disk
 - Generate reports later when problems are resolved
- Avoid multiple instances of the same backend
 - Wait for previous instances that are still processing the raw data
 - Detect dead locks and memory starvations

- 27 routers
- 207 interfaces
- >30Gb of raw Netflow data every day
- 400.000 new entries in the db every hour
- >450 millions entries in a single table
- >700Gb database size





Performance



<http://www.ist-lobster.org>

Data from January 17 between 08:00-09:00

	PC1	PC2	PC3	Total
Netflow size	537MB	161MB	399MB	1097MB
Sequentially	9min 17s	3min 8s	5min 51s	18min 16s
No insert in DB	7min 11s	1min 48s	4min 52s	13min 51s
Simultaneously	9min 21s	3min 7s	5min 56s	18min 24s
# of new DB entries	164702	69549	184706	418957
# of entries/second	295.69	369.94	526.23	382.26

Report

Time

of entries in table

IP Protocol overview report	614ms	17,228,300
IP Protocol overview report (previous timeperiod)	524ms	
IP Protocol detailed report	509ms	
Top src port overview	1221ms	454,034,919
Top src port overview (previous timeperiod)	717ms	
Top src port detailed	498ms	
Top src port plot (one day, two ports and obs. points)	1590ms	



Some links

- <http://www.switch.ch/tf-tant/floma/software.html>
- <http://software.uninett.no/>
- <http://www.splintered.net/sw/flow-tools/>
- <http://nfdump.sourceforge.net/>
- <http://www.ietf.org/html.charters/ipfix-charter.html>
- http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html