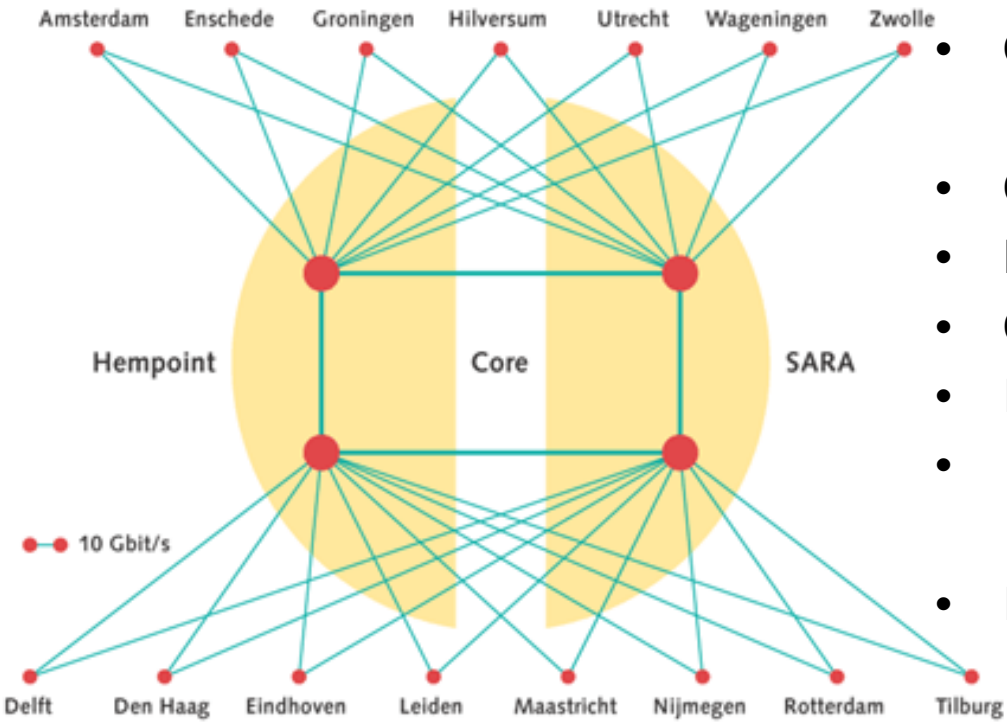
NERD:
Network Emergency Responder & Detector

Wim.Biemolt@surfnet.nl

2nd FloCon, Pittsburgh, September, 2005.

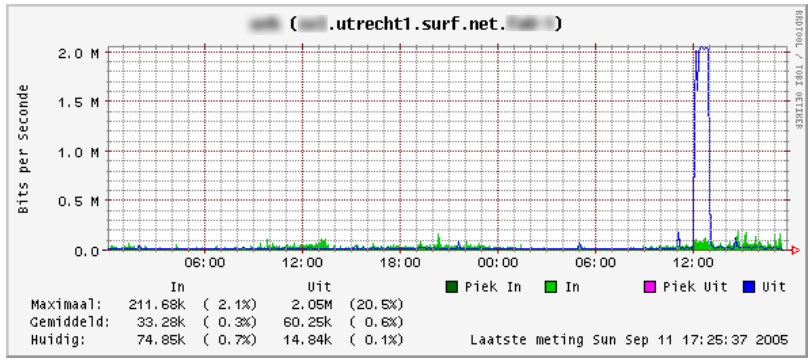
SURFnet5 network

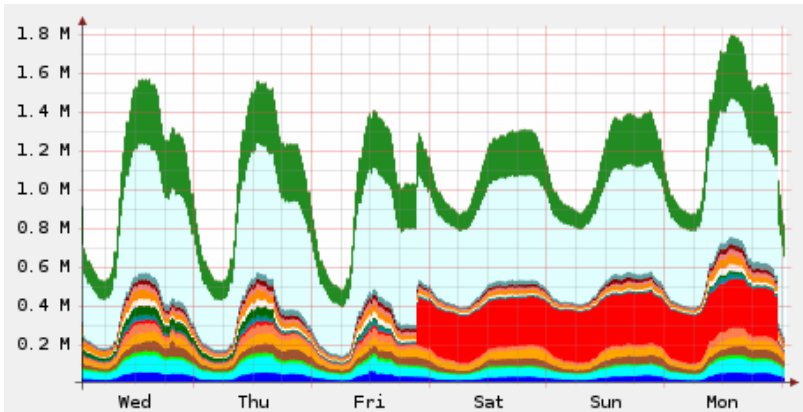


- Operational
  - Since September 2001
- Cisco 12416 routers
- Backbone: 10Gbps
- Connections: 1Gbps
- Dual stack (6PE)
- Incident detection
  - SURFnet & TNO: 2002
- Decommissioning
  - End of December 2005

Incident response tools

- SURFstat
  - mrtg/rrdtool
- Research
  - syslog
  - Netflow
    - promising at the required speeds (>10 Gbps)
    - sampled (`ip flow-sampling-mode packet-interval 100`)
  - Full data analysis requires high-end equipment
- Prototype
  - cflowd (caida)
    - no longer supported
  - gnuplot, mysql, php
  - Not open-source





Prototype

Network **E**mergency **R**esponder & **D**etector

Show all alarms from 0 days ago, up to 0 days ago. Show

The alarms between **2005-09-11** and **2005-09-12**

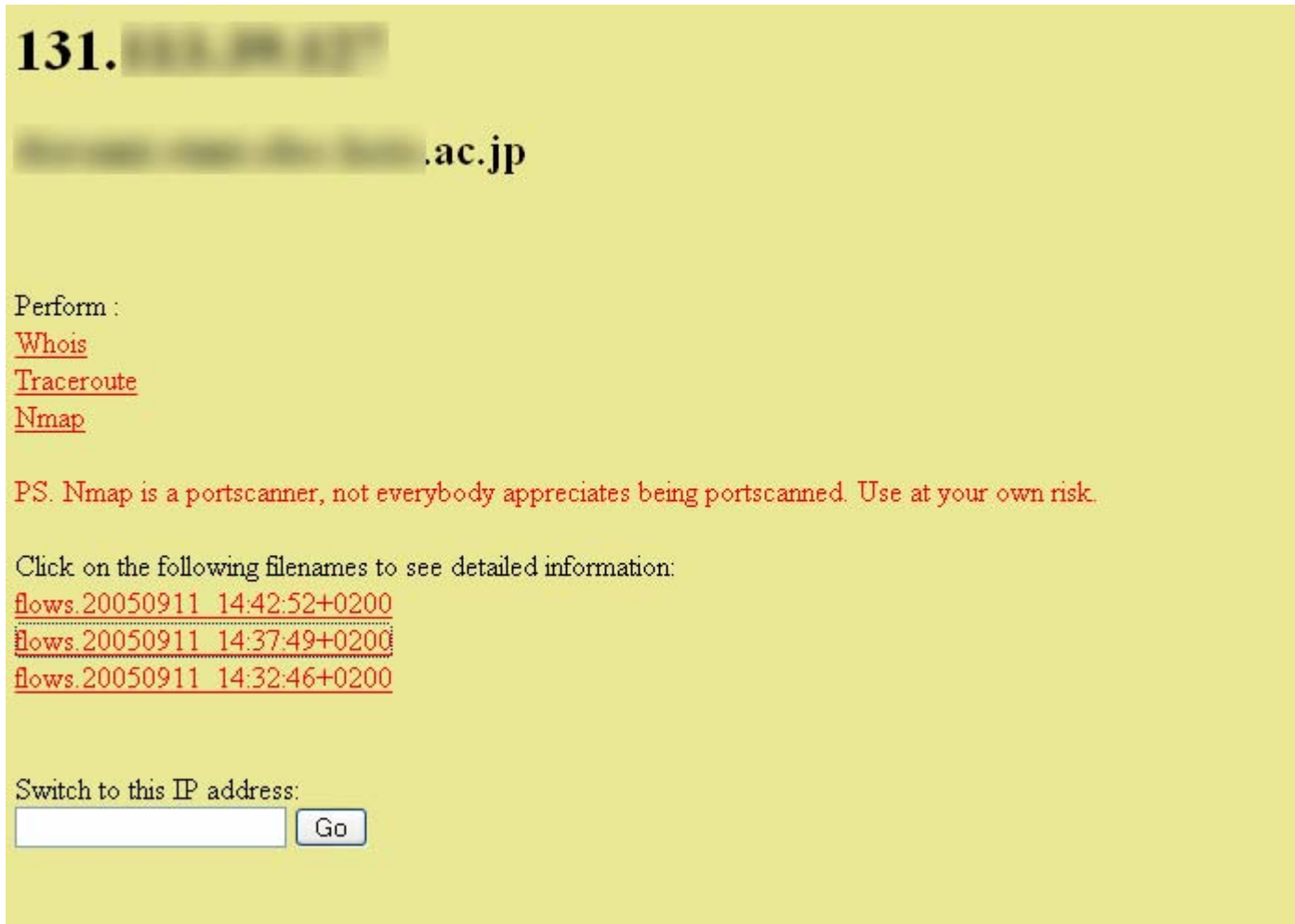
The query took approximately 0.019 seconds.

NETFLOW
- Alarms
- ddos-rs v2
- spammerts
- Configuration
- Overall summary
- Analyse
- List

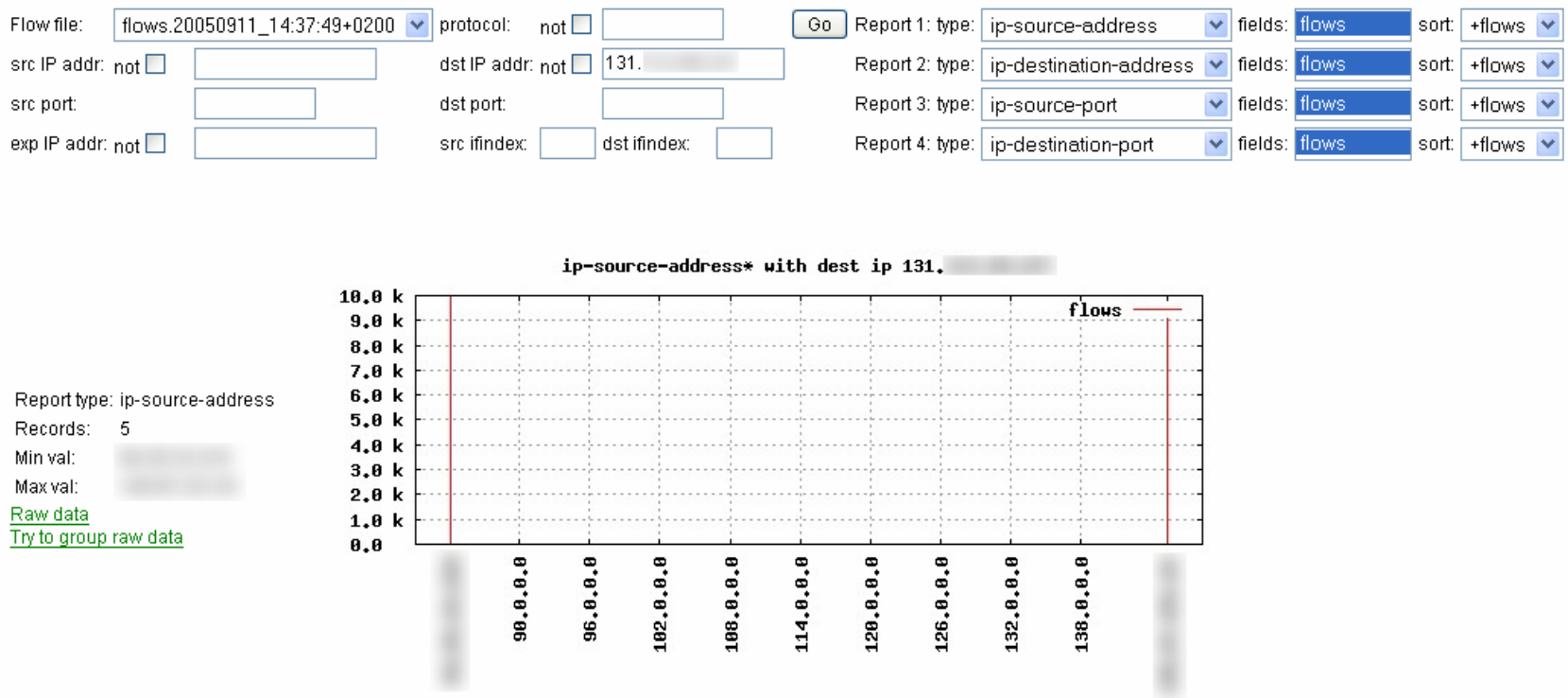
SYSLOG
- Alarms
- TOP 10
- Rules
- Messages
- PoP-map
- Search

Destination IP address	Hostname	Flows per 5 minutes	Average packets per flow	Average bytes per flow	Average destination port	Starttime	Stoptime	Continuing
140.	com	6542	1	157	47467	2005-09-11 14:15:07	2005-09-11 14:39:06	1
131.	.ac.jp	29700	1	74	39930	2005-09-11 14:33:05	2005-09-11 14:39:06	1
216.	-	5555	1	142	47329	2005-09-11 14:39:06	2005-09-11 14:39:06	1
194.	co.uk	15955	1	157	47286	2005-09-11 11:03:03	2005-09-11 11:27:03	0
216.	-	4012	1	149	47560	2005-09-11 09:45:06	2005-09-11 09:45:06	0

Alarm

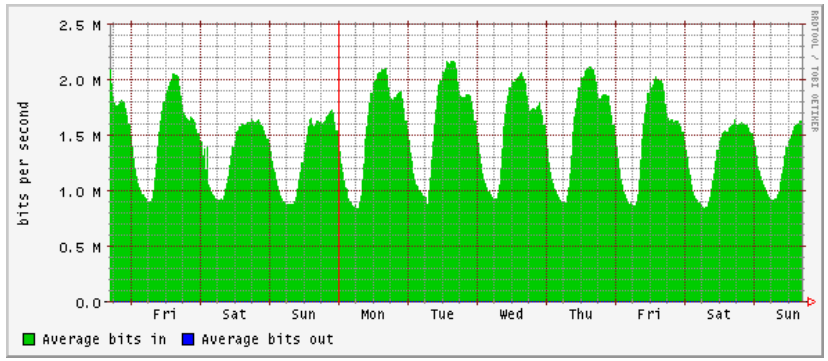

131.
.ac.jp
Perform :
Whois
Traceroute
Nmap
PS. Nmap is a portscanner, not everybody appreciates being portscanned. Use at your own risk.
Click on the following filenames to see detailed information:
flows.20050911_14:42:52+0200
flows.20050911_14:37:49+0200
flows.20050911_14:32:46+0200
Switch to this IP address:
Go

Analyse

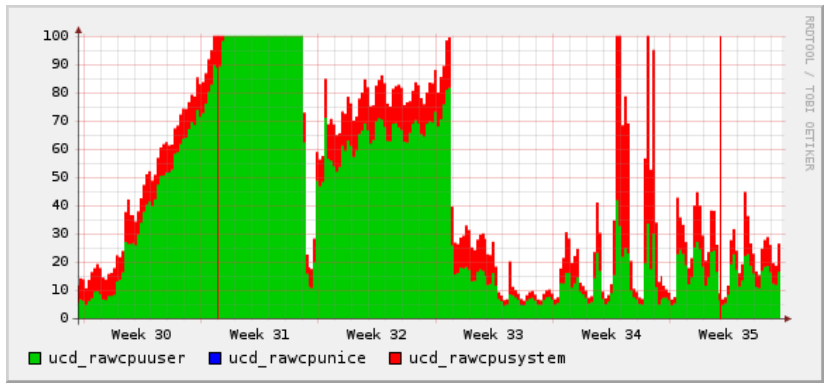

Flow file: flows.20050911_14:37:49+0200
protocol: not
Go
Report 1: type: ip-source-address fields: flows sort: +flows
src IP addr: not
dst IP addr: not 131.
Report 2: type: ip-destination-address fields: flows sort: +flows
src port:
dst port:
Report 3: type: ip-source-port fields: flows sort: +flows
exp IP addr: not
src ifindex:
dst ifindex:
Report 4: type: ip-destination-port fields: flows sort: +flows
ip-source-address* with dest ip 131.
flows
10.0 k
9.0 k
8.0 k
7.0 k
6.0 k
5.0 k
4.0 k
3.0 k
2.0 k
1.0 k
0.0
90.0.0.0
96.0.0.0
102.0.0.0
108.0.0.0
114.0.0.0
120.0.0.0
126.0.0.0
132.0.0.0
138.0.0.0
Report type: ip-source-address
Records: 5
Min val:
Max val:
Raw data
Try to group raw data

Hardware

- Dell PowerEdge 1650
  - 04-2002, RedHat 7
  - 1x 1.4GHz, 1GB, 3x 36GB
- Dell PowerEdge 2650
  - 12-2003, FreeBSD 4.11
  - 2x 3GHz, 4GB, 5x 146GB
- Dell PowerEdge 2850
  - 10-2004, FreeBSD 5.4
  - 2x 3.4GHz, 6GB, 6x 146GB
- Dell PowerEdge 2850
  - 06-2005, FreeBSD 6.0
  - 2x 3.6GHz, 4GB, 6x 300GB
- SunFire V240
  - 12-2004, Solaris 10
  - 2x 1.5GHz, 4GB, 4x 146GB



http://www.switch.ch/tf-tant/floma/sw/samplicator/

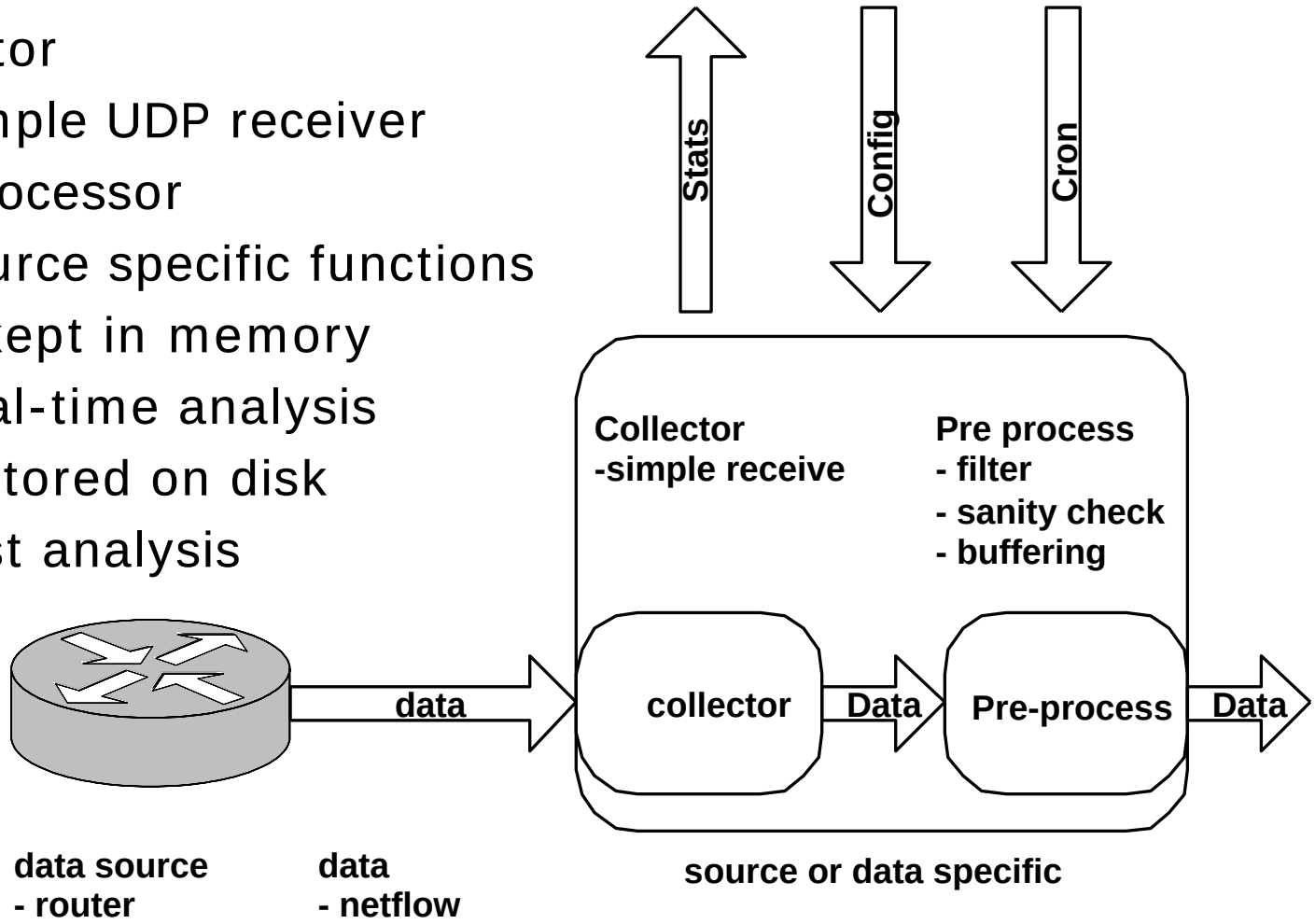


Some specs of the new NERD

- nerdd, analysis
  - boost libraries, MySQL database, php, plplot
- Netflow versions
  - V5 (tested)
  - V9 (IPFIX)
- Platforms tested
  - FreeBSD
  - Linux
- Apache Open Source Licence v2.0

Software Architecture

- Collector
  - Simple UDP receiver
- Pre-processor
  - Source specific functions
- Data kept in memory
  - Real-time analysis
- Data stored on disk
  - Post analysis



Real-time and post analysis

- Real time analysis
  - Rules can be used for ‘real-time’ analysis
    - A rule is a combination of filters, clusters and a threshold for some metric (e.g. number of flows)
  - Example of a rule
    - Filter “port=445”, cluster “dst IP”, threshold=1000 flows/min
  - Results in an alarm if a host receives more then 1000 flows/min on TCP port 445
  - Output formatting: alarm in database
  - Every x minutes the rules (1…n) are executed
- Post analysis
  - Executed at user request
  - Rules without threshold
  - Output formatting: flow-tools like text file, graphical output

Functionality – Filters & Clusters

- Sample of Netflow data

src	prt	dst	prt
10.0.0.1	2000	10.0.0.2	23
10.0.0.3	1000	10.0.0.2	22
10.0.0.6	2000	10.0.0.2	22
10.0.0.1	1000	10.0.0.3	23
10.0.0.1	1000	10.0.0.3	23

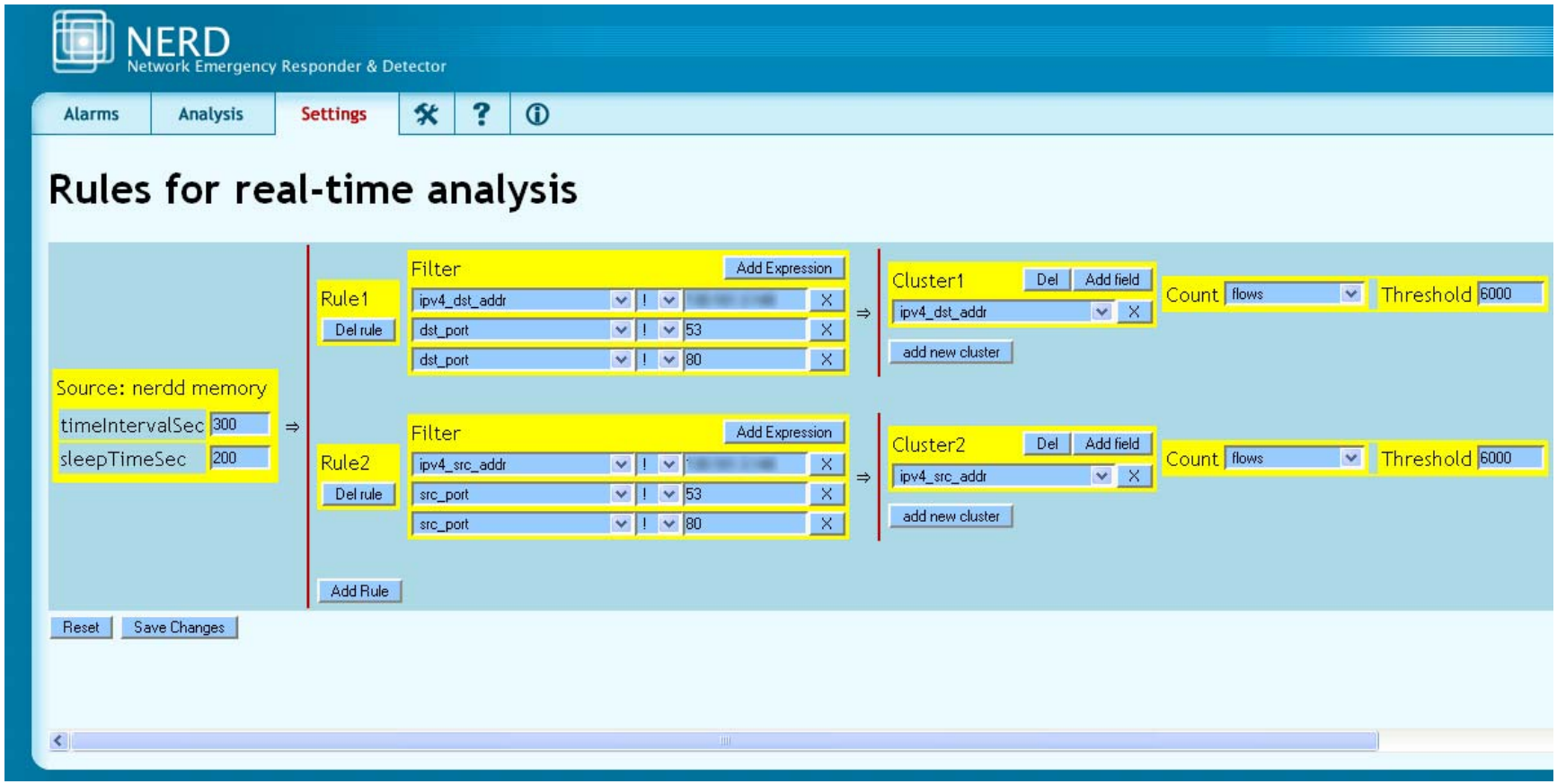
- Example: filter “src port=2000”

src	prt	dst	prt
10.0.0.1	2000	10.0.0.2	23
10.0.0.6	2000	10.0.0.2	22

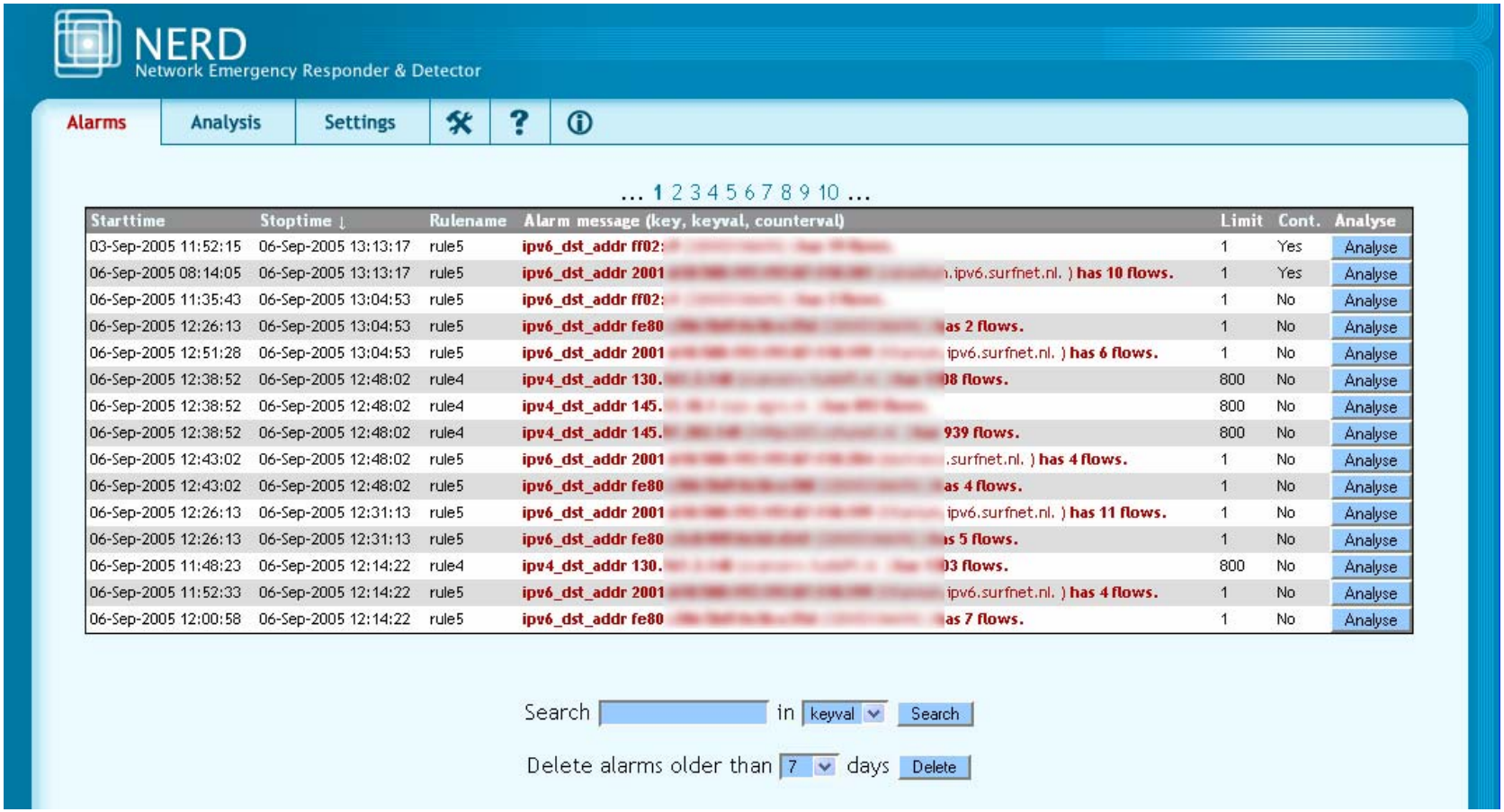
- Example: filter, cluster “dst port” & count flows

prt	# of flows
22	1
23	1

Real-time analysis - configuration



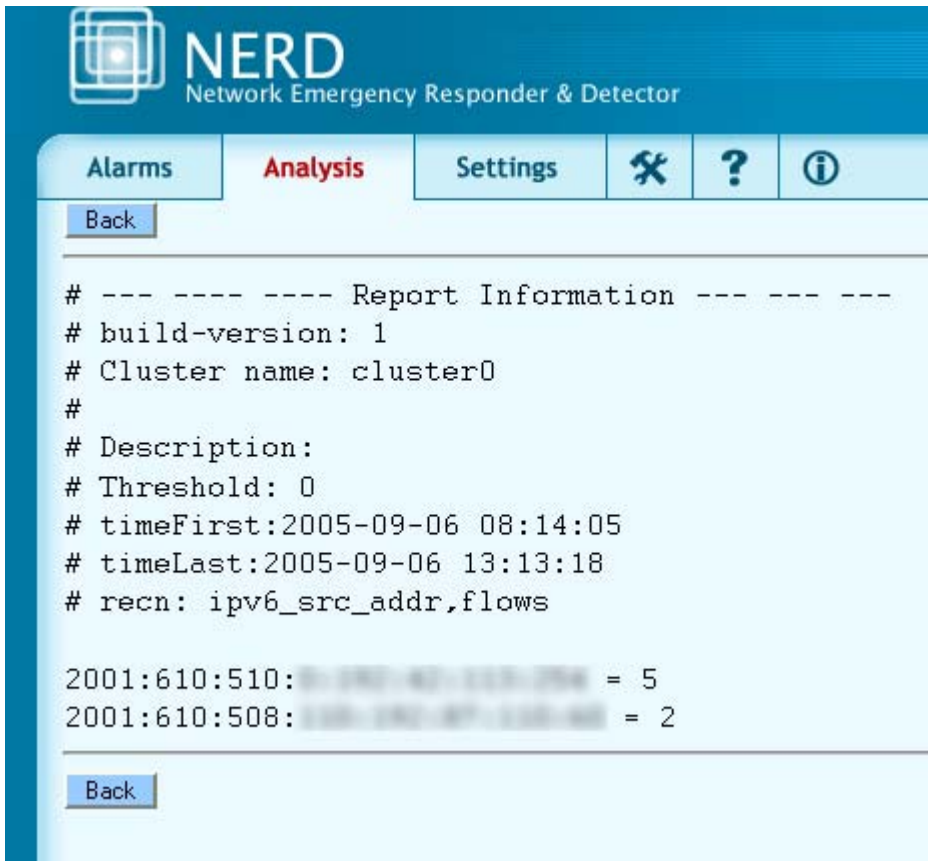
Alarms

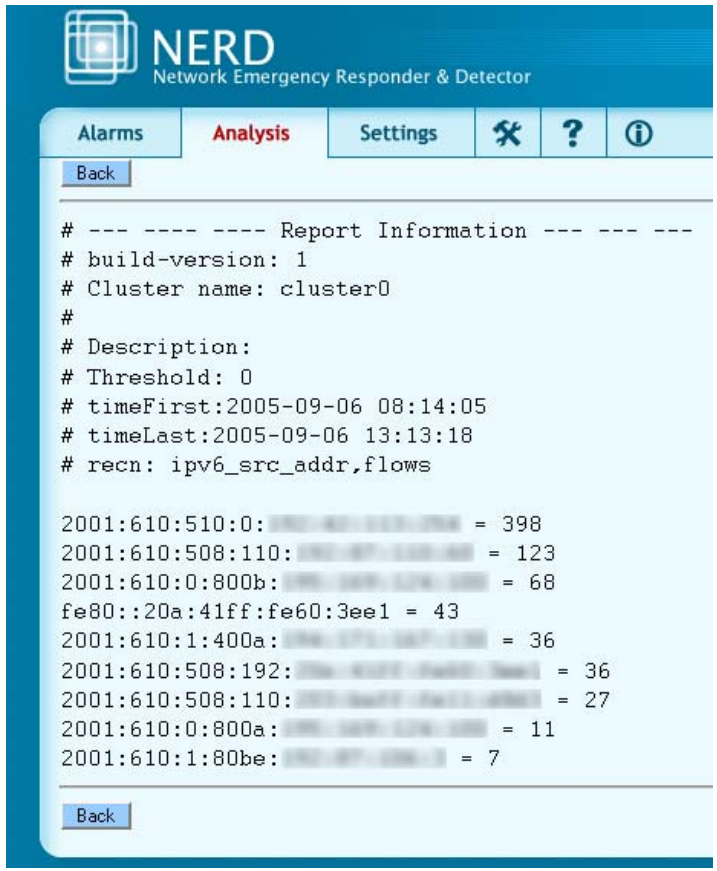


Starttime	Stoptime ↓	Rulename	Alarm message (key, keyval, counterval)	Limit	Cont.	Analyse
03-Sep-2005 11:52:15	06-Sep-2005 13:13:17	rule5	ipv6_dst_addr ff02:	1	Yes	Analyse
06-Sep-2005 08:14:05	06-Sep-2005 13:13:17	rule5	ipv6_dst_addr 2001 .ipv6.surfnet.nl.) has 10 flows.	1	Yes	Analyse
06-Sep-2005 11:35:43	06-Sep-2005 13:04:53	rule5	ipv6_dst_addr ff02:	1	No	Analyse
06-Sep-2005 12:26:13	06-Sep-2005 13:04:53	rule5	ipv6_dst_addr fe80 as 2 flows.	1	No	Analyse
06-Sep-2005 12:51:28	06-Sep-2005 13:04:53	rule5	ipv6_dst_addr 2001 ipv6.surfnet.nl.) has 6 flows.	1	No	Analyse
06-Sep-2005 12:38:52	06-Sep-2005 12:48:02	rule4	ipv4_dst_addr 130. 08 flows.	800	No	Analyse
06-Sep-2005 12:38:52	06-Sep-2005 12:48:02	rule4	ipv4_dst_addr 145.	800	No	Analyse
06-Sep-2005 12:38:52	06-Sep-2005 12:48:02	rule4	ipv4_dst_addr 145. 939 flows.	800	No	Analyse
06-Sep-2005 12:43:02	06-Sep-2005 12:48:02	rule5	ipv6_dst_addr 2001 .surfnet.nl.) has 4 flows.	1	No	Analyse
06-Sep-2005 12:43:02	06-Sep-2005 12:48:02	rule5	ipv6_dst_addr fe80 as 4 flows.	1	No	Analyse
06-Sep-2005 12:26:13	06-Sep-2005 12:31:13	rule5	ipv6_dst_addr 2001 ipv6.surfnet.nl.) has 11 flows.	1	No	Analyse
06-Sep-2005 12:26:13	06-Sep-2005 12:31:13	rule5	ipv6_dst_addr fe80 s 5 flows.	1	No	Analyse
06-Sep-2005 11:48:23	06-Sep-2005 12:14:22	rule4	ipv4_dst_addr 130. 03 flows.	800	No	Analyse
06-Sep-2005 11:52:33	06-Sep-2005 12:14:22	rule5	ipv6_dst_addr 2001 ipv6.surfnet.nl.) has 4 flows.	1	No	Analyse
06-Sep-2005 12:00:58	06-Sep-2005 12:14:22	rule5	ipv6_dst_addr fe80 as 7 flows.	1	No	Analyse

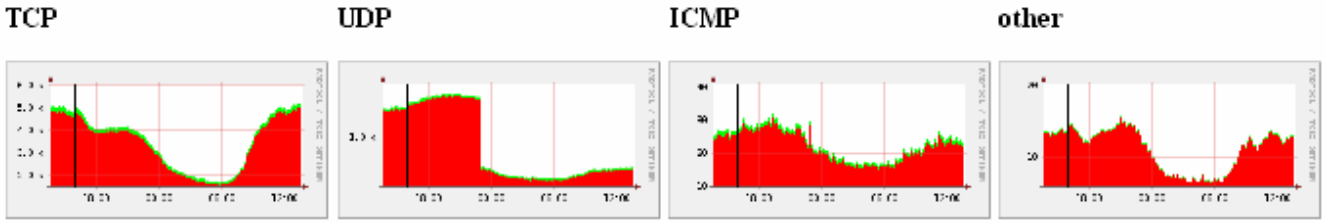
Analysis – IPv4

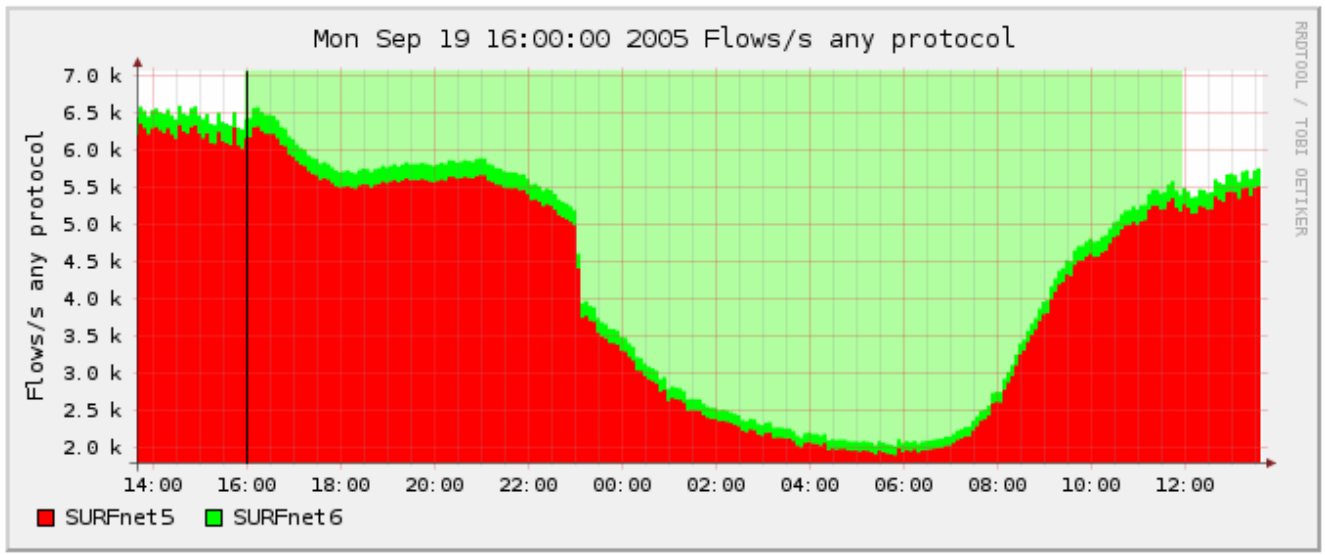
Analysis – IPv6





SURFnet6





Statistics timeslot Sep 19 2005 - 16:00 - Sep 20 2005 - 12:00

Source:	Flows:	Packets:	tcp:	udp:	icmp:	other:	Traffic:	tcp:	udp:	icmp:	other:
SURFnet5	3.8 K/s	19.5 K/s	14.5 K/s	4.6 K/s	29.9 /s	337.4 /s	120.0 Mb/s	89.6 Mb/s	28.8 Mb/s	27.5 Kb/s	1.6 Mb/s
SURFnet6	170.4 /s	663.9 /s	573.6 /s	84.8 /s	2.4 /s	3.1 /s	3.4 Mb/s	3.2 Mb/s	249.4 Kb/s	1.5 Kb/s	22.9 Kb/s

All None

Display: Sum Rate

Current Research and Development

- Geant2 JRA2
  - NERD is one of the monitoring toolsets
- LOBSTER project
  - Integration
- Student
  - Analysis and visualisation of worm behaviour
- Ph.D. from Vrije Universiteit (VU)
  - Interaction of Netflow and Full Packet inspection
- From application to framework
  - Other data sources, combining different data
  - Other data output

Questions

- More information and download of NERD
  - www.nerdd.org