

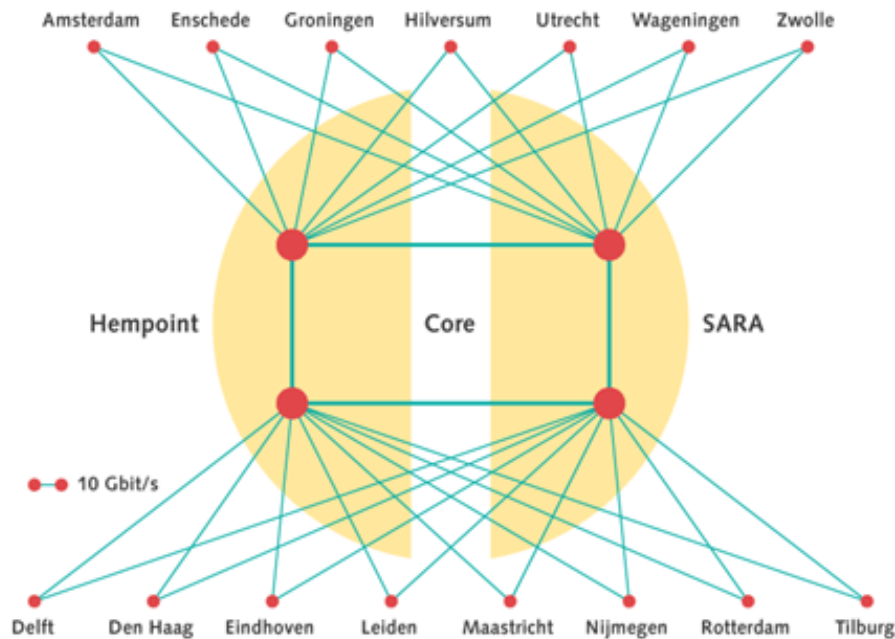


NERD: Network Emergency Responder & Detector

Wim.Biemolt@surfnet.nl

16th TF-CSIRT, Lisboa, September, 2005.

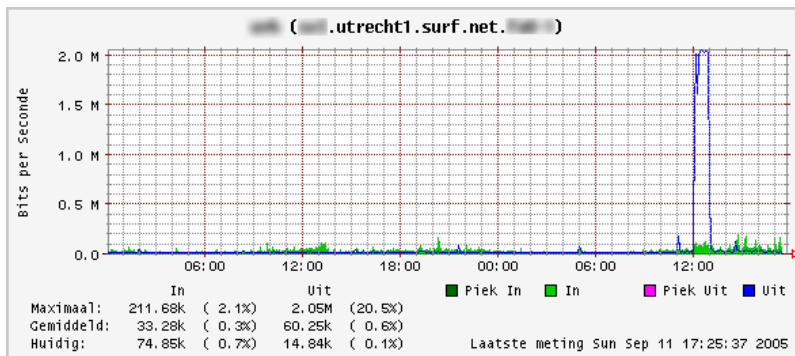
SURFnet5 network



- 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
 - 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

SURFnet



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

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

The query took approximately 0.019 seconds.

NETFLOW

[Alarms](#)

[ddos-rs v2](#)

[spammeris](#)

[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
140.193.122.1	hulst-hulst.computer.com	6542	1	157	47467	2005-09-11 14:15:07	2005-09-11 14:39:06	1
131.111.29.102	hawaii.ac.jp	29700	1	74	39930	2005-09-11 14:33:05	2005-09-11 14:39:06	1
216.19.108.10	-	5555	1	142	47329	2005-09-11 14:39:06	2005-09-11 14:39:06	1
194.193.122.1	co.uk	15955	1	157	47286	2005-09-11 11:03:03	2005-09-11 11:27:03	0
216.19.108.10	-	4012	1	149	47560	2005-09-11 09:45:06	2005-09-11 09:45:06	0

Alarm

131. [REDACTED]

[REDACTED].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:

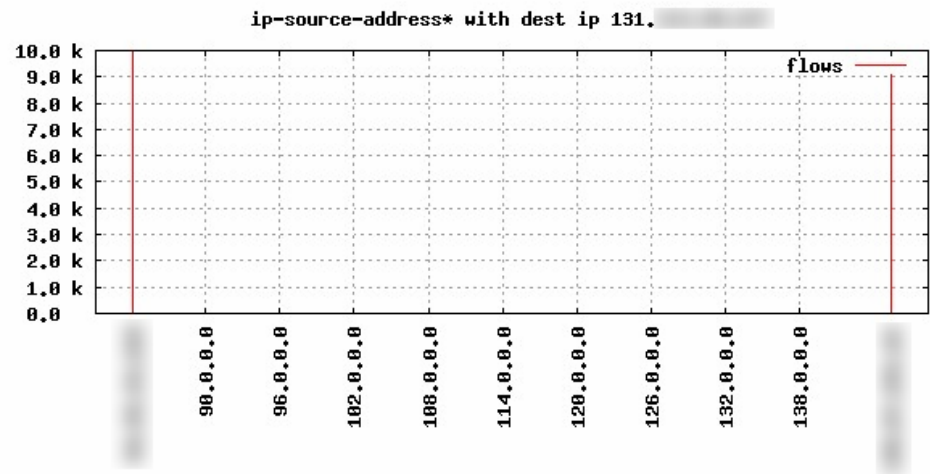
Go

Analyse

Flow file: protocol: not
src IP addr: not dst IP addr: not
src port: dst port:
exp IP addr: not src ifindex: dst ifindex:

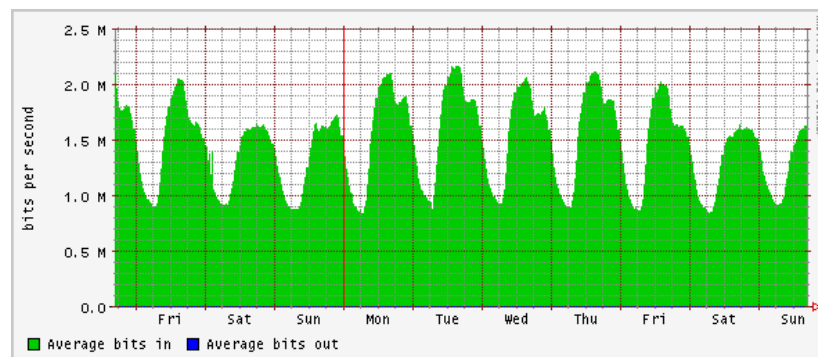
Report 1: type: fields: sort:
Report 2: type: fields: sort:
Report 3: type: fields: sort:
Report 4: type: fields: sort:

Report type: ip-source-address
Records: 5
Min val:
Max val:
[Raw data](#)
[Try to group raw data](#)

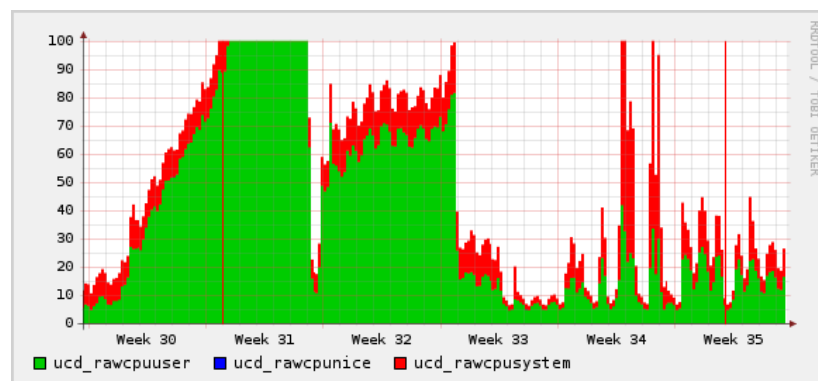


Hardware

- 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



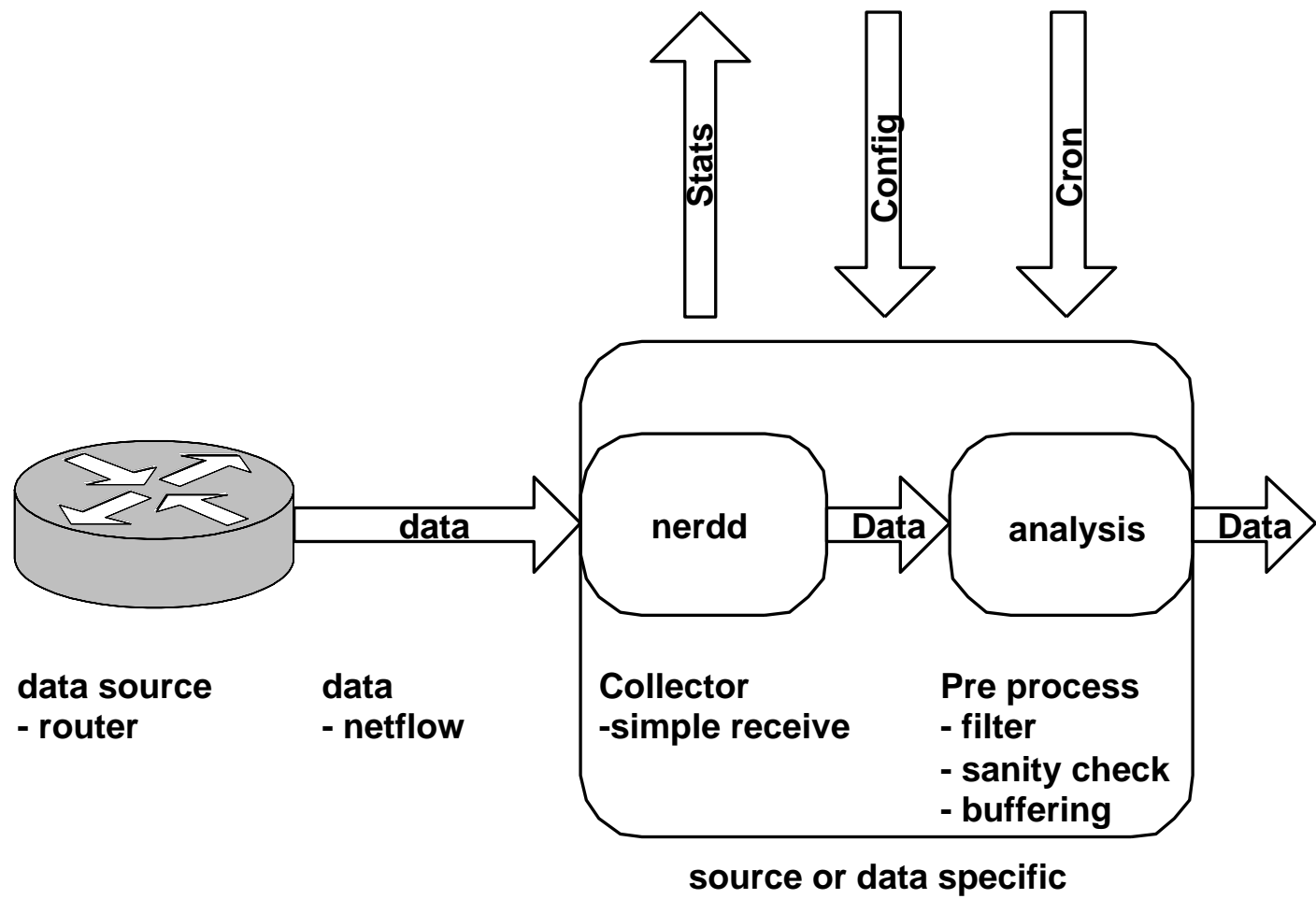
<http://www.switch.ch/tf-tant/floma/sw/samplicator/>



Some specs of NERD

- nerdd, analysis
 - boost libraries, MySQL database, php, plplot
- Netflow versions
 - V5 (tested)
 - V1
 - V9 (IPFIX)
- Platforms tested
 - FreeBSD
 - Linux
- Apache Open Source Licence v2.0

Software Architecture



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
 - Cluster "dst IP", filter "port=445", threshold=1000 flows/ min
 - Results in an alarm if a host receives more than 1000 flows per minute on TCP port 445

Functionality – Clusters & Filters

- Sample of Netflow data

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

- Example: cluster “dst port” & count flows

prt	# of flows
22	5

- Example: filter “src port=2000”

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

Real-time analysis - configuration

The screenshot shows the NERD (Network Emergency Responder & Detector) configuration interface. The top navigation bar includes 'Alarms', 'Analysis', and 'Settings' (which is active). Below the navigation bar, the title 'Rules for real-time analysis' is displayed. The main configuration area is divided into several sections:

- Source:** nerdd memory
- timeIntervalSec:** 300
- sleepTimeSec:** 200

Two rules are configured:

- Rule1:** Filter includes 'ipv4_dst_addr', 'dst_port' (53), and 'dst_port' (80). It is linked to 'Cluster1'.
- Rule2:** Filter includes 'ipv4_src_addr', 'src_port' (53), and 'src_port' (80). It is linked to 'Cluster2'.

Each cluster (Cluster1 and Cluster2) has a 'Count' set to 'flows' and a 'Threshold' set to 6000. There are 'Del' and 'Add field' buttons for each cluster, and an 'add new cluster' button. At the bottom, there are 'Reset' and 'Save Changes' buttons.

Alarms

NERD
Network Emergency Responder & Detector

Alarms
Analysis
Settings
✖
?
i

... 1 2 3 4 5 6 7 8 9 10 ...

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: ... 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: ... 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: ... 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: ... has 11 flows.	1	No	Analyse
06-Sep-2005 12:26:13	06-Sep-2005 12:31:13	rule5	ipv6_dst_addr fe80: ... as 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: ... 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

Search in keyval Search

Delete alarms older than 7 days Delete

Analysis – IPv4

The screenshot displays a network analysis tool interface. At the top, a graph titled "cluster3" shows the distribution of flows across destination ports. The y-axis is labeled "flows" and ranges from 0.0 to 1.0. The x-axis is labeled "dst_port" and ranges from 36000 to 60000. The graph shows several vertical red lines representing individual flows, with a significant concentration between 36000 and 40000. The period of the data is "2005-09-06 12:38:52 - 2005-09-06 12:48:03".

Below the graph is a "Debug Info" button. The main interface is divided into several sections:

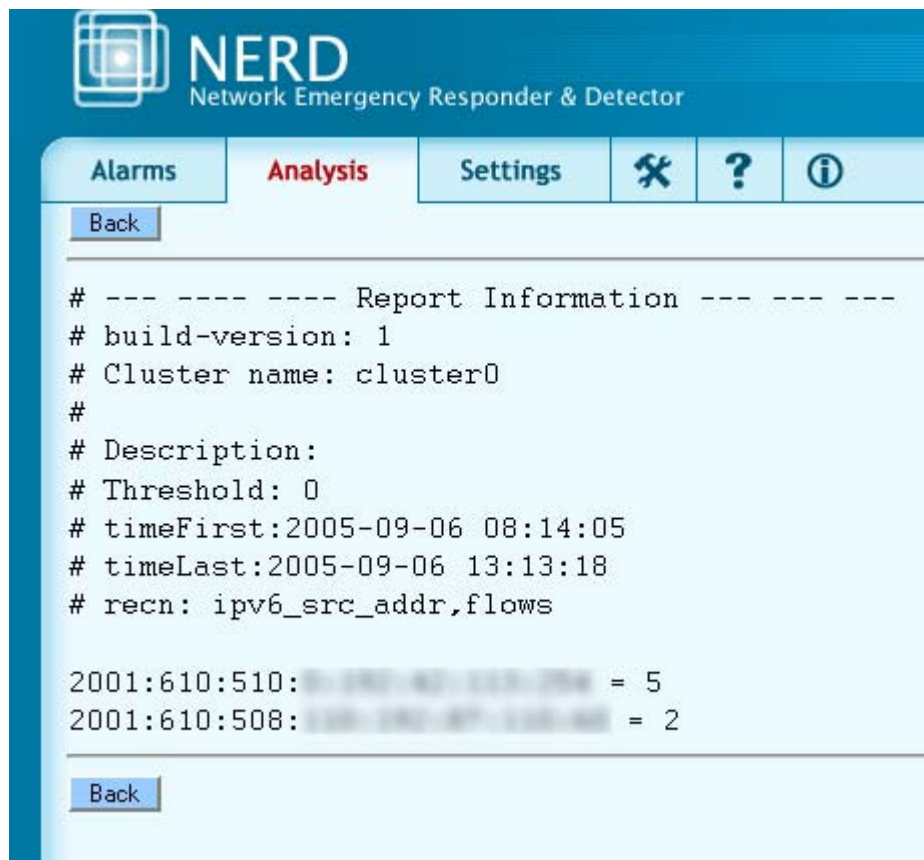
- NERD-flow archive:** A dropdown menu set to "sampled (100)".
- Flow Statistics:**

First flow:	04-Sep-2005 23:27:23
Last flow:	11-Sep-2005 15:54:41
# flows:	55117147
Avg flow/s:	95
- Filter:** A section for defining filters. It includes a dropdown for "ipv4_dst_addr" and a comparison operator set to "=". Below this, two time-based filters are defined:




timestamp_arrival	>	06-Sep-2005 12:38
timestamp_arrival	<	06-Sep-2005 12:48
- Cluster Configuration:** A list of clusters with their respective fields and control buttons:
 - Cluster0: Del, Add field, ipv4_src_addr
 - Cluster1: Del, Add field, ipv4_dst_addr
 - Cluster2: Del, Add field, src_port
 - Cluster3: Del, Add field, dst_portAn "add new cluster" button is located at the bottom of this section.

At the bottom of the interface are "Reset" and "Analyse" buttons.

Analysis – IPv6



NERD
Network Emergency Responder & Detector

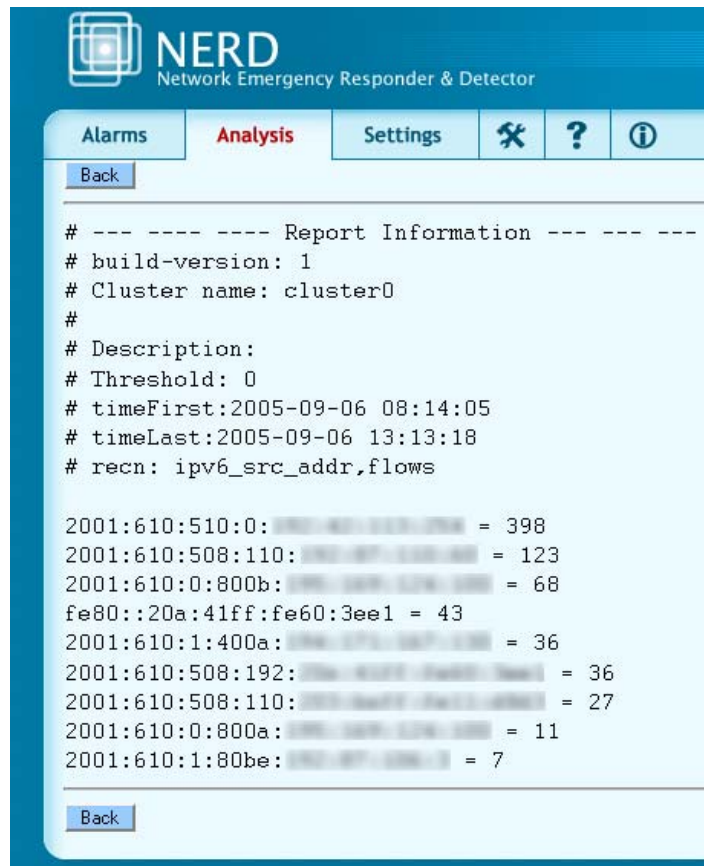
Alarms **Analysis** Settings   

Back




```
# --- ---- Report Information --- ----
# build-version: 1
# Cluster name: cluster0
#
# Description:
# Threshold: 0
# timeFirst:2005-09-06 08:14:05
# timeLast:2005-09-06 13:13:18
# recn: ipv6_src_addr,flows

2001:610:510: [redacted] = 5
2001:610:508: [redacted] = 2
```

Back



NERD
Network Emergency Responder & Detector

Alarms **Analysis** Settings   

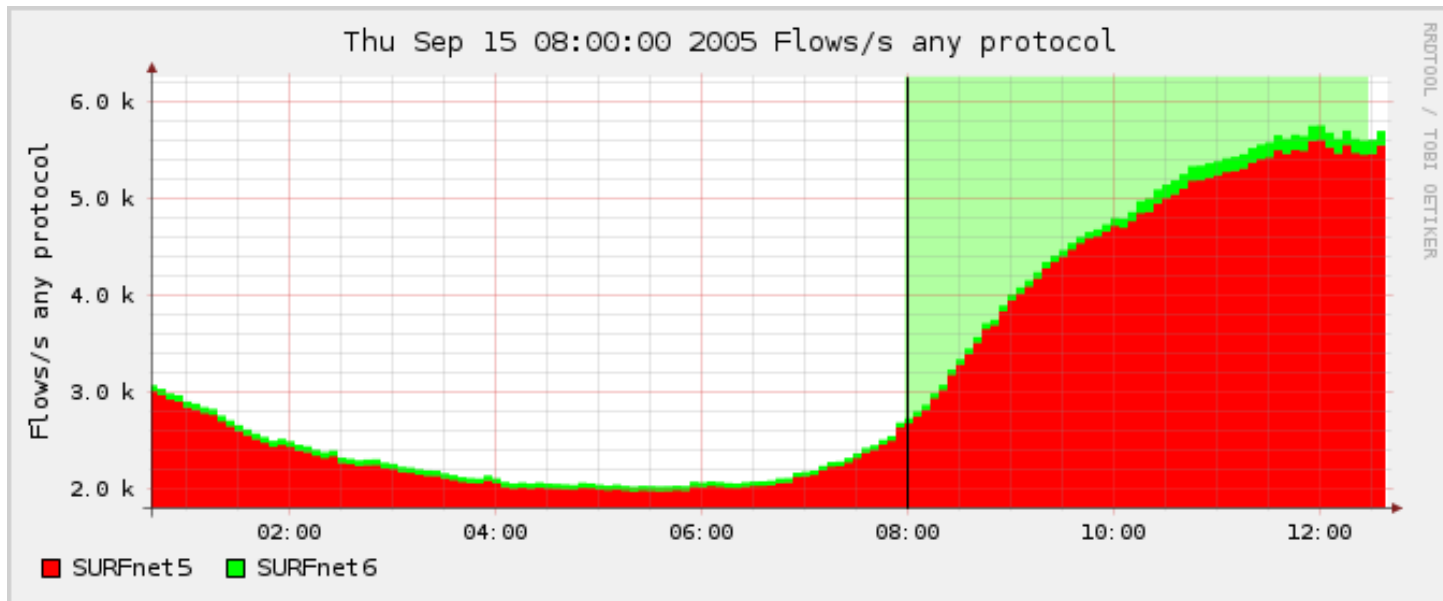
Back

```
# --- ---- Report Information --- ----
# build-version: 1
# Cluster name: cluster0
#
# Description:
# Threshold: 0
# timeFirst:2005-09-06 08:14:05
# timeLast:2005-09-06 13:13:18
# recn: ipv6_src_addr,flows

2001:610:510:0: [redacted] = 398
2001:610:508:110: [redacted] = 123
2001:610:0:800b: [redacted] = 68
fe80::20a:41ff:fe60:3ee1 = 43
2001:610:1:400a: [redacted] = 36
2001:610:508:192: [redacted] = 36
2001:610:508:110: [redacted] = 27
2001:610:0:800a: [redacted] = 11
2001:610:1:80be: [redacted] = 7
```

Back

SURFnet6



Statistics timeslot Sep 15 2005 - 08:00 - Sep 15 2005 - 12:30

Source:	Flows:	Packets:	tcp:	udp:	icmp:	other:	Traffic:	tcp:	udp:	icmp:	other:
<input checked="" type="checkbox"/> SURFnet5	4.4 K/s	19.5 K/s	15.9 K/s	2.9 K/s	37.8 /s	599.2 /s	99.0 Mb/s	92.1 Mb/s	4.2 Mb/s	35.3 Kb/s	2.7 Mb/s
<input checked="" type="checkbox"/> SURFnet6	97.8 /s	456.6 /s	419.0 /s	35.7 /s	0.5 /s	1.4 /s	2.4 Mb/s	2.4 Mb/s	47.9 Kb/s	547.6 b/s	4.2 Kb/s

Display: Sum Rate

Current Research and Development

- Geant2 JRA-2
 - NERD is one of the monitoring toolsets
- LOBSTER project
 - Demonstrate the usefulness of full Packet inputs
- Ph.D. from Vrije Universiteit (VU)
 - Interaction of Netflow and Full Packet inspection
- Student
 - Analysis and visualisation of worm behaviour

Questions

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

