

NERD

A Netflow analysis application for security

TNO | Knowledge for business



Naam

Agenda

- Security problem from an operator viewpoint
- Background of NERD
- Case: Denial of Service attacks
- Basic functionality of NERD
- Software architecture
- Specifications
- Screenshots
- Research and Development

The security problem from an operator viewpoint

- Customers can be both victim and source of incidents and suffer damage in terms of cost and image
 - Kabinet.nl, nederland.nl, overheid.nl and regering.nl unreachable for days because of DDoS attacks (nu.nl, Sep 2004)
 - Hundreds of powerful computers at the Defense Department and U.S. Senate were hijacked by hackers who used them to send spam e-mail (USA Today, Aug 2004)
- Capacity-loss, consumer complaints, and image-loss for operators
 - Computer worms cost European ISPs 123 Million € (The Register, May 2004)
 - Worm outbreaks result in large increase in helpdesk calls
 - Between 5% and 12% of all Internet traffic is malicious

Detection as a way to reduce the operator's problem

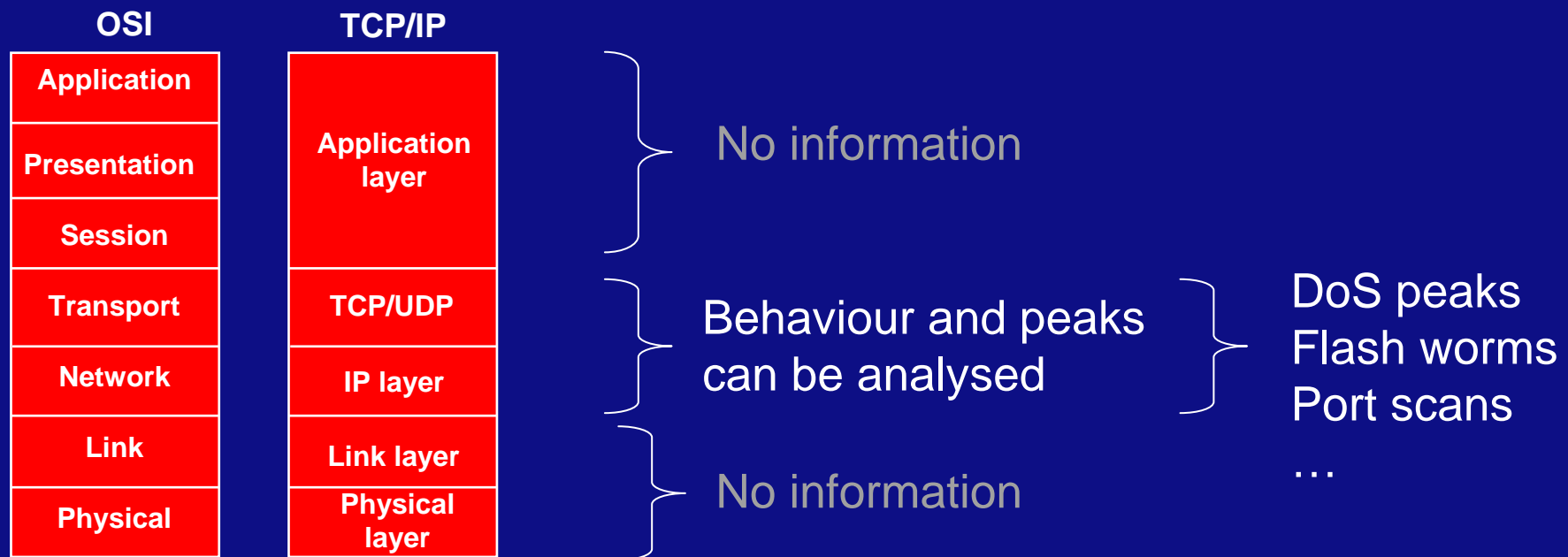
- Classical approach to incident detection...
 - wait until a customer complains
- Better approach
 - detect incident 'near real-time' and respond (semi-automatically) with for example filters to block attack source traffic
- Question is: how can this latter approach be realised?
 - Backbone is in potential a rich source of security information
 - But data analysis causes some obvious practical problems...
 - High speeds of data transfer
 - Transport of large quantities of data
 - Large geographic region, multiple countries
 - Peering traffic with other networks



Feasibility study for incident detection on SURFnet5

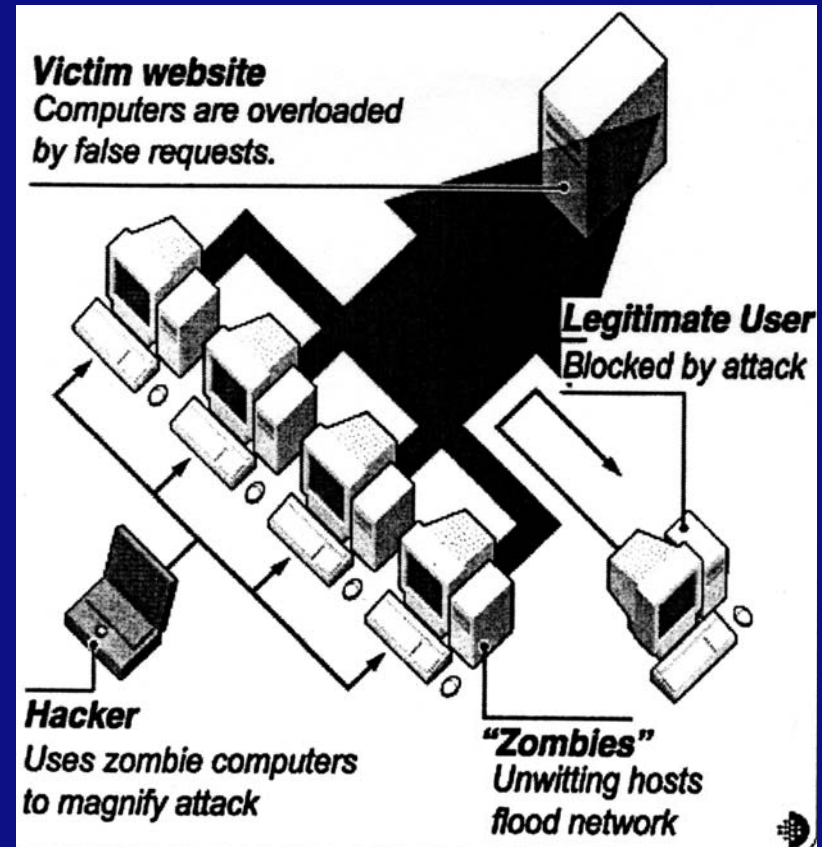
- Study of options to secure SURFnet5 (TNO, SURFnet, 2002)
 - In-depth analysis of possibilities for incident detection
 - Conclusion
 - Statistical traffic data (= Netflow) can be analysed for intrusion detection at the required speeds (>10 Gbit/s)
 - Full data analysis requires high-end equipment (e.g. LOBSTER)
- TNO developed a prototype IDS for SURFnet
 - Network Emergency Responder & Detector (NERD)
 - Based on analysis of Netflow and Syslog data
 - Tool is used by the SURFnet-CERT

Netflow's usefulness and limitations for security



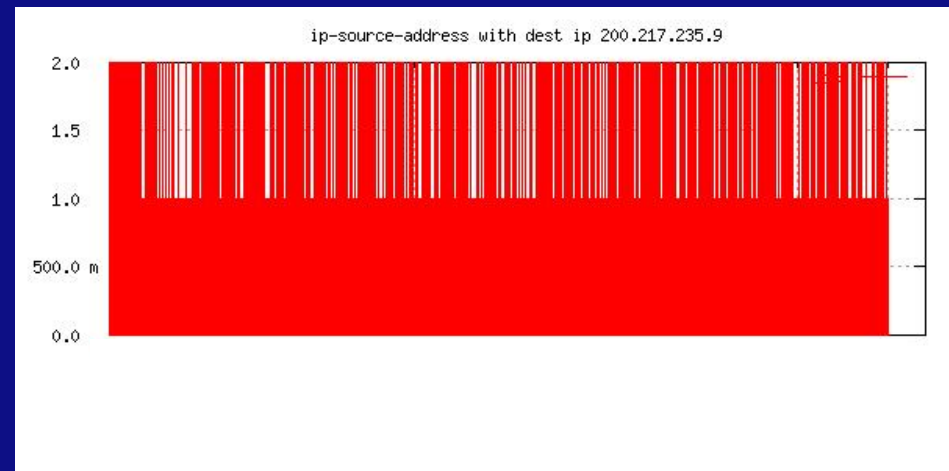
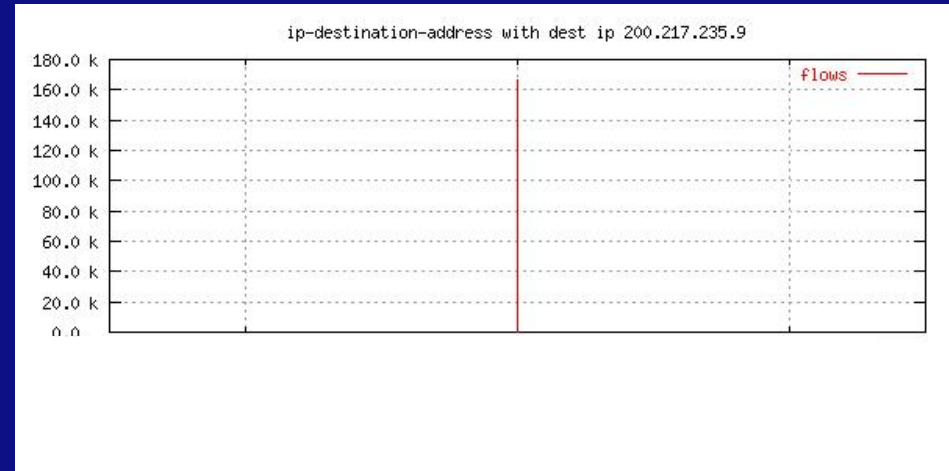
Case - Detection of DoS

- DoS is characterized by
 - Lot of traffic to one destination
 - One or more sources
 - Similar flows
- These characteristics are statistically significant and can therefore be detected by analysing Netflow



Case - Detection of DoS (2)

- NERD generates an alarm after the DoS attack has started
- This example: 40,000 packets/min are send to a destination IP
- Analysis reveals spoofed sources
- Further analysis determines the upstream ISP
- CSIRT co-operation is needed to continu the analysis



Functionality of NERD – Clusters

- Sample of Netflow data

Input flows

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

- Example 1: cluster “dst prt” & count flows

Result 1

prt	# of flows
23	5

- Example 2: cluster “dst IP & src prt” & count flows

Result 2

dst	src prt	# of flows
10.0.0.2	2000	2
10.0.0.2	1000	1
10.0.0.3	1000	3



Functionality of NERD – Filters

- Sample of Netflow data

Input flows

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

- Example: filter “src prt=2000”

Result

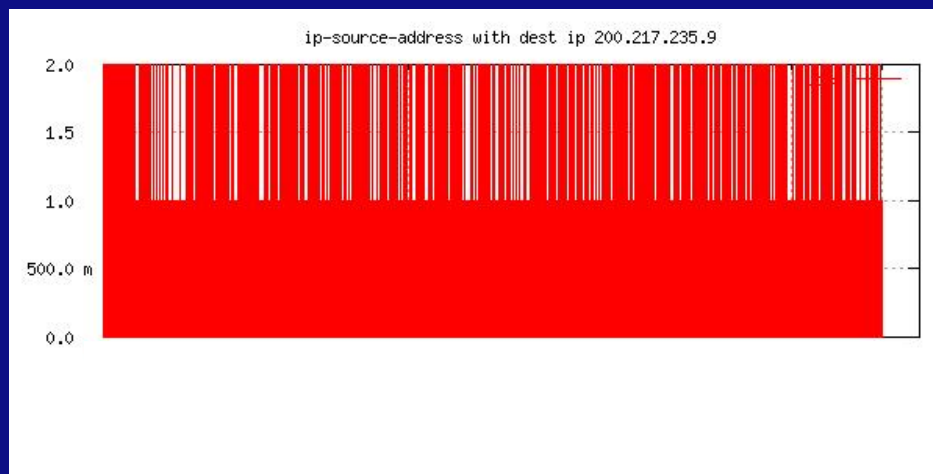
src	prt	dst	prt
10.0.0.1	2000	10.0.0.2	23
10.0.0.6	2000	10.0.0.2	23

Functionality of NERD – Real-time analysis

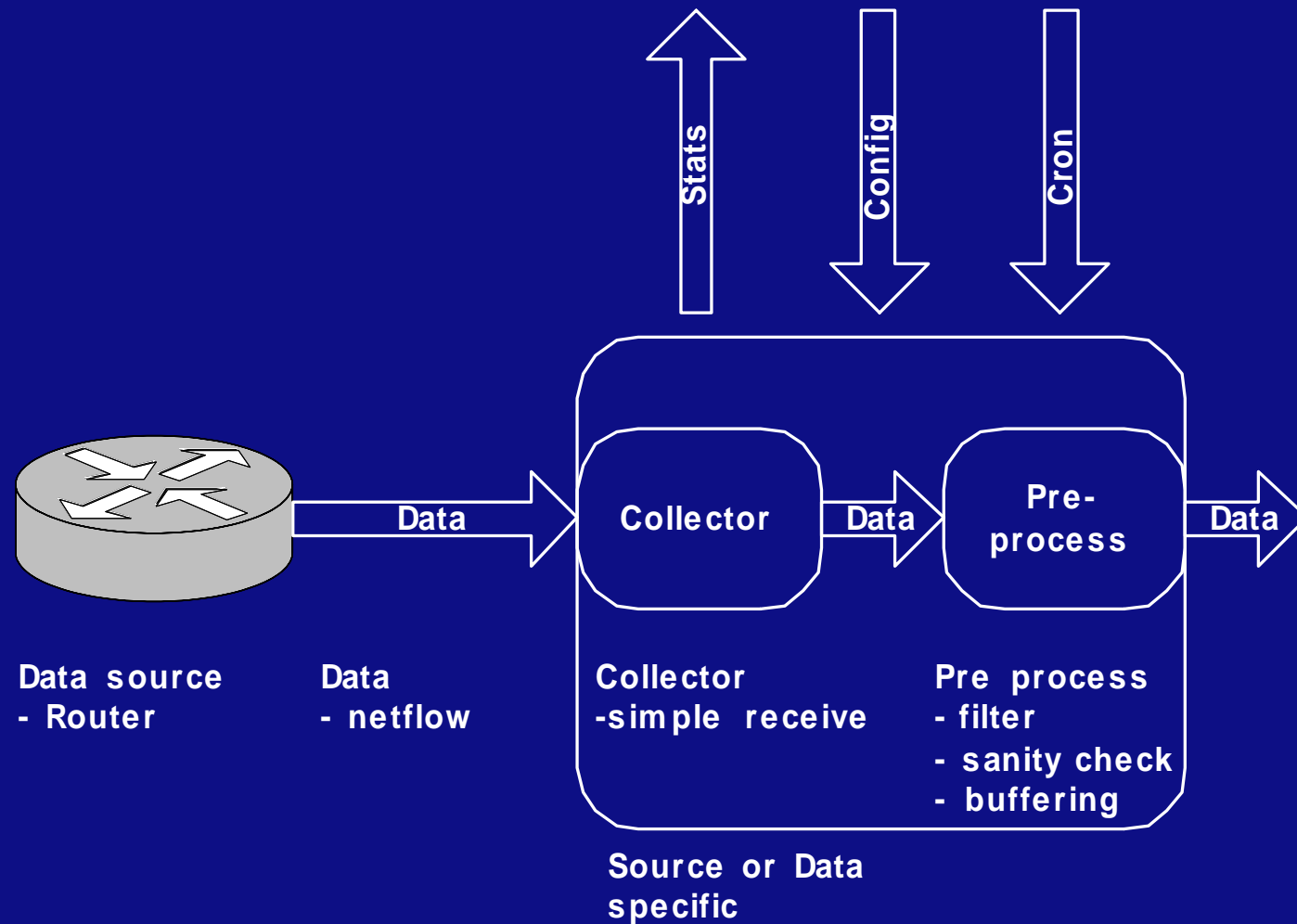
- Rules can be used for ‘real-time’ analysis
 - A rule is a combination of filters, clusters and a threshold for some metric (e.g. # of flows)
- Example of a rule
 - Cluster “dst IP”, filter “port=445”, threshold=1000 flows/ min
 - Results in an alarm if a host receives more than 1000 flows per minute on TCP port 445

Functionality of NERD –Post analysis

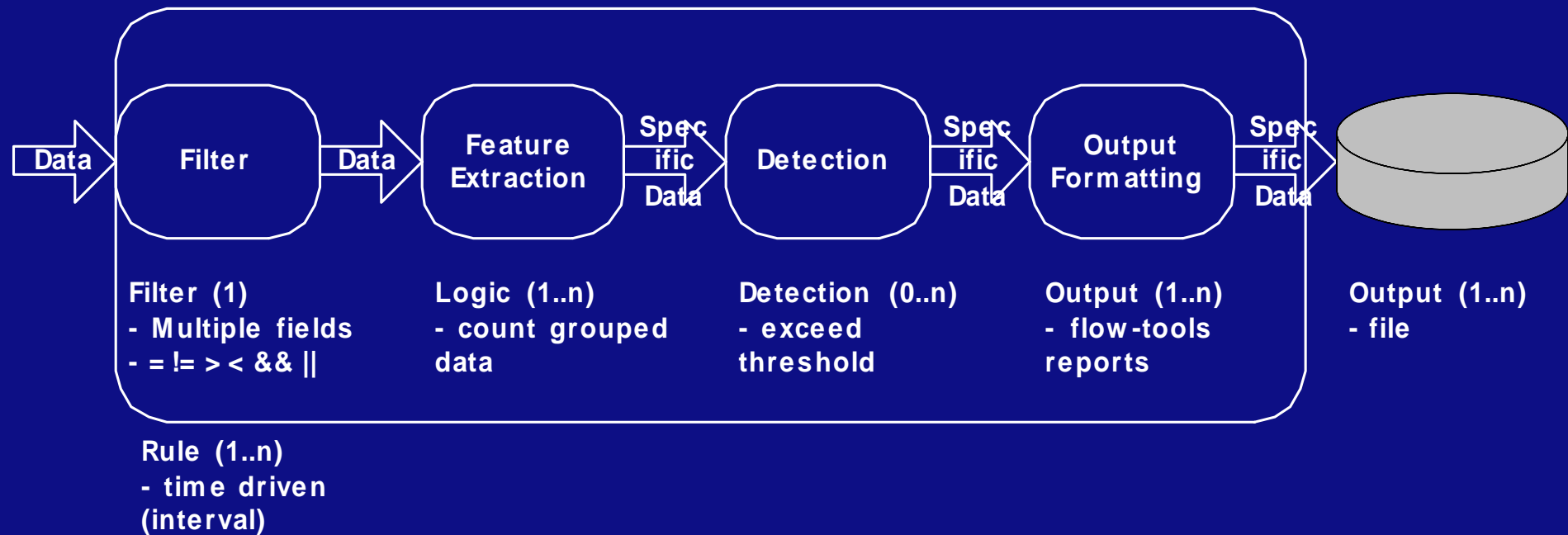
- Filters and Clusters can be made, or loaded, for post analysis
- Example of a post analysis graph
 - Cluster “src IP”
 - Filter “dst IP=a.b.c.d”
 - View “number of flows”
 - Time interval = “today”



Software Architecture (1)



Software Architecture (2)



Some specs of NERD

- Netflow versions: V5 (tested), V1, V9 (IPFIX)
- nerdd, analysis, MySQL database
- Linux and FreeBSD platforms tested
- Apache Open Source Licence v2.0

Screenshots (1)



Alarms

Analysis

Settings



Set Analysis

Load Cluster

Display

Number of flows

Group by

IPv4 source address

IPv4 destination address

Load Filter

Filter by

Protocol	=	7
Destination Port	<	1024
Source IPv4 address	!=	10.0.0.138

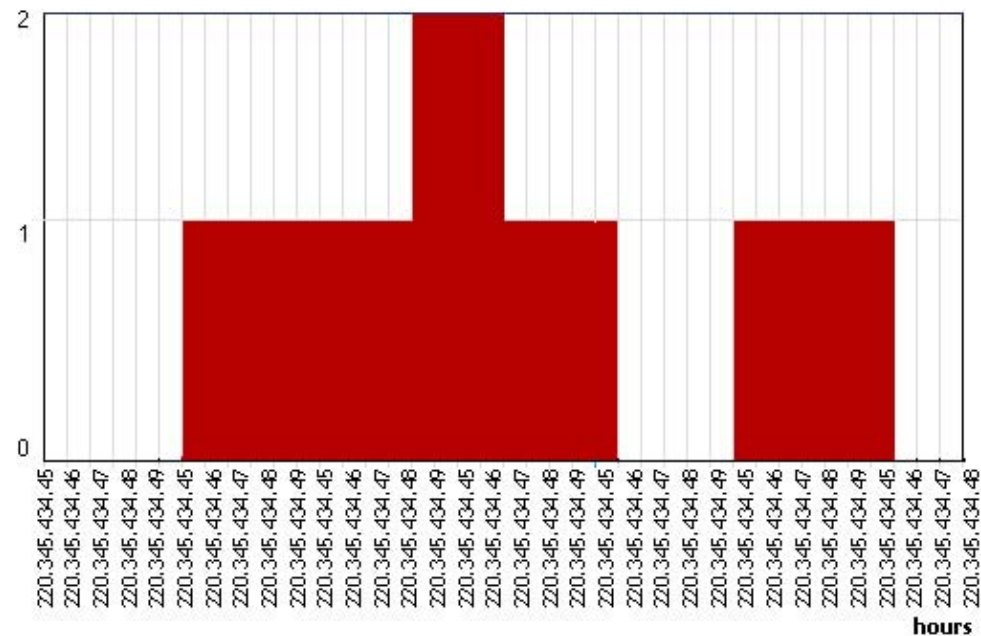
Analyse

IPv4 source address & IPv4 destination address

Records: 165395 Min val: 0.0.23.52 Max val: 223.255.225.21

Raw data

flows



Screenshots (2)



NERD

Network Emergency Responder & Detector

Alarms

Analysis

Settings



Alarms of Wednesday, September 8th 2004

Previous day

Next day

Search for Alarms

Starttime (GMT+1)	Stoptime (GMT+1)	Rulename	Alarm message	Trigger
Wed, Sept 8th, 11:00	Wed, Sept 8th, 12:31	Flood detection	Source IP address 10.0.0.138 with Destination IP address 192.168.0.2 has 12832 connections in 5 minutes	9000 connections in 5 minutes Analyse
Wed, Sept 8th, 12:50	* Not stopped *	Portscan detection	Source IP address 127.0.0.1 has 20316 destination ports in 5 minutes	15000 destination ports in 5 minutes Analyse

Current Research and Development

- NERD is one of the monitoring toolsets for Geant2 JRA-2
- Demonstrate the usefulness of full Packet inputs in the LOBSTER project (security and other monitoring apps)
- Ph.D. from Vrije Universiteit (VU) working on interaction of Netflow and Full Packet inspection
- Student working on analysis and visualisation of worm behaviour

Questions?

- More information and download of NERD:
www.nerdd.org (up soon), or contact us
- Hans Hoogstraaten
(31-15) 2857 137
hans.hoogstraaten@tno.nl
- Rutger Coolen
(31-15) 2857 068
rutger.coolen@tno.nl