TNO Information & Communication– Technology

Update Lobster & NERD

TNO | Knowledge for business

Agenda

- Lobster:
    - What is Lobster?
    - Status
- NERD:

Lobster

- Main goal:
  - To develop an advanced European infrastructure for passive network monitoring.
- 9 Partners:
  - ALCATEL, CESNET, ENDANCE, FORTH, FORTHNET, Vrije Universiteit Amsterdam, Terena, TNO, UNINETT
- Duration: oct 2004 – dec 2006

Possible Lobster Applications

- Accurate traffic characterisation for programs using dynamic ports
- Spread of zero-day worms
- European Internet measurement service
- End-to-end performance debugging
- Application performance measurement
- Trace DoS attacks
- Test platform for IPFIX attributes

Lobster

- High speed network monitoring (10Gbps)
- Use of Dedicated programmable hardware (fpga cards – DAG, SCAMPI)
- Monitoring application programming interface (MAPI)
- Multiple network sensor API (distributed MAPI)
- Cross domain monitoring
- Anonymisation framework
- Access control
- Demo applications

Lobster vs. Geant2

- Same ‘member’ community
- Lobster also tries to include commercial members (ISPs)
- Passive monitoring only
- Use same (passive) measurement data
- Equal infrastructure design (Lobster adapts from JRA1)
- Same security applications
- Not only security applications
- Lobster has shorter time span (2 years) (more pressed for demo apps)

Lobster status

- Requirements analysis – done!
  - Req. collection, acceptable use policy for fair sharing

- Monitoring infrastructure design – due Oct ’05
  - Anonymisation framework definition, Common access platform definition, first-tier encryption definition, integrated architecture definition

- Monitoring infrastructure realisation – due Apr ’06
  - Prototype

- Monitoring infrastructure deployment – due Jan ’06
  - LOBSTER applications, Monitoring infrastructure

NERD

Network Emergency Responder & Detector

- History
- How does it work?
  - real-time analysis
  - post analysis
  - web user interface
- Status
- Future
  - from application to framework
  - Integration in LOBSTER, Geant2.

History

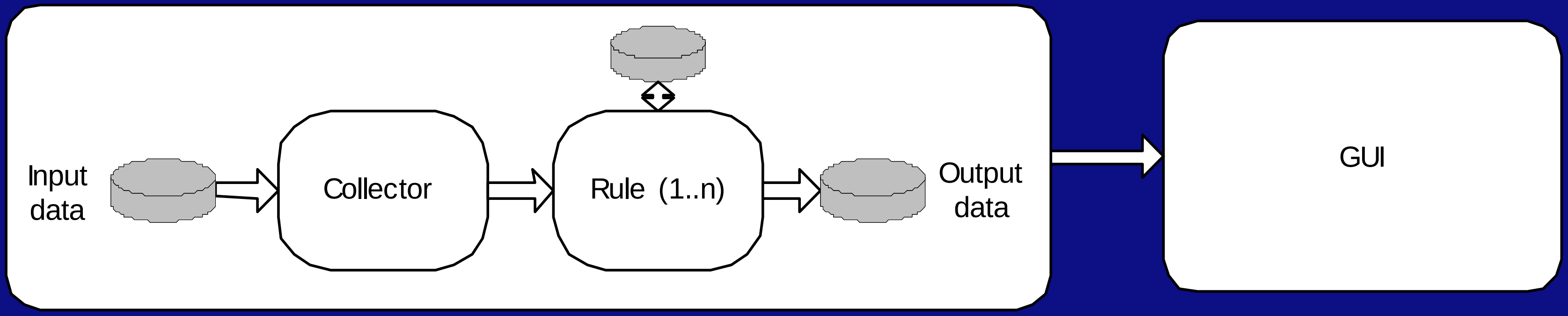
- 2002: SURFnet and TNO initiated a research project into DoS detection on the SURFnet network
- End of 2002: Prototype (NERD v0.1) finished, based on Caida’s cflowd, flowtools, gnuplot and shell scripts.
- 2004: Design & development of NERD v0.5, removed third party tools by rewriting the daemon
- 2004: Design & development of NERD v1.0, bugfixes on daemon and new user interface
- 2004: Application to be used in Lobster
- 2005: potential security tool used in GN2/JRA2 (SURFnet)
- 2005 March 18: Open source release NERD (1.03beta)

- NERD – Network Emergency Responder & Detector

- Collects NetFlow
- A tool that detects DoS attacks
- raises Alarms
- flexible search through stored NetFlow data

How does it work?

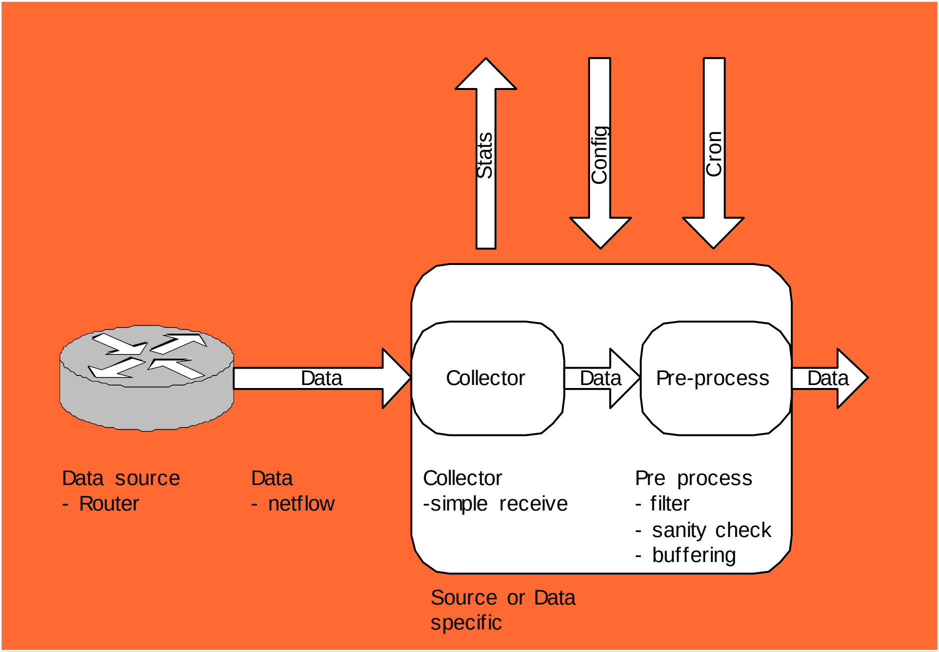
- Input data: NetFlow
- real-time analyse
  - Output: alarms in database
- post analysis
  - Output: flow-tools style data (text)
- web based GUI



The collector

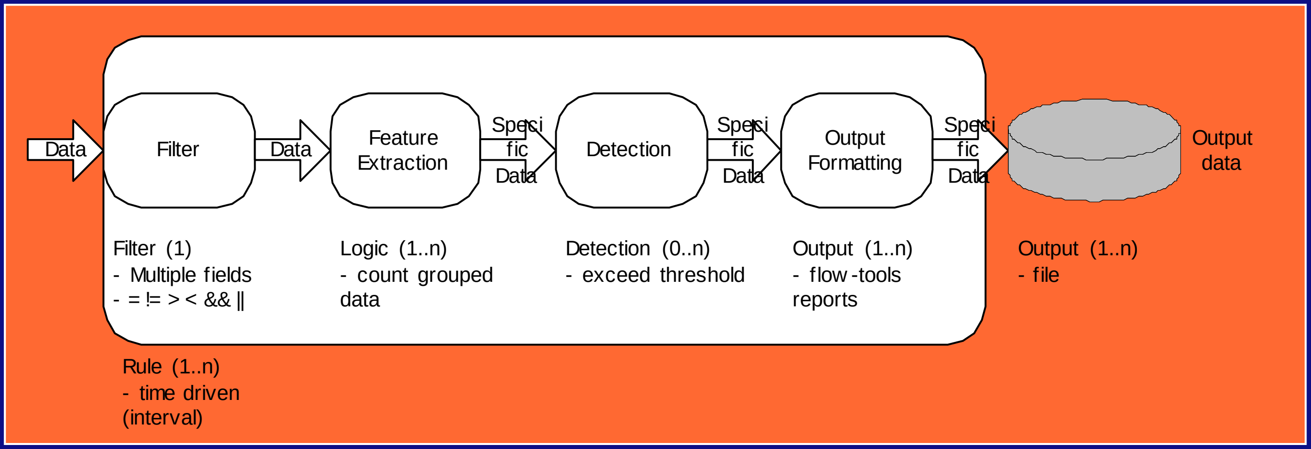
- Collector
  - simple UDP receiver (binds to multiple IP/port)
- Pre-processor
  - source specific functions (ex. filter double flows)

- Data stored on disk
  - for the post analysis
- Data kept in memory
  - for real-time analysis



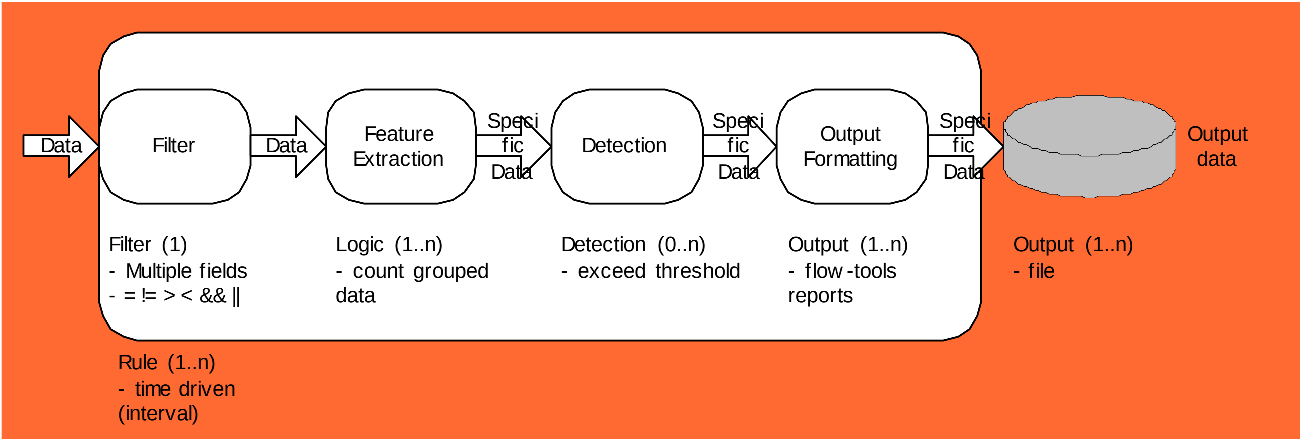
Real-time analysis

- Every x minutes the Rules (1..n) are executed
- Rule:
  - 1 filter (ex. src_addr = 123.0.0.0/16 and dst_port != 80)
  - 1..n clusters (cluster on dst_ip and count flows)
  - threshold (#flows > 1,000,000)
  - output formatting (alarm in database)



Post analysis

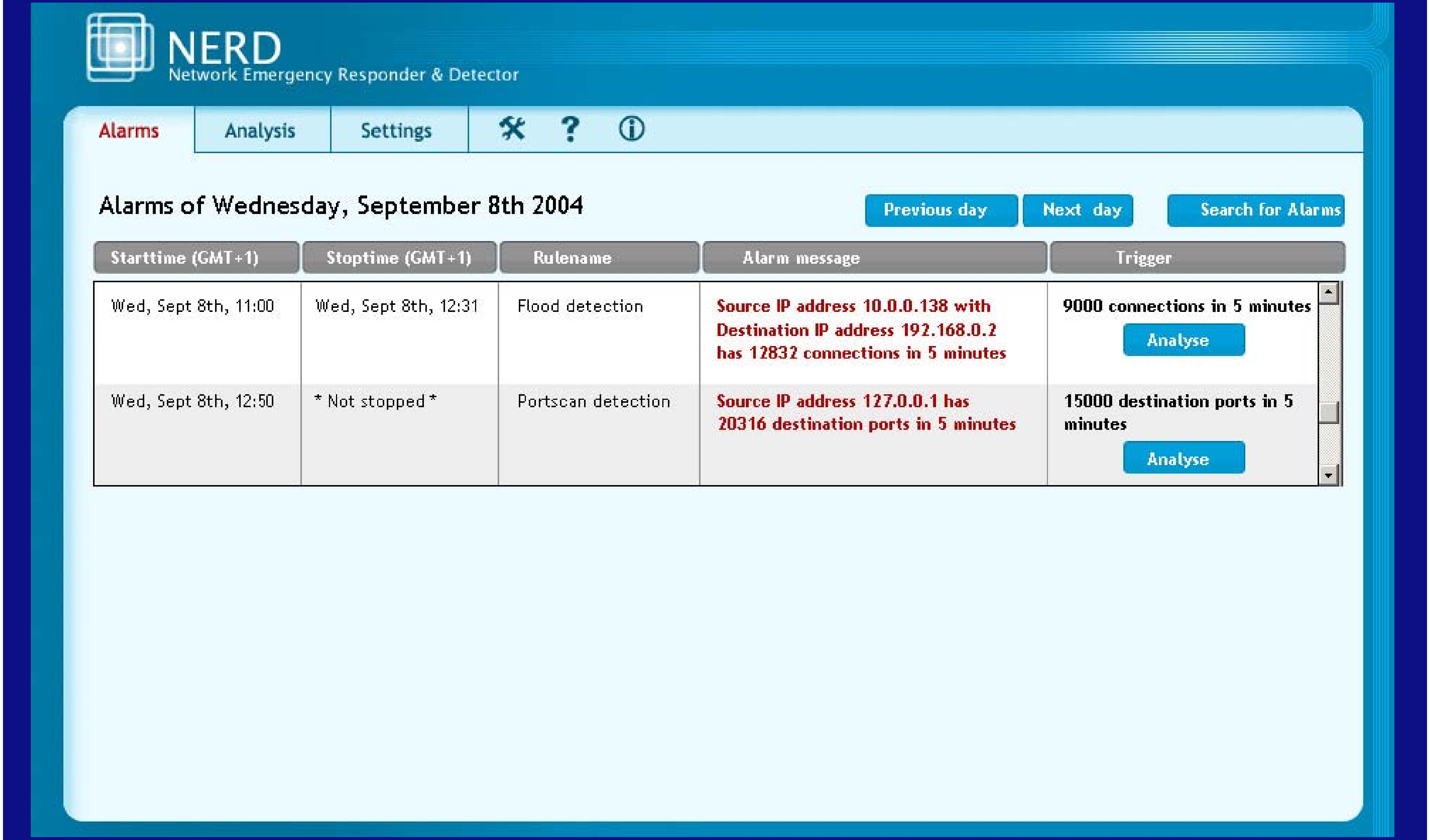
- Executed at users request
- Rule:
    - 1 filter (same as real-time analysis)
    - 1..n clusters (same as real-time analysis)
    - (no threshold)
    - output formatting (flow-tools like text files)



Configuration

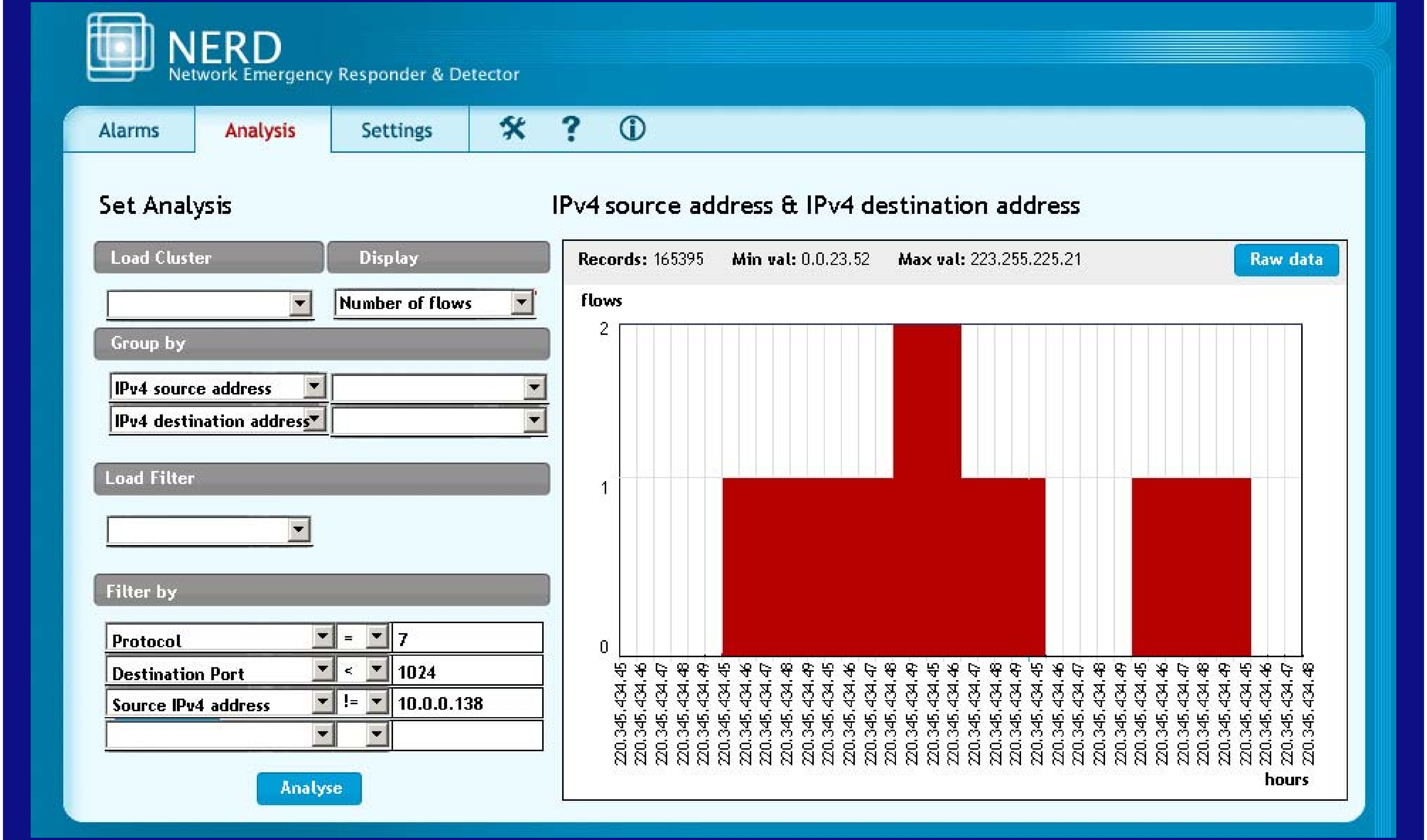
- Stored in database
- Rule record = filter + cluster
  - making filters and clusters reusable
  - multi user prepared

GUI screenshots



Alarms of Wednesday, September 8th 2004

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
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



Set Analysis

Load Cluster

Display: Number of flows

Group by

IPv4 source address

IPv4 destination address

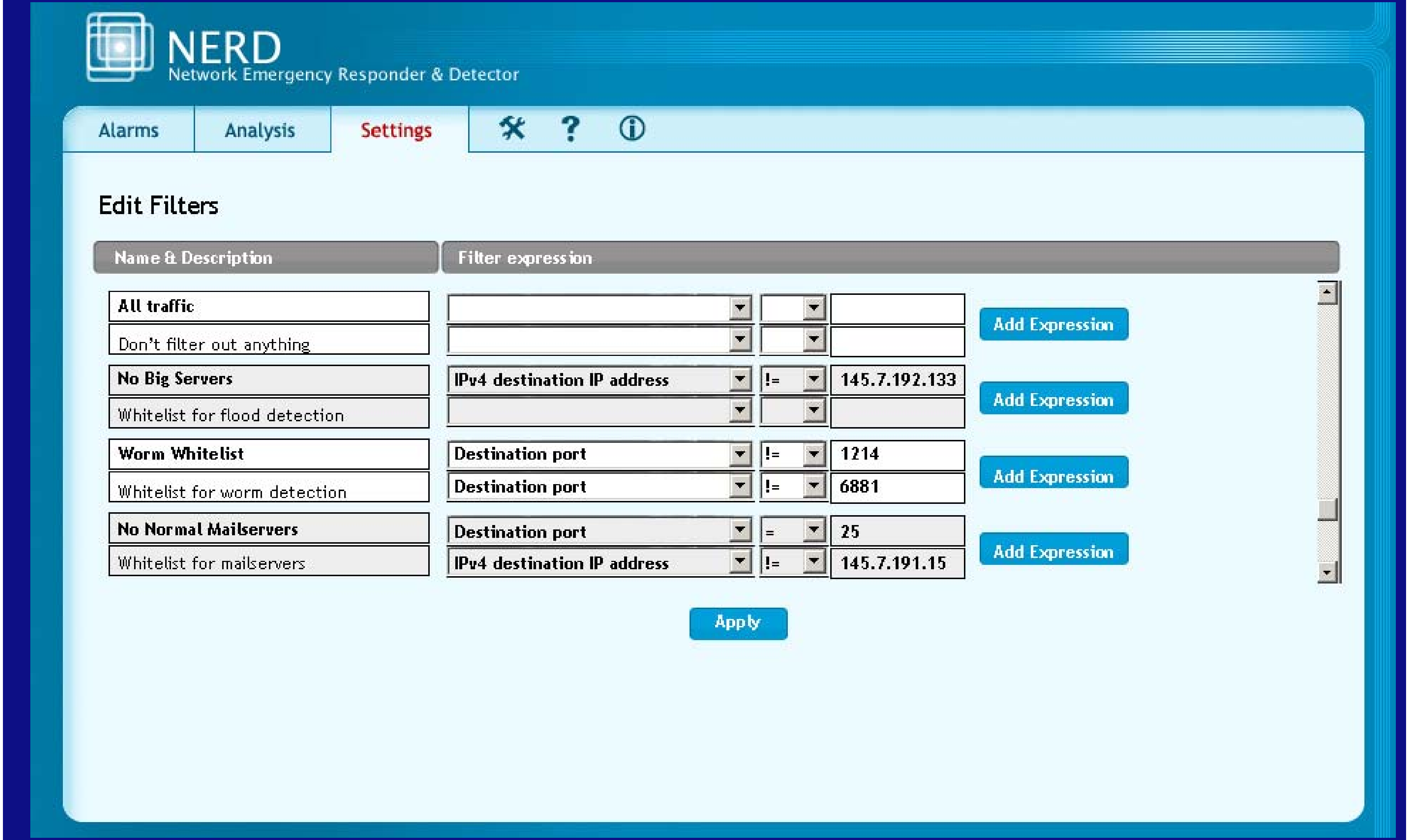
Load Filter

Filter by

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

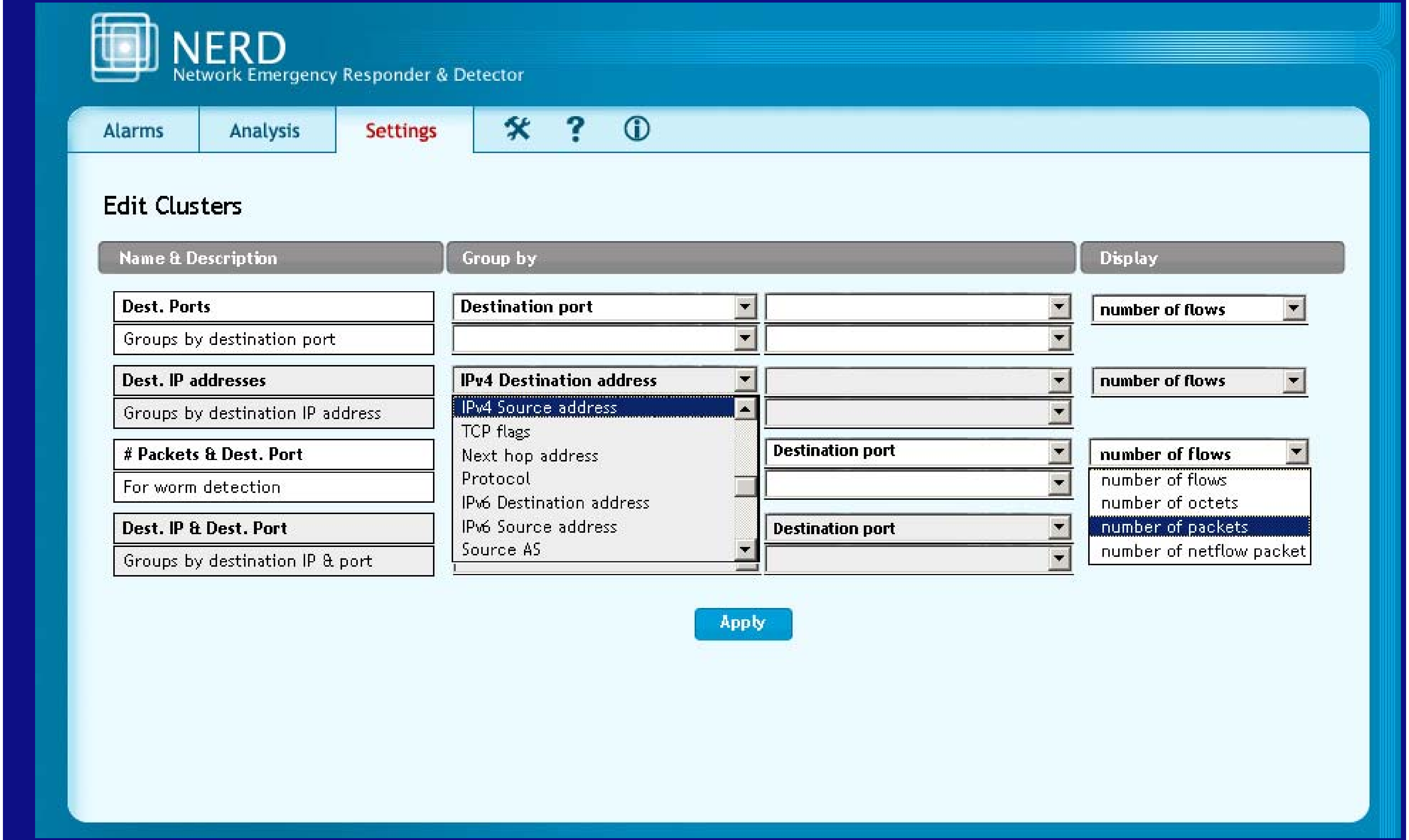
IPv4 source address & IPv4 destination address

Records: 165395 **Min val:** 0.0.23.52 **Max val:** 223.255.225.21



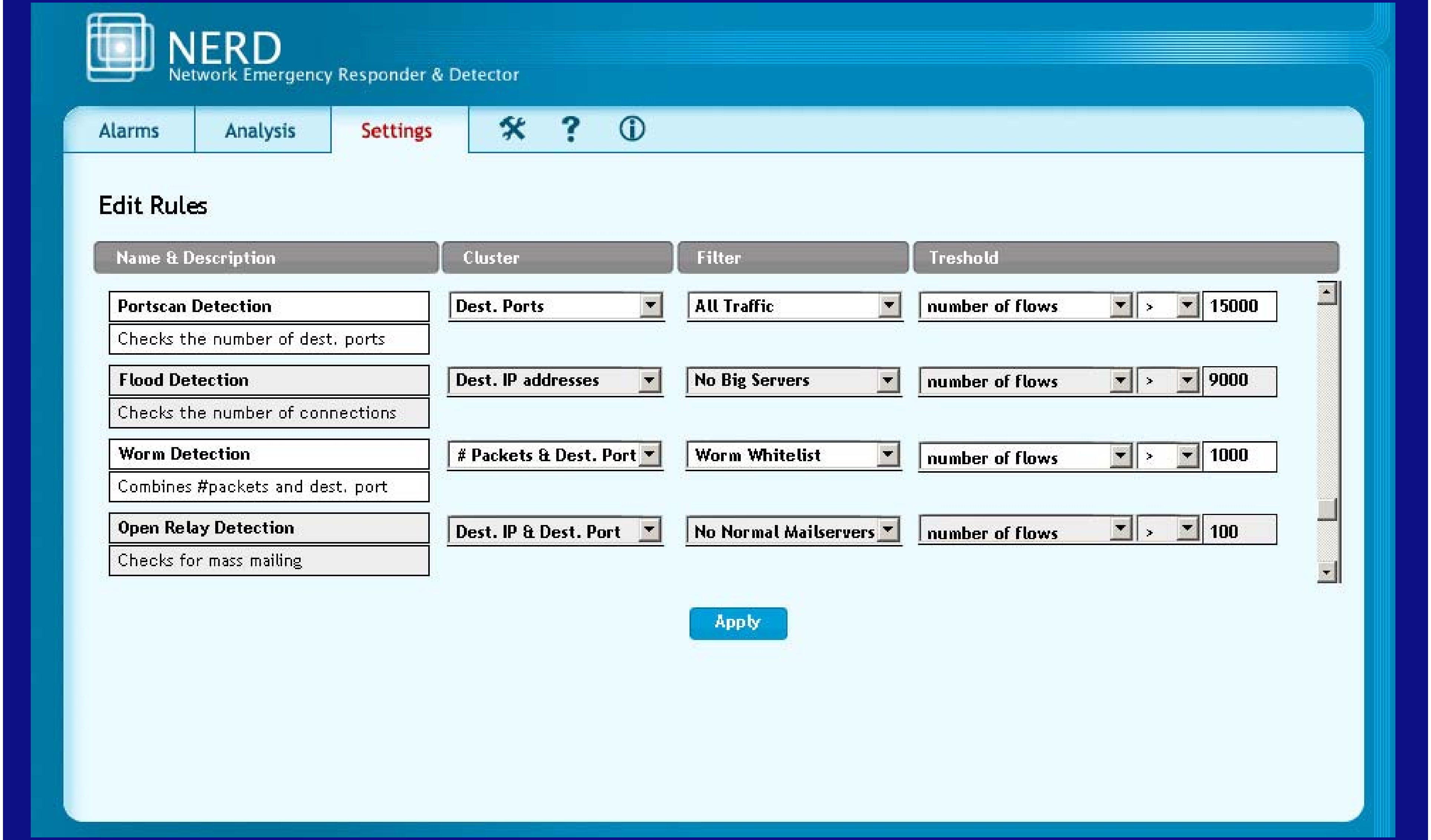
Edit Filters

Name & Description	Filter expression		
All traffic			
Don't filter out anything			
No Big Servers	IPv4 destination IP address	!=	145.7.192.133
Whitelist for flood detection			
Worm Whitelist	Destination port	!=	1214
Whitelist for worm detection	Destination port	!=	6881
No Normal Mailservers	Destination port	=	25
Whitelist for mailservers	IPv4 destination IP address	!=	145.7.191.15



Edit Clusters

Name & Description	Group by		Display
Dest. Ports	Destination port		number of flows
Groups by destination port			
Dest. IP addresses	IPv4 Destination address		number of flows
Groups by destination IP address			
# Packets & Dest. Port		Destination port	number of flows
For worm detection			
Dest. IP & Dest. Port		Destination port	
Groups by destination IP & port			



Edit Rules

Name & Description	Cluster	Filter	Treshold		
Portscan Detection Checks the number of dest. ports	Dest. Ports	All Traffic	number of flows	>	15000
Flood Detection Checks the number of connections	Dest. IP addresses	No Big Servers	number of flows	>	9000
Worm Detection Combines #packets and dest. port	# Packets & Dest. Port	Worm Whitelist	number of flows	>	1000
Open Relay Detection Checks for mass mailing	Dest. IP & Dest. Port	No Normal Mailservers	number of flows	>	100

Status

- Beta testers wanted!

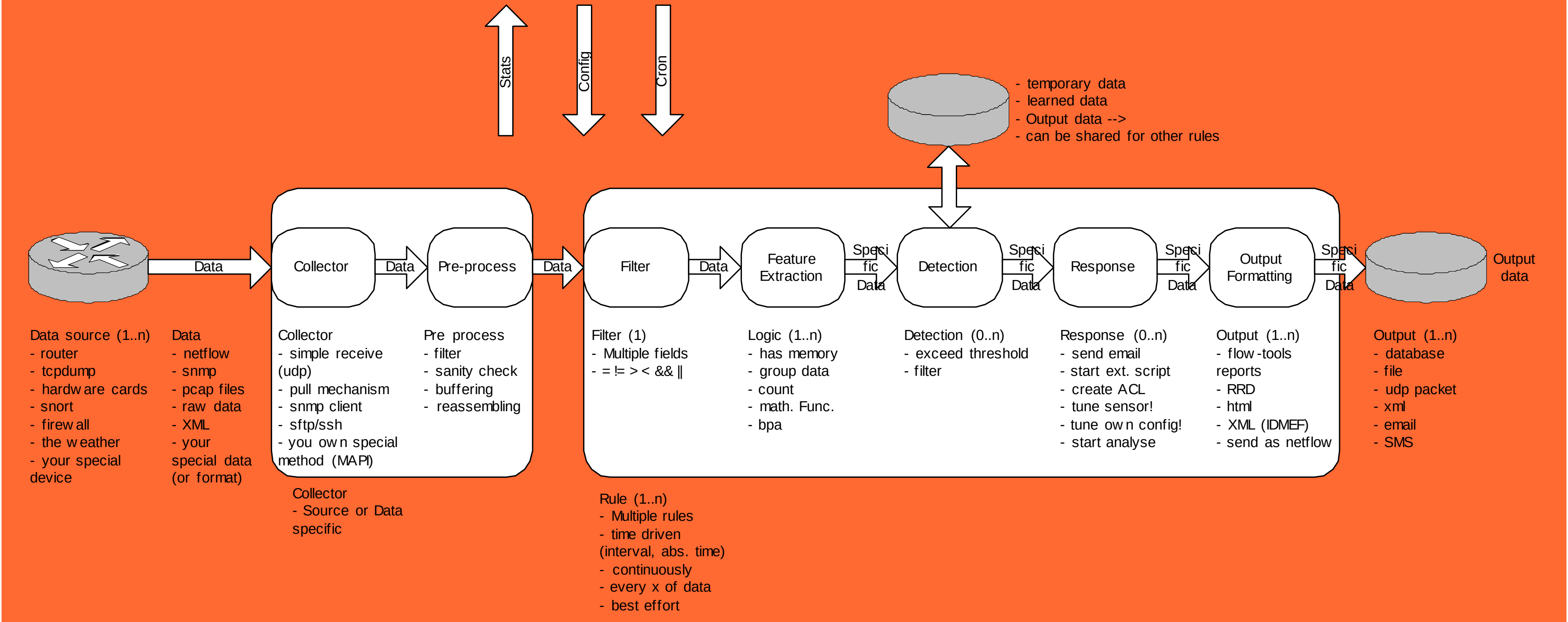
- Short term todo list:
  - web-site/ subversion
  - documentation/ white paper
  - more intuitive interface
  - ipv6 & netflow v9 bug fixes

- Mid-long term (next year)
  - worm detection
  - 3D data representation (student)
  - Flexible data analysis (connection to ROOT/ MatLab etc.)
  - Integration into JRA1/ Lobster architecture
  - from application to framework…

From application to framework

- Other (data) sources
  - tcpdump, hardware cards, snort, firewall,
  - pcap/ raw format, alarms/ logging, XML,
- Combining different data
  - ex. fw or httpd log with network data for worm detection
- Other data output
  - graphs, alarms, top 10 list, XML reports, NetFlow
- Modular building bocks
  - basic function blocks
- Offer APIs for self-made feature extraction

Framework



- temporary data
- learned data
- Output data -->
- can be shared for other rules

Data source (1..n)
- router
- tcpdump
- hardware cards
- snort
- firewall
- the weather
- your special device

Data
- netflow
- snmp
- pcap files
- raw data
- XML
- your special data (or format)

Collector
- simple receive (udp)
- pull mechanism
- snmp client
- sftp/ssh
- you own special method (MAPI)

Pre process
- filter
- sanity check
- buffering
- reassembling

Collector
- Source or Data specific

Filter (1)
- Multiple fields
- = != > < && ||

Logic (1..n)
- has memory
- group data
- count
- math. Func.
- bpa

Detection (0..n)
- exceed threshold
- filter

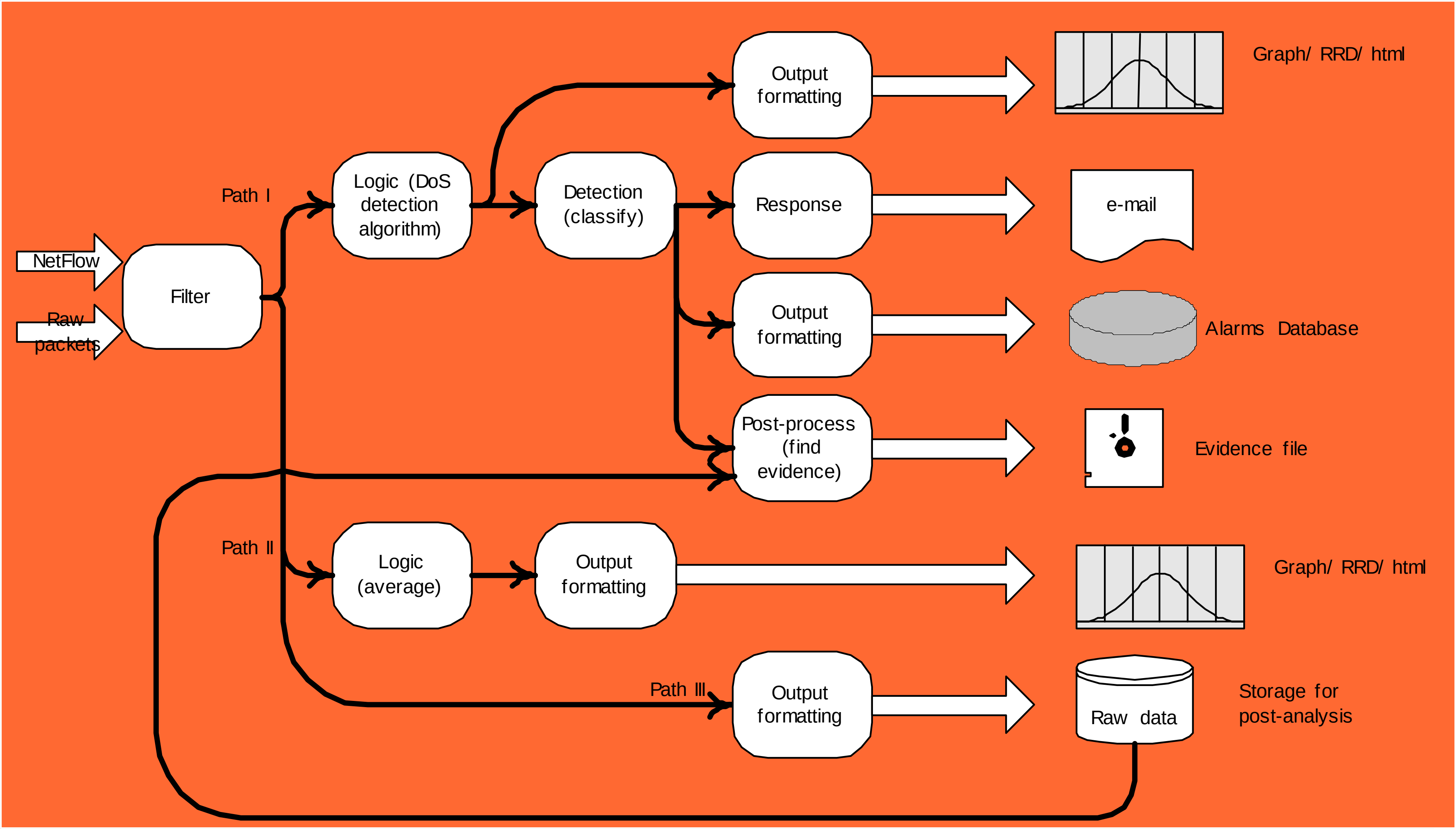
Response (0..n)
- send email
- start ext. script
- create ACL
- tune sensor!
- tune own config!
- start analyse

Output (1..n)
- flow-tools reports
- RRD
- html
- XML (IDMEF)
- send as netflow

Output (1..n)
- database
- file
- udp packet
- xml
- email
- SMS

Rule (1..n)
- Multiple rules
- time driven (interval, abs. time)
- continuously
- every x of data
- best effort

Configuration Example



NERD

Network Emergency Responder & Detector

- Lobster site: www.ist-lobster.org

- NERD: www.nerdd.org (will be up soon)
- info@nerdd.org

- Hans Hoogstraaten
- J.M.Hoogstraaten@telecom.tno.nl

- TNO - To apply scientific knowledge with the aim of strengthening the innovative power of industry and government - www.tno.nl