

Toa: A web based NetFlow data monitoring system

José R. Ortiz Ubarri, Humberto Ortiz-Zuazaga
Eric Santos, Albert Maldonado, Jhensen Grullon
Computer Science Department
University of Puerto Rico
Flocon 2015, Portland Oregon



Outline



- Background
- Toa Backend
- Toa GUI
- Plugins

Previous work



- FlowScan
- NetFlow Sensor (tied to nfdump)
- NVisionIP (FloCon 2005)
- FloVis (FloCon 2009)
- Stager (FloCon 2010)
- FlowViewer (FloCon 2013)
- Rayon & Prism (FloCon 2014)

Toa features

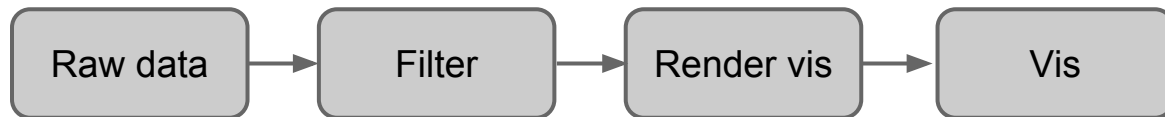


- Web implementation based in bootstrap.
 - main web interface fits nicely in tablets and smartphones
- Interactive charts capable of listening to events.
 - used to connect charts to plugins
- Allows to query the sensor data in the database and generate graphs.
- Parallel implementation of the parser and the grapher.
- Parsing (aggregation) of the raw data for all the graphs done in one pass.

Generic data preparation process

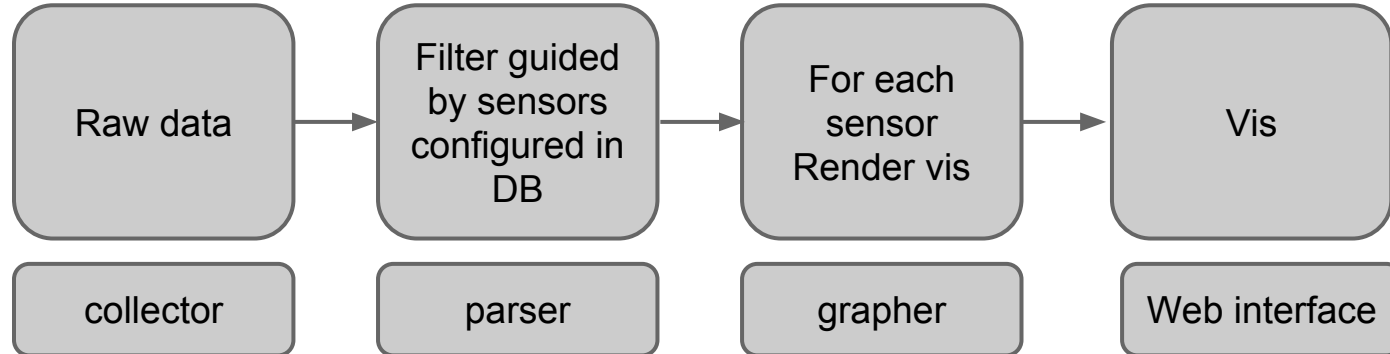


For each sensor:



Reference: http://resources.sei.cmu.edu/asset_files/Poster/2014_020_001_300460.pdf

Toa data preparation process

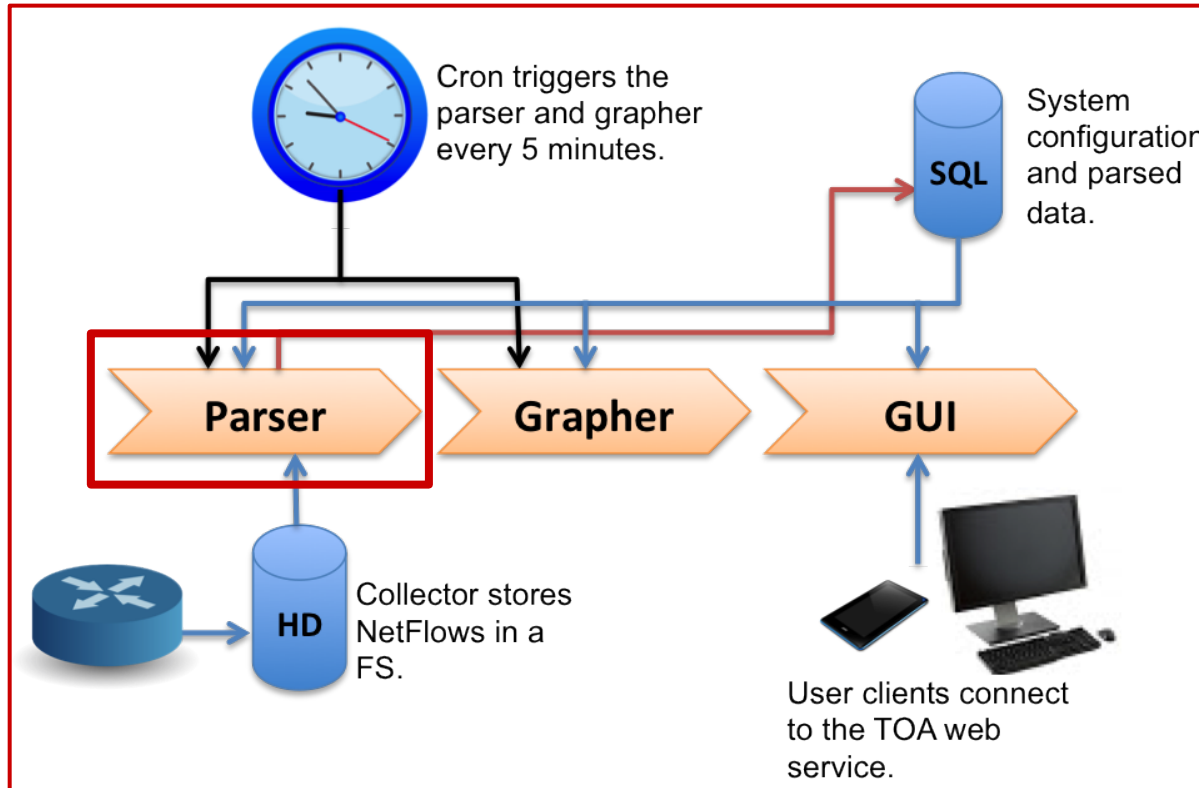


Toa: Dictionary



- Structure that is dynamically generated using configurations stored in the database
- Integral to the framework since it is:
 - used to know the data to be parsed
 - used to know the graphs to be generated
 - used to generate the GUI menus.

Toa Parser:

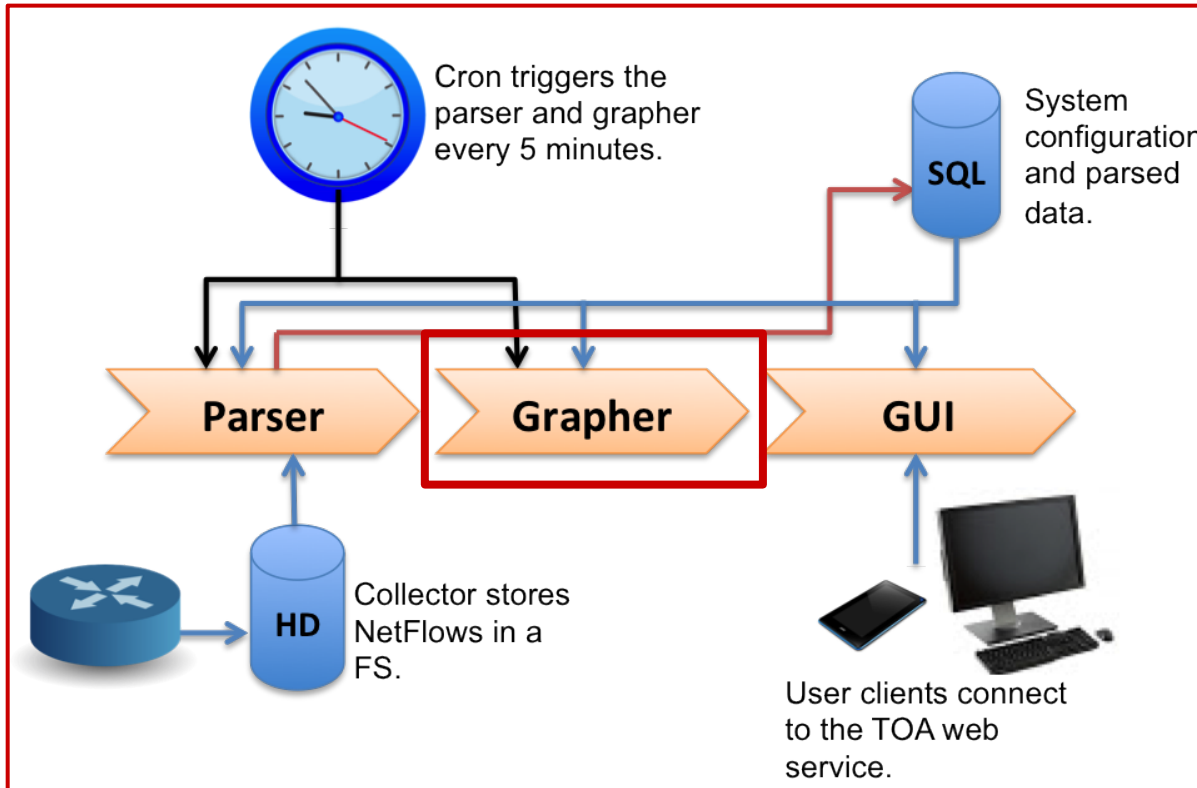


Toa Parser



- Reads the NetFlow data collected.
- Aggregates data, packets and flow traffic by:
 - device interface,
 - autonomous system number (AS),
 - and network block.
- Aggregates port traffic in each network
- Aggregates net to net traffic.
- The complexity is determined by the degree of the network. (How many flows per 5 minutes)

Toa: Grapher:

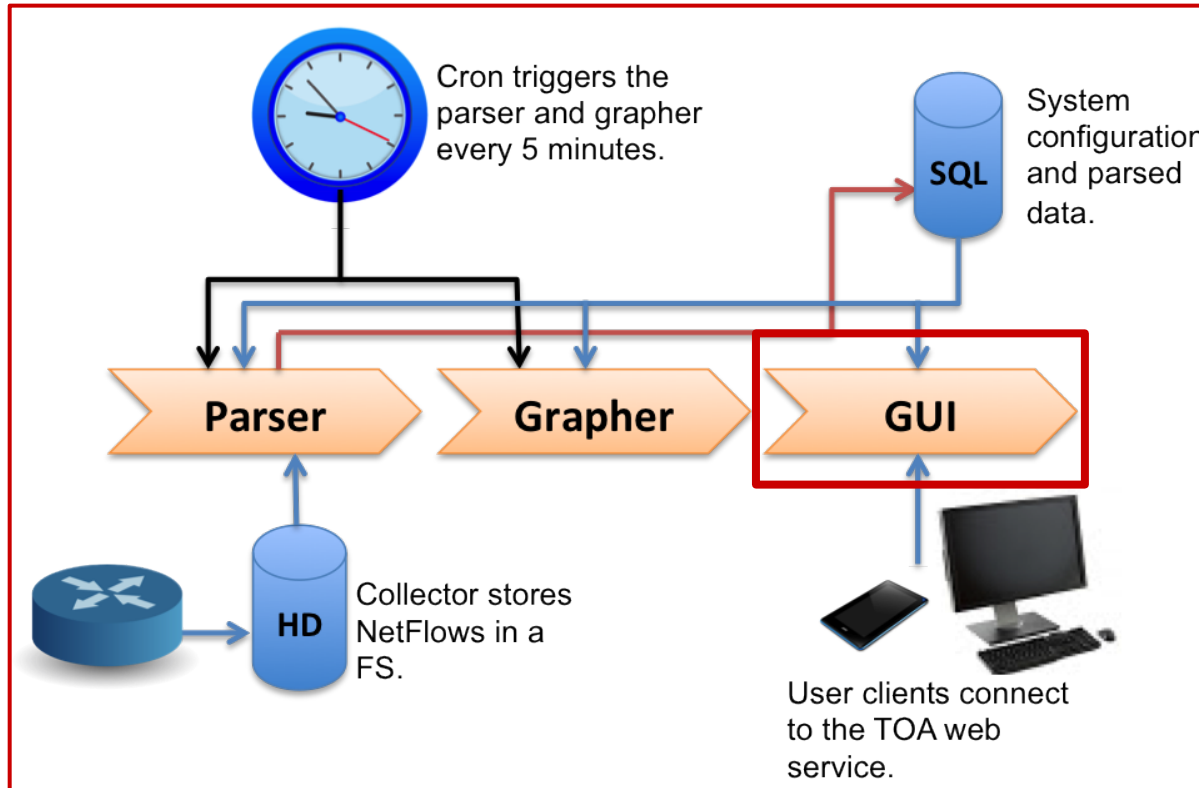


Toa Grapher



- Runs after the parser is executed.
- Generates the graphs to be displayed in the GUI
 - To avoid DoS
- To generate graphs dynamically the user needs to login.
- The graphs are generated using the google charts library.
 - They are in javascript and respond to events.
- No more than 300 points per graph.
 - Weekly, monthly and yearly data is averaged similar to RRDTools.

Toa: GUI



Toa GUI



Shared with me - Google Drive Toa BSides - Google Drive ToaNMS

flows.hpcf.upr.edu/~eric/toa/public_html/

Toa Network Monitoring System

Home Device

RUM

connections:

- FIU
 - Objects: 19217789
 - Packets: 53002
 - Flows: 4932
- HPCI
 - Objects: 91482088
 - Packets: 66378
 - Flows: 9
- AD
 - Objects: 0
 - Packets: 0
 - Flows: 0
- RUM
 - Objects: 0
 - Packets: 0
 - Flows: 0
- PDI
 - Objects: 0
 - Packets: 0
 - Flows: 0
- RPP
 - Objects: 0
 - Packets: 0
 - Flows: 0

Username

Password

Login

GUI Menu



The screenshot displays the Toa Network Monitoring System interface. At the top, there are browser tabs for 'Toa BSides - Google Drive' and 'ToaNMS', and the address bar shows 'flows.hpcf.upr.edu/~eric/toa/public_html/'. The main heading is 'Toa Network Monitoring System'. Below this is a navigation bar with 'Home' and 'Device' tabs. A dropdown menu is open under 'Device', listing various network devices: RUM, RCM, RRP, CAYEY, FIU, HPCf, CUH, PSM, AO, and Eric. A sub-menu is open for 'RUM', showing 'Interface Graph', 'Port Graph' (with a value of 22), and 'Net2Net Graph' (with a value of 1433). The main content area features a circular network diagram with nodes labeled RUM, RCM, RRP, CAYEY, FIU, HPCf, CUH, PSM, AO, and Eric. To the right of the diagram is a 'connections:' section with a list of statistics for each device. On the far right, there is a login form with fields for 'Username' and 'Password', and a 'Login' button.

connections:

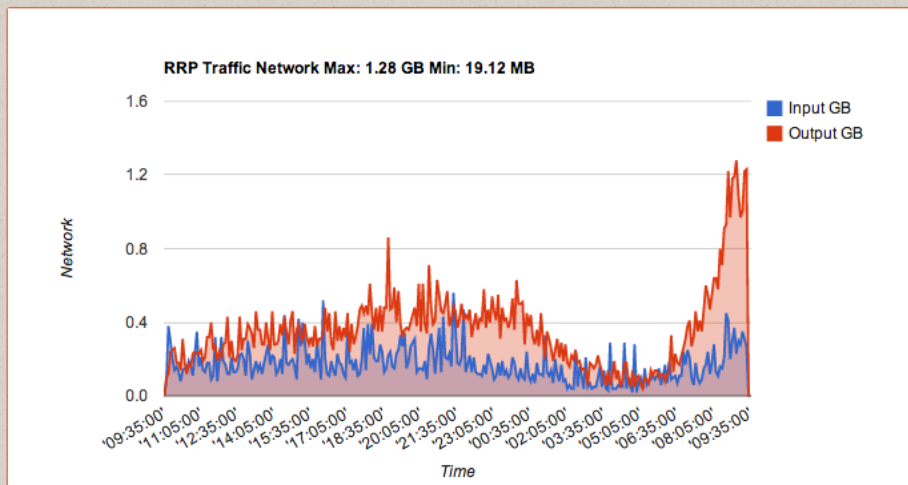
- FIU
 - Octects: 19217789
 - Packets: 53802
 - Flows: 4932
- HPCf
 - Octects: 91482888
 - Packets: 86376
 - Flows: 9
- AO
 - Octects: 0
 - Packets: 0
 - Flows: 0
- CUH
 - Octects: 0
 - Packets: 0
 - Flows: 0
- PSM
 - Octects: 0
 - Packets: 0
 - Flows: 0

By Netlabel: RRP



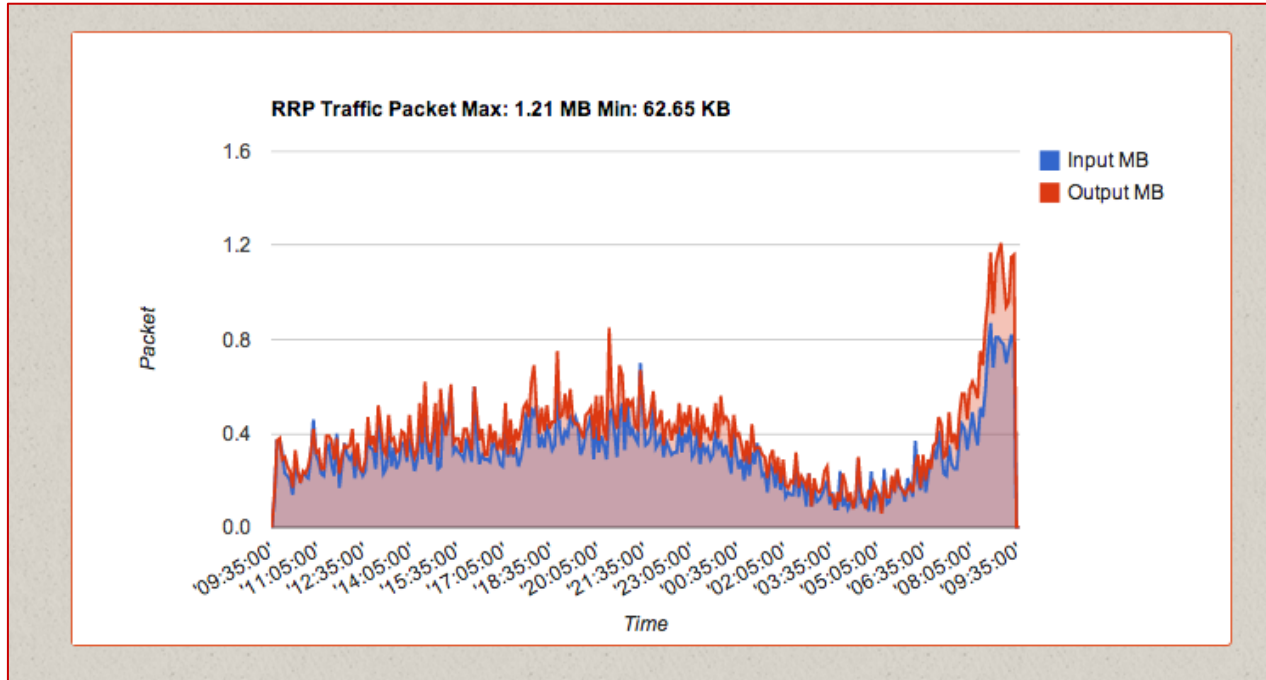
Day Week Month Year

RRP Interface Graphs by Day



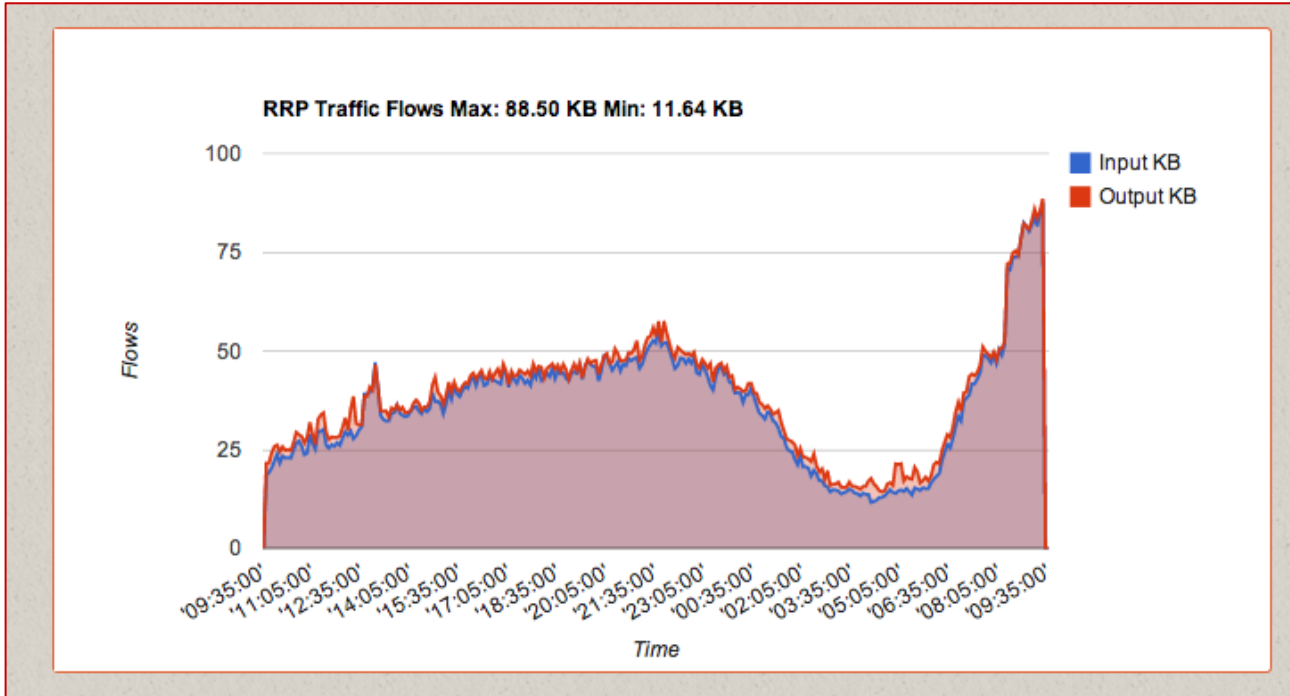
- Octets

By Netlabel: RRP



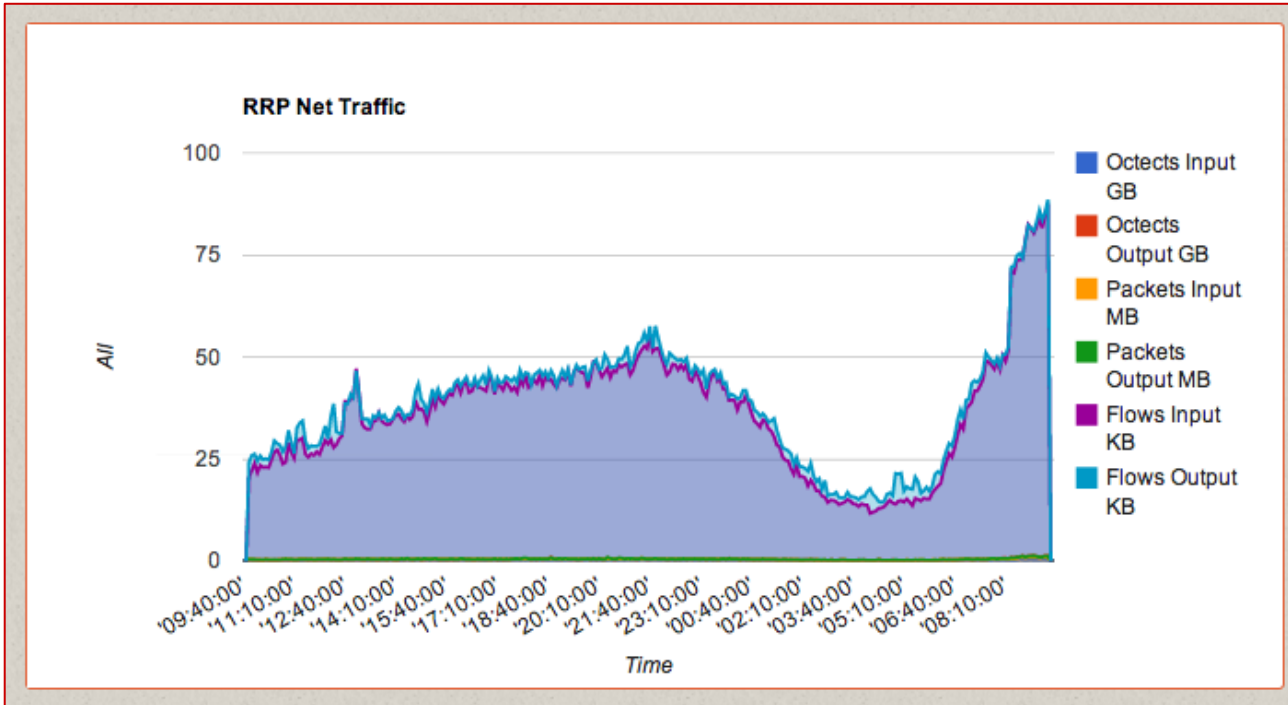
- Octets
- Packets

By Netlabel: RRP



- Octets
- Packets
- Flows

By Netlabel: RRP



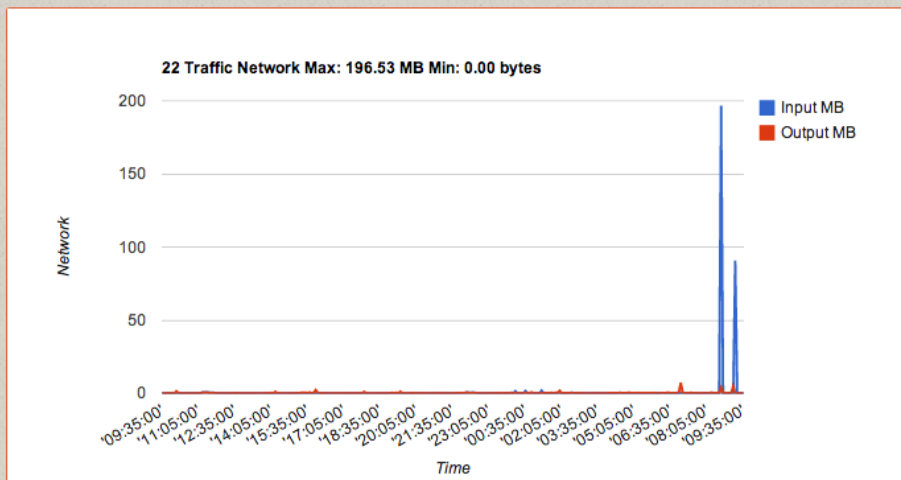
- Octets
- Packets
- Flows
- Combined

By Netlabel: RRP, port 22 (ssh)



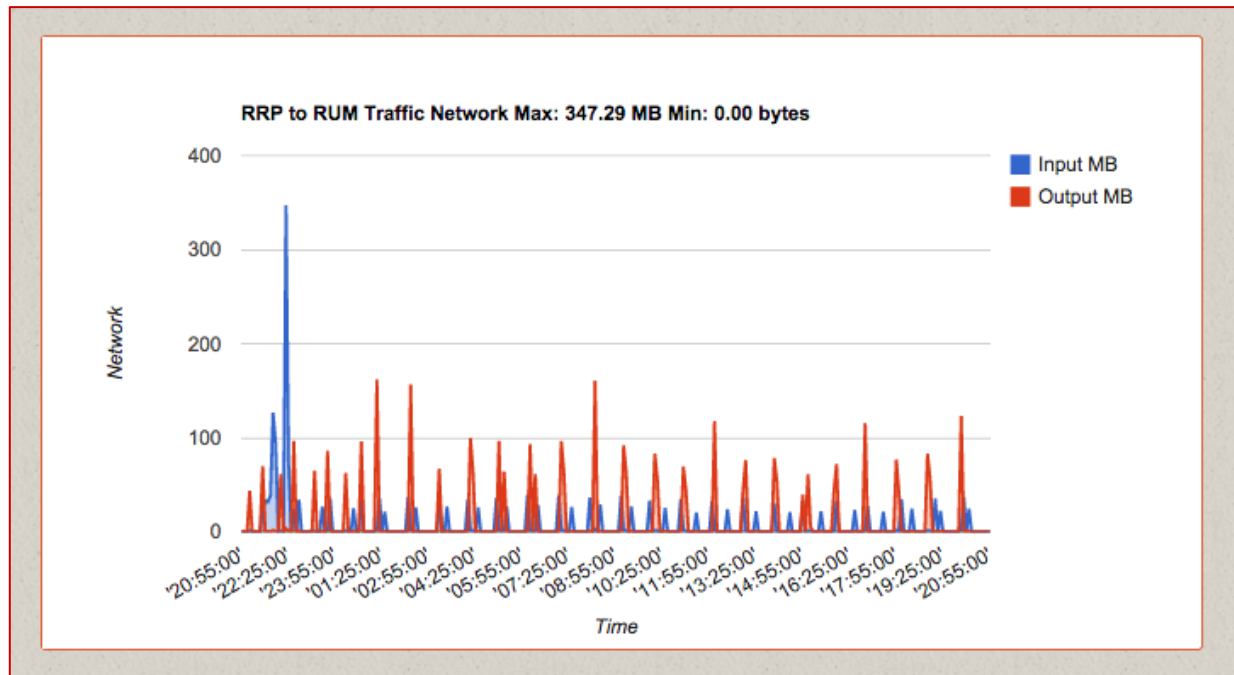
Day Week Month Year

RRP Port 22 Graphs by Day



- Octets
- Packets
- Flows
- Combined

From Netlabel 2 Netlabel



- Octets
- Packets
- Flows
- Combined

Custom Query Interface



Custom Graph Query

RRP

- I/O: The general amount of traffic in this network
- Port: The traffic of a specific port
- P2P: Traffic from one point in the network to another

22

2014-03-13 12:29:00 2014-03-12 12:29:00

Query

2.0
1.5

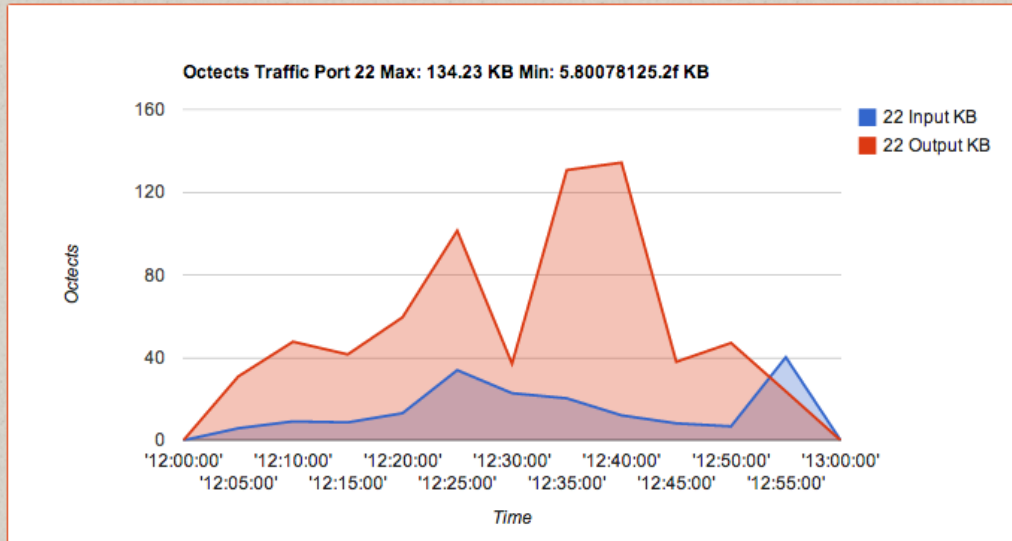
Input GB
Output GB

- Graphs data from any time interval.
- Has a menu where user chooses what to visualize.
- Menu options generated dynamically to represent contents of the database
- Translates menu choices into queries
- Graphs the results

Custom Query Interface



Custom Query Result



Top 100



Top 100

Flows Octects Packets

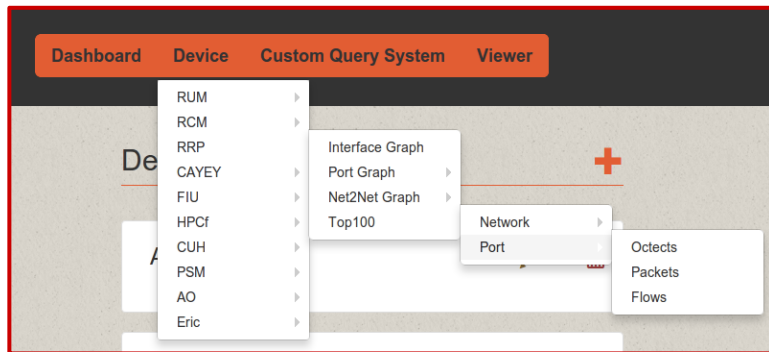
136.145.101.15	72.85-KB	62.37-MB	64.00-bytes
136.145.182.24	161.12-KB	31.32-MB	24.31-KB
136.145.182.21	200.90-KB	20.03-MB	22.76-KB
136.145.138.238	12.87-KB	18.26-MB	11.00-bytes
136.145.185.198	6.34-KB	8.79-MB	1.00-bytes
136.145.180.150	4.22-KB	5.27-MB	594.00-bytes
136.145.87.47	4.54-KB	5.12-MB	574.00-bytes
136.145.180.118	5.68-KB	4.07-MB	29.00-bytes
136.145.182.11	38.37-KB	2.94-MB	5.85-KB
136.145.196.137	3.21-KB	2.92-MB	506.00-bytes
136.145.239.180	17.36-KB	2.67-MB	2.77-KB
136.145.180.200	4.83-KB	2.56-MB	821.00-bytes
136.145.239.179	24.30-KB	2.50-MB	3.34-KB
136.145.180.154	1.91-KB	2.23-MB	495.00-bytes

The screenshot shows the Toa web interface with a navigation bar containing "Dashboard", "Device", "Custom Query System", and "Viewer". A dropdown menu is open under "Device", listing various devices: RUM, RCM, RRP, CAYEY, FIU, HPCf, CUH, PSM, AO, and Eric. A sub-menu is open for "CAYEY", showing "Interface Graph", "Net2Net Graph", and "Top100". Another sub-menu is open for "Top100", showing "Network" and "Port". A final sub-menu is open for "Port", showing "Octects", "Packets", and "Flows".

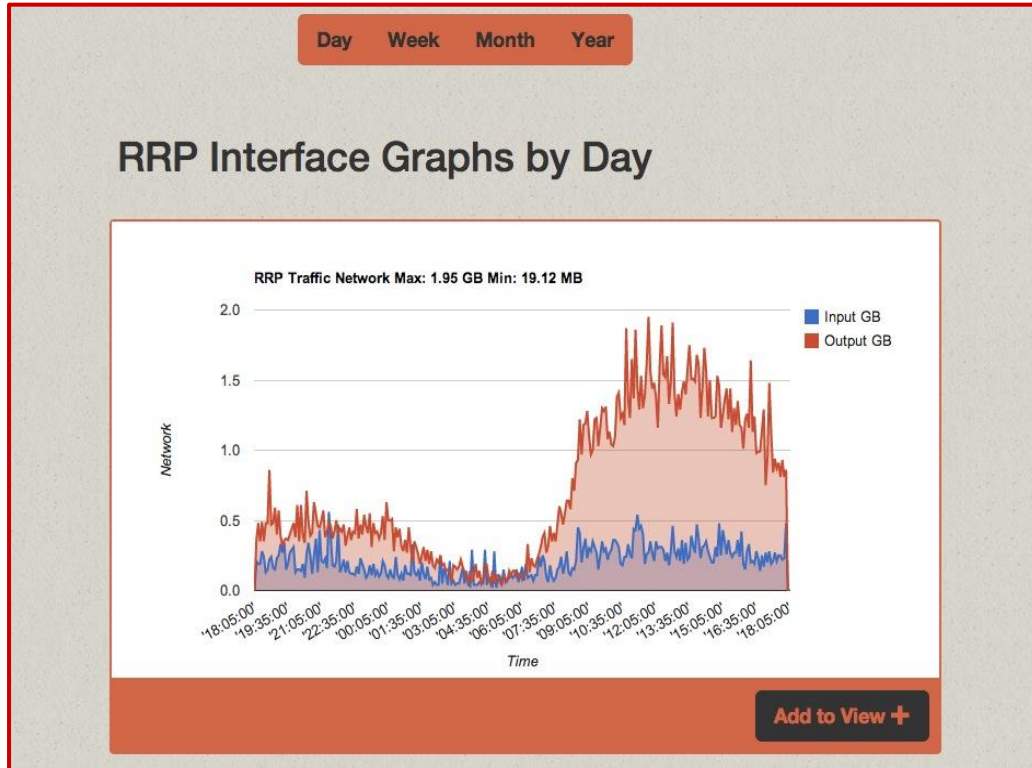
Top 100 ports



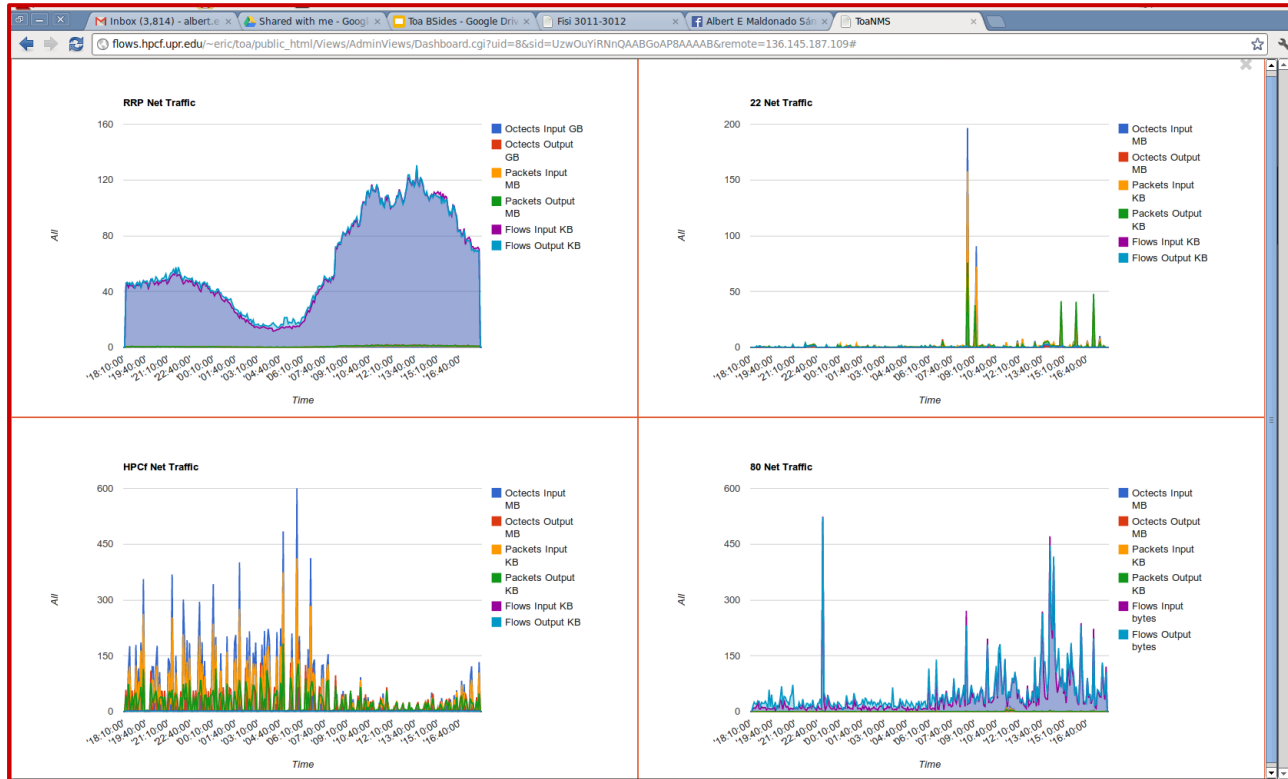
Top 100	Flows	Ocfects	Packets
443	221.50-KB	52.95-MB	41.80-KB
80	359.69-KB	25.40-MB	36.44-KB
49135	15.09-KB	17.49-MB	1.00-bytes
465	9.95-KB	11.73-MB	31.00-bytes
26181	7.54-KB	10.44-MB	2.00-bytes
59040	7.37-KB	8.26-MB	1.00-bytes
5001	3.47-KB	5.09-MB	1.00-bytes
65199	3.54-KB	5.07-MB	1.00-bytes
18514	2.98-KB	4.17-MB	1.00-bytes
50378	2.43-KB	3.36-MB	2.00-bytes
35765	1.46-KB	2.00-MB	1.00-bytes
41130	1.28-KB	1.86-MB	1.00-bytes
55443	1.10-KB	1.60-MB	1.00-bytes
28123	1.26-KB	1.51-MB	1.00-bytes
39039	1.94-KB	1.44-MB	2.00-bytes



Views | a panel of graphs



Views | a panel of graphs



Admin Interface



The screenshot shows a web browser window displaying the Toa Network Monitoring System Admin Interface. The browser address bar shows the URL: `flows.hpcf.upr.edu/~eric/toa/public_html/Views/AdminViews/Dashboard.cgi?uid=1&sid=UzBcwYiRNnQAAHZSBukAAAAF&remote=64.237.224.49`. The page title is "Toa Network Monitoring System" and the user is logged in as "cheo@hpcf.upr.edu".

The interface features a navigation menu with the following items: Dashboard, Device, Custom Query System, and Viewer. The "Device" menu item is currently selected.

The main content area is divided into two sections:

- Device List**: A list of devices with edit and delete icons for each.

Device Name	Edit	Delete
AO		
CAYEY		
CUH		
Eric		
- View List**: A list of views with a delete icon for each.

View Name	Delete
FirstView TestView	

Admin Interface



Toa Network Monitoring System

eric.leinad92@gmail.com ▾

Dashboard Device Custom Query System Viewer

<input type="text" value="Network Label"/>	<input type="text" value="Interface"/>
<input type="text" value="I/F Interface Id"/>	<input type="text" value="AS AS Number"/>
<input type="text" value="Min Bytes Size"/>	<input type="text" value="Max Bytes Size"/>

Add Network

Admin Interface



Toa Network Monitoring System

eric.leinad92@gmail.com ▾

Dashboard Device Custom Query System Viewer

Device Port Net2Net NetBlock

📁	RRP	As	▾
I/F	55	AS	65003
↓	None	↓	None

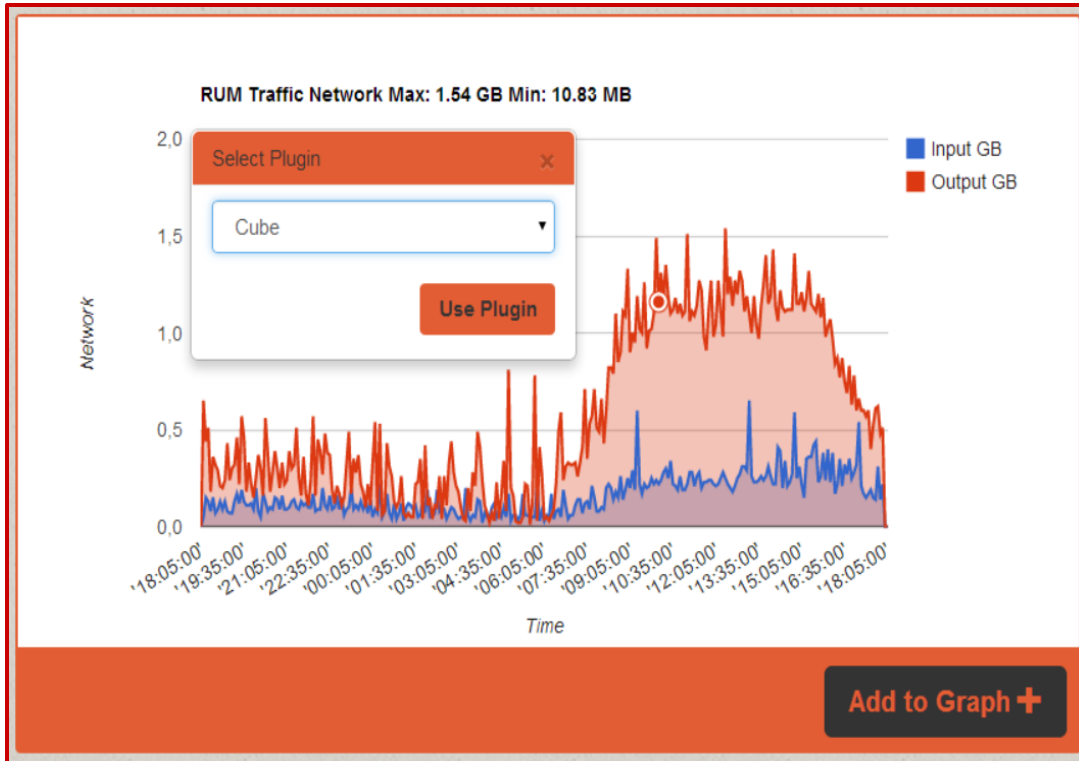
Save Network

Plugins



- Represent flow data events through different visualizations.
- Easy access.
- Currently two implemented plugins
 - Cube
 - Undirected Graph

Graph Events



- A dialog generated when the user clicks a time point.

Cube

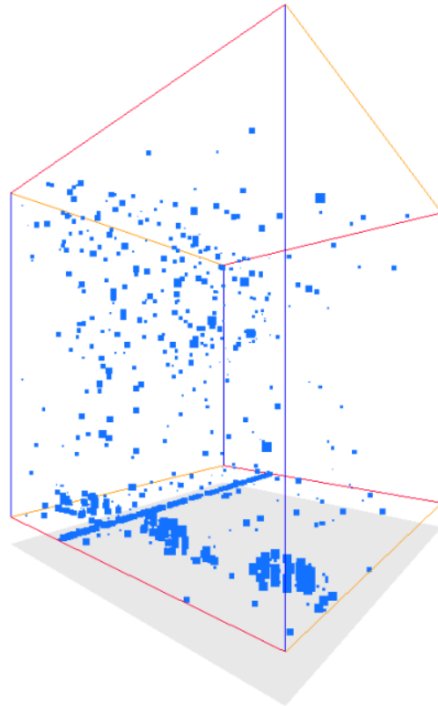


- A three dimensional visualization based on the reimplementation of the Spinning Cube of Potential Doom.
- Uses WebGL and Three.js
- Controls - Options to find flows and filter data. Rotate the cube and change axis colors.
- Threats such as network and port scan can be detected.

Cube Example



-  X Axis
-  Y Axis
-  Z Axis



Settings

HIDE MENU

Flow Info

Flow Date:

Time:

Filter Connections

/24 ▾

/16 ▾

Threshold

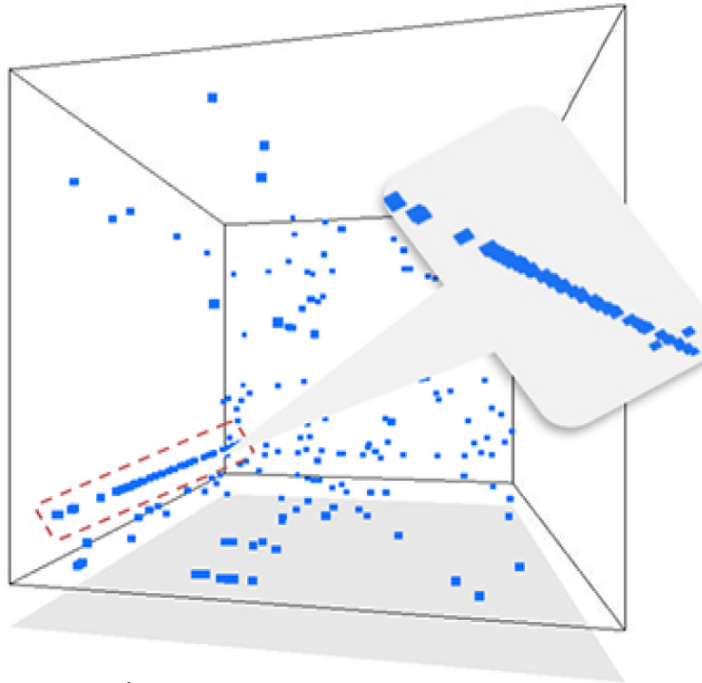
Octets ▾ MB ▾

X: RED ▾

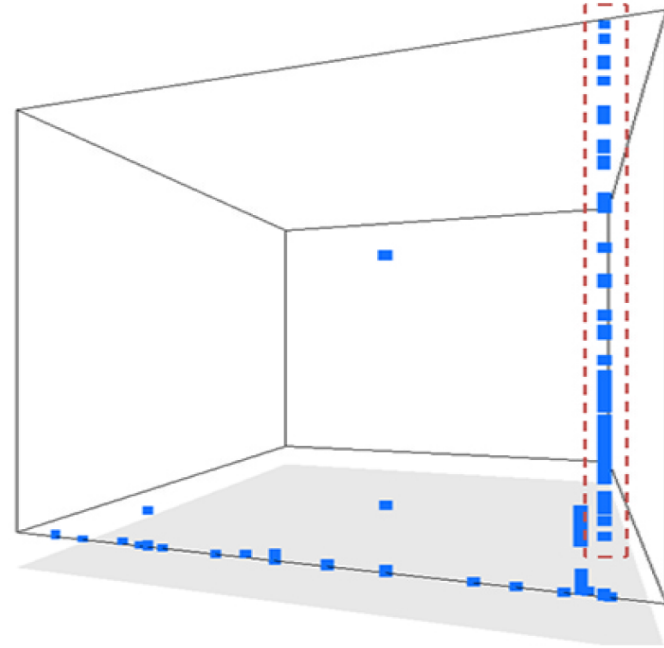
Y: BLUE ▾

Z: ORANGE ▾

Possible Threats Example



Network scan



Port scan

Undirected Graph



- Visualization of source and destination IP through an undirected graph.
- JavaScript Infovis Toolkit.
- Controls - Options to find flows and filter data. Zoom in and out to the graph and interact with nodes.
- Possible attempts of denial of services could be detected.

Graph Example

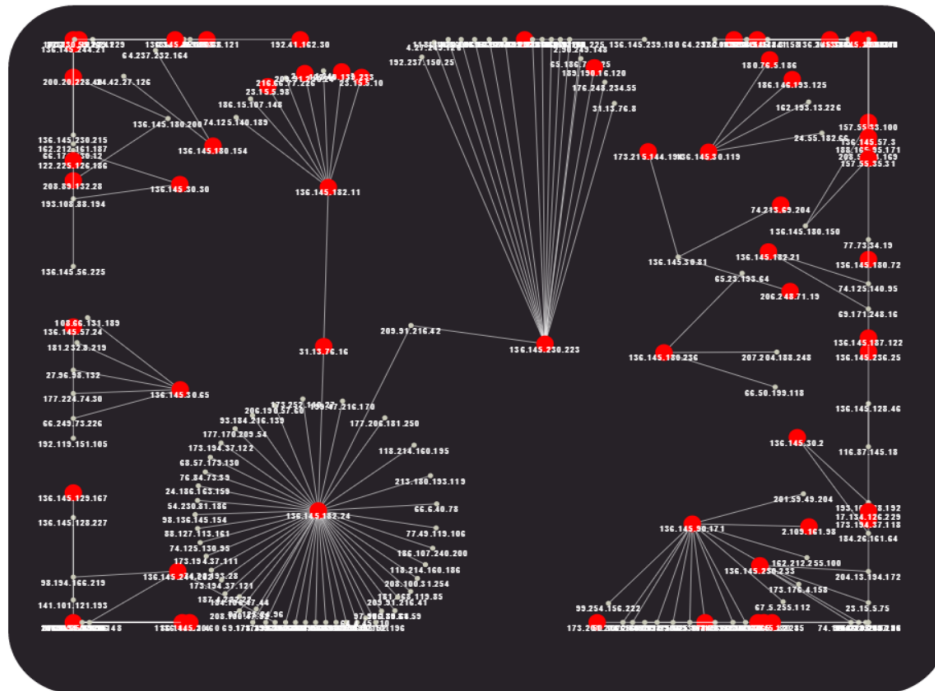


Ip address: 136.145.230.223

Connected to:

- 2.90.249.148
- 65.186.73.125
- 96.16.98.72
- 31.13.76.8
- 173.252.100.27
- 118.214.160.115
- 192.237.150.25
- 118.214.160.184
- 4.27.249.126
- 17.167.195.42
- 118.214.160.81
- 118.214.160.122
- 118.214.160.225
- 96.16.98.78
- 108.160.162.114
- 209.91.216.42
- 176.248.234.55
- 189.190.16.120

Force Directed Static Graph



Settings

Flow Date:

Time:

Connections Filter:

Source IP ▼

Destination IP ▼

References:



- Dave Plonka. Flowscan: A network traffic flow reporting and visualization tool. In USENIX LISA, pages 305-317, 2000.
- A.Oslebo. Stager – A Generic Tool for Presenting Network Statistics http://www.cert.org/flocon/2010/presentations/Oslebo_Stager.pdf
- Joe Loiacono, FlowViewer Maintaining NASA’s Earth Science Traffic Situational Awareness, <http://www.cert.org/flocon/2013/presentations/loiacono-joe-flowviewer.pdf>
- Bearavolu et al., NVisionIP: An Animated State Analysis Tool for Visualizing NetFlows <http://www.cert.org/flocon/2005/presentations/Bearavolu-NVisionIP-FloCon2005.pdf>.
- Taylor et al. Flovis, Security Visualizations with FloVis. http://www.cert.org/flocon/2009/presentations/Taylor_FloVis.pdf
- Phil Groce, The Rayon Tools: Visualization at the Command Line http://resources.sei.cmu.edu/asset_files/Poster/2014_020_001_300465.pdf
- Paul Krystosek, Visualization of Network Flow Data http://resources.sei.cmu.edu/asset_files/Poster/2014_020_001_300460.pdf



Questions?

Thank you!