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

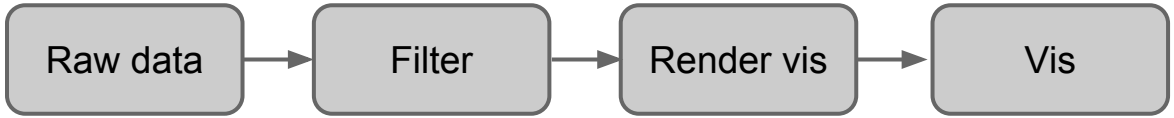
- FlowScan
- NetFlow Sensor (tied to nfdump)
- NVisionIP (FloCon 2005)
- FloVis (FloCon 2009)
- Stager (FloCon 2010)
- FlowViewer (FloCon 2013)
- Rayon & Prism (FloCon 2014)

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.

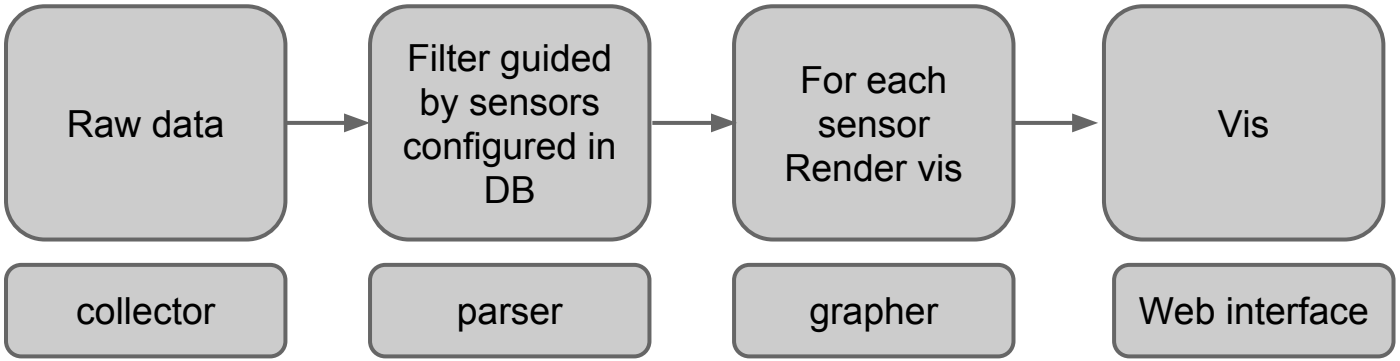
Generic data preparation process

For each sensor:

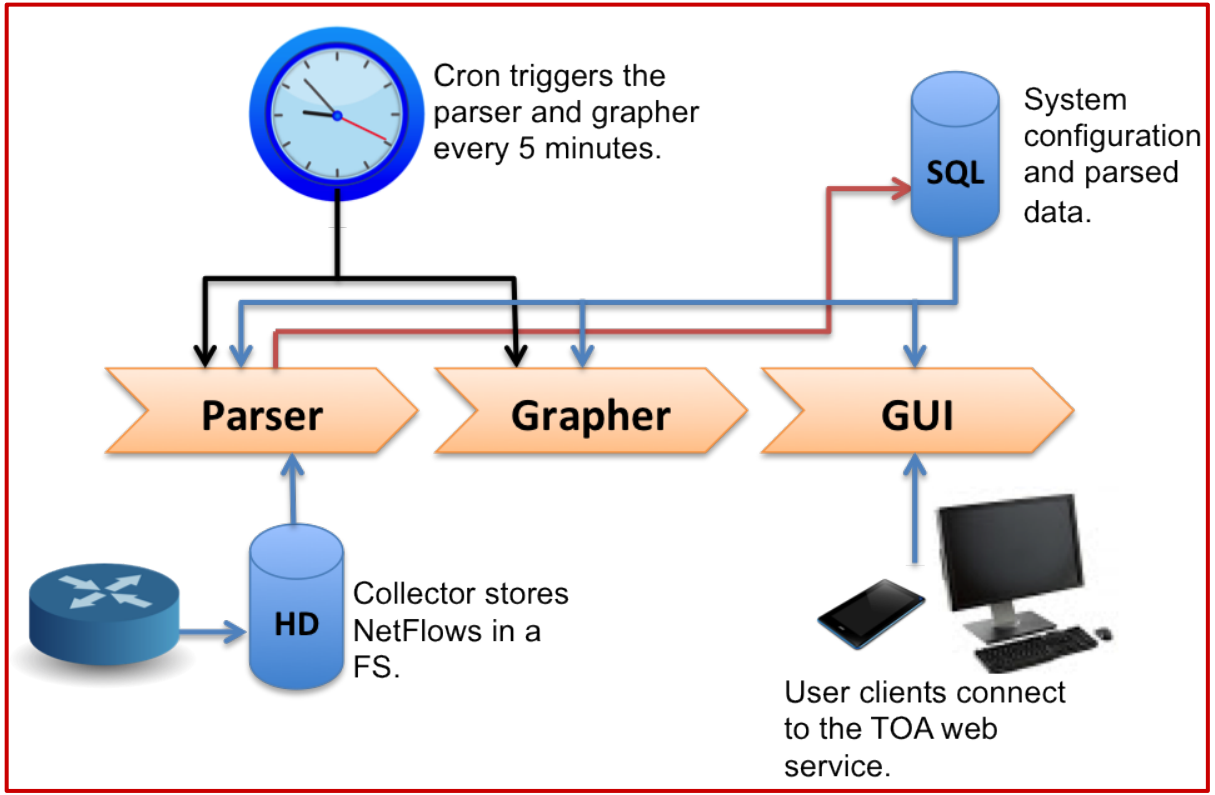


Reference: http://resources.sei.cmu.edu/asset_files/Poster/2014_020_001_300460.pdf

Toa data preparation process



Toa: Overview

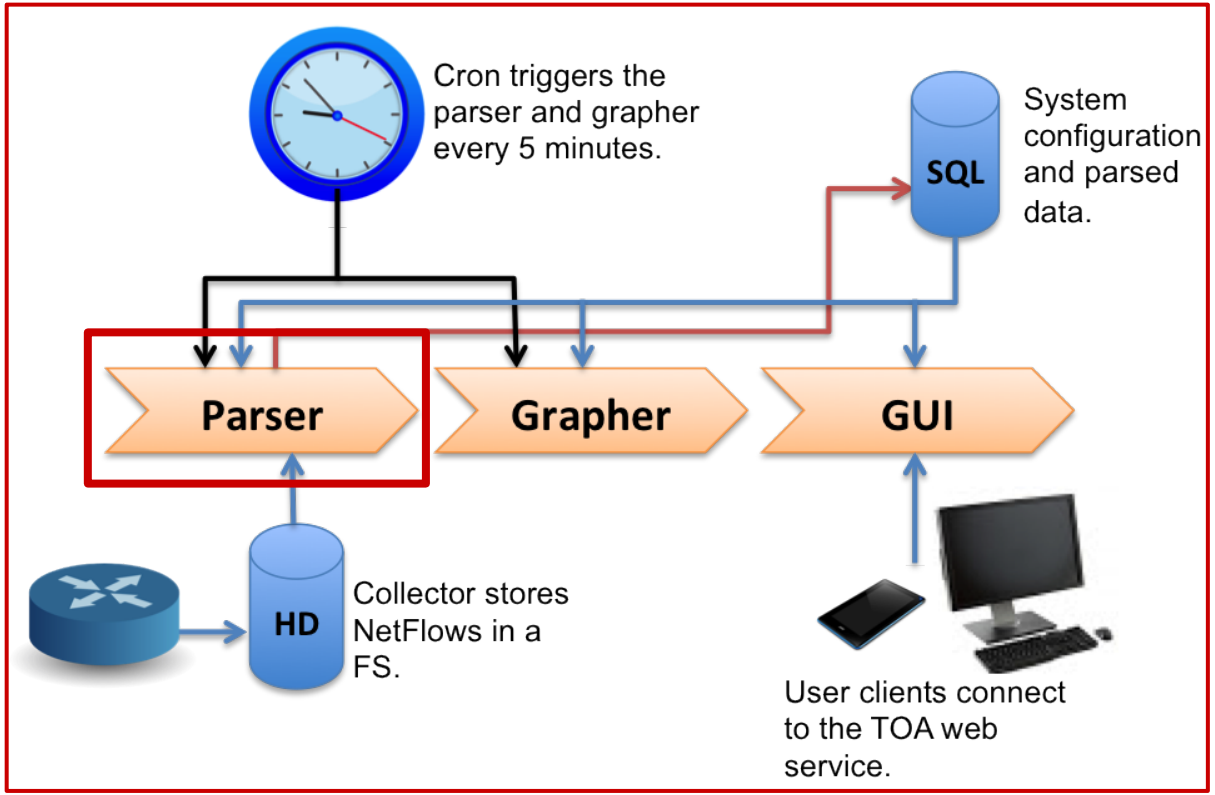


Toa: Dictionary

- 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.

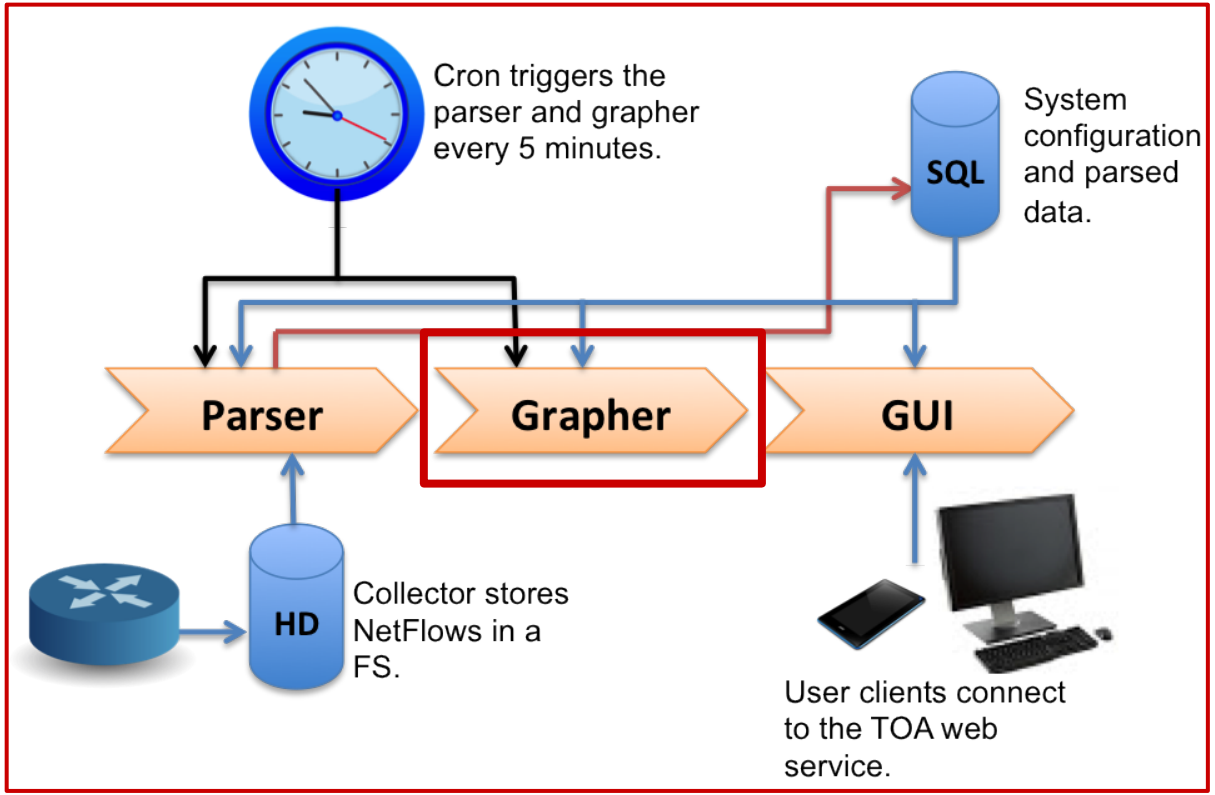
Toa Parser:


Cron triggers the parser and grapher every 5 minutes.
SQL
System configuration and parsed data.
Parser
Grapher
GUI
HD
Collector stores NetFlows in a FS.
User clients connect to the TOA web service.

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)

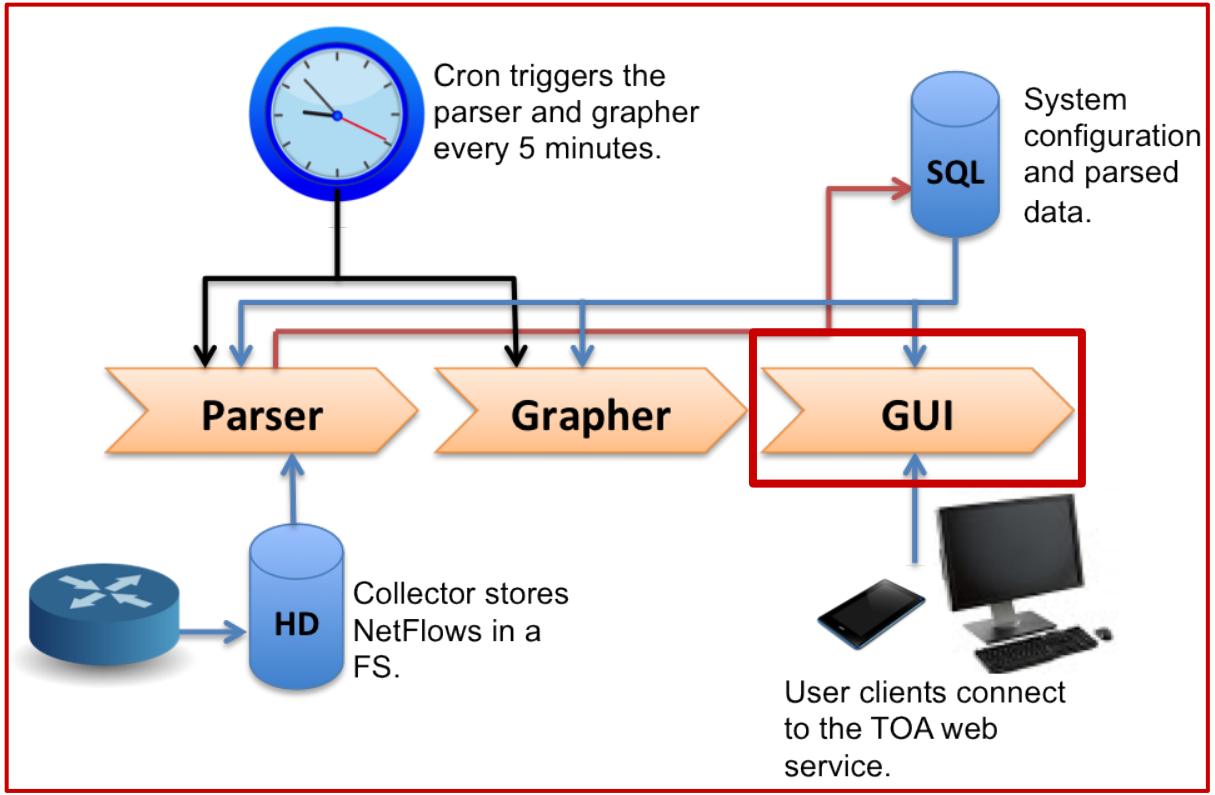
Toa: Grapher:


Cron triggers the parser and grapher every 5 minutes.
SQL
System configuration and parsed data.
Parser
Grapher
GUI
HD
Collector stores NetFlows in a FS.
User clients connect to the TOA web service.

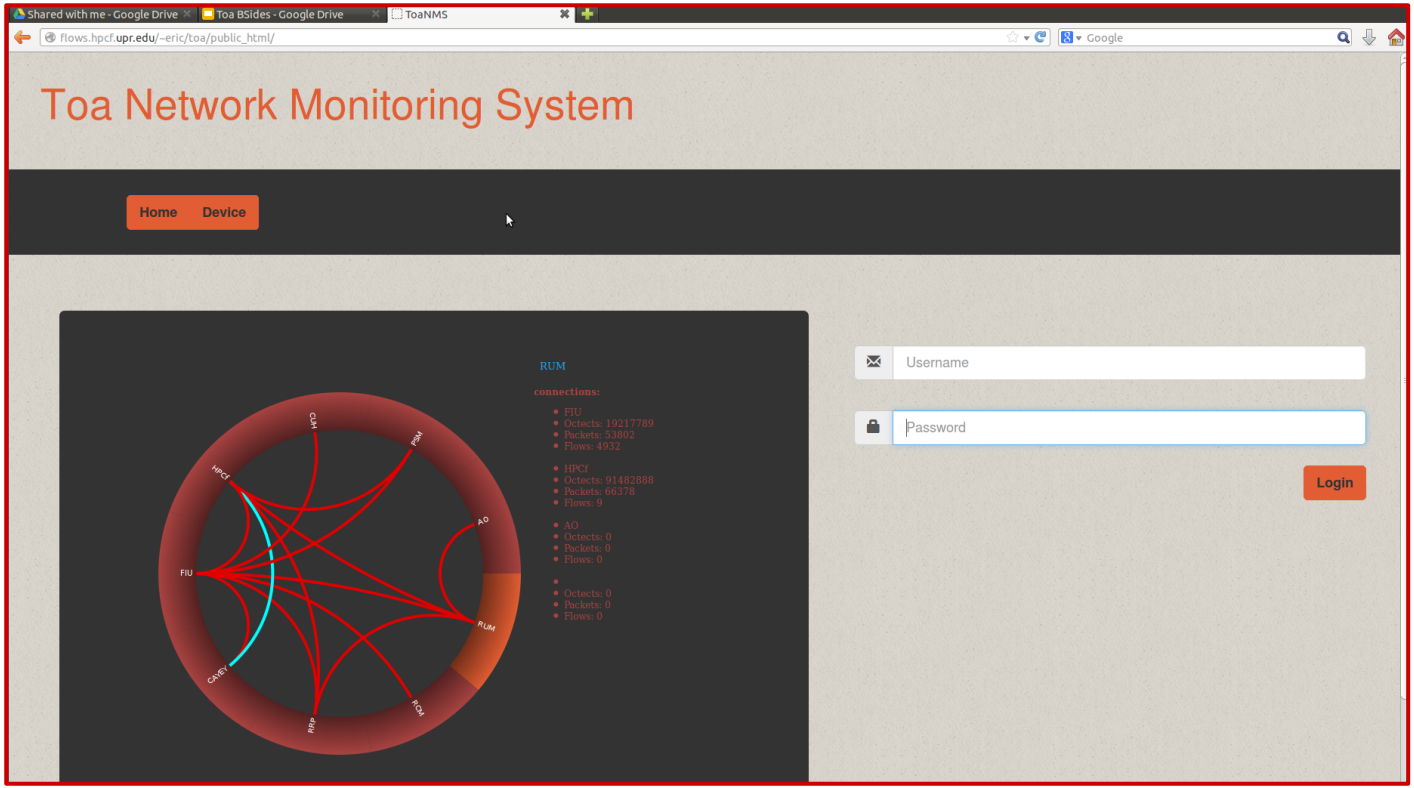
Toa Grapher

- 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.

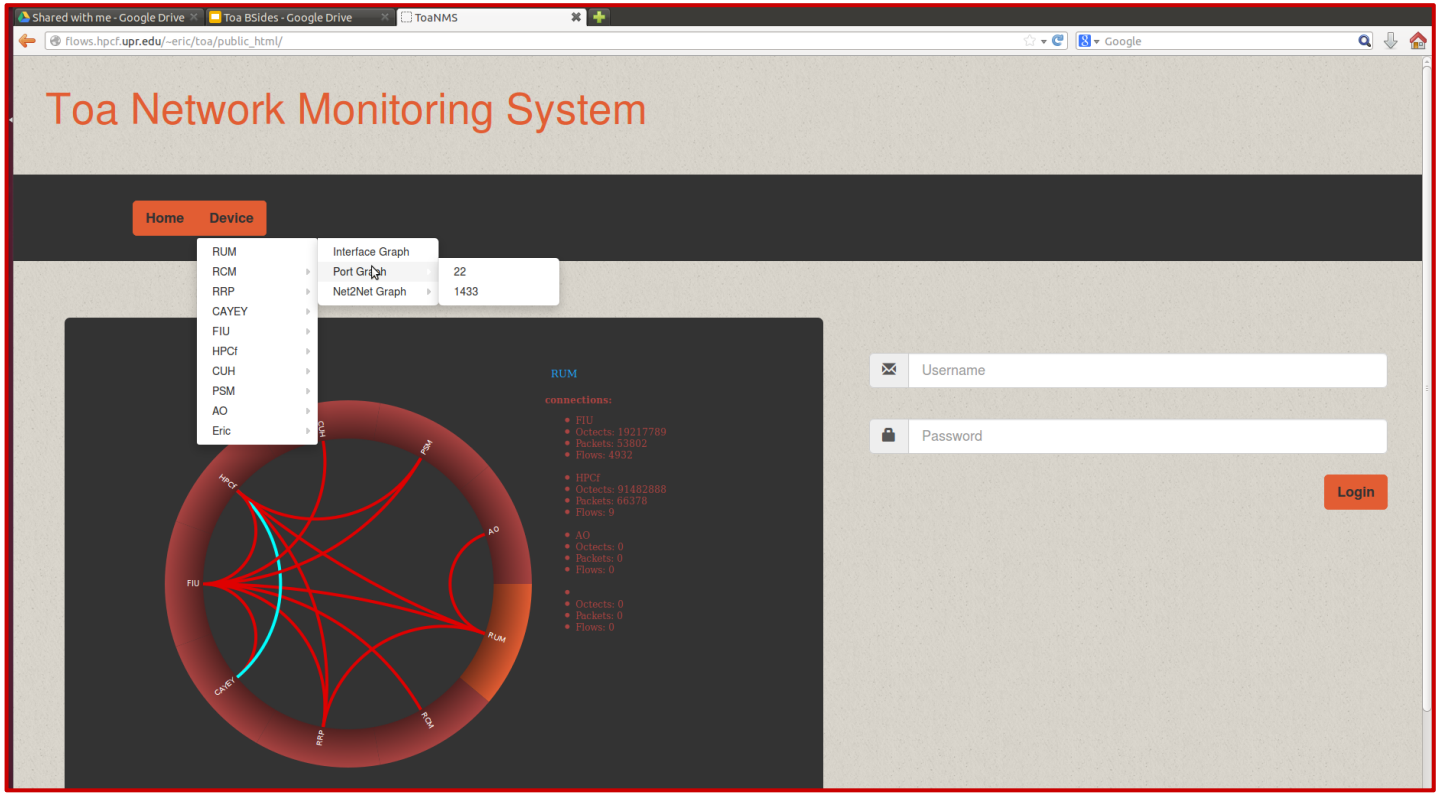
Toa: GUI


Cron triggers the parser and grapher every 5 minutes.
SQL
System configuration and parsed data.
Parser
Grapher
GUI
HD
Collector stores NetFlows in a FS.
User clients connect to the TOA web service.

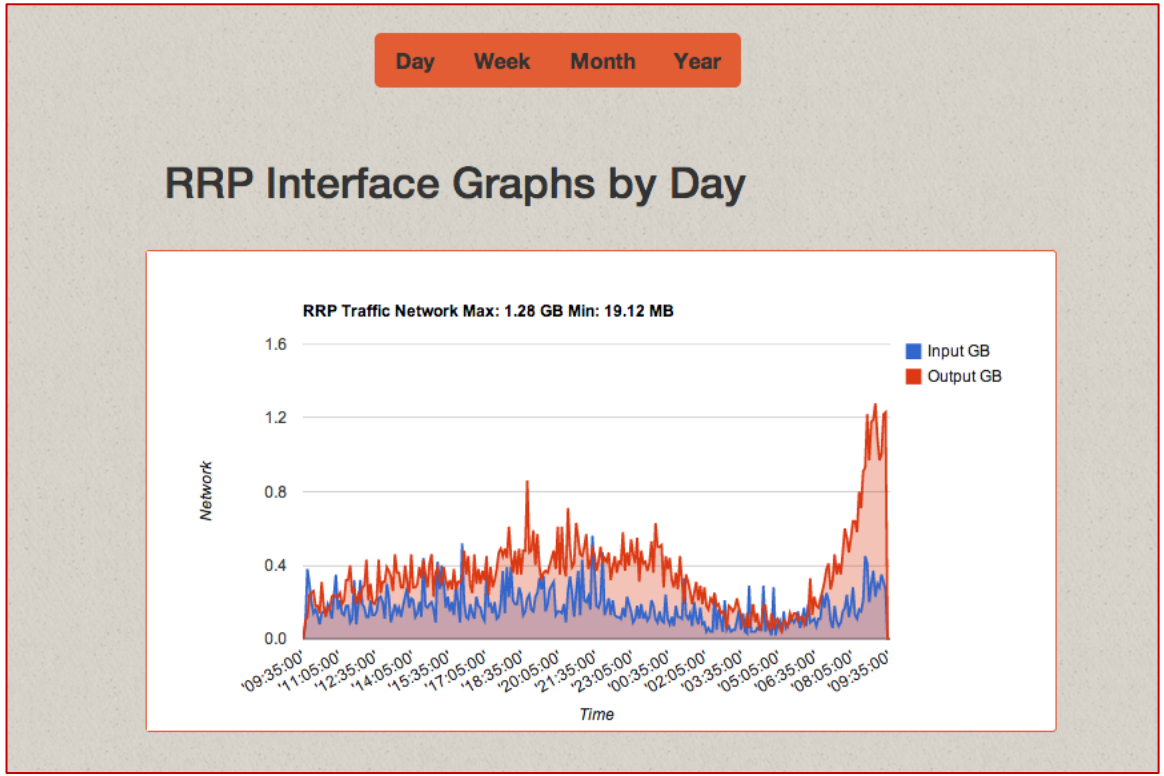
Toa GUI


Shared with me - Google Drive
Toa BSides - Google Drive
ToaNMS
flows.hpcf.upr.edu/~eric/toa/public_html/
Google
Toa Network Monitoring System
Home
Device
RUM
connections:
FIU
Octects: 19217789
Packets: 53802
Flows: 4932
HPCf
Octects: 91482888
Packets: 66378
Flows: 9
AO
Octects: 0
Packets: 0
Flows: 0
Octects: 0
Packets: 0
Flows: 0
CUH
PRM
HPCf
AO
FIU
RUM
CAHEY
PRP
RCM
Username
Password
Login

GUI Menu

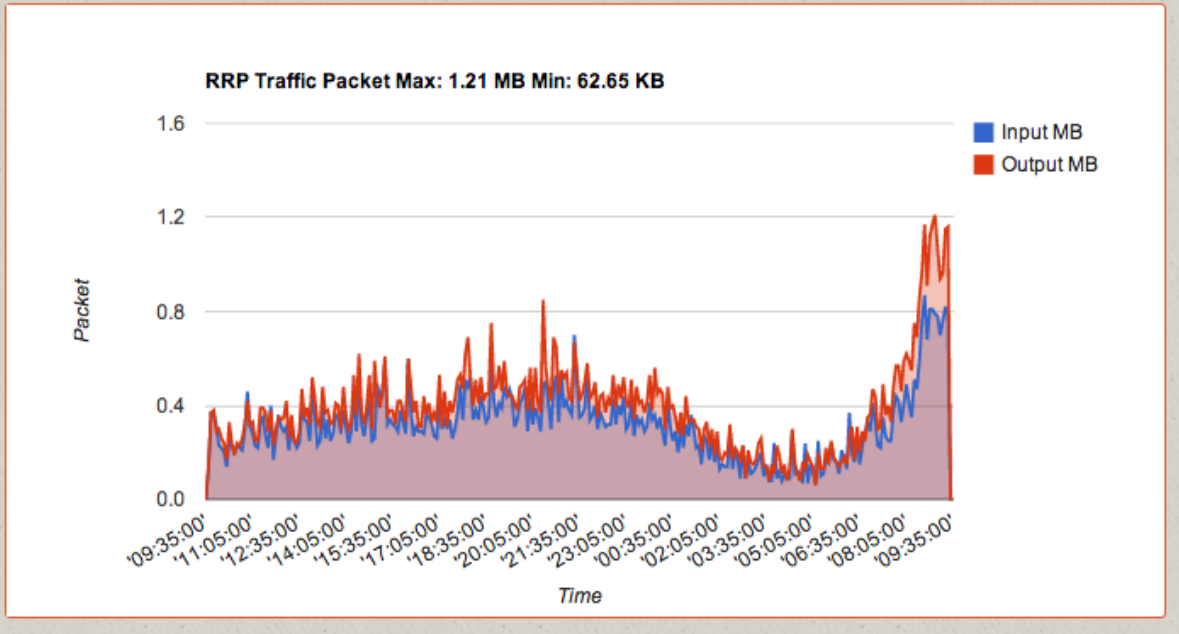

Shared with me - Google Drive
Toa BSides - Google Drive
ToaNMS
flows.hpcf.upr.edu/~eric/toa/public_html/
Google
Toa Network Monitoring System
Home
Device
RUM
RCM
RRP
CAYEY
FIU
HPCf
CUH
PSM
AO
Eric
Interface Graph
Port Graph
Net2Net Graph
22
1433
RUM
connections:
FIU
Octects: 19217789
Packets: 53802
Flows: 4932
HPCf
Octects: 91482888
Packets: 66378
Flows: 9
AO
Octects: 0
Packets: 0
Flows: 0
Octects: 0
Packets: 0
Flows: 0
Username
Password
Login

By Netlabel: RRP



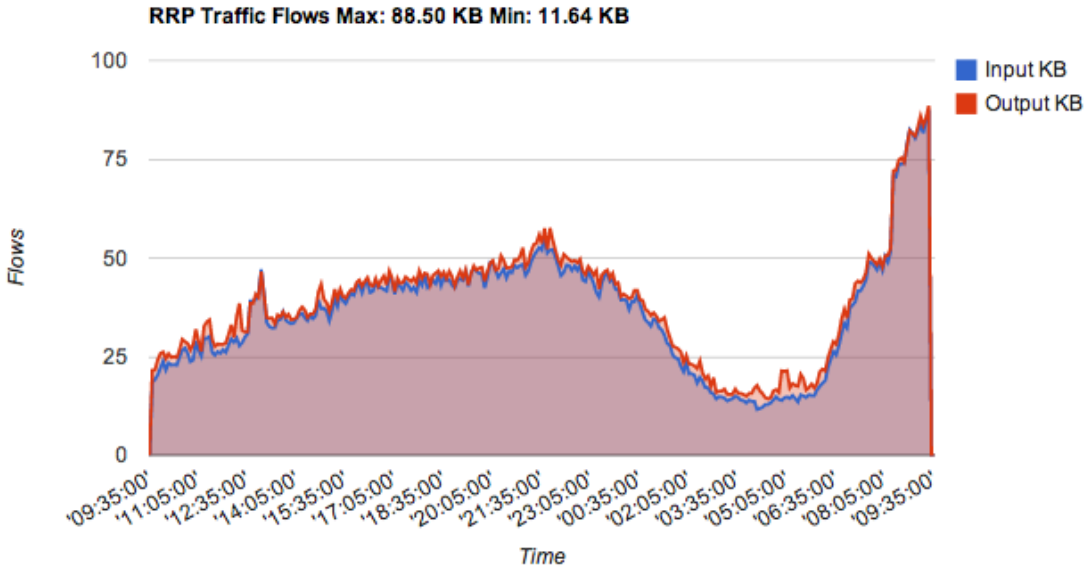
- Octets

By Netlabel: RRP



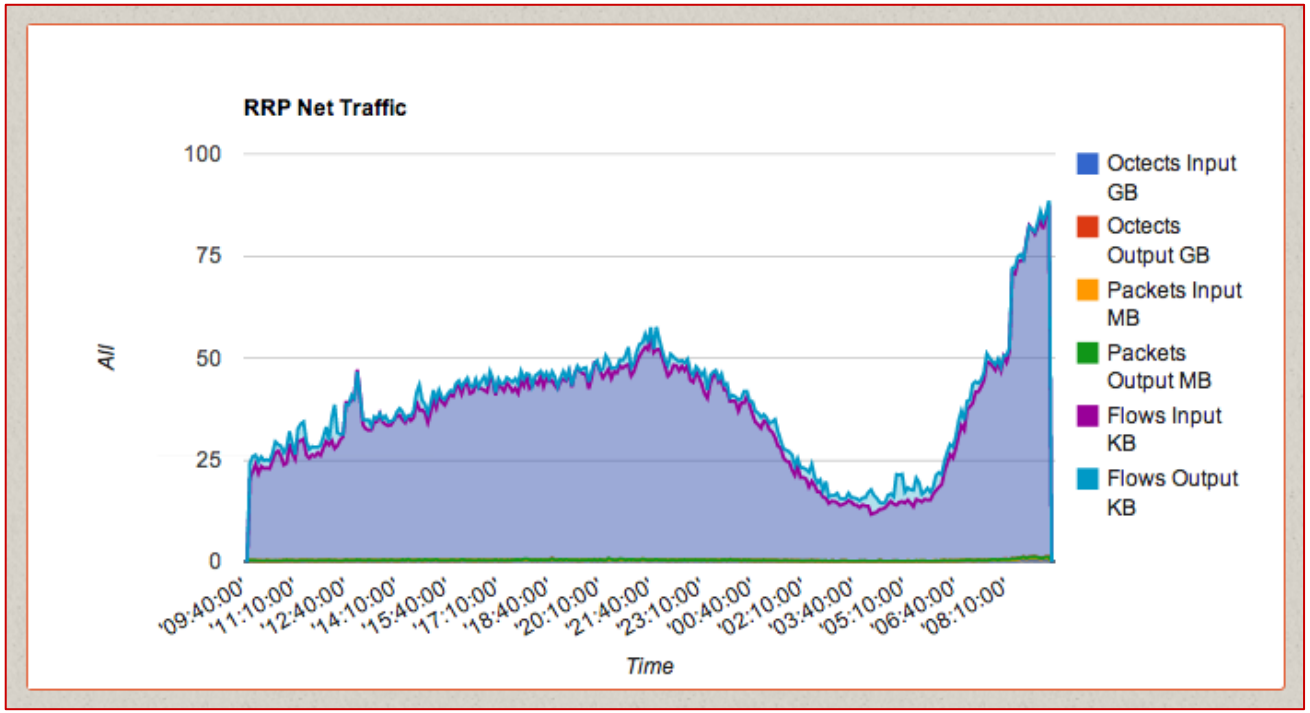
- Octets
- Packets

By Netlabel: RRP



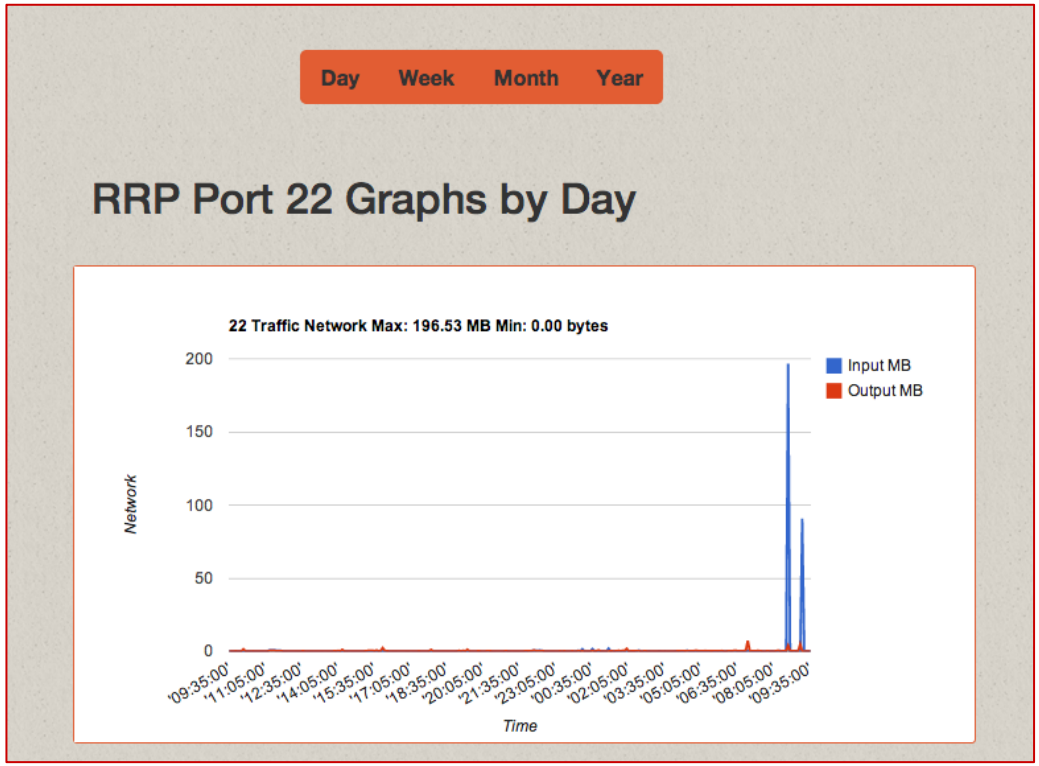
- Octets
- Packets
- Flows

By Netlabel: RRP



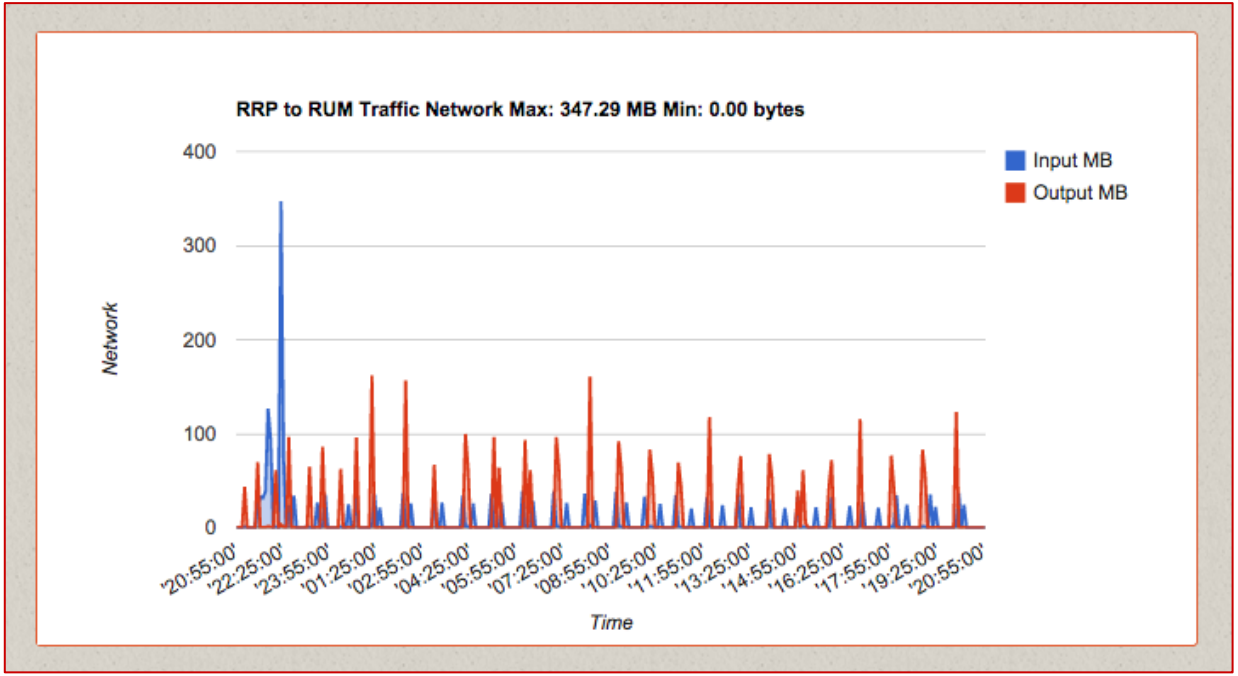
- Octets
- Packets
- Flows
- Combined

By Netlabel: RRP, port 22 (ssh)



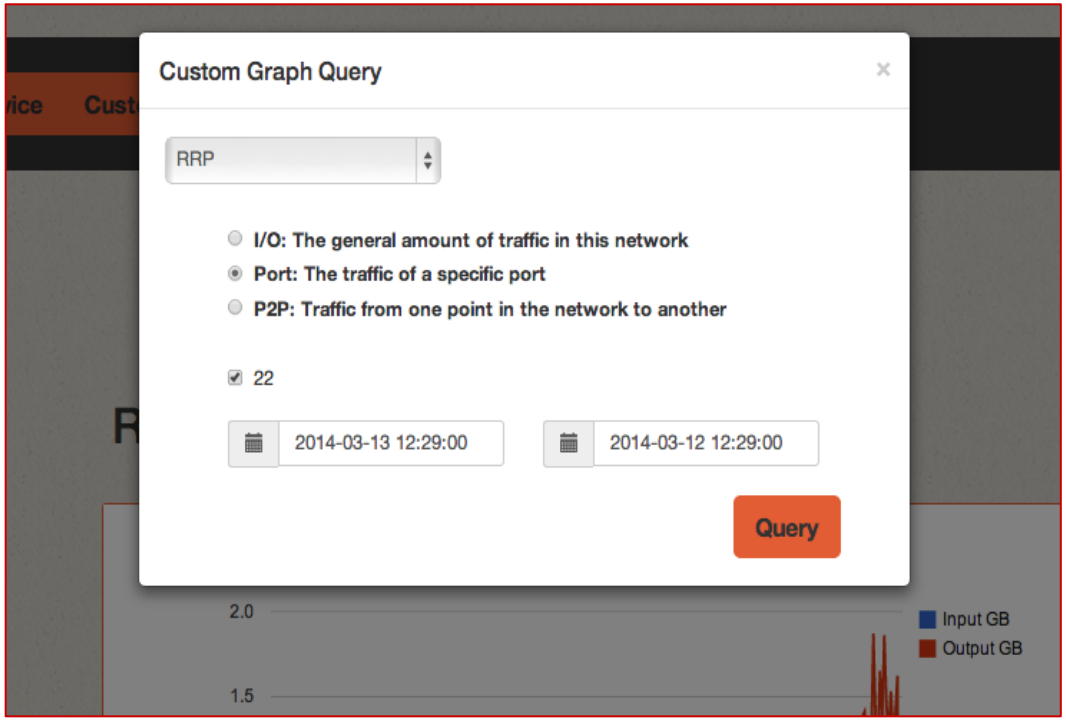
- Octets
- Packets
- Flows
- Combined

From Netlabel 2 Netlabel



- Octets
- Packets
- Flows
- Combined

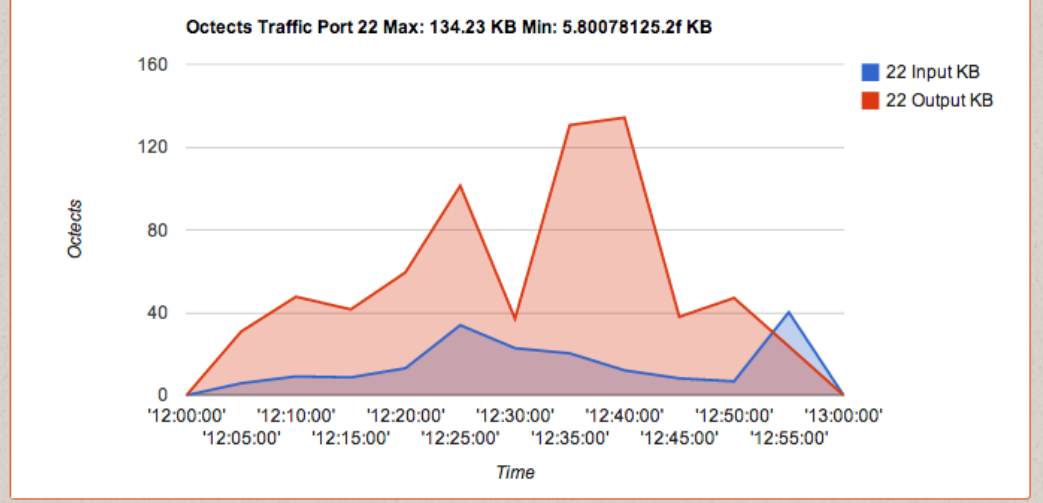
Custom Query Interface



- 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

Qustom Query Interface

Custom Query Result

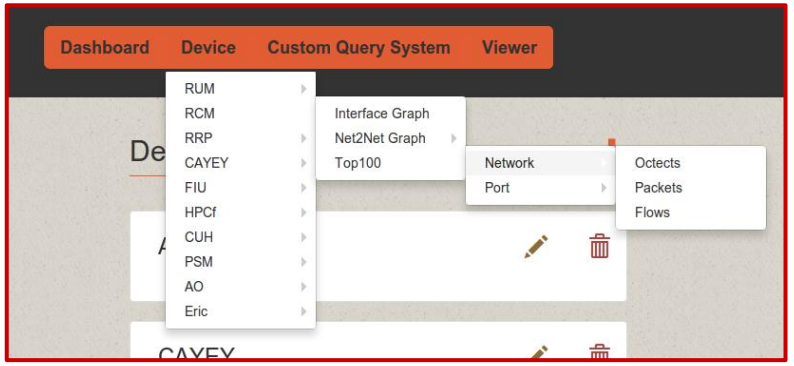


Top 100

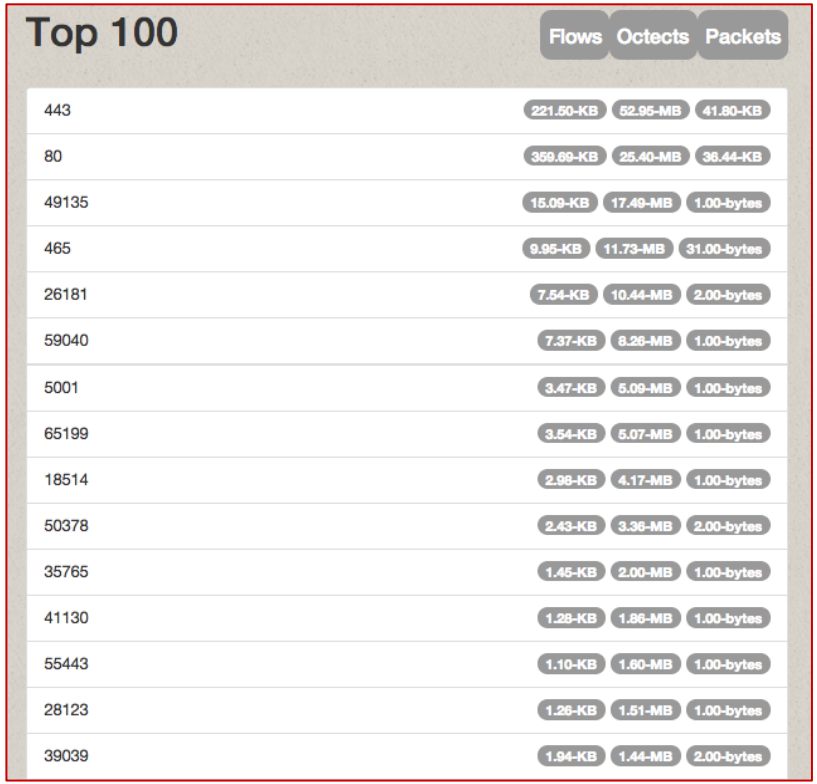
Top 100

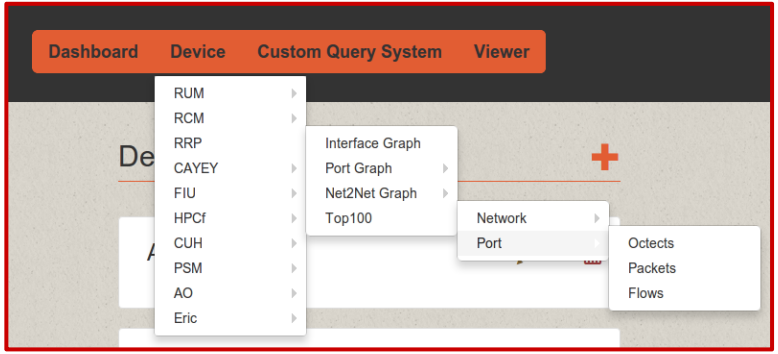
Flows | Octects | Packets

136.145.101.15	72.85-KB	52.37-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

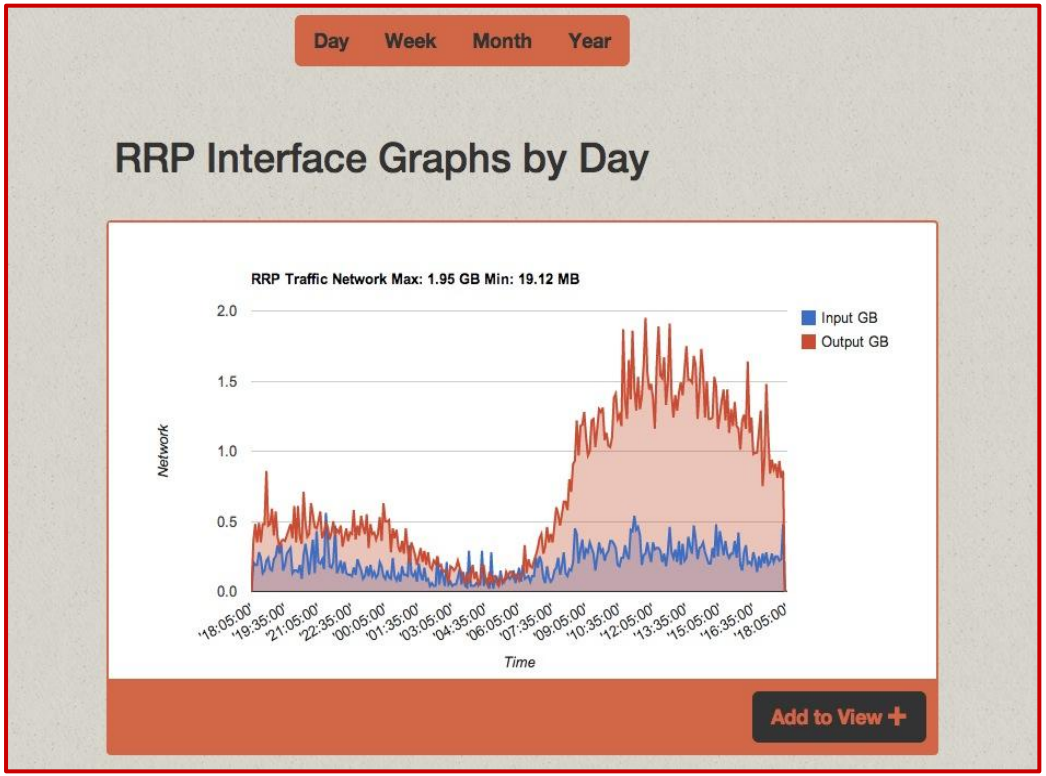


Top 100 ports

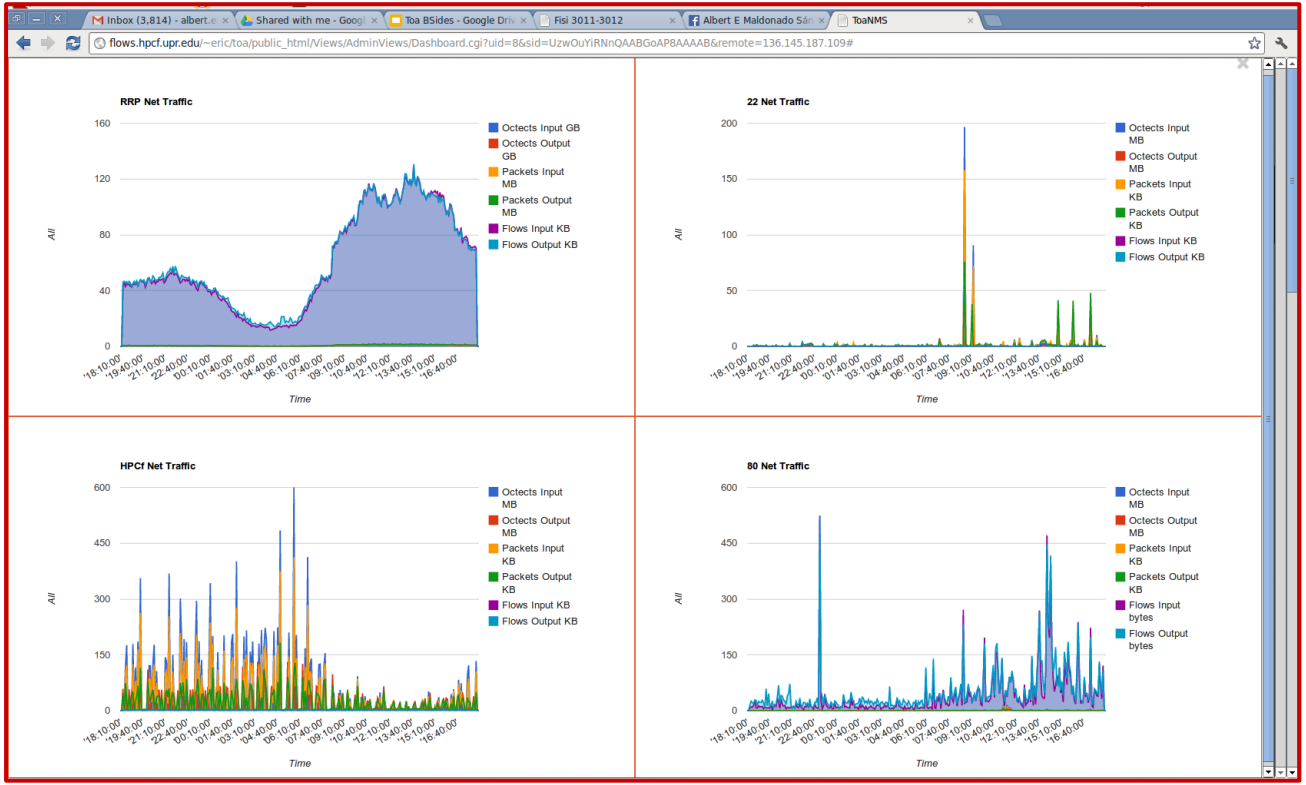




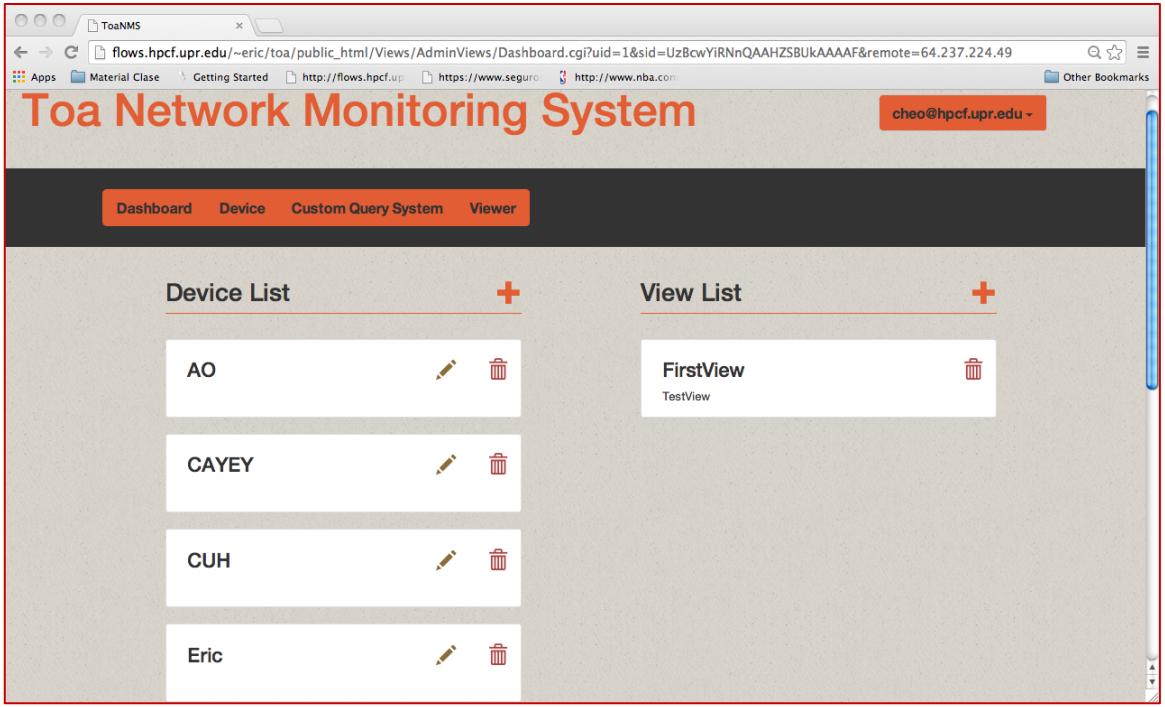
Views | a panel of graphs



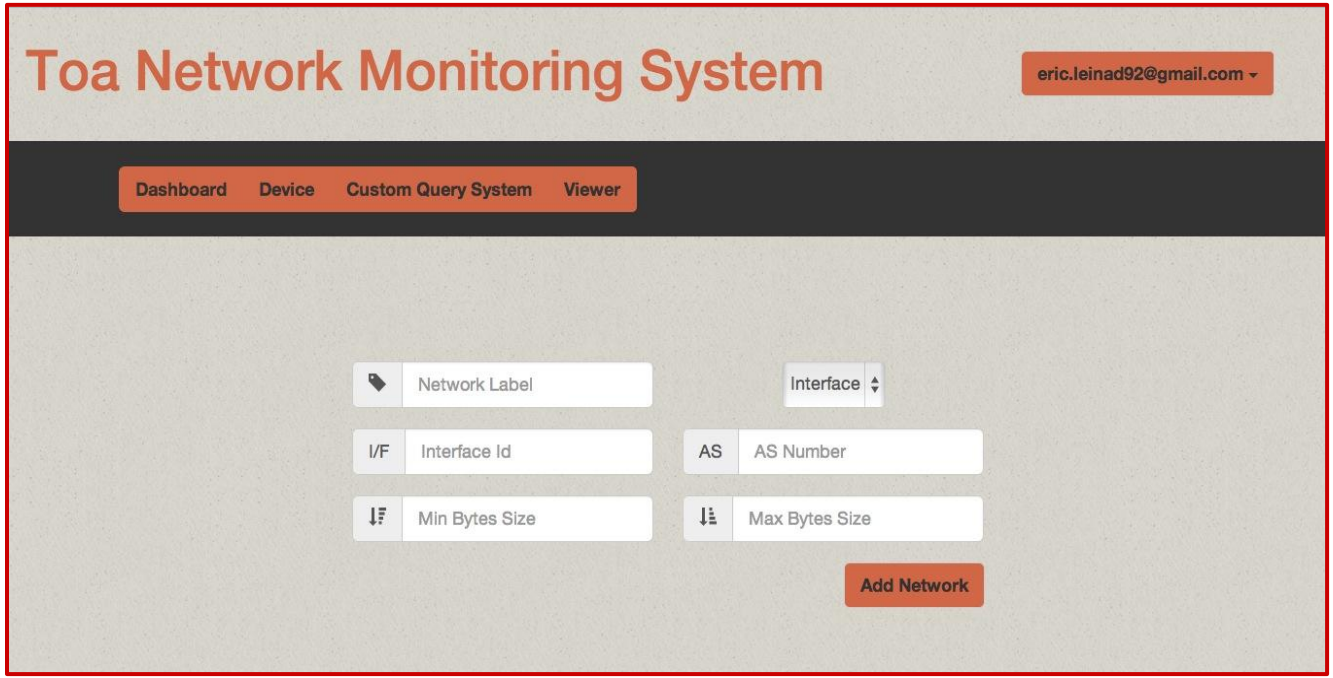
Views | a panel of graphs



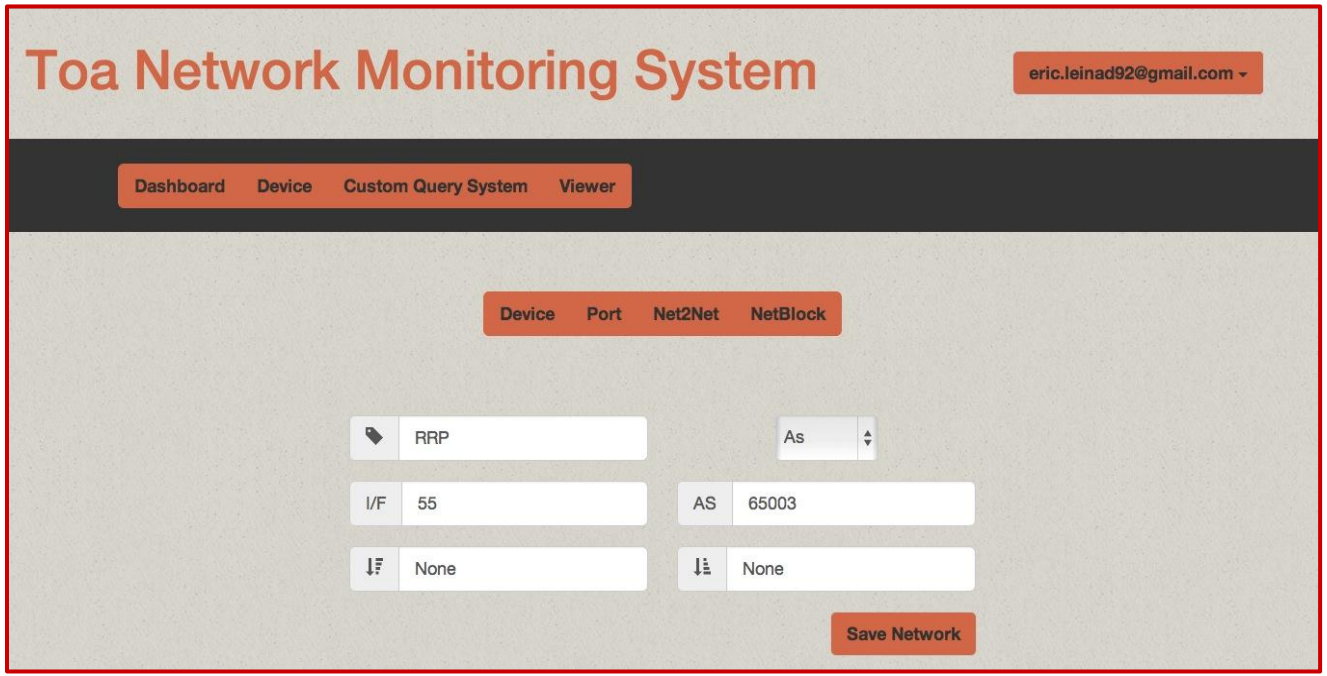
Admin Interface



Admin Interface



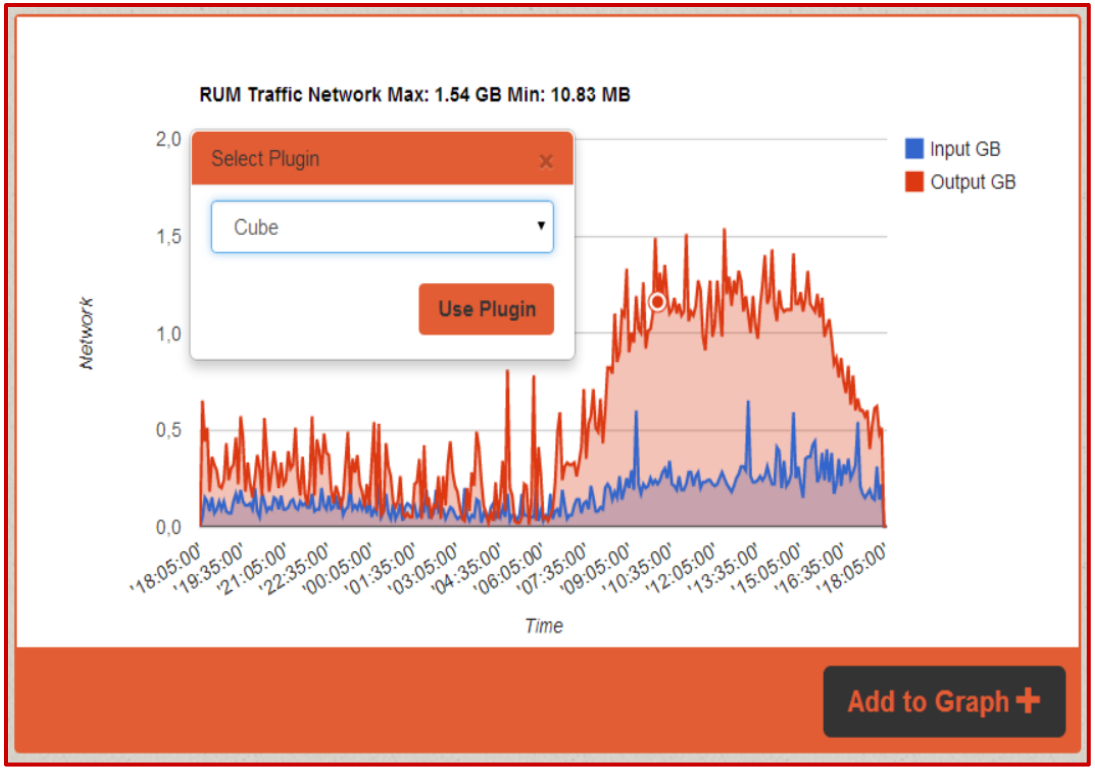
Admin Interface



Plugins

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

Graph Events



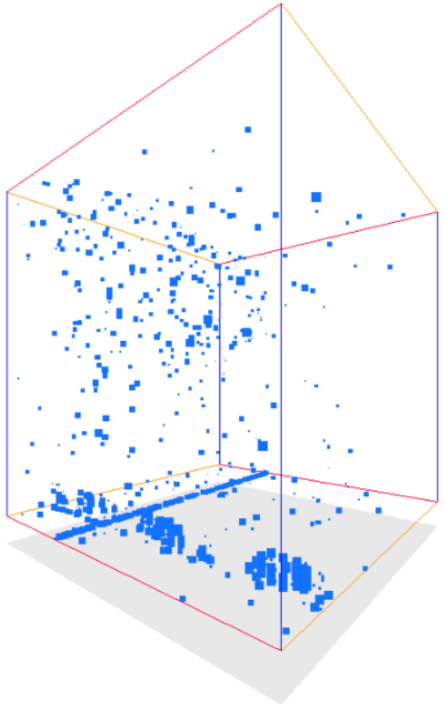
- A dialog generated when the user clicks a time point.

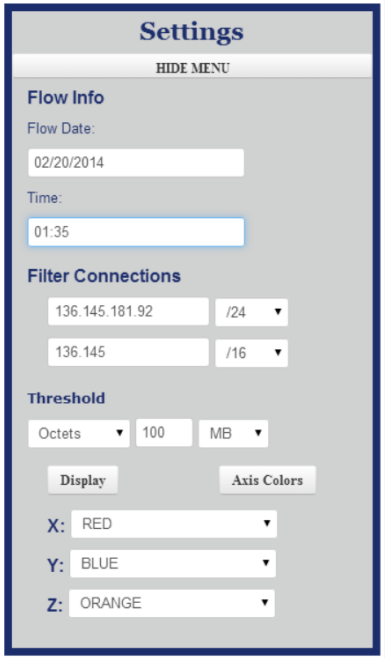
Cube

- 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.

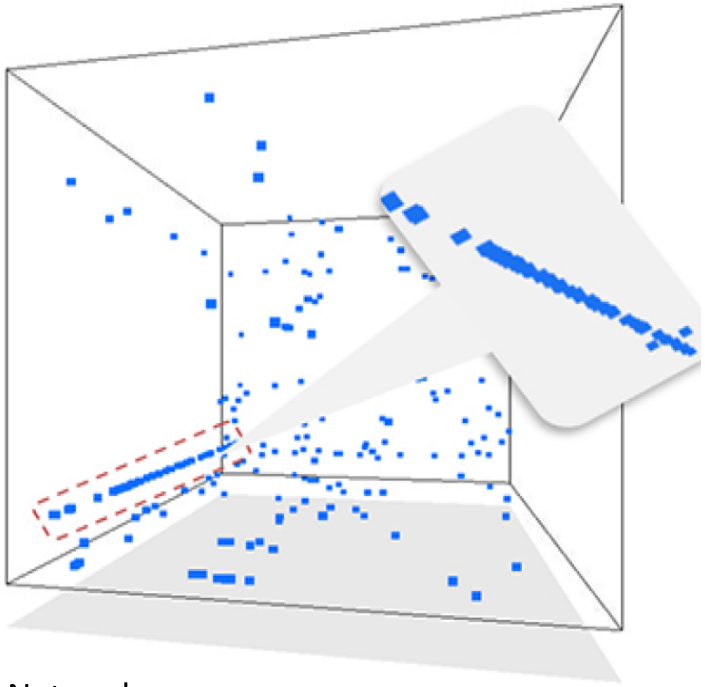
Cube Example

X Axis
Y Axis
Z Axis

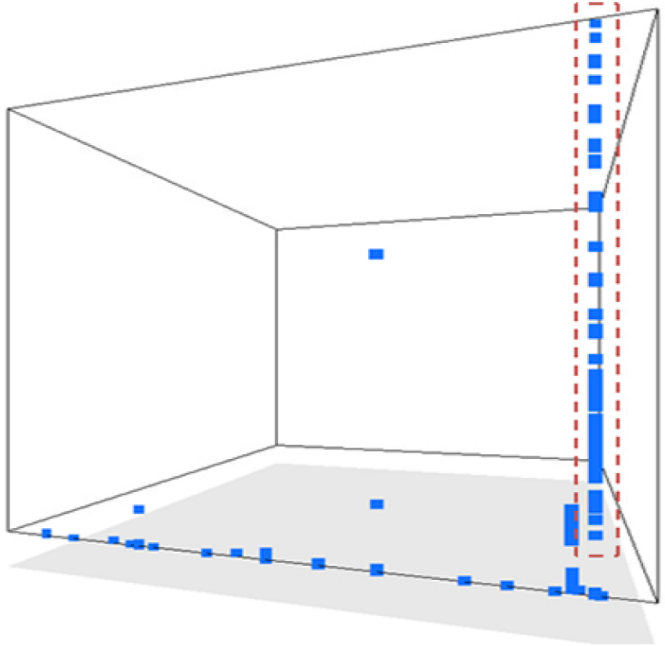




Possible Threats Example



Network scan

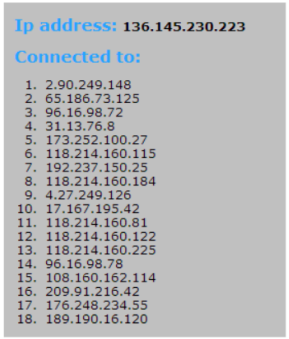


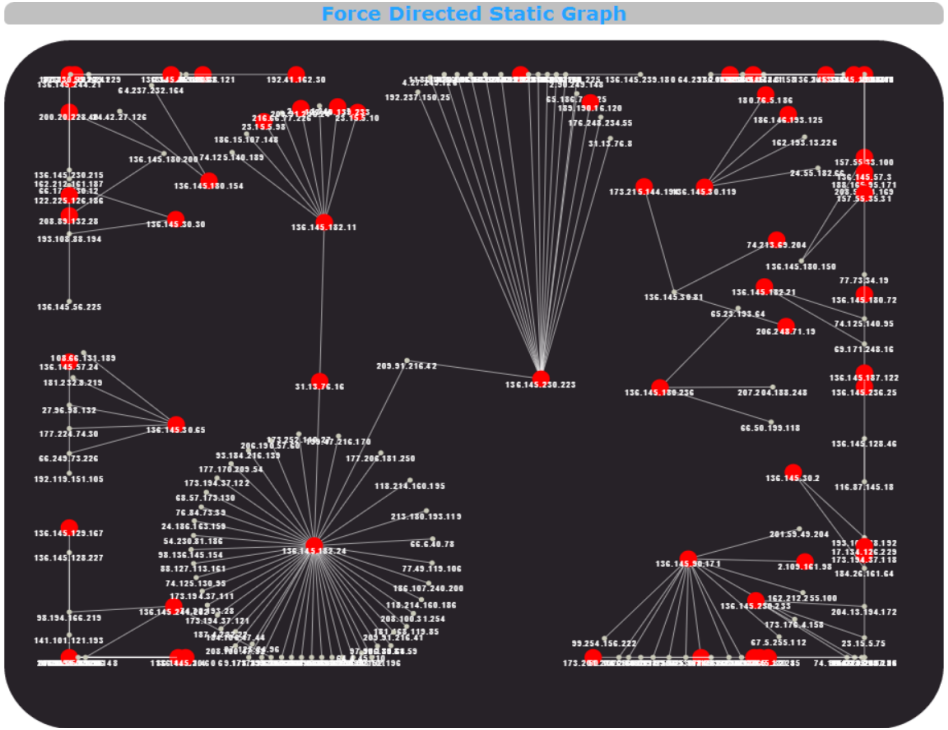
Port scan

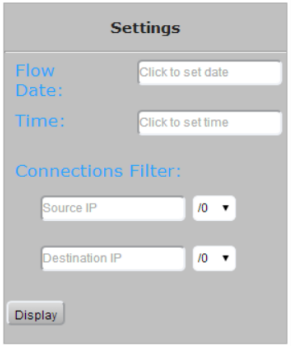
Undirected Graph

- 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







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!