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:

Raw data → Filter → Render vis → Vis

Reference: [http://resources.sei.cmu.edu/asset_files/Poster/2014_020_001_300460.pdf](http://resources.sei.cmu.edu/asset_files/Poster/2014_020_001_300460.pdf)
Toa data preparation process

1. **Raw data**
2. **Filter guided by sensors configured in DB**
3. **For each sensor Render vis**
4. **Vis**

- **collector**
- **parser**
- **grapher**
- **Web interface**
Toa: Overview

Cron triggers the parser and grapher every 5 minutes.

System configuration and parsed data.

Parser

Grapher

GUI

HD

Collector stores NetFlows in a FS.

User clients connect to the TOA web service.
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.

Collector stores NetFlows in a FS.

System configuration and parsed data.

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.

Collector stores NetFlows in a FS.

System configuration and parsed data.

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.

System configuration and parsed data.

Parser

Grapher

GUI

Collector stores NetFlows in a FS.

User clients connect to the TOA web service.

SQL
Toa GUI

Toa Network Monitoring System

Username
Password
Login
GUI Menu

Toa Network Monitoring System

Toa: A web based NetFlow data monitoring system | Computer Science Department | University of Puerto Rico - Rio Piedras | FloCon 2015
By Netlabel: RRP

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)

- 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.
Custom Query Interface

Custom Query Result

Octects Traffic Port 22 Max: 134.23 KB Min: 5.80078125.2f KB

- 22 Input KB
- 22 Output KB

Time

'12:00:00' '12:05:00' '12:10:00' '12:15:00' '12:20:00' '12:25:00' '12:30:00' '12:35:00' '12:40:00' '12:45:00' '12:50:00' '12:55:00'
### Top 100

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Flows</th>
<th>Octets</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>136.145.101.15</td>
<td>72.85-KB</td>
<td>92.37-MB</td>
<td>64.00-byte</td>
</tr>
<tr>
<td>136.145.182.24</td>
<td>161.12-KB</td>
<td>31.33-MB</td>
<td>24.31-KB</td>
</tr>
<tr>
<td>136.145.182.21</td>
<td>200.90-KB</td>
<td>20.03-MB</td>
<td>22.76-KB</td>
</tr>
<tr>
<td>136.145.138.238</td>
<td>12.87-KB</td>
<td>18.26-MB</td>
<td>11.00-byte</td>
</tr>
<tr>
<td>136.145.185.198</td>
<td>6.34-KB</td>
<td>8.79-MB</td>
<td>1.00-byte</td>
</tr>
<tr>
<td>136.145.180.150</td>
<td>4.22-KB</td>
<td>8.27-MB</td>
<td>564.00-byte</td>
</tr>
<tr>
<td>136.145.87.47</td>
<td>4.64-KB</td>
<td>5.12-MB</td>
<td>574.00-byte</td>
</tr>
<tr>
<td>136.145.180.118</td>
<td>5.68-KB</td>
<td>4.07-MB</td>
<td>29.00-byte</td>
</tr>
<tr>
<td>136.145.182.11</td>
<td>203.37-KB</td>
<td>29.04-MB</td>
<td>5.85-KB</td>
</tr>
<tr>
<td>136.145.196.137</td>
<td>3.21-KB</td>
<td>2.92-MB</td>
<td>506.00-byte</td>
</tr>
<tr>
<td>136.145.239.180</td>
<td>17.38-KB</td>
<td>2.67-MB</td>
<td>2.77-KB</td>
</tr>
<tr>
<td>136.145.180.200</td>
<td>4.63-KB</td>
<td>2.56-MB</td>
<td>821.00-byte</td>
</tr>
<tr>
<td>136.145.239.179</td>
<td>24.30-KB</td>
<td>2.90-MB</td>
<td>3.34-KB</td>
</tr>
<tr>
<td>136.145.180.154</td>
<td>9.19-KB</td>
<td>2.33-MB</td>
<td>485.00-byte</td>
</tr>
</tbody>
</table>
Top 100 ports
Views | a panel of graphs

RRP Interface Graphs by Day

RRP Traffic Network Max: 1.95 GB Min: 19.12 MB

Add to View
Views | a panel of graphs
Admin Interface

Toa Network Monitoring System

Device List

- AO
- CAYEY
- CUH
- Eric

View List

- FirstView
  - TestView
Admin Interface

Toa Network Monitoring System

Dashboard Device Custom Query System Viewer

Network Label Interface
I/F Interface Id AS AS Number
If Min Bytes Size Max Bytes Size

Add Network
Admin Interface

Toa Network Monitoring System

Device  Port  Net2Net  NetBlock

- RPP
- I/F 55
- None

AS 65003
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 reimplemention 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
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:

● A.Oslebo. Stager – A Generic Tool for Presenting Network Statistics
● Bearavolu et al., NVisionIP: An Animated State Analysis Tool for Visualizing NetFlows
● 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!