FlowViewer

Maintaining NASA’s Earth Science Traffic Situational Awareness

Graphic credit: Arizona/New Mexico Fire Imagery, USDA Forest Service; Remote Sensing Application Center; Image acquired from Aqua MODIS; NASA GSFC; June 7, 2011
FlowViewer provides a convenient web-based user interface to Mark Fullmer’s flow-tools suite, and now with v4.0, CMU NetSA group’s SiLK. The inclusion of the underlying SiLK tool set enables FlowViewer users to continue to use the tool with the newer IPFIX netflow data protocol.

FlowViewer has been developed for NASA’s Earth Sciences Data and Information System (ESDIS) networks, and credit goes to NASA for their usual outstanding support of innovation.
FlowViewer Features

- Complete open-source netflow collector analyzer
- Web-based UI provides dynamic front-end to open source collectors
- Dashboard provides user keep network traffic 'situational awareness'
- Ability to analyze IPFIX netflow (e.g., v9) data captured by SiLK
- Ability to continue to support netflow v5 installations via flow-tools
- Users can graph filtered traffic sets across a specified time period
- Background software tracks filtered traffic over long-term (ala MRTG)
- Ability to save filters and reports for later use and review
- Users can be alerted by email to abnormal data traffic situations
The Earth Observing System Data and Information System (EOSDIS) is a core capability in NASA’s Earth Science Data Systems Program. It provides end-to-end capabilities for managing NASA’s Earth science data from various sources – satellites, aircraft, field measurements, and various other programs. The EOSDIS serves a broad international community of Earth Science and meteorological scientists and users. Several TBytes of satellite and science data traverse its network every day.

- In 2003 NASA and CSC worked to capture netflow data to help monitor traffic
- Initial capture/analysis system was based on ‘cflowd’
- FlowViewer was developed to aid traffic analysis (away from the command line)
- Today, NASA monitors over 200 Earth Science flows of interest (FlowTrackings)
FlowViewer is an entirely open source netflow collector, analyzer and reporter. HTML/CSS user interface provides easy and wide deployability.
FlowViewer Main Screen

FlowViewer provides a dynamic web front-end to two powerful open-source netflow data collector and analyzers, flow-tools and SILK. FlowViewer provides the user with the ability to quickly extract network management information of interest from voluminous quantities of stored netflow data. The user can configure a Dashboard of continuously updating FlowTrackings to maintain a situational awareness of his organization’s network traffic. All generated reports and filters can be saved for future application. FlowViewer consists of three primary tools: FlowViewer, FlowGrapher and FlowTracker. The user can switch between the tools preserving the previously specified filter.

FlowViewer enables the user to create text based reports from filtered netflow data. Several different reporting formats are provided. Each of these reports can be sorted by column heading.

FlowGrapher enables the user to graph the bandwidth used by a filtered subset of netflow data during a specified time period. Resulting reports include the graph and a textual listing of the largest flows.

FlowTracker enables the user to maintain a long-term history of a particular traffic subset. FlowTrackings consist of five graphs of traffic over successive longer time periods: Daily, Weekly, Monthly, Yearly, and Last 3 Years.

Manage Dashboard
User’s Guide
FlowViewer Main Screen

- Links to various tools
- User specified links
- Saved Reports
- Dashboard (left)
- Dashboard (right)
- Dashboard Management

FlowViewers provides a dynamic web front-end to two powerful open-source netflow data collector and analyzers, FlowTools and SLK. FlowViewer provides the ability to quickly extract network management information of interest from vast quantities of stored netflow data. The user can configure a Dashboard to continuously update FlowTrackings to maintain situational awareness of their organization's network traffic. All generated reports and filters can be saved for future use. FlowViewer consists of three primary tools: FlowViewer, FlowGrapher, and FlowTracker. The user can switch between the tools presenting the previously specified filter.

FlowTracker enables the user to maintain a long-term history of a particular traffic subset. FlowTrackings consist of the graphs of traffic over successive longer time periods: Daily, Weekly, Monthly, Yearly, and Last 3 Years.
FlowViewer Input Screen
FlowViewer Input Screen - 1

- **Setting up a FlowViewer Report**
- **Report time frame**
- **Source information**
- **Destination information**
- **Named interfaces**
- **Report type**
- **Report output format**
FlowViewer Input Screen - 2

- Reuse saved filter
- Select from different devices
- Autonomous systems (flow-tools only)
- Report types

Create a FlowViewer Report

Saved Filters
- Select Saved Filter
- esro32-core-01a

Netflow Source
- Select Exporter

Start Date
- 10/24/2012

Start Time
- 18:00:00

End Date
- 10/24/2012

End Time
- 17:00:00

Source IP Addresses

Source Port

Source AS

Source I/F

Source IP Name

Interface Names

Destination IP Addresses

Dest Port

Dest AS

Dest I/F

Dest IP Name

Interface Names

TOS Field

TCP Flags

Protocol

Nexthop IPs

Reporting Parameters

Statistics Reports
- Source/Destination IP
- Select Statistics Report
- UDP/TCP Source Port
- UDP/TCP Destination Port
- UDP/TCP Port
- Destination IP
- Source IP

Printed Reports
- Select Print Report

Cutoff Lines

Cutoff Octets

Sampling Multi

Report types
- Source/Destination IP
- Source or Destination IP
- IP Protocol
- Input Interface
- Output Interface
- Input/Output Interface
- Source AS
- Destination AS
- Source/Destination AS
- IP ToS
- Source Prefix
- Destination Prefix

FlowViewer
FlowTracker
Excluding within a network

Multiple entries

Excluding (works on all fields)

TCP Flags

Sampling multiplier

Additional reports

When using SiLK devices
FlowViewer Report

- Can switch to other tools with filtering criteria preserved
- Aggregation filtering
- Sortable by column
- Save the filter
- Save the report
FlowGrapher Input Screen

- Setting up a FlowGrapher Report
- Same filtering criteria
- Resolved host names or IP addresses

How to determine statistics (Max, 95th, Avg, Min)

Number of longest flows to list in detail

Time “bucket” size for accumulating bits / period
FlowGrapher Report

- Review of input filtering criteria
- Graph of Mbps over specified time period
- Calculated statistics
- Sortable Columns
- Largest flows (e.g., top 200)
- Mbps per flow (calculated)

**FlowGrapher Report from router-main-01a**

- **Start Time:** 4/24/2012 6:00 06 UTC
- **End Time:** 4/24/2012 14:00 UTC
- **Bucket Size:** 5 sec
- **Expiry:** 4/24/2012 14:00 UTC
- **Source IPs:** seven77.highup.arl.com
- **Source Ports:**
- **Destination Ports:**
- **Source AS:**
- **Destination AS:**
- **Top Flows:**
- **Graph Width:** 1

**Flow data from ncur37-core-01a**

<table>
<thead>
<tr>
<th>Start</th>
<th>End</th>
<th>Len</th>
<th>Source Host</th>
<th>S Port</th>
<th>Destination Host</th>
<th>D Port</th>
<th>Total Bytes</th>
<th>Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>05:34</td>
<td>05:36</td>
<td>2</td>
<td>seven77.highup.arl.com</td>
<td>55555</td>
<td>192.168.84.128</td>
<td>7326</td>
<td>236,163,048</td>
<td>6.980</td>
</tr>
<tr>
<td>05:35</td>
<td>05:39</td>
<td>2</td>
<td>seven77.highup.arl.com</td>
<td>55185</td>
<td>192.168.84.204</td>
<td>9514</td>
<td>229,663,483</td>
<td>1.130</td>
</tr>
<tr>
<td>05:37</td>
<td>05:40</td>
<td>2</td>
<td>seven77.highup.arl.com</td>
<td>57460</td>
<td>192.168.84.207</td>
<td>9603</td>
<td>259,650,793</td>
<td>1.140</td>
</tr>
<tr>
<td>05:44</td>
<td>05:46</td>
<td>2</td>
<td>seven77.highup.arl.com</td>
<td>52632</td>
<td>219.239.44.225</td>
<td>41191</td>
<td>327,014,700</td>
<td>1.360</td>
</tr>
<tr>
<td>05:47</td>
<td>05:53</td>
<td>6</td>
<td>seven77.highup.arl.com</td>
<td>66451</td>
<td>192.168.84.201</td>
<td>36882</td>
<td>317,091,740</td>
<td>1.320</td>
</tr>
<tr>
<td>05:54</td>
<td>06:04</td>
<td>20</td>
<td>seven77.highup.arl.com</td>
<td>56662</td>
<td>192.168.84.201</td>
<td>1146</td>
<td>233,483,583</td>
<td>1.160</td>
</tr>
<tr>
<td>05:56</td>
<td>06:46</td>
<td>242</td>
<td>seven77.highup.arl.com</td>
<td>57036</td>
<td>cloudsp-blue.larc.arl.com</td>
<td>14721</td>
<td>863,054,833</td>
<td>28.460</td>
</tr>
</tbody>
</table>

**Sortable Columns**

- Flow Grapher
- Save Filter
- Save Report

**Select an Active or Archived Flow Tracking**

**Flow Viewer**

**Monitoring EOS Science Data Flows**

**CSC**

January 11, 2013
Creating a FlowTracking

Option to start a FlowTracking in the past

Same filtering criteria

Email alerting

Individual or Group FlowTrackings

Alert thresholds

Alert frequency choices

Creating a FlowTracking in the past

Same filtering criteria

Email alerting

Alert thresholds

Alert frequency choices
FlowTracker Group Input Screen

'Groups' stack Individual FlowTrackings

Select Individual FlowTracking Group components

Can have components above and below X-axis

Adjust Group components

Netflow exports to Collector 15b
Netflow exports to Collector

Above 02 auto mixed2
Above 01 auto mixed1
New Color: auto mixed2
New Color: auto mixed1
Move: Leave Alone
Move: Leave Alone

Add Component
Reset Values

This group is composed of these components:
FlowTracker Report – General Example

FlowTracking filtering criteria

Statistics kept for graph time period

List individual values

Familiar ‘MRTG’ graph set

Save Report

Ability to annotate graphs about significant change events

Can quickly link to either FlowViewer or FlowGrapher (with filter preserved) for more detailed analysis

Scroll down for longer term MRTG-like graphs
This FlowTracking documents the delivery of NPP data to the University of Wisconsin. One can see a switch from two (Atmospheric Science) servers to one only, and then all to the other of the pair.

This is an example where you might want to save a FlowTracking

Access to all saved reports
This example depicts a situation where traffic shaping was invoked to manage limited network resources. This FlowTracking Group helps identify if perhaps there is one ‘big player’ for which a different network arrangement might mitigate the problem.
FlowTracker Management

Pulldown of all FlowTrackings

Listing of all FlowTrackings

Case Studies

Components of an Interface

Satellite data in

Science data out

To service provider

Gray line preserves highest 5-minute measurement over the longer term graphs.

These graphs help NASA monitor an expensive high-rate circuit between a polar ground station in Norway and the GSFC in Maryland. The circuit is shared with other Federal agencies through the use of MPLS tunnels.

This depression of peak values indicates that there may be an issue with the network or the MPLS tunnel (or the servers, or software or, ... )
Around the time of last summer’s hurricane Isaac, Land, Atmosphere Near-Real-Time Capability for EOS (LANCE-MODIS*) system managers noted a sharp increase in traffic.

The FlowTracker Re-create capability was invoked to create a FlowTracking Group which isolated the new user that had come on line: the National Severe Storms Laboratory.

* MODIS - Moderate Resolution Imaging Spectroradiometer
Users can modify each of the eight Dashboard positions by:

1) Install new FlowTracking
2) Remove FlowTracking
3) Move FlowTracking up
4) Move FlowTracking down

Dashboard FlowTrackings can be:

1) Individual
2) Group
3) Any of the five periods

Each Dashboard FlowTracking is updated every 5 minutes
Each Dashboard graph links back to the original FlowTracking
Upon FlowViewer installation, the FlowTracker_Collector and FlowTracker_Grapher scripts are placed in the Linux background. They will “wake up” every five minutes and collect a 5-minute value for each active FlowTracking. The FlowTracking and Dashboard graphs are updated with the latest data point.
Closing Thoughts

- FlowViewer distribution includes “analyze_netflow_packets” utility
- FlowViewer has supported flow-tools for over five years; but is new to SiLK
- Integration with SiLK may not be optimized as a result
- Would welcome SiLK related improvement suggestions
- At the same time … some ‘requests’ of SiLK 😊. Please include:

  - IPFIX Information Element (IE) [5]: ipClassOfService
  - IPFIX Information Element (IE) [16]: bgpSourceAsNumber
  - IPFIX Information Element (IE) [17]: bgpDestinationAsNumber
  - IPFIX Information Element (IE) [70]: mplsLabelStackSection
  - IPFIX Information Element (IE) [71]: mplsLabelStackSection2
  - IPFIX Information Element (IE) [72]: mplsLabelStackSection3
Thank You

Joe Loiacono
Network Engineer, CSC
jloiacon@csc.com

http://earthdata.nasa.gov/esdis

NASA Official: Kevin Kranacs
Manager, ESDIS Networks

FlowViewer is available from:
https://sourceforge.net/projects/flowviewer