Dell SonicWall Visualization Report

Wanzhang Sheng
Kaiming Yang
Michelle Gao
Xi Han

December 7, 2014

Chapter 1

Introduction

Chapter 2

Specification

Chapter 3

Implementation

Chapter 4

Test Plan

Chapter 5

Deliverables

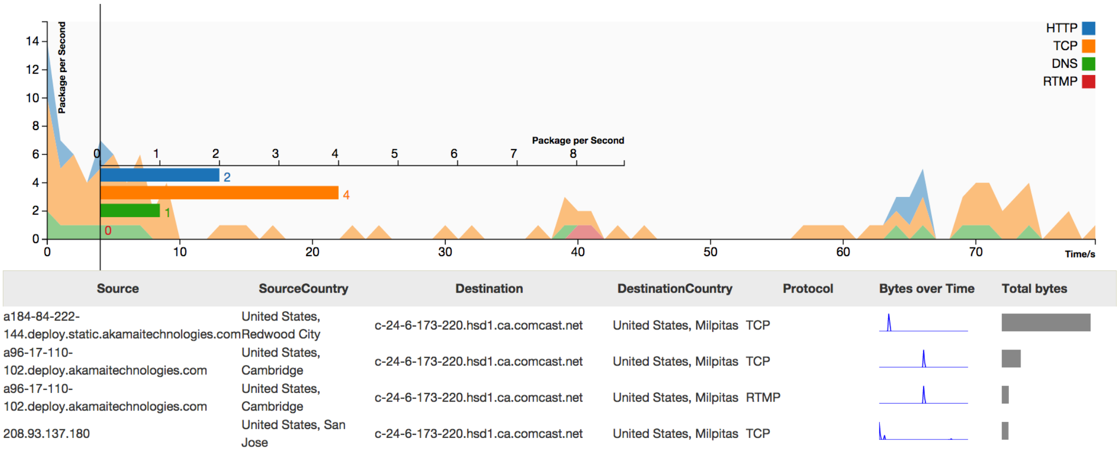
5.1 Primary Deliverables

Our main deliverables are our demo visualizations and the website we created for this project.

5.1.1 Demo Visualizations

Dashboard

Figure 5.1 aims to create a overview of the network traffic. We limited the result only show a summary of top ten traffic. It includes two parts. The top one is an area chart shows networking packages over time, separated by protocols. Users can click on it to show traffic details at the corresponding time. The bottom one is an sortable table. Each row indicates a different traffic by source, destination and protocol, along with a spark-line to show the trend, and a bar to show the total bytes. When users hover their mouse over any row, the area chart can change to the sub-dataset correspondingly. And also users can select a row or select multiple rows by holding command/option/shift key with a clicking to lock the dataset, then users can move their mouse to the area chart to inspect more details.



Source	SourceCountry	Destination	DestinationCountry	Protocol	Bytes over Time	Total bytes
a184-84-222-144.deploy.static.akamaitechnologies.com	United States, Redwood City	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a96-17-110-102.deploy.akamaitechnologies.com	United States, Cambridge	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		
a96-17-110-102.deploy.akamaitechnologies.com	United States, Cambridge	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	RTMP		
208.93.137.180	United States, San Jose	c-24-6-173-220.hsd1.ca.comcast.net	United States, Milpitas	TCP		

Figure 5.1: Dashboard

Data-maps

Figure 5.2 is a map visualization. It shows the traffic on a a map. User can switch map scope between USA and world. Arcs between cities indicate connections and the thickness indicates the volume. Circles indicate traffic volume of the cities. Cyan for source volume and red for destination volume. Users can toggle circles by clicking on legends.

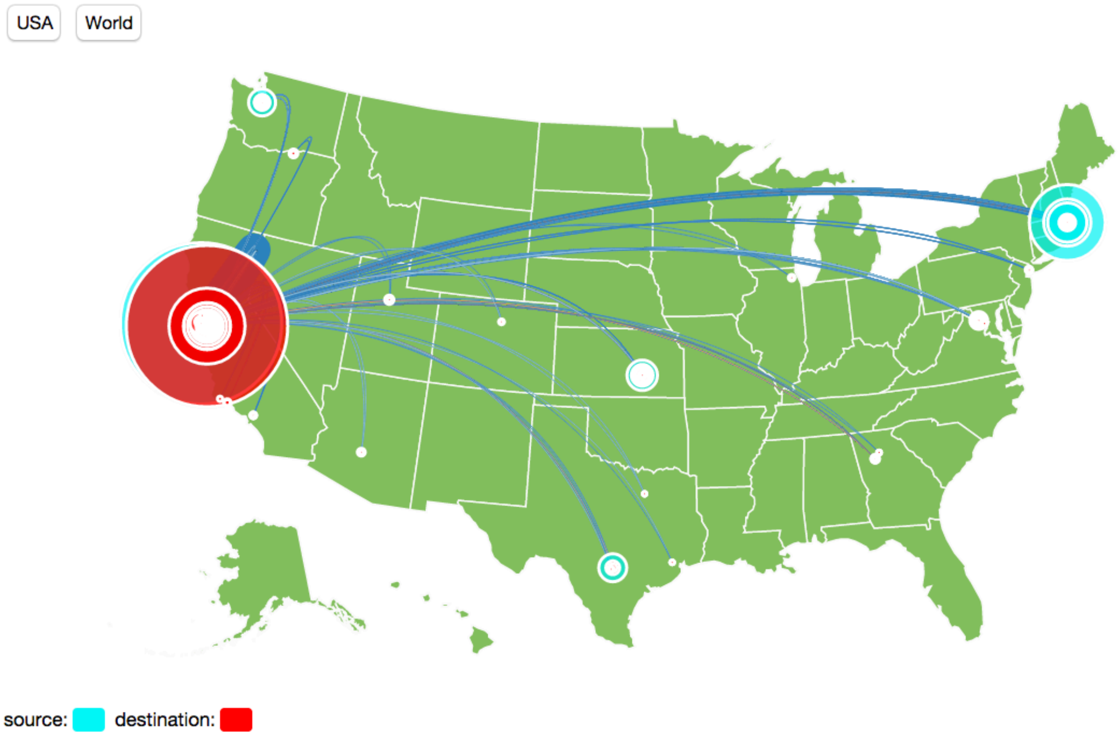


Figure 5.2: Data-maps

Realtime Map Plot

Figure 5.3 is a map visualization which keeps receiving realtime data from our back-end. Lines on the map indicate connections. By hovering on any line, users are allowed to inspect details of that connection with line charts and bar charts. And click to make it horizontal which make it easier to watch.

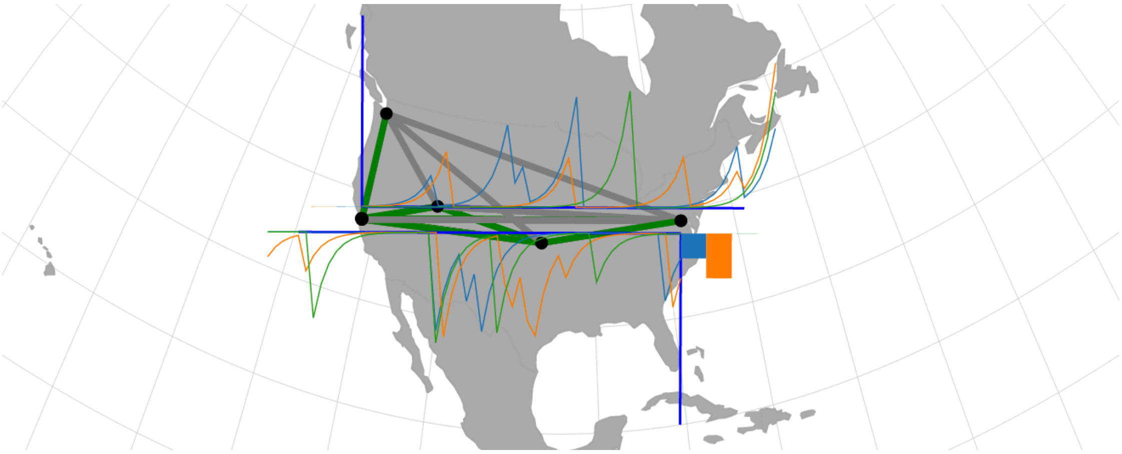


Figure 5.3: Realtime Map Plot

5.1.2 Website

Because our project is about D3 visualization, we created a website at http://sjengle.cs.usfca.edu/cs690-sonicwall/ to show our work. There are several pages on it.

Home
This page shows a brief introduction to this project. Why we worked on this project and the basic timeline of the whole process.

Visualizations
This page lists all visualizations we created for this project, including all attempts before the final visualization.

Data
This page shows where did we pick the data for our visualizations, and how we transformed it and mixed geography information to fit our needs.

Tools
This page lists main open-source libraries or visualization tools we used during the development.

Team
This page lists all team members and sponsors with avatars and biographies.

Deliverables
THis page shows main deliverables including this report, usage video and slides used in the presentation.

Our works are mainly in page Visualizations. We have seven sections indicate different attempts. In most sections, every team member has their own attempts. By hovering mouse on any attempt, you can see a thumbnail of the visualization. We wished by this way, we can explore as wide as we can, to find the best way to visualize the data.

5.1.3 Code Files

```
/
├── index.html
├── visual.html
├── data.html
├── tools.html
├── team.html
├── deliverables.html
├── assets/ ............................................ Assets for pages above
│   ├── default.css
│   ├── *.png
│   └── *.jpg
└── public/
    ├── demo/ .................................................... Demo page
    │   ├── index.html
    │   ├── style.css
    │   ├── g1.js ......................................... Reusable area chart
    │   └── table.js .................................. Reusable sortable table
    └── lib/
        └── sparkcharts/
            └── sparkcharts.js ............................ Reusable spark chart
```

5.1.4 SLOC

We use a JavaScript tool SLOC to calculate source-line-of-code:

```
sloc . --exclude "(jquery|bootstrap|d3|p5|tip|modernizr|datamaps).*\.(js|css)|.*\.(csv|
    json)|nsa6600|xihan/lib"
```

This command means when it analytics files, it will exclude files which filename or pathname match the given regular expression. By this, we remove libraries or data we used or generated in the project to make the result more meaningful and convincing. And the result is in Table 5.1.

Table 5.1: SLOC Result

Physical	Source	Comment	Single-line comment	Block comment	Mixed	Empty	Number of files
9978	8226	621	384	238	62	1210	123

5.2 Other Deliverables

5.2.1 Data Files

```
/
└─ public/
   ├─ prepare.rb ........................ Ruby script for preparing data
   ├─ geoip.csv (11K) ................... Geography information table
   ├─ sfgate.csv (1.2M) ................. Wireshark data
   ├─ sfgate_with_geoip.csv (1.6M) ...... Wireshark data with geography information mixed in
   ├─ sfgate_summary.csv (3.3K) ......... Wireshark data summary of top 10 connections in CSV
   ├─ sfgate_summary.json (12K) ......... Wireshark data summary of top 10 connections in JSON
   ├─ sfgate_subset.csv (8.3K) .......... Wireshark subset data with top 10 connections in CSV
   ├─ sfgate_subset.json (16K) .......... Wireshark subset data with top 10 connections in JSON
   └─ nsa6600/ .......................... SonicWall data
      └─ merged.csv (240K) .............. SonicWall data merged
```

5.3 Documentation

Chapter 6

Conclusion