Dell SonicWall Visualization Report

Wanzhang Sheng
Kaiming Yang
Michelle Gao
Xi Han

December 10, 2014

Chapter 1

Introduction

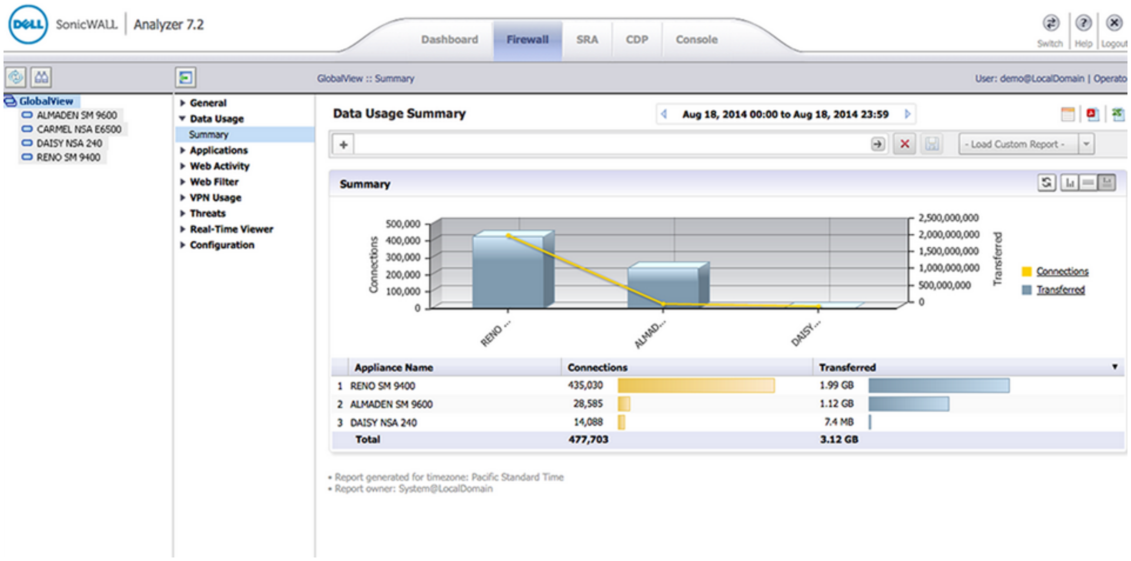
1.1 Project Overview

In this project, we use D3 to build stand-alone prototype visualizations of Dell SonicWALL firewall data that could be integrated into their Dell SonicWALL Analyzer product.We learn SonicWALL data format. We use wireshark data which is similar to the firewall data of Dell SonicWALL products, and generate dashboard,datamaps, and realtime map plot.

1.1.1 Dell SonicWALL Analyzer

Analyzer

Figure 1.1 is the current visualization of data usage of Dell SonicWALL Analyzer.The analyzer streamlines and summarizes web traffic and network data.We want to generate visualizations that could be interated into the Analyzer product to show near real-time analysis of traffic and network data.



Data Usage Summary

Aug 18, 2014 00:00 to Aug 18, 2014 23:59

Summary

	Appliance Name	Connections	Transferred
1	RENO SM 9400	435,030	1.99 GB
2	ALMADEN SM 9600	28,585	1.12 GB
3	DAISY NSA 240	14,088	7.4 MB
	Total	477,703	3.12 GB

- Report generated for timezone: Pacific Standard Time
- Report owner: System@LocalDomain

Figure 1.1: Analyzer

1.2 Team Overview

1.2.1 Team Members

Our team members are Wanzhang Sheng, Kaiming Yang, Jie Gao and Xi Han.

Wanzhang Sheng is a Computer Science graduate student of University of San Francisco. He has worked on Ruby on Rails for over four years. Finished internship in Twitter working on Backbone.js.

Jie Gao is a Computer Science student at University of San Francisco. She has experiences in Java and C. She has built two-layer web service using Java.She used to study Electrical Engineering and has worked as a Information System administrator for over a year.

Xi Han is a Computer Science graduate student of University of San Francisco. He mainly focuses on data mining and data visualization on several fields using C#, python and javascript libraries. During his internship he was working on SQL error comparison visualization in Honeywell(China). And he also has experiences working on protein molecule visualization using OpenGL under his professor.

Kaiming Yang is a Computer Science student at University of San Francisco. He has experiences in many programming languages like C/C++, Java and Python. He used to study physics and worked a lot on scientific computation.

Chapter 2

Specification

Chapter 3

Implementation

Chapter 4

Test Plan

Chapter 5

Deliverables

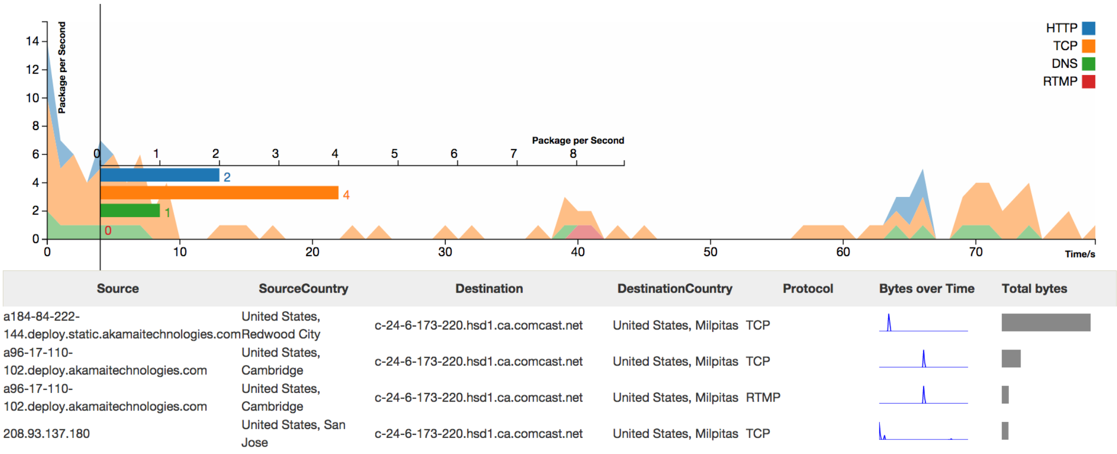
5.1 Primary Deliverables

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 an overview of the network traffic. We limited the result only shows a summary of top ten connections. 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 a sortable table. Each row indicates a different connection by source, destination and protocol, along with a spark-line to show the trend, and a bar to show the total bytes of the connection. By hovering mouse over a row, the area chart can change to the subset data correspondingly. And also, users are allowed to select one single row by a simple click or select multiple rows by holding command/option/shift key with a clicking to lock the dataset, then users can move their mouses 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

Datamaps

Figure 5.2 is a map visualization. It shows the traffic on a a map. User can switch map scope between USA and the world. Arcs between cities indicate connections and thicknesses indicate the volumes. Circles indicate the traffic volume of the city. Cyan for outgoing volume and red for incoming volume. Users can toggle circles by clicking on the legend.

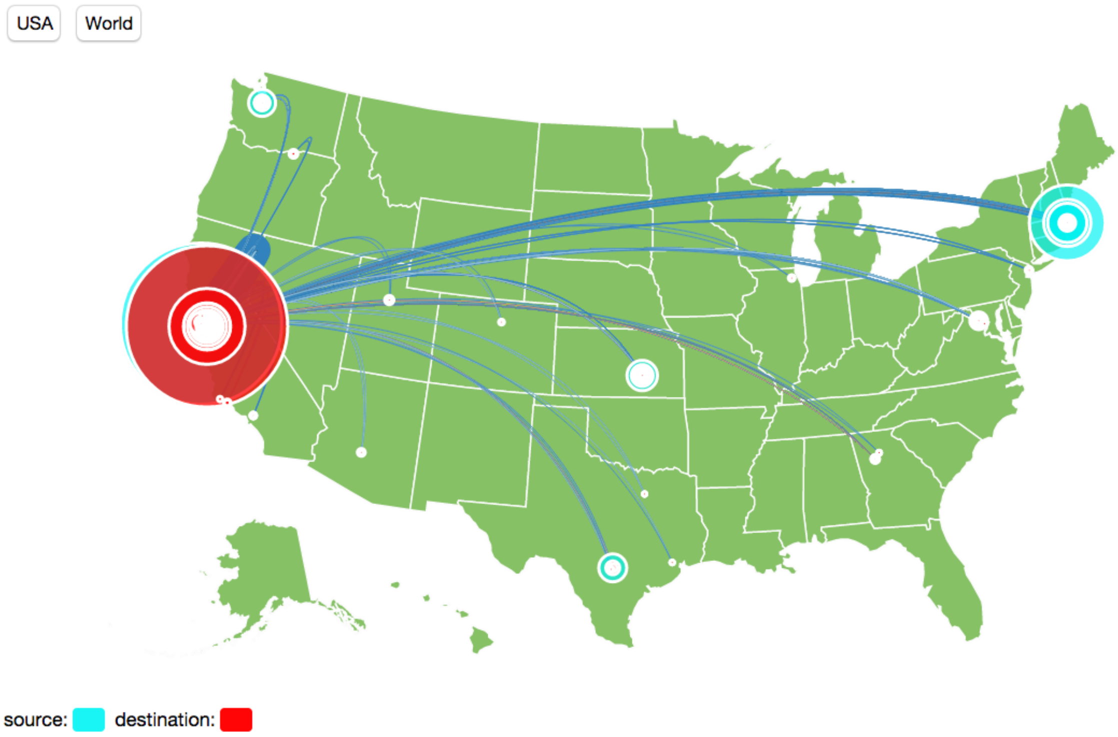


Figure 5.2: Data-maps

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 two line charts and two bar charts for both directions. And by clicking, to make it horizontal which is easier for users to watch the charts.

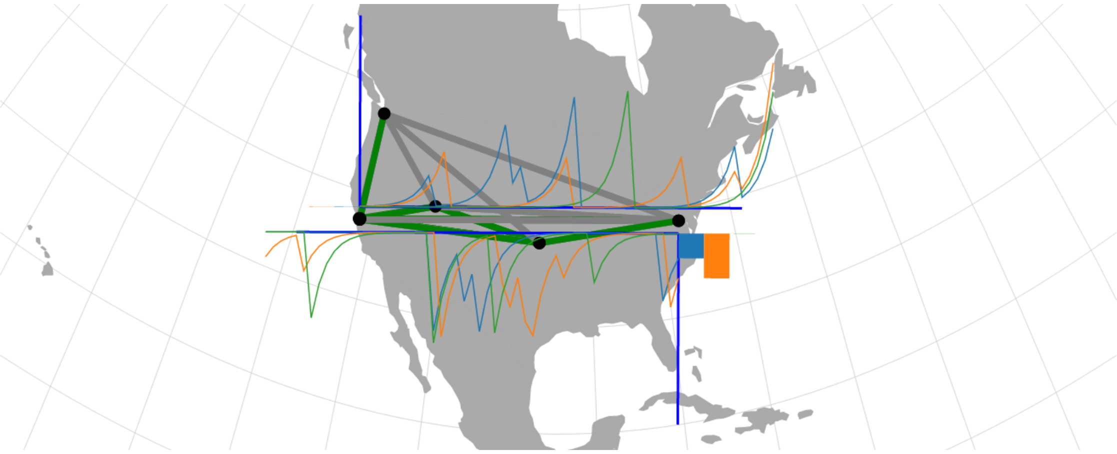


Figure 5.3: Realtime Map Plot

5.1.2 Website

Because our project is about visualizations, we created a website to show our work at http://sjengle.cs.usfca.edu/cs690-sonicwall/ with Bootstrap. 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 visualizations.

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 videos and slides used in the final presentation.

Our works are mainly in page Visualizations. We have seven sections list different attempts. In most sections, every team member has their own attempts. By hovering mouse on any item, it will show a thumbnail of the visualization correspondingly. By this way, we can explore as wide as we could, 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 Source Lines of Code

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 whose filename or pathname matches 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

The usage videos in the Deliverables page are our user documentations, in which we descript our user interface, our main features, and how to use them. Those videos can also be found on YouTube:

Dashboard http://youtu.be/4Hakf4k9Lig

Realtime Map Plot http://youtu.be/KNbSRVzx_gY

Data Structure http://youtu.be/YU_TZmgiooQ

We also maintained README file for background description and resources links, and Wikis for development progress notes, on the Github repository.

Chapter 6

Conclusion