Welcome to

4. SIEM Visualization

KEA Kompetence SIEM and Log Analysis

Henrik Kramselund Jereminsen hkj@zencurity.com @kramse

Slides are available as PDF, kramse@Github

4-visualization-siem.tex in the repo security-courses

Goals for today

Todays goals:

- Visualizations see a lot of examples, knowing possibilities makes it possible to choose
- Kibana features like importing/exporting dashboards
- Look at alerting

Photo by Thomas Galler on Unsplash

Plan for today

Subjects

- Visualizations examples
- Tool examples
- Kibana features like importing/exporting dashboards

Exercise theme: Make it easy and pretty

- Importing dashboards

Reading Summary

DDS 6. Visualizing Security Data 22

DDS 10. Designing Effective Security Dashboards

Skim: DDS 11. Building Interactive Security Visualizations

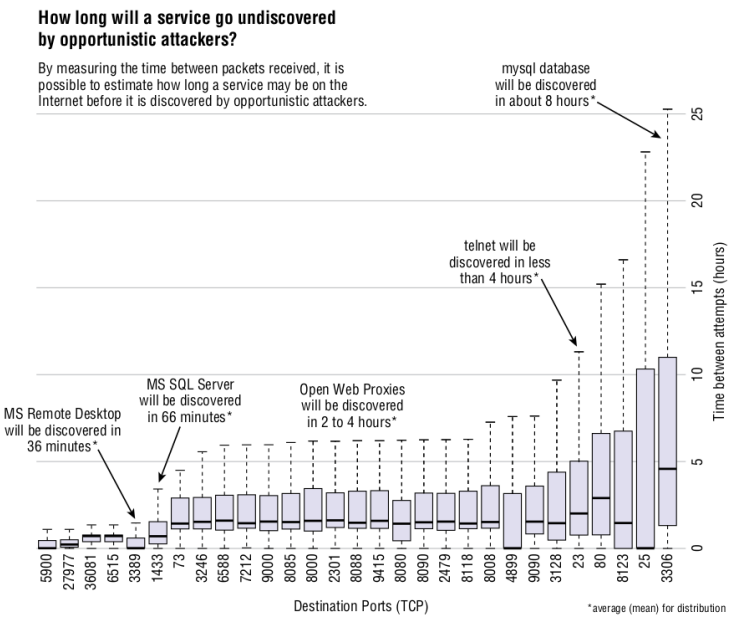
Reading Summary, continued

- **Data visualizations communicate complexity quickly.** Descriptive statistics (mean, median, variance, and so on) exist to describe and simplify data but tend to remove subtleties that exist. It's possible to communicate millions of data points in seconds while minimizing the loss of detail and resolution through visualization.
- **Data visualizations enable recognition of latent patterns.** Patterns that would never be apparent using statistical methods or scanning the data may be revealed through visualization. When data is visually presented, patterns in a single variable or relationships across many variables may leap off the screen.
- **Data visualizations enable quality control on the data.** Mistakes and errors in data collection or preparation can often be revealed through visualization. Data visualizations can serve as a good and quick sanity check on your work.
- **Data visualizations can serve as a muse.** It's been said that most breakthroughs in science didn't start with a "Eureka!" but instead with a "Huh, that's odd." Laying out the data visually can give you a new perspective and help facilitate your thinking and discovery processes.

Source: DDS 6. Visualizing Security Data

- A light reading chapter, color, eye movements etc.

Example plot 6-17



Source: DDS 6. Visualizing Security Data

- Interesting graph, and interesting results Changing away from standard ports delay attackers!

Reading Summary, continued

- **A Dashboard Is Not a Report** ... However, the top-level view should be designed solely to give the viewer situational awareness of the desired task.
- **A Dashboard Is Not an Art Show**
- **Take Care with Colors** - talks about printing, but color blindness is a real problem
- **Use Fonts Wisely** - be sure to select one that scales consistently, supports variable width text, and has fixed-width numbers.
- **No One Dashboard to Rule Them All** - An iterative process

Source: DDS 10. Designing Effective Security Dashboards

Going through dashboards must be part of a procedure

Reading Summary, continued

> Getting started with D3 requires only three things—a text editor, the D3 JavaScript library, and a web server. To prove this, read through this annotated, basic example of a static bar chart (Figure 11-11) to see what it's like to code in D3.

Source: DDS 11. Building Interactive Security Visualizations

- Skim read chapter!
- D3.js is fantastic and also fantastically complex, beautiful examples `https://d3js.org/`
- I learned similar things from the NoStarch book, Data Visualization with JavaScript by Stephen A. Thomas March 2015, 384 pp. ISBN-13: 978-1-59327-605-8 `https://nostarch.com/datavisualization`

- Today you can easily start out with Kibana, and defaults
- Finding recipes for running a full screen Dashboard with a rPi are easy to find


THE
END
IS
NEAR

Conferences and web sites

- Multiple sites and resources are available in this area
- FloCon, the international conference on "Using Data to Defend," `https://resources.sei.cmu.edu/news-events/events/flocon/`
- Zeek (BroCon) events `https://zeek.org/past-events/`
- IEEE Symposium on Visualization for Cyber Security, `https://vizsec.org/`
- Secviz older web site I have browsed from time to time, seeing examples, tools, data `https://secviz.org/`
- Greg Conti `http://rumint.org/`
- List a couple of tools you should know by name at least
- graphviz `https://graphviz.org/`
- afterglow `http://afterglow.sourceforge.net/`, examples Raffael Marty `https://raffy.ch/blog/2012/03/24/advanced-network-graph-visualization-with-afterglow/`

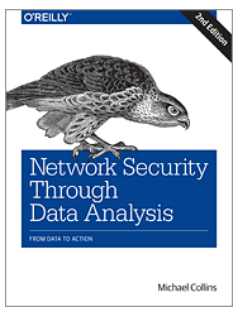
Take names, make a list - note the tools and people working with this

Newer tools

- https://www.brimsecurity.com/ Brim is packaged as a desktop app, built with Electron just like Slack. Once installed, you can open a pcap with Brim and it will transform the pcap into Zeek logs in the ZNG format.
- https://seaborn.pydata.org/ Seaborn is a Python data visualization library based on matplotlib. It provides a high-level interface for drawing attractive and informative statistical graphics.
- https://www.scikit-yb.org/en/latest/ Yellowbrick extends the Scikit-Learn API to make model selection and hyperparameter tuning easier. Under the hood, it's using Matplotlib.
- https://altair-viz.github.io/ Altair is a declarative statistical visualization library for Python, based on Vega and Vega-Lite, and the source is available on GitHub.
- https://github.com/gtkcyber/griffon-vm Griffon is a environment for data science. Griffon is based on Ubuntu MATE and includes numerous data science tools, all installed and configured for immediate use.

Recommended by Charles Givre in the article:
https://www.oreilly.com/content/improving-security-through-data-analysis-and-visualizations/

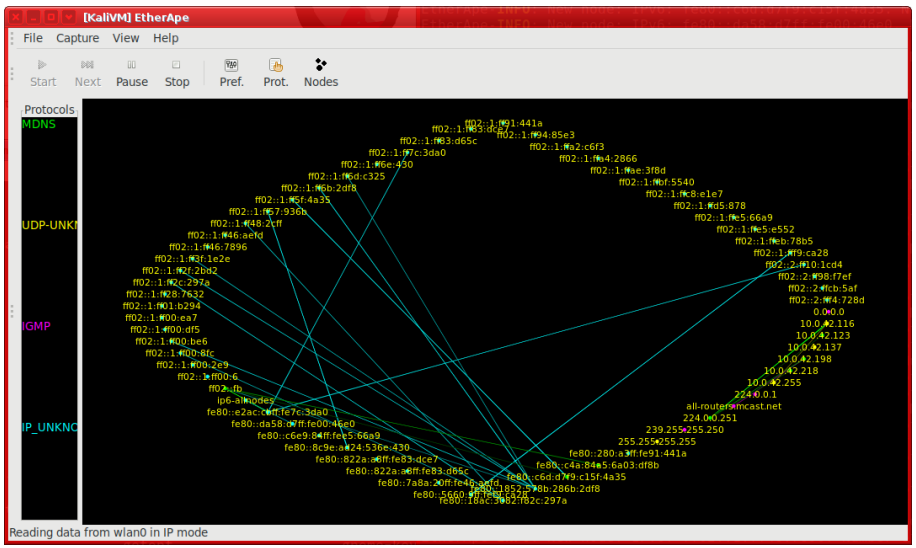
Books: Network Security Through Data Analysis



Network Security through Data Analysis, 2nd Edition By Michael S Collins Publisher: O'Reilly Media 2015-05-01: Second release, 348 Pages

- *Applied security visualization*, Rafael Marty, 2009
- *Security Data Visualization: Graphical Techniques for Network Analysis*, Greg Conti 2007
- *Visualize This: The FlowingData Guide to Design, Visualization, and Statistics*, Nathan Yau ISBN: 978-0-470-94488-2 July 2011 384 Pages

Example tools and graphs



- Graph types not in the book
- Etherape shown

Parallel coordinate plots

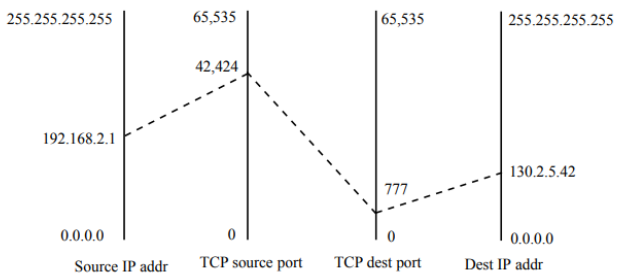
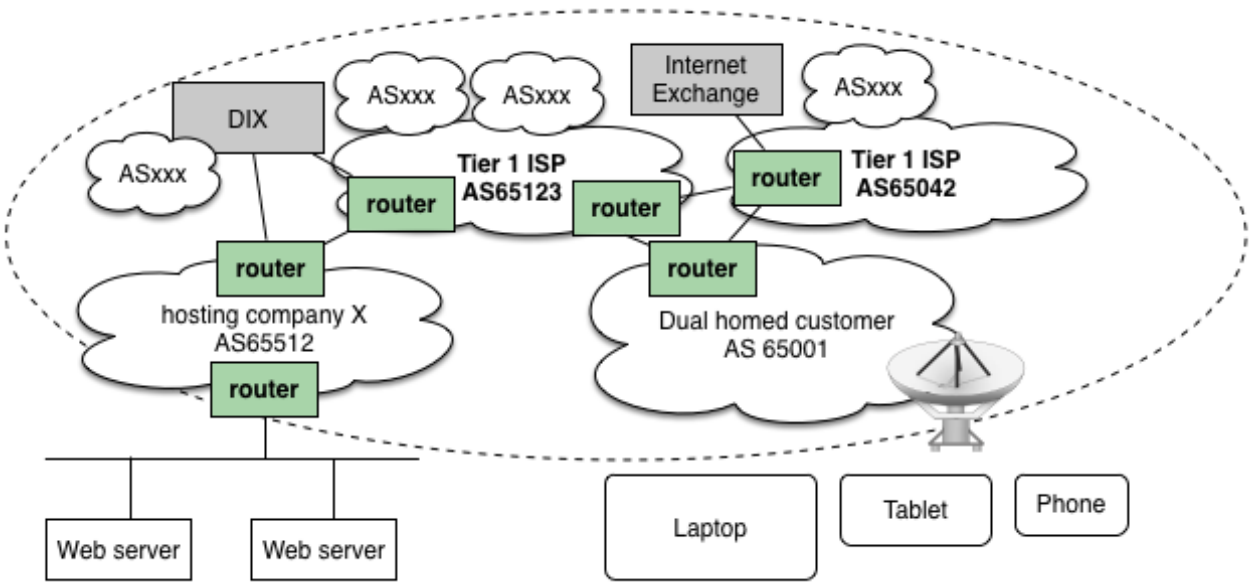


Figure 7: Parallel coordinate plot for a TCP packet from 192.168.1.1:42424 to 130.2.5.42:777.

image from Network Security Visualization Keith Fligg and Genevieve Max `https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2013/Resources/presentations/2012/topic13-final/report.pdf`

- `https://en.wikipedia.org/wiki/Parallel_coordinates`

Hosting and internet providers



- BGP networks are used for all of the Internet
- New standards like Resource Public Key Infrastructure (RPKI) are underway

Monitor your network

MRTG The Multi Router Traffic Grapher - simple, great, fast
`http://oss.oetiker.ch/mrtg/`

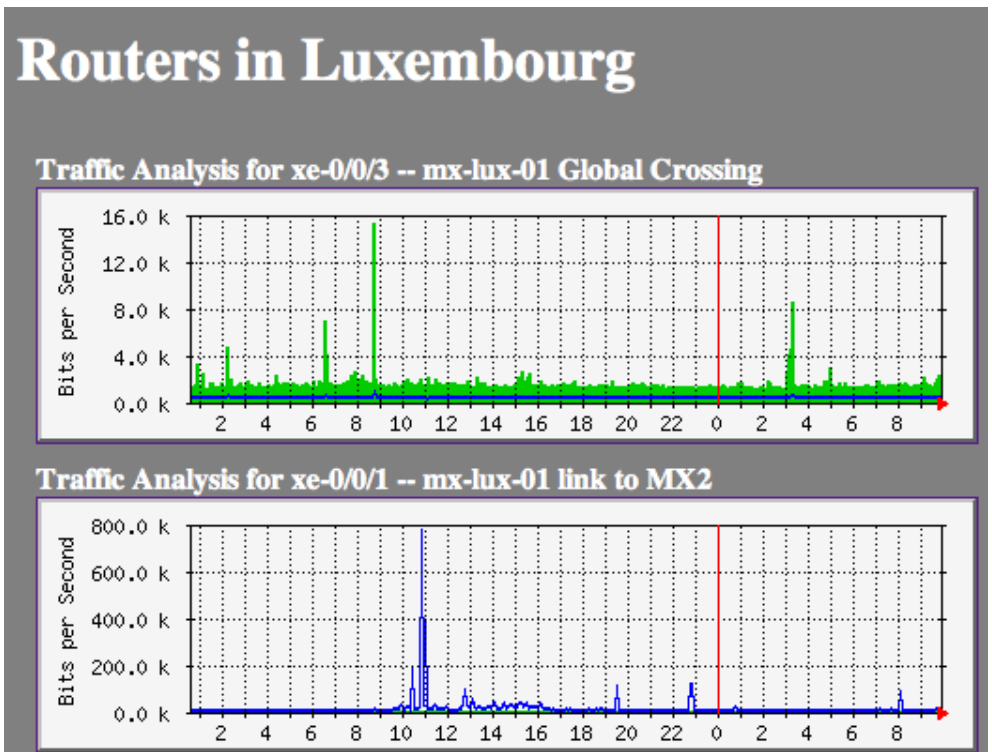
Smokeping Network Latency measurements - network quality
`http://oss.oetiker.ch/smokeping/`

NFsen Netflow monitoring - turn on at selected routers/switches

LibreNMS `https://www.librenms.org/`

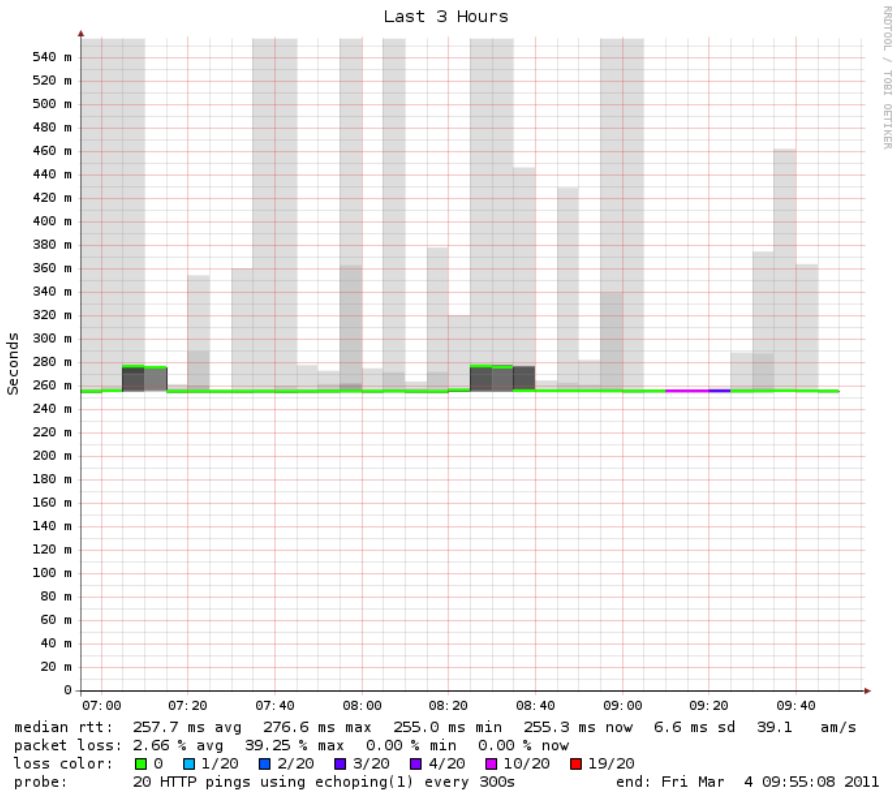
Manual tools, My Traceroute, Nping

MRTG SNMP monitoring made easy



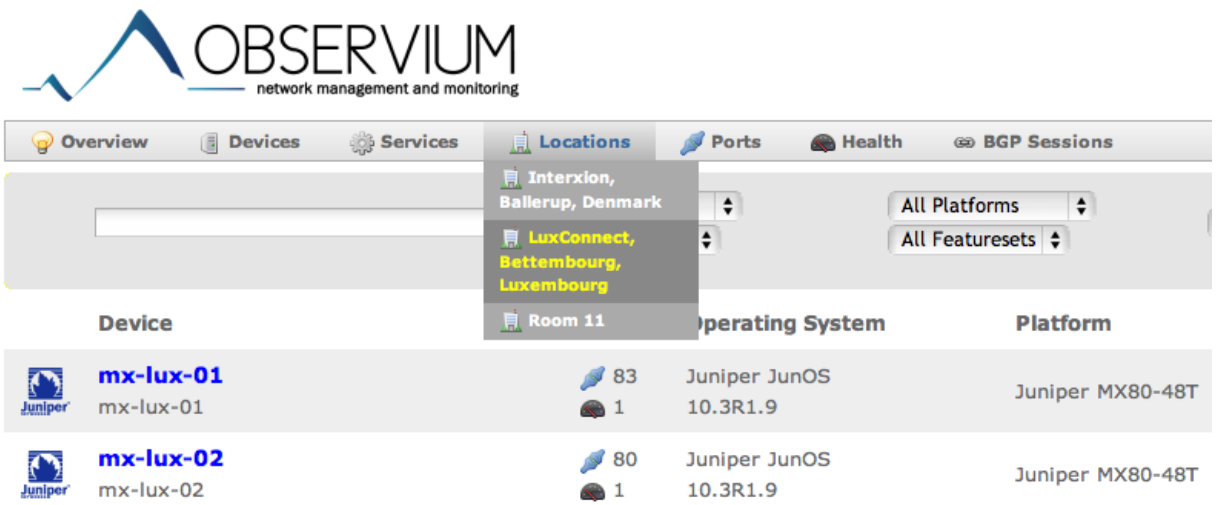
Run configmaker, indexmaker - almost done

Smokeping packet loss



Smokeping latency changed

Autoconfiguration: location

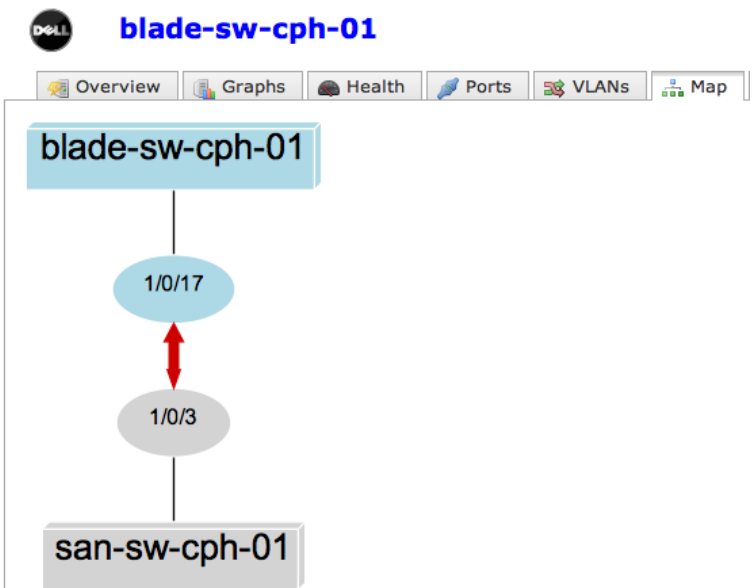


Observium picks up the location from SNMP :-)

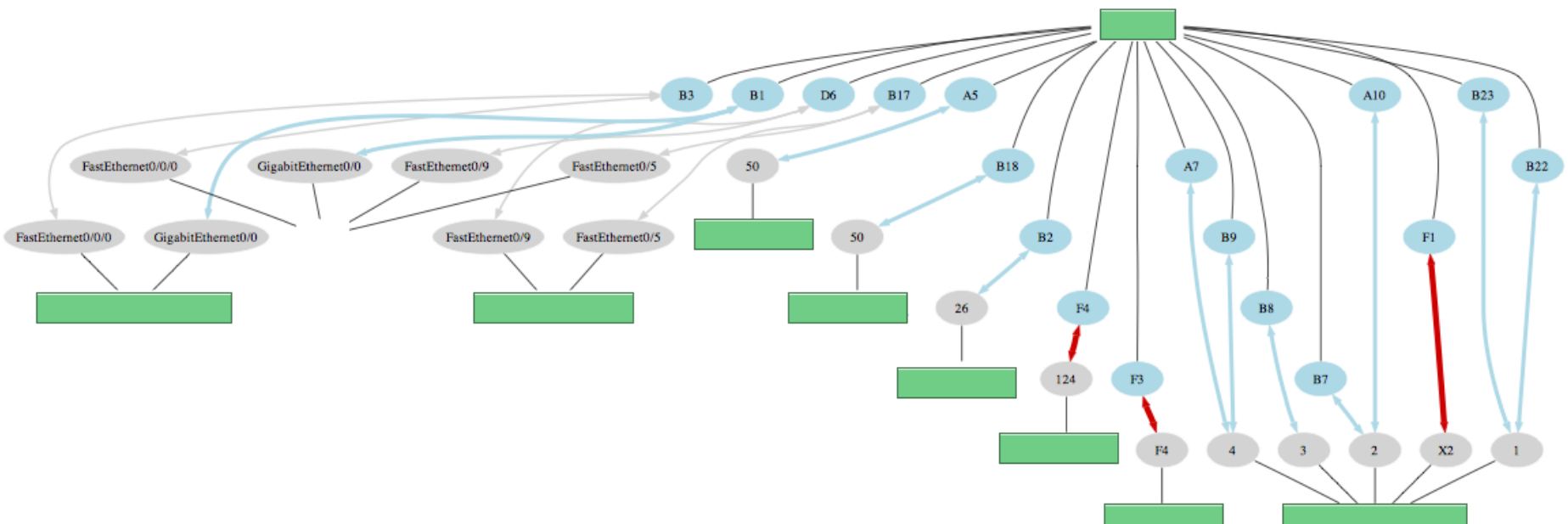
Config example: LLDP

Dell 8024F switch LLDP

```
interface ethernet 1/xg17
mtu 9216
lldp transmit-tlv port-desc sys-name sys-desc sys-cap
lldp transmit-mgmt
exit
```

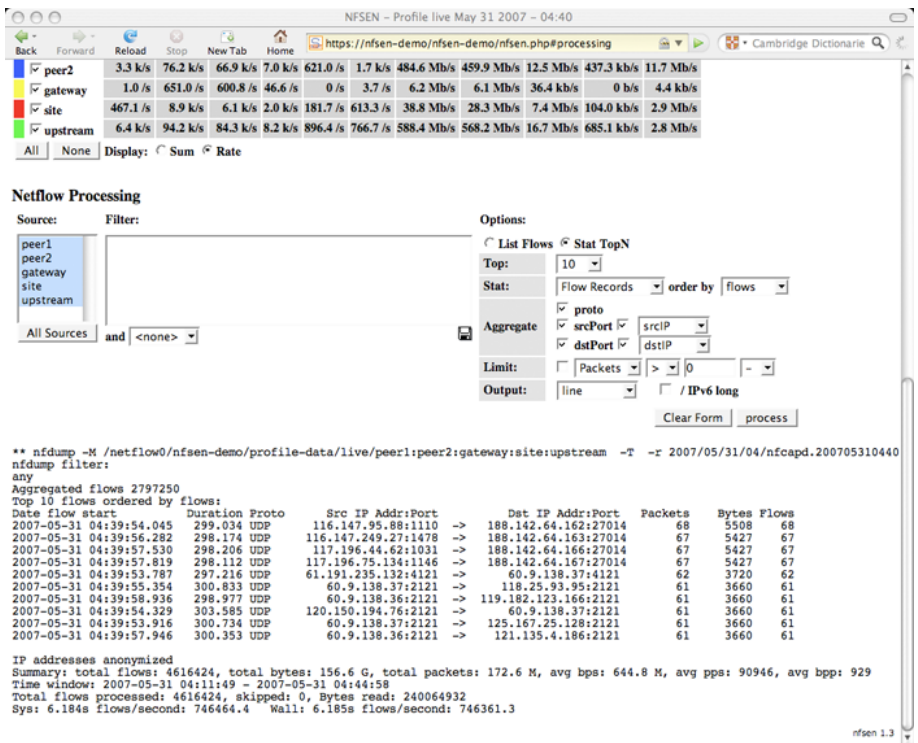


Autoconfigured maps from LLDP



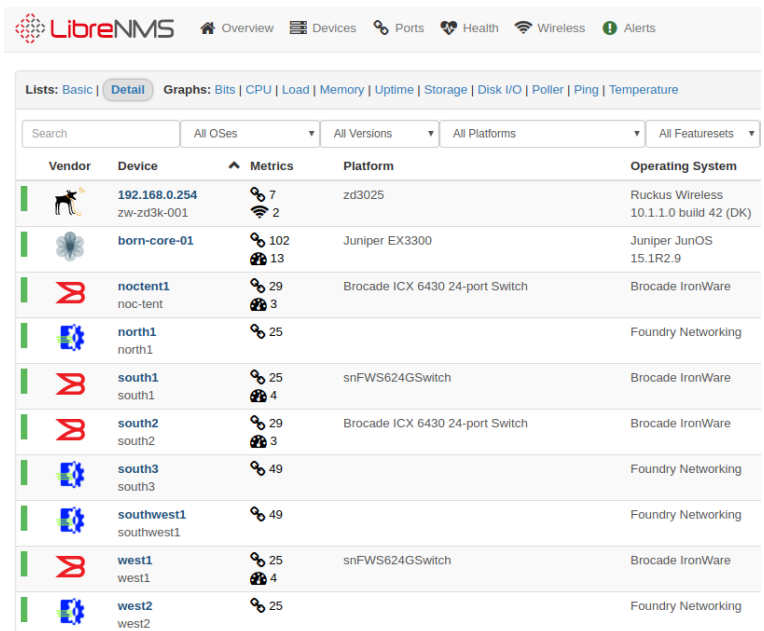
LLDP is needed!

Netflow processing from the web interface



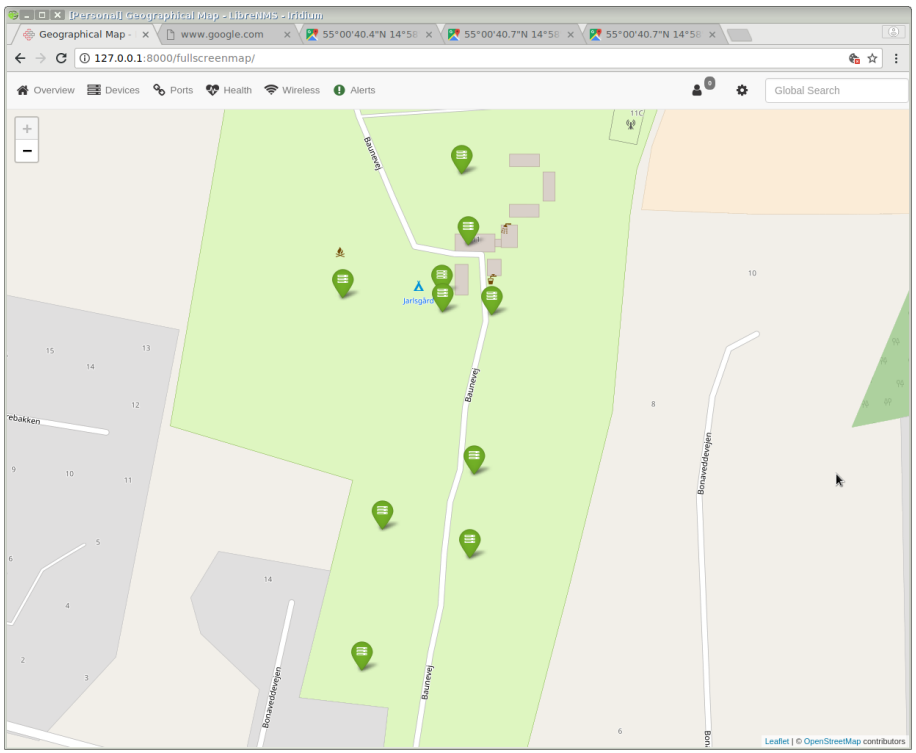
Bringing the power of the command line forward

LibreNMS Automatic discovery

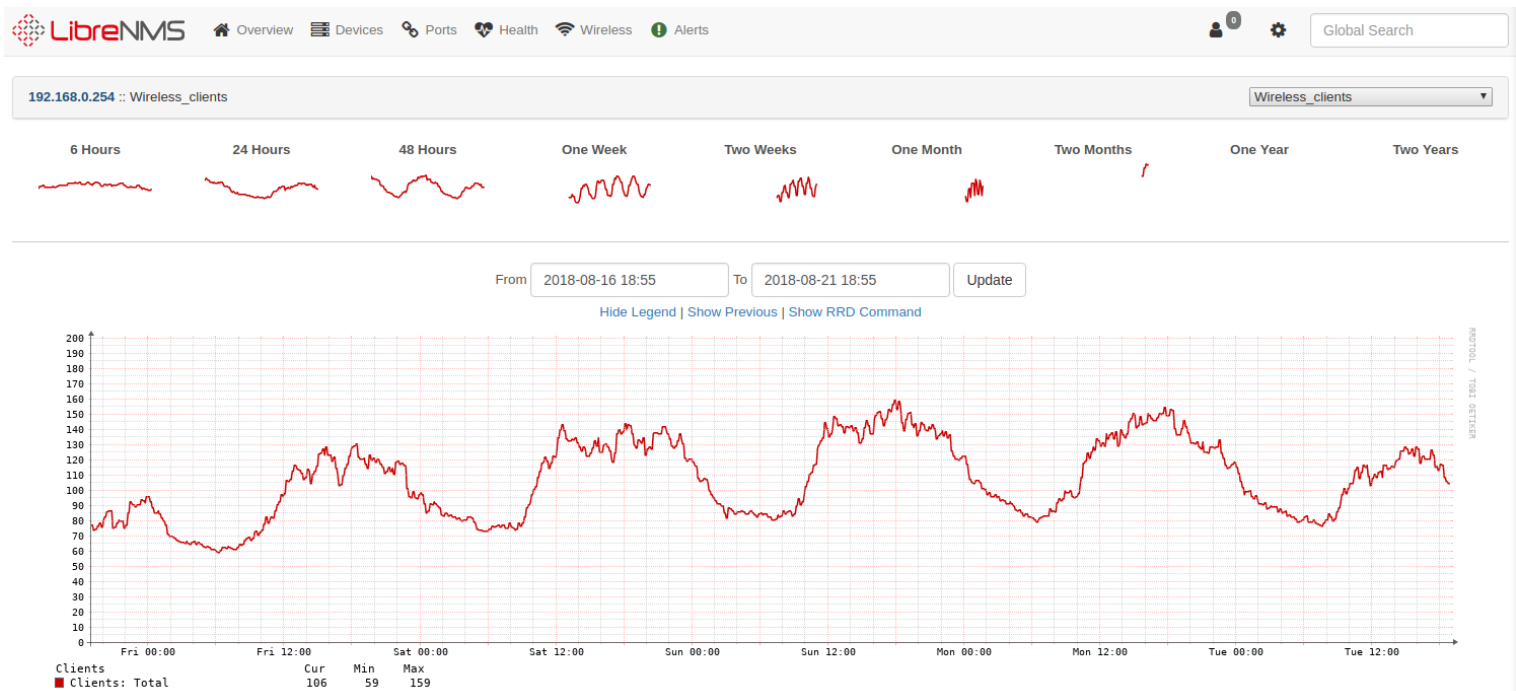


Automatically discover your entire network using CDP, FDP, LLDP, OSPF, BGP, SNMP and ARP.

LibreNMS Geo Location



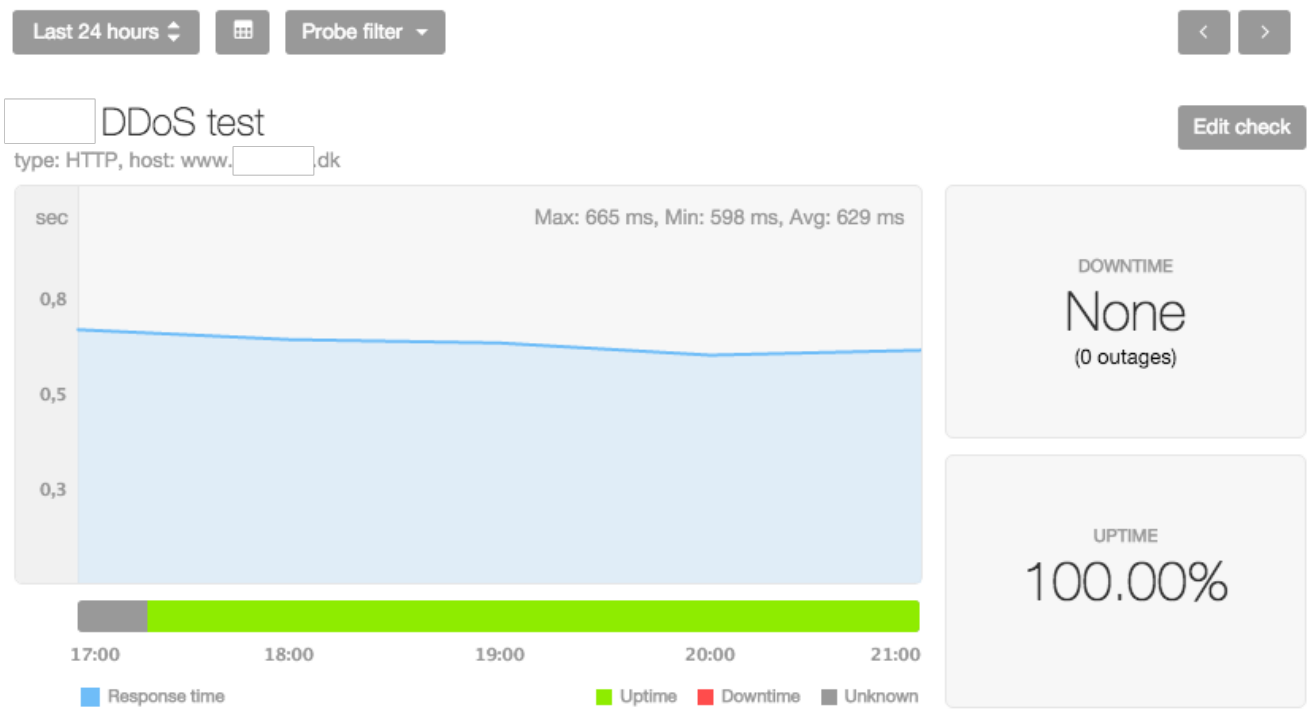
LibreNMS wireless clients



Demo

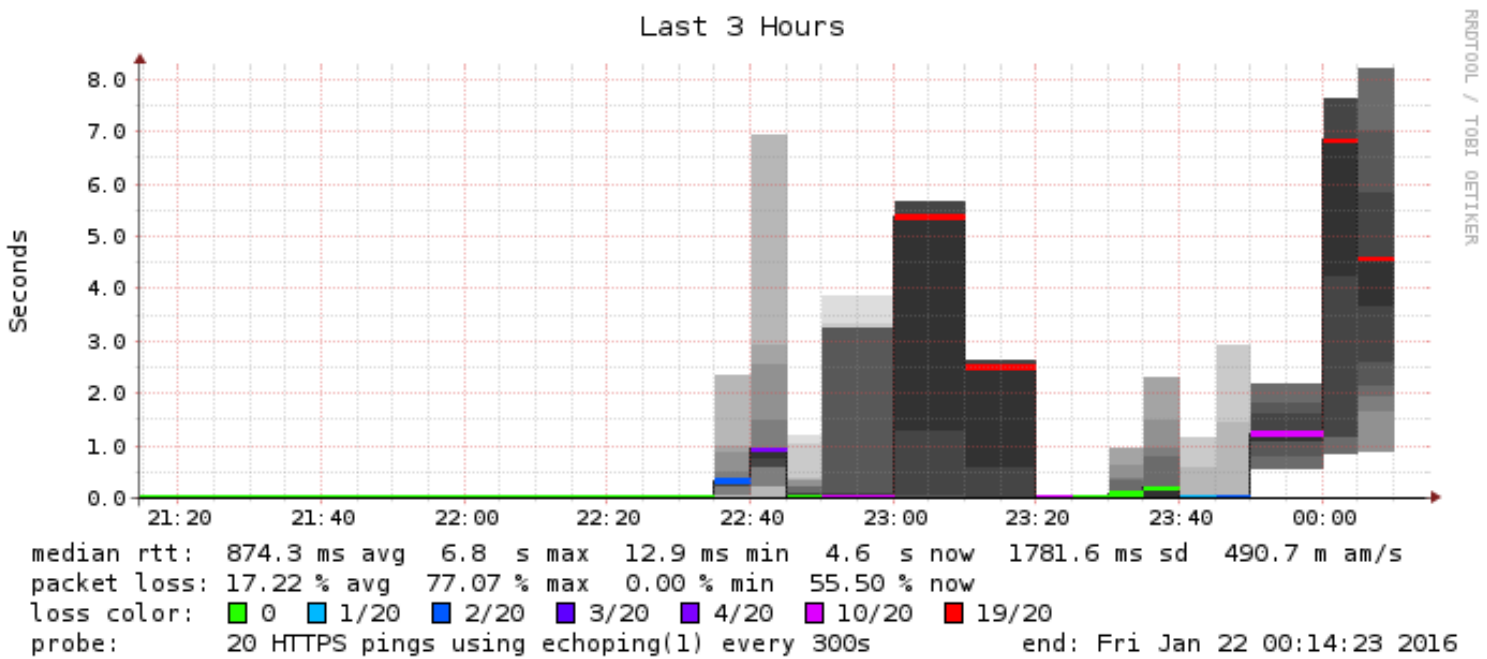
- Demo: Unifi dashboard
- Demo: LibreNMS and Smokeping

Before testing: Pingdom



Another external monitoring from Pingdom.com

Problems in the network



Oh no DDoS attack?

What to put into the Dashboard

Chapter 11. Anomaly-Based Detection with Statistical Data

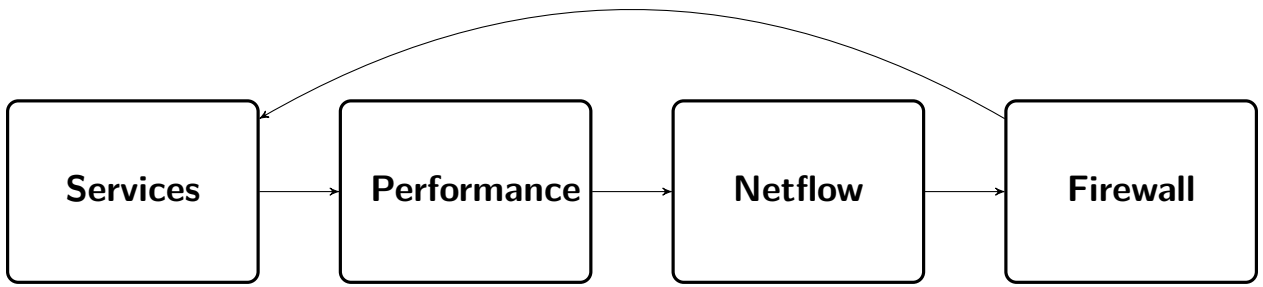
Good advice found in the book:

- Top Talkers with SiLK
- Service Discovery with SiLK
- Furthering Detection with Statistics
- Visualizing Statistics with Gnuplot
- Visualizing Statistics with Google Charts
- Visualizing Statistics with Afterglow

Newer and other tools exist, but the process is the same.

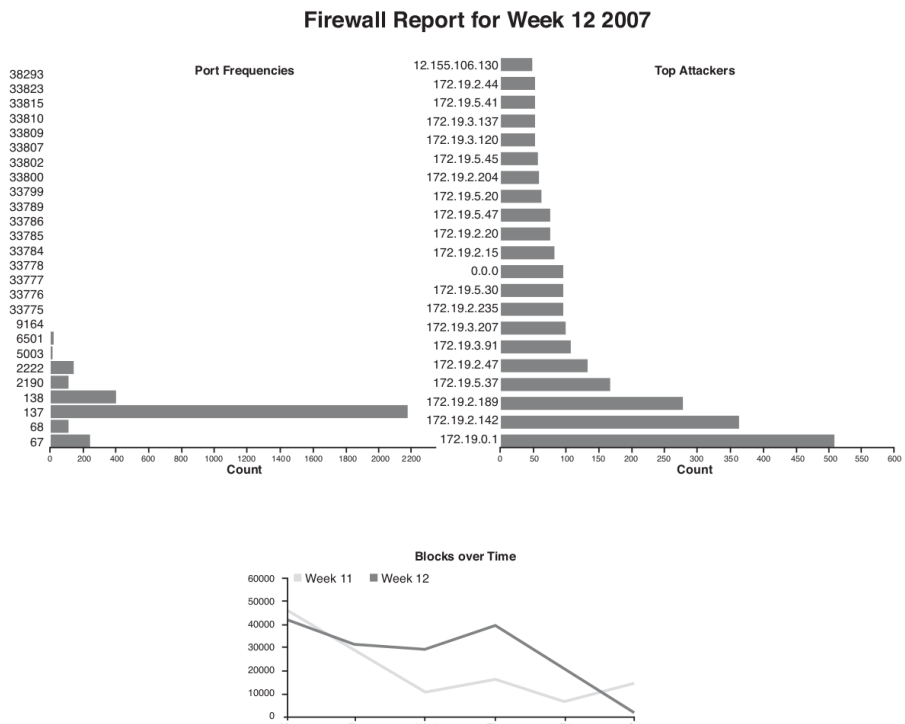
Source: Applied Network Security Monitoring Collection, Detection, and Analysis, 2014 Chris Sanders ISBN: 9780124172081

Map sources to dashboards!



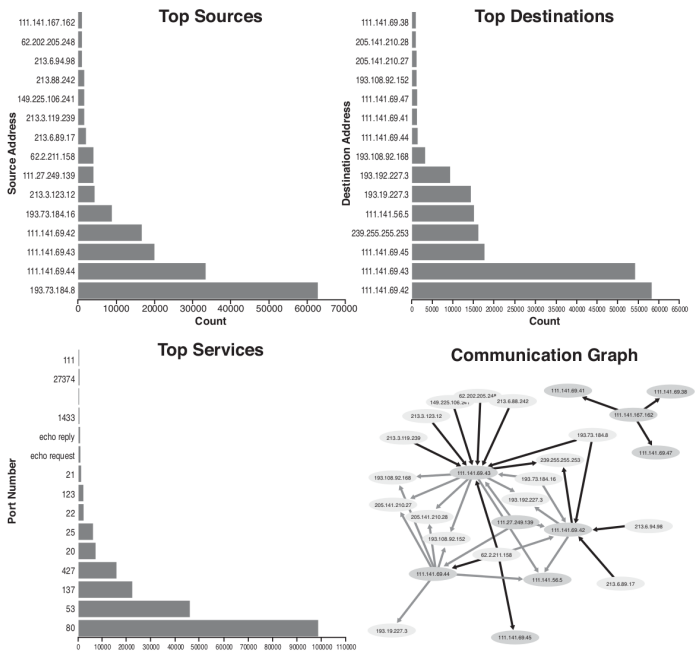
- There are many input sources available
- Dont put them all in ONE DASHBOARD
- I had luck in creating multiple dashboards, and then having a display cycle through them
- Maybe use Elastic Spaces for this? `https://www.elastic.co/guide/en/kibana/master/xpack-spaces.html`

Applied Security Visualization examples



Source: Firewall Report in *Applied security visualization*, Rafael Marty, 2009

Applied Security Visualization examples



Source: Network Flow Data in *Applied security visualization*, Rafael Marty, 2009

Drill down process

1. Get an overview
2. Research top talkers,
3. When identified and handled, remove with filter `not host 10.1.2.3`
4. Look at the next ones

Look into details, lookup hostsnames – hopefully your tool allows some help

Alerting

We're excited to announce a new alerting framework that delivers a first-class alerting experience natively within the SIEM, Uptime, APM, and Metrics applications as part of the Kibana 7.7 release.

Alerting is a fundamental use case across the Elastic Stack, which is why we're making it part of the core experience within Kibana. Whether you are monitoring application transactions or tracking brute force login attempts, our goal is to provide a tailored experience that allows you to build powerful alerts in the normal flow of your task. The new alerting framework is built from the ground up and designed to offer more than just convenient interfaces. We understand the need to go beyond just notifying people which is why we've also incorporated the ability to trigger predefined actions that can do anything from sending an email to using brand new third-party integrations with platforms like Slack and PagerDuty.

The new alerting framework is being introduced as a beta in the 7.7 release of Kibana and is available immediately on the Elasticsearch Service on Elastic Cloud, or for download.

- `https://www.elastic.co/blog/introducing-the-new-alerting-framework-for-observability-securit`
- `https://www.elastic.co/what-is/kibana-alerting`
- `https://www.elastic.co/blog/alerting-in-the-elastic-stack`

Alerting everywhere

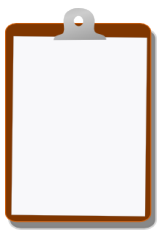
> Alerting everywhere: Kibana 7.7 introduces ubiquitous alerting for Elastic Observability, Elastic Security, and the Elastic Stack. Users can now create alerts directly from within the SIEM, APM, Metrics, and Uptime applications as well as for any index.

- Seems a lot has happened with alerting in the new version!
- Lets try to work with the alerting framework, note: sending email can sometimes be tricky without some configuration.

Moving to next time, with baseline your data

Discussion! Writing and presenting are two very different things, so are dashboards and reports!

For Next Time



Think about the subjects from this time, write down questions

Check the plan for chapters to read in the books

Visit web sites and download papers if needed

Retry the exercises to get more confident using the tools