Network Monitoring: The Foundation of Campus Security

Philip Smith

philip@nsrc.org

PacNOG 26 Online

30th June 2020

UNIVERSITY OF OREGON

Last updated 29th June 2020

NSRC

Network Startup Resource Center

Security is Hard

- Securing and monitoring the security of a campus network is difficult
- Campus networks need to be fairly open
  - Research and Education needs flexible and open networks
  - NAT makes some things hard (eg H.323 video conferencing)
  - Filtering makes it hard for researchers, teachers, and students to do interesting things
  - Your campus network must not be the bottleneck
- Always will have viruses, attacks, and people generally acting bad

Campus Networks and Security

- Goal: Prepare for problems you **will** have
  - You **will** have compromises and hackers
  - You **will** have viruses
- You get a call from your ISP saying that they have a report that one of your hosts is participating in a Denial of Service (DoS) attack
  - What do you do?
  - How do you find the host (can be very hard with NAT)?

Security is a Process

You can never achieve security – it is a process that you have to continually work on

- Assessment – what is at risk
- Protection – efforts to mitigate risk
- Detection – detect intrusions or problem
- Response – respond to intrusion or problem
- Do it all over again

Security Outline

- Policy Framework
- Security Foundation = Network Management
- Encryption
- Virus Protection
- Authentication and Authorization
- Blocking Certain Types of Traffic
- Network Architecture and Firewalls

Security Foundation

- You **must** have managed equipment in your network
- You **must** have some basic network management running

- Network Management is the foundation that virtually all of the security framework operates on

Core Network Monitoring & Management Concepts

- What & Why we Monitor
- Baseline Performance
- Network Attack Detection
- What & Why we Manage
- Network Monitoring & Management Tools
- The NOC: Consolidating Systems

Network Monitoring & Management

Monitoring

- Check the status of a network

Management

- Processes for successfully operating a network

Monitoring Systems & Services

- Systems
  - Routers
  - Switches
  - Servers
- Services
  - DNS
  - HTTP
  - SMTP
  - SNMP

Why do we Monitor?

- Are Systems and Services Reachable?
- Are they Available?
- What’s their Utilisation?
- What’s their Performance
  - Round-trip times, throughout
  - Faults and Outages
- Have they been Configured or Changed?
- Are they under Attack?

Why do we Monitor?

- Know when there are problems – before our customers!
- Track resource utilisation, and bill our customers
- To Deliver on Service Level Agreements (SLAs)
  - What does management expect?
  - What do customers expect?
  - What does the rest of the Internet expect?
- To prove we're delivering
  - What would Five Nines take? 99.999%
- To ensure we meet SLAs in the future
  - Is our network about to fail? Become congested?

Uptime Expectations

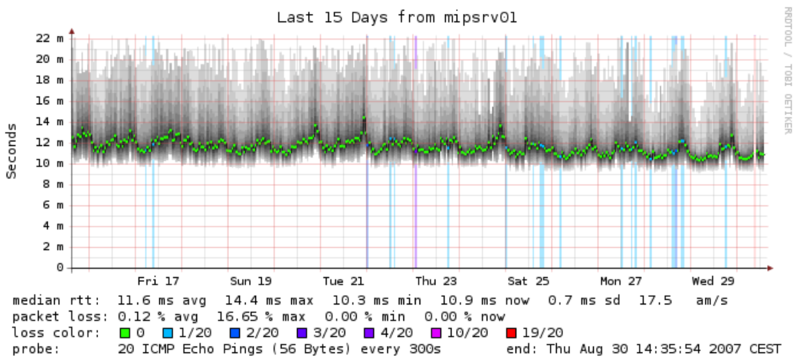
- What does it take to deliver 99.9% uptime?
  - – Only 44 minutes of downtime a month!
- Need to shut down one hour a week?
  - – 168 hours in week
  - – That's only 99.4% uptime ((168-1)/168 = .99404762...)
- What does 99.999% uptime really mean?
  - – 525960 (approx) minutes in a year
    - 99.999% uptime means 5 minutes and 15 seconds downtime!
    - For most of us this is just a fun exercise, not realistic.
- Maintenance might be negotiated in SLAs

Uptime Expectations

- What is meant by the network is “up”?
  - Does it work at every location?
  - Does it work at every host?
  - Is the network up if it works at the Boss’s desk?
  - Should the network be reachable from the Internet?
  - Does uptime include or exclude “Scheduled Maintenance”?

Establishing a Baseline

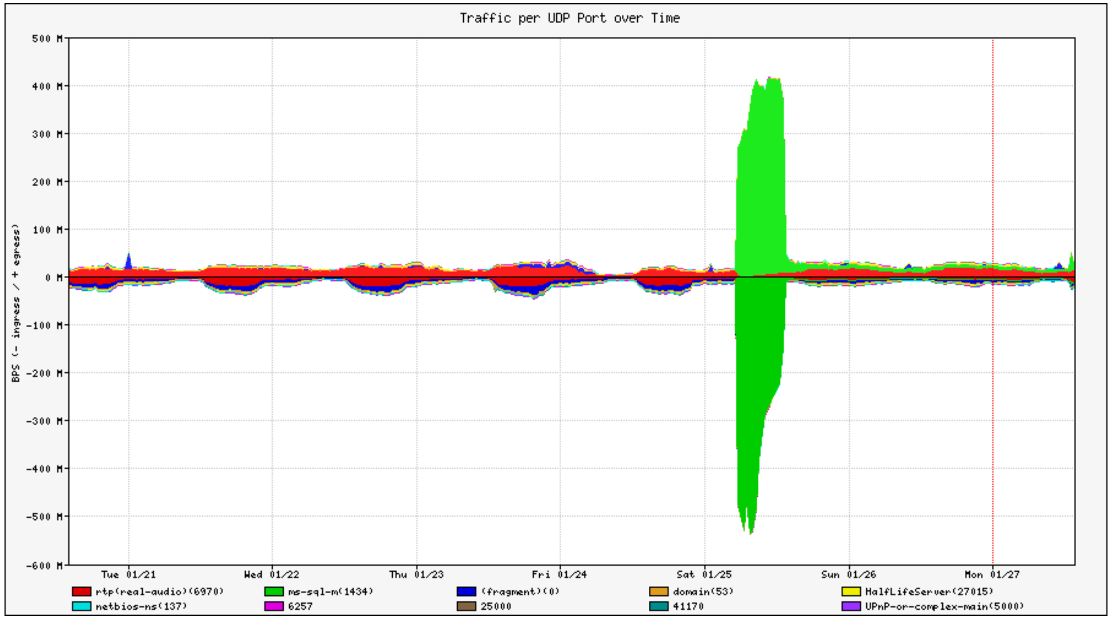
- **Monitoring** can be used to **Establish a Baseline**
- Baseline = What’s normal for your network?
  - Typical latency across paths
  - Jitter across paths (shown in graph)
  - Load on links
  - Percent Resource Utilisation
  - Typical amounts of noise
    - Network scans & random attacks from the Internet
    - Dropped packets
    - Reported errors or failures



```
median rtt:   11.6 ms avg   14.4 ms max   10.3 ms min   10.9 ms now   0.7 ms sd   17.5   am/s
packet loss:  0.12 % avg   16.65 % max   0.00 % min   0.00 % now
loss color:   🟩 0   🟦 1/20   🟦 2/20   🟪 3/20   🟪 4/20   🟪 10/20   🟥 19/20
probe:        20 ICMP Echo Pings (56 Bytes) every 300s          end: Thu Aug 30 14:35:54 2007 CEST
```

Detecting Attacks

- Deviation from baseline can mean an attack…
- Are there more flows than usual?
- Is the load higher on some servers or services?
  - CPU usage on border router?
- Have there been multiple service failures?



Any of these might mean attack

What do we Manage?

- Asset management: What equipment have we deployed?
  - What software is it running
  - What's its configuration (hardware & software)
  - Where is it installed
  - Do we have spares?
- Incident management: fault tracking and resolution
- Change management: Are we satisfying user requests?
  - Installing, moving, adding, or changing things
- Staff management

Why do we Manage?

- To ensure we meet business requirements for service level, incident response times, etc.
- To make efficient use of our resources (including staff)
- To learn from problems and make improvements to reduce future problems
- To plan for upgrades, and make purchasing decisions with sufficient lead time
- To help maintain a secure network

Key Network Management Tools

- Are some devices not responding or responding poorly, possibly because of a DoS attack or break-in?
  - Nagios
  - Smokeping
- Are you seeing unusual levels of traffic?
  - Cacti
  - LibreNMS
  - NetFlow with NfSen (sFlow, J-Flow, IPFix), Elastiflow

Network Traffic Analysis

- It is important to know what traverses your network
  - You learn about a new virus and find out that all infected machines connect to 128.129.130.131
  - Can you find out which machines have connected?
- Some tools that are available
  - NetFlow
  - Snort: open source intrusion detection system that is very useful to find viruses

Log Analysis

- Can be just as important as traffic analysis
- Central syslog server and gather logs from:
  - DHCP server, DNS servers, Mail servers, switches, routers, etc.
  - Now, you have data to look at
  - Given an IP, you can probably find user
- Lots of tools to correlate logs and alarm on critical events

NetFlow

- Routers can generate summary records about every traffic session seen
  - src addr, src port, dst addr, dst port, bytes/packets
- Software to record and analyze this data
  - e.g. Nfdump + NfSen or Elastiflow
- Easily identify the top bandwidth users
- Drill down to find out what they were doing

Beware: Network Flows and NAT

- You need to see the real (internal) source IP addresses, not the shared external address
- If you are doing NAT on the border router that’s not a problem
  - Generate Network flows on the interface before the NAT translation
- If you are doing NAT on a firewall then you need to generate Network flow data from the firewall, or from some device behind the firewall

Anomalous Traffic

- Intrusion Detection Systems (e.g. Snort) can identify suspicious traffic patterns, e.g.
  - machines using Bittorrent
  - machines infected with certain viruses/worms
  - some network-based attacks
- Typically connect IDS to a mirror port
- Risk of false positives, need to tune the rules
- Starting point for further investigation

Associating IP address to user

- ARP/DHCP logs map IP to MAC address
- Bridge tables map MAC address to switch port
  - Several tools can do this, e.g. Netdot, LibreNMS
- 802.1x/RADIUS logs for wireless users
- AD logs for domain logins to workstations
- Network Access Control
  - e.g. PacketFence, forces wired users to login

Using Net Management

- BAYU: “Be Aware You’re Uploading”
- Detect P2P like Bittorrent and automatically send a warning E-mail telling the user to check whether what they’re doing is legal
- Amazingly effective when people realize they’re being watched!
- Some users may not be aware they had Bittorrent installed, and will uninstall it
- University of Oregon did this and Bittorrent use is now virtually non-existent.

Other Network Management Tools

- Ticket Systems: RT (Request Tracker)
  - Manage provisioning & support
- Configuration Management: RANCID or Oxidized
  - Track network device configurations
- Network Documentation: NetBox
  - Inventory, Location, Ownership of Network Assets

A few Open Source NMM Tools

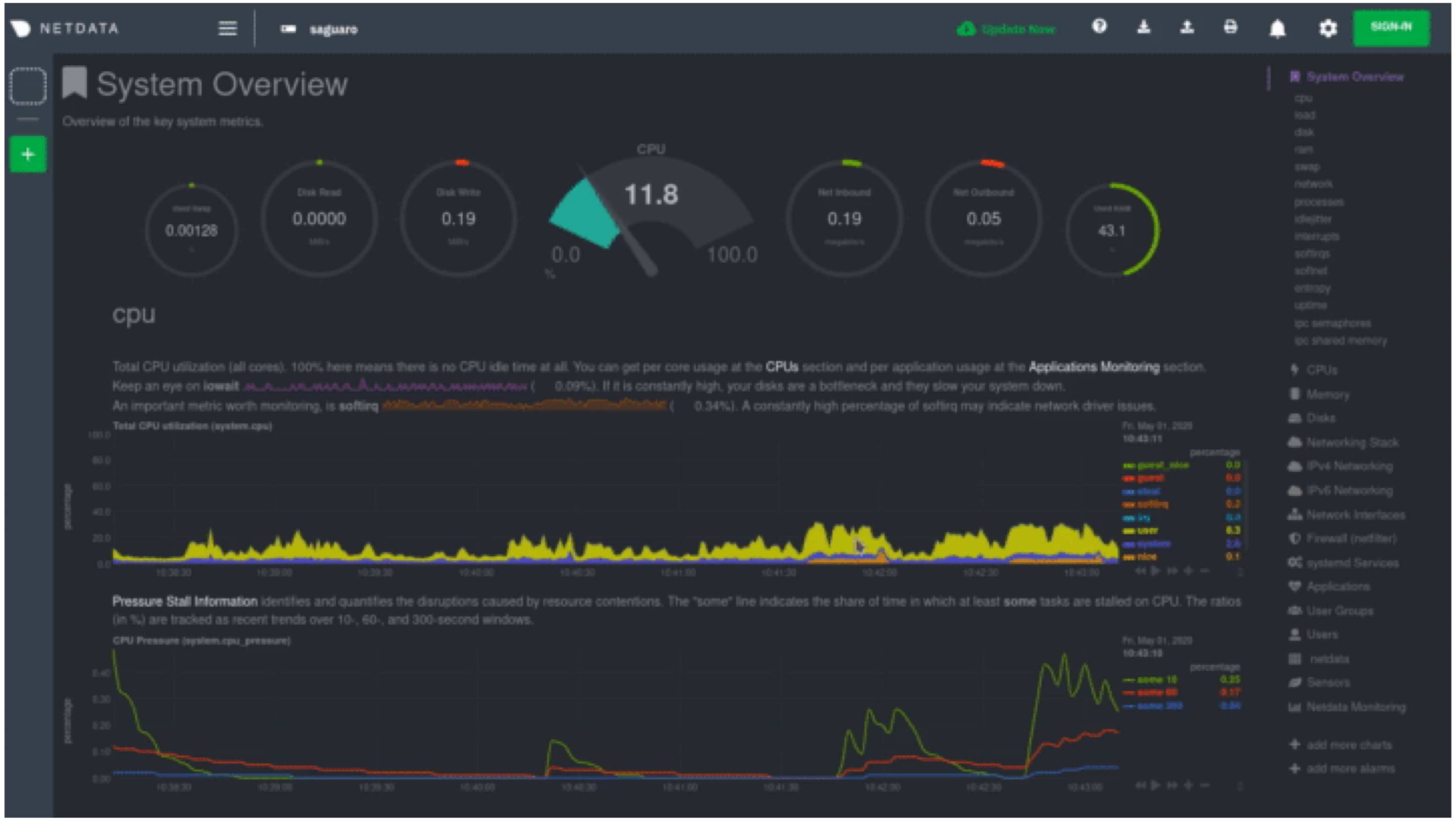
Performance	**Change Management**	**Net Management**	**Ticketing**
Cricket	Mercurial	Big Brother	OTRS
Elastiflow	RANCID	Cacti	RT
flowc	Oxidized	Hyperic	Trac
IPFix	CVS	LibreNMS	Redmine
mrtg	Subversion	Nagios	**Documentation**
NetFlow	git	OpenNMS	IPplan
NfSen	Security/NIDS	Prometheus	Netdisco
ntop	Nessus	Sysmon	Netdot
perfSONAR	OSSEC	Zabbix	NetBox
pmacct	Prelude	**Logging**	**Utilities**
RRDTool	Samhan	Loki	SNMP, Perl
Sflow	SNORT	Swatch	Ping, Regex
SmokePIng	Untangle	Tenshi	Shell scripting

What about NMM 2.0?

- The model we present is:
  - Classic polling model
  - Course data collection (5 minute intervals typically)
- In current use includes:
  - Telemetry
  - Pull methodology and agent-based
  - Time series databases (large) often NoSQL based
  - Collectors and parsers
- Common terminology you may have heard of:
  - ELK, TICK, Kafka, Prometheus Stacks
  - Grafana, InfluxDB, MongoDB
  - Beats, Elasticsearch, Elastiflow, fluentd, Kabana, etc…

NMM 2.0: Netdata

– https://github.com/netdata/netdata/wiki
– Real-time, fine-grained, detailed host monitoring.



System Overview

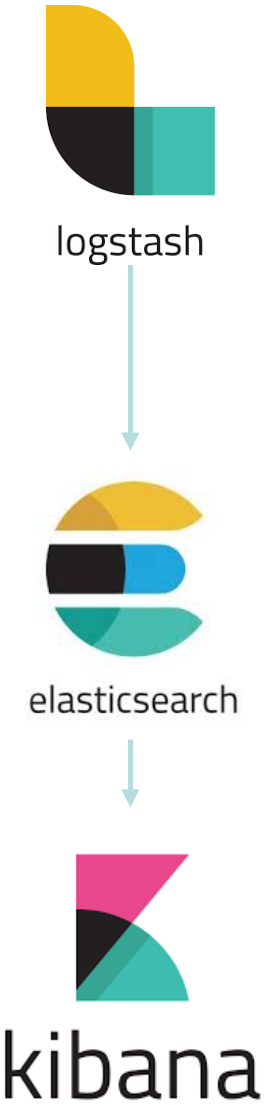
Overview of the key system metrics.

cpu

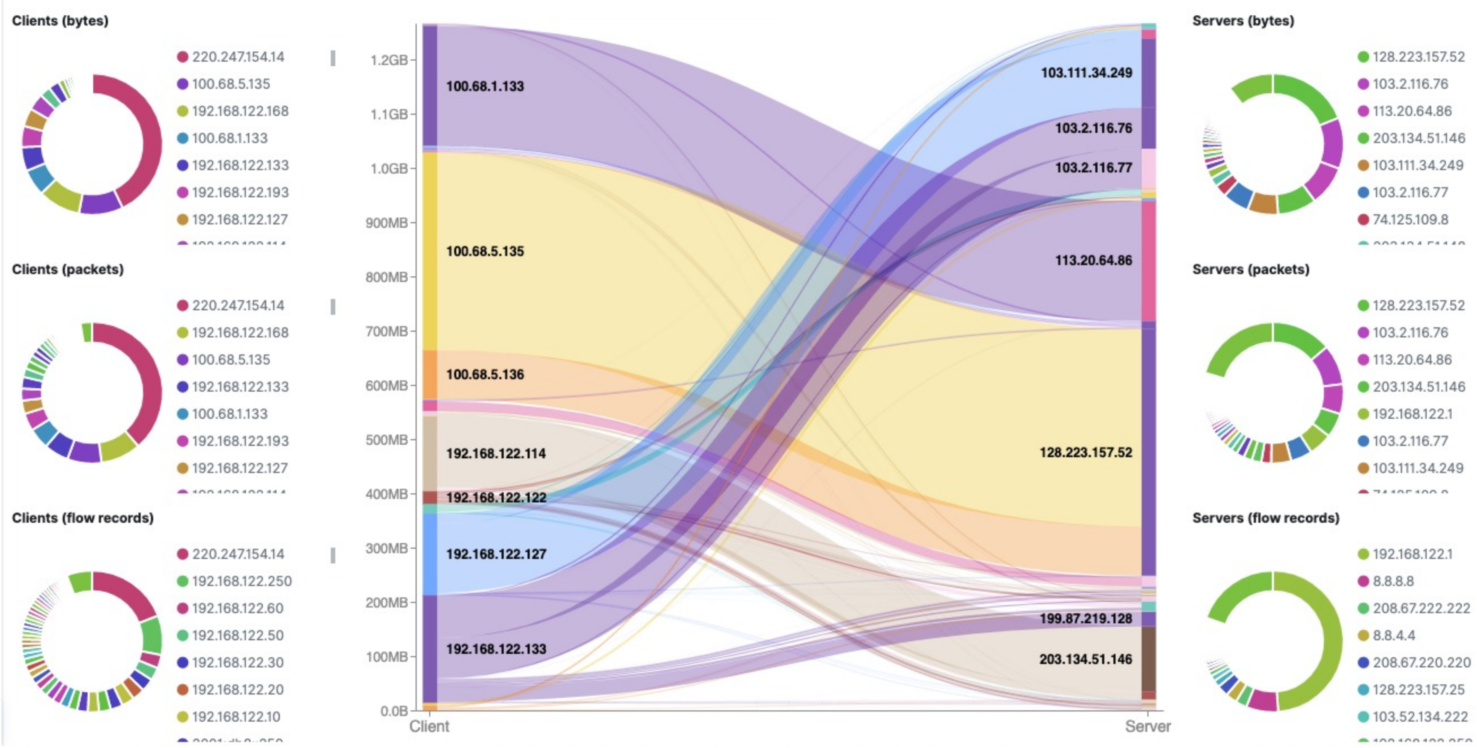
Total CPU utilization (all cores). 100% here means there is no CPU idle time at all. You can get per core usage at the **CPUs** section and per application usage at the **Applications Monitoring** section.
Keep an eye on **iowait** (0.09%). If it is constantly high, your disks are a bottleneck and they slow your system down.
An important metric worth monitoring, is **softirq** (0.34%). A constantly high percentage of softirq may indicate network driver issues.

Pressure Stall Information identifies and quantifies the disruptions caused by resource contentions. The "some" line indicates the share of time in which at least **some** tasks are stalled on CPU. The ratios (in %) are tracked as recent trends over 10-, 60-, and 300-second windows.

NMM 2.0: ElastiFlow

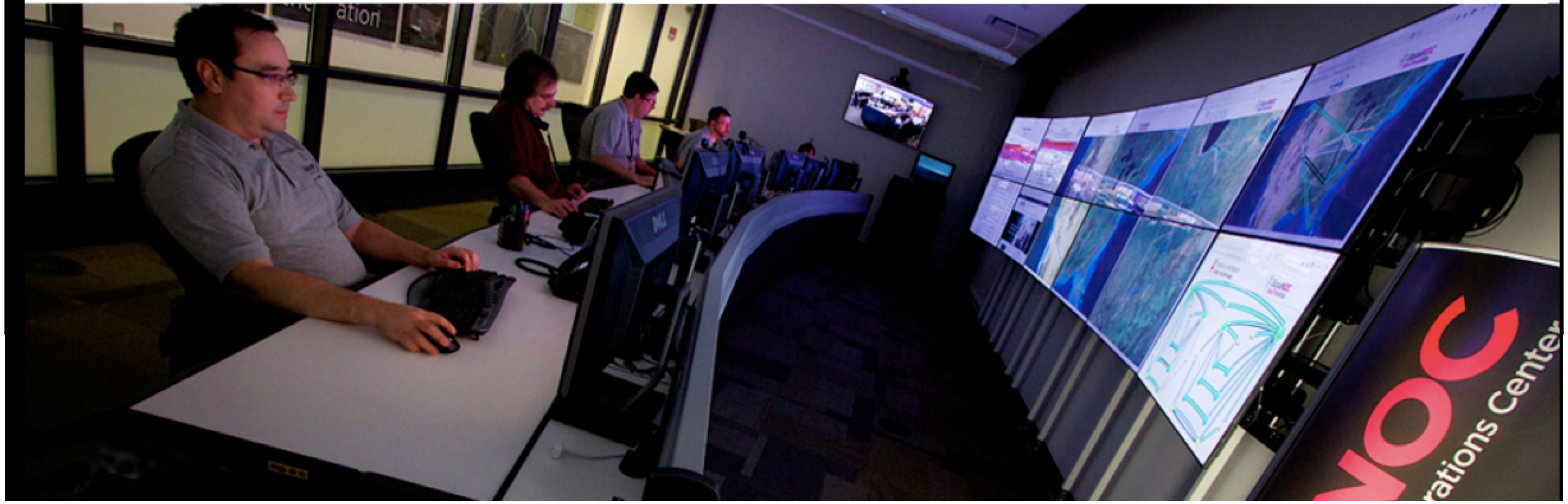


- Takes the following flow protocols
  - Netflow – IPFix – Sflow
  - Instead of NfSen
  - https://github.com/robcowart/elastiflow



NOC: Consolidating NMM Systems

- NOC = Network Operations Center
  - Coordination of tasks, handling of network related incidents (ticketing system)
  - Status of network and services (monitoring tools)
  - Where the tools are accessed
  - Store of Documentation (wiki, database, repository => network documentation tool(s))
- NOC Location
  - NOC is an organizational concept
  - Does not need to be a place, or even a single server
  - Remote / Distributed NOC is valid with OOB Management


ation
NOC
rations Center

NMM Review

- Campus Security Foundations
- What & Why we Monitor
- Baseline Performance & Attack Detection
- Network Attack Detection
- What & Why we Manage
- Network Monitoring & Management Tools
- The NOC: Consolidating Systems

Questions?