New Network!

Now, let's secure it.

Adair Thaxton
Cyberinfrastructure Security Engineer
Internet2

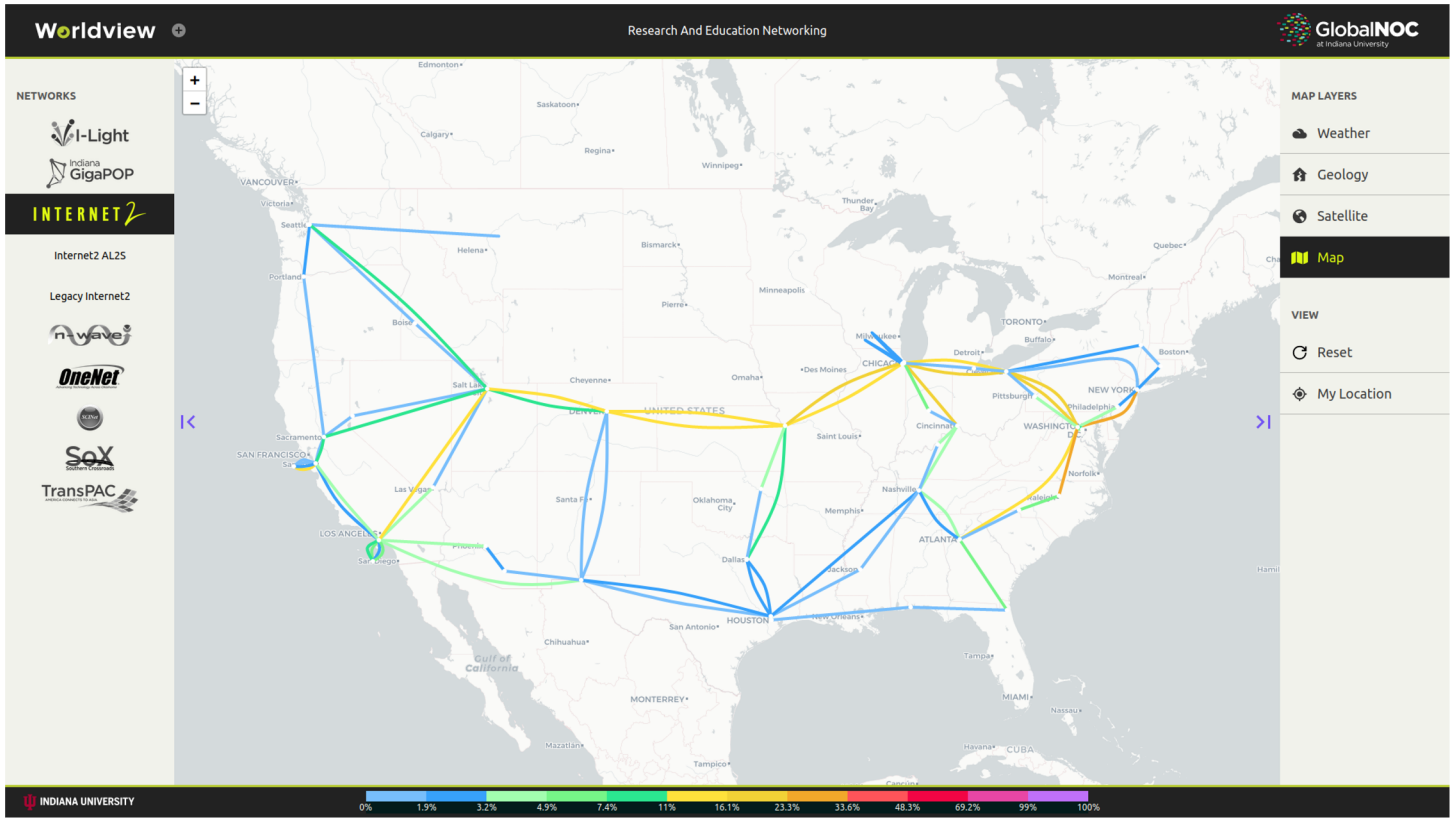
A brief warning

What is Internet2?

Internet2 is the non-profit research and education community's high-speed backbone network within the United States, connecting US researchers and students with peers across the globe. We're in 350 PoPs nationwide.

Requisite network map

11:45am on a school day



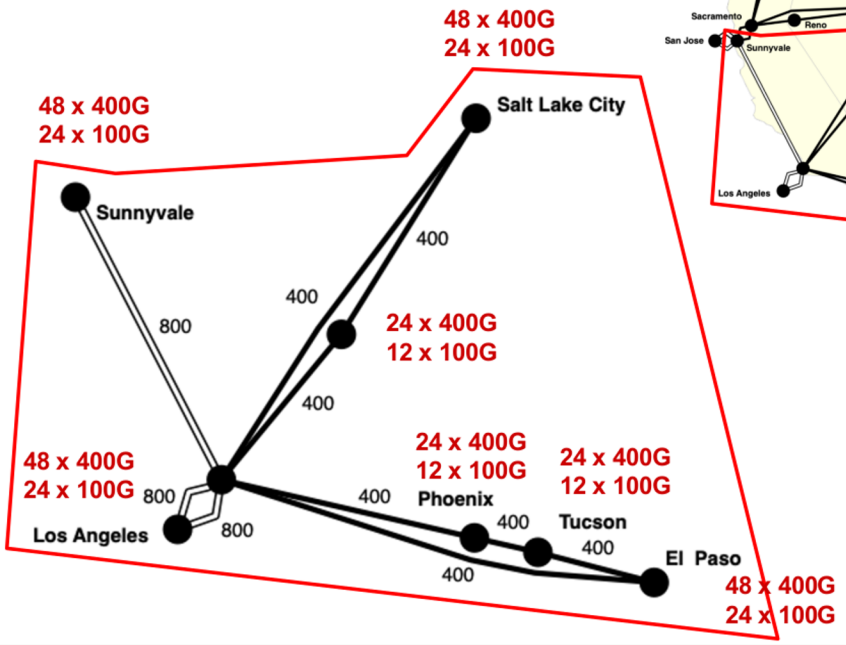
NGI and SMN

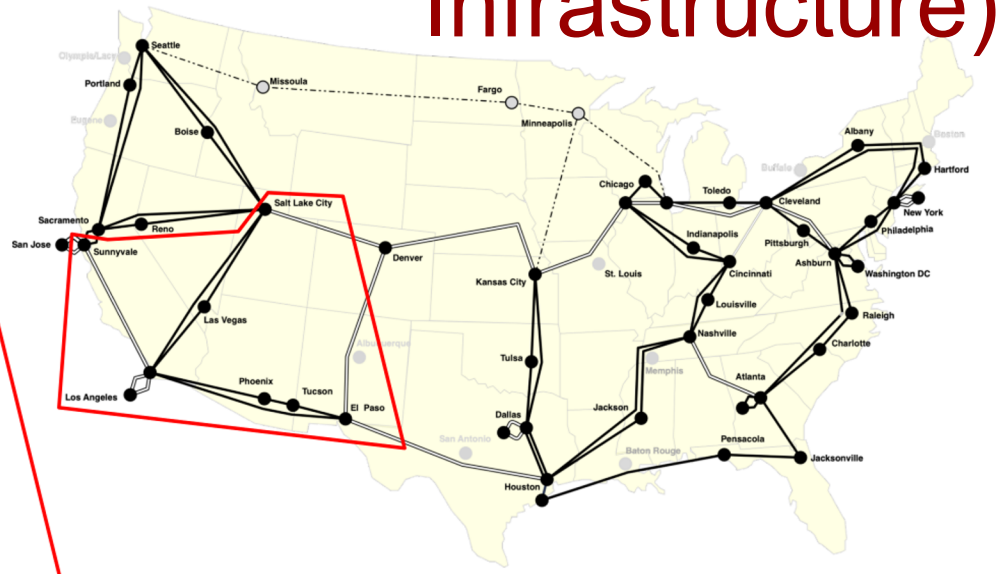
Internet2 has spent the past six years preparing for, planning, and completing the upgrade to our Next Generation Infrastructure (NGI).

Planning for the Secure Management Network (SMN) began in 2017.

Network Upgrades In NGI (Next Generation Infrastructure)

NGI System As Built





Data-Intensive Research

- 2 x 400 Gbps minimum intra-node capacity
- 2.4+ Tbps exit capacity available many 3-way sites (some have 3.2 Tbps)

What are we trying to address?

- We had previously used ACLs, but ACLs aren't stateful.
- We had incorporated some thresholding for control-plane policing, but the values were chosen somewhat randomly.
- We also wanted to filter OUTBOUND traffic, too.

Previous network management

In-band SSH to devices (same for telemetry, etc)

Out-of-band:

- Cisco 2600s and 2900s, configured for reverse telnet
- Terminal servers

Secure Management Network: A strategic shift

- What needs to go via SMN (out-of-band)?
  - Everything R/W, some telemetry (SNMP, etc)
  - Primary path for traffic required to restore network access
- What needs to go in-band?
  - Anything bandwidth intensive
  - Potentially RO telemetry (netflow)
  - Software limitations

Tooling changes

We have extensive home-grown tools, but the “primary key”, so to speak, has always been a single IP address. This meant that we needed to make major changes to those tools, allowing for a primary access path (SMN) and a backup access path (in-band), minimizing impact during a potential SMN outage.

Secure Management Network topology

SMN Firewall - Bigger firewall at Entry/Exit Sites

- Individual firewall zones routed via BGP as VRFs on the SMN routers

SMN Router - Dedicated router at every POP

- IS-IS to adjacent nodes
- Basic MPLS for VRFs

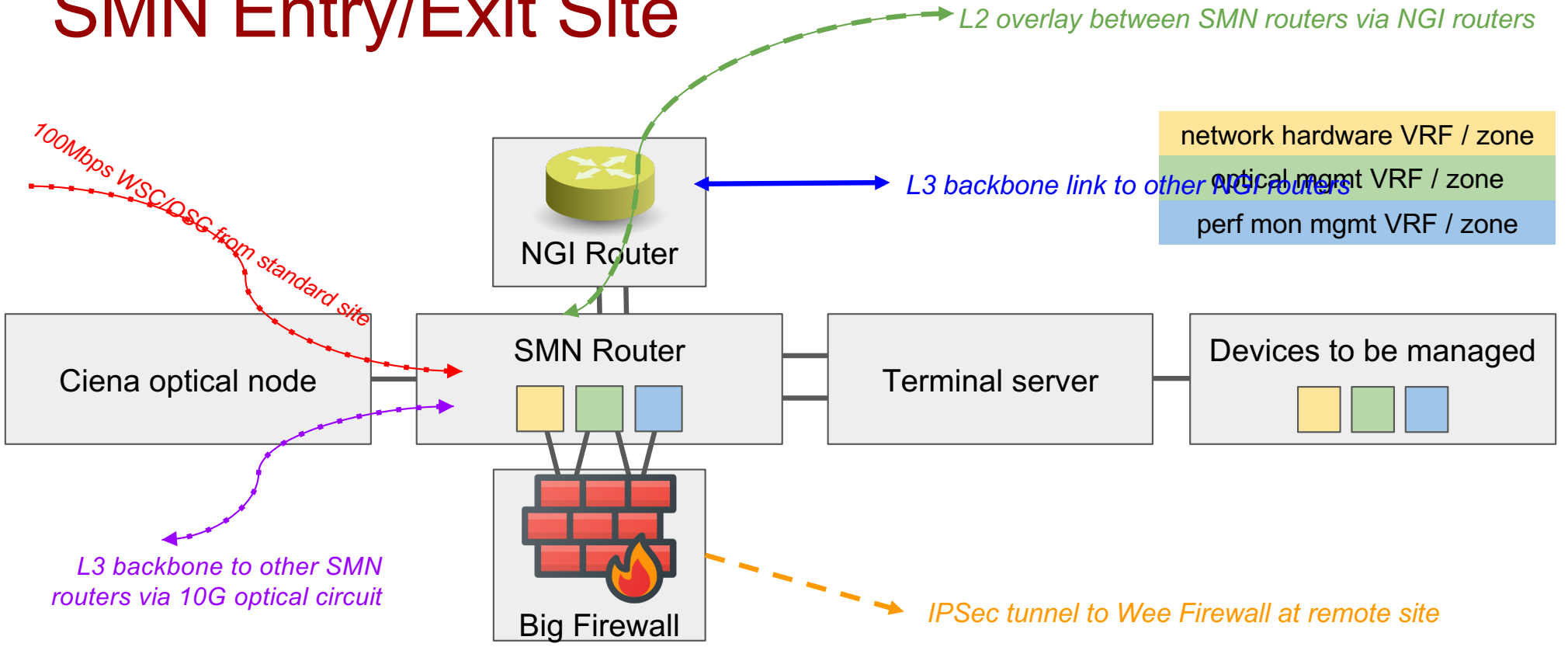
Console Server - Upgraded terminal servers

Greenfield Secure Management Network

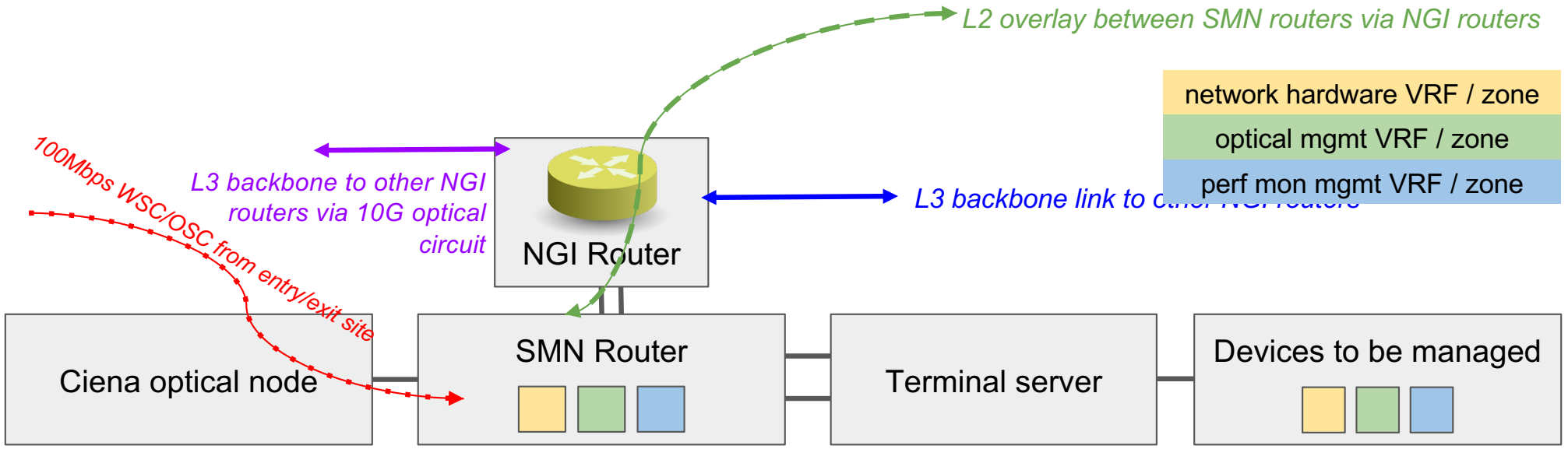
Three site types (each has an SMN router and console server)

- Entry/exit - sites with a bigger firewall and rules
- Standard - sites with no firewall
- Remote - sites with a smaller firewall using IPSec tunnels back to entry/exit sites

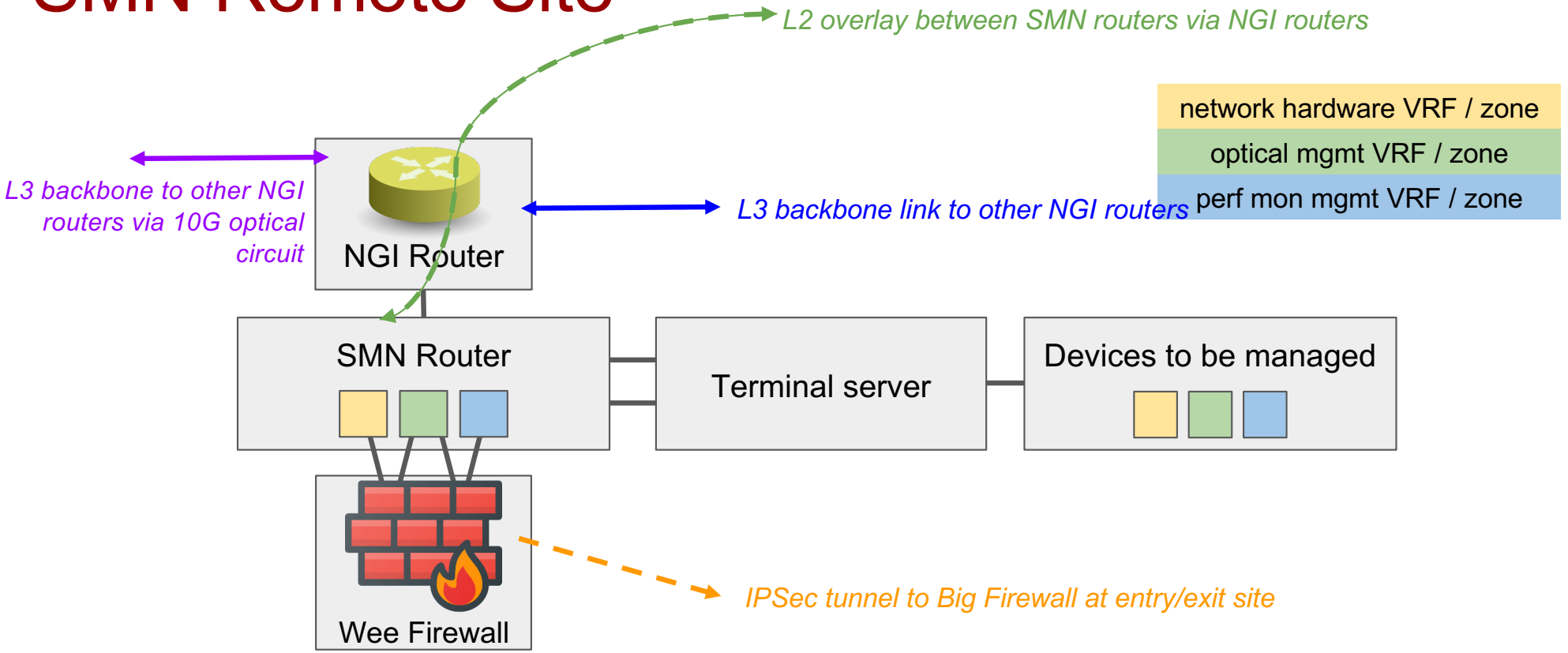
SMN Entry/Exit Site



SMN Standard Site



SMN Remote Site



SMN management

- Treated as first-class production network
  - 24/7 NOC monitoring and alerting
- Working to integrate Cisco NSO
  - Automated/standardized configuration
  - Policy change management

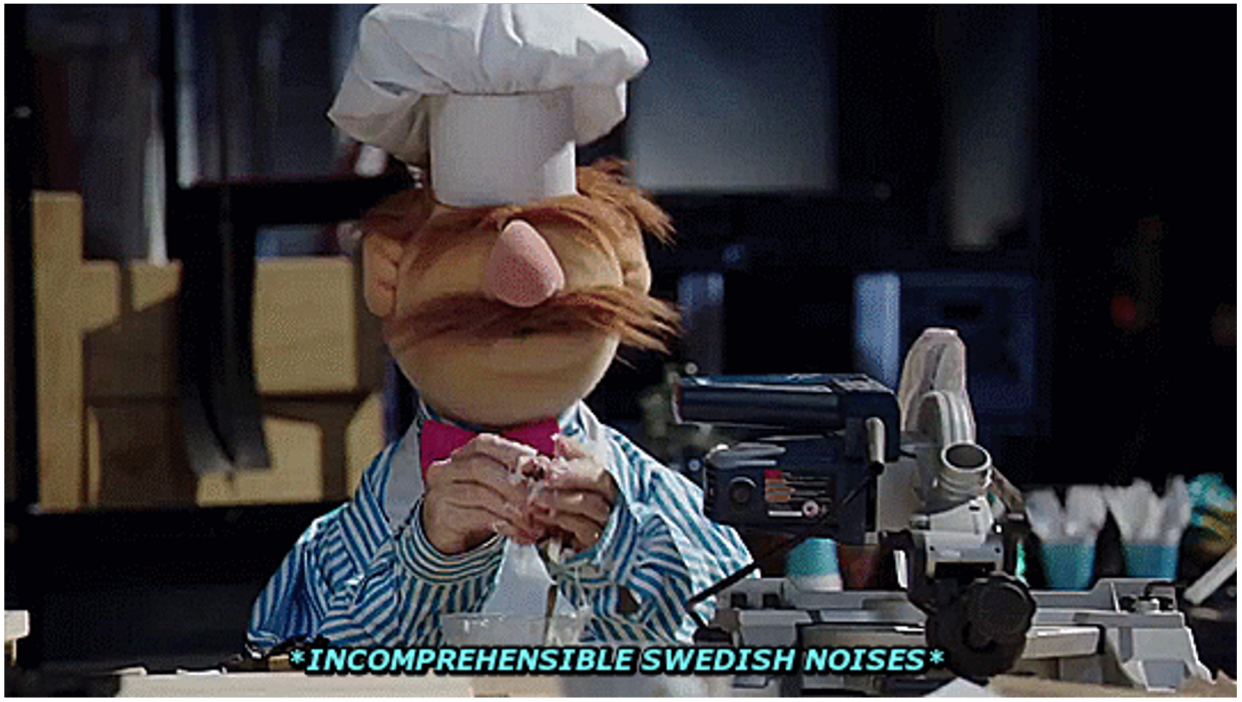
Creating the rules

- What do we know from existing rules?
  - The ACLs were pretty old…
  - What's changing?
  - What do we NOT know?

Cleaning up the rules

- Many things in permit-and-log, clean those up first
- Established Slack channels with stakeholders for each zone
- Creating and documenting policies for additions and changes
- All changes go through change management (retroactively, if necessary)

More firewall stuff



What's next?

- Quarterly reviews of rules and address-books
- Continuing to establish policies and procedures
- Refinement of the config auditing process
- External and internal scanning to verify that the rules and host configs are working properly.
- Failover testing to verify traffic flow in an outage.
- Training other engineers

Conclusion

This is still a work in progress, but we're working hard to get the Secure Management Network completed despite some delays.

Questions?