firewall tightening update

UNIX town hall
2016-09-22

why

DOE Enterprise Assessment finding:

SLAC network is too open to attack.

Reduce the porosity of its network perimeter

what

enable *application filtering* on our existing perimeter firewall

- only traffic between SLAC and the Internet is affected
- applications must be explicitly permitted
  - all applications needed for SLAC's operation will be supported
  - list of applications that are currently permitted is available on Confluence:
    "Applications Allowed to/from SLAC Building Office Network"
- both inbound and outbound traffic is covered
- high-volume scientific data transfers will bypass the firewall

very smart firewall

Palo Alto Networks 5060

stateful

knows about applications

inspects packets, layers 1-7

has dynamic threat database

i.e., *not your grandpappy’s firewall*

status

- about ~20 buildings now covered by the new firewall rules
  - 15, 23, 24, 25, 26, 27, 28, 30, 31, 33, 34, 35, 41, 50, 52, 53, 55, 81, 83, 102, 104
  - about 50% of SLAC employee offices
- some administrative data center networks are on the new rules as well
- currently working with science departments

- schedule:
  - target is to have most, if not all, of this work done by the end of this month

  - however, we will not put the mission at risk in order to meet that goal.

how

heads-up to each science ALD/department head, asked for technical contact if they wanted to pursue testing

for each subnet we're monitoring traffic in advance, to look for applications that are not yet supported.

we can then set up test periods:

- we temporarily apply the rules to specific machines or subnets specified by the technical contacts
- owners exercise their applications
- we watch for denied requests, technical contacts reflect back any issues

help us test

if you are concerned that the tightened firewall may impact your work, join a test

- Submit a ServiceNow ticket, or email ithelp@slac
  - subject: “Firewall testing”
- Provide your device name, IP, and hardware (MAC) address if possible

perfection is elusive

even with analysis and testing, it’s impossible to discover 100% of network application usage in advance

even if we could, a new user, employee, or good idea can appear at any time

we can open a filtered application quickly *post hoc*…
...but we’re working to be as proactive as possible

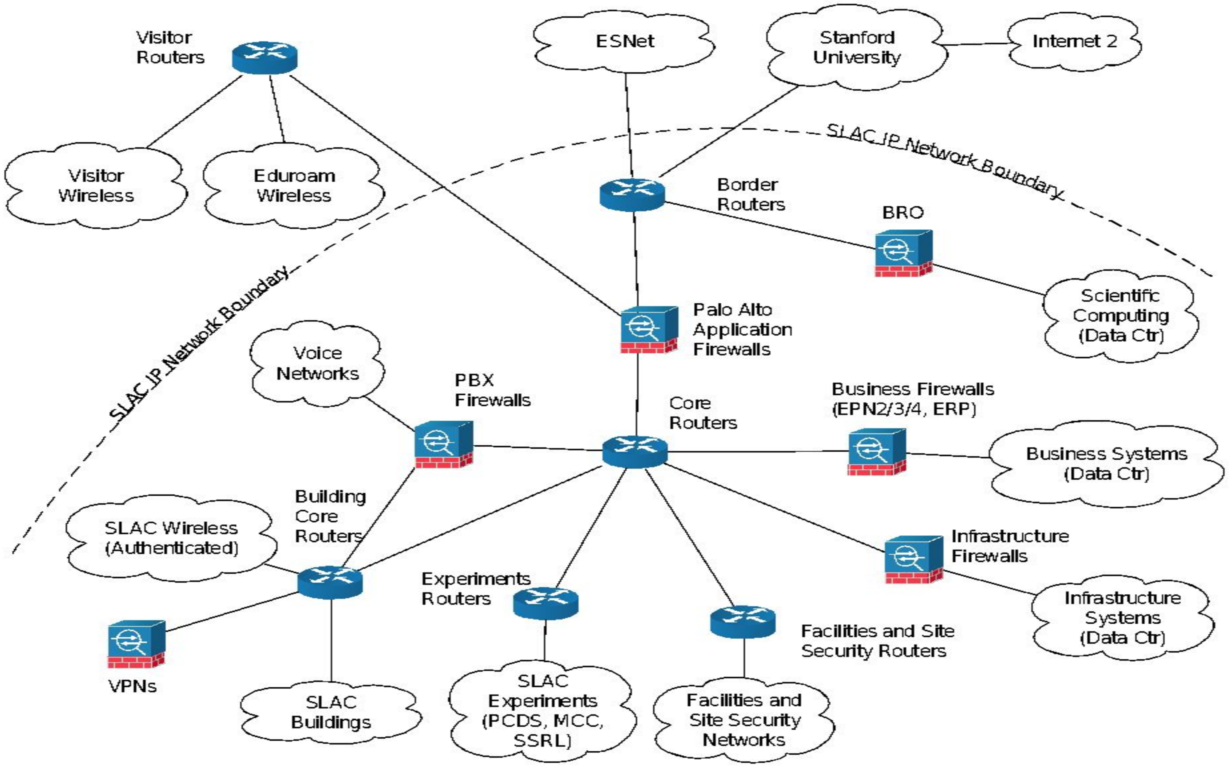
salience

once the new rules are in place, we’ll all have to remember the firewall is filtering

don’t want researchers struggling with firewall-induced problems

SLAC Computing will provide periodic reminders to revive salience fin.

SLAC net => Firewall <= Internet


Visitor Routers
ESNet
Stanford University
Internet 2
SLAC IP Network Boundary
Visitor Wireless
Eduroam Wireless
Border Routers
BRO
SLAC IP Network Boundary
Palo Alto Application Firewalls
Scientific Computing (Data Ctr)
Voice Networks
PBX Firewalls
Core Routers
Business Firewalls (EPN2/3/4, ERP)
Business Systems (Data Ctr)
Building Core Routers
SLAC Wireless (Authenticated)
Infrastructure Firewalls
Experiments Routers
Infrastructure Systems (Data Ctr)
Facilities and Site Security Routers
VPNs
SLAC Buildings
SLAC Experiments (PCDS, MCC, SSRL)
Facilities and Site Security Networks