NetGuru-10 Notes

Wednesday, February 2, 2011

Madren Conference Center, Meeting Room III
Clemson University
Clemson, SC

IP Cameras and Video Networking

- Place devices on a separate network?
- Using QoS?
- Short term storage in building and permanent archive centrally
- If network disruptions, store locally
- Private IP addresses in a private VRF
- Viewing workstations dual homed
- Cameras for safety, not security
- Once recording keep it for for how long?
- Archive for how long?
- What about a freedom of information request?
- Cameras use PoE
- Video conferencing on:
    - Telepresence on VoIP LAN
    - VRF
    - a LAN
    - Video Conferencing VLAN
- New Tandberg can do 802.1X
- Firewall performance issues
    - avoid firewall
    - H.460 tunnel around firewall
- Capture lecture audio/video
- Echo360, Video Furnace
- Multicast?
- DIRECTV IP-Advantage (MFH3)
- Campus televideo

IPv6 Server Security

- How to get your top level web on IPv6 but not defaced
- Proxy it
- Dual stacked, just check the IPv4 side?
- F5 Global server load balancing (GSLB)
- Security office wants to disable IPv6 on server
- I2 workshop on IPvv6 on Layer 4 and above (server/DNS/www/security/desktop
- Have local 6to4 and terado gateways
- Tracking IPv6 address on a switch port
    - privacy addresses
    - Scrape neighbor table
    - enforce a SLAAC on a port
- DHCPv6
- DHCPv6 helper?
- SRX / ASA / FWSM
- BlueCat / InfoBlocks
- RA Guard or filter RA on switch port
- Eliminate firewalls with ACLs on routers?
- TCAMs
- IDS inline
- Snort
- QRadar
- ISS
- Taps to IDS boxen
- Juniper STRM
- FireEye
- Bot detection
- Firewall
- Host patching better more effective than cleaning the network
- Barracuda Load Balancer with IPS
- Web filter proxying system
- IPv6 black hole route injection
- Protections from IPv6
    - privacy addresses and ACLs
    - security office wants DHCPv6
    - Don't just port IPv4 tools to IPv6
- DHCP snooping and dynamic arp inspection
- MAC authentication
    - VLAN placement based on MAC
    - registration VLAN

- If users fail 802.1X, fail back to captive portal

OTP

- Enterprise level stuff
- Bastian host for network administration
- Gold vs Silver on token
- RSA vs Alladin
- TACCAS
- RADIUS
- Groups to control which users can administrate what devices
- Command accounting
- Placating auditors
- Change management
    - RANCID
    - templates
    - RAT
    - home grown PERL scripts

Thursday, February 3, 2011

Peer to Peer

- Abandoning Packeteer
- Anagran
- Use Packeteer to find DDOS
- What do you use when DDOS
    - inMon and alarms
    - QRadar
    - Red lamda
- Education not technology
- Warn user when detected
- BAYU - be aware what you're uploading
- Passively monitor, if detected email user
- Sandvine and Procera
- Packeteer not as good since Blue Coat acquisition
- Taps on outbound traffic
- OC3mon and argus
- Statseeker
- Traffic Sentinel
- Firewalls notice more quickly
- Don't notice, just absorb attacks
- NetFlow and flow-tools
- Border router rolls over on DDOS, when detected - mitigate
- Juniper policers, rate limit the flows
- Cisco put traffic in a scavanger class
- Control plane policy on core cisco routers
- Comcast uses Sandvines for power boost
- What about research traffic?
- Not shaping from campus to R&E networks
- Tippingpoint to block P2P

MPLS

- PE device in building
- Just in the core
- Cisco 6524
- Juniper MX80
- VRF on a single router
- VRF lite or MPLS

Subnet sizing

- /21 for wireless
- 100 to 150 hosts per subnet

Data Center

- Trill
- LISP
- L2 focus
- vMotion
- GLSB
- Opti-man fiber circuit

Measurement

- PerfSonar
- iperf

- Cisco IP LSA
- Smokeping, multicast beacon

VoIP e911 Location Granularity

- Building
- 50 foot radius
- Floor of building
- Building, room, floor
- Records of phone jack to location
- Limit access to closets to prevent users moving devices
- If port not used in six months recover port, reuse port in one year

WiMax

- least spectrum
- Carrier hotel for out of band management
- CLEAR, Sprint

DAS

- Sprint/Nextel and 800mhz public safety in deep tunnels
- Leaky coax in the tunnels
- Verizon/AT&T

OpenFlow

- NAC in the future
- Replacement for gigamon boxes; stripe flows for snort and like boxes
- Arista switch - 10G
- Standards base solution
- How soon for production?
- Ifmap?

Self Service

- VLAN port assignment
- Query port status
- No packet capture

IPv6 Reverse DNS

- Static addresses no problem
- Wild card domain reverse?
- Must be static if want reverse?
- Fill DNS cache if someone walks it

RADIUS Certificate Expiration

- Use a four year certificate to minimized issue
- Use a three year inCommon Comodo certificate
- Build an .exe and instruction sheet?
- idEngines?
- Cloudpath?
- AD policy push?

Cisco Catalyst 6509

- Tune buffers and hold queues
- SVI interfaces - traffic is bumped to supervisor
- Remember dropping some packets is a good thing, TCP cannot work without it

Wireless

- Access points under auditorium seats
- People make good attenuators
- Turn off low data rates, 11 and below
  - In high density areas, turn off 5 and below
  - System wide, turn off 1 and 2
  - But! Nintendo DS only 1 or 2

Game Consoles

- Look the other way when users put own wireless in dorm room
- Register consoles separately
- PPPoE?
- uPnP?
- MAC OIU - DHCP differently
- DHCP client identifier