SECTION 17

Millstone Plant Process Computer Firewalls

Paul Sucholet

Dominion Nuclear, Millstone

MILLSTONE PLANT PROCESS COMPUTER FIREWALLS

Network Security

Rtime Users Group 2005

PPC-PCE Firewalls

- HARDWARE:
- Cluster of Six Sparc 5 Unix Workstations
- One Intel Windows 2000 Mgt Station
- 9 Private LAN Segments
- Various Network Connections

PPC-PCE Firewalls

- SOFTWARE:
- Solaris version 2.6 latest patches 1/2003
- Checkpoint Firewall-1 (all) vs4.1
- RSA Integralis Authentication vs 4.1
- Authentication on MP2/MP3 Simulator/Plant
- Client Firewall -1 (MGT STA only) vs 4.1
- RSA Client (MGT station only)
- Motif GUI on Simulator F.W.’s (Local)

What is the Point -- of Firewalls

Six Firewalls to protect 9 Private LAN Segments

Isolate PPC LAN's within Corporate Firewall.

Protect Plant Control Systems LAN Segments

Originally For MP3 MSR System Now meets these needs

- OFIS / ERDS
- SIMULATOR Protection
- MP2/MP3 PPC LAN Protection
- EXTERNAL INTERNAL HACKERS

- Common MGT of all Firewalls
- Adds redundancy for Authentication
- Common Software and hardware Platforms

How does it work?

- Six Firewalls run independent vers of Firewall-1 protection software.
- 4 of the six run RSA authentication software. 2-Clients, 1 master, 1 slave.
- All firewall policy's are stored on Mp3client-1 MGT station in Modcomp Lab.
- The 4 RSA authentication Servers are also managed from Mp3client-1 and authentication user database.

How does it work continued……

- Policies are also stored locally on each Firewall.
- Upon boot up, Firewalls “fetch” policy from MP3-CLIENT-1 in lab.
- If unavailable, F.W. loads last “pushed” policy from local D.B.
- Fully automated, no login required.

Connectivity

- Common connection is through site network.
- TSC - EOF firewalls have direct access to PPC LAN’s
- PPC LAN’s are MP2, MP3 and now MP1 Central Monitor System.
- MP2 Firewall Protects MP1 CM LAN also.
- New LAN’s are created at EOF and TSC.
- EOF network and firewall have UPS and generator backup.
- TSC has UPS and Switchable power source.

Logging Into Firewalls - Sparc5

- Solaris root account
- Administrator account
- User accounts

Logging Into MGT Station

- Windows Accounts include Administrator and user accounts.
- Firewall GUI
- RSA GUI
- Compaq Insight manager
- Rtime

Documentation and Backups

- All system disks on Firewalls are duplicated and stored in Data Center Media room.
- Above MGT Station is F.W. Docs and Manuals.
- MP3Client-1 MGT Station has backup tapes in Modcomp lab.
- Above MGT Station is all manuals and Docs.

Compaq Rtime Servers

Training - Info

Rtime Servers Who - Where

- MP2-SRVR-2
- MP3-SRVR-2
- MP3CONVPC-A
- MP3CONVPC-B
- MP2CONVPC-A
- MP2CONVPC-B
- MP-DEV
- MP-DEV-A
- MP-SIM2-1
- MP-SIM3-1

- Compaq DL580
- Compaq DL580
- Compaq 6400R
- Compaq 6400R
- Compaq 6400R
- Compaq 6400R
- Compaq 6500
- Compaq 6500R
- Compaq ML330
- Compaq ML330

Server Operating Systems and Upgrades

- All Servers run Windows 2000 Servers
- Rtime Server vs 11.9
- Developer Studio on MP-DEV, vs 5 and 6.
- Rtime Source is on those machines also.
- Rtime vs 11.9 complete on Unit 2 3/2005.
- Rtime vs 11.9 scheduled 7/2005.
- Looking for Server hardware upgrades in 2006.

Server Management

- MP3CLIENT-1 watches all Rtime servers for hardware and software failures.
- Pages Paul, and displays alarm conditions in Lab MGT Station.

Rtime Server Backups

- MP2-SRVR-2 Runs Veritas Open File Backup Utility.
- It can also backup all Rtime servers.
- Each Server also can back itself up using W2K backup utilities.
- Backups Stored in MP3 Cabinet in Media Storage Room.
- Backups can be done on DLT or DAT tape drives.

RAID5 Disks

- All servers except Simulator, use RAID5 arrays for system and archiving.
- Windfall from NU application servers allow large archives on all RAID5 servers.
- W2K upgrades allow remaining system disks to move to RAID from NT Mirroring.

OFIS - ERDS

- Callback modems installed using RAS, on Conversion P.C.'s.
- Calls back Armory1 and Armory2 Rtime Clients.
- MP2 - MP3 callback scheme on Prints.
- MP3 ERDS activated through Aydin Displays sends ERDS activate to Master Conversion P.C.
- MP2 ERDS activated through MP2 Rtime control room workstations.

Documentation for Rtime Servers

- Master installation Guide located in Modcomp Lab Near MGT Station.

- All installation Software disks will be stored in Media Storage room in large binder.
- Some installation disks must come from IT Services.

Common Failures

- Application errors.
- Loss of power, including dirty power.
- Power supplies.
- Disks.
- System Crashes.
- Alarms.

Parts for Servers and Firewalls

- Compaq service support for all Compaq hardware.
- Spare parts in-house stored in PPC storage room bldg. 437.

Support

- Firewalls had 7x24 from various vendors.
- All contracts expired 4/2003.
- Blanket Corporate support under security group in VA.
- Unix O.S. support local.

- Compaq servers are in good hands.
- Compaq 7x24 support and warranties active.
- Software maintained by PCE.

Accomplishments

- Network upgrade to CISCO switches for all PPC LAN segments.
- Built Development system to test Rtime upgrades.
- Completed testing of Net Advocent “Digital” video switch.
- Moved Firewalls out of Datacenter into plant.
- Integrated MP1 CM to Firewall PPC LANS

Accomplishments cont…..

- Reconfigured Firewalls/Servers to 100baseT.
- Updated PPC LAN Prints.
- Rebuilt lab servers on Compaq 6500 platforms.

Challenges

- Firewall -1 vs 4.1 will no longer be supported.
- Firewall hardware obsolete.
- New hardware and software upgrades to current corporate standards.

- Update Rtime Clients to vs 4.39
- Continue to work with less money, time and people.
- Rtime Server upgrades.
- MP3 control room Client upgrades.
- Rtime 11 Upgrades.

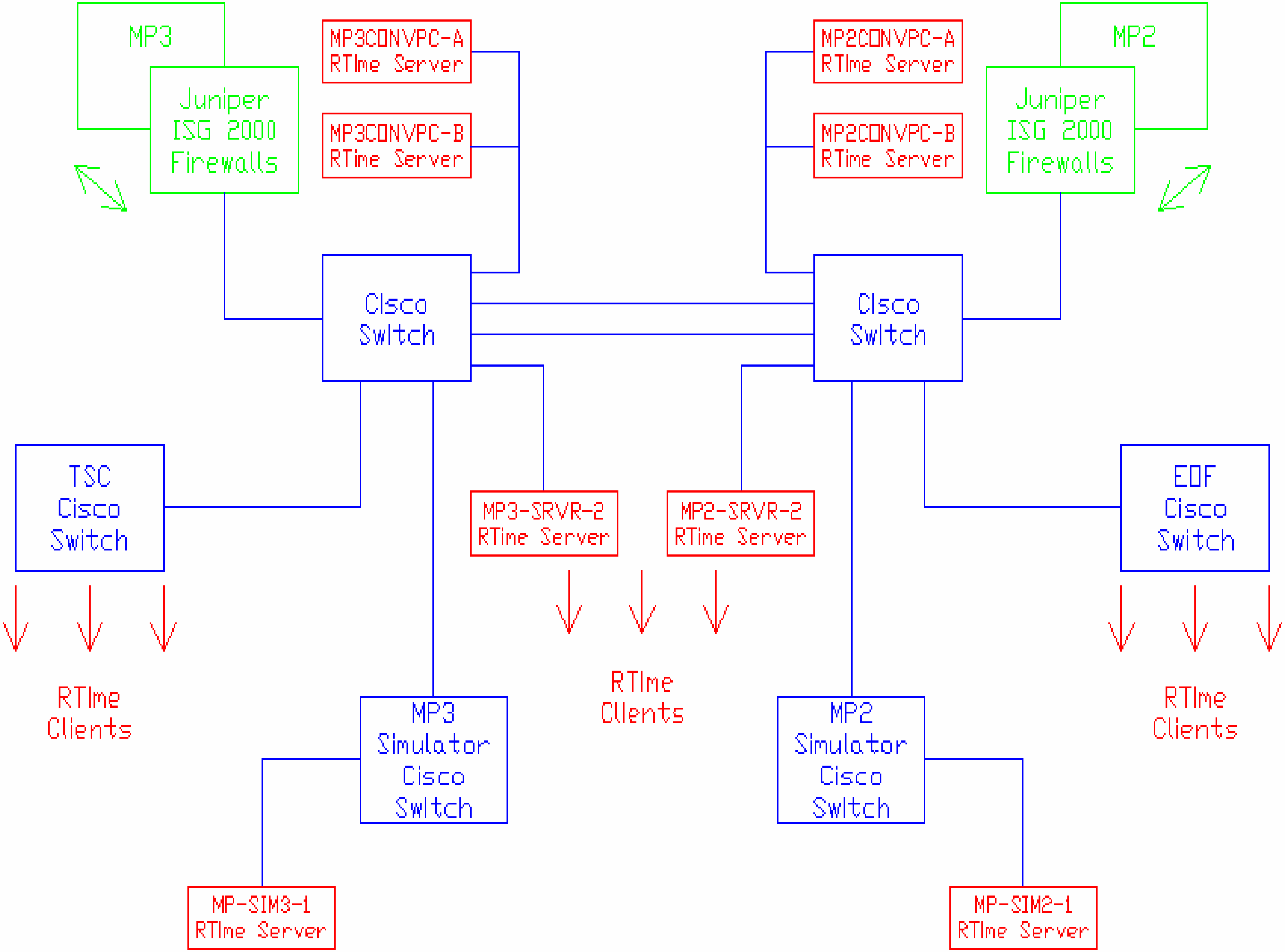
2005 – 2006 Security Improvements

- Replace existing protecting firewalls
- Netscreen Juniper IGS 2000 Redundant pairs.
- IGS 2000 is a fully redundant diskless system.
- Upgrade existing LANS to VLANS using truncking.
- Consolidate 6 independent Firewalls to two redundant pairs.
- Provide central Monitoring and control of both firewall pairs.
- Upgrade main Cisco switches to add redundancy.
- Use corporate RSA authentication servers.

2005 – 2006 Facility Upgrades

- Add Commercial DSL service to Armory At State Capital.
- Secure connections using VPN tunnel.
- Upgrade Rtime servers to new Compaq servers.
- Install Common Disk system for Rtime redundant servers.
- Install Private Rtime workstations for MP3 Control room.

2005 Juniper Netscreen Firewall System



THE END

Thanks