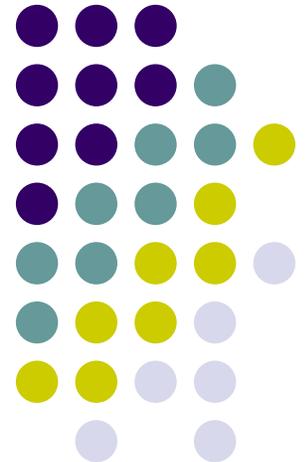


Network Operations Security Center Brief

6/20/06





Purpose of this briefing

- To answer the following questions about the Network Operation Security Center:
 - What are the capabilities for the NOSC?
 - How can we organize and examine 100's of servers and network devices to determine security issues in IHS?
 - What functionality will the NOSC give to the IT staff within IHS?
 - How will the NOSC team meet the needs of both IHS, HHS SOC, and other security mandates.

Overview of the NOSC Project



- Analex/ComGlobal has been contracted to work this project starting Aug 2005- the present. We have over 500 hours into developing the systems you will see today.
- When the NOSC goes live it will be a 24/7 operation, providing support for Network Security, and eventually Network Operations.
- We will have 13 people in the NOSC over 3 shifts 7 days a week. We have over 20 Cisco certifications in our current staff including CCIE's, CCSP, and INFOSEC.
- NOSC is based out of two redundant facilities – Las Vegas, NV, and San Jose, CA. The servers are housed in a facility that does TopSecret related work for the US Navy.
- The NOSC is made up of 12 servers running over 10 monitoring applications. The events are collected in a terrabyte raid array running Raid10, and are arranged in over 8 databases.
- The main vendor for our software is an IBM Tivoli software division called Micromuse.

Network Operational Support



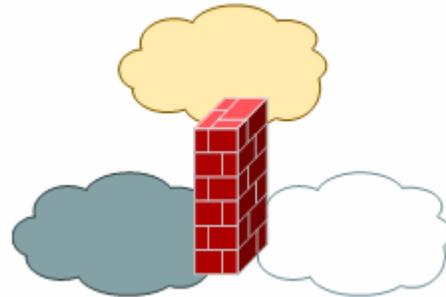
- Demarcation: Core network, routers, firewalls, IDS Devices, VPNs, network circuits.
- Types of Services: circuit turn-ups, circuit repairs, firewall related requests, routing, routing redundancies, QOS, VPNs.

Network Operational Transitions



Area	Start	Finish
ABQ	5/30/06	6/1/06
OKC	6/2/06	6/7/06
AKA	6/8/06	6/8/06
OIT	6/9/06	6/12/06
HQ	6/13/06	6/14/06
CAL	6/16/06	6/20/06
POR	6/21/06	6/26/06
ABR	6/27/06	7/4/06
DAL/SEA OEH	7/5/06	7/6/06
TUC	7/10/06	7/11/06
NAS	7/12/06	7/17/06
BJI	7/18/06	7/20/06
NAV	7/21/06	7/26/06
BIL	7/28/06	8/2/06
CRIHB	8/3/06	8/7/06
PHX	8/8/06	8/11/06
TUC DIR	8/14/06	8/14/06

NOSC Security Management



- Demarcation: Routers/Firewalls, Intrusion Detection/Prevention Systems, some server related functions.
- Types of Services: Analyzing logs, security events, active vulnerability scanning, bandwidth, address space management, and other functions.

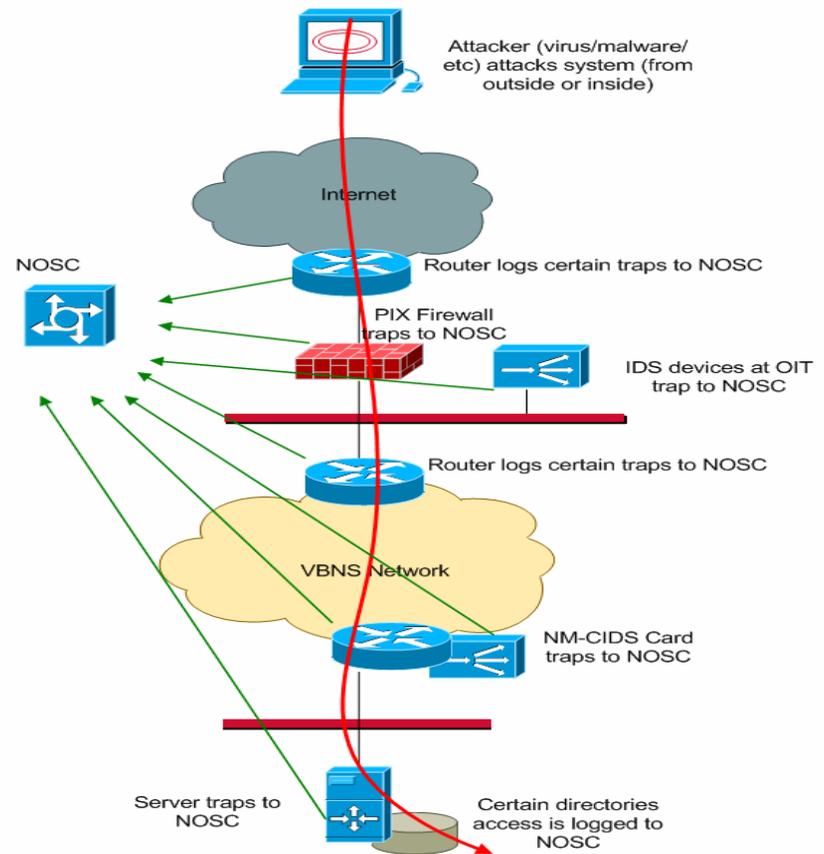
How the NOSC Collect Data



- Devices participating in the NOSC:

- Intrusion Detection/Prevention Devices at the core sites.
- Intrusion Detection/Prevention Devices at each remote site connection to the Core Network.
- Firewalls at sites.
- Server Agents that send Event View information/Syslog data to the NOSC.
- Router Syslog/SNMP Data..
- Network Sweeps done by the NOSC servers.

Correlated Event Analyst



Software Components of the NOSC



- Network Monitoring/Security
- Vulnerability Analysis
- Router Configuration Management
- Incident Tracking
- IP Address Utilization
- Central Router User Management
- Bandwidth Utilization

Network Monitoring



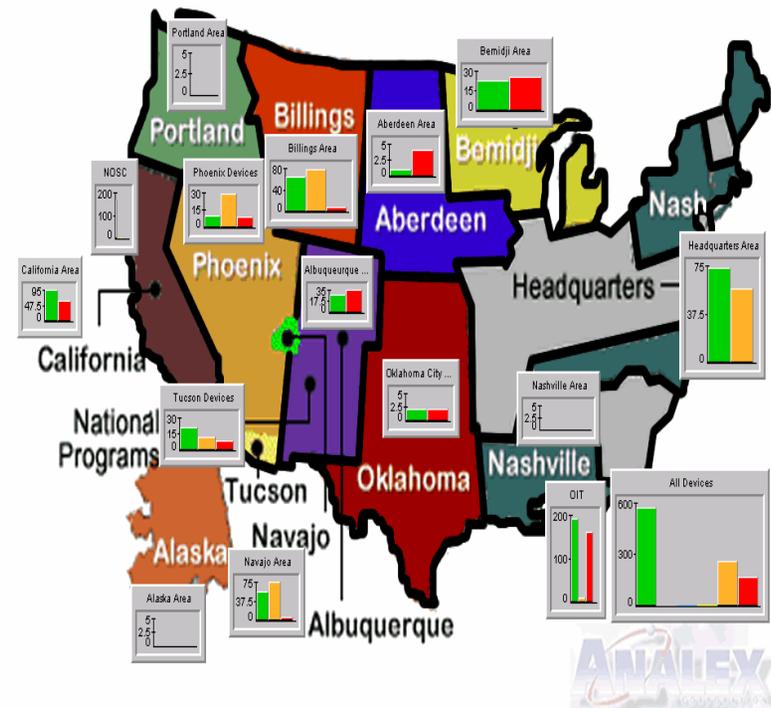
- Product: IBM Tivoli—
Micromuse Netcool
Network Monitor
- Products:
 - Netcool Omnibus
 - Netcool MTTrap Probe
 - Netcool Internet Service Manager
 - Netcool System Service Monitor
 - PRTG Passler Router Traffic Grapher



U.S. Department of Health and Human Services
Indian Health Service
The Federal Health Program for American Indians and Alaska Natives



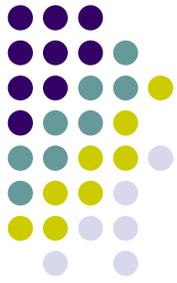
Network Operations
Security Center



Individual Area Links: [Aberdeen](#) - [Alaska](#) - [Albuquerque](#) - [Bemidji](#) - [Billings](#) - [California](#) - [Nashville](#) - [Navajo](#) - [OIT](#) - [Oklahoma](#) - [Phoenix](#) - [Portland](#) - [Tucson](#)

Netcool Omnibus

- Takes in data from all monitoring applications and sorts and displays it.
- Can be setup with different views so each Area can see the event for their area only.



Active Event List Window - Microsoft Internet Explorer

Address: http://sj-its-netcool:8080/AELView?entity=NAV&datasource=NCOMS

http://sj-its-netcool:8080/NAV@NCOMS/

Count	Node	AlertGroup	Agent	Last Occurrence	Location
2	OIT-01-VBNS-CORE	NAV-01-NAVAJO-3745 NAV.its.nosc	Navajo_Routers	3/21/06 1:10:26 AM	SJ-ITS-NETCOOLHS.NOS
2	OIT-01-VBNS-CORE	NAV-08-FTDEFERANCE NAV.its.nosc	Navajo_Routers	3/21/06 1:10:26 AM	SJ-ITS-NETCOOLHS.NOS
2	OIT-01-VBNS-CORE	NAV-02-GIMC NAV.its.nosc	Navajo_Routers	3/21/06 1:10:26 AM	SJ-ITS-NETCOOLHS.NOS
2	OIT-01-VBNS-CORE	NAV-04-CISCO-ROUTER NAV.its.nosc	Navajo_Routers	3/21/06 1:10:26 AM	SJ-ITS-NETCOOLHS.NOS
2	OIT-01-VBNS-CORE	NAV-05-PINON_2811 NAV.its.nosc	Navajo_Routers	3/21/06 1:10:26 AM	SJ-ITS-NETCOOLHS.NOS
1	OIT-01-VBNS-CORE	NAV-02-GIMC NAV.its.nosc	Navajo_Routers	3/21/06 8:31:16 PM	SJ-ITS-NETCOOLHS.NOS
269	NAV-01-NAVAJO-374	NAV-03-NAVCH-B NAV.its.nosc	Navajo_Area	3/22/06 9:41:40 PM	SJ-ITS-NETCOOLHS.NOS
269	NAV-05-PINON_281	NAV-05-NAVPHC-DHCP NAV.its.nosc	Navajo_Area	3/22/06 9:41:38 PM	SJ-ITS-NETCOOLHS.NOS
268	NAV-02-GIMC NAV.its	NAV-02-NAVGALL-CTK2 NAV.its.nosc	Navajo_Area	3/22/06 9:41:33 PM	SJ-ITS-NETCOOLHS.NOS
268	NAV-05-PINON_281	NAV-05-NAVPHC NAV.its.nosc	Navajo_Area	3/22/06 9:41:35 PM	SJ-ITS-NETCOOLHS.NOS
267	NAV-02-GIMC NAV.its	NAV-02-NAVGALL-S2 NAV.its.nosc	Navajo_Area	3/22/06 9:41:37 PM	SJ-ITS-NETCOOLHS.NOS
265	NAV-02-GIMC NAV.its	NAV-02-NAVGALL-B1 NAV.its.nosc	Navajo_Area	3/22/06 9:41:36 PM	SJ-ITS-NETCOOLHS.NOS
6	NAV-01-NAVAJO-374	NAV-03-NAVCH-WIEB1 NAV.its.nosc	Navajo_Area	3/22/06 9:41:40 PM	SJ-ITS-NETCOOLHS.NOS
5	NAV-02-GIMC NAV.its	NAV-02-NAVGLD1DC1 NAV.its.nosc	Navajo_Area	3/22/06 5:11:29 PM	SJ-ITS-NETCOOLHS.NOS
4	NAV-01-NAVAJO-374	NAV-01-2ndflr_NAOC4507 NAV.its.nosc	Navajo_Area	3/21/06 1:10:24 AM	SJ-ITS-NETCOOLHS.NOS
4	NAV-02-GIMC NAV.its	NAV-02-NAVGLA NAV.its.nosc	Navajo_Area	3/22/06 5:21:29 PM	SJ-ITS-NETCOOLHS.NOS
4	NAV-02-GIMC NAV.its	NAV-02-NAVGALL-CTK3 NAV.its.nosc	Navajo_Area	3/22/06 5:21:34 PM	SJ-ITS-NETCOOLHS.NOS
4	NAV-02-GIMC NAV.its	NAV-02-NAVGALL-B1 NAV.its.nosc	Navajo_Area	3/22/06 5:31:34 PM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-01-MTKHSWIEB1 NAV.its.nosc	Navajo_Area	3/21/06 1:10:24 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-01-NAO_C6509 NAV.its.nosc	Navajo_Area	3/21/06 1:10:24 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-03-NAVCH-FS NAV.its.nosc	Navajo_Area	3/21/06 1:10:25 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-03-NAVCHSDW NAV.its.nosc	Navajo_Area	3/21/06 1:10:26 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-01-NAVA NAV.its.nosc	Navajo_Area	3/21/06 1:10:24 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-01-NAV1E2K1 NAV.its.nosc	Navajo_Area	3/21/06 1:10:24 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-03-NAVCHFNETCH NAV.its.nosc	Navajo_Area	3/21/06 1:10:26 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-01-NAV1D1DC4 NAV.its.nosc	Navajo_Area	3/21/06 1:10:24 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-03-NAVCH-P NAV.its.nosc	Navajo_Area	3/21/06 1:10:25 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-03-NAVCH-MREC NAV.its.nosc	Navajo_Area	3/21/06 1:10:25 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-03-NAVCH-WIEB1 NAV.its.nosc	Navajo_Area	3/21/06 1:10:26 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-01-NAV1D1DC1 NAV.its.nosc	Navajo_Area	3/21/06 1:10:24 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-01-NAV1D1DC2 NAV.its.nosc	Navajo_Area	3/21/06 1:10:24 AM	SJ-ITS-NETCOOLHS.NOS
2	NAV-01-NAVAJO-374	NAV-01-NAV1A0CACHE2 NAV.its.nosc	Navajo_Area	3/21/06 1:10:24 AM	SJ-ITS-NETCOOLHS.NOS

55 73 6 All Events (134)

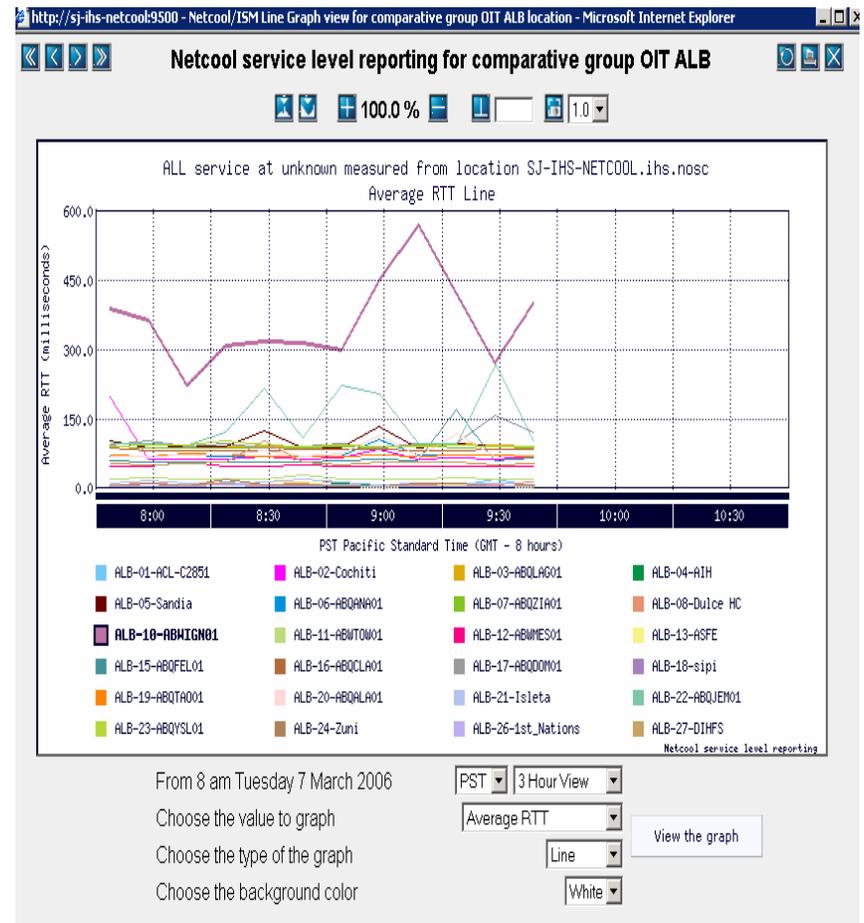
134 rows inserted, 134 rows updated, and 0 rows deleted. NOCS sj-its-netcool:8080

Applet: com.micromuse.wave.applets.ael.AEL started Trusted sites

Netcool ISM



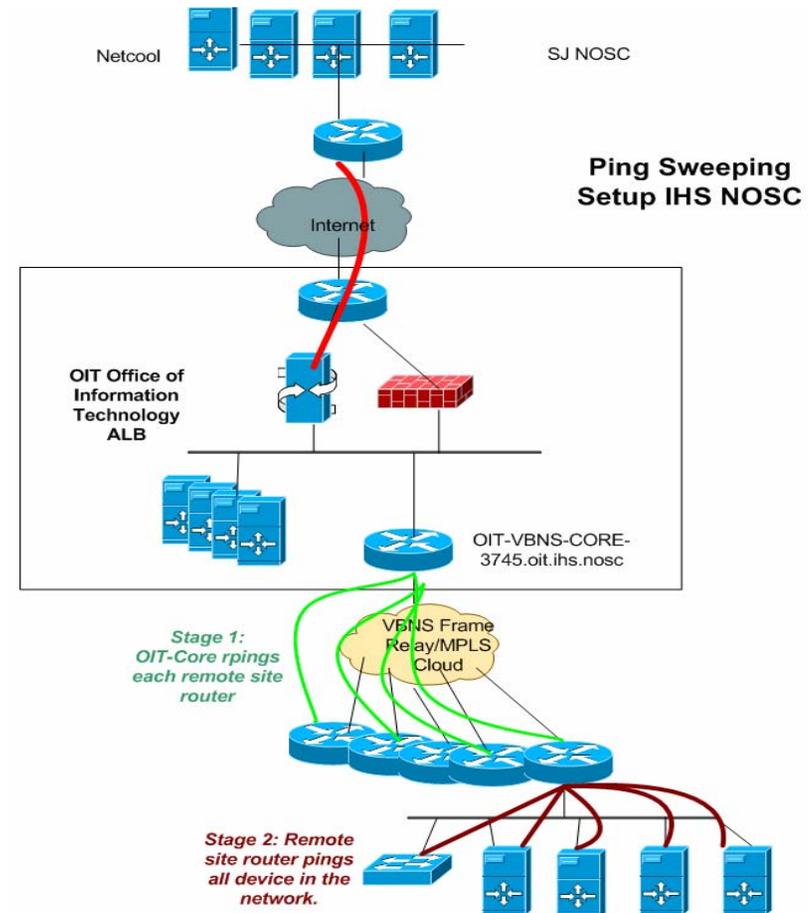
- Monitors Network Device Reachability:
 - Latency Response
 - Whether the host is up/down.
 - Whether the router/server is flapping.
 - What section of the network is having problems.
 - Feeds into Netcool Masterconsole.



Netcool ISM – Isolating the network response



- Network Sweeping via SNMP:
 - Sweep each site from OIT, testing reachability from the site to OIT.
 - Sweep all devices at each site from their local gateway
 - If a network problem is detected, it will show which segment of the network is experiencing issues.



Netcool System State Monitor (SSM)



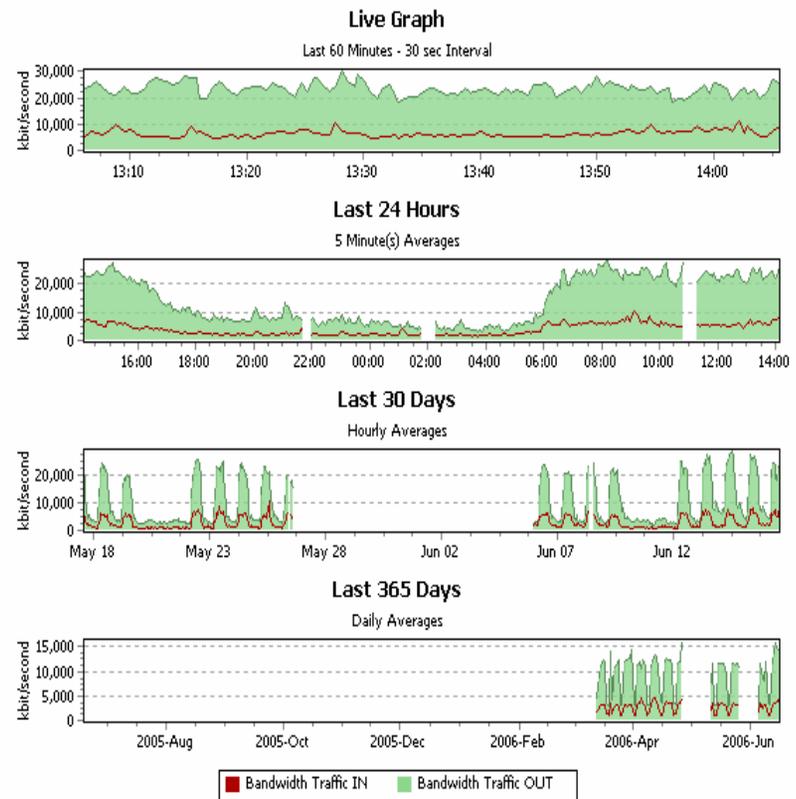
- SNMP Agent based monitor that is loaded on any server:
 - Supports Windows/ Unix / Linux servers.
 - Uses server MIBS to trap errors with the systems to the Omnibus
 - Tracks server info like
 - Out of disk space
 - High CPU utilization
 - TCP connections
 - This info can be correlated with other network events to determine security incidents.

PRTG Passler Router Traffic Grapher



- Based on MRTG
- Grabs bandwidth utilization information from routers every 5 mins.
- Will be accessible for any admin from a webpage.

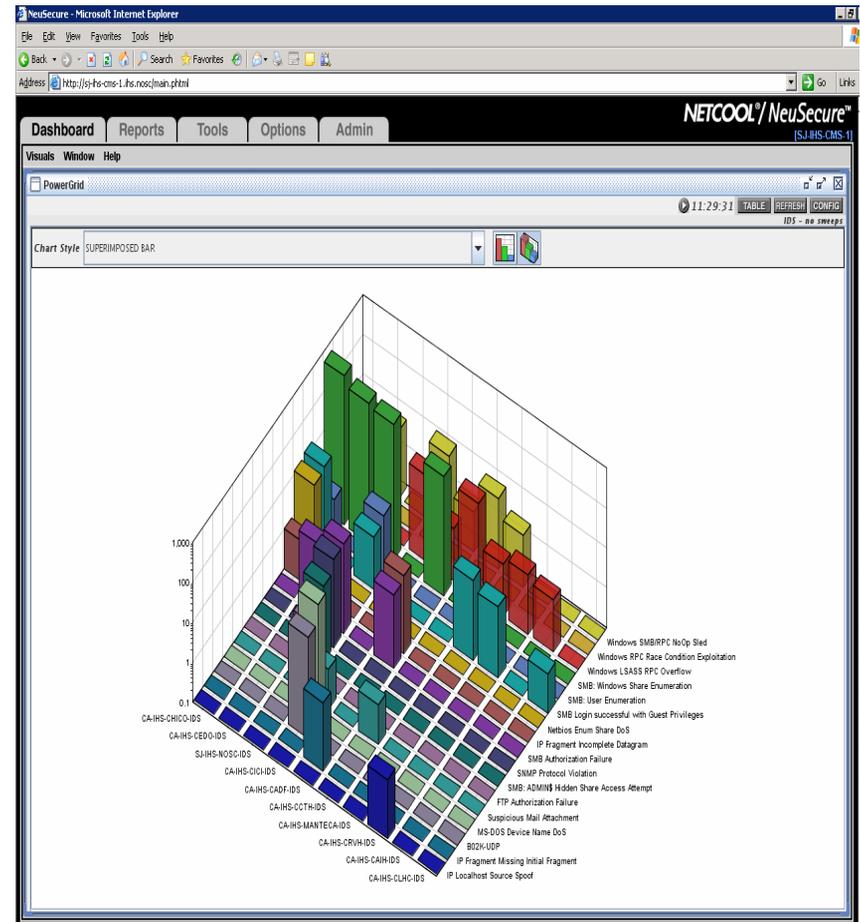
Port Se4/0 on OIT-01-VBNS-CORE-3745 (OIT-01-VBNS-CORE-3745.OIT.ihs.nosc)



Network Security



- IBM Tivoli - Netcool NeuSecure
 - Firewall, Intrusion Detection-Prevention System, Event Log Analyzer
 - Brings in data from different sources and sorts it for correlated analysis.





Vulnerability Analysis

- We use Nessus Vulnerability scanner to integrate Vulnerability data with the NeuSecure data.
- This will cause any attack on a device that is vulnerable to that type of attack to create a new Meta event that shows the analyses of an attack on a vulnerable system.

Nessus Scan Report - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.nessus.org/demo/report.html>

This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which were alive and responding during test	9
Number of security holes found	54
Number of security warnings found	113

Host List	
Host(s)	Possible Issue
10.163.156.10	Security hole(s) found
10.163.156.9	Security hole(s) found
10.163.155.4	Security hole(s) found
10.163.155.3	Security hole(s) found
10.163.155.2	Security hole(s) found
10.163.156.1	Security hole(s) found
10.163.155.6	Security hole(s) found
10.163.156.205	Security hole(s) found
10.163.156.16	Security hole(s) found

[return to top]

Analysis of Host		
Address of Host	Port/Service	Issue regarding Port
10.163.156.10	echo (7/tcp)	Security warning(s) found
10.163.156.10	telnet (23/tcp)	Security hole found
10.163.156.10	ssh (22/tcp)	Security hole found
10.163.156.10	ftp (21/tcp)	Security hole found
10.163.156.10	chargen (19/tcp)	Security warning(s) found
10.163.156.10	daytime (13/tcp)	Security warning(s) found
10.163.156.10	discard (9/tcp)	No Information
10.163.156.10	smtp (25/tcp)	Security hole found
10.163.156.10	time (37/tcp)	Security notes found
10.163.156.10	finger (79/tcp)	Security warning(s) found
10.163.156.10	sunrpc (111/tcp)	Security notes found
10.163.156.10	login (513/tcp)	Security warning(s) found
10.163.156.10	exec (512/tcp)	Security warning(s) found
10.163.156.10	printer (515/tcp)	Security notes found
10.163.156.10	shell (514/tcp)	Security warning(s) found
10.163.156.10	uucp (540/tcp)	Security notes found
10.163.156.10	sometimes-rpc16 (32776/udp)	Security warning(s) found
10.163.156.10	sometimes-rpc14 (32775/udp)	Security warning(s) found
10.163.156.10	sometimes-rpc10 (32773/udp)	Security hole found
10.163.156.10	lockd (4045/udp)	Security warning(s) found
10.163.156.10	snmp (161/udp)	Security hole found

Router Configuration Management



- This tool does an hourly check of each router, and determines if the configuration file stored has any differences with the running configuration on the router.
- If a difference is found the new configuration file is saved, and the diff is emailed to the admins.

IHS NOSC Cisco Configs

SJ-IHS

Device Name	Config	Config File Date	Previous Config	File Date
SJ-IHS-INET-GTM-FAD-1.ihs.nosc	Config	03/07/2006 11:01:07	Prev Config	03/02/2006 3:01:08

CAL-IHS

Device Name	Config	Config File Date	Previous Config	File Date
CAL-IHS-CYLB-GTM-SD-0-0.cal.ihs.nosc	Config	02/28/2006 4:01:17	N/A	N/A
CAL-IHS-HOOPA-GTM-SD-0-0.cal.ihs.nosc	Config	03/03/2006 2:01:32	N/A	N/A


```
!RANCID-CONTENT-TYPE: cisco
!
!
!Memory: nvram 239K
!
!
!Image: Software: C2800NM-ADVSECURITY9-M, 12.4(3b), RELEASE SOFTWARE (fc3)
!Image: Compiled: Fri 09-Dec-05 10:53 by alnguyen
!Image: flash:c2800nm-advsecurity9-mz.124-3b.bin
!
!BOM Bootstrap: Version 12.4(1r) [hqluong lr], RELEASE SOFTWARE (fc1)
!
!Flash: #- --length-- -----date/time----- path
!Flash: 1 19261944 Dec 28 2005 16:44:54 -08:00 c2800nm-advsecurity9-mz.124-3b.bin
!Flash: 2 1646 Dec 28 2005 16:55:04 -08:00 sdaconfig-2811.cfg
!Flash: 3 4052480 Dec 28 2005 16:55:34 -08:00 sda.tar
!Flash: 4 812032 Dec 28 2005 16:55:54 -08:00 es.tar
!Flash: 5 1007616 Dec 28 2005 16:56:16 -08:00 common.tar
!Flash: 6 1038 Dec 28 2005 16:56:36 -08:00 home.shtml
!Flash: 7 113152 Dec 28 2005 16:56:52 -08:00 home.tar
!Flash: 8 511939 Dec 28 2005 16:57:12 -08:00 128MB.sdf
!Flash: 38240256 bytes available (25776128 bytes used)
!
!Flash: nvram: Directory of nvram:/
!Flash: nvram: 229 -rw- 7266 <no date> startup-config
!Flash: nvram: 230 ---- 1955 <no date> private-config
!Flash: nvram: 231 -rw- 7266 <no date> underlying-config
!Flash: nvram: 1 -rw- 0 <no date> ifIndex-table
!Flash: nvram: 2 -rw- 597 <no date> IOS-Self-Sig#3501.cer
```



Incident Tracking Database

- Custom Incident Database designed to grab the data associated with security events.
- Designed by Analex to help our security analyst work his/her shift, and give checklists to the systems and functions necessary.

Http://10.10.10.10:8080/ANALEX/NOSEC/Shift_Summary.aspx - Microsoft Internet Explorer

Engineer Name: Jonathan Dugette
Shift Time: 0900 - 1700
Shift Date: 3/7/2006
Shift ID: 1

ANALEX CORPORATION
Network Operations Security Center

Areas of Responsibility:
Aberdeen Alaska
Albuquerque Arizona
Billings California
ITSC Devices Nashville
Navajo NOSC Devices
Oklahoma City Phoenix
Portland Tucson

Shift Menu:
• Shift Information
• Incidents
• Internal Audit
• Consider Shift
Search Shift Reports
Administration

Traffic Mgmt for all Areas Checked to be in correct Parameters
 Support Email/Voice/Chat Box Checked for any Customer Tickets Related to the Areas
 Checked IP Space Allocation Database for Changes in Related Areas

Open Traffic Mgmt Incident
 Open Customer Ticket Incident
 Open IP Allocation Incident

Each Management checked to verify all network elements in the Areas are up and functioning
 Check Configuration Change Management Queue to Determine Whether Any Devices in These Areas Changed Configurations
 Checked Network Topology Changes in Related Areas

Open Operational Incident
 Open Configuration Incident
 Open Network Topology Incident

Shift Summary

Save Shift Summary

Incident - Microsoft Internet Explorer

Engineer Name: Jonathan Dugette
Date: 3/7/2006
Incident Report Number: New
Search On Previous Incidents

ANALEX CORPORATION
Network Operations Security Center
Incident Report

Areas Affected in this Incident Report:
 Aberdeen Nashville
 Alaska Sturgis
 Albuquerque NOSC Devices
 Arizona Oklahoma City
 Billings Phoenix
 California Portland
 ITSC Devices Tucson
Uncheck All

Incident Categorization:
 Attack causes loss of service
 Malicious Code Infection Prevention
 Traffic Management
 Configuration Change Incident
 Network Topology Incident
 Disabled CE Service
 Customer Ticket Incident
 Operational Incident
 Malicious Code Infection
 Inappropriate usage
 Other
 Broken and Crises - Selected
 IP Allocation Incident
 Probe and Scans posing serious threat
 Unauthorized Access
 Internal Audit Incident
 IP Allocation Incident

Incident Short Summary

Enter Text

Incident Detail

IP Address Utilization



- Solarwinds Address Management Application.
 - Scans each network on a hourly basis to determine what IP Addresses are in use.
 - Sends the output to a webpage that will be available to any admin in IHS to reference.
 - Shows the last time an IP address was in use.
 - DHCP Address ranges can be commented, so statics are not chosen out of this range.

SolarWinds IP Address Management - Microsoft Internet Explorer

Address: http://198.45.5.26/ABE/default.htm

SOLARWINDS.NET
Network Management Tools

IP Address Management

Subnet	Address	Mask	Subnet Size	Available Addresses	Reserved Addresses	Used Addresses	Last Scan
ABE-Aberdeen-1	161.223.10.0	255.255.255.0	254	62	0	192	3/7/2006 8:26:50 AM
ABE-Aberdeen-2	161.223.11.0	255.255.255.192	62	30	0	32	3/7/2006 8:27:03 AM
ABE-AllenCinc	161.223.19.104	255.255.255.248	6	5	0	1	3/7/2006 8:27:05 AM
ABE-Belecourt-1	161.223.23.0	255.255.255.128	126	41	0	85	3/7/2006 8:27:32 AM
ABE-Belecourt-2	161.223.22.0	255.255.255.0	254	63	0	171	3/7/2006 8:28:10 AM
ABE-Explorette	161.223.14.0	255.255.255.128	126	49	0	77	3/7/2006 8:28:32 AM
ABE-FlaudreauSchoolBldgCtr	161.223.29.128	255.255.255.192	62	61	0	1	3/7/2006 8:28:43 AM
ABE-FTThompson	161.223.27.0	255.255.255.128	126	58	0	68	3/7/2006 8:29:02 AM
ABE-FTTotten-1	161.223.23.192	255.255.255.192	62	32	0	30	3/7/2006 8:29:13 AM
ABE-FTTotten-2	161.223.23.128	255.255.255.192	62	24	0	30	3/7/2006 8:29:23 AM
ABE-FVYates-1	161.223.17.0	255.255.255.240	14	0	0	6	3/7/2006 8:29:26 AM
ABE-LowerBrute	161.223.27.128	255.255.255.192	62	12	0	50	3/7/2006 8:29:43 AM
ABE-Macy	161.223.17.32	255.255.255.224	30	24	0	6	3/7/2006 8:29:48 AM
ABE-MandersonHRStation	161.223.19.112	255.255.255.240	14	12	0	2	3/7/2006 8:29:56 AM
ABE-MandersonHRStation	161.223.19.96	255.255.255.248	6	2	0	4	3/7/2006 8:30:05 AM
ABE-MartinOEHE	161.223.11.96	255.255.255.224	30	15	0	15	3/7/2006 8:30:18 AM
ABE-MelanderHRBldgCtr	161.223.17.128	255.255.255.192	63	37	0	26	3/7/2006 8:30:33 AM
ABE-MinorOEHE	161.223.11.192	255.255.255.224	30	16	0	14	3/7/2006 8:30:38 AM
ABE-Mobridge	161.223.17.64	255.255.255.192	62	37	0	25	3/7/2006 8:30:52 AM
ABE-MobridgeOEHE	161.223.11.128	255.255.255.240	14	3	0	11	3/7/2006 8:30:56 AM
ABE-Newtown-FortBerthold	161.223.28.0	255.255.255.192	62	65	0	7	3/7/2006 8:31:12 AM
ABE-PineRidge-1	161.223.21.224	255.255.255.224	30	28	0	2	3/7/2006 8:31:18 AM
ABE-PineRidge-2	161.223.18.0	255.255.255.0	254	225	0	29	3/7/2006 8:31:59 AM
ABE-PanolaHRWellnessCtr-1	161.223.15.192	255.255.255.224	30	28	0	2	3/7/2006 8:32:05 AM

SolarWinds IP Address Management - Microsoft Internet Explorer

Address: http://198.45.5.26/ABE/161.223.10.0.htm

SOLARWINDS.NET
Network Management Tools

ABE-Aberdeen-1

Status	Subnet Address	IP Address	Last Response	Comments	Response Time	DNS
Subnet Address	161.223.10.0					
Used	161.223.10.1		Today		94 ms	
Used	161.223.10.2		Today		100 ms	
Available	161.223.10.3					
Available	161.223.10.4					
Used	161.223.10.5		Today		95 ms	ABR-DATASERVER1
Available	161.223.10.6					
Available	161.223.10.7					
Available	161.223.10.8					
Used	161.223.10.9		Today		90 ms	
Available	161.223.10.10					
Available	161.223.10.11					
Used	161.223.10.12		Today		96 ms	ABR-AC5
Used	161.223.10.13		Today		95 ms	
Used	161.223.10.14		Today		93 ms	NAABRDC1
Used	161.223.10.15		Today		99 ms	ABRD1DC1
Used	161.223.10.16		Today		98 ms	ABRD1DC2
Used	161.223.10.17		Today		106 ms	
Used	161.223.10.18		Today		95 ms	ABRD1EX1
Used	161.223.10.19		Today		97 ms	
Used	161.223.10.20		Today		95 ms	
Used	161.223.10.21		Today		96 ms	



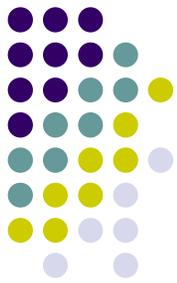
Router User Management

- CiscoSecure ACS Tacacs Server
- Database allows tracking of every command entered into every router.
- Allows for each user to have their own passwords, so no central passwords necessary.

The screenshot shows the CiscoSecure ACS web interface. The main content area displays a table titled "Tacacs+ Administration active.csv" with columns for Date, Time, User-Name, Group-Name, cmd, priv-lvl, service, and NAS-Portname. The table contains several rows of data, including commands like "write terminal <cr>", "show running-config <cr>", and "dir /all nvram:startup-config nvram:private-config nvram:underlying-config nvram:ifindex-table nvram:IOS-SE-Log#3501.cer nvram:persistent-data <cr>".

Date	Time	User-Name	Group-Name	cmd	priv-lvl	service	NAS-Portname
03/07/2006	10:59:09	configtracker	Administrators	write terminal <cr>	15	shell	tty322
03/07/2006	10:59:09	configtracker	Administrators	show running-config <cr>	15	shell	tty322
03/07/2006	10:59:07	configtracker	Administrators	dir /all nvram:startup-config nvram:private-config nvram:underlying-config nvram:ifindex-table nvram:IOS-SE-Log#3501.cer nvram:persistent-data <cr>	15	shell	tty322
03/07/2006	09:59:09	configtracker	Administrators	write terminal <cr>	15	shell	tty322
03/07/2006	09:59:09	configtracker	Administrators	show running-config <cr>	15	shell	tty322
				dir /all nvram:startup-config nvram:private-config			

Bandwidth Utilization



- The NOSC will be creating reports of each sites bandwidth utilization over time.(daily, weekly, monthly, yearly)
- Format Percentage of the Bandwidth used for the following:
 - http related traffic internal
 - http related external traffic
 - RPMS traffic
 - VOIP traffic
 - Video over IP Traffic
 - Email Traffic
 - Monitoring/management traffic
 - Window RPC (share) traffic
 - Any other traffic type IHS needs us to monitor
- This reporting will not require any additional devices in the enterprise, instead relying on each sites Cisco Router to gather the information

