CHAPTER 1

Net Audits and Security

The following provides an overview of a Net Audit, some of the benefits of a Net Audit, and brief description of the security standards set and provided by Cisco.

What is a Net Audit?

Advanced Network Services (ANS) Net Audits provide a comprehensive view of the health of your network. Audits focus attention on areas to ensure maximum network performance and stability. Managers increasingly recommend Net Audits before and after major system modifications and upgrades to document and quantify performance gains.

Created by senior Cisco Support Engineers and designed to address specific areas of stability, Net Audit reports concentrate on a three types of technologies: node stability, protocol stability, and media stability.

The ANS primary, team, and possibly the ANS Consulting organization carefully review each Net Audit. Recommendations are made jointly by the team to comment on the findings of the customer data and create a ‘task list’ which can add to future stability.

The Net Audits use "show" commands gathered via telnet. There is a lot of data not available through SNMP which can be gathered from an interactive telnet session. Examples are routing tables, IPX SAP tables, etc. But for some types of audits such as Voice Over IP readiness audit, both telnet as well as SNMP data is used.

In brief, a Net Audit will:

- Take a 'snapshot' of network health, which will identify a smaller, more manageable list of possible problem area for more detailed analysis.
- Target critical network elements and quickly identify problem areas through best practices and acceptable tolerances.

- Provide a comprehensive understanding of the overall network stability and the ability to view areas of concern in detail.
- Provide a team-based recommendation from the ANS primary engineer and ANS virtual teams to have input to final report.
- Present data in a format that allows relative comparison of dissimilar network nodes.

Benefits of a Net Audit

Some of the benefits of having an ANS Net Audit include:

- Developed by senior Customer Support Engineers (CCIE).
- Co-developed by Cisco Development Engineers
- Provide a quick 'snapshot' of the network to identify a smaller, more manageable list of nodes to monitor.
- Uses highlighting to target critical areas and quickly identify problem areas through best practices and acceptable tolerances.
- Uses a top down methodology of reporting in order to break down values
- Provide network, node, and interface views to give a comprehensive understanding of the overall stability with the ability to dive further to isolate areas of concern.
- Provide a team-based recommendation from the ANS primary engineer, their team members, ANS consulting team, Cisco Account Team, Critical Accounts, Escalation Engineers and others to summarize the overall stability for each specific Net Audit.
- Present correlations of data using formulas and percentages rather than raw numbers to allow the relative comparison of nodes in the network.

Security Standards

Application Security

- Apache Web Server version is 1.3.0 (NATkit 2.0).

- No access to look at files from the web as the Web access is protected by ID and password
- Data downloaded by FTP or PFTP or HTTP through proxies is provided with DES 56 or proprietary 160 bits.

Transport and Backend Security

- Data is encrypted using 56 bit or 160 bit proprietary DES.
- Data is pushed through CCO without de-encrypting.
- Password for logging onto CCO is never in clear text.
- Only ANS engineers may view the full extent of data.
- TAC has view of certain pieces of data, such as inventory, syslog, but no configs.
- Access to backend database is restricted to web access.

ANS Best Practices

- Always have password encrypted on Cisco IOS devices.
- Recommended to use Cisco Secure, TACACS, XTACACS, TACACS+, AAA for managing access into Cisco IOS devices.
- Recommended to have a banner denoting device name and contact information.
- Recommended to have SNMP variables like syslocation and syscontact for better management of Cisco IOS devices through management software.
- Recommended to run CDP where available.
- Turn off features such as TCP & UDP small servers on Cisco IOS devices which enhance denial of service attacks.
- Turn off source router switching.
- Turn on web server on Cisco IOS devices.

Data Security and Integrity within Cisco

The following information deals with possible security issues a customer may have once their data is received by Cisco.

- The customer's network data being transported is only decrypted once it reaches a production server inside Cisco's firewall.
- The data is only viewable by the web interface.
- Cisco’s network is completely switched with regards to desktop access. Hence, sniffing data packets is very difficult as one has to have physical access to important socket connections which are under Cisco IT control.