

Firewall Review

Section 1 FIREWALL MANAGEMENT & ADMINISTRATION

Common management practices with regard to administering the (company) network should be in accordance with company policies and standards. In addition, complete and current network documentation and design plans should be maintained.

Consider and Document

Management Administration

1. Determine the adequacy of the (company) Firewall Management department Data security infrastructure with regard to the following elements:

- The degree of centralization and decentralization of various functions.
- Data Security department functions with regard to operations and control.
- Future organization plans.

2. Firewall Management Tools used to monitor and control the Firewall Environment.

Maintenance

3. Evaluate the controls over network management and maintenance.

- Change control process and Firewall problem logs and resolutions.
- From paper file select a sample of hardware and software changes made to the Firewall Environment.
- Trace the selected items to the Firewall Rules Tunnels and Filters.
- Determine if the change was properly approved and authorized.
- Review the broadcast list to determine (from a sample) if there was adequate notification before the changes were implemented.
 - Determine if firewall changes are adequately tested.
 - Ascertain if firewall documentation is updated in a timely manor.

4. Problem management

- Firewall Services

Section 2 FIREWALL POLICIES & PROCEDURES

Objective: Complete and current network “Rules Based” policies should be maintained in order to ensure network integrity, security and on-going maintenance.

Consider and Document

Site Security Policy

1. Obtain and review the (company) Network Firewall Security policy with regard to the following elements:
 - Overall Rules Based policy statement
 - The specified level of monitoring, redundancy and control
2. Determine if the Site Security policy includes the following policy subsections:
 - Remote User Advanced Authentication
 - Dial-in/out
 - Password and account security
3. Determine if the overall firewall objectives detailed in security policy is consistent with current needs and is based on an acceptable level of risk. The overall objectives should address the following:
 - Identify the resources that will be protected and potential threats
 - Identify relevant organization protection roles
4. Ensure that there are adequate control practices in place for the detection, containment, recovery, eradication and follow-up.
 - Identify the detection and identification practices in place to ensure the prompt discovery of an intrusion.
 - Determine if procedures in place are adequate to inform the appropriate personnel in a timely manner once an intrusion has been detected.
 - Identify the containment and recovery procedures necessary to facilitate a quick recovery with minimal loss.
 - Identify the follow-up and education practices needed to ensure that the problem does not occur again.

Section 3 TOPOLOGY & PLANNING

Objective: Complete and current network diagrams should be maintained in order to ensure network integrity, security and on-going maintenance.

Consider and Document

Firewall Configuration

1. Obtain and review the latest network diagrams with regard to the following function:
 - External and internal Firewall configuration

2. Determine if the implemented Firewall design provides the following:
 - Fault Tolerance
 - Ease of recoverability
 - Disaster Recovery

3. Firewall design-testing methodology
 - Configuration testing
 - System logging and audit event reporting verification
 - Use of automated testing tools
 - Third party verification

4. Planning future Firewall/IDS implementation methodology regarding:
 - New services and their resulting allowable access levels
 - Protection of new attached hosts and networks
 - Firewall upgrades
 - Protection against new potential threats (e.g. Active X and Rogue Java Applets)

Section 4 FIREWALL SECURITY

Objective: To ensure an adequate level of network integrity and security, compliance with the BONY site security and rules based policies should be followed.

Consider and Document

Firewall Security

1. After careful review of Network Firewall Policies and the implemented Firewall Component Design noted in the other sections perform tests discussed below. The objective of these tests is to audit the security of the Firewall by evaluating the operating system, firewall application and the services enabled through the firewall (use the security software monitoring tools currently in employed by the Data Security Department).

Test A1 Evaluate, with the aid of a Technical Liaison, the Firewall Operating System for the following (observe and review documentation):

1. Operating system is running and system name
 - Which naming service is used?
 - Which DNS (Domain Name System) is running & name server used to bind to,
 - What is the most recent system backup date,
 - Is email received directly on the system or is a mail exchange used?

Test B1 Evaluate Firewall application and services filtering effectiveness as follows:

1. Management Scenarios (Discussions and observations)
 - Remote firewall management
 - Use of CERT Advisories
 - Access control to internal and external networks
 - Controlling access to multiple servers
 - Logging capabilities
2. Probing System for Security Weakness (Port Scanners, Sniffers)
 - List of ports and services open for attacks
 - Denial of Service Attacks
 - Source IP Spoofing Attacks
 - Source Routing attacks
 - Tiny fragment attacks
 - Brute force attacks (password guessing)
 - Known software bugs (CERT Alerts)
3. Ensure that there are adequate control practices in place for the detection, containment, recovery, eradication and follow-up.
 - Determine the status of the Incident Response Team:
 - Who are the team members
 - Are they from a cross section of areas, and
 - Does it provide response and escalation procedures appropriate to the seriousness of each security breach?
4. Identify the detection and identification practices in place to ensure the prompt discovery of an intrusion.
 - Determine if procedures in place are adequate to inform the appropriate personnel in a timely manner once an intrusion has been detected.
 - Identify the containment and recovery procedures necessary to facilitate a quick recovery with minimal loss.
 - Identify the follow-up and education practices needed to ensure that the problem does not occur again.

5. ISS RealSecure - is a network-based product primarily used to identify and thwart Internet attacks. It was installed in February 1999.

- Identify the location of the RealSecure engines.
- Ascertain if they are strategically located in the network to detect potential external attacks prior to the firewall and after the firewall but before the internal network.
- Determine if the use of RealSecure provides for study of attacks that the network may be subject to.
- Determine if RealSecure is currently being used to analyze and identify suspicious network traffic.
- Determine if a reevaluation of the firewall can be performed based on the current use of RealSecure.

Section 5 FIREWALL COMPONENT DESIGN

Objective: Complete and current network policies should be maintained in order to ensure network integrity, security and on-going maintenance.

Consider and Document

Firewall Network Configuration

1. Review firewall Topology and planning documentation in Section 3. In addition to the previous use discussion with management and through observations, determine the adequacy of the implemented firewall configuration. Determine the following:

- Firewall interface configuration:
 - Internal Network
 - External Network (VANS, Internet)
 - DMZ (demilitarized zone) with WEB & FTP Servers
- Are Dual DNS systems used?
- Is packet filtering routers used on external segments before the firewall?
- Is tunneling used with authentication and encryption to set up VPNs?

Firewall Application Configuration

2. Review Raptor and Checkpoint firewall configurations for adequacy and compliance with Site Security policies regarding the following configuration elements:

- Network entities, groups, users and services
- Authorization rules and notifications
- Virtual Private Networks
- Application event logging and notification
- Use of proxies and stateful inspection