

# FIREWALL AUDIT PROGRAM

## OBJECTIVE

Determine whether the connection to an external network is secured with an application/filtering firewall. Also, determine that controls associated with the firewall are effective to ensure that confidentiality, integrity, authenticity, and availability of member data and program files are protected from an untrusted entity.

PROCEDURE	INITIAL S	DATE	WP
<b>A. Organization and Administration</b>			
<i>Determine that internal controls are adequate with regards to organizational structure and administrative functions. Perform the following:</i>			
1. Obtain a copy of the Network Security policy and ensure it contains:			
a. Company's expectations of proper computer and network use;	_____	_____	_____
b. Procedures to prevent and respond to security incidences; and	_____	_____	_____
c. Descriptions of network application proxies and where connections may be initiated (for trusted network connections initiated from the internal network and untrusted network connections initiated from the external network).	_____	_____	_____
2. Review firewall network operations and control procedures to ensure that procedures are documented and in place to back up security configuration files and properly restore these files after system failures, or software or operating system upgrades.	_____	_____	_____
3. Verify the administrator is receiving up to date information on firewall security issues and implementing corrective action on a timely basis (new hacking techniques, change in configuration).	_____	_____	_____
<b>B. Access Controls</b>			
<i>Determine that internal controls are adequate with regards to access through the firewall, both internal and external. Perform the following:</i>			
1. Identify and assess the appropriateness of administrators' access to view and modify the firewall configuration.			
Review and investigate several changes with the administrator to ensure that they are authorized changes.	_____	_____	_____
2. Review the firewall authentication process to ensure effectiveness (validating claimed identity).	_____	_____	_____

PROCEDURE	INITIAL S	DATE	WP
3. Analyze the operating system (Windows 2000) configuration on the firewall server (run the Internet Security Scanner) to ensure the following security parameters are activated and appropriate: <ul style="list-style-type: none"> <li>a. User accounts,</li> <li>b. File and directory permissions, and</li> <li>c. Auditing.</li> </ul>	_____	_____	_____
4. Ensure that the firewall's host operating system has been properly modified to disable services that could be used to subvert the security of the firewall software program. <ul style="list-style-type: none"> <li>a. Through Control Panel, Network, Protocols, TCP/IP properties, ensure that IP datagram routing has been disabled in the operating system kernel.</li> </ul>	_____	_____	_____
<ul style="list-style-type: none"> <li>b. Ensure remote access services are disabled. (Do not want remote access to the firewall machine; instead allow remote access from the Internet to a Telnet or FTP proxy server.)</li> </ul>	_____	_____	_____
5. Obtain a list of analog lines and verify they are authorized and adequately restricted to prevent unauthorized access.	_____	_____	_____
<b>C. Router Configuration</b>			
<i>Ensure router management (including routers managed by another organization) and access controls are adequate to effectively secure unauthorized access to the network. Perform the following:</i>			
1. Determine that Telnet and console access ports are appropriately restricted and password protected by router passwords. <ul style="list-style-type: none"> <li>a. Verify Telnet access to the router has been completely disabled on routers, which connect to external networks. (In most cases, it should be disabled to lessen the risk of Telnet access from the external network.</li> </ul>	_____	_____	_____
<ul style="list-style-type: none"> <li>b. Using Telnet, attempt to connect to a sample of routers to ensure that access is properly restricted with passwords. Verify that a warning banner is in effect to inform users that access to the router is restricted and that their actions are being monitored.</li> </ul>	_____	_____	_____
<ul style="list-style-type: none"> <li>c. Ensure that all router passwords are stored in encrypted form, using a secure encryption algorithm.</li> </ul>	_____	_____	_____
2. Review SNMP access to the router to ensure that SNMP sets are restricted to authorized control workstations and that the default community string passwords have been changed from their default values to more secure, confidential formats.	_____	_____	_____
3. Determine whether router port number filters are properly set to read the status flag on packets to allow return packets on connections initiated from the internal network to pass through. Make sure the filters block packets trying to initiate a connection from an external network to the internal network.	_____	_____	_____

PROCEDURE	INITIAL S	DATE	WP
4. Examine the router configuration file for routers that connect server and user networks to external networks (i.e., ISP).			
a. Ensure that filter rules are established to filter and drop incoming and outgoing application packets based on their UDP and TCP port numbers (i.e., SNMP, Telnet Bootp).			
b. Ensure that the router ignores ICMP redirect messages, which could be used to modify the routing table.			
c. Review for logging of router access and access violations. Determine that logs are reviewed and followed up in a timely manner.			
5. Determine whether routers have defined static paths to allow traffic to pass from only a specified router on the connected external network (often the case when connecting to vendor networks, affiliated businesses, etc.).			
<b>D. Firewall Configuration</b>			
<i>Determine whether the connection to an external network is secured the firewall is properly configured (inbound and outbound). Perform the following</i>			
1. Review the configuration of the firewall software and assess the controls are adequate to safeguard the network. Review the authorization rules for the following:			
a. Compare the configuration to the Network Security policy description of authorized services. Investigate any deviations from policy;			
b. IP address restrictions;			
c. Service and protocol restrictions;			
d. User and group restrictions;			
e. Alert thresholds and logging; and			
f. Review WebNOT configuration to block unauthorized access and determine if it is appropriate.			
2. Analyze the firewall configuration by running the Internet Security Scanner (ISS). Complete checklist and review results to ensure the appropriate security parameters are activated.			
3. Review the directory structure to ensure that no other application programs, language compiler, interpreters, or other utilities are loaded on the system.			

PROCEDURE	INITIAL S	DATE	WP
<p>4. For all proxies that allow network connections to be initiated from the Internet (HTTP, FTP &amp; SMTP), ensure that strong password authentication controls are implemented (challenge-response, encryption) or that third-party security schemes have been implemented (Secure ID, S/key).</p> <p>a. Review the port number and IP source and destination restrictions to ensure they are correctly designed to restrict this traffic.</p> <p>b. For each proxy, determine that adequate logging mechanisms have been activated and that logs are reviewed on a timely basis.</p>			
<p>5. Determine whether the firewall software is configured to alert management on a real time basis of security events that require prompt attention (alerts such as SNMP traps, email messages, pagers, etc.).</p> <p>Test the alerts are properly functioning by sending messages that would create a security event to send an alert.</p>			
<b>E. Audit/Monitoring</b>			
<i>Determine that internal controls are adequate with regards to monitoring the system for security violations.</i>			
<p>1. Review any third-party and/or in house monitoring policies (i.e., maximum coverage, Web Watcher, Attack Detector, Session Recorder, Protocol Analyzer) and verify they are adequately monitoring critical activity and corrective action taken is appropriate (i.e., automatic alerts, automatic termination of attacks). Using the Policies editor, view the following:</p> <p>a. Security events (known attacks)</p> <p>b. Connection events</p> <p>c. User-specified filters (ignores certain network traffic, such as email out), and</p> <p>d. User-specified actions.</p>			
<p>2. Obtain reports and verify corrective action was taken in a timely manner.</p>			
<p>3. Using the firewall software set up a filter for the log to generate a report for Emergency and Critical events that occurred, in addition to Alerts that were sent. Verify corrective action was taken in a timely manner.</p>			
<p>4. Review the previous scans of the firewall and verify if corrective action was taken in a timely manner.</p>			
<p>5. Obtain reports received from the ISP, if any, regarding access violations, either against the ISP or the company. Follow up on corrective action and determine if it was timely.</p>			

PROCEDURE	INITIAL S	DATE	WP
<b>F. Change Management</b>			
<i>Determine that the internal controls associated with change control are effective to ensure that only properly authorized and approved changes are implemented to minimize the likelihood of disruption, unauthorized alterations, and errors.</i>			
1. Evaluate change control and ensure that the authority to alter the system is appropriately restricted.	_____	_____	_____
2. Obtain the event logs; select a random sample of system changes; and verify they were authorized, tested, and approved.	_____	_____	_____
<b>G. Backup and Recovery</b>			
<i>Determine that internal controls are adequate with regards to backup and recovery. Perform the following:</i>			
1. Review the firewall network operations and control procedures.			
a. Ensure that procedures are documented and in place to back up security and configuration files.	_____	_____	_____
b. Ensure that procedures are adequate to restore these files after system failures, or software/operating system upgrades.	_____	_____	_____