

**Audit Checklist #7
Auditing Firewalls**

INSTRUCTIONS FOR COMPLETING THE CHECKLIST

Answer the following questions by placing an X or a \checkmark in the appropriate "YES" or "NO" boxes. If you have to provide a written answer, please use the space provided.

GENERAL INFORMATION

Obtain documents covering the following items: Check the items that are attached.

- A. Schematic of Internal Network Topography _____
- B. Schematic of Firewall Topography _____
- C. Security Policy _____
- D. Organization Chart and Security Staff Position Descriptions _____
- E. Listing of Allowable Internet Services and Browsers _____
- F. Listing of Information Stored on the Firewall Hardware _____

The primary objective of this review is to determine if the organization has a firewall in place and to determine the adequacy of the controls over information that is passed through the firewall. Firewalls will vary from a single router to a sophisticated dual homed gateway firewall. The firewall should be evaluated in consideration of the importance of the information/data to the organization. The work described in this checklist should be done by auditors, analysts and examiners as an essential part of assignment planning. All findings should be documented.

A. GENERAL				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
1. What type of Internet connection is installed: a. Direct connection to ISP (Internet Service Provider)? b. Dedicated line or leased line? c. Dial in/out (modem)? d. Microwave or Satellite?				
2. Are modems disconnected when not in use?				
3. Recognizing that more than one type of firewall can be used at the same time, what type of firewall is in place: a. Packet filtering/screening router? b. Circuit-level gateway? c. Application-level gateway? d. Proxy server?				
4. Is a schematic of the internal network topography available? If so, request a copy for review.				
5. Is a schematic of the firewall topography available and does it provide a description of the system? If so, request a copy for review.				

A. GENERAL				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
6. Was the firewall developed in-house? If the firewall was commercially purchased, note the name of the product, version number, vendor, and when installed.				
7. Has the firewall product been certified? If so, under what conditions was it tested and by whom?				
8. Does the organization have a public server (i.e. web site) on the premises? If so, is the server behind the firewall?				
9. Is the internal network (i.e., Intranet) supported by the firewall?				
B. Is the firewall transparent to users of the network?				
B. Have all protocols allowed and applications used been tested with the firewall to ensure interoperability?				
12. Are reports and logging procedures detailing hardware and software failures and repairs generated and maintained? Are these reports/logs regularly reviewed by management?				

A. GENERAL				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
13. Are maintenance agreements and software licensing agreements maintained?				
B. SECURITY				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
1. Is physical security provided for the servers, routers and/or host machine (firewall)? a. All firewall equipment secured (preferably in an area inaccessible to all but authorized systems personnel)? (1) Physical access is authorized? (2) Physical access is controlled and monitored? b. Is unrelated equipment and supplies stored in the secure area? If so, provide a description.				
2. Is the area where the firewall equipment maintained equipped with temperature controls, fire detection devices, extinguishers, and UPS backup?				

A. GENERAL				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
3. Do existing security procedures prevent unauthorized removal of equipment from the premises?				

B. SECURITY				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
4. Do existing security procedures prevent unauthorized removal of equipment from the premises?				
5. Is on-site storage of all system media adequate to prevent unauthorized access, including: a. Server and/or firewall software and backup media? b. Firewall related passwords, security policy (base rule), configuration etc.?				
6. Can we determine how many entry points or interfaces there are to the firewall and/or internal host computer? If so, record the total number.				
7. Has a risk analysis of the entire network been performed to ensure that all entry points identified are equally protected?				
8. Are there connections to vendors and/or servicers, or affiliated businesses?				
9. Are scanning tools such as SATAN or ISS used by the security administrator to identify open ports on the system? If so, review scanned reports.				

B. SECURITY				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
10. Does the firewall have audit and security logging capabilities and are they being used? This includes: a. Audio alarms and paper connections? b. Security logs, management reports, hacking reports? (Determine if the security logs can be exported to another machine, i.e., remote syslogd, via e-mail.)				
11. Do management reports or audit logs exist that record all connections and attempted connections, services accessed, protocols used, and a list of session dates and times?				
12. Are the security reports reviewed by someone in management? If so, how often are they reviewed and how long are the reports maintained?				
13. Is a message displayed at logon to discourage unauthorized access?				

B. SECURITY				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
14. Are the following areas addressed in the Security Policy: a. Site access controls? b. Modems? c. Passwords? d. Encryption? e. Authorization? f. Remote access? g. Auditing/logging of both outbound and inbound traffic? h. Training?				
15. Are security controls outlined in the Security Policy being enforced?				
16. Is encryption available, being used, and compatible with all applications?				
17. Has the firewall being tested against various levels of attacks? If so, are the records maintained and how often is the system tested?				

B. SECURITY				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
18. If an attacker were to subvert the gateway host, does the organization have mechanisms in place to detect the event? Would alerts be initiated, would the administrator shut the system down, etc.?				
19. Does the organization have a policy or program addressing suspected intrusions? If so, does it address the following: a. Internal and external attacks? b. Logs to be maintained, or other records of intrusions? c. Procedures in case of attempted or actual intrusion, i.e., would the system be shut down, would the attack be ignored, etc.?				
20. If the firewall software failed, will traffic still pass through the gateway?				
21. Are changes to important directories and files (e.g., su, root, bin, uucp) monitored?				
22. Are procedures in place to control changes to: a. Firewall hardware and software? b. Firewall configuration? c. Routers?				

B. SECURITY				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
23. Is testing of changes performed in the 'Test' environment? The system should be disconnected from the Internet and local network.				
24. Have all vendor supplied patches been installed? Compare installed patches to current patches available from Vendor. (This can be accomplished via the Vendor's website.)				
25. Is the firewall backed up periodically? If so, how often?				
26. Is there a traveling licensing agreement for firewall software for use at the hot site?				

C. SECURITY ADMINISTRATION				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
1. Are copies of the organizational chart and security staff position descriptions available? If so, request copies.				
2. Has management assigned the responsibility for security administration to one individual? If so, have that person identified.				
3. Is the security administrator qualified for the position? Request biographical information.				
4. Have the security administrator's duties and responsibilities been clearly defined and reviewed for appropriateness?				
5. Does the security administrator have any conflicting duties?				
6. Is all security administrator documentation maintained and available for review?				
7. Is access to security administrator documentation restricted? Where it is maintained?				

D. VENDOR/OUTSOURCING				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
1. Did management evaluate the firewall vendor or supplier for expertise, internal controls, financial stability, ability to provide updates, etc., before purchasing the product?				
2. Were update tests performed by the vendor or supplier to address new threats on networked systems provided to the entity?				
3. If the firewall is outsourced, does anyone know what type of firewall product is being used by the service organization? Additionally, do they know: <ul style="list-style-type: none"> a. The types of controls that are in place at the service organization's location? b. The types of monitoring reports available to the entity by the service organization? How often are the monitoring reports received? c. Has the entity or service organization identified what would constitute an attack and when the entity would be notified of an attempted attack? d. Is outside servicing of the firewall covered by blanket bond insurance? e. Has the entity's legal counsel reviewed the contract? 				

E. MANAGEMENT				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
1. Was a risk analysis performed and reviewed by management before implementation of the firewall? Were the following factors considered in the risk analysis: a. What will the firewall protect against? b. How will the firewall impact current services and business practices? c. How will the firewall fit into the overall security plan? d. What is the value of the information being protected?				
2. Has management considered outsourcing and network monitoring?				
3. Does management review user's Internet protocol access levels periodically for appropriateness?				
4. Are there management approved written user instructions and procedures for the network and Internet use? Is there an appropriate use' policy which users must sign before gaining Internet access?				

F. CONFIGURATION				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
1. Can the IP routing be turned off in the host? If IP routing is enabled, verify that the firewall product being used will over ride the operating system routing.				
2. Is a Domain Name System (DNS) used? If so, does the DNS server provide host address translations for both inside and outside access without leaking naming information to the outside?				
3. Is a listing of Internet services and browsers that are allowed inbound and outbound available for review? If so, does it provide a description of all available ports? (Note: Generally this information will be provided in the security policy or defined in the base rules.)				
4. Does the base rule for the firewall provide for either of the following: a. Denies all packets unless expressly permitted? b. Permits all packets unless expressly denied?				

F. CONFIGURATION				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
5. If a proxy server is being used, does it limit access to specific applications/protocols such as: <ul style="list-style-type: none"> a. Telnet (Telecommunication Network)? b. FTP (File Transfer Protocol)? c. HTTP (Hypertext Transfer Protocol)? d. Usenet (User Network)? e. Gopher? f. MTP (Mail Transfer Protocol)? g. Rlogin? h. X 11 Window 				
6. Are permissible and denied applications identified in the Security Policy? For example, the policy expressly: <ul style="list-style-type: none"> a. Allows inbound mail to gateway machine only? b. Denies inbound FTP? c. Denies inbound Telnet and Rlogin? 				
7. Is a packet-filtering router used? If so, determine:: <ul style="list-style-type: none"> a. How it is configured. b. If it is password protected and is it encrypted. c. If it can be configured remotely. 				

F. CONFIGURATION				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
8. Is the router configured for: a. Source and destination IP addresses? b. Source and destination TCP flags?				
9. Are all appropriate destination ports less than 1024 blocked or limited to only specific connections, i.e.: a. FTP? b. SSH (S ecure S hell)? c. Telnet? d. DNS (D omain N ame S ystem)? e. SMTP (S imple M ail T ransfer P rotocol)? f. Web? g. Pop 3 (P ost O ffice P rotocol version 3)? h. IMAP (I nternet M essage A ccess P rotocol)? Note: The most common ports are FTP (21), SSH (22), Telnet (23), SMTP (25), Web (80), Pop 3 (110), and IMAP (143). The most commonly blocked ports are port 80 and port 25. Port 80 is the default port for http traffic. Port 25 is the default port for sending and receiving mail.				

F. CONFIGURATION				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
10. Where specific connections are allowed, or destination ports are unblocked, is management's decision to allow protocols documented and available for review? Note: Tools are available to remotely verify if a port is open or closed. These utilities can be useful in checking to see if a server is running or a firewall or ISP is blocking certain ports.				
11. Are adequate precautions taken to prevent IP spoofing attacks? If so, what action is taken?				
12. Does the Security Administrator have procedures in place to identify spoofing attacks when they occur?				
13. Can a list of information stored on the Firewall machine be obtained? If services such as NIS, NFS, FTP, X-11 Window, and anonymous FTP are available, determine the necessity for these services. (Note: This should be included in the security policy or base rules.)				

F. CONFIGURATION				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
14. Is the screening router configured to deny Internet Control Message Protocol (ICMP) packets and redirect messages? (Note: Redirect messages should be obeyed by trusted host machines only, not routers. When a router is connected to an ISP, ICMP may be required to network troubleshooting. Access control lists should specify specific IP addresses allowed to use ICMP.)				
15. Has the router or firewall been configured to deny Routing Information Protocol (RIP) packets?				
16. Are Finger (Port 79) and WHOIS (Port 43) protocols allowed? If so, are they logged and reviewed?				
17. Are incoming Remote Procedure Calls (RPCs) and portmappers blocked at the firewall? If not, review procedures and management's decision to allow.				
18. Are inbound requests for X11 windows blocked by the firewall? (Note: X11 is used primarily by UNIX.)				

F. CONFIGURATION				
STEP	YES	NO	N/A	COMMENTS/REFERENCES
19. Does the firewall reject IP loose source routing options so that someone using TCP connections to specify an explicit path to a destination will be denied?				
20. Is communication with other hosts denied? If so, how is this controlled?				
21. If the firewall is running on a Windows operating system, are unnecessary Windows services turned off? (Note: In the Windows NT environment, this could include services such as NetBios, Network browser, Workstation, or Server Services.)				
G. DOCUMENTING THE COMPLETED CHECKLIST				
<p><i>If you answered "NO" to any of the above questions, you may need to perform a more in-depth analysis of those specific areas to determine the significance of the problem and the potential impact on controls. This checklist should be clearly documented in the audit documentation or TeamMate and that the results of the assessment are reported in the audit scope and methodology.</i></p>				