

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p><u>Firewalls</u></p> <ol style="list-style-type: none"> 1. Follow up on prior management points. 2. Does the organization maintain a security policy? Obtain a copy if available. 3. Does the organization maintain a firewall security plan? Obtain a copy if it is available. Consider where the firewall fits in with the security policy. 4. Are there any changes to the network that would affect the firewall? This includes additional software, added services, hardware, and configuration changes. 5. Does an outside entity or vendor manage and/or consult on any function or configuration of the firewall? 6. Who can access the firewall's operating system? <ol style="list-style-type: none"> a. Verify this through a log. b. Determine if the users are active employees. Do these users need accounts to perform their job duties? c. Any temporary or vendor accounts? Are these accounts necessary? d. Which of these users are responsible for configuring the firewall? 7. Who configured the firewall? Determine if that person has the adequate skills to properly configure and maintain the firewall. 8. What type of firewall does the organization use (application proxy, packet filtering, etc.)? <ol style="list-style-type: none"> a. Is the firewall stateful? b. What version of the operating system is used? 9. Determine which hardware is connected to the firewall. Trace all connections. 10. List all types of packets allowed into the network. 11. List the types of protocols that have access into the network. 12. Is the firewall configured to report its default banner? 		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>13. Prompts:</p> <ul style="list-style-type: none"> a. PIX1> unprivileged mode b. PIX1# enable mode c. PIX1 (config)# configure terminal <p>14. Try the default password, “cisco”, to log on.</p> <p>15. Are passwords required to be changed regularly? Does the system allow reused passwords? If so, does an adequate amount of time pass before it can be used again?</p> <p>16. What is the limit on the number of failed login attempts? Are login failures logged?</p> <p>17. Can root Telnet to the system?</p> <p>18. Use the command <code>show config</code> to print the firewall’s configuration. Print hard copy if possible.</p> <p>19. Use a port scanner (<i>nmap</i>) to determine which firewall is used. Disable ICMP pinging because most firewalls do not respond to this.</p> <ul style="list-style-type: none"> a. To counter this, disable port scans at the routers in front of the firewalls. Intrusion detection systems (IDS) should be configured to detect scans, including random scans. <ul style="list-style-type: none"> i. If the organization’s ISP manages the routers, then ensure that the ISP blocks scans. ii. If routers are setup not to detect port scans, then the firewall should not allow port scans. <p>20. Use <i>tracert</i> to trace the paths to determine which firewall is used.</p> <ul style="list-style-type: none"> a. If ICMP TTL packets are not returned, then firewall may be easier to locate. The firewall is probably where the ICMP is being blocked. b. To counter this, restrict response to expired TTL packets by the routers and firewalls. This helps to prevent firewalking. This may have adverse affects to legitimate connections. Also, ICMP TTL Exceeded messages should not leave the network. c. Ideally, all unnecessary UDP traffic should be 		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>blocked at the routers.</p> <p>21. Use <i>netcat</i> to grab the firewall banner. Look at all available ports. Try port 21 (ftp), port 25 (SMTP), and port 23 (telnet).</p> <ol style="list-style-type: none"> a. To counter this, the banners should be reconfigured so they do not divulge too much information or anything but the default banner. The default banner could allow someone to determine which firewall is used. <p>22. If <i>netcat</i> doesn't produce any results, then use <i>nmap</i> to determine which ports respond. Sometimes a response indicates that a port is firewalled. Use <i>tcpdump</i> to review the output.</p> <ol style="list-style-type: none"> a. Block IP unreachable messages. b. Disable the router's response to the ICMP type 13 packet. This would also help to prevent an <i>hping</i> attack. c. Note any ports reported in the output. <p>23. Who determines the ACL rules?</p> <ol style="list-style-type: none"> a. Is there a master listing of all rules? b. Does it limit who can connect and where? c. Do the rules require a source IP address and the hard-coding of the destination IP address? d. If possible, obtain the ACL. e. If ACLs aren't used, is the conduit feature used instead? f. Is TurboACL enabled? Check the <code>show access_list</code> command. If the first line says that the access list is compiled, then TurboACL is enabled. g. <code>show access_list</code> will display the access configuration. Print out if possible. To determine if the ACL list is working, run the <code>hitcnt</code> command. <p>24. Does the firewall allow DNS downloads?</p> <ol style="list-style-type: none"> a. Is RIP and DNS lookup traffic enabled? b. If DNS traffic must pass, then is there a rule that specifies authorized DNS servers? c. Does the firewall allow ICMP ECHO, ICMP ECHO REPLY, and UDP packets? ICMP ECHO and ICMP REPLY must be disabled to prevent an attack using <i>loki</i>. 		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>d. Does the organization's ISP use ICMP pings to check on the systems?</p> <p>25. Does the organization use a proxy firewall?</p> <p>a. Which proxy firewall is used (vendor, version, etc.)?</p> <p>b. If so, determine if there are any default user ID's and passwords.</p> <p>c. Try to logon to the proxy firewall from within the Information Systems department.</p> <p>d. At the prompt, key in localhost. Then key in a known ID and password. If access is successful, then an attack using <i>rdist</i> could cause a buffer overflow.</p> <p>e. To counter, do not allow localhost logons. If localhost is necessary, then apply a TCP wrapper program.</p> <p>26. To determine if unauthenticated external proxy access is possible, while inside the network, change the browser to use a proxy (80, 8080, etc.). Try to connect to a website.</p> <p>a. Also, try to connect to an internal web page. Look at the homepage's source html code for an IP address.</p> <p>b. To counter, disallow external access via a proxy. Restrict proxy access at the routers.</p> <p>27. Does the organization use any desktop firewalls? Are the XP machines configured to run the firewall software?</p> <p>28. Does the organization have a DMZ?</p> <p>a. If so, what is in the DMZ?</p> <p>b. What traffic is allowed/disallowed and by what servers or IP addresses?</p> <p>29. Is the firewall configured to filter URLs so the Internet use is in line with the acceptable use policy?</p> <p>30. Check the list of IP addresses that the firewall issues and ensure that the addresses are from 10, 172, and 192 networks.</p> <p>31. Is a backup firewall used? If so, then:</p> <p>a. Do they communicate with each other?</p>		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>b. Are they the same models (515 and 515E are not the same models)?</p> <p>c. Have the same amount of memory?</p> <p>d. Have the same number of interfaces?</p> <p>e. Have the same type of activation key type (DES, 3DES, etc.)?</p> <p>f. Which type of licenses do the primary and fail-over firewalls have?</p> <p>g. With stateful failover enabled, there are no interruptions in processing. Packets will not be dropped. To determine what is replicated (HTTP, UDP, etc.) during a failover, use the <code>show failover</code> command. This command also prints the failover configuration. The stateful failover interface must be a Fast Ethernet or Gigabit Ethernet interface and must be dedicated to the passing of state information. The firewalls are connected to each other via a crossover Ethernet cable, a dedicated hub or switch (no other hosts connected), or a dedicated VLAN on a switch. Token Ring and FDDI interfaces are not supported.</p> <p style="padding-left: 40px;">i. <code>show failover</code> can be run on the primary and stateful failover firewalls.</p> <p>h. If a backup firewall is not used, then is the current firewall backed up?</p> <p style="padding-left: 40px;">i. Is it backed up to a protected network or server?</p> <p style="padding-left: 40px;">ii. How often is it backed up?</p> <p style="padding-left: 40px;">iii. Are the backups included in the disaster recovery backups?</p> <p style="padding-left: 40px;">iv. What media is used?</p> <p>32. Check the version of the firmware/software. For the Cisco PIX, enter <code>show version</code> at the prompt. Note the Licensed Features and serial number.</p> <p>33. How is the IT department notified of firmware/software updates?</p> <p>34. What TFTP server is used? Is it running?</p> <p style="padding-left: 40px;">a. What is stored on the TFTP server? Configuration files (not recommended)?</p>		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>35. Is remote access enabled?</p> <ul style="list-style-type: none"> a. Is it used through Telnet? b. Is encryption used over Telnet? <p>36. According to the IT department’s security policy, what type of traffic is allowed and disallowed through the firewall? Consider Java and ActiveX.</p> <p>37. Through the <code>connection_limit</code> parameter, how many concurrent active connections are allowed? The default is set to “0.” This means unlimited connections.</p> <p>38. Through the <code>embryonic_limit</code> parameter, how many concurrent half-open connections are allowed? The default is set to “0.” This means unlimited connections. With a setting of “0”, a DoS attack is possible.</p> <p>39. After changes are made, is the <code>clear xlate</code> command run to clear the cache?</p> <p>40. Is http inspection enabled? Even if URL screening rules are configured, http inspection could be disabled.</p> <p>41. Is Voice over IP (VoIP) used?</p> <p>42. Is Skinny Client Control Protocol (SSCP), which Cisco IP Phones use, enabled? The default port is 2000.</p> <p>43. Is Session Initiation Protocol (SIP) enabled? SIP is a protocol used in session control for VoIP. The default port is 5060. TCP or UDP can be used.</p> <p>44. Is URL filtering used to enforce acceptable use policies? Is a filtering server involved? It could be used to filter Java and ActiveX.</p> <ul style="list-style-type: none"> a. Are ACLs used to filter URLs? If so, then the firewall’s performance may suffer, and there is less flexibility in management. <p>45. Is auditing used? If so, then:</p> <ul style="list-style-type: none"> a. Obtain a listing of the rules if possible. b. What is the action set to: alarm (default), drop, or reset? 		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>46. What are the IT department's policies with regard to the firewall and IDS? Is the firewall configured to act as an IDS?</p> <p>47. Use the <code>show ip audit signature</code> command to determine if there are any signatures enabled or disabled.</p> <p>48. Is Fragmentation Guard enabled? By default, it is disabled. Run the <code>show sysopt</code> command to determine if it is enabled or disabled.</p> <ul style="list-style-type: none"> a. If it is enabled, then determine the setting for each of the following: <ul style="list-style-type: none"> i. fragment size- max number of blocks for reassembly. ii. fragment chain- max number of fragments which one IP packet is split. iii. fragment timeout b. Check the fragments database with the command <code>show fragment</code>. <p>49. Is Floodguard enabled? By default it is enabled. Floodguard helps to protect against DoS attacks. It reclaims resources that are not in an active state.</p> <p>50. If version 5.3 or later is used, then TCP Intercept may be enabled. No packets enter until there is a three way handshake. Does the version used enable this feature?</p> <p>51. Is Reverse-Path Forwarding enabled? This allows the PIX to check the packet's source address against the table. It ensures that the packet arrived on the same interface that is listed in the entry. If it is not listed, then it is presumed to be spoofed. It is disabled by default.</p> <p>52. Is Reverse Path Forwarding (RPF) verification enabled?</p> <p>53. Use the <code>show route</code> command to look up the entries in the routing table.</p> <p>54. Does the firewall use a server for authentication?</p> <ul style="list-style-type: none"> a. If not, then what is used for authentication? 		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>b. If so, then which security protocol is used (TACACS+, RADIUS, etc.)? Cisco Server AAA is software for firewalls.</p> <p>c. If AAA is used, then is it used to control access to a network device (firewall, router) or control access to network resources through the device (web services through a firewall or router, for example)?</p> <p>d. If possible, obtain a listing of all levels of users that authenticate (local accounts, privilege accounts- with levels 0-15, etc.).</p> <p>e. If authentication is used, then determine if there is a local account setup using the <code>nopassword</code> keyword. This setup creates a local account that requires no password.</p> <ul style="list-style-type: none"> i. To access the Cisco Secure ACS HTML interface, open browser and key in <code>http://<ACS IP address>:2002</code> ii. What are policies or rules to determine what type of access a user needs? iii. Determine the access method for each user. For example, Telnet, SSH, serial, etc. iv. If possible, determine which databases the users have access to. v. If possible, determine which commands users or groups can use. vi. If possible, determine which network devices users or groups have access to. <p>55. How often do users have to re-authenticate? Usually done when a user tries to connect after the timer expires. If virtual HTTP is enabled, then <code>uauth</code> should not be set to "0." Use the <code>show virtual http</code> command to determine the setting.</p> <p>56. Is virtual Telnet enabled? This allows pre-authentication for services (other than HTTP, FTP, or Telnet) that do not provide authentication. Telnet is used to authenticate users before certain services are used. Virtual Telnet can be used to log-in and log-out.</p> <ul style="list-style-type: none"> a. Use the <code>show virtual telnet</code> command to determine the configuration. <p>57. Use <i>Output Interpreter</i>, available on Cisco's website www.cisco.com/cgi-</p>		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>bin/Support/OutputInterpreter/home/pl , to verify the AAA configuration.</p> <p>58. Is logging enabled?</p> <ul style="list-style-type: none"> a. Who has access to these logs? b. Who reviews the logs and how often? c. Are logs reviewed in real-time? d. How are the logs protected from unauthorized access, manipulation, and deletion? e. What is the message count set to? The default is 512. f. Is time stamping used for logging? g. Is encryption used if logs are sent over the wire? h. Are the logs archived? i. If so, then is it local or remote? Remote logging allows for an analysis of the messages. <ul style="list-style-type: none"> i. Is the command-line interface or Cisco PDM remote access used? j. What level of logging is used (0-7)? k. Do the logs capture URL and FTP requests and actions performed? l. Are the logs limited in size? Helps prevent an attack from using all the storage space. m. Is SSH used without AAA? If so, ensure that the default username <i>pix</i> has been changed. SSH is better than Telnet because SSH is encrypted. The PIX can only be a Telnet server and not a Telnet client. n. Is SNMP used to manage network devices and gather information? If so, then: <ul style="list-style-type: none"> i. Ensure that the default string of <i>public</i> is not used. Use a string with non-dictionary characters such as @#\$%. ii. Is SNMP used to gather statistical data? o. If logging is used with PIX Device Manager (PDM), then obtain graphs for the last 5 days. Graphs available are VPN Connections, system, connection (perfmon), misc. (IDS, misc requests, replies, and attacks), and interface (buffer overruns and collision counts) graphs. p. Run the show cpu usage command to determine if the CPU is overworked. The 		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>usage should be below 30%.</p> <ul style="list-style-type: none"> i. If the CPU usage is above 30%, then run the <code>show processes</code> command. This report will show all processes running. q. Run the <code>show perfmon</code> command to show the average values for the number of translations and connections by protocol. This will help to determine if a certain connection is using too much CPU or memory. r. Run the <code>show memory</code> command to determine how much memory is be used at the time the command is run. Encryption tends to use more memory. s. Run the <code>show xlate</code> command to determine how much memory address translation is using. The report will print something similar to: <pre>PIX# show xlate 200 in use, 355 most used</pre> <p>Then multiply the 200 by 56 bytes to determine how much memory is used. This would be 11200 bytes used for address translation.</p> t. Run the <code>show block</code> command to determine much memory is used for special traffic. These sizes are reserved: <ul style="list-style-type: none"> i. 4: DNS, IKE, TFTP, etc. ii. 80: stores failover hellos and TCP intercept acknowledgements iii. 256: stores stateful failover messages iv. 1550: used for Ethernet (10 and 100) v. 16384: used for Gigabit Ethernet vi. The MAX column is the amount of memory allocated. vii. The LOW column indicates the lowest amount of blocks available since the firewall booted. viii. The CNT column shows the available number of blocks. ix. The LOW and CNT counters can be reset with the <code>clear blocks</code> command. 		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<ul style="list-style-type: none"> u. Run the <code>show traffic</code> command to determine how much activity was received and transmitted on the inside and outside of the network. v. Determine if the logs report: <ul style="list-style-type: none"> i. Successful and unsuccessful logins ii. Successful logouts iii. Successful and unsuccessful use of privileged commands iv. Successful and unsuccessful application and session initiation v. Successful and unsuccessful use of the <code>print</code> command vi. Successful and unsuccessful access control permission modification vii. Unsuccessful unauthorized access attempts to files viii. Successful and unsuccessful shutdown and startup <p>59. Is the date and time correct on the firewall? Ensure the accuracy with the <code>show clock</code> command. Which time zone is it set for? This helps to determine exactly when an event occurred.</p> <ul style="list-style-type: none"> a. Is the Network Time Protocol (NTP) used to keep accurate time? Enabling NTP will help to prevent hackers from attacking based on time (expired time blocks, etc.). <p>60. Does the organization use a VPN?</p> <ul style="list-style-type: none"> a. If not, then ensure that the firewall is not configured for use with a VPN. <p>61. Is IDS enabled on the firewall? If so, what is reported to management?</p> <p>62. Does the firewall provide ingress filtering?</p> <p>63. Does the firewall provide egress filtering?</p> <p>64. Is spoof detection enabled?</p> <p>65. How does the firewall handle packet fragments?</p> <p>66. How does the firewall handle oversized packets?</p> <p>67. How does the firewall overlapped packets?</p>		

Information Systems Internal Audit Program

Audit Procedure	W/P Ref.	Performed By
<p>68. How does the firewall handle an ongoing stream (flooding) of SYN packets?</p> <p>69. How does the firewall handle enumeration attempts?</p> <p>70. If the firewall should fail, how will the IT department compensate?</p> <p>71. Is the firewall's configuration backed up? If so, how often?</p> <p>72. Is a change log file maintained for the firewall?</p> <p>73. Does the firewall have compilers, editors, and/or any other type of development tool? There shouldn't be.</p> <p>74. Are the following protocols run through the firewall (they should be disabled):</p> <ul style="list-style-type: none"> a. tftp b. NIS c. NFS d. UUCP e. X f. finger <p>75. On the email gateway, is EXPN and VRFY enabled?</p> <p>76. Is the firewall configured to trust any other system? It should not trust any other system. Test this.</p>		