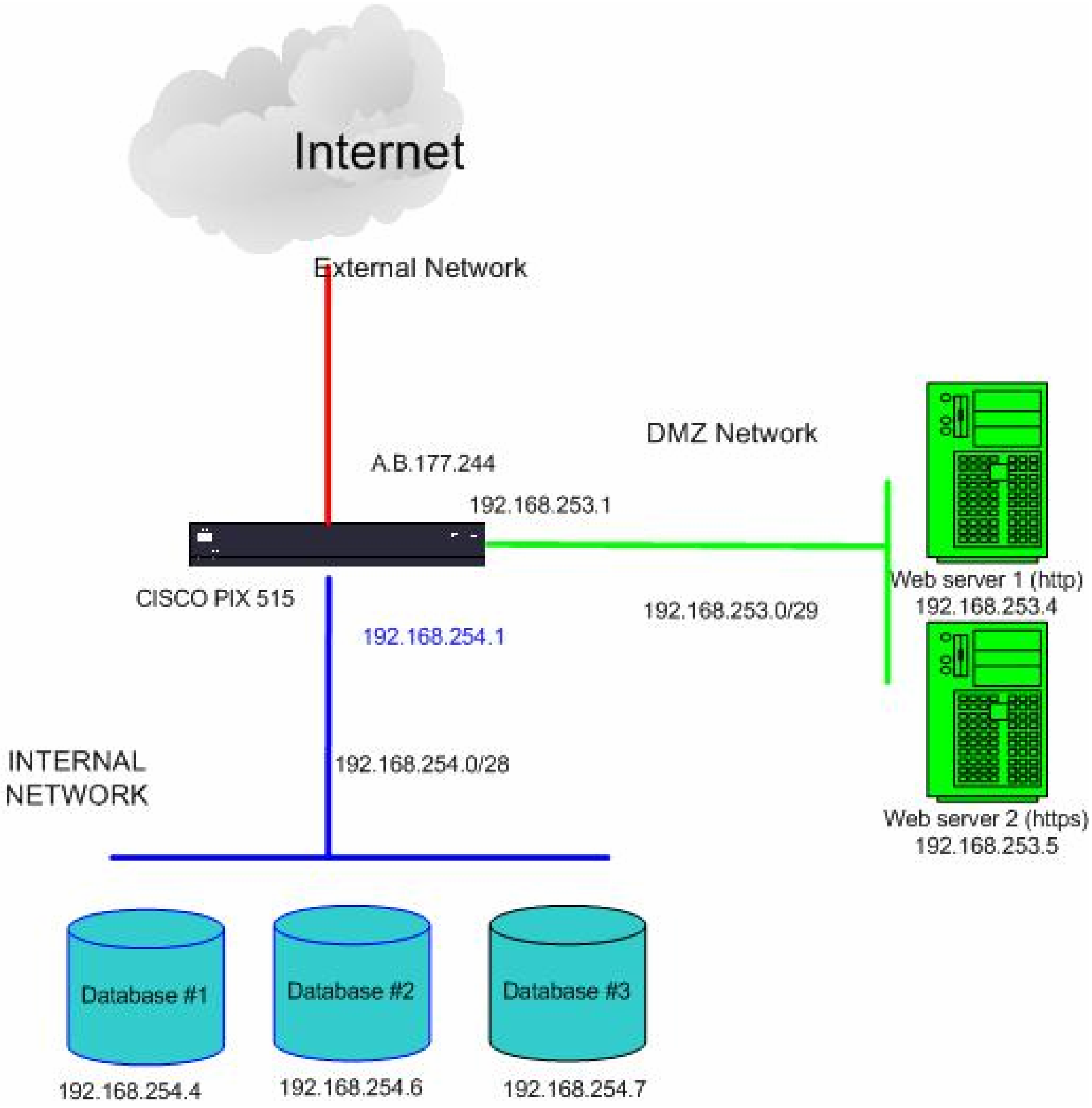
Auditing a Cisco PIX firewall: An Auditor Perspective

Rick W. Yuen

April 15, 2003
GSNA Assignment Version 2.1

Introduction:
ABC Company is a mid-sized online marketing company. The web infrastructure shown is located in a co-location centre with 724 security, it conducts online surveys and provides report for authorized customers. ABC Company uses a Cisco PIX515 firewall to protect this infrastructure.

Network Diagram:



1.1) System to be audited

System Profile

Brand Name	Cisco
System Type	PIX 515

Memory	2 x 64Mb Ram
CPU	200 MHz
Ethernet 0	10/100 Onboard Mbps interface
Ethernet 1	10/100 Onboard Mbps interface
Ethernet 2	PIX-1FE 10/100 Mbps interface
Ethernet 3	PIX-1FE 10/100 Mbps Interface (currently unused, for future expansion)
Flash	16Mb Flash On board
Serial Number	18061XXX
PIX Firewall Version	6.2(2)

I am auditing a Cisco PIX firewall running with version 6.22 operating system software. This firewall is the only defence to protect ABC Company's web infrastructure. The firewall conducts traffic filtering, protect servers from attack and provide basic intrusion detection service. This audit covers the following area: physical security, network security, packet filtering, backup, change monitoring and how attacks and reconnaissance attempts are handled by the firewall.

1.2) Risk Evaluation

1) Risk	Equipment can get stolen or damaged
Probability	Medium
Severity	High
Consequences	Data can get lost or high equipment replacement cost can ensue. As well, users will not able to connect to ABC's website.

2) Risk	Attacker gains shell access to the firewall
Probability	Low, Cisco PIX drops all connections destined to itself by default.
Severity	High
Consequences	Once attacker gains shell access to the firewall, he might escalate privileges and alter firewall configuration to expose the firewall and the protected hosts.

3) Risk	Attacker breaches legacy Operating System or Firmware.
Probability	High
Severity	High, Certain legacy operating system or firmware releases are subject to multiple vulnerabilities.
Consequences	Attack could take control of the device.

4) Risk	Firewall can fall victim of a Denial of Service (DOS) attack.
Probability	Medium, DOS tools are readily available and easy to use.
Severity	High
Consequences	Firewall will be overwhelmed and cannot handle legitimate packets. Web service will be unavailable for legitimate customers and users.

5) Risk	Attacker can exploit protected hosts due to a too permissive ingress filtering policy.
Probability	Low. Cisco PIX denies all service by default unless explicitly allowed.
Severity	High
Consequences	The internal hosts can be exploited and used for consecutive internal attacks on the LAN.

6) Risk	Protected servers can spread viruses/worms and leak out sensitive information due to a too permissive egress filtering policy.
Probability	High. Cisco PIX uses Adaptive Security Algorithms (ASA), which allows traffic flow from a secure network to a less secure network (For example: from DMZ to outside, or from inside to outside) by default.
Severity	High
Consequences	Loss of reputation and customers.

7) Risk	Attacker gain system information by eavesdropping clear text admin traffic.
Probability	Medium. Encryption license is required if administrator decides to encrypt traffic.
Severity	High
Consequences	Attacker might learn system information, including username/password combinations by sniffing clear text admin traffic and take control of the firewall.

8) Risk	Firewall might be unable to recover from corrupted/tempted configuration in a timely manner.
Probability	Medium
Severity	High
Consequences	Web service will be unavailable for legitimate customers and users. ABC company will not be able to conduct business.

9) Risk	Firewall might provide insufficient logging and auditing.
Probability	High. Logging is not enabled by default.
Severity	Medium. Cisco PIX can buffer up to 100 messages internally. All systems logs shall be sent to a Syslog server or they will be lost.
Consequences	Without system log or audit trail, client would not be able to perform debugging, intrusion detection, forensic analysis effectively.

10) Risk	Hardware failure can occur.
Probability	Medium, Cisco PIX firewall is known to be reliable.
Severity	High
Consequences	If firewall fails to function, web service will be unavailable for legitimate customers and users and ABC company will not be able to conduct business.

11) Risk	Malicious packets can circumvent firewall.
Probability	Medium. Cisco PIX firewall is EAL4 and ICSA certified.
Severity	Medium
Consequences	Attacker might craft packets to circumvent the firewall in order to attack the protected hosts or gain information on them.

1.3) Current State of practice.

There are many sources of information available on the Internet for firewall auditing. Here is a list of resources I referenced to create my checklist:

- Firewall Checklist, Krishni Naidu
- Auditing your firewall setup, Lance Spitzner, Dec2002
- Securing Firewall Using Cisco PIX Version 5.3(2), Frank Boldewin, Aug 2001
- PIX 500 Series Firewall Technical Support, Cisco Systems
- SANS Track-7 Courseware, Various, 2002
- Cert.org www.cert.org
- Original Contribution base on personal experience.
- Online man page for nmap, hping2 and tcpdump
- GSNA Certified Students and posted practical, http://www.giac.org/GSNA.php

Naidu's paper is a good start, it is a vendor neutral firewall checklist that provides very detailed information on which ports should be blocked and what kinds of packets should be filtered.

Spitzner's paper is more targeted toward Checkpoint Firewall-1 administrators/ auditors. It also recommends some techniques (e.g.: udp/tcp filtering, ttl firewalking) and tools (e.g.: nmap, hping2), which are good for any kind of firewall auditing. Neither Naidu nor Spitzner touch topics like backup and change management/monitoring.

Boldewin's paper is tailored for Cisco PIX Version 5.3(2). He wrote it from an administrator's prospective and focuses on what built-in feature an administrator can use to enforce stronger security. Although the paper is written for PIX Version 5.3(2), most features are still valid in current version 6.2(2). Boldewin did not mention how Cisco PIX firewall handles SYN flood attack, SYN flood attack is a simple yet effective denial of service attack. This paper is not in checklist format, it does not include compliance standard and testing.

Cisco website has extensive amount of documentation and configuration examples. I also used Cert.org and Cisco Bug Tool Kit (requires CCO account and login) to research known bugs, vulnerabilities related to Cisco PIX firewall.

Cisco PIX firewall is more than just a stateful firewall. Cisco PIX firewall also has attack guards against common attacks and basic intrusion detection capability; and its configuration could be backed up to a plain text file easily. Most of these features are either not included or work differently on other firewall. The checklist I am presenting includes objectives and testing methods only valid for Cisco PIX firewall and its configuration.

2.0) Cisco PIX Firewall Checklist

Terms:

1) This checklist is designed to audit ABC Company's Cisco PIX firewall.
2) Audit involves scanning and attacks on the firewall and protected hosts. Auditor MUST have written permission and authorization from the Chief Technology Officer (CTO) of ABC Company before the audit starts.
3) Auditor should have 2 or 3 laptop computers with latest version of Linux, tcpdump, nmap and hping2 installed. Most tests require 2 laptop computers, one working as an attacker/scanner; the other one working as an intrusion detector/sniffer to collect data on the destination network.
4) Tcpdump, nmap and hping2 are frequently used in the audit tests. Auditor shall refer to online manuals and product websites for latest documentation and release notes.

   Tcpdump website: www.tcpdump.org
   Hping2 website: www.hping.org
   Nmap website: http://www.insecure.org/nmap/index.html

5) Auditor should conduct the audit with the administrator that has root privilege to the firewall, the administrator being responsible to type in ALL audit command on the firewall and demonstrate the result.

Number	1
Reference	Personal Experience
Control Objective	Physical security.
Risk	Theft and vandalism cause service interruptions. ABC company will not be able to conduct online business if the firewall is stolen or damaged. Probability: Medium Severity: High Consequence: Data can get lost or high equipment replacement cost can ensue. Customers of ABC Company will not be able to connect to the website if the firewall is stolen or damaged.
Compliance	Firewall must be rack-mounted in a locked cabinet.
Testing	Visit the site and ensure the firewall is rack-mounted in a locked cabinet.
Objective /Subjective	Objective.

Number	2
Reference	Cisco Security Advisories http://www.cisco.com/warp/public/707/advisory.html Cisco PIX multiple vulnerabilities. http://www.cisco.com/warp/public/707/pix-multiple-vuln-pub.shtml Cert.org http://www.cert.org/
Control Objective	PIX firewall is running an image that is not subject to any known vulnerability.
Risk	Cisco PIXOS 6.1.3 and earlier are subject to multiple vulnerabilities. System vulnerabilities can result in a total security breach. Probability: Medium Severity: High Consequence: A successful breach can give the attacker full control of the system.
Compliance	PIXOS version must be newer than 6.1.3.
Testing	1) ***show version*** shows the PIXOS version, and the value must be over 6.1.3.
Objective / Subjective	Objective

Number	3
Reference	Own experience
Control Objective	Integrity of Firewall Configuration.
Risk	Configuration corruption or tempting can prevent the firewall from enforcing the security policy. Probability: Medium Severity: High Consequence: Firewall rule does not comply with corporate security policy.
Compliance	The time and the person who did the last change and the cryptography checksum of the configuration must match the maintenance log.
Testing	1) **show version** shows the person who last modified the firewall configuration and the time change was made. 2) **show checksum** shows the cryptography checksum of the current configuration. 3) All 3 pieces of information must match the maintenance log.
Objective / Subjective	Objective

Number	4
Reference	1) Original Contribution 2) Cisco PIX Firewall Command Reference Version 62 (http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/cmdref/index.htm)
Control Objective	Cisco Firewalls are running with right activation key that allows 3DES encryption.
Risk	Attacker can gain system information by eavesdropping clear text admin traffic. Probability: Medium, SSH requires a valid DES/3DES encryption activation-key which is not included by default. Severity: High Consequence: Attacker might obtain system information, including username/password combinations by sniffing clear text admin traffic and taking control of the firewall.
Compliance	VPN-3DES is enabled.
Testing	1) **show version** shows the activation key, and status of all feature. 2) VPN-3DES must be enabled.
Objective /	Objective

Subjective

Number 5

Reference
1) Original Contribution
2) Firewall Checklist, Krishni Naidu
3) Securing Firewall Using Cisco PIX Version 5.3(2), Frank Boldewin, Aug 2001

Control Objective Anti-spoofing filter is setup on every interface to drop spoofed packets.

Risk Attacker might use spoofed packet to attack servers or hijack connections. It is very important to drop and log spoofed packets or malicious packets will circumvent firewall.
Probability: High, anti-spoofing filter is not enabled by default.
Severity: High
Consequence: Attacker can steal legitimate user's identity or overwhelm protected hosts in order to disable web services.

Compliance Ensure spoofed packets cannot traverse the Firewall.

Testing

1) Connect a laptop to the same segment with each interface of the Cisco PIX firewall, use hping2 to created spoofed packets and send them across the firewall.

2) Connect a laptop running tcpdump to the destination network and sniff for the traffic created by hping2.

3) Sniffer shall not detect any spoofed packet created by the auditor.

4) System log shall show spoofed packets created by hping2 scanner are dropped.

Hping2 Instruction:
External Segment:

```
hping2 –a 192.168.254.X  -1 <ip_of_protected_web_server>
```

DMZ Segment:

```
hping2 –a <any_ext_ip> -1 <any_ext_ip>
```

Internal Segment:

```
Hping2 –a <any_ext_ip> -1 <any_ext_ip>
```

Tcpdump instruction:

```
tcpdump -Nn host <dst_ip>
```

Objective/ Subjective: Objective

Number: 6

Reference:

1) Original Contribution
2) Cisco Security Specialist's Guide to PIX Firewall, Syngress, 2002
3) Securing Firewall Using Cisco PIX Version 5.3(2), Frank Boldewin, Aug 2001

Control Objective: Ensure that external fragmented packets will not reach protected hosts.

Risk: Attacker might craft fragmented packets to attack systems or to circumvent firewalls.
Probability: Medium
Severity: High
Consequence: Fragmented packets might overwhelm or crash firewall and protected servers.

Compliance Testing: Protected hosts shall not receive ANY fragmented packets.

1) Ensure fragguard is turned on. Request administrator to show the running configuration; auditor shall see ***"sysopt security fragguard"*** in it.

2) Use hping2 to send streams of fragmented TCP packets to port 80 of the web server #1 and port 443 of web server #2. Connect tcpdump to the DMZ network and tcpdump shall NOT see any fragmented packet coming from the hping2 host.

   Scanner: hping2 -S -p 80 –f <ip_of_www_server>
   Detector: tcpdump –Nn <src_ip_of_attacker>

Objective/ Subjective: Objective

Number: 7

Reference:

1) Cisco PIX Firewall Command Reference Version 62 (http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_62/cmdref/index.htm)
2) Network intrusion detection 2nd edition, Northcutt, 2001

Control Objective: Firewall protect web server against SYN flood attack.

Risk

Firewall or protected host fall victims of SYN Flood Attack.
SYN Flood is a very common and effective denial-of-service attack.
Probability: Medium, attack tools are readily available and easy to use.
Severity: High
Consequence: Server under attack cannot handle legitimate service requests until the buffer is freed up after the bogus requests timeout.

Compliance

Firewall will allow no more than 50 half-open connections to the web server at any given time.

Testing

1) Cisco PIX firewall uses **static** command to setup static network address translation (NAT) or port address translation (PAT). The last 2 parameters of ***static*** command are optional, they set the maximum number of established connections and half-open connections the destination server will receive.
2) Confirm the ***static*** statements for the web servers are set to limit the number of half-open connection. The value of the last parameter needs to be 50 or less.
3) Use hping2 to send stream of SYN packets to tcp/80 of the web server.
   Command: hping2 -a <IP_of_offline_host> -S -p 80 <IP_of_webserver>
4) Sniffer in the DMZ segment shall not see more than 50 SYN packets forwarded to the web server until the web server times out any of the half-open connections.

Objective/ Subjective

Objective

Number

8

Reference

1) Own Contribution
2) Network intrusion detection 2nd edition, Northcutt, 2001
3) Cisco PIX Firewall Command Reference Version 62

Control Objective

Ensure PIX Firewall drops ANY kind of ICMP packets

Risk

Attacker can use ICMP packets for reconnaissance and Denial-of Service attacks.
Probability: High
Severity: High
Consequence: Attacker might use the acquired information to refine attacks against the protected servers or DOS the server so that it cannot service legitimate users.

	Remark: ICMP Type 3 Code 4 (destination unreachable, fragment needed) is generally allowed in most setup. In this case, web servers are protected behind the firewall and will NOT initiate a connection. Therefore, it is safe to drop all ICMP packets.
Compliance	Ensure Firewall drops all ICMP packets.
Testing	1) Use any tool to generate and send at least 3 different kinds of ICMP packets to the protected server. 2) Sniffer at the destination network shall not detect the icmp packets generated by auditor. 3) Firewall log shows packets are dropped.
Objective / Subjective	Objective

Number	9
Reference	Own Experience
Control Objective	Ensure System shell access is available at an authorized IP address via secure shell SSH.
Risk	SSH Server is subject to brute force password attacks. Probability: Medium Severity: High Consequence: Attacker might crack the password and gain admin privilege on the firewall and expose all the protected hosts.
Compliance	Firewall only accepts SSH connections initiated from A.B.C.D to the external interface. Ensure only authorized personnel at the specific IP address can logon to Firewall using SSH.
Testing	1) Use an SSH client to connect to the Firewall from A.B.C.D. User will be prompted for username and then password. *2)* Use nmap to scan tcp/22 of against all interfaces of the firewall from unauthorized IP addresses. ***nmap –v –sS –P0 –p22 <IP_address_of_firewall>*** Nmap shall show that the port 22/tcp is filtered on all firewall interfaces.
Objective/ Subjective	Objective

Number	10
Reference	1) Own Experience 2) Building your firewall rulebase, Lance Spitzner
Control	Ensure firewall only pass through authorized packets.

Objective	
Risk	Attacker can exploit protected hosts due to a too permissive ingress filtering policy. Probability: Low Severity: High Consequence: The internal hosts can be exploited and used for consecutive internal attacks on the LAN.
Compliance	Firewall only accepts http to web server 1 and https to web server 2.
Testing	1) Review the access-list with the Firewall administrator. 2) Use nmap to perform tcp SYN and udp scan against the IP range protected by the firewall. Command: nmap -v -sS -P0 A.B.177.244-246 Command: nmap -v -sU -P0 A.B.177.244-246 3) Nmap shall show all scanned ports are filtered except tcp/80 and tcp/443 on web server 1 and web server 2 respectively. 4) Firewall log shall show that all scan traffic is dropped except that destined to tcp/80 (http) to web server A and tcp/443 (https) web server B.
Subjective or Objective	Objective
Number	11
Reference	1. Own Experience 2. Building your firewall rulebase, Lance Spitzner
Control Objective	Ensure only authorized traffic can go from the DMZ network to the internal network.
Risk	Once attacker compromises web server in the DMZ segment, he might use the compromised host as a platform to launch attack against SQL servers in internal network if firewall allows any traffic from DMZ to internal network. Probability: Low Severity: Medium Consequence: Attacker might access corporate database with sensitive data.
Compliance	Firewall allows web servers in the DMZ network to contact SQL server in the internal network on tcp/1521 and drop otherwise.
Testing	1. Review the access-list with the Firewall administrator. 2. Connect a scanner in the DMZ network and a sniffer in the internal network. 3. Initiate a TCP SYN and UPD scan from DMZ to internal network using nmap. Scan should shows only tcp/1521 is allowed from DMZ to internal network.

	4. Firewall log shall show that all scan traffic is dropped except that destined to tcp/1521 (http) to SQL servers in internal network.
Objective/ Subjective	Objective
Number	12
Reference	1) Own Experience 2) Building your firewall rulebase, Lance Spitzner
Control Objective	Ensure only authorized traffic can leave the DMZ network to external network.
Risk	Due to a too permissive egress policy for DMZ outbound traffic, Web servers might help spreading viruses/worms and leak out sensitive information. Probability: Medium Severity: High Consequence: Loss of reputation and customers.
Compliance	Firewall drops all connection initiated from the DMZ network to the external network.
Testing	1) Review the access-list with the Firewall administrator; ensure there is a rule to drop all traffic initiated from the DMZ network explicitly. 2) Connect an Nmap scanner to the DMZ network and a tcpdump sniffer to the external network. 3) Run TCP SYN scan and UPD scan against the target in an external network. Nmap shall report ALL scanned ports are filtered. Test fails if Nmap detects any open port. 4) Correlate the scan result to the port status on the target host using "netstat –an".
Objective/ Subjective	Objective
Number	13
Reference	1) Own Experience 2) Building your firewall rulebase, Lance Spitzner
Control Objective	Ensure only authorized traffic can leave the internal network.
Risk	SQL might help spreading viruses/worms and leak out sensitive information if firewall allows any outgoing traffic initiated from internal network. Probability: Medium Severity: High

	Consequence: Loss of reputation and customer.
Compliance	Firewall drops all traffic initiated in the internal network.
Testing	1) Review the access-list with the Firewall administrator; ensure there is a rule to drop all traffic initiated from the internal network explicitly. 2) Connect an Nmap scanner to the internal network and initiate TCP SYN scan and UPD scan against test machines in DMZ and an external network. Nmap shall report ALL scanned ports are filtered. Test fails if Nmap detects any open or closed port. 3) Target host shall not see any traffic initiated from the scanner or test will fail. 4) Correlate the scan result to the port status on the target host using “netstat –an”.
Objective/ Subjective	Objective

Number	14
Reference	Personal Experience
Control Objective	Verify that Firewall log is sent to syslog server.
Risk	Firewall might provide insufficient logging and auditing. Probability: High, Logging is not enabled by default. Cisco PIX firewall can only log a very small amount of log locally. It must use a syslog server to collect log or old logs will be overwritten. Severity: Medium Consequence: Without system log, client would not be able to perform debugging, intrusion detection, forensic analysis effectively.
Compliance	Firewall log is sent to a syslog server.
Testing	Monitor the log provided by the syslog server and correlate it to the real-time traffic.
Objective or Subjective	Objective

Number	15
Reference	1) Own experience 2) Attack guards and IDS features, Richard Deal 3) Cisco PIX Firewall System Log Message 4) Nessus Security Scanner http://www.nessus.org/
Control	Firewall detects and logs reconnaissance attempts and attacks.

Objective	
Risk	Hosts on the Internet are being probed and attacked constantly and can be compromised. Probability: High Severity: High Consequence: If security administrator fails to detect and response to intrusion attempts, attacker has the opportunity to further exploit the system.
Compliance	Ensure the firewall is able to detect and log traffic that matches any of the *information/attack signatures built into Cisco PIX firewall (reference #2).*
Testing	1) Use nmap, hping2, nessus or other tools to generate at least 3 recognized attacks (reference #2) of different kind on the firewall or the protected hosts. 2) System log shall show the attacks and the corresponding signatures.
Objective or Subjective	Objective

Number	16
Reference	1) Checkpoint Secure Knowledge Base, Stealth Rule 2) Building your firewall rulebase, Lance Spitzner
Control Objective	The PIX firewall should drop and log all non-administrative traffic destined to it.
Risk	Attackers can initiate direct connections to the firewall and probe it for vulnerability. Probability: High Severity: Medium Consequence: Attacker might confirm the existence of the firewall and attack it if the firewall response to illegitimate packets.
Compliance	Firewall drops and logs any connection destined to it.
Testing	1) Run Nmap TCP SYN and UPD scan against all Firewall interfaces. 2) Nmap shall report that all ports on the firewall are filtered. 3) System log shall show that all traffic from the scan host is dropped.
Objective / Subjective	Objective

Number	17

Reference	Personal Experience
Control Objective	Ensure Firewall is backed up weekly.
Risk	In some events configuration could be lost or corrupted and the Cisco PIX firewall could go down. The Administrator should be able to bring it up in a short time. Probability: High Severity: High Consequence: ABC company will not be able to conduct online business if administrator fails to bring up the firewall in a short time.
Compliance	1) Firewall configuration is backed up weekly, before and after configuration changes. 2) Content of last backup must match the current configuration.
Testing	1) Examine and correlate backup files, and maintenance log to ensure firewall is backed up weekly, before and after configuration changes. 2) ***show running-config*** shows the router configuration. The output must match the content of last backup file.
Objective or Subjective	Objective.

Number	18
Reference	Firewall Checklist, Krishni Naidu
Control Objective	High availability of firewall
Risk	If firewall fails to function, web service will be unavailable for legitimate customers and users and ABC company will not be able to conduct business. Probability: Medium Severity: High Consequence: In case of hardware failure, corporate website will be out of service.
Compliance	Ensure firewall has at least one load-sharing or hot-standby peer.
Testing	1) Ensure the presence of a hot-standby or load-sharing peer. 2) Let administrator run system commands to show the status of high availability or load sharing operation.
Objective or Subjective	Objective.

Number	19
Reference	Firewall Checklist #23, Krishni Naidu

Control Objective	Ensure firewall keep track of session state.
Risk	Attackers can circumvent the firewall by sending out-of-state packets. Probability: Low, Cisco PIX is a stateful firewall by default. Severity: High Consequence: Attacker might send malicious packet through the firewall for to gain system information or attack protected server.
Compliance	Firewall drops all ACK packets that do not correspond to any previously established TCP session.
Testing	1. Connect computers running tcpdump (or other protocol analyser) in the dmz and internal network. 2. Run Nmap ACK scan against external interface and protected hosts from external segment. Command: nmap –sA A.B.177.244-246 3. Nmap shall not report that any ports is UNfiltered. 4. System log shall show that all traffic from the scan host is dropped. 5. Tcpdump shall not see any ACK traffic generated by the nmap scanner.
Objective/ Subjective	Objective

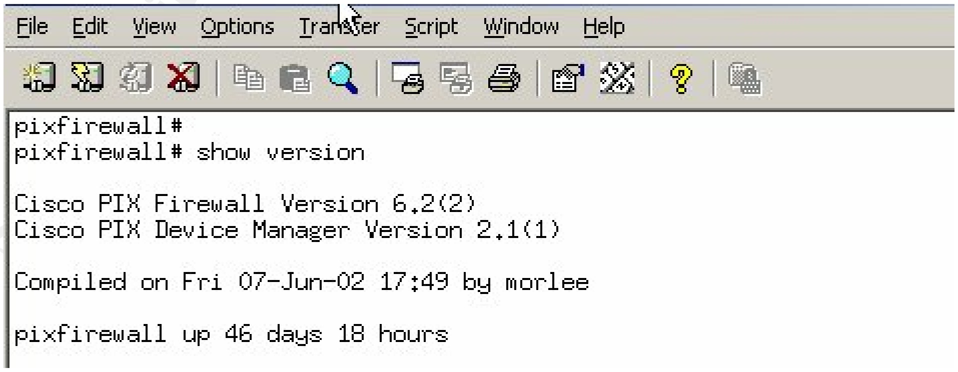
Number	20
Reference	Personal Experience
Control Objective	Ensure every administrator has own account login.
Risk	System's accountability could be compromised by use of shared accounts and passwords. Probability: High Severity: Medium, Consequence: Not being able to tell who made a particular change even with proper logging makes difficult incident investigation and reporting.
Compliance	1) Ensure each administrator has his/her own account. 2) Ensure there is no extra or backdoor account.
Testing	1) Ask administrator to issue "show user" to see there is a user account for each administrator. 2) The number of accounts on the firewall must match the number of administrators that need to log on to it.
Objective / Subjective	Objective

3.1 Conduct the Audit

Number	1
Control Objective	Physical Security
Compliance	Firewall must be rack-mounted in a locked cabinet.
Testing and result	Verified the firewall is rack mounted in a locked cabinet.
Pass/Fail	**Pass**

Number	2
Control Objective	PIX firewall is running an image that is not subject to any known vulnerability.
Compliance	PIXOS version must be newer 6.1.3.
Testing and result	"Show version" output shows Cisco PIX Firewall Version is 6.2.2, newer than 6.1.3

```
pixfirewall# show version

Cisco PIX Firewall Version 6.2(2)
Cisco PIX Device Manager Version 2.1(1)

Compiled on Fri 07-Jun-02 17:49 by morlee

.....
```



```
pixfirewall#
pixfirewall# show version

Cisco PIX Firewall Version 6.2(2)
Cisco PIX Device Manager Version 2.1(1)

Compiled on Fri 07-Jun-02 17:49 by morlee

pixfirewall up 46 days 18 hours
```

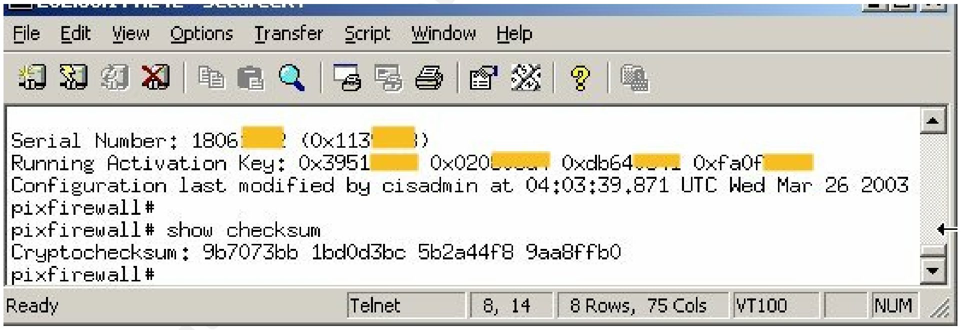
Pass/Fail	**Pass**

Number	3
Control Objective	Integrity of Firewall Configuration.

Compliance The time and the person who did the last change and the cryptography checksum of the configuration must match the maintenance log.

Testing and result Username, time, and checksum match the maintenance log.

```
pixfirewall# sh version

…output snipped..

Serial Number: 1806???? (0x113????)
Running Activation Key: 0x3951???? 0x0208???? 0xdb64????
0xfa0????
Configuration last modified by cisadmin at 04:03:39.871 UTC Wed
Mar 26 2003
pixfirewall#
pixfirewall# show checksum
Cryptochecksum: 9b7073bb 1bd0d3bc 5b2a44f8 9aa8ffb0
pixfirewall#
```



```
Serial Number: 1806[redacted] (0x113[redacted])
Running Activation Key: 0x3951[redacted] 0x020[redacted] 0xdb64[redacted] 0xfa0f[redacted]
Configuration last modified by cisadmin at 04:03:39.871 UTC Wed Mar 26 2003
pixfirewall#
pixfirewall# show checksum
Cryptochecksum: 9b7073bb 1bd0d3bc 5b2a44f8 9aa8ffb0
pixfirewall#
```

Pass/Fail **Pass**

Number 5

Control Objective Anti-spoofing filter is setup on every interface to drop spoofed packets.

Compliance Spoofed packets cannot traverse the Firewall.

Testing & result Firewall detected and dropped all spoofed packets. Tcpdump on the destination network did not detect any spoofed packets either.

Test #1 Generate spoof packets (4.5.6.7) from internal network (192.168.254.0/28) to external network.
Command used: “hping2 –a 4.5.6.7 -1 1.2.3.4”

Syslog Message:
Feb 11 15:28:50 pixfirewall %PIX-1-106021: ***Deny icmp reverse***

path check from 4.5.6.7 to 1.2.3.4 on interface inside

Tcpdump did not detect the spoofed packets created by the hping2 scanner.

Test #2 Generate spoof packets (4.5.6.7) from dmz (192.168.253.0/28) to external network.
Command used: “hping2 –a 4.5.6.7 -1 1.2.3.4”

Syslog Message:
Feb 11 15:32:02 pixfirewall %PIX-1-106021: ***Deny icmp reverse path check*** from 4.5.6.7 to 1.2.3.4 on interface dmz

Tcpdump did not detect the spoofed packets created by the hping2 scanner.

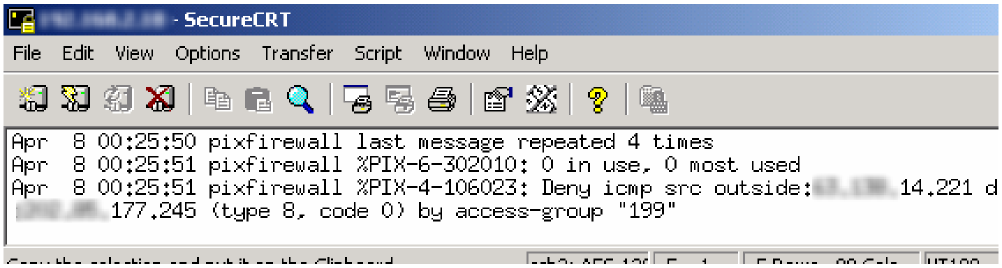
Test #3 “Generate spoof packets (192.168.254.3) from external network to external network.
Command used: hping2 –a 192.168.254.3 -1 A.B.177.245

Syslog Message:
Feb 11 15:40:55 pixfirewall %PIX-1-106021: ***Deny icmp reverse path check*** from 192.168.254.3 to A.B.177.245 on interface outside

Tcpdump did not detect the spoofed packets created by the hping2 scanner.

Pass/Fail	**Pass**

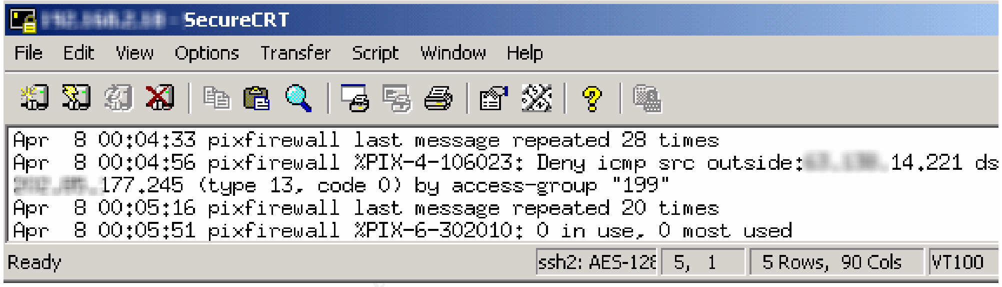
Number	8
Control Objective	PIX Firewall drops ANY kind of ICMP packets
Compliance	Ensure Firewall drops all ICMP packets.
Testing & result	**Test #1** (ping web server 1) 1) Command: ping A.B.177.245 2) Corresponding Syslog message: Apr 8 00:25:51 pixfirewall %PIX-4-106023: Deny icmp src outside:A.B.14.221 dst inside:X.Y.177.245 (type 8, code 0) by access-group "199" 3) Tcpdump on the destination network did not detect the packet.



```
Apr  8 00:25:50 pixfirewall last message repeated 4 times
Apr  8 00:25:51 pixfirewall %PIX-6-302010: 0 in use, 0 most used
Apr  8 00:25:51 pixfirewall %PIX-4-106023: Deny icmp src outside:[redacted].14.221 d
[redacted].177.245 (type 8, code 0) by access-group "199"
```

Test #2 (send timestamp-request to web server 1)

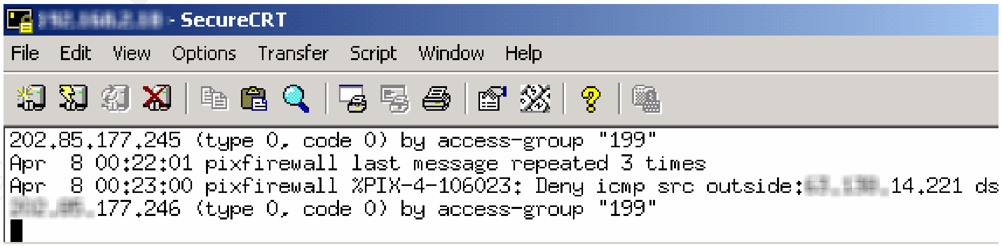
1) Command: hping2 -1 -C 13 A.B.177.245
2) Corresponding Syslog message:
   Apr 8 00:04:56 pixfirewall %PIX-4-106023: Deny icmp src outside: A.B.14.221 dst inside:X.Y.177.245 (type 13, code 0) by access-group "199"
3) Tcpdump on the destination network did not detect the packet.



```
Apr  8 00:04:33 pixfirewall last message repeated 28 times
Apr  8 00:04:56 pixfirewall %PIX-4-106023: Deny icmp src outside:[redacted].14.221 ds
[redacted].177.245 (type 13, code 0) by access-group "199"
Apr  8 00:05:16 pixfirewall last message repeated 20 times
Apr  8 00:05:51 pixfirewall %PIX-6-302010: 0 in use, 0 most used
```

Test #3 (send echo reply to web server 2)

1) hping2 -1 -C 0 A.B.177.246
2) Corresponding Syslog message:
   Apr 8 00:21:58 pixfirewall %PIX-4-106023: Deny icmp src outside:A.B.14.221 dst inside: X.Y.177.245 (type 0, code 0) by access-group "199"
3) Tcpdump on the destination network did not detect the packet.



```
202.85.177.245 (type 0, code 0) by access-group "199"
Apr  8 00:22:01 pixfirewall last message repeated 3 times
Apr  8 00:23:00 pixfirewall %PIX-4-106023: Deny icmp src outside:[redacted].14.221 ds
[redacted].177.246 (type 0, code 0) by access-group "199"
```

Pass/Fail	**Pass**

Number	12
Control Objective	Egress filtering
Compliance	Firewall drops all connection initiated from the DMZ network to

external network.

Testing & result

1) Firewall administrator cannot find any ACL rule to drop traffic initiated in DMZ network.

2) Ran Nmap TCP and UDP scan against a test machine, nmap detected open port. The open ports reported by nmap match “netstat –an” output on the destination server.

The matching result proves machines in DMZ network have unrestricted access to the outside world.

=============nmap output ====================

```
www:~# nmap -v -sS -P0 A.B.177.2
Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host SNIFFER_TARGET(X.Y.Z.A) appears to be up ... good.
Initiating SYN Stealth Scan against SNIFFER_TARGET(X.Y.Z.A)
Adding open port 25/tcp
Adding open port 13/tcp
Adding open port 23/tcp
Adding open port 22/tcp
Adding open port 9/tcp
Adding open port 37/tcp
The SYN Stealth Scan took 378 seconds to scan 1554 ports.
Interesting ports on SNIFFER_TARGET(X.Y.Z.A):
(The 1548 ports scanned but not shown below are in state:
closed)
Port       State       Service
9/tcp      open        discard
13/tcp     open        daytime
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
37/tcp     open        time


www:~# nmap -v -sU -P0 A.B.177.2

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host SNIFFER_TARGET(X.Y.Z.A) appears to be up ... good.
Initiating UDP Scan against SNIFFER_TARGET(X.Y.Z.A)
The UDP Scan took 1935 seconds to scan 1459 ports.
Adding open port 514/udp
Adding open port 9/udp
Interesting ports on SNIFFER_TARGET(X.Y.Z.A):
(The 1457 ports scanned but not shown below are in state:
```

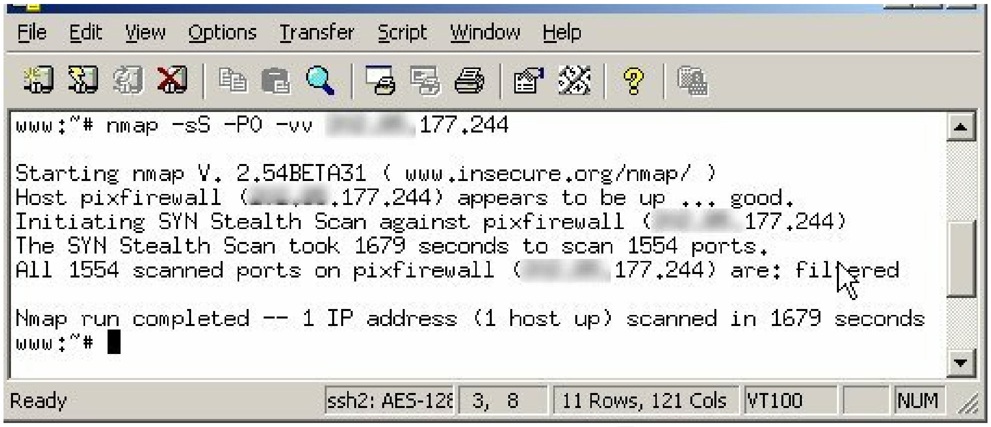
```
closed)
Port       State      Service
9/udp      open       discard
514/udp    open       syslog


=========netstat output from destination server =========
XYZ:~# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address          Foreign Address
State
tcp        0      0 0.0.0.0:37             0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:9              0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:13             0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:22             0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:23             0.0.0.0:*              LISTEN
tcp        0      0 0.0.0.0:25             0.0.0.0:*              LISTEN
tcp        0    272 H.I.J.18:22            H.I.J.40:1060
ESTABLISHED
tcp        0      0 H.I.J.18:22            H.I.J.40:1083          ESTABLISHED
tcp        0      0 H.I.J.18:22            H.I.J.40:1052          ESTABLISHED
udp        0      0 0.0.0.0:514            0.0.0.0:*
udp        0      0 0.0.0.0:9              0.0.0.0:*

…output snipped….
XYZ:~#
```

Pass/Fail **Fail**

Number	16
Control Objective	Firewall logging
Compliance	Firewall drops and logs any connection destined to it.
Testing & result	***Testing:*** Run Nmap tcp Syn scan against the firewall from external network.

```
www:~# nmap -sS -P0 -vv A.B.177.244

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host pixfirewall (A.B.177.244) appears to be up ... good.
Initiating SYN Stealth Scan against pixfirewall (A.B.177.244)
The SYN Stealth Scan took 1679 seconds to scan 1554 ports.
All 1554 scanned ports on pixfirewall (A.B.177.244) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1679
```

seconds
www:~#

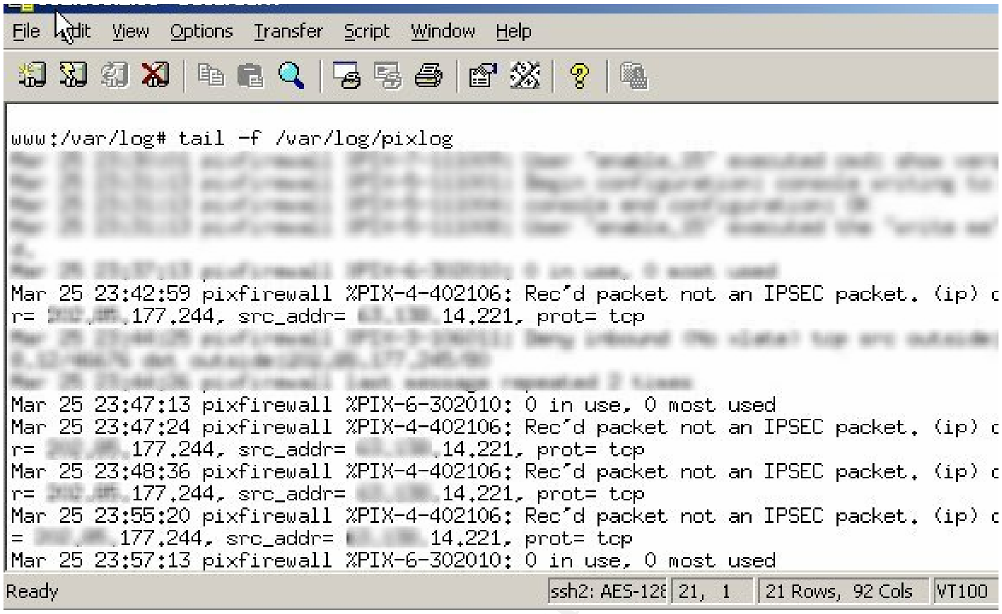


```
www:~# nmap -sS -P0 -vv [redacted].177.244

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host pixfirewall ([redacted].177.244) appears to be up ... good.
Initiating SYN Stealth Scan against pixfirewall ([redacted].177.244)
The SYN Stealth Scan took 1679 seconds to scan 1554 ports.
All 1554 scanned ports on pixfirewall ([redacted].177.244) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in 1679 seconds
www:~#
```

Result: Nmap shows all 1554 tcp ports are filtered. However, syslog only shows 5 irrelevant entries out of 1554 received tcp packets.

Syslog messages generated by the scan:

```
Mar 25 23:42:59 pixfirewall %PIX-4-402106: Rec'd packet not an
IPSEC packet. (ip) dest_addr= A.B.177.244, src_addr= X.Y.14.221,
prot= tcp
…
Mar 25 23:47:13 pixfirewall %PIX-6-302010: 0 in use, 0 most used
Mar 25 23:47:24 pixfirewall %PIX-4-402106: Rec'd packet not an
IPSEC packet. (ip) dest_addr= A.B.177.244, src_addr= X.Y.14.221,
prot= tcp
Mar 25 23:48:36 pixfirewall %PIX-4-402106: Rec'd packet not an
IPSEC packet. (ip) dest_addr= A.B.177.244, src_addr= X.Y.14.221,
prot= tcp
Mar 25 23:55:20 pixfirewall %PIX-4-402106: Rec'd packet not an
IPSEC packet. (ip) dest_addr= A.B.177.244, src_addr= X.Y.14.221,
prot= tcp
```



```
www:/var/log# tail -f /var/log/pixlog
[redacted]
Mar 25 23:42:59 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) d
r= [redacted].177.244, src_addr= [redacted].14.221, prot= tcp
[redacted]
Mar 25 23:47:13 pixfirewall %PIX-6-302010: 0 in use, 0 most used
Mar 25 23:47:24 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) d
r= [redacted].177.244, src_addr= [redacted].14.221, prot= tcp
Mar 25 23:48:36 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) d
r= [redacted].177.244, src_addr= [redacted].14.221, prot= tcp
Mar 25 23:55:20 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) d
= [redacted].177.244, src_addr= [redacted].14.221, prot= tcp
Mar 25 23:57:13 pixfirewall %PIX-6-302010: 0 in use, 0 most used
```

TCP SYN scans against internal and DMZ interfaces produced the same result.

Pass/Fail **Fail**

Number 17

Control Objective Ensure Firewall is backed up weekly.

Compliance Firewall configuration is backed up weekly, before and after configuration changes.
Content of last backup must match the current configuration.

Testing & result

1) Checked backup files and maintenance log, confirmed that firewall is backed up weekly on Friday evening, before and after configuration change.
2) ***show running-config*** shows the firewall configuration is identical to the content of the last backup file.

Pass/Fail **Pass**

Number 9

Control Objective Only SSH connections from an authorized IP address are allowed to the external interface.

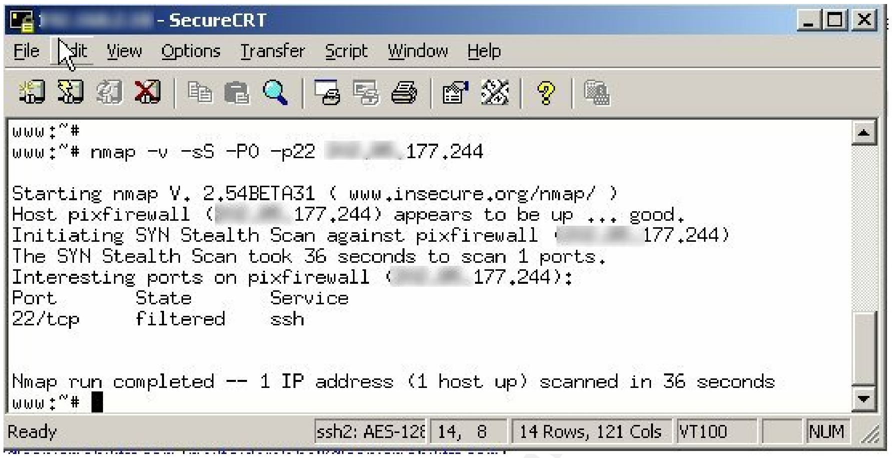
Compliance Firewall only allows SSH connections initiated from A.B.C.D to its external interface.

Testing & result

1) Auditor was able to connect using SSH to the external interface of the firewall from A.B.C.D.
2) Ran Nmap SYN scan against the firewall from other IP addresses. It shows the SSH port (tcp/22) on all firewall

interfaces is filtered.

Nmap Scan Result against external interface:



```
www:~#
www:~# nmap -v -sS -P0 -p22 [redacted].177.244

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
Host pixfirewall ([redacted].177.244) appears to be up ... good.
Initiating SYN Stealth Scan against pixfirewall ([redacted].177.244)
The SYN Stealth Scan took 36 seconds to scan 1 ports.
Interesting ports on pixfirewall ([redacted].177.244):
Port       State       Service
22/tcp     filtered    ssh

Nmap run completed -- 1 IP address (1 host up) scanned in 36 seconds
www:~#
```

Nmap scan against tcp/port 22 on dmz and internal interfaces produced same result: Firewall does not accept and filters SSH connection from unauthorized host.

Pass/Fail **Pass**

Number 15

Control Objective Firewall detects, logs reconnaissance attempts and attacks.

Compliance Ensure the system is able to detect and log traffic matching any of the *information/attack signatures built into Cisco PIX firewall.*

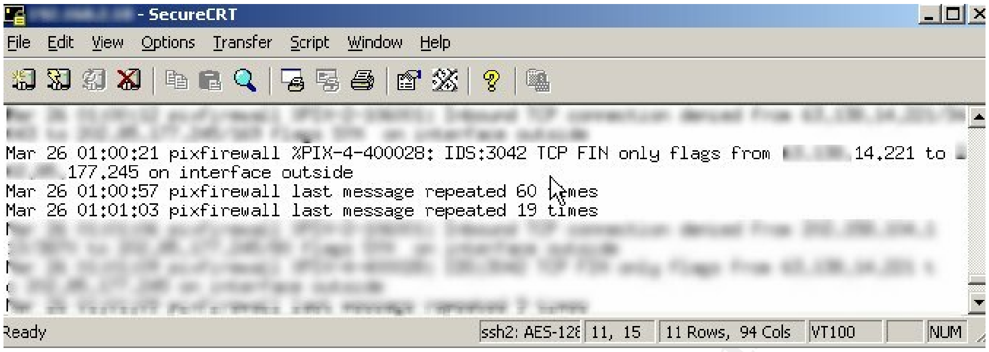
Testing and result

Test #1: TCP FIN SCAN

Auditor ran TCP FIN scan against web server A.

- www:~# nmap -sF -P0 A.B.177.245

- SYSLOG MESSAGE
  Feb 26 01:00:21 pixfirewall %PIX-4-400028: IDS:3042 TCP FIN only flags from AB.CDE.14.221 to A.B.177.245 on interface outside



```
[redacted]
Mar 26 01:00:21 pixfirewall %PIX-4-400028: IDS:3042 TCP FIN only flags from [redacted].14.221 to [redacted]
[redacted].177.245 on interface outside
Mar 26 01:00:57 pixfirewall last message repeated 60 times
Mar 26 01:01:03 pixfirewall last message repeated 19 times
[redacted]
Ready    ssh2: AES-128  11, 15  11 Rows, 94 Cols  VT100    NUM
```

- Result: Firewall detected and logged the scan.

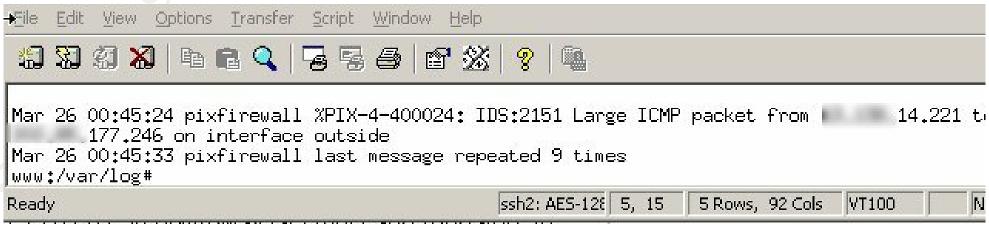
==

Test #2: Large ping packet
Auditor sent large ping packet to web server B.

- www:~# hping2 -1 -d 1234 A.B.177.246
  HPING A.B.177.246 (eth0 A.B.177.246): icmp mode set, 28 headers + 1234 data bytes

  --- A.B.177.246 hping statistic ---
  26 packets tramitted, 0 packets received, 100% packet loss
  round-trip min/avg/max = 0.0/0.0/0.0 ms
  www:~#

- SYSLOG MESSAGE
  Mar 26 00:45:24 pixfirewall %PIX-4-400024: IDS:2151 Large ICMP packet from X.Y.14.221 to A.B.177.246 on interface outside
  Mar 26 00:45:33 pixfirewall last message repeated 9 times



```
Mar 26 00:45:24 pixfirewall %PIX-4-400024: IDS:2151 Large ICMP packet from [redacted].14.221 t
[redacted].177.246 on interface outside
Mar 26 00:45:33 pixfirewall last message repeated 9 times
www:/var/log#
Ready    ssh2: AES-128  5, 15  5 Rows, 92 Cols  VT100    N
```

- Result: Firewall detected and logged the attack

===

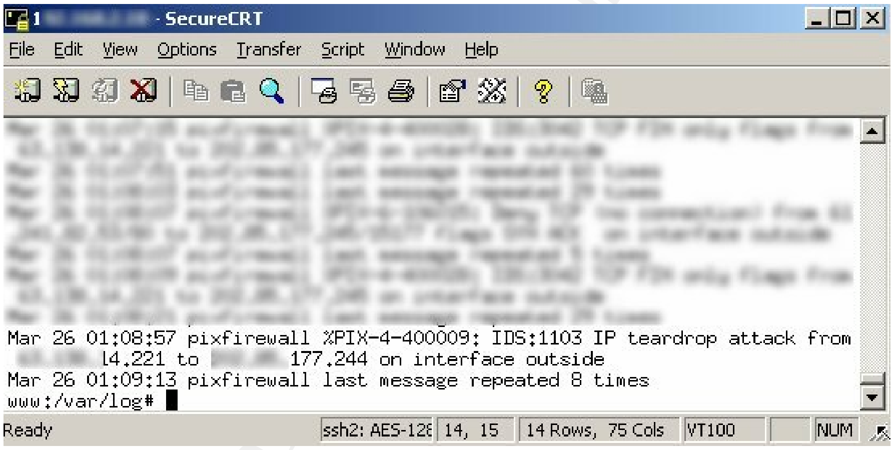
Test #3 Teardrop attack
Auditor generated teardrop attack against the firewall.

- www:~# hping2 -fg 5 -S A.B.177.244
  HPING A.B.177.244 (eth0 A.B.177.244): S set, 40 headers +

0 data bytes

--- A.B.177.244 hping statistic ---
6 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
www:~#

- SYSLOG MESSAGE
  Mar 26 01:08:57 pixfirewall %PIX-4-400009: IDS:1103 IP teardrop attack from X.Y.14.221 to A.B.177.244 on interface outside
  Mar 26 01:09:13 pixfirewall last message repeated 8 times



```
[redacted]
Mar 26 01:08:57 pixfirewall %PIX-4-400009: IDS:1103 IP teardrop attack from
 [redacted] 14.221 to [redacted] 177.244 on interface outside
Mar 26 01:09:13 pixfirewall last message repeated 8 times
www:/var/log#
```

- Tcpdump trace from the attacker, fragmented packet are
  01:08:56.530204 T.J.2.18.2865 > A.B.177.244.0: [|tcp] **(frag 56:16@0+)**
  01:08:56.530048 T.J.2.18.2866 > A.B.177.244.0: [|tcp] **(frag 56:16@0+)**

- Result: Firewall detected and logged the attack

Pass/Fail **Pass**

3.2) Measure Residual Risk

This Cisco PIX failed on 2 items on the checklist: 1) Firewall logging (item #16), 2) Egress filtering for DMZ network (item #12).

1) Firewall logging: The Cisco PIX firewall being audited was not able to log or detect any port scan or packets destined to the firewall. Firewall administrator checked the configuration and confirmed logging was configured properly. We did not see the packets destined to the firewall

even while logging at the debug level. Firewall administrator opened a TAC case with Cisco System. Cisco replied and explained that this feature is not implemented in current PIX OS version 6.22. According to Cisco bug toolkit (Bug ID 30202 and 61325), PIX OS versions 4.22, 4.16, 4.07 and 4.21 do not have this feature implemented either. The Cisco engineer indicated that this bug would be fixed in the next PIX OS. That problem cannot be fixed by reconfiguration at this point. In the meantime, ABC Company shall request the ISP to provide logging report at the border router, or connect a protocol analyser (sniffer) to the external segment to collect logs as a compensating solution. ABC Company would be able to download the software for free once it is available based on the current support contract with the firewall vendor. ABC shall test the new PIX OS release in a lab environment, ensure it is bug free and then upgrade the production firewall.

2) Egress filtering: The PIX firewall being audited allowed *unrestricted* access initiated from the DMZ network to the external network. Firewall shall enforce effective egress filtering to prevent worms spread or root kits download by an attacker that gained access to the system. ABC Company shall update the corporate security policy, and the firewall ACL accordingly. The fix could be done in-house for free.

3) Intrusion Detection: Test #15 shows that this firewall is configured properly to detect intrusion attempts, however Cisco PIX has less than 60 built-in intrusion signatures whereas specialized intrusion detection systems (IDS) are updateable and detect over a thousand kinds of attacks and probes, including application layer attacks, stealth scans and more. Based on the business nature of the ABC Company and the importance of this web infrastructure, I recommend having a specialized IDS sensor in each segment if possible. Though there are many commercial IDS programs, Snort is regarded as one of the best free IDS, and it works on a wide range of OS and hardware platforms. The software and updates are free of charge.

3.3) Is the system auditable?

The audit objectives were to test the following area: physical security, network security, packet filtering, backup, change monitoring and intrusion detection. Each control objective could be validated by one or more objective tests.

Test #16 shows that Cisco PIXOS 6.22 software does not provide sufficient log and audit trail. Therefore, auditor shall always correlate Cisco PIX system logs to reports, or logs provided by other systems (e.g. protocol analyser, scanner, or any tools used in the audit) for more accurate results and modify the testing procedures if necessary.

Overall, I believe that any auditor could reproduce the audit result by following the checklist. The system, Cisco PIX 515 firewall, is very auditable.

4.1, 4.2) Executive Summary, Audit finding

ABC Company uses Cisco PIX515 firewall as the primary defence for the web infrastructure. Audit was very successful. The audit shows the PIX firewall is being monitored closely and is well maintained; it is also configured properly to protect servers from external threats and to detect intrusion attempts supported by PIX firewall.

However, the audit also uncovers that:

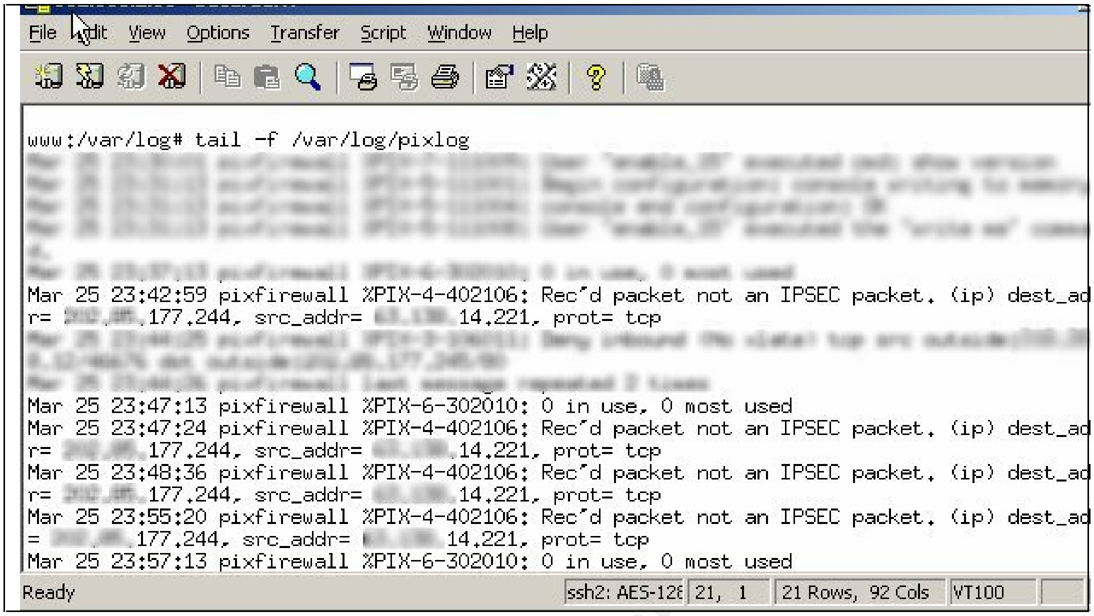
- Firewall logging is not providing sufficient details. (item #12)

  A TCP SYN scan was initiated from an external host against the PIX firewall. All 1554 scanned ports were filtered; however, only 5 irrelevant entries were logged. The test showed that packets destined to Cisco PIX firewall couldn't be logged properly.

Scan Result:
All **1554 scanned ports** on pixfirewall (A.B.177.244) are: **filtered**

Corresponding Syslog Message

```
Mar 25 23:42:59 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC
packet. (ip) dest_addr= A.B.177.244, src_addr= X.Y.14.221, prot= tcp
…
Mar 25 23:47:13 pixfirewall %PIX-6-302010: 0 in use, 0 most used
Mar 25 23:47:24 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC
packet. (ip) dest_addr= A.B.177.244, src_addr= X.Y.14.221, prot= tcp
Mar 25 23:48:36 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC
packet. (ip) dest_addr= A.B.177.244, src_addr= X.Y.14.221, prot= tcp
Mar 25 23:55:20 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC
packet. (ip) dest_addr= A.B.177.244, src_addr= X.Y.14.221, prot= tcp
```



```
www:/var/log# tail -f /var/log/pixlog
[redacted]
Mar 25 23:42:59 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_ad
r= [redacted].177.244, src_addr= [redacted].14.221, prot= tcp
[redacted]
Mar 25 23:47:13 pixfirewall %PIX-6-302010: 0 in use, 0 most used
Mar 25 23:47:24 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_ad
r= [redacted].177.244, src_addr= [redacted].14.221, prot= tcp
Mar 25 23:48:36 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_ad
r= [redacted].177.244, src_addr= [redacted].14.221, prot= tcp
Mar 25 23:55:20 pixfirewall %PIX-4-402106: Rec'd packet not an IPSEC packet. (ip) dest_ad
= [redacted].177.244, src_addr= [redacted].14.221, prot= tcp
Mar 25 23:57:13 pixfirewall %PIX-6-302010: 0 in use, 0 most used
```

Firewall allows any traffic initiated from the DMZ network to the external network. (Checklist item #16)

A network scan initiated from the DMZ network against a target host (detector) in the external network displays the status of ALL scanned ports correctly. In other words, firewall allows unrestricted outgoing access from the DMZ network, the outbound filtering policy is too permissive.

```
Scan Result

The SYN Stealth Scan took 378 seconds to scan 1554 ports.
Interesting ports on SNIFFER_TARGET(X.Y.Z.A):
(The 1548 ports scanned but not shown below are in state: closed)
Port      State     Service
9/tcp     open      discard
13/tcp    open      daytime
22/tcp    open      ssh
23/tcp    open      telnet
25/tcp    open      smtp
37/tcp    open      time


Interesting ports on SNIFFER_TARGET(X.Y.Z.A):
(The 1457 ports scanned but not shown below are in state: closed)
Port      State     Service
9/udp     open      discard
514/udp   open      syslog
```

- Firewall is able to detect no more than 60 attacks out of thousands different kind of attacks on the Internet. (Checklist item #15)

4.3) Risk

Lack of System Log and audit trail (Item 12) Firewall is not able to log packets destined to the firewall. In other words, attacks against the firewall will be undetected; attackers can have unlimited time to exploit and circumvent the firewall until they succeed.

Ineffective egress filtering (item 16) Firewall allowed unrestricted outbound traffic initiated from the Web server (DMZ) network. In case a virus or a worm infects the servers, servers might download a malicious code from the Internet, or even launch attacks against other hosts on the Internet. This, in turn, might lead to resource exhaustion, full security breach or bad press if the incident becomes public.

Intrusion Detection (item 15) Test 15 shows that this firewall is configured properly to detect intrusion attempts. However, Cisco PIX has less than 60 built-in intrusion signatures out of thousands of attacks on the Internet, a lot of attacks will be undetected.

4.4) Recommendations

Recommendation for Item 12

Cisco Systems confirmed that the current Firewall software does not log the packets that hit the firewall directly. Firewall administrator checked the configuration and ensured logging was configured properly. We did not see the packets destined to the firewall even while logging at the highest (debug) level. Cisco Systems confirmed this feature is not implemented in the current Firewall software. According to Cisco Systems, this issue will be addressed in the next software release. ABC Company shall download and test out the new software on a test system before upgrading the production firewall.

Recommendation for Item 16

Firewall outbound policy was too lax and administrators did not catch it. Corporate security policy shall be updated to reflect the current business needs and to not allow outbound traffic from DMZ or internal network. Firewall security policy shall be updated accordingly as well.

Recommendation for item 15 (Intrusion detection) Firewall is configured properly to detect and log intrusion attempts that match any of the information or attack signatures built into the firewall. However, Cisco PIX can detect no more than 60 attacks whereas a specialized IDS system is updateable and detects over thousands of attacks and probes including Denial-of-service, buffer overflows and more. Based on the business nature of the ABC Company and the importance of this web infrastructure, ABC Company shall download, evaluate and then deploy specialized IDS system on each segment if possible instead of depending on the IDS feature provided by the existing firewall.

General Recommendation

Most trained security professionals would be able to identify the above risks. Though network administrator demonstrated very good knowledge in networking and firewall administration, it is recommended that ABC Company provide network security and awareness training to administrators to minimize the potential risks in the future. IT staff and management shall subscribe to security bulletins, advisories and information security magazine, go to product seminars and sales presentation to increase security awareness level.

4.5) Costs

Recommendation for Item 12

ABC Company will be able to get the new firewall OS image free of charge based on the service level agreement with its vendor. Firewall OS evaluation can be done in-house, and shall take less than 30 man-hours. Software upgrade shall require no more than 1 hour of down time of the production firewall.

Recommendation for Item 16

The cost will be 5 man-hours to update the corporate security policy and 3 man-hours for the administrator to review and update the firewall access control list accordingly.

Recommendation for item 15

ABC Company shall allow at least 3 months to evaluate different intrusion detection technologies and systems. Deployment cost depends on the system of choice, configuration and topology.

General Recommendation
For cost management, ABC Company should allow budget for regular information security training. Training cost varies from technologies, training centre, format and other factors.

4.6) Compensating Controls

Recommendation for Item 12 & 15
Instead of placing an commercial IDS system on each segment and waiting for the new Firewall software release, ABC Company can connect a locked down Linux machine running snort IDS to the external network segment using a receive-only cable (http://www.snort.org/docs/faq.html). Both the firewall and the Linux machine shall synchronize to the same time source. The data collected by snort IDS can compensate for the insufficient logs and IDS data provided by the PIX firewall.

Recommendation for Item 16
Firewall administrator Firewall administrator took 2 hour to review and modify the access control list. This problem was fixed and documented on the spot. Firewall passed test #16 after the modification.

General Recommendation
Most security bulletins, advisories and sales presentation are free of charge.

Reference:

- Comment from GSNA graders.
- Firewall Checklist, Krishni Naidu
- Auditing your firewall setup, Lance Spitzner, Dec2002
- Securing Firewall Using Cisco PIX Version 5.3(2), Frank Boldewin, Aug 2001
- PIX 500 Series Firewall Technical Support, Cisco Systems
- SANS Track-7 Courseware, Various, 2002
- Cert.org www.cert.org
- Original Contribution base on personal experience.
- Online man page for nmap and hping2
- GSNA Certified Students and posted practical, http://www.giac.org/GSNA.php
- Cisco Systems, Inc www.cisco.com
- Cisco Security Specialist's Guide to PIX Firewall, Syngress publishing
- Snort FAQ http://www.snort.org/docs/faq.html

160403