

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Security Audit of a Cisco PIX 515 Firewall

GSNA Practical Assignment Version 3.1 Option 1

Randy Hensel

20 August 2004

© SANS Institute 2004, Author retains full rights.

Abstract

This paper is my submission for the practical portion of the requirements of the GSNA (GIAC Systems and Network Auditor) certification. This paper consists of four parts as follows:

1. Preliminary research. Preliminary research consists of researching the subject of the audit, its configuration and the environment in which it runs. Also included in the preliminary research is the most significant risks to the system and the current state of practice in regard to the auditing of this system.

2. A check list to be used in the actual auditing of this particular system.

3. Part three is the evidence and findings of an actual audit using the above mentioned checklist.

4. The audit report which includes an executive summary, findings and recommendations.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Table of Contents 2
Introduction 3
Firewall Policy 3
System Characterization 3
Network Diagram 4
Most Significant Risks 5
Threat Sources 5
Information Assets 6
Vulnerabilities 6
Current State of Practice 8
Audit Checklist 9
1. Physical Security 9
2. Cisco advisory CSCeb20276 (SNMPv3) 10
3. Cisco advisory CSCec20244 (VPNC) 11
4. Verify software is up-to-date 12
5. TCP Syn Scan 12
6. UDP Scan 13
7. Spoofed packets don't cross firewall 13
8. Egress filtering 13
9. Secure access to admin tools 13
10. Logging 14
11. Change Management 15
12. DMZ configuration 15
Audit findings 16
1. Physical Security 16
2. Cisco advisory CSCeb20276 (SNMPv3) 17
3. Cisco advisory CSCec20244 (VPNC) 17
4. Verify software is up-to-date 18
5. TCP Syn Scan 19
6. UDP Scan 20
7. Spoofed packets don't cross firewall 20
8. Egress filtering 21
9. Secure access to admin tools 22
10. Logging 23
11. Change Management 24
12. DMZ configuration 24
Audit report 25
Summary 25
Findings 25
Recommendations 26
Logging 26
Change Management 26
DMZ 27
References 28

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Introduction

National Engineering is an engineering company that provides engineering services for clients nationwide. National Engineering relies heavily on the Internet for research and communication. National Engineering has used a Cisco PIX 515 for the past several years to secure their corporate network from the public Internet. Basic configuration was done by the company that the firewall was purchased from. At the time of installation the company did not have a formal firewall policy. In order to provide a baseline against which an audit could be performed, the following informal firewall policy was created.

Firewall Policy

1. The following services are provided to external entities, by a single server:
    a. Public web site. The public Web site's purpose is to provide marketing information to clients and potential clients; it needs to be accessible to any computer on the Internet.

    b. FTP server. The FTP server needs to be accessible to any client on the Internet. The firewall should allow FTP access to any IP address and will be secured through username and password.

    c. Mail server. Any computer on the Internet should be able send email to the mail server via SMTP.

2. The employees of National Engineering must have unfettered access to all Internet resources.

System Characterization

The subject of this Audit is a Cisco PIX Firewall. The PIX is part of the security architecture that protects National Engineering's corporate information assets from external threats.

The Firewall is Cisco PIX 515 restricted license, running IOS Version 6.3(1). It is configured with 32 MB RAM and two network interfaces. The PIX is a stateful inspection based hardware firewall that runs on the proprietary PIX OS. The version details are listed below.

```
Cisco PIX Firewall Version 6.3(1)
Cisco PIX Device Manager Version 3.0(0)141
Compiled on Wed 19-Mar-03 11:49 by morlee
pixfirewall up 15 days 23 hours
Hardware:   PIX-515, 32 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB
0: ethernet0: address is 0003.6bf7.4481, irq 11
1: ethernet1: address is 0003.6bf7.4482, irq 10
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Enabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited
This PIX has a Restricted (R) license.
```

National Engineering has placed their PIX 515 between the Internet and the corporate network, with one interface facing the internet and the other interface facing their corporate network, see figure 1. Access from the outside is limited to a single server running FTP, HTTP and SMTP servers. Employees also make extensive use of the Internet to share data and communicate with clients and vendors. Access is limited to FTP, HTTP, HTTPS and SMTP. All users need to be able to use FTP, HTTP and HTTPS, but outgoing SMTP connections should be limited to the SMTP server.

The IP addresses in this paper have been "sanitized" with RFC1918 IP addresses. The 192.168.1.0/24 network is designated the "outside network" and the 192.168.2.0/24 network is designated the "inside network", see figure 1 below.

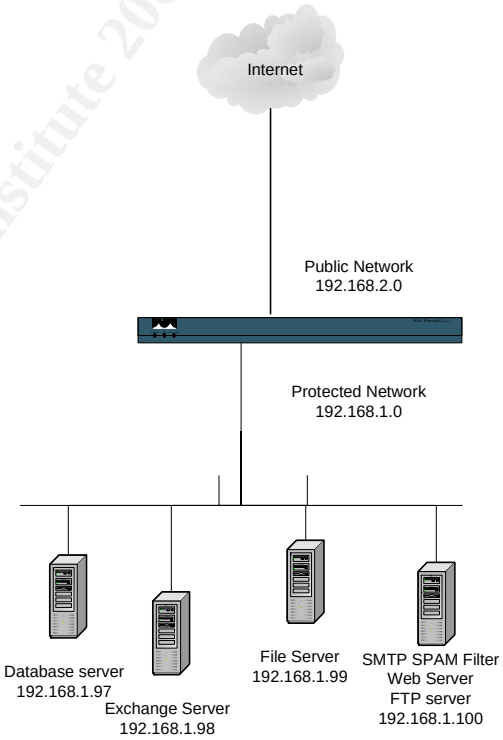


Figure 1

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Most significant risks

The National Institute of Standards defines risk as:

> A function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization or on individuals (NIST, Page 10).

In the following sections I will identify the threat sources and vulnerabilities, their likelihood and the potential impact they may have on the organization.

Threat Sources

There are three main categories of threats: Human, natural and environmental. Because this system is located in an area where natural threats like tornado, earthquakes or hurricanes are uncommon, the likelihood of a natural threat exercising a vulnerability is low. This system is far more likely to succumb to an environmental or human threat. The table below lists the threat categories and what potential damage may occur. If exercised these threats could cost the company revenue and reputation not to mention the time and money needed to replace assets and repair the damage.

Threat	Possible damage
Natural: tornado, earthquake, hurricane etc.	Damage or destruction of firewall hardware, causing loss of communication with clients and vendors.
Human: poorly trained administrators	Misconfigured firewall causing denial of service or disclosure of private or proprietary data.
Human: disgruntled employee	Captures clear text admin traffic to the firewall enabling him to modify the configuration, or gain control of the system.
Human: external malicious entity	Successful system penetration could cause the compromise of company data, including deletion, corruption, website defacement and many other activities.
Environmental: fire suppression sprinklers in data center.	There is the possibility of a water pipe breaking in the data center causing damage to or destruction of the firewall.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Information assets

The following table describes the primary information assets that are protected by the Cisco PIX firewall. These assets are critical to National Engineering's ability to provide products and services to their clients.

Asset	Description
File servers	File servers contain client jobs which if compromised would severely limit the company's ability fulfill contractual obligations.
Database server	The database server contains customer relation data as well as job specification data, which if acquired by a competitor, would put the company at severe disadvantage, and if corrupted, would limit the company's ability to provide products to clients.
Web server	National Engineering maintains a corporate web site that contains basic company information and marketing materials.
Email servers	Email communications with clients and vendors is critical to the daily operations of the business.
Internet connectivity	The company depends heavily on its network infrastructure to communicate with clients and vendors. Disruption of these communication channels would severely hamper business.

Vulnerabilities

The following table lists the potential vulnerabilities of the PIX firewall and how likely those vulnerabilities are to be exploited and what the consequences might be of a successful exploitation. The last column, which is the combination of the potential impact and the likelihood, represents the overall risk that that vulnerability creates for the firewall. The risk is categorized as low, medium or high.

Vulnerability	Potential impact	Likelihood	Risk
Building's use of sprinklers for fire suppression. Fire or malfunction of the sprinkler system could cause irreparable damage to the firewall.	High Total loss of the firewall resulting in a denial of service.	High	High
CSCeb20276 The Cisco PIX firewall crashes and	Medium If successfully exploited, this	Low	Low

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

reloads while processing a received SNMPv3 message when **snmp-server host <if_name> <ip_addr>** or **snmp-server host <if_name> <ip_addr> poll** is configured on the Cisco PIX firewall. This happens even though the Cisco PIX firewall does not support SNMPv3.	vulnerability could result in denial of service.		
CSCec20244 (VPNC) Under certain conditions an established VPNC IPSec tunnel connection is dropped if another IPSec client attempts to initiate an IKE Phase I negotiation to the outside interface of the VPN Client configured Cisco PIX firewall.	Low If successfully exploited, the vulnerability would cause a denial of service against VPN sessions to remote networks. The loss of a VPN client connection would only result in the loss of communication with a remote network. The corporate network and its connection to the internet would not be affected.	Low	Low
Inadequate physical security	High If, by malicious or unintentional act, the firewall were damaged or removed, many services would be unavailable to clients.	High	High
The firewall is administered via Telnet.	High An insider monitoring telnet traffic could intercept authentication information and then have the ability to modify the firewall configuration.	High	High
Software version not up-to-date	High A vulnerability may be found in the firewall software, and if not patched could lead to compromise of the system.	High	High

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Inadequate configuration backups	Medium In the case of a failure where the configuration is lost, down time is significantly increased because configuration must be recreated.	Medium	Medium
Permissive ingress filters	High Permissive ingress filters allows access to vulnerable internal system.	High	High
Permissive egress filter	High Without egress filtering a compromised system on the local LAN could send sensitive information out of the LAN, or could be a launching point for attacks on other systems.	Medium	High

Current State of Practice

There are many sources of information regarding the security and audit of PIX firewalls, the following is a list of the most significant documentation related to the security of firewalls in general and in particular the Cisco PIX firewall. These sources range from the very general to very specific. The NIST paper is a very comprehensive guide to assessing the risk to any Information Technology system, while Rick Yuen's check list is specific to a PIX running OS version 6.2(2).

1. Yuen, Rick W. Auditing a Cisco PIX Firewall: An Auditor Perspective. April 15, 2003. http://www.giac.org/practical/GSNA/Rick_Yuen_GSNA.pdf. This is a good comprehensive audit checklist of the Cisco PIX firewall running PIX OS version 6.2(2).

2. Boldewin, Frank. Secure Firewall using Cisco PIX Version 5.3(2). http://www.securityfocus.com/guest/6811. While not a comprehensive checklist, this article has good descriptions of some of the security features of the PIX firewall. Although it is a bit dated as it is based on PIX OS 5.3(2).

3. Naidu, Krishni Firewall Checklist. http://www.sans.org/score/firewallchecklist.php This is a general firewall checklist not specific to the Cisco PIX but a good place to start for general firewall security recommendations.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4. NIST. Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology Special Publication 800-30 Rev A,Gary Stoneburner, Alice Goguen, and Alexis Feringa. http://csrc.nist.gov/publications/drafts.html#SP80027-RevA. This is a very comprehensive guide to assessing the risk to any Information Technology system.

5. Cisco. Cisco PIX Firewall and VPN Configuration Guide, Cisco Systems. http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a0080172852.html. An on-line book that describes PIX configuration commands by function. It gives good descriptions as well as configuration examples.

6. Spitzner, Lance. Auditing Your Firewall Setup. http://www.spitzner.net. General recommendations for auditing any firewall.

7. Osipov, Vitalya, et al. Security Specialist's Guide to PIX Firewalls. Syngress Publishing Inc., 2002. This is a comprehensive book whose sole subject is the configuration of the PIX firewall.

8. Deal, Richard A. Cisco PIX Firewalls. McGraw Hill/Osborne, 2002. Similar to the previous book with a different slant.

9. Chris Brenton. What is Egress Filtering and How Can I Implement It? http://www.sans.org/rr/papers/21/1059.pdf

Audit checklist

Number 1

Description: Physical Security – Verify system is adequately protected from physical tampering.

Reference: Generally accepted practice. Security of any device will typically include a physical component.

Risk: Vulnerability – Physical damage or loss of the system
Degree of exposure - Low
Severity of loss – High, loss or damage of this system will impact the company's short term ability to conduct business and affect its long term reputation as a leader in its market.

Test Procedure: Visit the facility to verify the device's physical status. The firewall should be in a room where physical access is restricted to company personnel who are responsible for the management of the firewall.

Objectivity: Objective

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Evidence:

Findings:

Number 2

Description: CSCeb20276 (SNMPv3) The Cisco PIX firewall crashes and reloads while processing a received SNMPv3 message.

Reference: Cisco security advisory.
http://www.cisco.com/en/US/products/products_security_advisory09186a00801e118a.shtml

Risk: Vulnerability: Denial of service
Degree of exposure: Low
Severity of Loss: short term loss of Internet Connectivity.

Test Procedure: 1. Use "sh ver" on PIX console to determine firmware version. Version 6.3(1) and lower are vulnerable.
2. If the version is confirmed to be vulnerable then check configuration for the following commands. `snmp-server host <if_name> <ip_addr>` or `snmp-server host <if_name> <ip_addr> poll`. The configuration must contain either of the previous two commands to be vulnerable.

Objectivity: Objective

Evidence:

Findings:

Number 3

Description: CSCec20244 (VPNC) Under certain conditions an established VPNC IPSec tunnel connection is dropped if another IPSec client attempts to initiate an IKE Phase I negotiation to the outside interface of the VPN Client configured Cisco PIX firewall.

Reference: Cisco security advisory.
http://www.cisco.com/en/US/products/products_security_advisory09186a00801e118a.shtml

Risk: Vulnerability: Denial of service to connected VPN Clients.
Degree of exposure: Low

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Severity of Loss: Low

Test Procedure: Run "sh ver" command from PIX console. Only versions 6.2 (2.119) to 6.2.3 are vulnerable.

Objectivity: Objective

Evidence:

Findings:

Number 4

Description: Verify version level of software is up-to-date

Reference: Spitzner

Risk: Vulnerability: Out of date Operating System software could have vulnerabilities that a newer Operating System does not.
Degree of exposure: Medium
Severity of Loss: High

Test Procedure: Run "sh ver" from the console to verify Software revision level. Search Cisco security advisories and BugTraq or other sources for vulnerabilities related to the running version of the software.

Objectivity: Objective

Evidence:

Findings:

Number 5

Description: TCP Syn Scan

Reference: Spitzner, Page 4

Risk: Vulnerability: Permissive ingress filter.
Degree of exposure: High
Severity of Loss: High

Test Procedure: With a computer on the outside interface use "nmap" to perform a TCP scan of all 65,000 ports. On a computer connected to the inside interface run packet

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

capture software (Windump or Ethereal work well) to capture any data that gets through the firewall.
"nmap" command line: `nmap –sN –PT –p1-65000`
-sN = SYN packet will all flags off

Objectivity: Objective

Evidence:

Findings:

Number 6

Description: UDP Scan

Reference: Spitzner, Page 5

Risk:
Vulnerability: Permissive ingress filter.
Degree of exposure: High
Severity of Loss: High

Test Procedure: Use Nmap to send UDP packets to all 65000 ports from the outside network while using Ethereal on the inside to monitor for any packets that may get through the firewall.
"nmap" command line: `nmap –sU –PT –p1-65000 "any inside IP"`

Objectivity: Objective

Evidence:

Findings:

Number 7

Description: Spoofed packets from the outside are not passed to the inside.

Reference: Krishni Naidu, Page 4
Rick Yuen

Risk:
Vulnerability: Denial of Service (DOS) attacks, and session hijacking.
Degree of exposure: Low
Severity of Loss: Low

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Test Procedure: Use nmap to craft spoofed packets and send them across the firewall.
From the outside network use an internal source IP address.
Command: `nmap –sS –P0 –e eth0 –S "any internal IP" –O –T 2 "any internal IP"`

From the inside network use an external source IP address.
Command: `nmap –sS –P0 –e eth0 –S "any external IP" –O –T 2 "any internal IP"`

Objectivity: Objective

Evidence:

Findings:

Number 8

Description: Egress filtering.

Reference: Chris Brenton
Rick Yuen

Risk: Vulnerability: Leakage of sensitive information or the spread of malware.
Degree of exposure: High
Severity of Loss: High

Test Procedure: From the inside network use Nmap to scan an outside IP address. Use Ethereal on the outside interface to capture any traffic coming from the inside network. Only traffic that is allowed by the firewall policy should be seen on the outside network.

Objectivity: Objective

Evidence:

Findings:

Number 9

Description: Secure access to administrative tools

Reference: SANS Track 7 course materials
Rick Yuen

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Risk: Vulnerability: Without secure access to the firewall configuration utility the administrative traffic is vulnerable to eavesdropping. This would enable a person with access to a packet sniffer to capture passwords passed over the network in clear text.
Degree of exposure: High
Severity of Loss: High

Test Procedure: Review firewall configuration. SSH command should be present only allowing access from authorized IP addresses:
Example: `SSH 192.168.1.100 255.255.255.255 inside`
Executing the following command will ensure that rsa keys used in the SSH authentication and encryption have been generated.
`Sh ca mypubkey rsa`

Objectivity: Objective

Evidence:

Findings:

Number 10

Description: Ensure logging is enabled and data is being sent to a syslog server.

Reference: Guide to Cisco PIX Firewall, page 290

Risk: Vulnerability: Without log information forensic analysis and intrusion detection are impossible.
Degree of exposure: High
Severity of Loss: High

Test Procedure: Review firewall configuration. The following commands should be present.
`Logging on`
`Logging host <interface> <syslog_server_IP>`
`Logging trap <level>` (level should be set to a minimum of 4 (Warning Condition). Once proper logging configuration is verified on the PIX, the administrator should be able to demonstrate that the syslog server is operational and receiving messages.

Objectivity: Objective

Evidence:

Findings:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Number 11

Description: Change management

Reference: Rick Yuen, Page 17

Risk: Vulnerability: Undocumented or unauthorized changes are made to the firewall configuration.
Degree of exposure: High
Severity of Loss: High, misconfiguration of the firewall could lead to unavailability of resources or a heightened degree of exposure to other threats.

Test Procedure: Review the change control policy and procedures, as well as the change control logs.

Objectivity: Objective

Evidence:

Findings:

Number 12

Description: Utilization of DMZ (demilitarized zone, or screened network) to host Internet accessible servers.

Reference: Naidu, Page 4
Spitzner, Page 2

Risk: Vulnerability: If a host that is accessible from the Internet becomes compromised, it could be used to launch attacks against other hosts on the same network.
Degree of exposure: High
Severity of Loss: High; a compromised host on the internal network could lead to the comprise of all data and hosts on the on the internal network.

Test Procedure:

1. Visually inspect hardware, configuration should include at least a third network interface to host the DMZ.
2. There should be no static mappings that map outside IP addresses to inside IP addresses. For example, the first two commands below map an outside IP to an inside IP. Then allows www traffic to the inside IP address. Instead of directing www traffic to a host on the inside network as the first two commands do we should see commands like the second two, that direct www traffic to the DMZ.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
static (inside,outside) "outside IP" "inside IP" netmask
255.255.255.255 0 0
access-list acl_outside permit tcp any host "Inside IP" eq www

static (DMZ,outside) "outside IP" "DMZ IP" netmask
255.255.255.255 0 0
access-list acl_DMZ permit tcp any host "DMZ IP" eq www
```

Objectivity: Objective

Evidence:

Findings:

Audit Findings

Number 1

Description: Physical Security – Verify system is adequately protected from physical tampering.

Reference: Generally accepted practice. Security of any device will typically include a physical component.

Risk: Vulnerability – Physical damage or loss of the system
Degree of exposure - Low
Severity of loss – High, Loss or damage of this system will impact the company's short term ability to conduct business and affect its long term reputation as a leader in its market.

Test Procedure: Visit the facility to verify the device's physical status. The firewall should be in a room whose physical access is restricted to company personnel who are responsible for the management of the firewall.

Objectivity: Objective

Evidence: During the site visit it was verified that the firewall was located in a building with good access control and the firewall itself was mounted in a rack that was located in a room where electronic keys limited access to IS staff and upper management.

Findings: While the rack itself was not locked, the building and the room where the firewall was located had good access control.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Number 2

Description:	CSCeb20276 (SNMPv3) The Cisco PIX firewall crashes and reloads while processing a received SNMPv3 message.
Reference:	Cisco security advisory. http://www.cisco.com/en/US/products/products_security_advisory09186a00801e118a.shtml
Risk:	Vulnerability: Denial of service Degree of exposure: Low Severity of Loss: short term loss of Internet Connectivity.
Test Procedure:	1. "sh ver" on PIX console Version 6.3(1) and lower are vulnerable. 2. If the version is confirmed to be vulnerable then check configuration for the following commands. **snmp-server host <if_name> <ip_addr>** or **snmp-server host <if_name> <ip_addr> poll**. The configuration must contain the either of the previous 2 commands to be vulnerable.
Objectivity:	Objective
Evidence:	A review of the firewall configuration confirms that the commands in question are not in use on the firewall and all SNMP options are disabled.
Findings:	The firewall administrator stated that he does not use SNMP to manage any network equipment. A check of the firewall configuration confirms this to be the case.

Number 3

Description:	CSCec20244 (VPNC) Under certain conditions an established VPNC IPSec tunnel connection is dropped if another IPSec client attempts to initiate an IKE Phase I negotiation to the outside interface of the VPN Client configured Cisco PIX firewall.
Reference:	Cisco security advisory. http://www.cisco.com/en/US/products/products_security_advisory09186a00801e118a.shtml
Risk:	Vulnerability: Denial of service to connected VPN Clients. Degree of exposure: Low Severity of Loss: Low
Test Procedure:	Run "sh ver" command from PIX console. Only versions 6.2 (2.119) to 6.2.3 are vulnerable.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Objectivity: Objective

Evidence:
```
pixfirewall# sh ver
Cisco PIX Firewall Version 6.3(1)
Cisco PIX Device Manager Version 3.0(0)141

Compiled on Wed 19-Mar-03 11:49 by morlee

pixfirewall up 21 days 1 hour

Hardware:   PIX-515, 32 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB
.
.
```
Output snipped for brevity.

Findings: The audit subject is running a software version 6.3(1) which is not vulnerable to this particular attack.

Number 4

Description: Verify version level of software is up-to-date

Reference: http://www.sans.org/score/firewallchecklist.php

Risk: Vulnerability: Out of date Operating System software could have vulnerabilities that a newer Operating System does not.
Degree of exposure: Medium
Severity of Loss: High

Test Procedure: Run "sh ver" from the console to verify Software revision level. Search Cisco security advisories and BugTraq or other sources for vulnerabilities related to the running version of the software.

Objectivity: Objective

Evidence:
```
pixfirewall# sh ver
Cisco PIX Firewall Version 6.3(1)
```

Findings: A check of the Cisco web site shows that the current software version of the PIX is 6.3(4). The running version is not the latest version available.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Number 5

Description: TCP Syn Scan

Reference: Spitzner

Risk: Vulnerability
Degree of exposure
Severity of Loss

Test Procedure: With a computer on the outside interface use nmap to perform a TCP scan of all 65,000 ports. On a computer connected to the inside interface run packet capture software (Windump or Ethereal work well) to capture any data that gets through the firewall.
Nmap command line: `nmap –sS –P0 –p1-65000`
`-sN = SYN packet will all flags off`

Objectivity: Objective

Evidence: Nmap results:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (192.168.2.99) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.2.99)
Adding open port 80/tcp
Adding open port 25/tcp
The SYN Stealth Scan took 530 seconds to scan 1601 ports.
Interesting ports on  (192.168.2.99):(The 1598 ports scanned but
not shown below are in state: filtered)
Port       State       Service
21/tcp     closed      ftp
25/tcp     open        smtp
80/tcp     open        http
Nmap run completed -- 1 IP address (1 host up) scanned in 530
seconds
```

Windump results:

```
No.  Time        Source              Destination       Protocol
Info
1 0.000000    192.168.2.100         192.168.1.100         TCP
52005 > http [SYN] Seq=0 Ack=0 Win=2048 Len=0
2 0.000479    192.168.1.100         192.168.2.100         TCP
http > 52005 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1260
3 0.000528    192.168.1.100         192.168.2.100         TCP
http > 52005 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1260
4 0.001091    192.168.2.100         192.168.1.100         TCP
52005 > http [RST] Seq=1 Ack=3611001176 Win=0 Len=0
5 45.366989   192.168.2.100         192.168.1.100         TCP
52005 > ftp [SYN] Seq=0 Ack=0 Win=2048 Len=0
6 45.367048   192.168.1.100         192.168.2.100         TCP
ftp > 52005 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
7 45.367129   192.168.1.100         192.168.2.100         TCP
ftp > 52005 [RST, ACK] Seq=0 Ack=0 Win=0 Len=0
8 61.290103   192.168.2.100         192.168.1.100         TCP
52005 > smtp [SYN] Seq=0 Ack=0 Win=2048 Len=0
9 61.290191   192.168.1.100         192.168.2.100         TCP
smtp > 52005 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1260
10 61.290271  192.168.1.100         192.168.2.100         TCP
smtp > 52005 [SYN, ACK] Seq=0 Ack=1 Win=25200 Len=0 MSS=1260
11 61.290871  192.168.2.100         192.168.1.100         TCP
52005 > smtp [RST] Seq=1 Ack=3061875042 Win=0 Len=0
```

Findings: The firewall only allows FTP, HTTP, and SMTP as described in the security policy.

Number 6

Description: UDP Scan

Reference: Spitzner

Risk: Vulnerability
Degree of exposure
Severity of Loss

Test Procedure: Use Nmap to send UDP packets to all 65000 ports from the outside network while using Ethereal on the inside to monitor for any packets that may get through the firewall.

```
Nmap –sU –P0 –T 3 IP_of_protected net
```

Objectivity: Objective

Evidence: None

Findings: Nmap scan turned up no open UDP ports, this was also verified by Ethereal on the other side of the firewall which detected no packets coming from the Nmap box.

Number 7

Description: Ensure spoofed packets with an inside source address are not passed from the outside to the inside. Also ensure that only inside source addresses are passed to the outside.

Reference: Krishni Naidu
Frank Boldewin
Rick Yuen

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Risk: Vulnerability
Degree of exposure
Severity of Loss

Test Procedure: Use nmap to craft spoofed packets and send them across the firewall.
From the outside network use an internal source IP address.
Command: `nmap –sS –P0 –e eth0 –S "any internal IP" –O –T 2 "any internal IP"`

From the inside network use an external source IP address.
Command: `nmap –sS –P0 –e eth0 –S "any external IP" –O –T 2 "any internal IP"`

Objectivity: Objective

Evidence: Ethereal detected no spoofed packets from the computer running Nmap.

Findings: The audit subject passed the test.

Number 8

Description: Egress filtering.

Reference: SANS Track 7 course materials
Rick Yuen

Risk: Vulnerability
Degree of exposure
Severity of Loss

Test Procedure: From the inside network use "nmap" to perform both UDP and TCP scans of an outside IP address. Use Ethereal on the outside interface to capture any traffic coming from the inside network. Only traffic that is allowed by the firewall policy should be seen on the outside network.

Objectivity: Objective

Evidence: TCP scan

```
No. Time   Source      Destination Protocol Info
19 159.970817  192.168.2.99  192.168.2.100 TCP  4319 > https
[ACK] Seq=1 Ack=1 Win=25200 Len=0
 20 159.975720  192.168.2.99  192.168.2.100 TCP  4319 > https
[RST] Seq=1 Ack=1 Win=0 Len=0
 21 175.991744  192.168.2.99  192.168.2.100 TCP  4397 > domain
[SYN] Seq=0 Ack=0 Win=25200 Len=0 MSS=1260
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
 24 176.489475  192.168.2.99  192.168.2.100 TCP  4397 > domain
[SYN] Seq=0 Ack=0 Win=25200 Len=0 MSS=1260
 27 176.990136  192.168.2.99  192.168.2.100 TCP  4397 > domain
[SYN] Seq=0 Ack=0 Win=25200 Len=0 MSS=1260
 66 234.083646  192.168.2.99  192.168.2.100 TCP  4691 > smtp
[SYN] Seq=0 Ack=0 Win=25200 Len=0 MSS=1260
 69 234.084378  192.168.2.99  192.168.2.100 TCP  4691 > smtp
[ACK] Seq=1 Ack=1 Win=25200 Len=0
 72 234.090939  192.168.2.99  192.168.2.100 TCP  4691 > smtp
[RST] Seq=1 Ack=1 Win=0 Len=0
 74 246.099053  192.168.2.99  192.168.2.100 TCP  4749 > ftp
[SYN] Seq=0 Ack=0 Win=25200 Len=0 MSS=1260
 77 246.099684  192.168.2.99  192.168.2.100 TCP  4749 > ftp
[ACK] Seq=1 Ack=1 Win=25200 Len=0
 80 246.101353  192.168.2.99  192.168.2.100 TCP  4749 > ftp
[RST] Seq=1 Ack=144553716 Win=0 Len=0
 89 255.113955  192.168.2.99  192.168.2.100 TCP  4799 > http
[SYN] Seq=0 Ack=0 Win=25200 Len=0 MSS=1260
 92 255.114585  192.168.2.99  192.168.2.100 TCP  4799 > http
[ACK] Seq=1 Ack=1 Win=25200 Len=0
 93 255.120822  192.168.2.99  192.168.2.100 TCP  4799 > http
[RST] Seq=1 Ack=1 Win=0 Len=0
```

Evidence: UDP scan yielded no results.

Findings: Results indicate that all outbound traffic is dropped except, HTTP, HTTPS, SMTP (only from 192.168.1.100), FTP and DNS queries, in accordance with the security policy.

Number 9

Description: Secure access to administrative tools.

Reference: SANS Track 7 course materials
Rick Yuen

Risk: Vulnerability: Without secure access to the firewall configuration utility the administrative traffic is vulnerable to eavesdropping. Enabling a person with access to a packet sniffer to capture passwords passed over the network in clear text.
Degree of exposure: High
Severity of Loss: High

Test Procedure: Review firewall configuration. SSH command should be present only allowing access from authorized IP addresses:
Example: `SSH 192.168.1.100 255.255.255.255 inside`
Executing the following command will ensure that rsa keys used in the SSH authentication and encryption have been generated.
`Sh ca mypubkey rsa`

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Objectivity: Objective

Evidence: Running "sh config" reveals that the following command is `present "ssh 192.168.1.87 255.255.255.255 inside"`. Also running `"sh ca mypubkey rsa` indicates that the encryption key was `generated"`. `Key pair was generated at: 20:51:46 UTC Jan 5 2004"`

Findings: The firewall is properly configured to allow secure shell access to the administrative console.

Number 10

Description: Ensure logging is enabled and data is being sent to a syslog server.

Reference: Guide to Cisco PIX, Page 290

Risk: Vulnerability
Degree of exposure
Severity of Loss

Test Procedure: Review Firewall config, the following commands should be present.
`Logging on`
`Logging host <interface> <syslog_server_IP>`
`Logging trap <level>` (level should be set to a minimum of 4 (Warning Condition). Once proper logging configuration is verified on the PIX, the administrator should be able to demonstrate that the syslog server is operational and receiving messages.

Objectivity: Objective

Evidence: Review of configuration reveals that logging is not enabled. The firewall administrator also does not have a syslog server running on the network.

Findings: No logging of any type is enabled. The firewall does not comply with this item on the checklist.

Number 11

Description: Change management.

Reference: SANS track 7 courseware.

Risk: Vulnerability: Undocumented or unauthorized changes are made to the firewall configuration.
Degree of exposure: High

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Severity of Loss: High, misconfiguration of the firewall could lead to unavailability of resources or a heightened degree of exposure to other threats.

Test Procedure: Review the change control policy and procedures, as well as the change control logs.

Objectivity: Objective

Evidence: Reviewed change control policy and logs.

Findings: There is no change control policy and the logs consist of a configuration file before the change was made and a configuration file after the change was made. It was not clear from the documentation provided if the configuration files accounted for all configuration changes or not. There was also no documentation as to what configuration changes were made short of comparing the two files.

Number 12

Description: Utilization of DMZ (demilitarized zone, or screened network) to host Internet accessible servers.

Reference: Naidu, page 4
Spitzner, page 2

Risk: Vulnerability: If a host that is accessible from the Internet becomes compromised, it could be used to launch attacks against other hosts on the same network.
Degree of exposure: High
Severity of Loss: High; a compromised host on the internal network could lead to the comprise of all data and hosts on the internal network.

Test Procedure:

3. Visually inspect hardware; configuration should include at least a third network interface to host the DMZ.
4. There should be no static mappings that map outside IP addresses to inside IP addresses. For example, the first two commands below map an outside IP to an inside IP. Then allows www traffic to the inside IP address. Instead of directing www traffic to a host on the inside network as the first two commands do we should see commands like the second two that direct www traffic to the DMZ.

```
static (inside,outside) "outside IP" "inside IP" netmask
255.255.255.255 0 0
access-list acl_outside permit tcp any host "Inside IP" eq www
```


© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

```
static (DMZ,outside) "outside IP" "DMZ IP" netmask
255.255.255.255 0 0
access-list acl_DMZ permit tcp any host "DMZ IP" eq www
```

Objectivity: Objective

Evidence: A physical inspection of the hardware indicates that the device is configured with only two network interface cards. Also, as shown below, inbound access lists direct traffic to the inside address 192.168.1.99.

```
static (inside,outside) 192.168.2.99 192.168.1.100 netmask
255.255.255.255 0 0
access-list aclinbound permit tcp any host 192.168.2.99 eq smtp
access-list aclinbound permit tcp any host 192.168.2.99 eq www
access-list aclinbound permit tcp any host 192.168.2.99 eq ftp
```

Findings: A DMZ is not being utilized.

Audit Report

Summary

This audit was done at the request of National Engineering in order to determine how effectively the PIX firewall is protecting the company's information assets. When National Engineering contracted to have the firewall installed, the technician installed and configured the device leaving the administrator with very little training. This has left the administrator, as well as management, a little uneasy about how effective the firewall is.

The audit was successfully performed and it was determined that the firewall as it is currently configured adequately protects the information assets of National Engineering . However, there are two short comings that need immediate attention; logging, and change management.

Findings

1. Item number 1: Physical security. The firewall has been adequately secured physically. This will greatly reduce the risk of theft, damage or tampering.

2. Items 3 and 4: Cisco advisories. The audit subject is not running the latest software revision. While it is recommended that the software be upgraded, this does not present a serious security risk because the only vulnerabilities found in the 6.3(1) version referenced in item number 2 does not affect this particular system because it has not been configured in such a way that it is vulnerable to the current Cisco advisories.

3. Items 5-8, TCP and UDP port scans: Port scans were performed from the inside and the outside to determine if the firewall would allow unauthorized packets through. It was

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

determined that only expected traffic traversed the firewall and it was not vulnerable to spoofed packets.

4. Item 9: Management access. Item 9 considers how the administrator accesses the firewall for management. This is done either through SSH or the console port. Very good.
5. Item 10 determines how logging is accomplished. This test failed because there is no logging enabled. Because there is no logging enabled the administrator is receiving no feedback about how the firewall is operating and no way to determine if attacks, successful or not, are being performed.

6. Item 11: Change management. No real change management is being performed. Only a snapshot of the before and after configuration is being created. This does allow the administrator to easily revert back to a working configuration if a change is implemented that breaks the firewall. Unfortunately this does not create a log of what changes were made and when and what desired effect the change would have on the firewall configuration. There is also no approval process for firewall changes. This leaves the administrator with the full responsibility for changes that create vulnerabilities.

7. Item 12: DMZ configuration the hardware is not configured with enough network interface cards to have a DMZ network. It was obvious then that the rule base would reveal static mappings and access lists that direct traffic to the inside network.

Recommendations

Logging

- Because there is no logging enabled, the administrator has no idea if there are any problems with the firewall and no information to look back on when trying to solve problems. The administrator should install a syslog server and configure the firewall rules to log every rule match.
- Costs: $100-1500. The basic Kiwi Syslog server is free while a more advanced version can be purchased for $99.00. Kiwi does not need a very powerful computer, but if an excess workstation is not available a new workstation and operating system can be purchased for $1,000-$1,500.
- Compensating controls. If setting up a Syslog server is not feasible because of cost or time, console logging should be enabled and the console monitored several times a day.

Change management

- A change management policy and procedure should be put in place. This policy should include a log of what changes were made, by whom, and what desired effect the change

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

is expected to have. The policy should also include an approval process that each change should go through before implementation. This will not only allow the administrator to track changes and the effect they have on the security of the device, it will also add at least one more set of eyes. This will reduce the risk of inadvertently making a change that undermines the security of the device, as well as relieving the administrator of some of the responsibility of misconfiguration. The current practice of creating a before and after snapshot of the configuration should not be discontinued, but be integrated into the formal policy.

- Cost: The cost of implementing a change management policy is small. A few hours to write the policy and set up the procedure, plus a small amount of time to have changes approved through another person or committee.

- Compensating Controls: In the absence of an official policy and procedure, the administrator should at least create a log to track changes in addition to the current practice of creating before and after snapshots of the configuration. It would also be wise to at least run configuration changes past a college just to ensure that the change is appropriate.

DMZ

- Currently the PIX is configured to allow SMTP, HTTP, HTTPS, and FTP traffic from the outside network to selected hosts on the inside network. As configured the traffic is limited just those protocols, but a new vulnerability found in one of those protocols could leave not only that particular host vulnerable, but other internal hosts as well. Implementing a DMZ and allowing external host access only to the DMZ network would improve the security of the internal network.

- Cost: An additional Ethernet interface card costs approximately $150.00. In addition to the interface card a hub or switch would need to be needed. An Ethernet switch will cost between $100 and $1,000 depending on brand preference and whether switch management is needed. 2-4 hours would also need to be allocated to perform the installation and reconfiguration of the rule base and server.

- Compensating controls: None, compensating controls would be strict firewall rules allowing access to internal servers from the outside. These compensating controls are already in place.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

1. Yuen, Rick W. Auditing a Cisco PIX Firewall: An Auditor Perspective. April 15, 2003. http://www.giac.org/practical/GSNA/Rick_Yuen_GSNA.pdf.

2. Boldewin, Frank. Secure Firewall using Cisco PIX Version 5.3(2). http://www.securityfocus.com/guest/6811.

3. Naidu, Krishni. Firewall Checklist. http://www.sans.org/score/firewallchecklist.php.

4. NIST. Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology Special Publication 800-30 Rev A, Gary Stoneburner, Alice Goguen, and Alexis Feringa. http://csrc.nist.gov/publications/drafts.html#SP80027-RevA.

5. Cisco. Cisco PIX Firewall and VPN Configuration Guide, Cisco Systems. http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_configuration_guide_book09186a0080172852.html.

6. Spitzner, Lance. Auditing Your Firewall Setup. http://www.spitzner.net.

7. Osipov, Vitalya et al. Security Specialist's Guide to PIX Firewalls. Syngress Publishing Inc. 2002.

8. Deal, Richard A. Cisco PIX Firewalls. McGraw Hill/Osborne, 2002.

9. Chris Brenton. What is Egress Filtering and How Can I Implement It? http://www.sans.org/rr/papers/21/1059.pdf.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.