GIAC
CERTIFICATIONS

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.

Auditing the Cisco PIX Firewall

GSNA Practical Assignment
Version 1.2

Jon Bolden
December 2001

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Foreword

In today's world of high technology eSolutions companies have leveraged their data networks to conduct business with their client base. This allows them to combine the high power of production, accounting, product replenishment and billing systems to interact in the area of conducting business. Everything from sales contact, product information and direct product sales were made available to the public with a simple connection to that magical medium that brought the world within reach, the Internet.

During the early years of this type of business model companies were mainly concerned with the ability to conduct business transactions or display related marketing materials with data security being of secondary concern if at all. With the rapid increase in technology the limits to this new way of conducting business seemed endless. While this statement may be true, what happened in the years to come was the realization that now the opportunity for malicious conduct was now becoming an increasing threat. A new term describing those who would dare to use this marvel in technology for illegitimate reasons was born, "hackers."

As time passed the need for security on these data networks was now becoming a business requirement. No more could companies endure the embarrassment or loss of assets that came from being hacked. Enter the firewall. Firewall, yes they vaguely remember hearing of this device that would save their networks, their business and their reputations. Just purchase and install right? This will keep us safe from those evildoers called "hackers."

We are well aware of the answer to the question above. Simply procuring equipment with the word security on its label or in its marketing slick does not secure a network. This paper will cover the topics of how to audit a firewall and then using the identified process, to verify the level of security it provides.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Contents:

Auditing the Cisco PIX Firewall 1
Foreword 2
Contents: 3
Part 1: Research in Audit, Measurement Practice and Control 4
Current State of Practice 4
Security Philosophy 4
Security Environment Questions 5
PIX Firewall Security Checklist 5
Objective Measurements 6
Subjective Measurements 7
Security Tools and Technology 9
Physical Security 9
Performance and Fault Management: 10
Part 2: Application of Audit Techniques to a Real World System 11
Audit Focus 11
Establishing the Security Philosophy 12
Security Environment 13
Firewall Checklist 14
System Evaluation 18
Audit Evaluation 22
Definitions 24
References 25

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Part 1: Research in Audit, Measurement Practice and Control

CURRENT STATE OF PRACTICE

At the time of this writing there are numerous philosophies and practices related to auditing firewalls. As this paper is focused on the Cisco PIX firewall in particular, ideas, practices and philosophies have been drawn from several resources. These resources include Cisco Systems Increasing Security on IP Networks Guide, CERT, security assessment practices developed by Quest and my own personal experience in auditing PIX firewalls amongst various other perimeter devices.

The term "firewall audit" is somewhat misleading as it infers that a single box is the target of the review. In order to conduct a comprehensive review, a broader focus must be embraced[1]. This is true in the sense that if we look directly at a firewall and its configuration we have a list of rules that will be carried out by the device. To identify if a firewall is working properly we must first identify what it is that a company is trying to accomplish. I have found through my experience that by identifying their philosophy as it relates to security and identifying the assets that are being protected, only then can we make a judgement regarding the effectiveness of their firewall.

From these sources, the main focus for auditing these devises is based on a company's security policy. The policies are responsible for defining what resources may be accessed by who and when. Once their security philosophy is identified the next step is to make sure that philosophy is reflected in their security policy. It is in this scenario that the company resources are best secured.

SECURITY PHILOSOPHY

A company's security philosophy although subjective will often dictate the level of security that company sees as required. Answering the following questions will help identify the organization's security philosophy.

- How important is the public image of the company in meeting its business objectives?
- Has the company suffered negative publicity as a result of security issues?
- How critical are data integrity, privacy and availability to the overall operation of the company?
- What are the company's internal users' understanding and concerns with data security?
- Are there security guidelines, regulations, or laws the company is required to follow? If so, does the company make an effort to meet these guidelines and rules?

[1] Cryptography and Network Security, William Stallings, 1998

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Do the company's business requirements take precedence over security where there is a conflict? If so, is this the right direction going forward?

- How much downtime or monetary loss has the company incurred due to security incidents in the past?
- Is management concerned about insider threats? Should internal users be trusted?
- What do internal users expect in the way of system security controls and procedures?
- Is remote access critical to meeting business objectives?
- How much sensitive information is on-line? What is the impact if this information is compromised or stolen?
- Does the company perceive a need for different levels of security in different parts of the organization?

SECURITY ENVIRONMENT QUESTIONS

- Has a security risk assessment been conducted to identify company assets?
- Does the company have a current security policy?
  If so, does the company's security policy address the protection of these assets?
  If not, has the purpose or role of the company firewall been defined?

PIX FIREWALL SECURITY CHECKLIST

The following is a security checklist derived from several sources as well as personal experience in conducting security audits. With this list, the state of security will be discovered by interviewing key personnel, reviewing existing policy and verifying the PIX firewall configuration against the company's security policy.

After the configurations have been verified as accurate they will be tested by a three-step process. First, the network tool Nmap will be used to test for the available hosts on the network. This is done from a security workstation running the Nmap application accessing the target network from the Internet. The following command will produce the results we are looking for: nmap –p 1-1024 –I –O –sR *network*

After the Nmap application completes its mapping of the available hosts on the network we will use the output to create a seed file. That seed file will be used as the target selection for the next security tool to be used, Nessus. Nessus is an application used to discover security threats on a network by probing the services offered by the network servers. This scanner is not limited to well known services but rather targets a system by performing a full TCP/UDP probe. As services are discovered, they are then individually tested for vulnerabilities by exercising destructive or non-destructive exploits against each service. This will verify that the PIX is filtering down to layer 4 on the protected servers and applications.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Once the Nessus process has been completed, it's time to move on to the third part of the process. It is here that each application is tested from a source that must pass through the firewall to not only verify what services or applications have been filtered but the successful operation of the services published for exterior use.

Configuration Audit Item	Yes/No	Pass/Fail
Telnet Access Allowed		
Telnet Access Restricted		
Secure Shell Configured		
Strong Passwords Used		
Access Control Lists used		
Access Control Lists/Conduits properly configured		
Access Control Lists/Conduits optimized for performance		
Access Control Lists/Conduits organized		
Static Addresses defined correctly		
Audit logging enabled		
Mail Guard Configured		
Addresses restricted as per company policy		
Services restricted as per company policy		
RIP used to populate routing table		
Security assignments on interfaces correct		
PIX Firewall configured for SNMP		
PIX Code at current revision level		

OBJECTIVE MEASUREMENTS

When auditing a Cisco PIX firewall there are several areas that are black and white in respect to declaring them right or wrong. These measurements are based on accepted best practices throughout the security community and are judged on an objective scale. Below are listed the objective measurements of the firewall audit.

Passwords: Passwords should contain at least 6 characters and have a combination of letters and numbers, uppercase and lowercase. Passwords should not resemble any word, name, idea, or concept that might appear in any dictionary anywhere in the world. A good example: **jY2Ehxqy**. Passwords not conforming to these minimum requirements would be out of spec.

Access Control Lists / Conduits: When configuring the PIX firewall to restrict addresses, both internal and external, the Access Control Lists or conduits must be configured correctly to include host IP addresses, ranges and masks. Access Control Lists that have incorrect parameters such as the above mentioned address and masks or data direction are considered out of spec.

Static IP Addresses: When using NAT in a PIX firewall configuration static IP addresses must be configured to match the outside public IP addresses with the inside

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

private IP addresses. Incorrect syntax here brings inoperative behavior and will result in an outcome that will be considered out of spec.

IP Address Restrictions: In accordance to company security policy, IP addresses will either be allowed or denied through a firewall. These restrictions specify what source address may contact what destination address and what the data direction will be. Once configured these IP addresses can be checked with tools such as Nessus and Nmap. The grading here is base on whether or not these tools can in fact be used to access the appropriate IP addresses tested in both data directions. If there is a breech or inconsistency with policy, the system will be considered out of spec.

Service Restrictions: In accordance to the company security policy, services will be restricted by the firewall. This will be done by utilizing UDP and TCP port assignments within the filters associated with the IP addresses. Any IP address configured in the firewall ruleset that is not restricted to the port level will be rated out of spec.

RIP: The Cisco PIX has the capability to populate its routing table using the RIP protocol. This is used only to build local routing tables as the PIX does not advertise routes to any other device using the RIP protocol. The danger here is that RIP packets can be manufactured to corrupt the PIX routing table. If there is no device specifically configured to pass RIP information to the PIX firewall, and the PIX has RIP enabled, it will be rated out of spec.

Interface Security Levels: The Cisco PIX makes decisions based on the security level assigned to an interface. This affects the filter mechanism as well as NAT and must be configured correctly for the PIX to function properly. The proper configuration is for the highest security level to be applied to the outside (i.e. Internet) interface of the PIX, the lowest to the inside (private) interface and any DMZ zones shall be configured in between. If this rule is not followed, the firewall shall be rated out of spec.

SUBJECTIVE MEASUREMENTS

In our checklist for the Cisco PIX firewall there are several items in which the measurement is not necessary right or wrong but instead subjected to best practices. That is to say that a particular configuration or placement practice may depend on the environment in which the firewall exists. These measurements are as follows:

Access Method: How is the PIX firewall accessed (i.e. telnet, secure shell, CSPM[1], etc.)? In this question we are auditing the access method to the PIX firewall. If the administration environment is trusted, telnet may be considered an appropriate access method. However, where telnet is used to connect to a PIX firewall, the source IP address for administration should be defined to restrict which workstations may be used for administrative purposes. When dealing with an unknown environment, access methods such as secure shell should be used to eliminate the transmission of information in clear text when administering the firewall.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Access Control Lists Used: The use of Access Control Lists or ACLs is the preferred method for configuring filters on the PIX firewall. In addition to ACLs, Conduits are also used in PIX configurations. However, as the PIX OS evolves, Conduits will be phased out as a configuration option. This is due to the current management platforms that are being released by Cisco Systems to configure and maintain PIX firewalls. Access Control Lists also offer bi-directional filtering and may be applied to any PIX interface as to where Conduits can not.

Audit Logging: The logging command lets you enable or disable sending informational messages to the console, to a syslog server, or to an SNMP server. In a best case scenario, the logging would be sent to a network management device where it could saved for review and forensic purposes. At the least, logging should be buffered on the PIX firewall to present some sort of record for current events. Having neither of these logging functions configured would result in and outcome of out of spec.

PIX Mail Guard: The fixup protocol commands let you view, change, enable, or disable the use of a through the PIX Firewall. The PIX Firewall's Mail Guard feature removes the need for an external mail relay in the perimeter or DMZ network[1]. Mail Guard, by design, only allows seven SMTP commands. The commands are HELO, MAIL, RCPT, DATA, RSET, NOOP and Quit. This configuration is necessary only when there is no external mail relay present in a network configuration. If the is no relay and the Mail Guard is not configured, the system shall be rated out of spec.

SNMP Configuration: The PIX firewall is equipped with basic SNMP capabilities. There can only be a read community set and basic contact information, etc. can be configured. If the client has no SNMP management station the string definitions should be omitted but there is nothing wrong with having the contact information present if it is used for some purpose as configuration tracking (last updated by). If there is no SNMP manager present and the system is fully configured, it shall be rated out of spec.

PIX OS Revision Level: The Cisco PIX firewall is a device that requires an operating system. Like all operating systems there are upgrades, patches, new features, etc. offered as time goes on. It is especially important in the security field to keep the latest code revisions loaded on the networking equipment. With new revisions come patches that may make the firewall stronger against newly developed security threats or enhance its ability to defend the devices and services within a network.

To determine the OS revision level of the PIX firewall one must first access the device either by telnet or console connection. At that point, access must be secured in user mode to issue the following command: show version. The output will display the hardware model, available memory, enhanced features and the OS revision level as can be seen in Figure 1. After the OS revision level is determined it can be compared to the latest major software release number. The latest PIX OS major revision level is version 6.1.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Figure 1

```
Telnet - 10.2.1.2
Connect  Edit  Terminal  Help
pixfirewall# show version

PIX Version 4.2(4)
Compiled on Wed 03-Mar-99 16:20 by pixbuild

pixfirewall up 23 days 15 hours

Hardware:   TC430HX, 8 MB RAM, CPU Pentium 133 MHz
Flash atmel @ base 0x300
0: ethernet0: address is 00a0.c986.0365, irq 10
1: ethernet1: address is 00a0.c925.3eee, irq 9
2: ethernet2: address is 00a0.c922.a412, irq 10
Serial Number:  6004700
pixfirewall#
```

When determining whether or not a system is in spec based on its OS revision level there must be several items taken into concern. First, what is the security philosophy of the owner? Second, is there a reason the current revision puts the company or its assets at risk? And finally, can the current hardware platform support the OS upgrade requirements? If these questions are answered satisfactorily, the PIX firewall may be rated as within spec even if the revision level is behind.

Security Tools and Technology

Security tools and technology, when combined with effective Security Management, Policies, and Processes will provide a comprehensive IT Infrastructure approach. The integrity and privacy of data communications is dependent on having the proper external and internal data access controls, monitoring and management tools in place. Such tools and technologies include firewalls, VPNs, access control lists, authentication, intrusion detection, fault and performance management, anti-virus control and content filtering. These tools and technologies will be listed in this audit as either existent or non-existent.

Physical Security

It is a given in firewall security if the system itself is not physically secure, nothing else about the system can be considered secure. With physical access to a machine, an intruder can halt the machine, bring it back up in privileged mode, replace or alter the configuration, or take any number of other undesirable (and hard to prevent) actions.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

[1] Managing Cisco Network Security, Chapter 10, Page 366

PERFORMANCE AND FAULT MANAGEMENT:

In addition to a firewall, it is strongly recommended that IT investigate tools that will support a greater level of proactive security and operations management. The ability to be proactive in IT is another commonly identified concern in the interviews of various IT management and staff. Infrastructure Performance and Fault Management tools provide the IT organizations with the low-level visibility they need to become more proactive in their approach to identifying, isolating and resolving security and operational issues.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

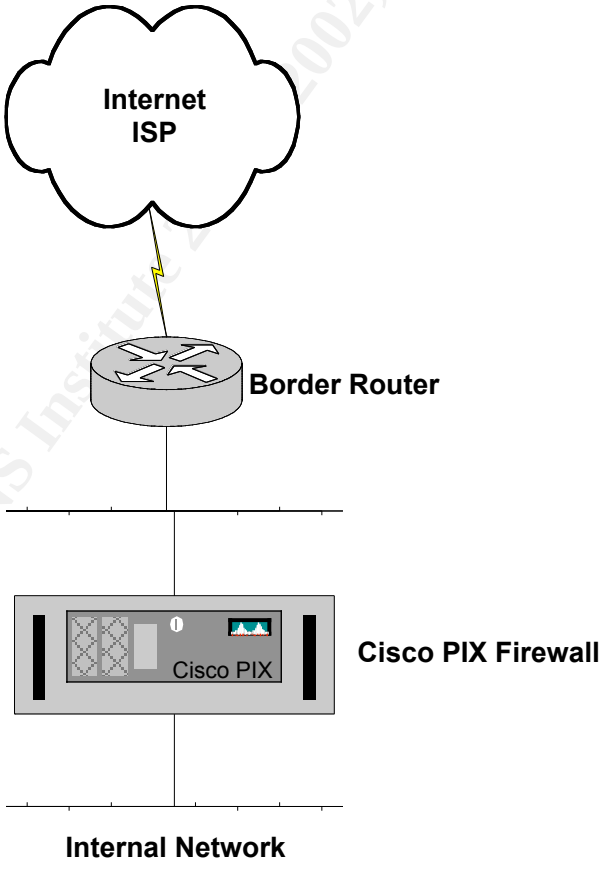
Part 2: Application of Audit Techniques to a Real World System

AUDIT FOCUS

This audit will be focused on a Cisco PIX firewall model 515 running PIX OS version 4.2.(4). The PIX is installed and configured as the primary perimeter defense device on the Internet border of a moderate sized business network. As can be seen in Figure 1 there is a CPE router in-line between the PIX and the Internet but it does not screen any packets before entry into the Cisco PIX firewall. The client's public Internet services are housed on the internal network and their addresses translated by the Cisco PIX firewall for access. These services are Internet email, Citrix Metaframe, WWW and a small range of extranet applications connecting to a single host.

During the audit attention will be focused on the firewall itself to evaluate its configuration to provide the services outlined above. Although there are several configuration modifications that should be made to the border router to activate it as a basic screening device, that is outside the scope of this document and will not be addressed herein.

Figure 1



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

ESTABLISHING THE SECURITY PHILOSOPHY

In order to aid with the subjective ratings of this audit, it was first important to ascertain the current security philosophy of the organization. Interviews were conducted with the key stakeholders in the security of the IT infrastructure as well as the business assets of the organization using the questioning outlined in Part I of this document. The outcome of those interviews is summarized below.

Company staff is very concerned with its public image in the marketplace today. When asked about the impact of a security breech such as a web server defacement, the overwhelming consensus is that it would be disastrous. This implies the security to the public access points such as www and email is critical.

When asked if the company had ever suffered a loss that can be attributed to an electronic security breech the answer was yes. At a point early last year one of the servers had been exploited and configured as an FTP site to be used for game distribution. The hackers, while using this server, had eliminated some of the company's archived data in order to free up disk resources for additional storage of non-company information. In addition to the data loss, the company's available bandwidth was depleted as the hackers transported their data. As we will be stated later in the document there is no logging or intrusion detection in place. This helped the auditor to determine the level of concern and commitment in regard to security.

As for the importance of the company's data and its integrity, the most important areas here were defined as the company's client list, accounting systems and their inventory logs. For the most part these systems are not accessible to the public with the exception of the automated ordering system. These systems are however, on the same network as the Internet reachable devices and need to be protected from exploitation.

At this time the company is not aware of any legal requirements for security. As they are not a government agency, medical institution or a financial organization there were no requirements found.

When it comes to providing required connectivity to drive their business security often takes a back seat. The state of mind is that the business operations must be addressed first and after they are established security is put in place. This concerns the IT personnel in the organization as security is not given the priority they feel it deserves once a new system has been put into production. With no policy to guide them, obtaining budget dollars to secure new systems is a hit and miss exercise at best.

The interviewees all agreed that insider access was not a problem. The organization currently has a philosophy of equal access with regards to corporate information save personal correspondence and email. Again with no policy in place they were unaware of how they might ensure that private information is not transmitted off premises.

The internal users of this company like so many others are not comfortable with extensive security measures. While they seems to be aware of the importance of the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

company's information they desire ease of use accommodations such as single sign-on. This is the current practice in place and there are no plans or requirements at this time for change.

The company does require remote access for its sales staff to conduct business outside of the immediate area. This however is not a function of the firewall and has been addressed via a VPN solution.

When asked about the sensitivity of on-line information all interviewees agreed that the above mentioned areas or accounting, inventory and client listings are extremely valuable to them. This information is seen as the company crown jewels and would cause extreme disruption in their current business practices should it be lost. It was their feeling that this is where their main focus on security should rest.

Upon the completion of the interviews it was clear that this organization has a moderate to high dependency on their security. They also believe for the most part that they are secure from a network infrastructure point of view and need to devote additional resources to host based systems. The over all philosophy of the company is that security is very important to them and that their IT organization should be dedicating 30 percent of their budget and 15 percent of their time towards security. They are also aware that this is not the current practice and need to perform additional studies to discover what changes are required to make it so.

SECURITY ENVIRONMENT

While conducting this audit it was discovered immediately that there is no security policy currently in affect. Several of the key stakeholders have some conceptual ideas on how security should be implemented and maintained but there is no formal guideline in place.

In addition to the lack of a security policy, no formal risk assessment has ever been conducted. There are thoughts throughout the organization that consider one thing or another to be important to keep intact while conducting business but, again there has been no formal assessment to establish the exact impact of loosing either equipment or information.

In the absence of a formal security policy the company currently relies on their current firewall ruleset. The current configuration represents the network connectivity requirements at a host level. They have not at this time locked access down to specific hosts, protocols and ports. At this time the company believes, that IT should be responsible for all policy and implementation. IT is not prepared with the current business and application requirements to carry out this assignment resulting in an impasse with a best effort attempt at securing the network.

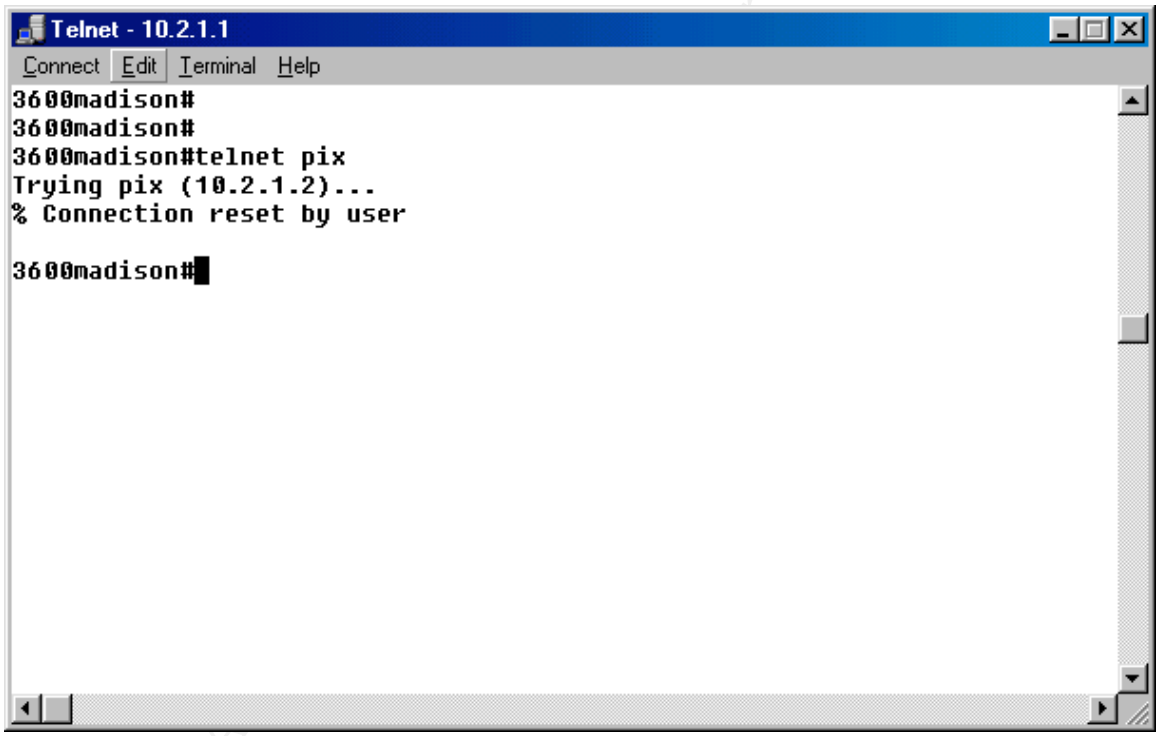
© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

FIREWALL CHECKLIST

Telnet Access Allowed: **Yes** **Pass**
Telnet access is allowed to the PIX firewall. Configured on default TCP port 23 with password protection. This is the primary method of administration for the firewall.

Telnet Access Restricted: **Yes** **Pass**
Configured telnet access for the PIX firewall is restricted to five administration workstations. All five workstations were accounted for during the audit and telnet access confirmed by issuing the command from each station. Access was attempted from several other devices on the network all resulting in a failed connection caused by the PIX as can be seen in figure 2.

Figure 2

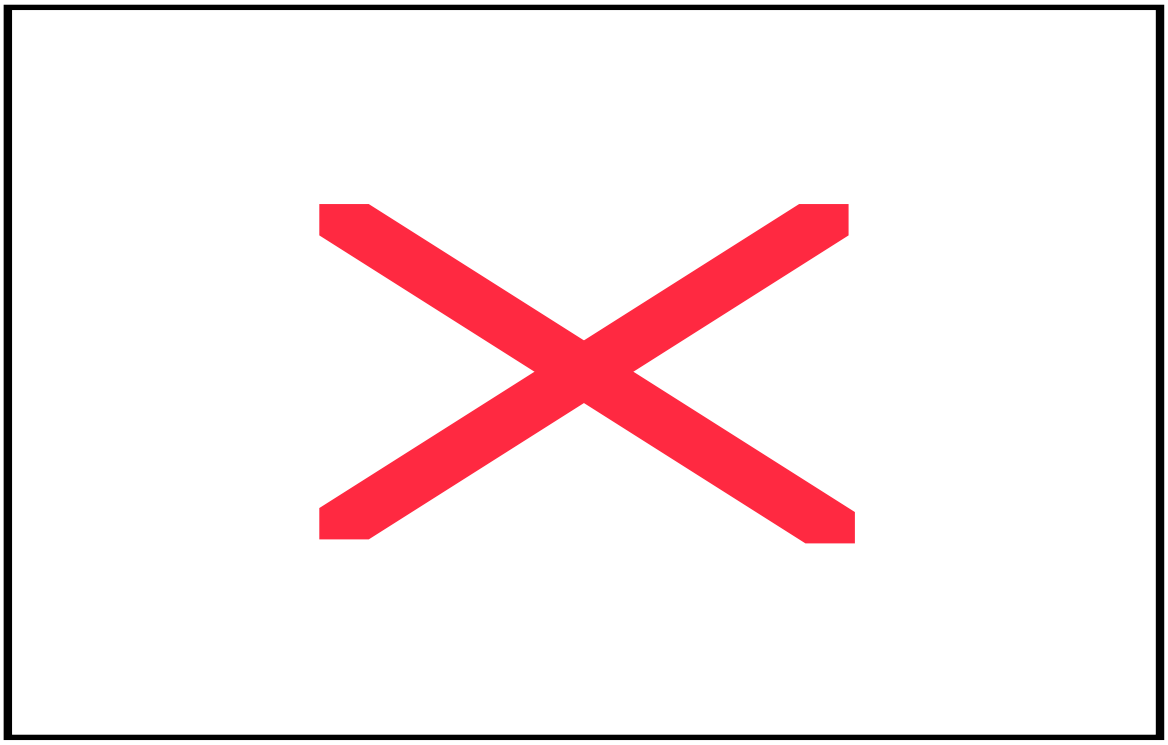


© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Access Control Lists Used: **No** **Pass**
Access Control Lists are not used in the company's PIX configuration. In their place, Conduits are used as the method for configuring inbound access filters. Even though ACLs are not used here the device receives a pass rating due to the fact that the current PIX OS used by the company does not provide for the use of ACLs. In addition to that, the company is not using Cisco Systems' management platform.

Access Control Lists / Conduits Configured Correctly: **Yes** **Pass**
As can be seen below in Figure 3 the Conduits are configured correctly based on syntax. To further evaluate this configuration the required publicly accessible devices were accounted for as well as the services they provide and matched against the configured conduits. The next step was to test the firewall's configured functionality by using a combination of tools and methods. First, Nmap was used to verify the static statements and reachability of the devices behind the PIX firewall. Next, Nessus was used as an extension to Nmap by testing for exploits on the firewall as well as through it. Finally the devices were tested by outside application connections. The results can be seen in table 2.

Figure 3



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Table 2

Host	Found by Nmap	Nessus Scan	Application Testing
XXX.4X.162.1	Yes	TCP 79 TCP 90 TCP 91 TCP 92	Router
XXX.4X.162.3	Yes	TCP 23 UDP 53/TCP53 TCP 113 TCP 515	Name Server/Zone Transfer
XXX.4X.162.4	Yes	TCP 23 UDP 53/TCP53 TCP 113 TCP 515	Name Server/ Zone Transfer
XXX.4X.162.5	Yes	ICMP	PIX
XXX.4X.162.35	Yes	TCP 25 TCP 110	Email: SMTP/POP3
XXX.4X.162.37	Yes	TCP 80 TCP 443 TCP1394	Metaframe Server
XXX.4X.162.70	Yes	TCP 80 TCP 443	WWW
XXX.4X.162.71	Yes	TCP 80 TCP 443	WWW

```
Nessus Scan Report
------------------

SUMMARY

 - Number of hosts which were alive during the test : 8
 - Number of security holes found : 5
 - Number of security warnings found : 7
 - Number of security notes found : 12



TESTED HOSTS

 208.44.162.1 (Security warnings found)
 208.44.162.3 (Security holes found)
 208.44.162.4 (Security holes found)
 208.44.162.5 (Security holes found)
 208.44.162.35 (Security warnings found)
 208.44.162.37 (Security warnings found)
 208.44.162.70 (Security warnings found)
 208.44.162.71(Security warnings found)
```

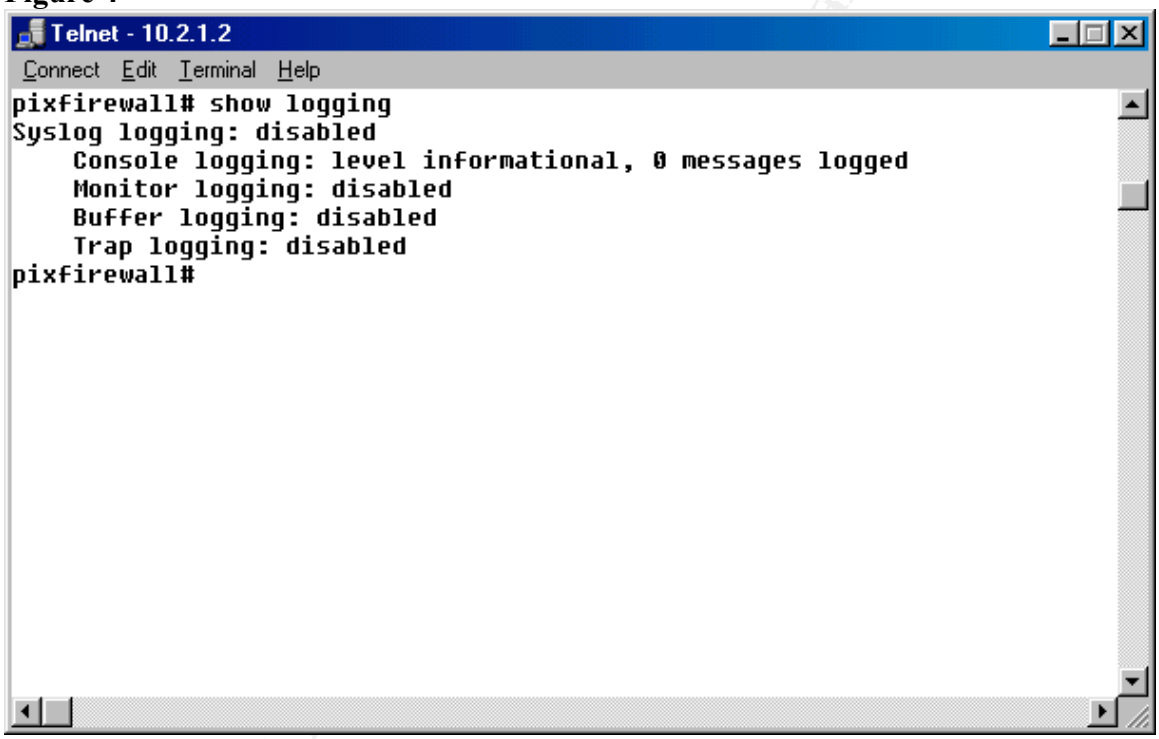

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Audit Logging Enabled: **No** **Fail**

Audit logging on the company's PIX firewall was not enabled. This eliminates any audit trail of activities that may have occurred that are not business related. There are no timed events or record of any debug messages that would aid in any incident response exorcise. Also, while the company is employing HP Openview as a trap management and notification platform, it can be seen from the configuration commands below that traps are not sent or recorded. The logging settings can be seen in Figure 4.

no logging on
no snmp-server enable traps

Figure 4

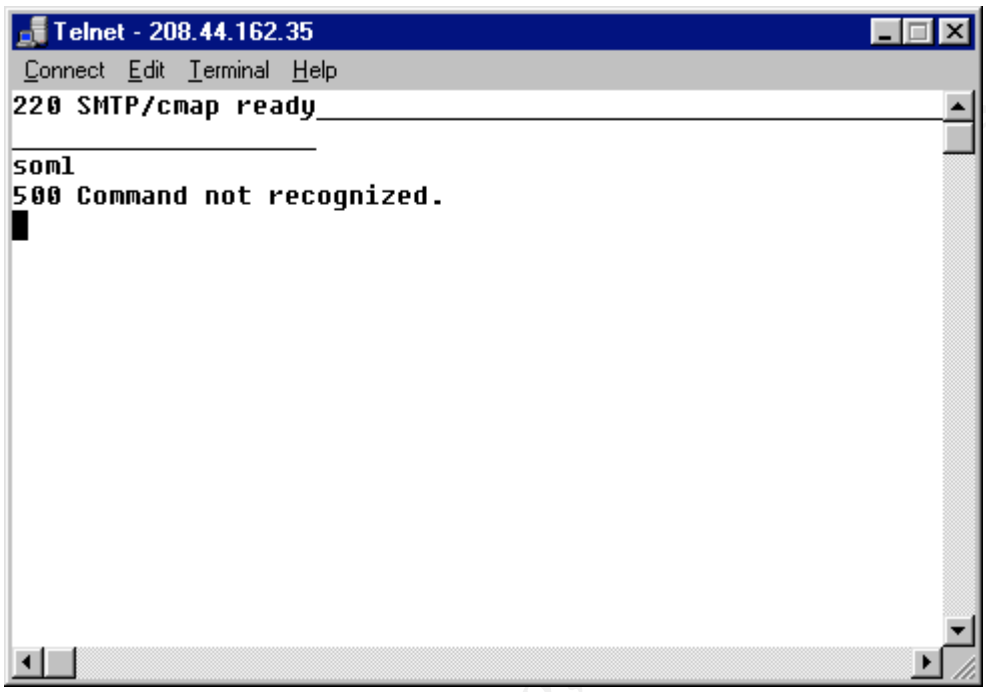


PIX Mail Guard Configured: **Yes** **Pass**

Fixup protocols were configured on the PIX firewall for the default services on the default ports. This includes the command "fixup protocol smtp 25" which was present in the PIX configuration. In this particular environment this command is a necessity due to the fact the mail exchanger is located on the private side of the network with no external SMTP relay. Without the Mail Guard feature configured here, all SMTP commands are available to the remote user and can be used to exploit a weakness in the mail system. This configuration was verified by accessing the mail exchanger from a remote location and issuing the SMTP command "soml". As can be seen in Figure 5, the PIX issued a "500 Command not recognized" error.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Figure 5



RIP Configured: No Pass

To determine the status of the PIX firewall in regards to its RIP configuration the configuration itself was reviewed. Also the routing table was review to ensure that all routes were derived from static statements within the configuration. There was no need for the PIX to learn its routes from exterior devices in the current environment deeming that the current routing configuration was accurate. To test the configuration a Cisco 2514 router was placed first on the internal network and then on the external network to broadcast RIP routing updates. At no time were the routes learned by the PIX firewall.

PIX OS Revision Level: Behind Fail

As can be seen from Part I, Figure 1, the PIX firewall is running OS level 4.2.(4). This is two major revisions behind the current version of 6.1.X. With the identified security philosophy of the company, this is not acceptable. There are approximately 175 open caveats (according to Cisco TAC) open with release 4.2.(4) with no revision. Also the software is no longer available from Cisco as it has been classified end of life.

SYSTEM EVALUATION

The overall evaluation of the company's PIX firewall and its implementation is average. Of major concern were the lack of a security policy, the OS revision level of the PIX firewall and the current filtering configuration. There is also a lot of opportunity for the company to leverage its security infrastructure by implementing some of the available tools on the market today. The following is a review of the recommended steps to mitigate the vulnerabilities found within the report.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Security Policy
During the interview and discovery process, company management communicated security policy definition is a current effort that was only recently started. Company management indicated that Email, Internet and Telecommuter policy statements were currently in development. However, these policy statements were not provided to the auditor.

The auditor recommends that the company start with a general Security Policy document that covers the protection of all Information Assets and Resources within the company's business facilities. This document should provide company management and staff with an understanding of the security policy, its purpose, guidelines for improving their security practices and definitions of security responsibilities across the company organizational structure. This will also serve to establish the company corporate philosophy on security. The company will need to identify compliance requirements and associated punitive or disciplinary actions against an employee, a business partner or other agency if compliance is not met.

The next step in policy development is the creation of an IT Security Policy. The IT Security Policy must be established to set the framework for how the company will secure its networks, applications, computers and data information. The IT Security policy must be easily understood and supported by both company management and staff. The policy should address threats posed by external and internal sources, while defining the acceptable uses of the corporate IT assets by company employees. Some examples of IT Security Policies are:

- Company Email should be protected by anti-virus software to preclude the introduction of a computer virus on company Email Servers and workstations.
- Firewalls and Content Management software should be installed to control company user access to and from the Internet and block potential intruders.
- Intrusion Detection Systems should be installed to identify external and internal threats to company IT resources before resources are compromised.

These are just a few examples of IT Security Policies that should be reviewed for applicability within the company IT environment.

Security and Operational Procedures
The enforcement of security policies should be driven through clearly defined and communicated procedures that provide detailed, step-by-step guidance for implementing, managing and monitoring security compliance and operational stability. Like policies, procedures need to be continually monitored and periodically audited to ensure that the IT operations and security continues to meet the needs of the business.

Security and Operational Procedures are critical to providing secure, reliable and manageable IT data communications. Documented procedures will create clarity and accountability in IT functions and improve customer service through organized security and operational problem response and resolution. This ultimately facilitates a greater level of alignment between the business and the IT Infrastructure. Typical security and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

operational procedures include incident response, periodic vulnerability assessments, monitoring and logging, security forensics, system backups, change management, outage response and escalation and employee, and contractor termination.

Change Management

Currently, the network team participates in change management discussions. This process is very informal and not currently documented. The network administrators meet prior to making changes and must reach a consensus before those changes are put into production. Since this is an informal process there is no audit trail associated with it. It is completely possible that changes can be made without the proper approvals. The auditor recommends that a Change Management process be developed and implemented for the IT Department as a whole. This process might even include business unit owners for visibility to changes. A change form should be created that identifies the purpose of the change, the personnel involved in the change, the change plan (step-by-step sequence of events), contingency (back-out) plan, departments involved, potential impact to other IT services and an escalation process to manage/communicate any resulting impact. This change form should be completed and submitted by the owner/implementer of the change at least one week prior to the change. A weekly change meeting should occur, with representatives from all IT functions and business units to communicate, validate and approve requested changes. It is typical for a Data Center Operations Manager, or in the company's case, possibly the CIO to chair these change meetings. Additionally, an application such as Tripwire would be extremely helpful in reinforcing the change management process.

PIX Best Practices

This section provides a non-syntax description of commonly used Cisco Pix Firewall IOS configuration commands to provide a best practices approach to Layer 3/4 security and Cisco device access security. Before implementing these recommendations, it is strongly advised that all Cisco IOS command recommendations be reviewed for applicability in the company network environment.

- Allow WWW traffic only to web servers.
- Allow Internet Email (SMTP) only to SMTP server.
- Allow File Transfer Protocol (FTP) only to FTP servers.
- Allow DNS traffic only to DNS servers.
- Filter DNS zones transfers by denying TCP port 53 from the outside to the primary and secondary DNS servers.
- Add access list entries into the Internet border router and firewall to protect against LAND and SMURF attacks.
- Apply the IP reverse path command to protect against DoS attacks.
- Add fragmentation protection to guard against DoS fragmentation attacks.
- Use the username and password along with setting the privilege level to 1.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Physical Security

The company's Physical Access Security was breached multiple times during an alert condition. An engineer, without a badge or escort walked through the lobby of the company's facility, up the elevators, into the offices on the 8th floor and into the Data Room on the 8th floor, multiple times. The engineer was then able to plug a laptop, loaded with a Network Protocol Analyzer into the core switch (Cisco 6500) and capture any and all data that traversed the company backbone network. Console access was also available, unrestricted, to the PIX firewall, 6509 core switch and several routers. This level of physical access violation required the cooperation of multiple company employees. Doors were held open to the 8th floor and the Data Room without any questioning or request for credentials.

Network Design

The company network design is not based on a defined security model. A recommended approach is to define the model, as discussed above, and then define security zones within the network to support varying levels of required security. Network zones should define the classification of services and the required levels of security. The connection protocol and initiation sequence should also be identified by zone. At a minimum, the company should define the network zone security requirements for Internet access, VPN remote access, regional office communication and core network services.

A quad port FE module should be purchased for the Pix Firewall to provide increased Internet access architecture design flexibility. This will effectively support the recommended change in DMZ configuration and facilitate the development of a web DMZ to place all publicly accessible servers.

Intrusion Detection

The implementation of network and host-based intrusion detection is more commonly used in today's security-conscientious IT environments. Hackers are constantly bombarding external network access points looking for firewall, router and system vulnerabilities to exploit. Intrusion detection tools provide real-time notification and blocking of non-desired data communications. I recommends that the company IT investigate the application and need for intrusion detection in the company IT environment. This need came to light as the vulnerability tests were conducted, not one person was aware of what was going on with the network. I was able to drive the T1 line to maximum capacity with a question.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Cost Review:

Cisco PIX Upgrade w/VPN	**$3700.00**
IDS System w/ 2 Probes	**$46000.00**
Labor	**$10000.00**
Total	**$59700.00**

AUDIT EVALUATION

In reviewing the effectiveness of this audit I found that technically the process outlined in Part I was very effective in determining the level of security at the company. The findings were as expected by not only myself but the company that received the audit as well.

I found as I have many times that one of the most critical determinations was that of the security policy of the company audited. There have been audits in the past where companies have been very focussed on security on have made strides to correct every single variance found. On the other hand I have run across companies that have little to know interest in their network security and are mainly concerned with connectivity. The interviews conducted during this audit gave important insight in to what steps lay ahead.

Since the audit was focused directly on a PIX firewall the checklist worked very well. Both objective and subjective topics were covered to reveal the company's security level at the PIX. However, I also see that performing an audit on a single device seems very narrow when looking at the overall picture. In my experience with audits in the past they have not been focussed on a single device but instead several areas. These areas include items such as policy, procedure, border devices, services, etc. In such a narrowly focused exorcise these items are often overlooked and the client is left with a confident feeling of security while he is left wide open to email, www and several hundred other exploits that are not controlled by the firewall alone.

I would never try to base an organization's level of security on any single area audit alone. It is in this arena where I think this audit would fall short in trying to determine the overall security of an organization.

When conducting these audits we are also left to the honesty of the client at times. This would not account for insecure machines taken out of the network for audit day. Change control and daily logs may in fact be for that day only or records manufactured.

Overall I believe the audit served its purpose and the client has a good understanding of where they stand. The audit itself took about 40 hours to conduct with an additional 80 hours of research, data gathering and documentation.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DEFINITIONS

DNS - The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

IDS – Intrusion Detection System. Security service that monitors and analyzes system events for the purpose of finding (and providing real-time or near real-time warning of) attempts to access system resources in an unauthorized manner.

IOS – Available on an extensive range of Cisco platforms, Cisco IOS® Software is a feature-rich, network systems software that provides a common IP fabric, functionality and command-line interface (CLI) across your network.

IP - The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet or over an intranet.

LAN – Local Area Network.

Mbps – Mega Bits per Second.

Network Mapper (nmap) - nmap is one of the premier port scanning tools available. Nmap provides basic TCP and UDP port scanning capabilities. Port scanning is the process of connecting to TCP and UDP ports on target systems to determine what services are running or in LISTENING state. Identifying listening ports is a method of determining the operating system or what applications are in use on a particular host. This information can then be used to manipulate or gain access to the host.

Nessus - Nessus is an application used to discover security threats on a network by probing the services offered by the network servers. This scanner is not limited to well known services but rather targets a system by performing a full TCP/UDP probe. As services are discovered, they are then individually tested for vulnerabilities by exercising non-destructive exploits against each service.

Throughput – The rate at which data is transmitted over a line in relationship to line capacity.

WAN – Wide Area Network.

Zone Transfer (DNS) - The process by which DNS servers interact to maintain and synchronize authoritative name data. When a DNS server is configured as a secondary master for a zone, it periodically queries another DNS server configured as its source for the zone. If the version of the zone kept by the source is different, the secondary master server will pull zone data from its source DNS server to synchronize zone data.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

REFERENCES

1. Hardie, Chris. "Security Audit Checklist" http://www.summersault.com/chris/techno/security/auditlist.html

2. Cisco. "Command Reference" (9/26/2001) http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v42/pix42cfg/pix42cmd. htm

3. Cisco. "Increasing Security on IP Networks" (4/26/2001) http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs003.htm

4. Spitzner, Lance. "Auditing Your Firewall Setup" (12/12/2000) http://www.enteract.com/~lspitz/audit.html

5. Lindstedt, Sandy. "Firewall Audit" (6/15/1999) http://www.theiia.org/itaudit/index.cfm?fuseaction=forum&fid=179

6. Wenstrom, Michael. "Managing Cisco Network Security" 2001
7. Stallings, William. "Cryptography and Network Security" 1998

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.