Center for Internet Security
Benchmark for Cisco Pix

Level 1 and 2 Benchmarks
Version 1.0

http://www.cisecurity.org
rat-feedback@cisecurity.org

September 7, 2004

Abstract

This document defines a set of benchmarks or standards for securing Cisco PIX Firewalls. The benchmark is an industry consensus of current best practices. It lists actions to be taken as well as reasons for those actions. It is intended to provide step-by-step guidance to front line system and network administrators. It may be used manually by itself or in conjunction with automated scoring tools. See Appendix D.2 for terms of use.

Contents

1 Introduction

1.1 How To Get Started Now

There are three ways to use this benchmark:

1. Dive in

   If you are well-versed in Cisco PIX operating system, and fit the other assumptions listed in the next section, and you are a highly skilled security professional confident in your knowledge of the functional/performance consequences of implementing the actions, then you may proceed directly to sections 2 and 3.

2. Slow and steady

   All others are strongly urged to complete the Audit Checklistin Section D and study the warnings and explanations in sections 2 and 3 before implementing any of the actions in sections 2 and 3. Many security actions can disable or otherwise interfere with the function or performance of software on your system, particularly applications. Note also that many of the actions in sections 2 and 3 are conditional. They only apply in certain situations.

3. Use a scoring tool

   The third option is to use a scoring tool. See section B.3 for availability.

1.2 Using This Document

1.2.1 Read This First

Read this section in its entirety. It tells you how to get started quickly using the benchmark to improve the security of your systems. It lists important information and assumptions. Failure to read this section could result in incomplete or incorrect application of the recommendations.

1.2.2 Prerequisites

This benchmark does not assume that any other benchmarks have been previously applied.

1.2.3 Assumptions About The System Environment

This benchmark assumes you are running Cisco PIX software 6.1or later.

1.2.4 Assumptions About The Reader

This benchmark assumes that the person applying the recommendations

- May or may not be an expert in networking or configuring the device.
- Is authorized to log in to the device and enable administrative privileges.
- Is able to enter basic configuration commands.
- Understands the business critical functions of the systems being secured.
- Understands local policies.
- Is capable of evaluating the potential impact of recommended changes on both function and policy.

1.2.5 Benchmark Format

The body of this document consists of the level-1 and level-2 benchmarks.
See B.1 for information on how levels are determined.
Each benchmark item is intended to contain information necessary to allow you to understand what's being recommended and to implement it quickly. Each item will contain a brief **Description** of the action to be taken, the **Action**, which is commands to type, a **Security Impact** section describing the reason for the action, the **Exact Rule** which gives, in most cases, a regular expression listing something that is required or forbidden in the config, an **Applicability** section which contains list of the OS versions and contexts in which the action applies, an **Importance** value reflecting the importance of the item on a 1-10 scale as assigned by the CIS consensus process, an **Rule Group** section showing the groups to which a rule belongs (SNMP, logging...), and a **For more information** section listing references to further information.
As a convenience an "Expanded Audit Checklist" is available at http://www.cisecurity.org/ If you intend to audit more than one device or intend to audit the same device several times, you are encouraged to print and copy this document.

1.2.6 Special Notation

This benchmark uses the following typographical conventions.

- The **Exact Rule** sections list a pattern that is expected (required) to be seen in a configuration file or that is expected not (forbidden) to be in a configuration file. For example `^snmp-server host\s+.*\s+poll` . These rules are Perl regular expressions that are used by the Router Audit Tool (RAT) to check a configuration file. In most cases, the user will not have to understand the details of the patterns.
- The **Action** section of each audit rule shows PIXcommands you can use to configure the PIXin compliance with the rule. The command prompts have been included in the command listing to give context.
- PIXcommands are shown in typewriter font, for example: `router(config)#` **`aaa new-model`**.
- Long commands are wrapped so that words do not get broken on line boundaries. This is a little different from how the command interface looks on a typical display. Be careful to check for wrapped lines when copying commands from this benchmark.
- Some fields and arguments to commands must be filled in with values from the Audit Checklist (Section D). These are shown as variables in uppercase italics, for example: **`no access-list`** *`$(VTY_ACL_NUMBER)`*. In these cases, you should replace the variable with the value you filled in on the Audit Checklist.
- Other fields, in which the fix script contains the word "INSTANCE" in italics, indicate that the fix must be applied one or more instances of interfaces, lines, etc. For example: **`interface`** *`INSTANCE`* indicates that the rule must be applied to all interfaces that match the rules conditions, such as **`Ethernet0`**, **`Ethernet1`**, etc. You will have to fill in the correct instance values to use the command.

1.3 What's Covered, What's Not Covered ?

1.3.1 What's Covered

- The **Secure Management** This benchmark is primarily concerned with secure management and operation of the Cisco PIX Firewalls. It is concerned with things such as making sure only authorized users can manage it and making sure there are accurate logs, etc.

1.3.2 What's Not Covered

The following are not covered by this benchmark because they are not directly related to management of the device or because there is not enough information available for an automated tool to check compliance.

- The **Firewall Rules** This benchmark does not cover firewall rules other than those used to protect the PIXitself.
- The **VPNs** This benchmark does not cover VPN setup.
- The **Software Updates** It is important to keep software up to date. Many bugs can not be fixed by configuration. Updated code from the vendor is needed. See section A.2.
- The **SSH Key Generation** This benchmark not have rules to check SSH key generation. See section A.1.

2 The Level-1 Benchmark

2.1 CIS Level 1

Description CIS Level 1 Config Class is the root for all Level 1 configurations.

2.2 PIX Rule - no snmp-server

Description Disable SNMP if not in use.
Action `pix(config)#` **`no snmp-server`**
Security Impact SNMP allows remote monitoring of the PIX device. Older version of the protocol do not use any encryption for the community strings (passwords). SNMP should be disabled unless you intend to use it.
Exact Rule Regular expression `^snmp-server` forbidden in config.
Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode
Importance 10
Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - SNMP Rules
For More Info See PIX Command Reference, Chapter 8 for more information.

2.3 PIX Rule - SNMP community public forbidden

Description Change SNMP Public Community String
Action `pix(config)#`**`no snmp-server community public`**
Security Impact SNMP allows remote monitoring of the PIX device. Older version of the protocol do not use any encryption for the community strings (passwords). SNMP should be disabled unless you intend to use it.
Exact Rule Regular expression `^snmp-server community public` forbidden in config.
Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode
Importance 10
Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - SNMP Rules
For More Info See PIX Command Reference, Chapter 8 for more information.

2.4 PIX Rule - SNMP private community forbidden

Description Change SNMP Private Community String
Action `pix(config)#`**`no snmp-server community private`**
Security Impact SNMP allows remote monitoring of the PIX device. Older version of the protocol do not use any encryption for the community strings (passwords). SNMP should be disabled unless you intend to use it.
Exact Rule Regular expression `^snmp-server community private` forbidden in config.
Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode
Importance 10
Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - SNMP Rules
For More Info See PIX Command Reference, Chapter 8 for more information.

2.5 PIX Rule - SNMP polling forbidden without IP address

Description Require SNMP to be restricted to certain stations.
Action `snmp-server host \[EDIT-BY-HAND-IF\] EDIT-BY-HAND-IP poll`
Security Impact If management station IP addresses are not explicitly supplied, then anyone with a valid SNMP community string may monitor the PIX. Management IP addresses should be explicitly designated for those hosts permitted to monitor the PIX via SNMP.
Exact Rule Regular expression `^snmp-server host \S+ poll` forbidden in config.
Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode
Importance 10
Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - SNMP Rules
For More Info See PIX Command Reference, Chapter 8 for more information.

2.6 PIX Rule - Prohibit PDM Service

Description Disable HTTP server unless it is needed for remote management.
Action `pix(config)#` **`no http server enable`**
Security Impact The HTTP server allows remote web-based management of the PIX device. It uses SSL to protect the management session, but still uses password-based authentication. The HTTP server should be disabled, unless it is deemed essential for remote management of the PIX.
Exact Rule Regular expression `^http server enable` forbidden in config.
Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode
Importance 6
Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - Access Rules
For More Info See ”Installation and Configuration for Common Criteria EAL4 Evaluated Cisco PIX Firewall Version 6.2(2)” for more information.

2.7 PIX Rule - Set the PIX Device Manager address

Description Define the Pix Device Manager (PDM) ip address.
Action `pdm location` *`$(PIX_DATA_ADMIN_NET)`* `inside`
Security Impact Management access via the PDM should be restricted to management workstations
Exact Rule Regular expression `^pdm location` *`$(PIX_DATA_ADMIN_NET)`* `inside.*` required in config.
Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode
Importance 5
Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - Access Rules
For More Info See PIX Command Reference, Chapter 7 for more information.

2.8 PIX_DATA_ADMIN_NET

Info Needed The IP address and netmask of hosts permitted to connect to the pix for management.
Default Value 192.168.1.0 255.255.255.0
How To Obtain Choose an address and netmask for hosts allowed to access the device for management

2.9 PIX Rule - require local password

Description Require local password to access the device via telnet or ssh. This requires a password to be set.

Action `pix(config)#` **`passwd EDIT-BY-HAND`**

Security Impact Password is set to default to ”cisco”. This is a known password and could allow unauthorized access to the PIX device via telnet.

Warning Store the new password in a manner consistent with your site’s security policy. Once you change this password, you cannot view it again.

Exact Rule Regular expression `ˆpasswd \S+` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 10

Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - Access Rules

For More Info See PIX Command Reference, Chapter 7 for more information.

2.10 PIX Rule - require enable passwords

Description Require enable password; a user must supply the correct enable password to gain full administrative privileges.

Action `pix(config)#` **`enable password EDIT-BY-HAND`**

Security Impact The enable command invokes privileged command mode. By default, a password is not required, a user can just press the Enter key at the Password prompt to start privileged mode. The enable password command causes the PIX to enforce use of a password to get into privileged mode. The PIX uses a strong, one-way encryption hash (MD5) to protect the password as it appears in the device configuration listing.

Warning If you change the password, store it in a manner consistent with your site’s security policy. Once you change this password, you cannot view it again. Also, ensure that all who need privileged access the PIX Firewall console are given this password.

Exact Rule Regular expression `ˆenable password \S+ encrypted` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 10

Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - Access Rules

For More Info See PIX Command Reference, Chapter 5 .

2.11 PIX Rule - Ensure no telnet access

Description Prohibit telnet access to the PIX device

Action `pix(config)#`**`clear telnet`**

Security Impact Only use SSH and-or Cisco PDM to manage the PIX. Do not use Telnet for remote administration of the PIX, it offers no confidentiality or integrity protections.

Exact Rule Regular expression `ˆtelnet \d+\.*` forbidden in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - Access Rules

For More Info See PIX Command Reference, Chapter 9 for more information.

2.12 PIX Rule - Set SSH session timeout

Description Set an timeout on SSH sessions.

Action `pix(config)#ssh timeout $(PIX_SSH_TIMEOUT)`

Security Impact A timeout value ensures that idle sessions are not left open indefinitely.

Exact Rule Regular expression `^ssh timeout $(PIX_SSH_TIMEOUT)` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - Access Rules

For More Info See PIX Command Reference, Chapter 8 for more information.

2.13 PIX_SSH_TIMEOUT

Info Needed This is the time that the PIX will leave open an idle ssh administrative session. Allowable values are 1 to 60 minutes.

Default Value 10

How To Obtain Select a time limit for an idle ssh session, in minutes.

2.14 PIX Rule - Set SSH access address

Description Restrict ssh access to particular addresses or networks

Action `pix(config)#ssh $(PIX_SSH_ADMIN_NET) inside`

Security Impact Management access via ssh should be restricted to management workstations. This command may also be used to restrict ssh access to a particular interface.

Exact Rule Regular expression `^ssh $(PIX_SSH_ADMIN_NET) .*` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 6

Rule Group CIS Level 1⇒PIX Group - Management Plane Level 1⇒PIX Group - Access Rules

For More Info See PIX Command Reference, Chapter 8 for more information.

2.15 PIX_SSH_ADMIN_NET

Info Needed The IP address and netmask of hosts permitted to connect to the PIX with ssh for remote management.

Default Value 192.168.1.0 255.255.255.0

How To Obtain Choose an address or address and netmask for hosts allowed to access the PIX device via ssh

2.16 PIX Rule - IDS ip audit info

Description Alarm via logging any IDS info event related to IP behaviour

Action `ip audit info action alarm`

Security Impact With ip audit info alarms enabled, the PIX IDS system will log info events, but take no action against them.

Exact Rule Regular expression `^ip audit info action alarm` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Logging Rules Level 1⇒PIX Group - IDS Rules

For More Info This command applies to all traffic. You can also set IDS controls on individual PIX interfaces. See PIX Command Reference, Chapter 6 for more information.

2.17 PIX Rule - IDS ip audit attack

Description Alarm any attack events related to IP sessions or behavior.

Action **`ip audit attack action alarm`**

Security Impact With ip audit attack alarms enabled, the PIX IDS system will log attack events that it detects, but will take no action against them. By adding the keyword ”drop” you can cause the PIX to drop the offending packet.

Exact Rule Regular expression `ˆip audit attack action alarm` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Logging Rules Level 1⇒PIX Group - IDS Rules

For More Info This command applies to all traffic. You can also set IDS controls on individual PIX interfaces. See PIX Command Reference, Chapter 6 for more information.

2.18 PIX Rule - enable logging

Description Enable logging

Action **`logging on`**

Security Impact Logging should be enabled to allow monitoring of both operational and security related events.

Exact Rule Regular expression `ˆno logging on` forbidden in config.

Applicability PIX OS 6.1 to 6.2 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Logging Rules Level 1

For More Info See PIX Command Reference, Chapter 6 for more information

2.19 PIX Rule - set syslog server

Description set syslog server(s).

Action **`logging host inside \d+\.\d+\.\d+\.\d+`**

Security Impact Cisco PIX devices can send log messages to a Unix-style syslog service. A syslog service simply accepts messages, and stores them in files or prints them according to a simple configuration file. This form of logging is the best available for the PIX, because it can provide protected long-term storage for logs. Some sites (double firewalls for examples) will require this to be an outside syslog server. This rule is intended for the majority.

Exact Rule Regular expression `ˆlogging host inside \d+\.\d+\.\d+\.\d+` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Logging Rules Level 1

For More Info See PIX Command Reference, Chapter 6 for more information

2.20 PIX Rule - logging timestamps

Description Require timestamps in log messages.

Action **`logging timestamp`**

Security Impact Including timestamps in messages will allow you to trace network attacks more credibly.

Warning The logging timestamp command requires that the PIX Firewall clock is already set (with the clock command).

Exact Rule Regular expression `^logging timestamp` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Logging Rules Level 1

For More Info See PIX Command Reference, Chapter 6 for more information

2.21 PIX Rule - set syslog facility

Description set syslog facility.

Action **`logging facility 20`**

Security Impact Define the syslog facility to be used when generating syslog messages.

Exact Rule Regular expression `^logging facility \d+` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 3

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Logging Rules Level 1

For More Info See PIX Command Reference, Chapter 6 for more information

2.22 PIX Rule - logging trap info or debug

Description set syslog message severity level.

Action **`logging trap 7`**

Security Impact This determines the severity of messages that will generate a syslog message.

Exact Rule Regular expression `^logging trap (7|6|debug|info)` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 3

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Logging Rules Level 1

For More Info See PIX Command Reference, Chapter 6 for more information

2.23 PIX Rule - logging console critical

Description set console logging level.

Action **`logging console 2`**

Security Impact This determines the severity of messages that will generate console messages. This form of logging is not persistent; messages printed to the console are not stored by the PIX. Console logging is handy for operators when they use the console, but are otherwise of little value unless some other device or piece of software preserves the output. It is possible that excessive log messages on the console could make it impossible to manage the PIX, even on the console. To prevent this, use 'no logging console' to turn off all console logging. 'term monitor' may be used to see log messages on the currently connected session without logging messages to the console.

Exact Rule Regular expression `^logging console 2` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 3

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Logging Rules Level 1

For More Info See PIX Command Reference, Chapter 6 for more information

2.24 PIX Rule - logging history 6

Description Set SNMP trap level to informational; when this is set all non-debug events should generate an SNMP trap.

Action **`logging history 6`**

Security Impact This determines the severity of messages that will generate an SNMP trap.

Exact Rule Regular expression `^logging history (6|info)` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 3

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Logging Rules Level 1

For More Info See PIX Command Reference, Chapter 6 for more information

2.25 PIX Rule - turn off DHCPD

Description Disable DHCP service/access on the PIX

Action `pix(config)#`**`clear dhcpd`**

Security Impact DHCP should not be provided from a production firewall as it provides a service available to DoS attacks, and hands out IP addresses to devices that go on net.

Exact Rule Regular expression `^dhcpd` forbidden in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 10

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Control Service Rules

For More Info See PIX Command Reference, Chapter 5 for more information.

2.26 PIX Rule - Disable packet interface route lookup

Description Disable interface based routing

Action **`no sysopt route dnat`**

Security Impact Disabling this feature ensures that packets use the route table instead of src/dst interfaces to determine routing.

Exact Rule Regular expression `^sysopt route dnat` required in config.

Applicability PIX OS 6.1 to 6.2 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 1⇒PIX Group - Control Plane Level 1⇒PIX Group - Routing Rules

For More Info See PIX Command Reference, Chapter 7 for more information.

2.27 PIX Rule - fixup protocol http

Description enable fixup for HTTP.

Action `pix(config)#`**`fixup protocol http 80`**

Security Impact This ensures that only legitimate http requests are permitted on the HTTP port.

Exact Rule Regular expression `^fixup protocol http` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 3

Rule Group CIS Level 1⇒PIX Group - Data Plane Level 1⇒PIX Group - Fixup Rules

For More Info See PIX Command Reference, Chapter 5 for more information.

2.28 PIX Rule - fixup protocol ftp

Description enable fixup for FTP.

Action `pix(config)#`**`fixup protocol ftp 21`**

Security Impact This ensures that only legitimate ftp requests are permitted on the FTP command port.

Exact Rule Regular expression `^fixup protocol ftp` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 3

Rule Group CIS Level 1⇒PIX Group - Data Plane Level 1⇒PIX Group - Fixup Rules

For More Info See PIX Command Reference, Chapter 5 for more information.

2.29 PIX Rule - fixup protocol smtp

Description enable fixup for SMTP.

Action `pix(config)#`**`fixup protocol smtp 25`**

Security Impact This ensures that only legitimate SMTP requests are permitted on the SMTP port.

Warning Take care when enabling the SMTP fixup, it is very strict; any SMTP command not found in RFC 821 will be overwritten with XXXs. This will prevent many modern servers, which use ESMTP, from operating at all.

Exact Rule Regular expression `^fixup protocol smtp` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 3

Rule Group CIS Level 1⇒PIX Group - Data Plane Level 1⇒PIX Group - Fixup Rules

For More Info See PIX Command Reference, Chapter 5 for more information.

2.30 PIX Rule - Floodguard

Description Enable floodguard to protect against flood attacks against the uauth system on the PIX. If the system is attacked with excessive tcp connections, the PIX will reclaim user connection slots which are ending. See the command reference regarding the order in which tcp connections are reclaimed (timewait, last-ack, finwait, etc)

Action `pix(config)#`**`floodguard enable`**

Security Impact Protect against flood/dos attacks

Exact Rule Regular expression `ˆfloodguard enable` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 3

Rule Group CIS Level 1⇒PIX Group - Data Plane Level 1

For More Info See PIX Command Reference, Chapter 5 for more information.

2.31 PIX Rule - Enable fragguard fragmentation checks

Description Enforce IP packet fragment checks

Action `pix(config)#`**`sysopt security fragguard`**

Security Impact Protect against teardrop, land, etc.

Warning If fragmentation is used, fragmented packets received out of sequential order will be discarded when using the fragguard service. This is especially problematic for some Linux hosts, which send fragmented packet streams in reverse order.

Exact Rule Regular expression `ˆsysopt security fragguard` required in config.

Applicability PIX Version 6\.[1] PIXGlobal configuration mode

Importance 7

Rule Group CIS Level 1⇒PIX Group - Data Plane Level 1

For More Info This command is deprecated in version 6.3, and is available but replaced with the fragment chain command in version 6.2. Use the fragment chain command in versions 6.2 and 6.3 See PIX Command Reference, Chapter 8 for more information.

2.32 PIX Rule - Enable fragment chain fragmentation checks

Description Enforce IP packet fragment checks

Action `pix(config)#`**`fragment chain 1 outside`**

Security Impact Protect against teardrop, land, etc.

Warning The fragment command will disable fragmentation on the external PIX interface as described above. In general fragmentation can be disabled without problems. If fragmentation is required, do not implement.

Exact Rule Regular expression `ˆfragment chain 1 outside` required in config.

Applicability PIX Version 6\.[23] PIXGlobal configuration mode

Importance 7

Rule Group CIS Level 1⇒PIX Group - Data Plane Level 1

For More Info This command is new in version 6.2 of the PIX firewall, replacing the fragguard service in previous PIX versions. The fragment command allows for fragmentation policies to be applied on a per-interface basis, not globally as the fragguard command required See PIX Command Reference, Chapter 5 for more information.

2.33 PIX Rule - Set the connection slot timeout

Description Define a timeout for idle sessions.

Action `pix(config)#` **`timeout conn`** *`$(PIX_CONN_TIMEOUT)`*

Security Impact This timeout command sets the idle time for connection slots. If the slot has not been used for the idle time specified, the resource is returned to the free pool. This reduces the risk of someone from accessing an already established but idle connection.

Exact Rule Regular expression `^timeout conn` *`$(PIX_CONN_TIMEOUT)`* required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 7

Rule Group CIS Level 1⇒PIX Group - Data Plane Level 1

For More Info See PIX Command Reference, Chapter 9 for more information.

2.34 PIX_CONN_TIMEOUT

Info Needed This is the time that the PIX will hold an idle connection open before closing it down. Short values are more secure, but may be more disruptive to users. This time must be no longer than the translation timeout.

Default Value 0:30:00

How To Obtain Select a time limit for idle connection, as hh:mm:ss. A typical value would be half an hour, expressed as 0:30:00

2.35 PIX Rule - Set the translation slot timeout

Description Define a timeout for idle translation slots.

Action `pix(config)#` **`timeout xlate`** *`$(PIX_XLATE_TIMEOUT)`*

Security Impact This timeout command sets the maximum idle time for address translation slots on the PIX. If the slot has not been used for the idle time specified, the translation resource is returned to the free pool. This reduces the risk of someone from accessing an already established but idle translated address.

Exact Rule Regular expression `^timeout xlate` *`$(PIX_XLATE_TIMEOUT)`* required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 1⇒PIX Group - Data Plane Level 1

For More Info See PIX Command Reference, Chapter 9 for more information.

2.36 PIX_XLATE_TIMEOUT

Info Needed This is the time that the PIX will hold a translation slot with no traffic. This time must be no shorter than the connection timeout.

Default Value 1:00:00

How To Obtain Select a time limit for idle connection, as hh:mm:ss. A typical value would be an hour, expressed as 1:00:00

3 The Level-2 Benchmark

3.1 CIS Level 2

Description CIS Level 2 Config Class is the root for Level 2 configurations.

3.2 PIX Rule - PIX - aaa-server tacacs

Description AAA Authentication methods (TACACS)

Action **`aaa-server TACACS\+ protocol tacacs\+`**

Security Impact Use AAA authentication methods for login authentication (fall back to local passwords).

Exact Rule Regular expression `^aaa-server TACACS\+ protocol tacacs\+` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 2⇒PIX Group - Management Plane Level 2⇒PIX Group - Centralized AAA Rules

For More Info See PIX Command Reference, Chapter 3 for more information

3.3 PIX Rule - PIX-OS - aaa-server radius

Description AAA Authentication methods (RADIUS)

Action **`aaa-server RADIUS protocol radius`**

Security Impact Use AAA authentication methods for enable authentication (fall back to local passwords).

Exact Rule Regular expression `^aaa-server RADIUS protocol radius` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 5

Rule Group CIS Level 2⇒PIX Group - Management Plane Level 2⇒PIX Group - Centralized AAA Rules

For More Info See PIX Command Reference, Chapter 3 for more information

3.4 PIX Rule - Unicast RPF Verification

Description Verify reverse path for IP spoofing protection.

Action **`ip verify reverse-path interface EDIT-BY-HAND`**

Security Impact Routing rules are checked to ensure valid source addresses

Warning Take care when enabling unicast reverse-path forwarding verification on the PIX. This feature can break traffic flow if all routes are not properly configured or maintained with routing protocols.

Exact Rule Regular expression `^ip verify reverse-path interface \S+` required in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 10

Rule Group CIS Level 2⇒PIX Group - Data Plane Level 2

For More Info See PIX Command Reference, Chapter 6 for more information

3.5 PIX Rule - Forbid Conduits

Description Avoid using PIX legacy conduit statements, use access lists instead.

Action `pix(config)#`**`no conduit EDIT-BY-HAND`**

Security Impact The conduit facility does not offer fine-grained control of traffic filtering. Also, the conduit facility is superseded by access lists in PIX 6.1 and later.

Exact Rule Regular expression `^conduit` forbidden in config.

Applicability PIX OS 6.1 to 6.3 PIXGlobal configuration mode

Importance 4

Rule Group CIS Level 2⇒PIX Group - Data Plane Level 2

For More Info See PIX Command Reference, Chapter 4 for more information.

A Other Things To Do

Some actions that are important to security can not be checked by a scoring tool. This can be due to lack of information in the configuration file or other reasons. A few of the more important issues relating to PIXsecurity are listed here

A.1 Configure SSH

The PIXconfiguration file does not display enough information to determine if all the configuration necessary to use SSH has been performed. In particular, it does not display enough information to determine if SSH keys have been generated ("ca generate..." and "ca save all"). This section gives a complete example of configuring SSH on the PIX

Before one can use SSH on the PIX, one must configure the PIXwith the following commands: hostname, domain-name, and ca generate RSA key. The following example sets the hostname to pix-fw, specifies the domain-name to example.org, creates an RSA key-pair with a modulus size of 1024 bits, and saves the RSA key-pair to Flash memory.

```
PIX(config)# hostname pix-fw
pix-fw(config)# domain-name example.gov
pix-fw(config)# ca generate rsa key 1024
pix-fw(config)# ca save all
```

One can create a list of IP addresses that are allowed to make SSH connections to the PIX. Below is an example for two systems, 10.1.1.1 and 10.1.1.2, on the inside network.

```
pix-fw(config)# ssh 10.1.1.1 255.255.255.255 inside
pix-fw(config)# ssh 10.1.1.2 255.255.255.255 inside
```

Finally, one can set the timeout value for how long an SSH session can be idle before being disconnected. The default value is 5 minutes. The allowable range is from 1 to 60 minutes. The following example shows a timeout of nine minutes.

```
pix-fw(config)# ssh timeout 9
```

A.2 Upgrade

[XXX How to check for and perform upgrades info goes here]

B Other Information

B.1 How Benchmark Items Are Determined

B.1.1 CIS Level-I Benchmarks the prudent level of minimum due care

Level-I Benchmark settings/actions meet the following criteria.

1. System administrators with any level of security knowledge and experience can understand and perform the specified actions.
2. The action is unlikely to cause an interruption of service to the operating system or the applications that run on it.
3. The actions can be automatically monitored, and the configuration verified, by Scoring Tools that are available from the Center or by CIS-certified Scoring Tools.

Many organizations running the CIS scoring tools report that compliance with a CIS ”Level-1” benchmark produces substantial improvement in security for their systems connected to the Internet.

B.1.2 CIS Level-II Benchmarks prudent security beyond the minimum level.

Level-II security configurations vary depending on network architecture and server function. These are of greatest value to system administrators who have sufficient security knowledge to apply them with consideration to the operating systems and applications running in their particular environments.
See http://www.cisecurity.org/bench.html for more information on how benchmarks are determined.

B.2 Understanding Technology, Risks and Your Organizational Goals

This Benchmark and related scoring are intended to be tools to assist in risk analysis and mitigation. The recommendations in the benchmark and tool should not be applied blindly and without thorough understanding of organizational goals and how technologies are applied to meet those goals.
For example, the benchmark recommends that you disable SNMP servers on Cisco PIX Firewalls. While this will lessen risk for certain classes of SNMP-based attacks, your organization may rely on SNMP for monitoring it’s critical infrastructure (routers). Disabling SNMP may result in the devices being un-monitored. Leaving it enabled may result in a downtime due to an exploited vulnerability. You need to understand both the risks and the organizational needs.

B.3 Scoring and Scoring Tools

The benchmarks are designed to make it possible to compute an overall score for each system. This can be done manually or with the aid of a scoring tool. The Center for Internet Security provides free scoring tools which are available from http://www.cisecurity.org. There are also third party tools score systems per CIS guidelines.
Overall system scores are defined as follows

$$10 * \frac{ActualScore}{PotentialScore}$$

where

$$ActualScore = \sum PassingTests * IndividualTestImportance$$

and

$$PotentialScore = \sum AllTests * IndividualTestImportance$$

So, for example, if the benchmark contained exactly one rule, say “exec-timeout” requiring each serial line to timeout idle sessions, and the rule was assigned an importance of “5”, and there were three serial interfaces in the config (con,aux,vty), and the test showed that the rule had been applied on only one of the three, then the Actual Score would be 5 (1*5), the potential score would be 15 (3*5) and the overall system score would be 3.3 (10 * 5/15).

B.4 Credits

Many people and organizations have contributed to this document. Some of the many to whom thanks are due are:

- John Banghart/CIS,
- Phil Benchoff/Virginia Tech,
- Jim Duncan/Cisco
- Daniel J. Duesterhaus
- Brian Ford/Cisco
- Eric Frostrom/RAEcore
- George Jones/The MITRE Corporation
- Jim Lentz
- Rajesh Nair/Corliant
- Janice Pryor
- Chris Smith/Calence
- Donald Smith/Qwest
- John Stewart/Cisco,
- John Traenkenschuh
- Trudy L. Wadsworth
- Neal Ziring/NSA

Thanks to all who have contributed but were not listed. If you want to be listed in future revisions, send mail to rat-feedback@cisecurity.org. Inclusion in this list is intended only to acknowledge contributions, not to imply endorsement by the individuals or organizations listed.

C Example Configuration

The example below is a Cisco PIX Firewallsconfiguration that passes all of the CIS Benchmark level 1 and 2 rules. It makes the following assumptions:

1. Inside network: 10.1.1.0/24
2. Outside network: 172.31.1.0/24
3. Gateway: 172.31.1.1
4. No ACLs applied to inside and outside interfaces
5. All machines in the inside network are translated to IP address assigned for outside segment
6. IP addresses of management workstation, AAA server, Syslog server, SNMP Management server and NTP server are selected at random
7. Commands specific to PDM (like name; location etc.), but that do not have operational significance have been removed.

```
PIX Version 6.2(2)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 3osC6hWjc.znriya encrypted
passwd RTxhdAJZxNxz9RzP encrypted
hostname firewall
domain-name company.com
clock timezone EST -5
clock summer-time EDT recurring
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
no fixup protocol smtp 25
pager lines 24
logging on
logging timestamp
no logging buffered
logging console critical
logging trap debugging
logging history debugging
logging facility 20
logging host inside 10.1.1.159
interface ethernet0 100full
interface ethernet1 100full
mtu outside 1500
mtu inside 1500
ip address outside 172.31.1.5 255.255.255.0
ip address inside 10.1.1.5 255.255.255.0
ip verify reverse-path interface outside
ip verify reverse-path interface inside
ip audit name infoaudit info action alarm
ip audit name attackaudit attack action alarm
ip audit interface outside infoaudit
ip audit interface outside attackaudit
ip audit info action alarm
ip audit attack action alarm drop
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address SOC 0.0.0.0
failover ip address NOC 0.0.0.0
arp timeout 14400
global (outside) 1 172.31.1.20-172.31.1.254
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 172.31.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:05:00 udp 0:30:00 rpc 0:10:00 h323 0:15:00 sip 0:30:00 sip_media 0:30:00
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
aaa-server AuthServer inside host 10.1.1.56 CiSecurity 5
aaa authentication ssh console LOCAL
aaa authentication http console AuthServer
aaa-server AuthServer protocol tacacs+
ntp server 10.1.1.5 source inside
ntp server 128.118.25.3 source outside
http server enable
http 10.1.1.155 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community 1Rde5Tyur8
snmp-server inside 10.1.1.4
snmp-server enable traps
floodguard enable
fragment chain 1 outside
sysopt security fragguard
sysopt connection permit-ipsec
no sysopt route dnat
ssh 10.1.1.155 255.255.255.255 inside
ssh timeout 5
terminal width 80
```

D Audit Checklist

This section lists all the groups, rules and data items in the benchmark. The items are listed in hierarchal fashion that shows the decisions the administrator will have to make in configuring the device. For each item, the question that must be answered by the administrator is listed. The question may be a YES/no question, or it may ask the user to supply some value, such as the IP address of a logging server.

For example, a group to "disable all unneeded services" may contain rules to disable FTP, echo, finger, etc. The group will have a YES/no answer. If the answer is YES, then the subsequent YES/no questions for each service must be answered.

DEFAULT ANSWERS are given in UPPERCASE. For items that require the user to supply a value the default is given, then a blank to fill in.

As a convenience an "Expanded Audit Checklist" is available at http://www.cisecurity.org/ If you intend to audit more than one device or intend to audit the same device several times, you are encouraged to print and copy this document.

D.1 Level-1

Apply some or all of CIS level 1 rules? (2.1) . . . . (YES/no)

  Check rules and data related to system management? (**??**) . . . . YES

    Use local authentication? (**??**) . . . . (YES/no)

    Apply standard SNMP checks? (**??**) . . . . YES

      Disable snmp-server? (2.2) . . . . (YES/no)

      Disallow snmp public community? (2.3) . . . . YES

      Disallow snmp private community? (2.4) . . . . YES

      Disallow SNMP polling without specific IP addresses? (2.5) . . . . YES

    Apply standard checks to PIX access controls? (**??**) . . . . (YES/no)

      Disable the PIX Device Manager (HTTPS) service? (2.6) . . . . (YES/no)

      Restrict access to PDM? (2.7) . . . . (YES/no)

        Address range for administrative hosts? (2.8) (192.168.1.0 255.255.255.0/__________________)

      Require local password? (2.9) . . . . YES

      Require enable passwords? (2.10) . . . . YES

      Disable telnet access to the PIX? (2.11) . . . . YES

      Check for ssh timeout? (2.12) . . . . (YES/no)

        ssh session timeout (minutes)? (2.13) . . . . (10/__________________)

      Restrict ssh admin access? (2.14) . . . . (YES/no)

Address or address range for ssh admin hosts? (2.15) . . . .(192.168.1.0 255.255.255.0/________________)

Disable unneeded management services? (**??**) . . . . (YES/no)

Check rules and data related to system control? (**??**) . . . . YES

Synchronize PIX device time via NTP? (**??**) . . . .(YES/no)

Apply standard logging rules? (**??**) . . . . (YES/no)

Use GMT for logging instead of localtime? (**??**) . . . . (YES/no)

Configure PIX Firewall IDS Capabilities? (**??**) . . . . (YES/no)

Enable basic IDS alarms for anomalous IP traffic? (2.16) . . . . .YES

Enable basic IDS alarms for known IP attacks.? (2.17) . . . . .YES

Enable logging? (2.18) . . . . YES

Set syslog server? (2.19) . . . . .YES

Enable logging timestamps? (2.20) . . . . YES

Set syslog facility? (2.21) . . . . YES

Set syslog logging level? (2.22) . . . . .YES

Set console logging level? (2.23) . . . . YES

Set SNMP trap logging level? (2.24) . . . . YES

Disable unneeded control services? (**??**) . . . .(YES/no)

Disable DHCPD server on PIX? (2.25) . . . . YES

Disable unneeded routing services? (**??**) . . . . (YES/no)

Disable routing based on destination interfaces? (2.26) . . . . .YES

Check rules and data related to data flow? (**??**) . . . . YES

Allow Fixup Rules? (**??**) . . . . (YES/no)

Enable HTTP protocol fixup? (2.27) . . . . YES

Enable FTP protocol fixup? (2.28) . . . . YES

Enable SMTP protocol fixup? (2.29) . . . .(yes/NO)

Enable Floodguard? (2.30) . . . . .YES

Enable ip fragmentation checks via the sysopt security fragguard command? (2.31) . . . . .YES

Enable ip fragmentation checks via the fragment command? (2.32) . . . . .YES

Set idle timeout for inactive sessions? (2.33) . . . . YES

Connection time-out time? (2.34) . . . . (0:30:00/________________)

Set idle timeout for inactive translations? (2.35) . . . . (YES/no)

Translation time-out time? (2.36) . . . . (1:00:00/________________)

D.2 Level-2

Apply some or all of CIS Level 2 rules? (3.1) . . . . (yes/NO)

Check rules and data related to system management? (**??**) . . . . (yes/NO)

Use TACACS Plus or Radius authentication? (**??**) . . . . (yes/NO)

Enable TACACS authentication? (3.2) . . . . YES

Enable RADIUS authentication? (3.3) . . . . YES

Check rules and data related to data flow? (**??**) . . . . (yes/NO)

Enable Reverse Path Forwarding checks? (3.4) . . . . YES

Prohibit (legacy) conduits? (3.5) . . . . YES

References

[1] Greg Bastien,Christian Degu
CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide
Cisco Press, 2003
ISBN 1587200678

[2] George M. Jones at al.
The Router Audit Tool and Benchmark
Center for Internet Security, 2002
http://www.cisecurity.org

[3] Elizabeth D. Zwicky, Simon Cooper and D. Brent Chapman
Building Internet Firewalls
O'Reilly and Associates, 2000
http://www.ora.com/catalog/fire2/

[4] Cisco Systems
Cisco PIX Firewall Command Reference, Version 6.3
Cisco Systems, 2003
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/cmdref/

[5] Cisco Systems
Cisco PIX Firewall and VPN Configuration Guide, Version 6.3
Cisco Systems, 2003
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/v_63/config/

E Agreed Terms of Use

Background

CIS provides benchmarks, scoring tools, software, data, information, suggestions , ideas, and other services and materials from the CIS website or elsewhere (“Products”) as a public service to Internet users worldwide. Recommendations contained in the Products (“Recommendations”) result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a “quick fix” for anyone’s information security needs.

No representations, warranties and covenants

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations “as is” and “as available” without representations, warranties or covenants of any kind.

User agreements

By using the Products and/or the Recommendations, I and/or my organization (“we”) agree and acknowledge that:

1. No network, system, device, hardware, software or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS’s negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and
6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights."

Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("CIS Parties" harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Term s of Use.

Special rules

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

E.1 What's Covered, What's Not Covered ?

E.1.1 What's Covered

- The **Secure Management** This benchmark is primarily concerned with secure management and operation of the Cisco PIX Firewalls. It is concerned with things such as making sure only authorized users can manage it and making sure there are accurate logs, etc.

E.1.2 What's Not Covered

The following are not covered by this benchmark because they are not directly related to management of the device or because there is not enough information available for an automated tool to check compliance.

- The **Firewall Rules** This benchmark does not cover firewall rules other than those used to protect the PIXitself.
- The **VPNs** This benchmark does not cover VPN setup.
- The **Software Updates** It is important to keep software up to date. Many bugs can not be fixed by configuration. Updated code from the vendor is needed. See section A.2.
- The **SSH Key Generation** This benchmark not have rules to check SSH key generation. See section A.1.