About Cisco PIX Firewalls

The PIX firewall requires extensive provisioning to meet both industry best practices and regulatory compliance. By default the firewall operating system allows various methods of anonymous and unaudited access, which must be fixed in order to properly secure the system, and ensure least privilege, which is represented by security 0. The vast majority of the settings listed below can be changed using a command line interface. An example would be using the software putty, or regular command line prompt on a Windows operating system. Please Note the PIX firewall is also end of life, and is replaced by the ASA.

Sorting Criteria Defined

The provisioning and hardening checklist provided below is organized to present security controls in a descending format, with more critical vulnerabilities being addressed first. Each item will be given a severity code derived from the applicable information, while a security control will first be assigned a code based on the area of information security to which it pertains, followed by the severity of the vulnerability addressed. For example: (General/Severity 1) indicates a security control which is of the General category, with the highest possible severity. Following the assigned severity code, will be a detailed description of how the control must be implemented to address the aforementioned vulnerability. Each control listed within this document, is an "industry best practice" and its implementation is subject to the specific requirements of the organization being audited.

Cisco PIX Firewall Provisioning and Hardening Checklist

General Information

Name of Individual Performing the Cisco PIX Provisioning and Hardening				
Last Name	**First Name**	**Middle Name**	**Title**	**Date of Review**

Additional Information			
Department	**Division**	**Office**	**Immediate Supervisor**

Firewall Information	
Hostname of Firewall Appliance	
FIPS Security Category	

Vulnerability Severity Codes

Severity 1	**Vulnerabilities which when exploited lead to immediate superuser access, unauthorized access to a machine, or allow an attacker to bypass security controls.**
Severity 2	**Vulnerabilities which provide an attacker information with a high probability of allowing unauthorized access to a machine, or to bypass security controls.**
Severity 3	**Vulnerabilities which grant an attacker information that may possibly lead to the compromise of a machine, or the bypassing of existing security controls**
Severity 4	**Vulnerabilities which generally degrade the overall security of a system when left unresolved.**

Operating System

	Task	Severity Code	Date Completed	Signature
(1).	The outside port should be set to security 0, and the inside port should be set to security 100	1		
Additional Information:				
(2).	**Task**	**Severity Code**	**Date Completed**	**Signature**
	login, and enable secret passwords should be enabled	1		

Additional Information:	

	Task	Severity Code	Date Completed	Signature
(3).	The firewall should have the latest image the hardware can handle on flash for the Pix 501 to 506 the latest official image to use is 6.3(x). For the 515 to 535 the latest official image to use is 8.0.4	2		

Additional Information:	

	Task	Severity Code	Date Completed	Signature
(4).	Ports not in use should be turned to the shutdown state	2		

Additional Information:	

Systems Auditing

	Task	Severity Code	Date Completed	Signature
(1).	enable logging: The level you specify means that you want that level and those less than the level. For example, if level is 3, syslog displays 0, 1, 2, and 3 messages. Possible number and string level values are:	2		

Additional Information:	**0—emergencies—System unusable messages** **1—alerts—Take immediate action** **2—critical—Critical condition** **3—errors—Error message** **4—warnings—Warning message** **5—notifications—Normal but significant condition** **6—informational—Information message** **7—debugging—Debug messages and log FTP commands and WWW URLs** [**no**] **logging on** [**no**] **logging buffered** *level* [**no**] **logging console** *level*

	logging device-id {**hostname	ipaddress** *if_name* **| string** *text*} **no logging device-id** [**no**] **logging facility** *facility* [**no**] **logging history** *level* [**no**] **logging host** [*in_if_name*] *ip_address* [*protocol* **/***port*] [**format emblem**] [**no**] **logging message** *syslog_id* [**level** *level*] [**no**] **logging monitor** *level* [**no**] **logging queue** *queue_size* [**no**] **logging standby** [**no**] **logging timestamp** [**no**] **logging trap** *level* **clear logging** [**disable**] **show logging** [**message** {*syslog_id* **| all**}	**level**	**disabled**] **show logging queue** **Syntax Description** **who** Shows the active administration sessions on the firewall. **all** All syslog message IDs. **buffered** Send syslog messages to an internal buffer that can be viewed with the **show logging** command. Use the **clear logging** command to clear the message buffer. New messages append to the end of the buffer. **clear** Clear the buffer for use with the **logging buffered** command.

	Task	Severity Code	Date Completed	Signature
(2).	Use command ip audit info Specifies the default action to be taken for signatures classified as informational signatures. The alarm option indicates that when a signature match is detected in a packet, PIX Firewall reports the event to all configured syslog servers. The drop option drops the offending packet. The reset option drops the offending packet and closes the connection if it is part of an active connection. The default is alarm. To cancel	2		

	event reactions, specify the ip audit info command without an action option.			

Additional Information:	

System Access Controls

(1).	Task	Severity Code	Date Completed	Signature
	Telnet access restricted. The reasoning behind restricting access for port 23 is any information passed through port 23 is shown in clear text.	1		

Additional Information:	

(2).	Task	Severity Code	Date Completed	Signature
	All forms of remote access to system services should be conducted using encrypted formats such as SSH or SSH2 if supported by the current running image	1		

Additional Information:	

(3).	Task	Severity Code	Date Completed	Signature
	Configure the system to lock an account for after 2 bad login attempts, for a specific amount of time.			

SECURITY POLICIES ONLINE.COM

You Have Just Viewed a Sample Portion of this Document

Purchase Full Document