



FIPS 140-2 Non-Proprietary Security Policy for the Cisco PIX 525/535 Security Appliance

Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco PIX 525 and PIX 535 security appliances, referred to in this document as PIX security appliances, devices, modules, or appliances. This security policy describes how the PIX security appliances meet the security requirements of FIPS 140-2 and how to run the devices in a FIPS 140-2 mode of operation.

This policy was prepared as part of the Level 1 FIPS 140-2 validation of the Cisco PIX 525 and PIX 535 security appliances.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at <http://csrc.nist.gov/cryptval/>.



Note

This document may be copied in its entirety and without modification. All copies must include the copyright notice and statements on the last page.

This document includes the following sections:

- [Submission Package, page 2](#)
- [Overview, page 2](#)
- [PIX Security Appliance Validation Level, page 3](#)
- [Physical Characteristics and Module Interfaces, page 3](#)
- [Roles and Services, page 6](#)
- [Authentication Mechanisms, page 7](#)
- [Cryptographic Key Management, page 8](#)
- [Self-Tests, page 11](#)
- [Mitigation of Other Attacks, page 12](#)
- [Secure Operation, page 12](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Approved Cryptographic Algorithms, page 15](#)
- [Non-FIPS Approved Algorithms, page 16](#)
- [Applying Tamper-Evident Labels, page 16](#)
- [Related Documentation, page 18](#)
- [Obtaining Documentation and Submitting a Service Request, page 19](#)
- [Definitions, page 19](#)

Submission Package

This security policy document is part of a complete FIPS 140-2 Submission Package. In addition to this document, the complete FIPS 140-2 Submission Package contains:

- Vendor Evidence
- Finite State Machine
- Other supporting documentation as additional references

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc. See [“Obtaining Technical Assistance” section on page 21](#) for more information.

Overview

The Cisco PIX security appliances deliver robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services in cost-effective, easy-to-deploy solutions. Cisco PIX security appliances provide comprehensive security, performance, and reliability for network environments of all sizes.

These PIX security appliances provide multiple integrated security and networking services, including:

- Application-aware firewall services
- Voice over IP (VoIP) and multimedia security
- Robust site-to-site and remote-access IPSec VPN connectivity
- Resiliency
- Intelligent networking services
- Flexible management solutions

The Cisco PIX 525 and PIX 535 security appliances are validated with the VPN Acceleration Card+ (VAC+), to provide hardware-accelerated IP Security (IPSec) VPN support for international cryptographic standards and scalable VPN tunnel aggregation in a solution that comes integrated with, or as an upgrade for, most Cisco PIX security appliances. Ranging from solutions for small to midsize businesses (SMBs) to large enterprises and service providers, the Cisco PIX security appliances offer integrated network security services and investment protection. The Cisco PIX VAC+ offloads VPN cryptographic functionality from the PIX device, enabling the Cisco PIX security appliances to deliver stateful inspection firewall services, advanced application and protocol inspection, inline intrusion protection, and robust multimedia and voice security services.

PIX Security Appliance Validation Level

Table 1 lists the level of validation for each area in the FIPS 140-2 security policy.

Table 1 Validation Level by Section

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

Physical Characteristics and Module Interfaces

The design of the Cisco PIX 525 and PIX 535 security appliances supports a combination of 10/100 Fast Ethernet interfaces and Gigabit Ethernet interfaces, with a redundant power supply on PIX 535.

Each PIX security appliance is a multi-chip standalone device. The cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” and “bottom” surfaces of the case, as well as the “backplane” of the case not supporting a removable interface or service card, and the inverse of the three-dimensional space within the case that would otherwise be occupied by an installed service card. The cryptographic boundary includes the connection apparatus between the service card and the motherboard/daughterboard that hosts the service card, but the boundary does not include the service card itself (except when a VAC+ is inserted into an available PIX Circuit Board Interface). In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed modular service card (except when a VAC+ is inserted into an available PIX Circuit Board Interface).

Each PIX security appliance provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the device are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output.

The logical interfaces and their mapping are described in [Table 2](#) and in [Table 3](#):

Table 2 Cisco 525 Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 Circuit Board Interfaces 0-2 Console Port	Data Input Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 Circuit Board Interfaces 0-2 Console Port	Data Output Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 Circuit Board Interfaces 0-2 Power Switch Console Port	Control Input Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 0 100Mbps LED 10/100BaseTX Ethernet 0 ACT LED 10/100BaseTX Ethernet 0 LINK LED 10/100BaseTX Ethernet 1 10/100BaseTX Ethernet 1 100Mbps LED 10/100BaseTX Ethernet 1 ACT LED 10/100BaseTX Ethernet 1 LINK LED Circuit Board Interfaces 0-2 Power LED System Activity LED Console Port	Status Output Interface
Main Power Plug	Power Interface
USB Port Serial Failover Interface	Unused Interface

Table 3 *Cisco 535 Physical Interface/Logical Interface Mapping*

Physical Interface	FIPS 140-2 Logical Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 Circuit Board Interfaces 0-8 Console Port	Data Input Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 Circuit Board Interfaces 0-8 Console Port	Data Output Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 Circuit Board Interfaces 0-8 Power Switch Console Port	Control Input Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 0 100Mbps LED 10/100BaseTX Ethernet 0 ACT LED 10/100BaseTX Ethernet 0 LINK LED 10/100BaseTX Ethernet 1 10/100BaseTX Ethernet 1 100Mbps LED 10/100BaseTX Ethernet 1 ACT LED 10/100BaseTX Ethernet 1 LINK LED Circuit Board Interfaces 0-8 Console Port	Status Output Interface
Power Plug(s)	Power Interface
USB Port Serial Failover Interface	Unused Interface

Roles and Services

The device can be accessed in one of the following ways.

- Console Port
- Telnet over IPsec
- SSH
- ASDM via HTTPS/TLS

As required by FIPS 140-2, there are two main roles in the PIX security appliance that operators may assume: a crypto officer role and user role. The PIX security appliance supports role-based authentication, and the respective services for each role are described in the “[Crypto Officer Services](#)” section on page 6, and the “[User Services](#)” section on page 6.

Crypto Officer Services

The crypto officer role is responsible for the configuration and maintenance of the PIX security appliance and authenticates from the **enable** command (for local authentication) or the **login** command (for AAA authentication) from the user services. The crypto officer services consist of the following:

- **Configure the Device**—Define network interfaces and settings; set the protocols the PIX security appliance will support; enable interfaces and network services; set system date and time; load authentication information; and configure authentication servers, filters and access lists for interfaces and users, and privileges
- **Define Rules and Filters**—Create packet filters that are applied to user data streams on each interface. Each filter consists of a set of rules, which define a set of packets to permit or deny based on characteristics such as protocol ID, addresses, ports, TCP connection establishment, or packet direction.
- **View Status**—View the configuration, routing tables, active sessions, use gets to view SNMP MIB statistics, health, temperature, memory status, packet statistics, review accounting logs, and view physical interface status.
- **Manage the Device**—Log off users, shutdown or reload the PIX security appliance, view complete configurations, view full status, manage user rights, and restore configurations.
- **Set Encryption/Bypass**—Set up the configuration tables for IP tunneling, set keys and algorithms to be used for each IP range or allow plaintext packets to be sent from specified IP address.
- **Install Service Card**— Remove tamper-evident seals to install or replace service cards.

User Services

Basic encryption and decryption services are performed by the User role. A user enters the system by accessing the console port with a terminal program or via IPsec protected telnet or SSH session to a LAN port. The PIX security appliance will prompt the user for their password. If the password is correct, the user is allowed entry to the executive program. The services available to the user role consist of:

- **Status Functions**—Image version currently running, installed hardware components, and version of hardware installed
- **Network Functions**—Initiate diagnostic network services, such as ping
- **Directory Services**—Display directory of files kept in Flash memory

Critical Security Parameters

The services accessing the Critical Security Parameters (CSPs), the type of access and which role accesses the CSPs are listed in the [Table 4](#).

Table 4 *Role and Service Access to Security Relevant Data Items*

CSP/Role/Service Access Policy	Critical Security Parameter	CSP 1	CSP 2	CSP 3	CSP 4	CSP 5	CSP 6	CSP 7	CSP 8	CSP 9	CSP 10	CSP 11	CSP 12	CSP 13	CSP 14	CSP 15	CSP 16
Role/Service																	
User role																	
Status Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Network Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Directory Services		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Crypto-Officer Role																	
Configure the Module		rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd
Define Rules and Filters		rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd
Status Functions																	
Manage the Module		rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd
Set Encryption/Bypass		rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd
Install Service Card																	

r = read w = write d = delete

148385

Authentication Mechanisms

The PIX security appliance supports either a password or digital certificates for authenticating IPSec users. To log on to the PIX security appliance for management purposes, an operator must connect to it through one of the management interfaces (Console Port, SSH, Telnet, or ASDM) and provide a password.

[Table 5](#) describes the estimated strength of the authentication mechanism.

Table 5 *Estimated Strength of Authentication Mechanism*

Authentication Type	Strength
Username Password mechanism	<p>Passwords must be a minimum of 6 characters (see the “Secure Operation” section on page 12). The probability of a false positive for a random password guess is less than 1 in 1,000,000. This is also valid for RADIUS or TACACS+ shared secret keys.</p> <p>The password can consist of alphanumeric values, a-zA-Z0-9, yielding 62 choices per character. The probability of a successful random attempt is $1/62^6$, which is less than 1/1,000,000.</p>
Certificate based authentication	<p>The PIX security appliance supports a public key based authentication with 1024 and 2048 (for RSA) bit keys, and thus the probability of a false positive from a random correct guess is less than 1 in 1,000,000.</p> <p>A 1024-bit RSA key has at least 80-bits of equivalent strength. The probability of a successful random attempt is $1/2^{80}$, is less than 1/1,000,000.</p> <p>A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is $1/2^{112}$, is less than 1/1,000,000.</p>

Cryptographic Key Management

The PIX security appliances use a variety of critical security parameters during operation.

[Table 6](#) lists the critical security parameters used by the PIX security appliance.

Table 6 Critical Security Parameters Used by the PIX Security Appliance

#	Key/CSP Name	Generation/Algorithm	Description	Storage	Zeroization
1	RSA public/private keys	ANSI X9.31/RSA	Identity certificates for the PIX security appliance itself and also used in IPsec, TLS, and SSH negotiations. While the PIX security appliance supports 512, 768, 1024 and 2048 bit RSA key sizes; 512 and 768 bit RSA keys shall not be used in FIPS mode. 1536 bit keys are not supported.	Private Key—NVRAM (plain text) and RAM (plain text) Public Key—NVRAM (plain text) and RAM (plain text)	Private Key—crypto key zeroize, write to startup config, then reboot. Public Key—delete trustpoint from configuration, write to startup config, then reboot.
2	DSA public/private keys	ANSI X9.31/DSA	Identity certificates for the PIX security appliance itself and also used in IPsec negotiations. The PIX security appliance supports 512, 768, 1024 and 2048 bit key sizes.	Private Key—NVRAM (plain text) and RAM (plain text) Public Key—NVRAM (plain text) and RAM (plain text)	Private Key—crypto key zeroize, write to startup config, then reboot. Public Key—delete trustpoint from configuration, write to startup config, then reboot.
3	Diffie-Hellman Key Pairs	ANSI X9.31 / DH	Key agreement for IKE, TLS, and SSH sessions. DH groups 1 (768 bits of keying strength), 2 (1024 bits), 5 (1536 bits), and 7 (2048 bits) are supported.	RAM (plain text)	Resetting or rebooting the PIX security appliance.
4	Public keys	DSA / RSA	Public keys of peers	RAM (plain text)	Resetting or rebooting the PIX security appliance.
5	TLS Traffic Keys	Generated using the TLS protocol (X9.31PRNG + HMAC-SHA1 + HMAC-MD5 + either DH or RSA) Algorithm: Also Triple DES & AES	Used in HTTPS connections	RAM (plain text)	Resetting or rebooting the PIX security appliance.
6	SSH Session Keys	ANSI X9.31 / Triple DES-AES	SSH keys	RAM (plain text)	Resetting or rebooting the PIX security appliance.
7	IPsec authentication keys	ANSI X9.31 / Triple DES-AES / DH	Exchanged using the IKE protocol and the public/private key pairs. These are Triple DES or AES keys.	RAM (plain text)	Resetting or rebooting the PIX security appliance.

Table 6 Critical Security Parameters Used by the PIX Security Appliance (continued)

#	Key/CSP Name	Generation/ Algorithm	Description	Storage	Zeroization
8	IPSec traffic keys	ANSI X9.31 / Triple DES-AES / DH	Exchanged using the IKE protocol and the public/private key pairs. These are Triple DES or AES keys.	RAM (plain text)	Resetting or rebooting the PIX security appliance.
9	IKE preshared keys	Shared Secret	Entered by the crypto officer in plain text form and used for authentication during IKE	NVRAM (plain text) and RAM (plain text)	Overwrite keys with new keys, or delete keys from the configuration via the erase flash: command. Write to startup configuration, then reboot.
10	IKE Authentication key	Generated using IKE (X9.31+HMAC-SHA1+DH). Algorithms: Triple DES, AES, SHA-1	Used to encrypt and authenticate IKE negotiations	RAM (plain text)	Resetting or rebooting the PIX security appliance.
11	IKE Encryption Key	Generated using IKE (X9.31+HMAC-SHA1+DH). Algorithms: Triple DES, AES, SHA-1	Used to encrypt IKE negotiations	RAM (plain text)	Resetting or rebooting the PIX security appliance.
12	RADIUS and TACACS+ shared secret keys	Shared Secret	Used for authenticating the RADIUS or TACACS+ server to the PIX security appliance and vice versa. Entered by the crypto officer in plain text form and stored in plain text form.	NVRAM (plain text) and RAM (plain text)	Overwrite keys with new keys, or delete keys from the configuration via the erase flash: command. Write to startup configuration, then reboot.
13	Username/ Passwords	Secret	Critical security parameters used to authenticate the user/crypto officer login.	NVRAM (plain text) and RAM (plain text)	Overwriting the passwords with new ones, write to startup config, then reboot.
14	Certificates of Certificate Authorities (CAs)	ANSI X9.31	This is a public key certificate, using signatures from a certificate authority (CA), to verify certificates issued by the CA. Install the CA certificate prior to installing subordinate certificates.	NVRAM (plain text) and RAM (plain text)	Delete trustpoint from configuration via erase flash: command, write to startup config, then reboot.

Table 6 Critical Security Parameters Used by the PIX Security Appliance (continued)

#	Key/CSP Name	Generation/Algorithm	Description	Storage	Zeroization
15	PRNG Seed Key	Entropy	Seed key for X9.31 PRNG. Entropy is 192 bits (Triple-DES key length).	RAM (plain text)	Zeroized with generation of new seed.
16	Failover Key	Pre-shared secret	Used to encrypt and authenticate LAN-based failover.	NVRAM (plain text) and RAM (plain text)	Overwrite keys with new keys, or delete keys from the configuration via the erase flash: command. Write to startup configuration, then reboot.

Self-Tests

The PIX security appliances include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

[Table 7](#) lists the PIX security appliance power-on self-tests.

Table 7 Security Appliance Power-On Self-Tests

Implementation	Tests Performed
PIX security appliance software	<ul style="list-style-type: none"> • Software/firmware test • Bypass test • DSA KAT (signature/verification) • RSA KAT (signature/verification) • RSA KAT (encrypt/decrypt) • AES KAT • Triple DES KAT • SHA-1 KAT • HMAC SHA-1 KAT • PRNG KAT
VAC+ (Broadcom 5823)	<ul style="list-style-type: none"> • DSA KAT (verification) • RSA KAT (signature/verification) • RSA KAT (encrypt/decrypt) • AES KAT • Triple DES KAT • SHA-1 KAT • HMAC SHA-1 KAT

The PIX security appliances perform all power-on self-tests automatically at boot-up when FIPS mode is enabled. All power-on self-tests must be passed before a user/crypto officer can perform services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to the initialization of the LANs; this prevents the device from passing any data during a power-on self-test failure. In the unlikely event that a power-on self-test fails, an error message is displayed on the console followed by a system reboot.

Table 8 lists the conditional self-tests that the PIX security appliance performs.

Table 8 *PIX Security Appliance Conditional Self-Tests*

Implementation	Tests Performed
PIX security appliance software	<ul style="list-style-type: none"> • Pairwise key consistency test for RSA • Pairwise key consistency test for DSA • Continuous Random Number Generator Test for all RNGs • Conditional Bypass test
VAC+ (Broadcom 5823)	<ul style="list-style-type: none"> • Pairwise key consistency test for DSA

Mitigation of Other Attacks

The PIX security appliances do not claim to mitigate any attacks in a FIPS-approved mode of operation above and beyond the protection inherently provided by the PIX security appliance.

Secure Operation

The Cisco PIX 525 and PIX 535 security appliances meet FIPS 140-2 Level 1 requirements.

This section describes how to place and keep the PIX security appliance in a FIPS-approved mode of operation. Operating the PIX security appliance without maintaining the settings described in the [“Crypto Officer Guidance – System Initialization”](#) section on page 12 and [“Crypto Officer Guidance – System Configuration”](#) section on page 14 will remove the PIX security appliance from the FIPS-approved mode of operation.

The Crypto Officer must ensure that the PC that is used for the console connection is a stand-alone or a non-networked PC.

Crypto Officer Guidance – System Initialization

The PIX security appliances were validated with software version 7.0.4. This is the only allowable image for FIPS-approved mode of operation.

Initialize the system using the procedure below:

Step 1 Ensure the security context mode is set to single mode.

```
(config)#mode single
```

Step 2 Ensure the firewall mode is set to routed.

```
(config)#no firewall transparent
```

- Step 3** Disable the console output of system crash information.

```
(config)#crashinfo console disable
```

- Step 4** Enable “FIPS Mode” to allow the device to internally enforce FIPS-compliant behavior, such as running power-on self tests and bypass test.

```
(config)#fips enable
```

- Step 5** Install Triple DES/AES licenses to require the device to use Triple DES and AES (for data traffic and SSH). (See http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a00800b0d85.html for additional information on PIX licenses.)

- Step 6** Disable password recovery.

```
(config)#no service password-recovery
```

- Step 7** Set the configuration register to bypass ROMMON prompt at boot.

```
(config)#config-register 0x10011
```

- Step 8** If failover is to be enabled, define the failover key to ensure encryption of the link to redundant devices prior to enabling failover.

```
(config)#failover key hex <key>
```



Note

Failover is not required for FIPS mode of operation. Only LAN-based failover is allowed for FIPS mode of operation; serial link failover is not allowed in FIPS mode of operation. Failover must not be configured over the lowest-numbered interface, such as Ethernet 0; ports Ethernet 1 or above should be used. If the lowest-numbered interface is already implemented as the failover interface, the crypto officer should take the following action:

- Before upgrading to V7.0.4, copy the configuration to a location off the device
- Use a text editor to modify the interface configuration
- Change the failover cables to the specified failover interface
- Upgrade to V7.0.4 and reload the modified configuration

- Step 9** Enable AAA authorization for the console.

```
(config-terminal)#aaa authentication serial console LOCAL
(config-terminal)#username <name> password <password>
```

- Step 10** Enable AAA authorization for SSH and Telnet.

```
(config-terminal)#aaa authentication ssh console LOCAL
(config-terminal)#aaa authentication telnet console LOCAL
```

- Step 11** Enable AAA authorization for Enable mode.

```
(config-terminal)#aaa authentication enable console LOCAL
```

- Step 12** Specify Privilege Level 15 for crypto officer and Privilege Level 1 for user and set up username/password for each role.

```
(config-terminal)#username <name> password <password> privilege 15
(config-terminal)#username <name> password <password> privilege 1
```

- Step 13** Ensure passwords are at least 6 characters long. Replace all default passwords, such as enable and telnet with new passwords.

- Step 14** Install one VAC+ in any available Circuit Board Interface of the PIX security appliance, if one is not already installed.



Note The crypto officer may install any service cards that only provide a physical interface, such as PIX-1FE, PIX-1GE-66, PIX-4FE-66. The PIX security appliances are validated only with the VPN Acceleration Card PLUS (VAC+) for cryptographic acceleration; the legacy VAC is not supported in FIPS approved mode of operation.

- Step 15** Apply tamper-evident labels as described in the [“Applying Tamper-Evident Labels”](#) section on page 16.
- Step 16** Reboot the PIX security appliance.

Crypto Officer Guidance – System Configuration

Configure the system using the following procedure:

- Step 1** Assign users a Privilege Level of 1.

- Step 2** Define RADIUS and TACACS+ shared secret keys that are at least 6 characters long and secure all traffic between the PIX security appliance and the RADIUS/TACACS+ server via IPsec tunnel.



Note Use only if RADIUS/TACACS+ is configured.

- Step 3** Configure the TLS protocol for key derivation using HTTPS to protect administrative functions. Due to known issues relating to the use of TLS with certain versions of the Java plugin, we recommend that the customer upgrade to JRE 1.5.0_05 or later. Use the following settings when launching ASDM in a TLS-only environment with JRE 1.5.0_05:

- Configure the device to allow only TLSv1 packets.
`(config)# ssl server-version tlsv1-only`
- Uncheck SSL Version 2.0 in both the web browser and JRE security settings.
- Check TLS V1.0 in both the web browser and JRE security settings.

- Step 4** Configure the PIX security appliance to use SSHv2.

`(config)# ssh version 2`



Note All operators must still authenticate after remote access is granted.

- Step 5** Configure the PIX security appliance to assure that any remote connections via Telnet are secured through IPsec.

- Step 6** Configure the PIX security appliance to assure that only FIPS-approved algorithms are used for IPsec tunnels.

- Step 7** Configure the PIX security appliance to assure that error messages can only be viewed by an authenticated crypto officer.

- Step 8** Configure SNMP to always use a secure IPsec tunnel.

- Step 9** Disable the TFTP server and disable the HTTP server from performing system management.

- Step 10** Assure that installed digital certificates are signed using FIPS approved algorithms.
- Step 11** Assure that 512-bit and 768-bit RSA keys are not used.
- Step 12** Assure that the DSA algorithm uses at least a 512-bit modulus.

Approved Cryptographic Algorithms

The PIX security appliances support many different cryptographic algorithms. However, only the following FIPS-approved algorithms may be used:

- AES encryption/decryption
- Triple DES encryption/decryption
- SHA-1 hashing
- SHA-1 HMAC for hashed message authentication
- RSA signing and verifying
- DSA signing and verifying
- X9.31 for RNG

In addition, the following algorithms are FIPS-allowed:

- RSA encryption/decryption (used only for key transport)
- TLS for Layer 7 security



Note

Pursuant to the DES Transition Plan and the approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation, the DES algorithm must not be used in FIPS-approved mode of operation.

Each cryptographic implementation in the PIX security appliance software release with on-board acceleration has achieved the certifications listed in [Table 9](#).

Table 9 **Algorithm Certificates**

Algorithm	PIX Security Appliance Software	VPN Acceleration Card+
AES	320	209
Triple DES	384	298
SHA-1	393	285
HMAC SHA-1	124	15
RNG	143	Not supported
RSA	105	107
DSA	150	152

Non-FIPS Approved Algorithms

The PIX security appliances implement the following non-FIPS-approved cryptographic algorithms:

- DES
 - SSL
 - RC4
 - MD5
 - MD5 HMAC
 - Diffie-Hellman (allowed for use in FIPS mode) (key agreement; key establishment methodology provides between 70 and 112 bits of encryption strength)
 - RSA (allowed in FIPS mode for key transport) (key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength)
-

Applying Tamper-Evident Labels

All Critical Security Parameters (CSPs) are stored and protected within the PIX security appliance tamper-evident enclosure. The administrator is responsible for properly placing all tamper-evident labels to comply with the FIPS 140-2 security policy. The security labels mandatory for FIPS 140-2 compliance are provided in FIPS Kit (CVPNPIXASAFIPS/KIT). These security labels are very fragile and cannot be removed without clear signs of damage to the labels.

The crypto officer should inspect the tamper-evident labels periodically to verify they are intact and the serial numbers on the applied tamper-evident labels match the records in the security log.



Note

The tamper-evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the PIX security appliance will damage the tamper-evident seals or the material of the PIX security appliance cover. Because the tamper-evident seals have non-repeated serial numbers, they may be inspected for damage and compared against the applied serial numbers to verify that the device has not been tampered with. Tamper-evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices. The word Open may appear if the label was peeled back. Extra tamper-evident seals have been included in your FIPS kit to accommodate maintenance of your chassis.

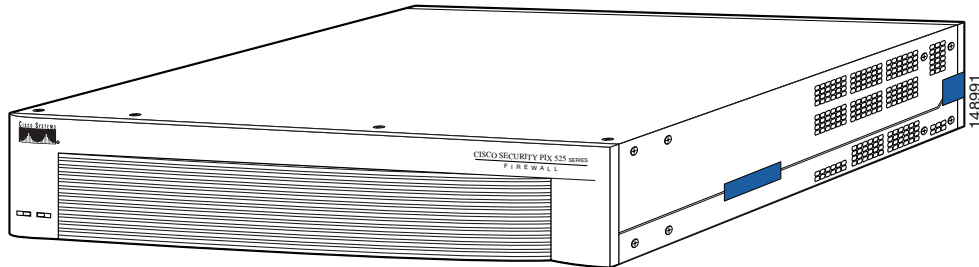
Apply the serialized tamper-evident labels by performing the steps in either the [“PIX 525” section on page 16](#) or the [“PIX 535” section on page 17](#).

PIX 525

- Step 1** Turn off and unplug the system before cleaning the chassis and applying labels.
- Step 2** Clean the chassis of any grease, dirt, or oil before applying the labels. Alcohol-based cleaning pads are recommended for this purpose.

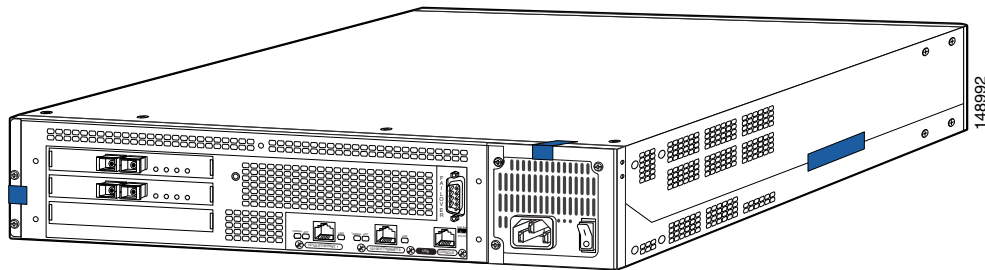
- Step 3** Apply one label on the side of the PIX security appliance as shown in [Figure 1](#). Apply a second label towards the back of the device and wrap it toward the back plate as shown in [Figure 1](#). See the same label from a different angle in [Figure 2](#).

Figure 1 Cisco PIX 525 Front Tamper-Evident Label Placement



- Step 4** On the back of the device, apply a label to cover the power supply, as shown in [Figure 2](#).
Step 5 Apply one label on the other side of the device as shown in [Figure 2](#).

Figure 2 Cisco PIX 525 Back Tamper-Evident Label Placement

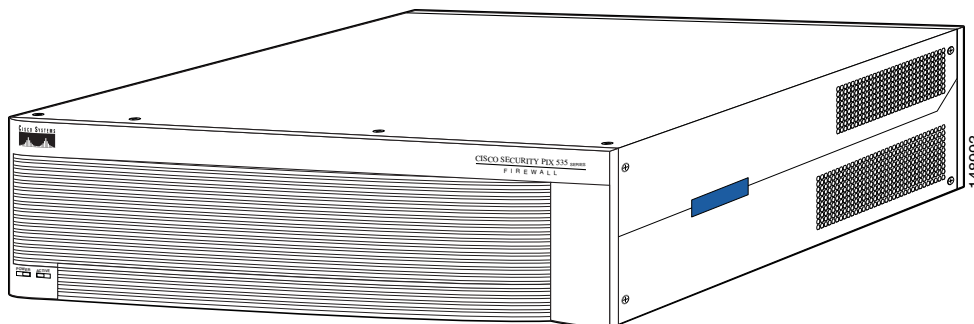


- Step 6** Record the serial numbers of the labels applied to the system in a security log.

PIX 535

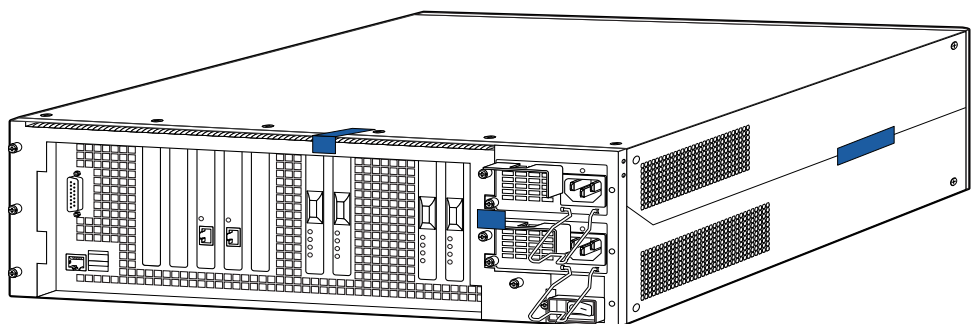
- Step 1** Turn off and unplug the system before cleaning the chassis and applying labels.
Step 2 Clean the chassis of any grease, dirt, or oil before applying the labels. Alcohol-based cleaning pads are recommended for this purpose.
Step 3 Apply one label on the side of the device as shown in [Figure 3](#), and a second label on the other side of the device as shown in [Figure 4](#).

Figure 3 Cisco PIX 535 Front Tamper-Evident Label Placement



Step 4 On the back of the device, apply labels to cover the power supplies and the removable component tray as shown in [Figure 4](#).

Figure 4 Cisco PIX 535 Back Tamper-Evident Label Placement



Step 5 Record the serial numbers of the labels applied to the system in a security log.

Related Documentation

This document deals only with operations and capabilities of the PIX security appliance in the technical terms of a FIPS 140-2 cryptographic device security policy.

More information is available on the PIX security appliance from the following sources:

- PIX security appliance software:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/tsd_products_support_series_home.html
- PIX security appliance licenses:
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_data_sheet09186a00800b0d85.html
- NIST Cryptographic Module Validation Program website contains contact information for answers to technical or sales-related questions for the PIX security appliance. (See <http://csrc.nsl.nist.gov/cryptval/>.)

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

Definitions

AES—Advanced Encryption Standard

CMVP—Cryptographic Module Validation Program

CSP—Critical Security Parameter

DES—Data Encryption Standard

DSA—Digital Signature Algorithm

FIPS—Federal Information Processing Standard

HMAC—Hashed Message Authentication Code

HTTP—Hyper Text Transfer Protocol

IKE—Internet Key Exchange

KAT—Known Answer Test

LED—Light Emitting Diode

MAC—Message Authentication Code

NIST—National Institute of Standards and Technology

NVLAP—National Voluntary Laboratory Accreditation Program

NVRAM—Non-volatile Random Access Memory

PRNG—Pseudo-Random Number Generator

RAM—Random Access Memory

RSA—Rivest Shamir and Adleman method for asymmetric encryption

Service Card—A service card may provide additional interfaces, feature acceleration or additional services. Service cards may take a Circuit Board form factor for PIX security appliances

SHA—Secure Hash Algorithm

SSL—Secure Sockets Layer

TLS—Transport Layer Security

Trustpoint—A trustpoint represents a CA identity and possibly a device identity, based on a certificate issued by the CA. When certificates are exchanged, the PIX/ASA device follows the trustpoint path upwards until it reaches the root CA to validate the certificate.

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Copyright © 2007 Cisco Systems, Inc.
All rights reserved.