



FIPS 140-2 Non-Proprietary Security Policy for the Cisco PIX 515/515E Security Appliance

Introduction

This is a non-proprietary Cryptographic Module Security Policy for the PIX515/515E, referred to in this document as the PIX security appliance, devices, modules, or appliances. This security policy describes how the PIX security appliance meet the security requirements of FIPS 140-2 and how to run the device in a FIPS 140-2 mode of operation.

This policy was prepared as part of the Level 2 FIPS 140-2 validation of the PIX515/515E security appliance.

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:

- [FIPS 140-2 Submission Package, page 2](#)
- [Overview, page 2](#)
- [Security Appliance Validation Level, page 3](#)
- [Physical Characteristics and Security Appliance Interfaces, page 3](#)
- [Roles and Services, page 5](#)
- [Authentication Mechanisms, page 6](#)
- [Cryptographic Key Management, page 7](#)
- [Self-Tests, page 10](#)
- [Mitigation of Other Attacks, page 11](#)



- [Secure Operation, page 11](#)
- [Approved Cryptographic Algorithms, page 13](#)
- [Non-FIPS Approved Algorithms, page 14](#)
- [Tamper-Evidence, page 15](#)
- [Related Documentation, page 16](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 16](#)
- [Definitions, page 17](#)

FIPS 140-2 Submission Package

The security policy document is one document in 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 Documentation, Obtaining Support, and Security Guidelines”](#) section on page 16 for more information.

Overview

The market-leading Cisco PIX security appliance delivers 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 purpose-built appliances provide multiple integrated security and networking services, including:

- Advanced application-aware firewall services
- Market-leading Voice over IP (VoIP) and multimedia security
- Robust site-to-site and remote-access IPSec VPN connectivity
- Award-winning resiliency
- Intelligent networking services
- Flexible management solutions

The Cisco PIX515/515E security appliances are validated with the VPN Acceleration Card+ (VAC+), which delivers high-performance, hardware-accelerated IP Security (IPSec) VPN support for state-of-the-art international cryptographic standards and highly scalable VPN tunnel aggregation in a solution that comes integrated with, or as an upgrade for, most models of the market-leading Cisco PIX security appliance. Ranging from solutions for small to midsize businesses (SMBs) to large enterprises and service providers, the Cisco PIX security appliance offers extensible platforms that provide robust, enterprise-class integrated network security services and solid investment protection. The Cisco PIX VAC+ takes full advantage of this extensibility and maximizes platform investment protection by off

loading computationally intensive VPN cryptographic functions. This enables the Cisco PIX security appliances to deliver higher-performance stateful inspection firewall services, advanced application and protocol inspection, inline intrusion protection, and robust multimedia and voice security services.

Among their capabilities, PIX515/515E security appliances offer the use of Online Certificate Status Protocol (OCSP). This provides an alternative to a Certificate Revocation List for obtaining the revocation status of X.509 digital certificates. Rather than requiring a client to download a complete and often large certificate revocation list, OCSP localizes the certificate status on a Validation Authority, which it queries for the status of a specific certificate. Use of OCSP for VPN tunnel establishment has been reviewed and approved for FIPS mode operation.

Security Appliance Validation Level

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

Table 1 Validation Level by Section

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

Physical Characteristics and Security Appliance Interfaces

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 and the "backplane" of the case which are not designed to accommodate a removable interface or service card, and 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](#):

Table 2 Cisco PIX515/515E Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 WIC/VIC/HWIC Interfaces 0-1 Circuit Board Interfaces 0-1	Data Input Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 WIC/VIC/HWIC Interfaces 0-1 Circuit Board Interfaces 0-1	Data Output Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 1 WIC/VIC/HWIC Interfaces 0-1 Circuit Board Interfaces 0-1 Power Switch Com 1 (Console Port)	Control Input Interface
10/100BaseTX Ethernet 0 10/100BaseTX Ethernet 0 100Mbps LED 10/100BaseTX Ethernet 0 ACT LED 10/100BaseTX Ethernet 1 10/100BaseTX Ethernet 1 100Mbps LED 10/100BaseTX Ethernet 1 ACT LED WIC/VIC/HWIC Interfaces 0-1 Circuit Board Interfaces 0-1 Power LED System Activity LED Network LED Com 1 (Console Port)	Status Output Interface
Main Power Plug	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 a 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 5](#), and the [“User Services” section on page 5](#).

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, shut down 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

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 the following:

- **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 3](#).

Table 3 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 Roles 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																	

rwd: r = read, w = write, d = delete.

Authentication Mechanisms

The PIX security appliance supports either a password or digital certificates for authenticating operators. 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, ASDM, or WebVPN) and provide a password.

[Table 4](#) describes the estimated strength of the authentication mechanisms.

Table 4 *Estimated Strength of Authentication Mechanism*

Authentication Type	Strength
Username Password mechanism	Passwords must be a minimum of 6 characters (see the “ Secure Operation ” section on page 11). 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. This is also valid for RADIUS or TACACS+ shared secret keys.
Certificate based authentication	The PIX security appliance supports a public key based authentication with 1024 and 2048 (for RSA) bit keys. A 1024-bit RSA key has at least 80-bits of equivalent strength. The probability of a successful random attempt is $1/2^{80}$, which is less than 1/1,000,000. A 2048-bit RSA key has at least 112-bits of equivalent strength. The probability of a successful random attempt is $1/2^{112}$, which is less than 1/1,000,000.
HMAC-SHA-1	With at least 80-bits of equivalent strength, the probability of a successful random attempt is $1/2^{80}$, which is less than 1/1,000,000.

The PIX security appliance provides protection against password guessing within a one-minute period. Specifically:

- Using passwords: It is possible for an unauthorized user to enter one password per second. This would result in 60 attempts per one minute period. This would leave a probability of one in 500 million. thus, the probability of an authentication within a one-minute period is much less than one in 100,000.
- Using HMAC-SHA-1 for IPSec packets: The PIX modules process 156,000 packets per second. The HMAC SHA-1 algorithm provides 80 bits of security, thus the probability of a successful random attempt is one in $(2^{80})/156,000$. Thus, the probability of a successful random authentication within a one-minute period is much less than one in 100,000.
- Using RSA digital signatures for IKE: Similar to HMAC-SHA-1, the probability of a successful random authentication within a one-minute period is $(2^{80})/156,000$, which is much smaller than one in 100,000.

Cryptographic Key Management

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

[Table 5](#) lists the critical security parameters used by the PIX security appliance.

Table 5 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 module itself and also used in IPSec, TLS, and SSH negotiations. The module supports 512, 768, 1024 and 2048 bit key sizes (512- and 768-bit key lengths are not to be used in FIPS mode)	Private Key - NVRAM (plaintext) and RAM (plaintext) Public Key - NVRAM (plaintext) and RAM (plaintext)	Private Key - crypto key zeroize, write to startup config, then reboot Public Key - delete trustpoint from configuration, write to startup config, then reboot
2	Failover Key	Pre-shared secret	Used to encrypt and authenticate LAN-based failover	NVRAM (plaintext) and RAM (plaintext)	Deleting keys from the configuration via erase flash: command (or replacing), write to 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), and 5 (1536 bits) are supported. Group 1 must not be used in FIPS mode of operation.	RAM (plain text)	Resetting or rebooting the PIX security appliance.
4	Public keys	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 TDES, AES, & ECDH	Used in HTTPS connections	RAM (plain text)	Resetting or rebooting the PIX security appliance.
6	SSH Session Keys	ANSI X9.31 / TDES-AES	SSH keys	RAM (plain text)	Resetting or rebooting the PIX security appliance.
7	IPSec authentication keys	ANSI X9.31 / TDES-AES / DH / ECDH	Exchanged using the IKE protocol and the public/private key pairs. These are TDES or AES keys.	RAM (plain text)	Resetting or rebooting the PIX security appliance.
8	IPSec traffic keys	ANSI X9.31 / TDES-AES / DH / ECDH	Exchanged using the IKE protocol and the public/private key pairs. These are TDES or AES keys.	RAM (plain text)	Resetting or rebooting the PIX security appliance.

Table 5 Critical Security Parameters Used by the PIX Security Appliance (continued)

#	Key/CSP Name	Generation/Algorithm	Description	Storage	Zeroization
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)	Deleting keys from the configuration via erase flash: command (or replacing), write to startup config, then reboot
10	IKE Authentication key	Generated using IKE (X9.31 + HMAC-SHA-1 + DH + ECDH). Algorithms: TDES, 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-SHA-1 + DH + ECDH). Algorithms: TDES, 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)	Delete keys from the configuration via the erase flash: command (or replacing), write to startup config, then reboot
13	Username/ Passwords	Secret	Critical security parameters used to authenticate the user/crypto-officer logging in on to the machine.	NVRAM (plain text) and RAM (plain text)	Overwriting the passwords with new ones, write to startup config, then reboot
14	Public Key Certificates of Certificate Authorities (CAs)	ANSI X9.31	Necessary to verify certificates issued by them; the CA's certificate should be installed before installing the certificate issued by it.	NVRAM (plain text) and RAM (plain text)	Delete trustpoint from configuration via erase flash: command, write to startup config, then reboot
15	PRNG Seed Key	Entropy (192 bits - TDES length)	Seed key for X9.31 PRNG	RAM (plain text)	Zeroized with generation of new seed
16	ECDH Key Pairs	ANSI X9.31 / DH	Key agreement for IKE; ECDH group 7 (K-163)	RAM (plain text)	Resetting or rebooting the PIX security appliance.

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 6](#) lists the PIX security appliance power-on self-tests.

Table 6 Security Appliance Power-On Self-Tests

Implementation	Tests Performed
PIX security appliance software	<ul style="list-style-type: none"> • Software/firmware Test • Bypass Test • RSA KAT (signature/verification) • RSA KAT (encrypt/decrypt) • AES KAT • TDES KAT • SHA-1 KAT • HMAC SHA-1 KAT • PRNG KAT
VAC+ (Broadcom 5823)	<ul style="list-style-type: none"> • RSA KAT (signature/verification) • RSA KAT (encrypt/decrypt) • AES KAT • TDES 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 LAN's interfaces; 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 7](#) lists the conditional self-tests that the PIX security appliance performs.

Table 7 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 • Continuous Random Number Generator Test for the FIPS-approved RNG and non-approved RNGs • Conditional Bypass test
VAC+ (Broadcom 5823)	<ul style="list-style-type: none"> • Pairwise key consistency test for RSA

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 PIX515/515E security appliances meet FIPS 140-2 Level 2 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 11 and [“Crypto Officer Guidance – System Configuration”](#) section on page 12 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 adaptive security appliance software version 7.2.2.18 (file name: pix722-18.bin) and the previous version 7.0.4 (file name: pix704.bin). These are the only allowable images for FIPS-approved mode of operation.

To initialize the system, the crypto officer must perform the following steps:

-
- Step 1** Ensure the security context mode is set to single mode by entering the following command:
`(config)# mode single`
 - Step 2** Ensure the firewall mode is set to routed mode by entering the following command:
`(config)# no firewall transparent`
 - Step 3** Disable the console output of system crash information by entering the following command:
`(config)# crashinfo console disable`
 - Step 4** Install TDES/AES licenses to require the device to use TDES and AES (for data traffic and SSH).
 - Step 5** Enable “FIPS Mode” to allow the device to internally enforce FIPS-compliant behavior, such as running power-on self tests and bypass test, by entering the following command:
`(config)# fips enable`
 - Step 6** Disable password recovery by entering the following command:
`(config)# no service password-recovery`
 - Step 7** Set the configuration register to bypass ROMMON prompt at boot by entering the following command:
`(config)# config-register 0x10011`
 - Step 8** Define the failover key to ensure encryption of the link to redundant modules prior to enabling failover by entering the following command:
`(config)# failover key hex <key>`



Note Failover is not required for FIPS mode of operation. If failover is to be enabled, then the above configuration should be followed. Also, only LAN-based failover is allowed for FIPS mode of operation; serial link failover is not allowed in FIPS mode of operation.

Step 9 Enable AAA authorization for the console by entering the following command:

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

Step 10 Enable AAA authorization for SSH and Telnet by entering the following command:

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

Step 11 Enable AAA authorization for Enable mode by entering the following command:

```
(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 by entering the following command:

```
(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.

Step 14 All default passwords (e.g., enable, Telnet) should be replaced with new passwords.

Step 15 Install a VAC+ card if one is not already installed.



Note Before applying Tamper Evidence Labels, the Crypto Officer may install any physical interface module (such as the PIX-1FE, PIX-1GE-66, or the PIX-4FE-66 cards) along with the required VPN Acceleration Card PLUS (VAC+) for cryptographic acceleration. The original VAC is not supported in the FIPS-approved mode of operation.

Step 16 Apply tamper-evident labels as described in the [“Tamper-Evidence” section on page 15](#).

Step 17 Reboot the PIX security appliance.

Crypto Officer Guidance – System Configuration

To configure the system, perform the following steps:

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 when using HTTPS to protect administrative functions. Due to known issues relating to the use of TLS with certain versions of the Java plugin, it is recommended that the customer upgrade to JRE 1.5.0_05 or later. The following configuration settings are known to work 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
(config)# ssl client-version tlsv1-only
```

- Uncheck the SSL Version 2.0 check box in both the web browser and JRE security settings.
- Check the TLS V1.0 check box in both the web browser and JRE security settings.

Step 4 Configure the PIX security appliance to use SSHv2 by entering the following command:

```
(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. This is accomplished by configuring the ISAKMP policy to use Diffie-Hellman Group 2, 5, or 7.

```
(config)# isakmp policy <priority>
sw8-5520 (config-isakmp-policy)# group <num>
```



Note <priority> is an integer between 1 and 65535. <num> is the Diffie-Hellman group number 2, 5, or 7. Group 1 should not be used in FIPS mode of operation.

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 servers.

Step 10 Disable HTTP for performing system management in FIPS mode of operation. HTTPS with TLS should always be used for Web-based management.

Step 11 Ensure that installed digital certificates are signed using FIPS approved algorithms.

Step 12 Ensure that 512-bit and 768-bit RSA keys are not used.

Approved Cryptographic Algorithms

The appliances support many different cryptographic algorithms; however, only FIPS approved algorithms may be used in the FIPS mode of operation. The following cryptographic algorithms are to be used:

- AES encryption/decryption
- TDES encryption/decryption
- SHA-1 hashing
- HMAC SHA-1 for hashed message authentication

- RSA signing and verifying
- X9.31 for RNG

In addition, the following algorithms are FIPS-allowed:

- TLS for Layer 7 security
- Diffie-Hellman (allowed for use in FIPS mode) (key agreement; key establishment methodology provides 80 or 96 bits of encryption strength; non-compliant less than 80-bits of equivalent strength). Diffie-Hellman Group 1 (768-bit) is not approved for the FIPS mode of operation.
- ECDH (allowed for use in FIPS mode) (key agreement; key establishment methodology provides 80 bits of encryption strength).
- RSA encryption/decryption (allowed in FIPS mode for key transport) (key wrapping; key establishment methodology provides 80 or 112 bits of encryption strength, non-compliant less than 80 bits of encryption strength).



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 should not be used in FIPS approved mode of operation. The DES algorithm must not be used when the TDES/AES licenses are installed.

Each cryptographic implementation in the PIX security appliance software and VAC+ module has achieved the certifications listed in [Table 8](#).

Table 8 **Algorithm Certificates**

Algorithm	PIX Security Appliance Software	VPN Acceleration Card +
AES	536	209
TDES	538	298
SHA-1	606	285
HMAC SHA-1	283	15
RNG	309	Not supported
RSA	242	107

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 80 or 96 bits of encryption strength; non-compliant less than 80-bits of equivalent strength). Diffie-Hellman Group 1 (768-bit) is not approved for the FIPS mode of operation.

- ECDH (allowed for use in FIPS mode) (key agreement; key establishment methodology provides 80 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, non-compliant less than 80 bits of encryption strength).

Tamper-Evidence

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. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit (Cisco-FIPS-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.



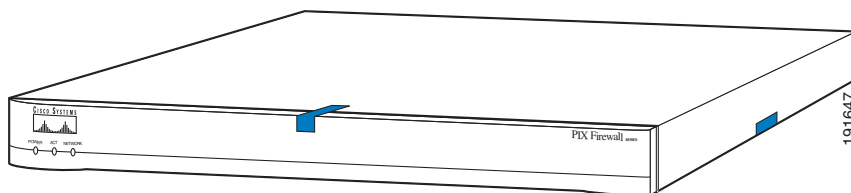
Note

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.

To apply the serialized tamper-evident labels, perform the following steps:

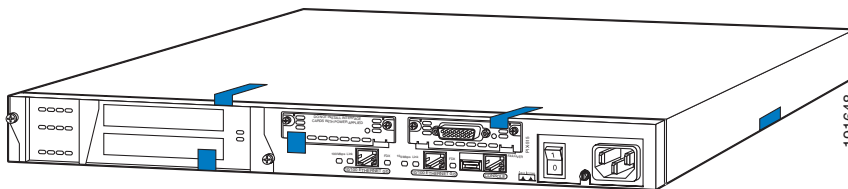
- Step 1** Turn off and unplug the system before cleaning the chassis and applying labels.
- Step 2** Clean the chassis of any grease, dirt, or oil before applying the labels. Alcohol-based cleaning pads are recommended for this purpose.
- Step 3** Apply a label on the front of the chassis so that the label covers the front plate and the top of the PIX515/515E chassis. See [Figure 1](#).
- Step 4** Apply a label to cover the PIX515/515E side and bottom portions of the chassis. See [Figure 1](#).

Figure 1 Cisco PIX 515/515E Front Tamper-Evident Label Placement



- Step 5** On the back of the chassis, apply labels to cover the interface slots. See [Figure 2](#).
- Step 6** Apply a label to cover the PIX515/515E side and bottom portions of the case on the opposite side as in Step 4. See [Figure 2](#).

Figure 2 Cisco PIX 515/515E Back Tamper-Evident Label Placement



Step 7 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 (hardware):
http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/tsd_products_support_series_home.html
- 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
- The 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.ncsl.nist.gov/cryptval/>.)

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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>

Definitions

AAA—Authentication, Authorization, and Accounting

AES—Advanced Encryption Standard

CMVP—Cryptographic Module Validation Program

CSP—Critical Security Parameter

DES—Data Encryption Standard

DH—Diffie-Hellman

ECDH—Eliptic Curve Diffie Hellman

FIPS—Federal Information Processing Standard

HMAC—Hash Message Authentication Code

HTTP—HyperText Transfer Protocol

ISAKMP—Internet Security Association and Key Management Protocol

KAT—Known Answer Test

LED—Light Emitting Diode

MAC—Message Authentication Code

NIST—National Institute of Standards and Technology

NVRAM—Non-Volatile Random Access Memory

OCSP—Online Certificate Status Protocol

PIX—Private Internet eXchange

RAM—Random Access Memory

RNG—Random Number Generator

RSA—Rivest Shamir and Adleman method for asymmetric encryption

SCEP—Simple Certificate Enrollment Protocol

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 appliance.

SHA—Secure Hash Algorithm

SSL—Secure Sockets Layer


TDES—Triple Data Encryption Standard

TLS—Transport Layer Security

Trustpoint—Represents a Certification Authority (CA) identity and possibly a device identity, based on a certificate issued by the CA. When certificates are exchanged, the ASA device follows the trustpoint path upwards until it reaches the root CA to validate the certificate.

VAC—VPN Acceleration Card

VPN—Virtual Private Network

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

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, 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, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, 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. (0601R)

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