



FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASA 5500 Series Security Appliance

Introduction

This is a non-proprietary Cryptographic Module Security Policy for Cisco ASA 5510, ASA 5520, and ASA 5540 security appliances. This policy describes how the Cisco ASA 5500 series security appliances meet the requirements of FIPS 140-2. This document also includes instructions for configuring the security appliance in FIPS 140-2 mode. This policy was prepared as part of the Level 2 FIPS 140-2 validation for the Cisco ASA 5500 series security appliances.



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.

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

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 7](#)
- [Authentication Mechanisms, page 8](#)
- [Cryptographic Key Management, page 9](#)
- [Self-Tests, page 11](#)
- [Mitigation of Other Attacks, page 12](#)
- [Secure Operation, page 12](#)
- [Non-FIPS Approved Algorithms, page 15](#)



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

© 2005 Cisco Systems, Inc. All rights reserved.

- [Tamper Evidence, page 16](#)
- [Related Documentation, page 17](#)
- [Definition List, page 17](#)
- [Documentation Feedback, page 18](#)
- [Cisco Product Security Overview, page 18](#)
- [Obtaining Technical Assistance, page 19](#)
- [Obtaining Additional Publications and Information, page 21](#)
- [Definition List, 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 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 19](#) for more information.

Overview

The Cisco ASA 5500 series security appliance leverages Cisco's expertise in security and VPN solutions, and integrates the latest technologies from Cisco PIX 500 series security appliances, Cisco IPS 4200 Series Intrusion Prevention Systems, and Cisco VPN 3000 series concentrators.

The Cisco ASA 5500 series security 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 ASA 5500 series security appliance is a high-performance, multifunction security appliance family delivering converged firewall, IPS, network anti-virus and VPN services. As a key component of the Cisco Self-Defending Network, it provides proactive threat mitigation that stops attacks before they spread through the network, controls network activity and application traffic, and delivers flexible VPN connectivity while remaining cost-effective and easy-to-manage.

In a single platform, the Cisco ASA 5500 series security appliance offers the following:

- Market-proven firewall, IPS, network anti-virus, and VPN capabilities
- Adaptive identification and mitigation services architecture providing granular policy control and future services extensibility
- Reduced deployment, operating costs, and complexity

Security Appliance Validation Level

Table 4 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

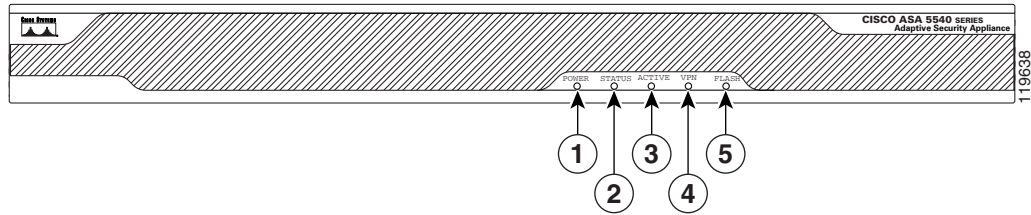
Physical Characteristics and Security Appliance Interfaces

The Cisco ASA 5500 series security appliance family delivers enterprise-class security for medium business-to-enterprise networks in a modular, purpose-built appliance. Its versatile one-rack unit (1RU) design supports up to 8 10/100/1000 Gigabit Ethernet interfaces (on the ASA5520 and ASA5540) and 1 10/100 Fast Ethernet Management interface, making it an excellent choice for businesses requiring a cost-effective, resilient security solution with demilitarized zone (DMZ) support.

Each appliance is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the “top,” “front,” “left,” “right,” and “bottom” surfaces of the case; all portions of the “backplane” of the case which are not designed to accommodate a removable interface or Cisco ASA 5500 series security appliance; and the inverse of the three-dimensional space within the case that would be occupied by an installed Cisco ASA 5500 series security appliance. The cryptographic boundary includes the connection apparatus between the Cisco ASA 5500 series security appliance and the motherboard/daughterboard that hosts the Cisco ASA 5500 series security appliance, but the boundary does not include the Cisco ASA 5500 series security appliance itself. In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed modular Cisco ASA 5500 series security appliance.

Figure 1 shows the ASA 5500 adaptive security appliance front panel LEDs.

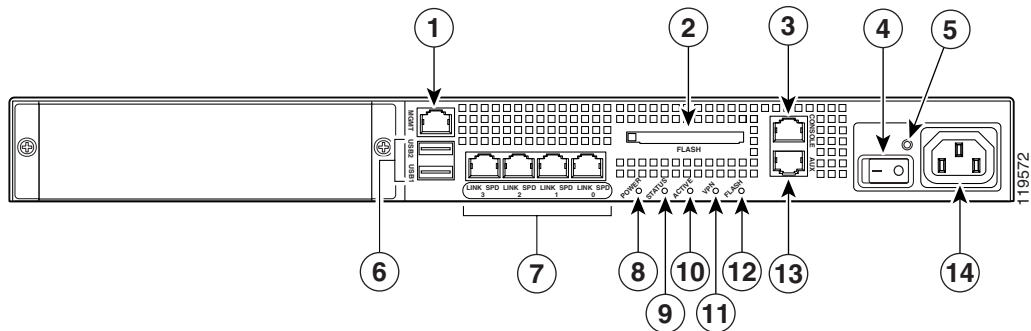
Figure 1 ASA 5500 Adaptive Security Appliance Front Panel LEDs



	LED	Color	State	Description
1	Power	Green	On	The system has power.
2	Status	Green	Flashing	The power-up diagnostics are running or the system is booting
			Solid	The system has passed power-up diagnostics.
			Amber	Solid
3	Active	Green	Flashing	There is network activity.
4	VPN	Green	Solid	VPN tunnel is established.
5	Flash	Green	Solid	The CompactFlash is being accessed.

Figure 2 shows the ASA 5500 adaptive security appliance rear panel LEDs and ports.

Figure 2 ASA 5500 Adaptive Security Appliance Rear Panel LEDs and Ports (AC Power Supply Model Shown)

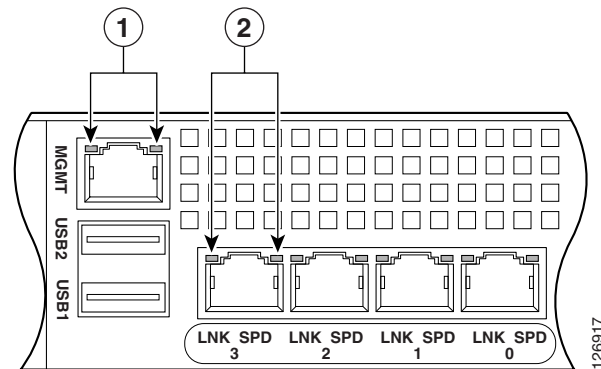


1	Management port ¹	6	USB 2.0 interfaces ²
2	External CompactFlash slot	7	Network interfaces ³
3	Serial Console port	8	Power indicator LED
4	Power switch	9	Status indicator LED
5	Power indicator LED	10	Active LED

1. The management 0/0 interface is a FastEthernet interface designed for management traffic only.
2. Not supported at this time.
3. GigabitEthernet interfaces, from right to left, GigabitEthernet 0/0, GigabitEthernet 0/1, GigabitEthernet 0/2, and GigabitEthernet 0/3.

Figure 3 shows the adaptive security appliance rear panel LEDs.

Figure 3 ASA 5500 Adaptive Security Appliance Rear Panel Link and Speed Indicator LEDs



1	MGMT indicator LEDs	2	Network interface LEDs.
----------	---------------------	----------	-------------------------

Table 2 lists the rear MGMT and Network LEDs.

Table 2 Link and Speed LEDs

Indicator	Color	Description
Left side	Solid green	Physical link
	Green flashing	Network activity
Right side	Not lit	10 Mbps
	Green	100 Mbps
	Amber	1000 Mbps



Note

The ASA 5510 adaptive security appliance supports only 10/100BaseTX. The ASA 5520 and the ASA 5540 support 1000BaseT.

Each security appliance provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the security appliance 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 3](#):

Table 3 *Cisco ASA 5500 Series Security Appliance Physical Interface/Logical Interface Mapping*

Physical Interface	FIPS 140-2 Logical Interface
GigabitEthernet 0-3 Multi-Function Service Card (MFSC) Interface MGMT Port Compact Flash Type 1 Com 1 (Console Port)	Data Input Interface
GigabitEthernet 0-3 Multi-Function Service Card (MFSC) Interface MGMT Port Compact Flash Type 1 Com 1 (Console Port)	Data Output Interface
GigabitEthernet 0-3 Multiple Service Function (MFS) Interface MGMT Port Power Switch Reset Switch Com 1 (Console Port)	Control Input Interface
GigabitEthernet 0-3 Multi-Function Service Card (MFSC) Interface MGMT Port Ethernet LEDs Power LED Status LED VPN LED Active LED CF Active LED Com 1 (Console Port)	Status Output Interface
Power Plug	Power Interface
USB Port Com 2 (Aux Port) ¹	Unused Interface

1. Physical interface not functional

Roles and Services

The security appliance 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 security appliance that operators may assume: a Crypto Officer role and User role. The security appliance supports role-based authentication, and the respective services for each role are described in the “[Crypto Officer Services](#)” section on page 7, and the “[User Services](#)” section on page 7.

Crypto Officer Services

The Crypto Officer role is responsible for the configuration and maintenance of the 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 Security Appliance:** Define network interfaces and settings; set the protocols the 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, memory status, packet statistics, review accounting logs, and view physical interface status.
- **Manage the Security Appliance:** Log off users, shut down or reload the 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 plain text packets to be sent from specified IP address.
- **Install Cisco 5500 Series Security Appliance:** Remove tamper evident seals to install or replace Cisco ASA 5500 series security appliances.

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 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.

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

Table 4 Cisco ASA 5500 Series Adaptive Security Appliance Validation Level by Section

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																	

148385

Authentication Mechanisms

The security appliance supports either a password or digital certificates for authenticating IPSec users. To log on to the appliances 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	Passwords must be a minimum of 6 characters (see Secure Operation section of this document). 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
Certificate based authentication	The security appliance supports a public key based authentication with 512, 768, 1024, and 2048 (for RSA) bit keys, and thus the probability of a false positive from a random correct guess s greater than 1 in 1,000,000.

Cryptographic Key Management

The appliances use a variety of Critical Security Parameters during operation.

Table 6 lists the cryptographic keys used by the Cisco ASA 5500 series security appliance.

Table 6 Cryptographic Keys Used by the ASA 5500 Adaptive Security Appliance

#	Key/CSP Name	Generation/Algorithm	Description	Storage	Zeroization
1	RSA public/private keys	ANSI X9.31/RSA	Identity certificates for the security appliance itself and also used in IPSec, TLS, and SSH negotiations. The security appliance supports 512, 768 and 1024 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.
2	DSA public/private keys	ANSI X9.31/DSA	Identity certificates for the security appliance itself and also used in IPSec negotiations.	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	RAM (plain text)	Resetting or rebooting the security appliance
4	Public keys	DSA / RSA	Public keys of peers	RAM (plain text)	Resetting or rebooting the security appliance
5	TLS Traffic Keys	Generated using the TLS protocol (X9.31PRNG + HMAC-SHA1 + HMAC-MD5 + either DH or RSA) Algorithm: Also 3DES & AES	Used in HTTPS connections	RAM (plain text)	Resetting or rebooting the security appliance
6	SSH Session Keys	ANSI X9.31 / 3DES-AES	SSH keys	RAM (plain text)	Resetting or rebooting the security appliance
7	IPSec authentication keys	ANSI X9.31 / 3DES-AES / DH	Exchanged using the IKE protocol and the public/private key pairs. These are 3DES or AES keys.	RAM (plain text)	Resetting or rebooting the security appliance
8	IPSec traffic keys	ANSI X9.31 / 3DES-AES / DH	Exchanged using the IKE protocol and the public/private key pairs. These are 3DES or AES keys.	RAM (plain text)	Resetting or rebooting the security appliance

Table 6 Cryptographic Keys Used by the ASA 5500 Adaptive Security Appliance (continued)

#	Key/CSP Name	Generation/Algorithm	Description	Storage	Zeroization
9	IKE pre-shared 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-SHA1+DH). Algorithms: 3DES, AES, SHA-1	Used to encrypt and authenticate IKE negotiations	RAM (plain text)	Resetting or rebooting the security appliance
11	IKE Encryption Key	Generated using IKE (X9.31+HMAC-SHA1+DH). Algorithms: 3DES, AES, SHA-1	Used to encrypt IKE negotiations	RAM (plain text)	Resetting or rebooting the security appliance
12	RADIUS and TACACS+ shared secret keys	Shared Secret	Used for authenticating the RADIUS or TACACS+ server to the 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)	Deleting keys from the configuration via erase flash: command (or replacing), write to startup config, then reboot.
13	Usernames/ 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	Necessary to verify certificates issued by the CA. Install the CA's 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.
15	PRNG Seed Key	Entropy	Seed key for X9.31 PRNG	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)	Deleting keys from the configuration via erase flash: command (or replacing), write to startup config, then reboot.

Self-Tests

The 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 insure all components are functioning correctly.

[Table 7](#) lists the ASA 5500 adaptive security appliance power-on self-tests.

Table 7 Security Appliance Power-On Self-Tests

Implementation	Tests Performed
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 • 3DES KAT • SHA-1 KAT • HMAC SHA-1 KAT • PRNG KAT
ASA On-board (Cavium Nitrox Lite)	<ul style="list-style-type: none"> • DSA KAT (signature/verification) • RSA KAT (signature/verification) • AES KAT • 3DES KAT • SHA-1 KAT • HMAC SHA-1 KAT • PRNG KAT

The security appliances perform all power-on self-tests automatically at boot 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 security appliance 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 security appliance reboot.

[Table 8](#) lists the conditional self-tests that the ASA 5500 adaptive security appliance performs.

Table 8 ASA 5500 Adaptive Security Appliance Conditional Self-Tests

Implementation	Tests Performed
Security Appliance Software	<ul style="list-style-type: none"> • Pairwise consistency test for RSA • Pairwise consistency test for DSA • Continuous Random Number Generator Test for the FIPS-approved RNG • Conditional Bypass test
ASA On-board (Cavium Nitrox Lite)	<ul style="list-style-type: none"> • Pairwise consistency test for RSA • Pairwise consistency test for DSA • Continuous Random Number Generator Test for the FIPS-approved RNG

Mitigation of Other Attacks

The security appliances do not claim to mitigate any attacks in a FIPS-approved mode of operation.

Secure Operation

The Cisco ASA 5510, ASA 5520, and ASA 5540 adaptive security appliances meet FIPS 140-2 Level 2 requirements. This section describes how to place and keep the security appliances in a FIPS-approved mode of operation. Operating the security appliances without maintaining the following settings will remove the security appliances from the FIPS-approved mode of operation.

Crypto Officer Guidance – System Initialization

The security appliances were validated with adaptive security appliance software Version (file name: asa704-k8.bin). This is the only allowable image for FIPS-approved mode of operation.

The Crypto Officer must configure and enforce the following initialization steps:

-
- 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, using the following command:
- ```
(config)#crashinfo console disable
```
- Step 4** Install 3DES/AES licenses to require the security appliance to use 3DES and AES (for data traffic and SSH).
- Step 5** Enable “FIPS Mode” to allow the security appliance to internally enforce FIPS-compliant behavior, such as run power-on self-tests and bypass test, using the following command:

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

**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 0x1001
```

**Step 8** Define the failover key to ensure encryption of the link to redundant security appliances prior to enabling failover.

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



**Note**

The **failover key hex <key>** command should be entered with failover disabled. If failover is already enabled, the **failover key hex <key>** command will be replicated to the standby unit and will result in the key being sent off-device in clear-text, violating FIPS.



**Note**

Failover is not required for FIPS mode of operation. If failover is to be enabled, then the configuration in [Step 8](#) 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. Failover should 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.

**Step 14** All default passwords, such as enable and telnet, should be replaced with new passwords.

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

**Note**

The Crypto Officer may install any modules that only provide a physical interface, such as PIX-1FE, PIX-1GE-66, and PIX-4FE-66.

**Step 16** Reboot the security appliance.

## Crypto Officer Guidance – System Configuration

To operate in FIPS mode, the Crypto Officer must 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 traffic between the security appliance and the RADIUS/TACACS+ server via IPsec tunnel.

**Note**

Perform this step only if RADIUS/TACACS+ is configured, otherwise proceed to [Step 3](#).

**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, we recommend that you 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:

a. Configure the device to allow only TLSv1 packets using the following command:

```
(config)# ssl server-version tlsv1-only
```

b. Uncheck SSL Version 2.0 in both the web browser and JRE security settings.

c. Check TLS V1.0 in both the web browser and JRE security settings.

**Step 4** Configure the security appliance to use SSHv2. Note that all operators must still authenticate after remote access is granted.

**Step 5** Configure the security appliance such that any remote connections via Telnet are secured through IPsec.

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

**Step 7** Configure the security appliance such that error messages can only be viewed by an authenticated Crypto Officer.

**Step 8** Configure SNMP v1 or v2c over a secure IPsec tunnel may be employed for authenticated, secure SNMP operations.

**Step 9** Disable the FTP, and TFTP servers as well as HTTP for performing system management.

**Step 10** Ensure that installed digital certificates are signed using FIPS approved algorithms (SHA-1).

**Step 11** Ensure that 512-bit and 768-bit RSA keys are not used.

**Step 12** Ensure that the DSA algorithm uses at least a 512-bit modulus.

## Approved Cryptographic Algorithms

The appliances support many different cryptographic algorithms; however, only FIPS approved algorithms may be used. Use the following cryptographic algorithms:

- AES encryption/decryption
- 3DES encryption/decryption
- SHA-1 hashing
- SHA-1 HMAC for hashed message authentication
- RSA signing and verifying
- DSA signing and verifying
- RSA encryption/decryption
- DSA encryption/decryption
- X9.31 for RNG
- 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 should not be used in FIPS approved mode of operation. The DES algorithm must not be used when the 3DES/AES licenses are installed.

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

**Table 9**      **Algorithm Certificates**

| Algorithm  | Adaptive Security Appliance Software | ASA On-board Acceleration |
|------------|--------------------------------------|---------------------------|
| AES        | 320                                  | 105                       |
| 3 DES      | 384                                  | 217                       |
| SHA-1      | 393                                  | 196                       |
| SHA-1 HMAC | 124                                  | 125                       |
| RNG        | 143                                  | 144                       |
| RSA        | 105                                  | 106                       |
| DSA        | 150                                  | 151                       |

## Non-FIPS Approved Algorithms

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

- DES
- SSL
- RC4

- MD5
- MD5 HMAC
- Diffie-Hellman (allowed for use in FIPS mode)

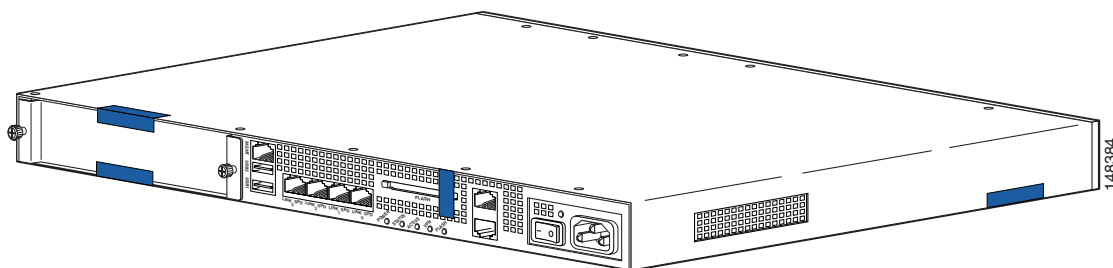
## Tamper Evidence

All Critical Security Parameters are stored and protected within each appliance’s 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 (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.

Apply the serialized tamper evident labels as follows (see [Figure 4](#)):

**Figure 4 Cisco ASA 5500 Series Security Appliance Tamper Evident Label Placement**



- 
- 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 tamper evident labels. Alcohol-based cleaning pads are recommended for this purpose.
  - Step 3** Apply a label to cover the security appliance’s bottom/side portions of the case.
  - Step 4** On the back of the security appliance, apply one label to cover the CompactFlash slot and two labels to cover the Multiple Service Function slot.
  - Step 5** Record the serial numbers of the labels applied to the system in a security log.

The tamper evident seals are produced from a special thin gauge vinyl with self-adhesive backing. Any attempt to open the device will damage the tamper evident seals or the material of the 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 security appliance 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.

## Related Documentation

This document deals only with operations and capabilities of the security appliance in the technical terms of a FIPS 140-2 cryptographic security appliance security policy. More information is available on the security appliance from the sources listed in this section and from the following source:

- The NIST Cryptographic Module Validation Program website (<http://csrc.ncsl.nist.gov/cryptval/>) contains contact information for answers to technical or sales-related questions for the security appliance.

## 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.

## Definition List

AES—Advanced Encryption Standard

ASA—Adaptive Security Appliance

CMVP—Cryptographic Module Validation Program

CSP—Critical Security Parameter

DES—Data Encryption Standard

FIPS—Federal Information Processing Standard

HTTP—Hyper Text Transfer Protocol

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

RAM—Random Access Memory

RSA—Rivest Shamir and Adleman method for asymmetric encryption

SCEP—Simple Certificate Enrollment Protocol

security appliance—A security appliance may provide additional interfaces, feature acceleration or additional services. Security appliances may take a Circuit Board form factor SSM (for ASA appliances)

SHA—Secure Hash Algorithm

SSL—Secure Sockets Layer

SSM—Security Services Module

TLS—Transport Layer Security

---

---

This document is to be used in conjunction with the documents listed in the [“Related Documentation”](#) section.

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, ASIST, 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, Empowering the Internet Generation, 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, StrataView Plus, TeleRouter, 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. (0502R)

Copyright © 2008 Cisco Systems, Inc.  
All rights reserved.