FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASA 5505 and 5550 Security Appliances

Introduction

This is a non-proprietary Cryptographic Module Security Policy for Cisco ASA 5505 and ASA 5550 security appliances. This policy describes how the Cisco ASA 5505 and 5550 security appliances meet the requirements of FIPS 140-2. This document also includes instructions for configuring the security appliances in FIPS 140-2 mode.

This policy was prepared as part of the Level 2 FIPS 140-2 validation for the Cisco ASA 5505 and 5550 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 security appliances. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

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:

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

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 22 for more information.

Overview

The Cisco ASA 5505 and 5550 security appliances leverage 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.

Among their capabilities, Cisco ASA 5505 and 5550 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.

ASA 5505

The Cisco ASA 5505 Adaptive Security Appliance is a next-generation, full-featured security appliance for small business, branch office, and enterprise teleworker environments. The Cisco 5505 delivers high-performance firewall, IPSec and SSL VPN, and rich networking services in a modular, "plug-and-play" appliance. Using the integrated Web-based Cisco Adaptive Security Device Manager,

the Cisco ASA 5505 can be rapidly deployed and easily managed, enabling businesses to minimize operations costs. The Cisco ASA 5505 features a flexible 8-port 10/100 Fast Ethernet switch, whose ports can be dynamically grouped to create up to three separate VLANs for home, business, and Internet traffic for improved network segmentation and security. The Cisco ASA 5505 provides two Power over Ethernet (PoE) ports, enabling simplified deployment of Cisco IP phones with zero-touch secure voice over IP (VoIP) capabilities, and deployment of external wireless access points for extended network mobility. The Cisco ASA 5505 also provides significant expandability and investment protection through its modular design, similar to the rest of the Cisco ASA 5500 Series, offering both an external expansion slot and multiple USB ports that enable the addition of services in the future.

ASA 5550

The ASA 5550 security appliance provides 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 ASA 5550 security appliance is a high-performance, multifunction security appliance 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 ASA 5550 security appliance offers the following:

- Market-proven firewall 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 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

Table 1   *Validation Level by Section*

No.	Area Title	Level
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

ASA 5505

The ASA 5505 security appliance delivers enterprise-class security for small business and large enterprise networks in a modular, purpose-built appliance. The ASA 5505 security appliance's compact design includes eight Fast Ethernet interfaces for businesses requiring a cost-effective security solution.

Each Cisco ASA 5505 is a multi-chip standalone device, 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 Security Service Card (SSC); and the inverse of the three-dimensional space within the case that would be occupied by an installed SSC. The cryptographic boundary includes the connection apparatus between the SSC and the motherboard/daughterboard that hosts the SSC, but the boundary does not include the SSC itself. In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed SSC.

Each security appliance provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the security appliances 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 for the ASA 5505 security appliance are described in Table 2:

Table 2   *Cisco ASA 5505 Physical Interface/Logical Interface Mapping*

Physical Interface	FIPS 140-2 Logical Interface
Fast Ethernet 0-7	Data Input Interface
Fast Ethernet 0-7	Data Output Interface
Fast Ethernet 0-7 Power Switch Reset Switch Com 1 (Console Port)	Control Input Interface

Table 2   Cisco ASA 5505 Physical Interface/Logical Interface Mapping (continued)

Physical Interface	FIPS 140-2 Logical Interface
Fast Ethernet 0-7 Ethernet LEDs Power LED Status LED VPN LED Active LED SSC LED Com 1 (Console Port)	Status Output Interface
Power Plug	Power Interface
USB Port	Unused Interface

ASA 5550

The ASA 5550 security appliance delivers enterprise-class security for small business and large enterprise networks in a modular, purpose-built appliance. The ASA 5550 security appliance's versatile one-rack unit (1RU) design includes two 4GE card interfaces, supporting eight 10/100/1000 Gigabit Ethernet interfaces and one 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 ASA 5550 security appliance is a multi-chip standalone device with a fixed configuration, and the cryptographic boundary is defined as encompassing the entire chassis.

Each security appliance provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the security appliances 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 for the ASA 5550 security appliance are described in Table 3:

Table 3   Cisco ASA 5550 Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
GigabitEthernet0/ 0-3 GigabitEthernet1/ 0-3 MGMT Port Compact Flash Type 1 Com 1 (Console Port)	Data Input Interface
GigabitEthernet0/ 0-3 GigabitEthernet1/ 0-3 MGMT Port Compact Flash Type 1 Com 1 (Console Port)	Data Output Interface

Table 3   *Cisco ASA 5550 Physical Interface/Logical Interface Mapping (continued)*

Physical Interface	FIPS 140-2 Logical Interface
GigabitEthernet0/ 0-3 GigabitEthernet1/ 0-3 MGMT Port Power Switch Reset Switch Com 1 (Console Port)	Control Input Interface
GigabitEthernet0/ 0-3 GigabitEthernet1/ 0-3 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] Serial Failover Interface	Unused Interface

1.   Physical interface not functional

Roles and Services

The security appliances 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 appliances that operators may assume: a Crypto Officer role and User role. The security appliances support 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 appliances 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 appliances 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 SNMP queries to view SNMP MIB statistics, health, temperature, 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 appliances, 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 Service Card**: Remove tamper evident seals to install or replace any applicable service cards.

- **Run Self-Tests:** Execute Known Answer Tests for each FIPS approved algorithm.

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 appliances 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
- **Run Self-Tests:** Execute Known Answer Tests for each FIPS approved algorithm.

Critical Security Parameters

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 5505 and 5550 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
Role/Service																
User Role																
Status Functions		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
Directory Services		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
Define Roles and Filters		rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd	rwd
Status Functions		r	r	r	r	r	r	r	r	r	r	r	r	r	r	r
Manage the Module		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
Install Service Card																

r = read   w = write   d = delete

Authentication Mechanisms

The security appliances support either a password or digital certificates for authenticating IPSec users. To log on to the 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	Passwords must be a minimum of 6 characters (see Secure Operation section of this document). The password can consist of alphanumeric values (a-z, A-Z, 0-9) 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 security appliances support a public key based authentication with 1024 or 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 $1/1,000,000$.

Cryptographic Key Management

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

Table 6 lists the cryptographic keys used by the Cisco ASA 5505 and 5550 security appliances.

Table 6   *Cryptographic Keys Used by the ASA 5505 and 5550 Adaptive Security Appliances*

#	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 appliances support 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 (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	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

Table 6   Cryptographic Keys Used by the ASA 5505 and 5550 Adaptive Security Appliances (continued)

#	Key/CSP Name	Generation/ Algorithm	Description	Storage	Zeroization
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 security appliances
4	Public keys	RSA	Public keys of peers	RAM (plain text)	Resetting or rebooting the security appliances
5	TLS Traffic Keys	Generated using the TLS protocol (X9.31PRNG + HMAC-SHA1 + HMAC-MD5 + either DH or RSA); Algorithms: Triple-DES & AES	Used in HTTPS connections	RAM (plain text)	Resetting or rebooting the security appliances
6	SSH Session Keys	ANSI X9.31 / Triple-DES-AES	SSH keys	RAM (plain text)	Resetting or rebooting the security appliances
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 security appliances
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 security appliances
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: Triple-DES, AES, SHA-1	Used to encrypt and authenticate IKE negotiations	RAM (plain text)	Resetting or rebooting the security appliances
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 security appliances

Table 6   *Cryptographic Keys Used by the ASA 5505 and 5550 Adaptive Security Appliances (continued)*

#	Key/CSP Name	Generation/ Algorithm	Description	Storage	Zeroization
12	RADIUS and TACACS+ shared secret keys	Shared Secret	Used for authenticating the RADIUS or TACACS+ server to the security appliances 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	Public Key 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 (192 bits - Triple-DES length)	Seed key for X9.31 PRNG	RAM (plain text)	Zeroized with generation of new seed

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 ensure all components are functioning correctly.

Table 7 lists the ASA 5505 and 5550 adaptive security appliances power-on self-tests.

Table 7   *Security Appliance Power-On Self-Tests*

Implementation	Tests Performed
Security Appliance Software	• Software/firmware Test • Bypass Test • RSA KAT (signature/verification) • RSA KAT (encrypt/decrypt) • AES KAT • Triple-DES KAT • SHA-1 KAT • HMAC SHA-1 KAT • PRNG KAT

Table 7   *Security Appliance Power-On Self-Tests (continued)*

Implementation	Tests Performed
ASA On-board (Cavium Nitrox Lite)	• RSA KAT (signature/verification) • RSA KAT (encrypt/decrypt) • AES KAT • Triple-DES 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 LAN's interfaces; this prevents the security appliances 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 5505 and 5550 adaptive security appliance perform.

Table 8   *ASA 5505 and 5550 Adaptive Security Appliance Conditional Self-Tests*

Implementation	Tests Performed
Security Appliance Software	• Pairwise consistency test for RSA • Continuous Random Number Generator Test for the FIPS-approved RNG and non-approved RNGs • Conditional Bypass test
ASA On-board (Cavium Nitrox Lite)	• Pairwise consistency test for RSA • 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 above and beyond the protection inherently provided by the ASA security appliance.

Secure Operation

The Cisco ASA 5505 and 5550 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.

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

Crypto Officer Guidance – System Initialization

The Cisco ASA 5505 and 5550 security appliances were validated with adaptive security appliance software version 7.2.2.18 (file name: asa722-18-k8.bin), 7.2.4.18 (file name: asa724-18-k8.bin), and 7.2.4.30 (file name: asa724-30-k8.bin). These are the only allowable images 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 Triple-DES/AES licenses to require the security appliances to use Triple-DES and AES (for data traffic and SSH).

Step 5 Enable "FIPS Mode" to allow the security appliances 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 0x10011
```

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 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.

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.

Step 16 Reboot the security appliances.

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 appliances 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
(config)# ssl client-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 appliances to use SSHv2. Note that all operators must still authenticate after remote access is granted.

```
(config)# ssh version 2
```

Step 5 Configure the security appliances such that any remote connections via Telnet are secured through IPSec.

Step 6 Configure the security appliances such that only FIPS-approved algorithms are used for IPSec tunnels.

Step 7 Configure the security appliances such 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.

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 the 512-bit and 768-bit RSA keys are not used.

Approved Cryptographic Algorithms

The Cisco ASA 5505 and 5550 security appliances support many different cryptographic algorithms; however, only the following FIPS approved algorithms may be used while in the FIPS mode of operation:

- AES encryption/decryption
- Triple-DES encryption/decryption
- SHA-1 hashing
- SHA-1 HMAC for hashed message authentication
- RSA 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 should not be used in FIPS approved mode of operation. The DES algorithm must not be used when the Triple-DES/AES licenses are installed.

Each ASA 5505 security appliance has achieved the certifications listed in Table 9.

Table 9   ASA 5505 Algorithm Certificates

Algorithm	Adaptive Security Appliance Firmware		ASA On-board Acceleration
	7.2.2.18	**7.2.4.18 and 7.2.4.30**	
AES	536	1010	564
Triple-DES	538	779	559
SHA-1	606	968	630
SHA-1 HMAC	283	567	301
RNG	309	570	329
RSA	242	485	261

Each ASA 5550 security appliance has achieved the certifications listed in Table 10.

Table 10   *ASA 5550 Algorithm Certificates*

Algorithm	Adaptive Security Appliance Firmware		ASA On-board Acceleration
	7.2.2.18	**7.2.4.18 and 7.2.4.30**	
AES	536	1010	105
Triple-DES	538	779	217
SHA-1	606	968	196
SHA-1 HMAC	283	567	125
RNG	309	570	144
RSA	242	485	106

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) (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)

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 (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.

ASA 5505

Apply the serialized tamper evident label as follows (see Figure 1):

Figure 1   *Cisco ASA 5505 Security Appliance Tamper Evident Label Placement*
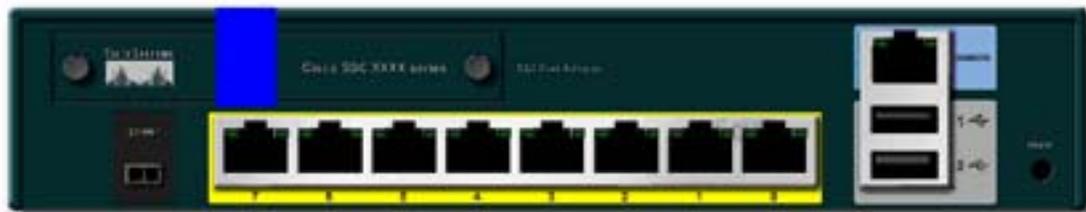
Step 1   Turn off and unplug the system before cleaning the chassis and applying labels.

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   On the back of the module, apply a label to cover the security appliances's SSC slots and top of the case.

Note   The Cisco ASA 5505 must be installed in an opacity shield/ventilation enclosure to obstruct viewing of internal components through the side air-ventilation holes of the chassis case. The user must install the ASA 5505 in the rack-mount enclosure to meet FIPS opacity requirements, but not necessarily install the mounted device in a rack. Refer to the Cisco ASA 5500 Series Hardware Maintenance Guide, Chapter 2, for specific rack installation instructions.

Step 4   Apply a tamper evidence label across one of the screws on the bottom of the ASA 5505 rack-mount enclosure (see Figure 2).

Figure 2   ***Bottom View of Rack-Mountable Enclosure with Tamper Evidence Label Placement***

Step 5   Record the serial numbers of the label 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 appliances 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 appliances 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.

ASA 5550

Apply the serialized tamper evident labels as follows (see Figure 3):

Figure 3   Cisco ASA 5550 Security Appliance Tamper Evident Label Placement
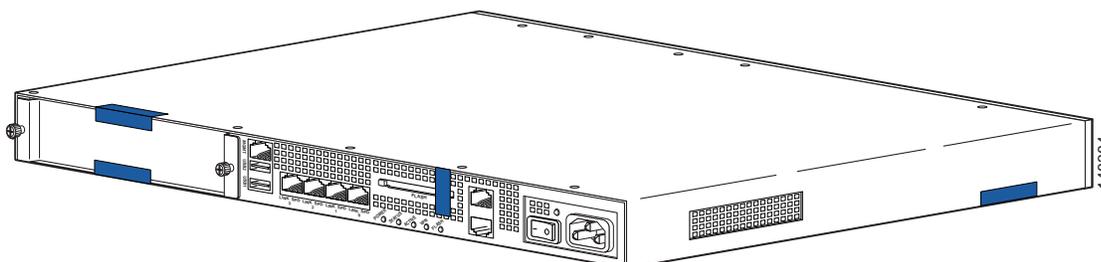
Step 1   Turn off and unplug the system before cleaning the chassis and applying labels.

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 appliances in the technical terms of a FIPS 140-2 cryptographic device security policy. More information is available on the security appliances 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 appliances.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page

at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

    http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

    http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

    http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

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

HMAC—Hash Message Authentication Code

HTTP—Hyper Text Transfer 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

OSCP—Online Certificate Status Protocol

RAM—Random Access Memory

RNG—Random Number Generator

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 appliance may take a Circuit Board form factor SSM (for ASA appliance)

SHA—Secure Hash Algorithm

SSC—Security Services Card

SSL—Secure Sockets Layer

SSM—Security Services Module

Triple-DES—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.