



FIPS 140-2 Non-Proprietary Security Policy for the Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, and 5580-40 Security Appliances

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation (Level 3 for Roles, Services and Authentication and Design Assurance)

Document Version: Version 1.1

October 4, 2010

INTRODUCTION

This is a non-proprietary Cryptographic Module Security Policy for CISCO ASA 5505, 5510, 5520, 5540, 5550, 5580-20, AND 5580-40 Security Appliances. This policy describes how Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, and 5580-40 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, 5510, 5520, 5540, 5550, 5580-20, and 5580-40 security appliances.

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

INTRODUCTION.....	2
FIPS 140-2 SUBMISSION PACKAGE	3
FIPS 140-2 NON-PROPRIETARY SECURITY POLICY FOR THE CISCO ASA 5505, 5510, 5520, 5540, 5550, 5580-20, AND 5580-40 SECURITY APPLIANCES	4
OVERVIEW	4
MODULE VALIDATION LEVEL	4
PHYSICAL CHARACTERISTICS AND MODULE INTERFACES	4
ROLES AND SERVICES	12
CRYPTO OFFICER SERVICES	12
USER SERVICES	13
UNAUTHENTICATED USER SERVICES	13
CRITICAL SECURITY PARAMETERS	13
CRYPTOGRAPHIC KEY MANAGEMENT	14
SELF-TESTS	17
MITIGATION OF OTHER ATTACKS.....	18
SECURE OPERATION	18
CRYPTO OFFICER GUIDANCE - SYSTEM INITIALIZATION	18
CRYPTO OFFICER GUIDANCE - SYSTEM CONFIGURATION	19
APPROVED CRYPTOGRAPHIC ALGORITHMS.....	20
NON-FIPS APPROVED ALGORITHMS ALLOWED FOR USE IN FIPS-MODE	21
NON-FIPS APPROVED ALGORITHMS	21
TAMPER EVIDENCE	21
ASA 5500 SERIES	22
RELATED DOCUMENTATION	25
OBTAINING DOCUMENTATION	25
CISCO.COM	25
PRODUCT DOCUMENTATION DVD.....	25
ORDERING DOCUMENTATION	26
DOCUMENTATION FEEDBACK	26
CISCO PRODUCT SECURITY OVERVIEW	26
REPORTING SECURITY PROBLEMS IN CISCO PRODUCTS	27

OBTAINING TECHNICAL ASSISTANCE	27
CISCO TECHNICAL SUPPORT & DOCUMENTATION WEBSITE	27
SUBMITTING A SERVICE REQUEST	28
DEFINITIONS OF SERVICE REQUEST SEVERITY	28
OBTAINING ADDITIONAL PUBLICATIONS AND INFORMATION	28

FIPS 140-2 Submission Package

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the 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 25 for more information.

FIPS 140-2 NON-PROPRIETARY SECURITY POLICY FOR THE CISCO ASA 5505, 5510, 5520, 5540, 5550, 5580-20, AND 5580-40 SECURITY APPLIANCES

Overview

The CISCO ASA 5505, 5510, 5520, 5540, 5550, 5580-20, AND 5580-40 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.

Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
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	3
11	Mitigation of Other Attacks	N/A

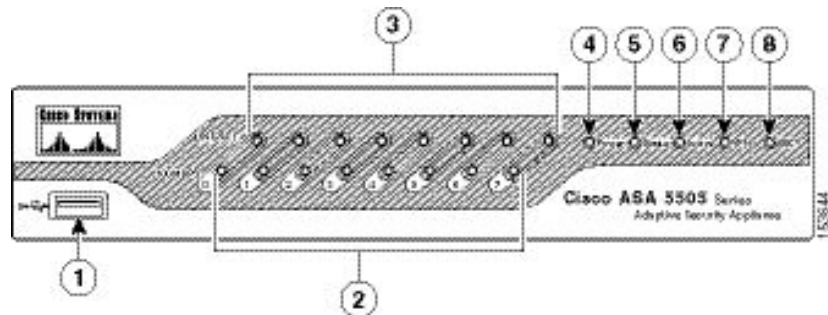
Table 1 – Validation Level by Section

Physical Characteristics and Module 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, 5505-5550) and four-rack unit (4RU, 5580-20, 5580-40) design supports up to 8 10/100/1000 Gigabit Ethernet interfaces (on the ASA5520 and ASA5540), 1 10/100 Fast Ethernet Management interface, and 4 10/100/1000 Gigabit Ethernet RJ45 interfaces, 4 Port Gigabit Ethernet fiber, and 2 10/100/1000 Gigabit Ethernet Management interface (on the 5580-20 and 5580-40) making it an excellent choice for businesses requiring a cost-effective, resilient security solution with demilitarized zone (DMZ) support.

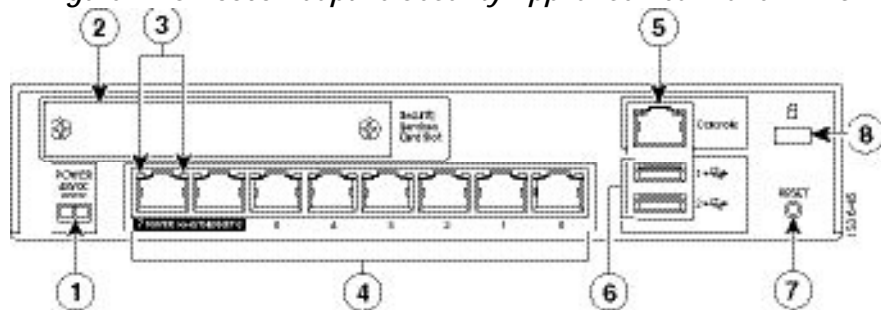
Each appliance is a multi-chip standalone security appliances, and the cryptographic boundary is defined as encompassing the "top," "front," "left," "right," and "bottom" surfaces of the case; all portions of the "backplane" of the case which are not designed to accommodate a removable interface or service card; and the inverse of the three-dimensional space within the case that would 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. In other words, the cryptographic boundary encompasses all hardware components within the case of the device except any installed modular service card.

Figure 1: ASA 5505 Adaptive Security Appliance Rear Panel LEDs



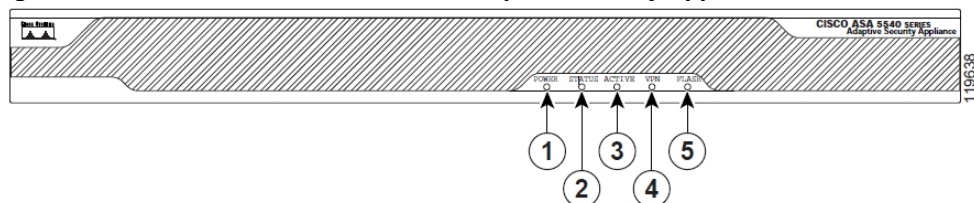
1	USB 2.0 interface	5	Status
2	100 Mbps	6	Active
3	LINK/ACT LEDs	7	VPN
4	Power	8	SSC

Figure 2 ASA 5505 Adaptive Security Appliance Rear Panel LEDs



1	Power 48VDC	5	Console Port
2	SSC Slot	6	USB 2.0 Interface
3	Network Interface LEDs	7	Reset Button
4	Network Interfaces	8	Lock Slot

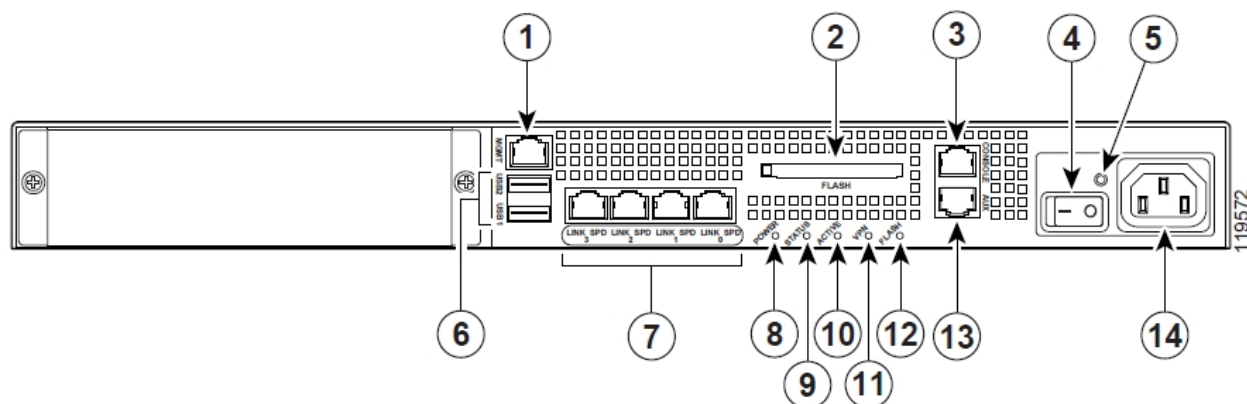
Figure 3 ASA 5510, 5520, 5540, and 5550 Adaptive Security Appliance Front Panel LEDs



	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	The power-up diagnostics have failed.
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 4 ASA 5510 , 5520, 5540, and 5550 Adaptive Security Appliance Rear Panel LEDs and Ports (AC Power Supply Model Shown)



1	Management port1	8	Power indicator LED
2	External CompactFlash slot	9	Status indicator LED
3	Serial Console port	10	Active LED
4	Power switch	11	VPN LED
5	Power indicator LED	12	Flash LED
6	USB 2.0 interfaces2	13	Aux Port
7	Network interfaces3	14	Power connector

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 5 ASA 5510, 5520, 5540, and 5550 Adaptive Security Appliance Rear Panel Link and Speed Indicator LEDs

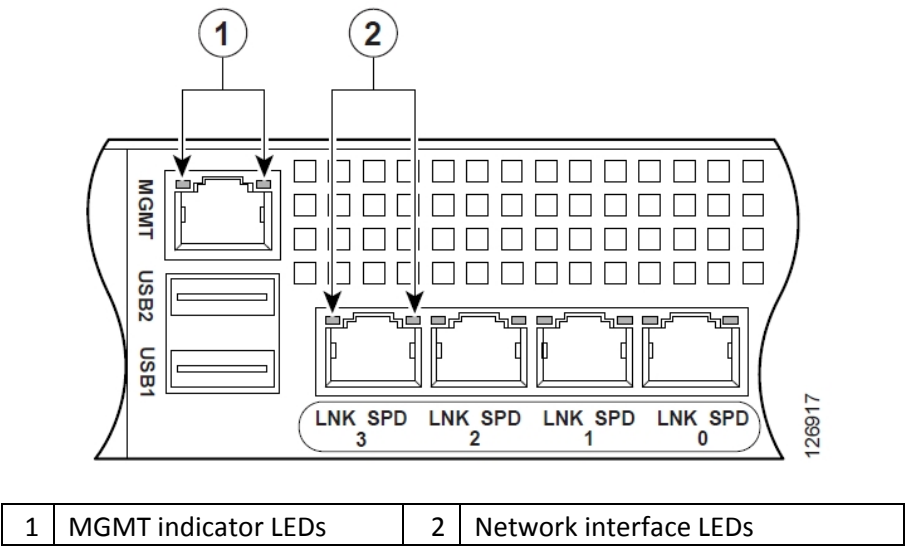


Table 2 Link and Speed LEDs.

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

Figure 6 ASA 5580 Adaptive Security Appliance Rear Panel LEDs

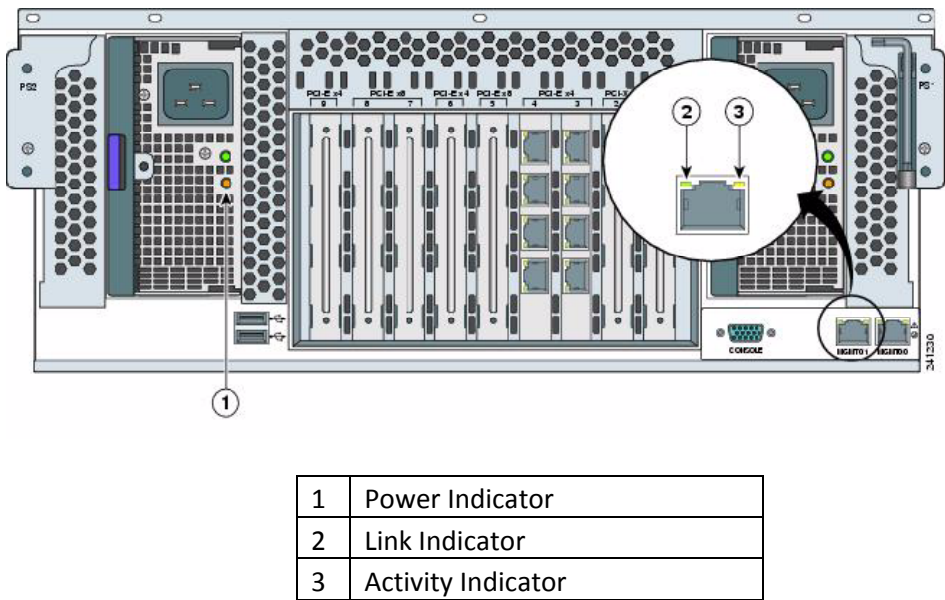
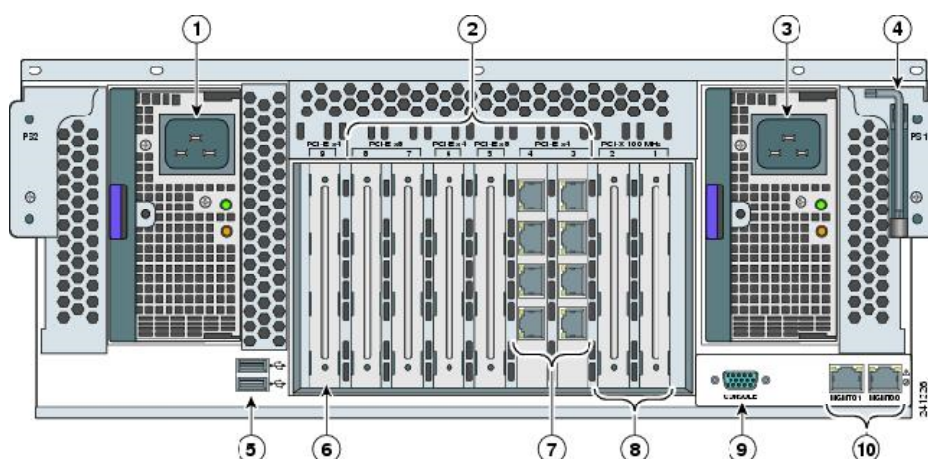
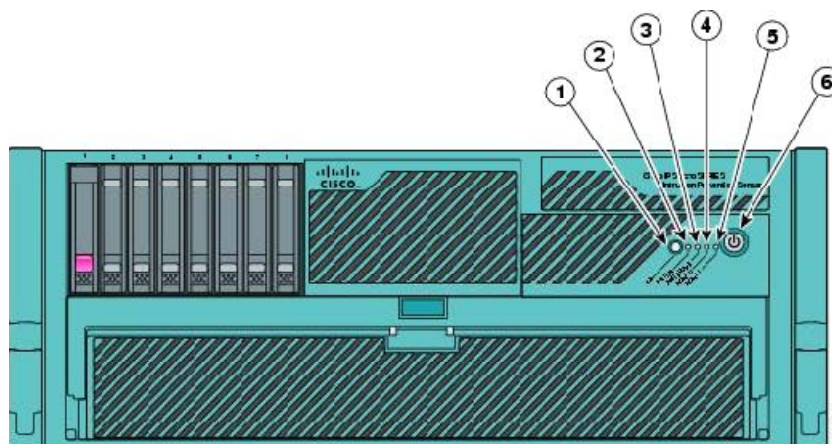


Figure 7 ASA 5580 Adaptive Security Appliance Rear Panel features



1	Power Supply	6	Reserved Slot
2	Interface Expansion Slots	7	Example of Populated Slot
3	Power Supply	8	Reserved Slot
4	T-15 Torx Screwdriver	9	Console port
5	USB Ports	10	Management ports

Figure 8 ASA 5580 Adaptive Security Appliance Front Panel LEDs



LED	Function
1	Active
2	System
3	Power Status
4	Management 0/0
5	Management 0/1
6	Power

Each module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module 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 5505 Series Security Appliance Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
FastEthernet 0-7 Security Services Module (SSM)* Console Port	Data Input Interface
FastEthernet 0-7 Security Services Module (SSM)* Console Port	Data Output Interface
FastEthernet 0-7 Reset Switch Console Port	Control Input Interface
FastEthernet 0-7 Ethernet LEDs Power LED Status LED VPN LED Active LED Console Port	Status Output Interface
Power Plug	Power Interface
USB Port	Unused Interface

* Disabled via TEL placement

Table 4 Cisco ASA 5510, 5520, and 5540 Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
FastEthernet 0-3 (ASA 5510) GigabitEthernet 0-3 (ASA 5520 and 5540) Security Services Module (SSM)* MGMT Port Compact Flash Console Port	Data Input Interface
FastEthernet 0-3 (ASA 5510) GigabitEthernet 0-3 (ASA 5520 and 5540) Security Services Module (SSM)* MGMT Port Compact Flash	Data Output Interface

Console Port	
FastEthernet 0-3 (ASA 5510) GigabitEthernet 0-3 (ASA 5520 and 5540) MGMT Port Power Switch Reset Switch Compact Flash Console Port	Control Input Interface
FastEthernet 0-3 (ASA 5510) GigabitEthernet 0-3 (ASA 5520 and 5540) MGMT Port Ethernet LEDs Power LED Status LED VPN LED Active LED CF Active LED Console Port	Status Output Interface
Power Plug	Power Interface
USB Port Aux Port ¹	Unused Interface

* Disabled via TEL placement

Table 5 Cisco ASA 5550 Security Appliance Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
GigabitEthernet (up to 8) Console Port MGMT Port Compact Flash	Data Input Interface
GigabitEthernet (up to 8) Console Port MGMT Port Compact Flash	Data Output Interface
GigabitEthernet (up to 8) MGMT Port Power Switch Reset Switch Compact Flash Console Port	Control Input Interface

GigabitEthernet (up to 8) MGMT Port Ethernet LEDs Power LED Status LED VPN LED Active LED CF Active LED Console Port	Status Output Interface
Power Plug	Power Interface
USB Port Aux Port ¹	Unused Interface

¹ Physical interface not functional

Table 6 Cisco ASA 5580 Security Appliance Physical Interface/Logical Interface Mapping

Physical Interface	FIPS 140-2 Logical Interface
GigabitEthernet (up to 24) 10GigabitEthernet (up to 12) MGMT Port 0/0 MGMT Port 0/1 Console Port	Data Input Interface
GigabitEthernet (up to 24) 10GigabitEthernet (up to 12) MGMT Port 0/0 MGMT Port 0/1 Console Port	Data Output Interface
GigabitEthernet (up to 24) 10GigabitEthernet (up to 12) MGMT Port 0/0 MGMT Port 0/1 Reset Switch Console Port	Control Input Interface
GigabitEthernet (up to 24) 10GigabitEthernet (up to 12) MGMT Port 0/0 MGMT Port 0/1 Ethernet LEDs Power LED System LED Management 0/0 LED Management 0/1 LED Active LED Console Port	Status Output Interface
Power Plug	Power Interface

USB Ports	Unused Interface
-----------	------------------

Roles and Services

The security appliances can be accessed in one of the following ways:

- Console Port
- Telnet over IPSec
- SSH v2
- ASDM via HTTPS/TLS

Authentication is identity-based. Each user is authenticated upon initial access to the module. 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 administrator of the security appliances assumes the Crypto Officer role in order to configure and maintain the router using Crypto Officer services, while the Users exercise only the basic User services. The module supports RADIUS and TACACS+ for authentication.

The User and Crypto Officer passwords and all shared secrets must each be at least eight (8) characters long, including at least one letter and at least one number character, in length (enforced procedurally). See the Secure Operation section for more information. If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 832,000,000. In order to successfully guess the sequence in one minute would require the ability to make over 13,000,000 guesses per second, which far exceeds the operational capabilities of the module. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence."

Additionally, when using RSA based authentication, RSA key pair has modulus size of 1024 bit to 2048 bit, thus providing between 80 bits and 112 bits of strength. Assuming the low end of that range, an attacker would have a 1 in 2^{80} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 1.8×10^{21} attempts per minute, which far exceeds the operational capabilities of the modules to support

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; provide for the entry and output of CSPs; 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, provide for the entry and output of CSPs, shutdown 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. Set up site to site VPN for IPv6.
- **Run Self-Tests:** Execute Known Answer Test on Algorithms within the cryptographic module.
- **SSL VPN (using TLSv1.0):** Configure SSL VPN parameters, provide entry and output of CSPs.
- **Local Certificate Authority:** Allows the ASA to be configured as a Root Certificate Authority and issue user certificates for SSL VPN use (AnyConnect and Clientless). The ASA can then be configured to require client certificates for authentication.

User Services

A user enters the system by accessing the console port with a terminal program or via IPSec protected Telnet or SSH v2 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 Test on Algorithms within the cryptographic module.

Unauthenticated User Services

The services for someone without an authorized role are to view the status output from the module's LED pins, perform bypass services and cycle power.

Critical Security Parameters

The services accessing the Critical Service Parameters (CSPs), the type of access, and which role accesses the CSPs, are listed in Table 3. CSPs are discussed more fully in Table 6.

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	CSP 17	CSP 18
Role/Service																			
User Role																			
Status Functions		r	r	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	r	r
Directory Services		r	r	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	rwd	rwd
Define Roles and Filters		rwd	rwd	rwd	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	r	r	r
Manage the Module		rwd	rwd	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	rwd	rwd

r = read w = write d = delete

Cryptographic Key Management

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

Table 7 *Cryptographic Keys Used by Cisco ASA 5505, 5510, 5520, 5540, 5550, 5580-20, AND 5580-40 Security Appliances*

#	Key/CSP Name	Generation/Algorithm	Description	Storage	Zeroization
1	RNG Seed	ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES Algorithms	Seed for X9.31 RNG	RAM (plain text)	Zeroized with generation of new seed
2	RNG Seed Key	ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES Algorithms	Seed key for X9.31 RNG	RAM (plain text)	Zeroized with generation of new seed
3	Diffie-Hellman Private Component	Diffie-Hellman	Key agreement for IKE, TLS, and SSH sessions. Diffie-Hellman 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	RSA 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)	Private Key - crypto key zeroize, write to startup config, then reboot.
5	Skeyid	Keyed SHA-1	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is terminated.	RAM (plain text)	Automatically after IKE session terminated.
6	skeyid_d	Keyed SHA-1	The IKE key derivation key for non ISAKMP security associations.	RAM (plain text)	Automatically after IKE session terminated.
7	ISAKMP 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.
8	IKE Authentication key	Generated using IKE (X9.31 + HMAC-SHA1 + Diffie-Hellman); Algorithms: Triple-DES, AES, SHA-1	Used to encrypt and authenticate IKE negotiations	RAM (plain text)	Resetting or rebooting the security appliances
9	IKE Encryption Key	Generated using IKE (X9.31 + HMAC-SHA1 + Diffie-Hellman); Algorithms: Triple-DES, AES, SHA-1	Used to encrypt IKE negotiations	RAM (plain text)	Resetting or rebooting the security appliances
10	IPSec authentication keys	ANSI X9.31 / Triple-DES-AES / Diffie-Hellman	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
11	IPSec traffic keys	ANSI X9.31 / Triple-DES-AES / Diffie-Hellman	Exchanged using the IKE protocol and the public/private key pairs. These are Triple-DES or	RAM (plain text)	Resetting or rebooting the security appliances

			AES keys.		
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	User passwords	Shared Secret	Critical security parameters used to authenticate the User/Crypto-Officer login.	NVRAM (plaintext or encrypted)	Overwriting the passwords with new ones, write to startup config, then reboot.
14	Enable password	Shared Secret	The plaintext password of the CO role. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
15	Enable secret	Shared Secret	The ciphertext password of the CO role. However, the algorithm used to encrypt this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password.	NVRAM (plaintext or encrypted)	Overwrite with new password
16	TLS pre-master secret	Shared Secret	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	DRAM (plaintext)	Automatically when session terminated.
17	TLS Traffic Keys	Generated using the TLS protocol (X9.31 RNG + HMAC-SHA1 + either Diffie-Hellman or RSA); Algorithms: Triple-DES & AES	Used in HTTPS connections	RAM (plain text)	Resetting or rebooting the security appliances

18	SSH v2 Session Keys	ANSI X9.31 / Triple-DES-AES	SSH keys	RAM (plain text)	Resetting or rebooting the security appliances
----	---------------------	-----------------------------	----------	------------------	--

Self-Tests

The modules 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 8 lists the modules power-on self-tests:

Table 8 *Cisco ASA 5500 Series Adaptive Security Appliance Power-On Self-Tests*

Implementation	Tests Performed
Security Appliance Software	Firmware Integrity Test Bypass Test RSA KAT (signature/verification) AES KAT Triple-DES KAT SHA-1 KAT HMAC SHA-1 KAT RNG KAT
ASA On-board (Cavium Nitrox Lite)	RSA KAT (signature/verification) AES KAT Triple-DES KAT SHA-1 KAT HMAC SHA-1 KAT RNG 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 9 *Cisco ASA 5500 Series Adaptive Security Appliance Conditional Self-Tests*

Implementation	Tests Performed
Security Appliance Firmware	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)	Continuous Random Number Generator Test for the 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 5500 Series meet overall 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 5500 series security appliances were validated with adaptive security appliance software version 8.3.2 (file names: asa832-k8.bin (for 5505, 5510, 5520, 5540, 5550) and asa832-smp-k8.bin (5580-20 and 5580-40)). 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 Enable AAA authorization for the console.

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

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

Step 9 Enable AAA authorization for SSH and Telnet.

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

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

Step 10 Enable AAA authorization for Enable mode.

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

Step 11 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 12 Ensure passwords are at least 6 characters long.

Step 13 All default passwords, such as enable and telnet, should be replaced with new passwords.

Step 14 Apply tamper evident labels as described in the [“Tamper Evidence” section on page 21](#).

Step 15 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 8 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 require 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 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
- HMAC-SHA-1 for hashed message authentication
- RSA signing and verifying
- RNG based on ANSI X9.31

Each ASA security appliances has achieved the certifications listed below in Table 10.

Table 10 Algorithm Certificates

Algorithm	Adaptive Security Appliance Software	ASA On-board Acceleration (5505)	ASA On-board Acceleration (5510, 5520, 5540, 5550)	ASA On-board Acceleration (5580-20, 5580-40)
-----------	---	--	---	--

AES	1394	564	105	1407
Triple-DES	954	559	217	960
SHA-1	1265	630	196	1277
HMAC SHA-1	818	301	125	828
RNG	763	329	144	772
RSA	680	261	106	684

Non-FIPS Approved Algorithms allowed for use in FIPS-mode

- Diffie-Hellman (allowed for use in FIPS mode)(key agreement; key establishment methodology provides between 80 and 112 bits of encryption strength; non-compliant less than 80-bits of equivalent strength).
- RSA (key wrapping; key establishment methodology provides 80 bits or 112 bits of encryption strength; non-compliant less than 80 bits of encryption strength)

Non-FIPS Approved Algorithms

The modules implement the following non-FIPS-approved cryptographic algorithms:

- DES
- RC4
- MD5
- MD5 HMAC

Note: Non-FIPS approved algorithms cannot be used in FIPS mode of operation.

Tamper Evidence

All Critical Security Parameters are stored and protected within each appliance's tamper evident enclosure. The Crypto Officer is responsible for properly placing all tamper evident labels. The security labels recommended for FIPS 140-2 compliance are provided in the FIPS Kit (Part Number DS-FIPS-KIT=), Revision -B0 (for ASA 5505, 5510, 5520, 5540 and 5550) and (ASA5580-FIPS-KIT=) for ASA 5580-20 and 5580-40. Both the FIPS kit includes 18 of the seals, as well as a document detailing the number of seals required per platform and placement information. Please be aware that the extra tamper evident labels/seals shall be securely stored by the Crypto Officer. These security labels are very fragile and cannot be removed without clear signs of damage to the labels. Further, opacity shields are required as follows:

1. The ASA 5505 model requires an additional 'clam-shell' typed of enclosure to ensure that the opacity requirements are met. This can be obtained by ordering the ASA 5505 FIPS Kit (ASA5505-FIPS-KIT=), Revision -A0
2. The ASA 5580-20 and 5580-40 require two opacity shields attached to the front and rear faces. This can be obtained by ordering the ASA5580-FIPS-KIT=.

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. The Tamper evident labels shall be applied as shown in the pictures below, for the module to operate in FIPS mode.

ASA model(s)	Number of Tamper Evident Labels
5505	2
5510, 5520, 5540, 5550	4
5580-20, 5580-40	16

ASA 5500 Series

Apply the serialized tamper evident labels as follows:

Figure 9 Cisco ASA 5505 Security Appliance Tamper Evident Label Placement



Figure 10 Cisco ASA 5505 Security Appliance Tamper Evident Label Placement, bottom view



Figure 11 Cisco ASA 5510, 5520, 5540, and 5550 Security Appliance Tamper Evident Label Placement

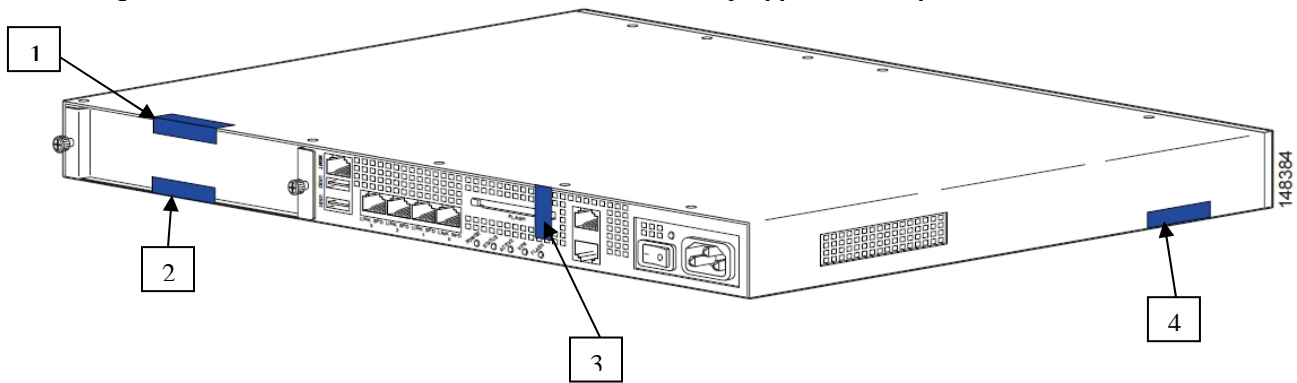


Figure 12 Cisco ASA 5580 Security Appliance Tamper Evident Label Placement (Front Face)

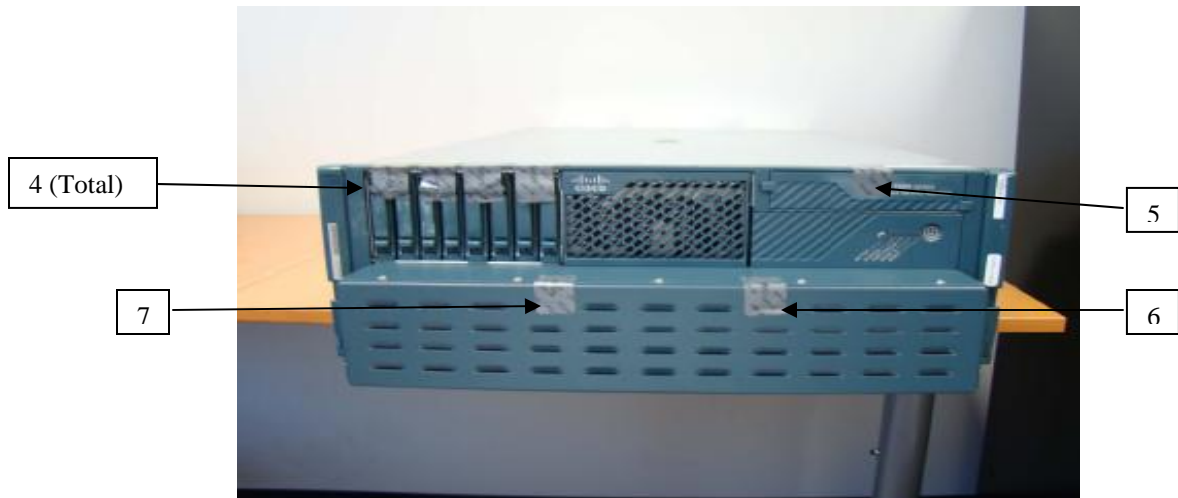


Figure 13 Cisco ASA 5580 Security Appliance Tamper Evident Label Placement (Back Face)



Figure 14 Cisco ASA 5580 Security Appliance Tamper Evident Label Placement (Side Face)

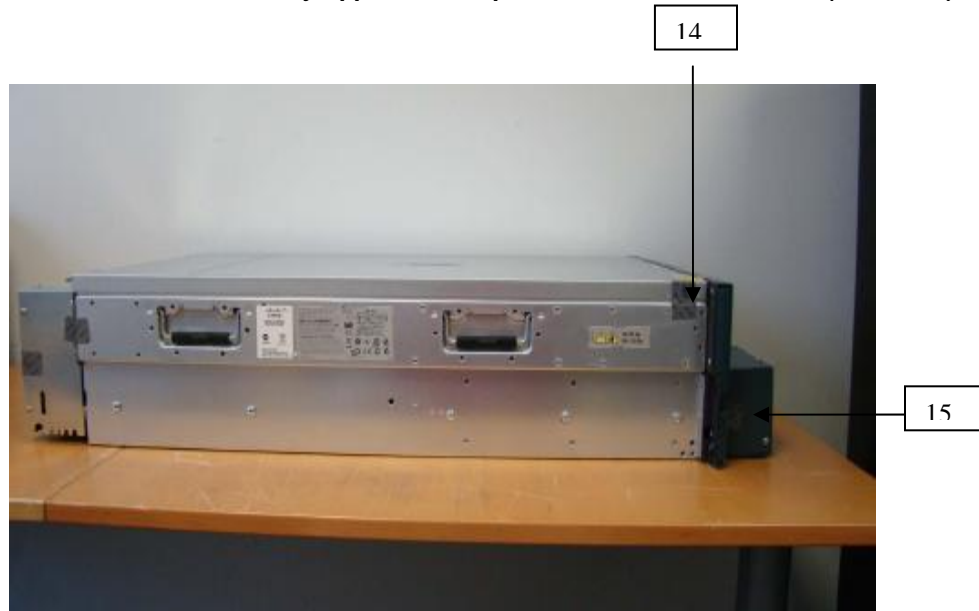


Figure 15 Cisco ASA 5580 Security Appliance Tamper Evident Label Placement (Side Face)



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 Attach opacity shields on 5505, 5580-20, and 5580-40 as depicted in the figures above.

Step 3 Apply a label to cover the security appliance as shown in figures above.

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 modules in the technical terms of a FIPS 140-2 cryptographic device security policy. More information is available on the modules from the sources listed in this section and from the following source:

- The NIST Cryptographic Module Validation Program website (<http://csrc.nist.gov/groups/STM/cmvp/index.html>) contains contact information for answers to technical or sales-related questions for the modules.

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 SystemsAttn:
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 ng products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL: Networking Professionals Connection is an interactive website for networking professionals to share <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>