Cisco Adaptive Security Appliances Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy
Level 2 Validation

Version 0.5

August 27, 2018

Table of Contents

TABLES

DIAGRAMS

FIGURES

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Adaptive Security Appliances Cryptographic Module running Firmware 9.8 referred to in this document as appliances. This security policy describes how the module meets the security requirements of FIPS 140-2 Level 2 and how to run the module in a FIPS 140-2 mode of operation and may be freely distributed.

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/index.html.

1.2 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	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**2**

Table 1 Module Validation Level

1.3 References

This document deals with the specification of the security rules listed in Table 1 above, under which the Cisco Adaptive Security Appliances Cryptographic Module will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2IG and additional rules imposed by Cisco Systems, Inc. More information is available on the modules from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems security. Please refer to the following websites:
http://www.cisco.com/c/en/us/products/index.html
http://www.cisco.com/en/US/products/ps6120/index.html

For answers to technical or sales related questions please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

The NIST Validated Modules website (http://csrc.nist.gov/groups/STM/cmvp/validation.html) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the Cisco Adaptive Security Appliances Cryptographic Module is referred to as Adaptive Security Appliances Cryptographic Module, ASA, Module, Appliance or the Systems.

1.5 Document Organization

The Security Policy document is part of the FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

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

This document provides an overview of the Cisco Adaptive Security Appliances Cryptographic Module on the 5500 Security Appliances models and explains the secure configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the appliances. Section 3 specifically addresses the required configuration for the FIPS-mode of operation.

With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Submission Documentation is Cisco-proprietary and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems.

2 Cisco Adaptive Security Appliance CM

Cisco® Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls provide balanced security effectiveness with productivity. This solution offers the combination of the industry's most deployed stateful firewall with a comprehensive range of next-generation network security services, intrusion prevention system (IPS), content security, secure unified communications, TLSv1.2, SSHv2, IKEv2 and Suite B.

Cisco Adaptive Security Appliance (ASA) Software is the core operating system for the Cisco ASA Family. It delivers enterprise-class firewall capabilities for the ASA devices in an array of form factors - standalone appliances tailor-made for small and midsize businesses, midsize appliances for businesses improving security at the Internet edge, high performance and throughput appliances for demanding enterprise data centers, high-performance blades that integrate with the Cisco Catalyst 6500 Series Switches, virtual instances to provide enterprise-class security for private and public clouds and Firepower services.

2.1 Cryptographic Module

The Cisco Adaptive Security Appliances Cryptographic Module is defined as a multiple-chip standalone cryptographic module running on the following Adaptive Security Appliances:

Small Scale Models:

- ASA 5506-X
- ASA 5506H-X
- ASA 5506W-X
- ASA 5508-X
- ASA 5516-X

Medium Scale Models:

- ASA 5525-X
- ASA 5545-X
- ASA 5555-X

The Cisco Adaptive Security Appliance, when deployed as next-generation firewall (NGFW) appliances, use Adaptive Security Appliance CM and the embedded Cisco® Firepower CM, Certificate# 3261 with these appliances. The Cisco Adaptive Security Appliance CM is the core operating system for the Cisco ASA Family. It delivers enterprise-class firewall capabilities for the ASA series appliances. Please refer to FIPS 140-2 Cert. #3261 for more information about the FIPS relevant security services provided by Cisco Firepower CM. The sections below detail the Adaptive Security Appliance CM FIPS compliance.

2.2 Cryptographic Module Physical Characteristics

The Cisco ASA 5500-X Series Security Appliances deliver enterprise-class security for business-to-enterprise networks in a modular, purpose-built appliance. It includes ASA 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X, 5525-X, 5545-X, and 5555-X models.

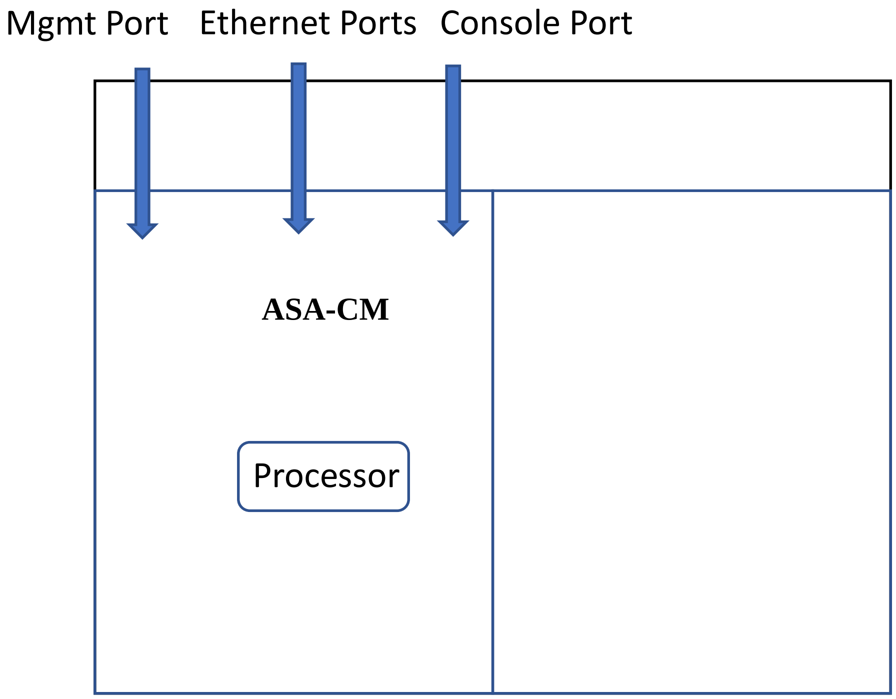


Diagram 1 Block Diagram

2.3 Module Interfaces

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input, status output, and power. The module provides no power to external devices and takes in its power through normal power input/cord. The logical interfaces and their mapping are described in the following tables:

FIPS 140-2 Logical Interface	ASA 5506-X, ASA 5506W-X, ASA 5506H-X, ASA 5508-X, ASA 5516-X, ASA 5525-X, ASA 5545-X, ASA 5555-X Physical Interface
Data Input Interface	Ethernet ports MGMT Port Console Port SFP Ports (on 5545-X and 5555-X)
Data Output Interface	Ethernet ports MGMT Port Console Port SFP Ports (on 5545-X and 5555-X)
Control Input Interface	Ethernet ports MGMT Port SFP Ports (on 5545-X and 5555-X) Console Port Reset Pin/Switch/Button (only on 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X, 5525-X)
Status Output Interface	Ethernet ports MGMT Port Console Port SFP Ports (on 5545-X and 5555-X) LED
Power Interface	Power Plug
Unused Interface	USB Port (USB Type A port and mini-USB Type B Console port)

Table 2 Module Interfaces

Figure 1   Cisco ASA 5506-X and ASA 5506W-X Appliance Font Panel

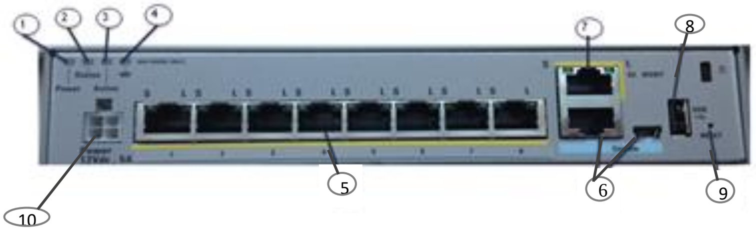


Figure 2 Cisco ASA 5506-X and ASA 5506W-X Appliance Rear Panel

1	Power LED: Green -> power applied OK	6	Console Ports: RJ-45 Console port and mini-USB Type B Console port. The mini USB Type B Console port is disallowed in FIPS mode.
2	Status LED: Green blinking -> system is booting up Green solid -> successful boot Orange -> error during boot-up	7	GE Management Port
3	Active LED: Green -> unit is Active in failover pair Orange -> unit is Standby in failover pair Off -> not part of a failover pair	8	USB port is disallowed in FIPS mode
4	WLAN Module Only lit for 5506W-X Controlled by AP module, same color/blink behavior as existing AP702i Access Point	9	Reset Pin
5	GE ports: Left-side LED Green -> link Right-side LED blinking -> network activity	10	Power Supply

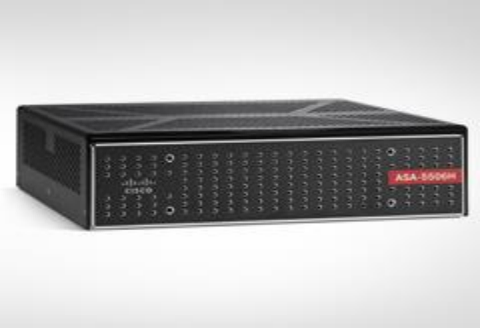


Figure 3 ASA 5506H-X Appliance Front Panel

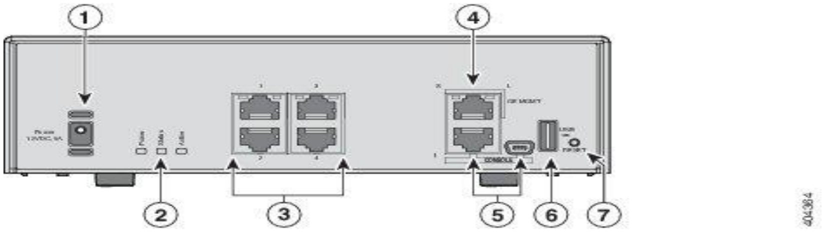


Figure 4 ASA 5506H-X Appliance Rear Panel

1	Power cord socket	The chassis power-supply socket. See Power Supply for more information about the chassis power supply. **Note** The ASA is powered on when you plug in the AC power supply.
2	Status LEDs	The locations and meanings of the status LEDs are described in Status Lights section.
3	Network data ports	Four Gigabit Ethernet RJ-45 (8P8C) network I/O interfaces. The ports are numbered (from top to bottom) 1, 2, 3, 4. Each port includes a pair of LEDs, one each for connection status and link status. The ports are named and numbered Gigabit Ethernet 1/1 through Gigabit Ethernet 1/4.
4	Management port	A Gigabit Ethernet interface restricted to network management access only. Connect with an RJ-45 cable.
5	Console ports	Two serial ports, a mini USB Type B and a standard RJ-45 (8P8C), are provided for management access via an external system. The mini USB Type B Console port is disallowed in FIPS mode.
6	USB port	A standard USB Type A port is disallowed in FIPS mode
7	Reset button	A small recessed button that if pressed for longer than three seconds resets the ASA to its default “as-shipped” state following the next reboot. Configuration variables are reset to factory default. However, the flash is not erased and no files are removed. **Note** You can use the **service sw-reset-button** to disable the reset button. The default is enabled.

Note: Please refer to Cisco ASA 5500-X Series Hardware Installation Guide for more information.

Figure 5 ASA 5508-X and ASA 5516-X Appliances Front Panel

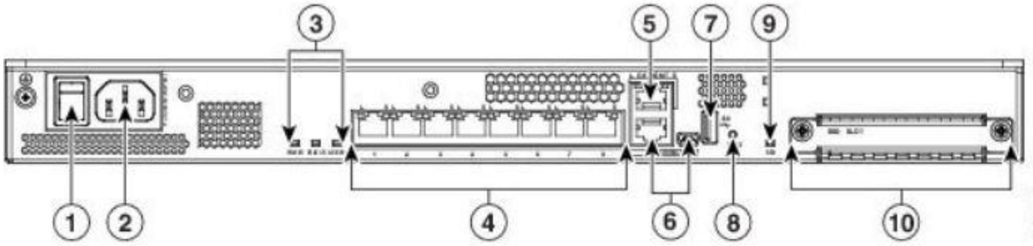


Figure 6 ASA 5508-X and ASA 5516-X Appliances Rear Panel

1	Power switch	Standard rocker-type power on/off switch.
2	Power cord socket	The chassis power-supply socket.
3	Status LEDs	The locations and meanings of the status LEDs are described in Status Lights.
4	Network data ports	Eight Gigabit Ethernet RJ-45 (8P8C) network I/O interfaces. The ports are numbered (from left to right) 1, 2, 3, 4, 5, 6, 7, 8. Each port includes a pair of LEDs, one each for connection status and link status. The ports are named and numbered Gigabit Ethernet 1/1 through Gigabit Ethernet 1/8. See Network Ports referred to Note 2 below for additional information.
5	Management port	A Gigabit Ethernet interface restricted to network management access only. Connect with an RJ-45 cable.
6	Console ports	Two serial ports, a mini USB Type B and a standard RJ-45 (8P8C) are provided for management access via an external system. See Console Ports referred to Note 2 below for additional information.
7	USB port	A standard USB Type A port is provided, allowing attachment of an external device such as mass storage. See Internal and External Flash Storage referred to Note 2 below for additional information.
8	Reset button	A small recessed button that if pressed for longer than three seconds resets the ASA to its default “as-shipped” state following the next reboot. Configuration variables are reset to factory default. However, the flash is not erased and no files are removed. **Note** You can use the **service sw-reset-button** to disable the reset button. The default is enabled.
9	SSD LED	Status light for installed solid-state drive (SSD). See Status Lights referred to Note 2 below for additional information.
10	SSD bay	Covered slot in which the SSD is installed. You can replace this drive if it fails. See Replace the SST in the ASA referred to Note 2 below for additional information.

Notes:

1. Both USB port and the mini USB Type B Console port are disallowed in FIPS mode. Please refer to section “Physical Security” for more details.
2. Please refer to Cisco ASA 5500-X Series Hardware Installation Guide for more information.

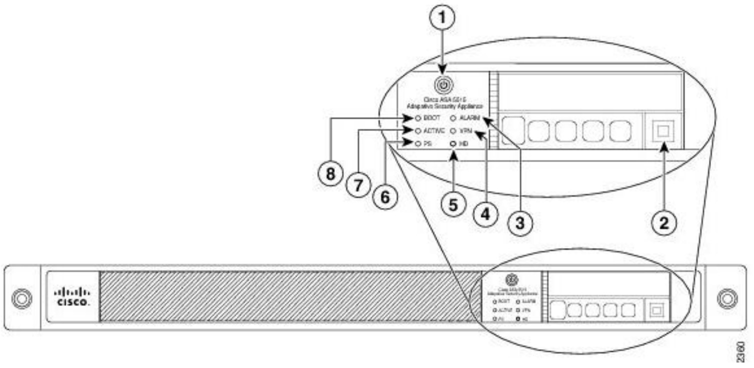


Figure 7 ASA 5525-X Appliances Front Panel

	LED	Description
1	Power Button	A hard switch that turns the system on and off. Once depressed, the button stays in the "on" position: • On–The power symbol on the button illuminates. • Off–The power symbol on the button is dark.
2	Hard disk release button	Releases the hard disk from the device.
3	Alarm	Indicates system operating status: • Off–Normal operating system function. • Flashing amber–Critical Alarm indicting one or more of the following: – a major failure of a hardware or software component. – an over-temperature condition. – power voltage is outside of the tolerance range.
4	VPN	Indicates VPN tunnel status: • Solid green–VPN tunnel is established. • Off–No VPN tunnel is established.
5	HD	Indicates Hard Disk Drive status: • Flashing green–Proportioned to read/write activity. • Solid amber–Hard disk drive failure. • Off–The power symbol on the button is dark.
6	PS	Indicates the power supply status.
7	Active	Indicates the status of the failover pair: • Solid green–Failover pair is operating normally. • Off– Failover is not operational.
8	Boot	Indicates power-up diagnostics: • Flashing green–Power-up diagnostics are running, or system is booting. • Solid amber–System has passed power-up diagnostics. • Off– Power-up diagnostics are not operational.

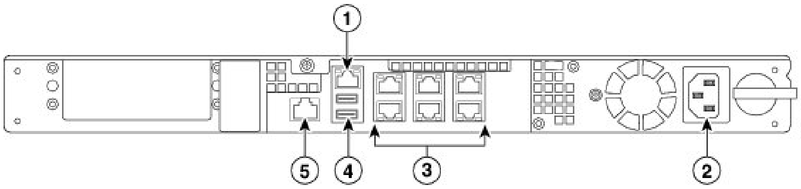


Figure 8 ASA 5525-X Appliances Rear Panel

		Description
1	Management 0/0 interface	Indicates the Gigabit Ethernet Interface that is restricted to management use only. Connect with an RJ-45 cable. (See the “Management 0/0 Interface on the ASA 5500-S Series” section.)
2	Power supply	Indicates the chassis power supply.
3	RJ-45 Ethernet ports	Indicates the Gigabit Ethernet customer data interfaces. The top row port numbers are (from left to right) 5, 3, 1. The bottom row port numbers are (from left to right) 4, 2, 0.
4	USB ports	Disallowed in FIPS mode
5	Console port	Indicates the console port that directly connects a computer to the ASA.

Note: Please refer to Cisco ASA 5500-X Series Hardware Installation Guide for more information.

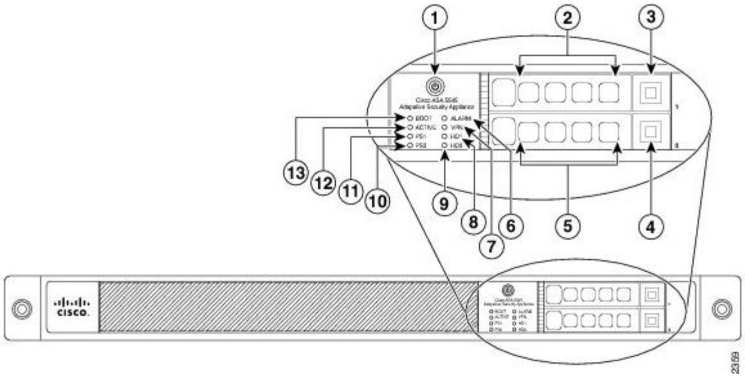
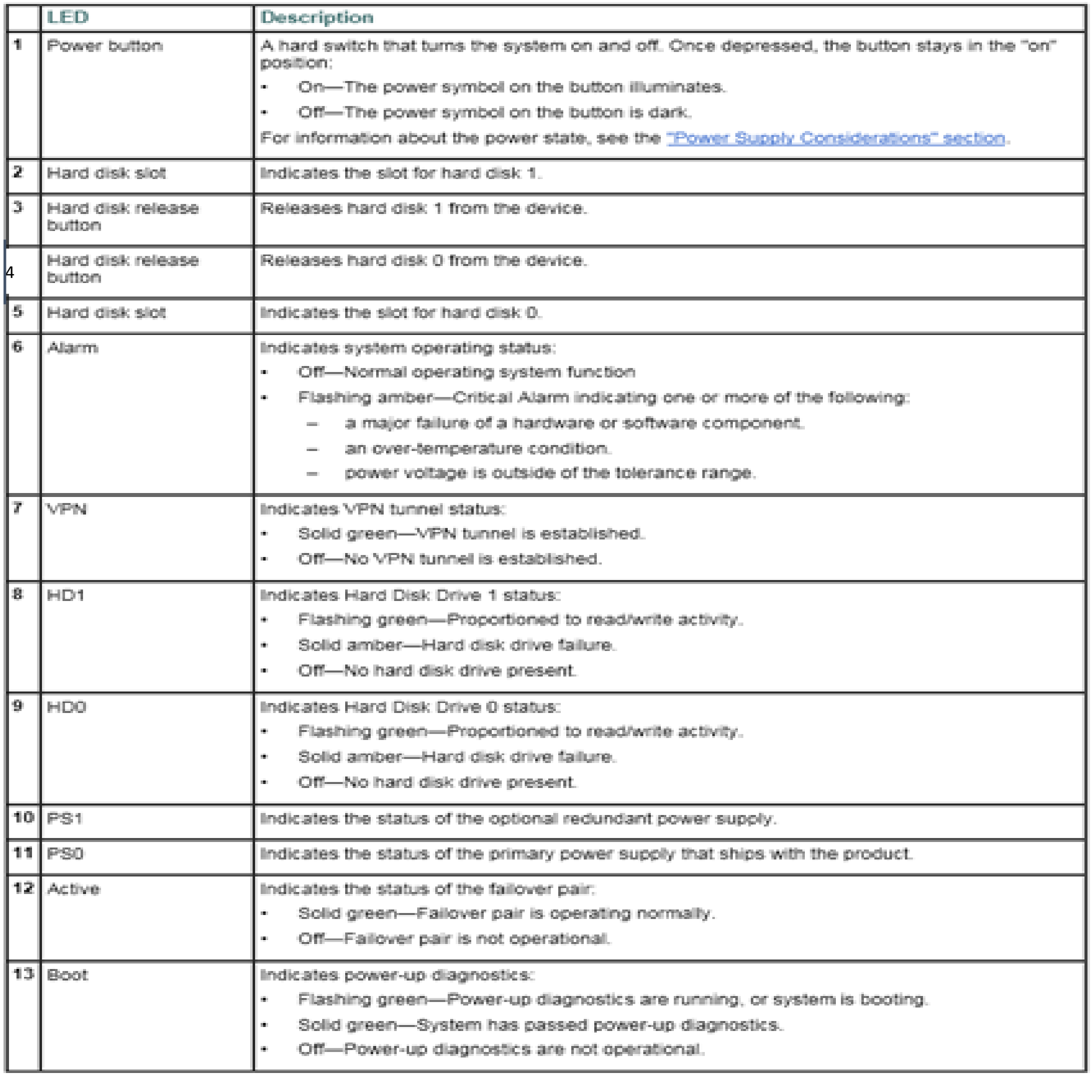


Figure 9 ASA 5545-X and ASA 5555-X Appliances Front Panel



	LED	Description
1	Power button	A hard switch that turns the system on and off. Once depressed, the button stays in the "on" position: • On—The power symbol on the button illuminates. • Off—The power symbol on the button is dark. For information about the power state, see the "Power Supply Considerations" section.
2	Hard disk slot	Indicates the slot for hard disk 1.
3	Hard disk release button	Releases hard disk 1 from the device.
4	Hard disk release button	Releases hard disk 0 from the device.
5	Hard disk slot	Indicates the slot for hard disk 0.
6	Alarm	Indicates system operating status: • Off—Normal operating system function • Flashing amber—Critical Alarm indicating one or more of the following: – a major failure of a hardware or software component. – an over-temperature condition. – power voltage is outside of the tolerance range.
7	VPN	Indicates VPN tunnel status: • Solid green—VPN tunnel is established. • Off—No VPN tunnel is established.
8	HD1	Indicates Hard Disk Drive 1 status: • Flashing green—Proportioned to read/write activity. • Solid amber—Hard disk drive failure. • Off—No hard disk drive present.
9	HD0	Indicates Hard Disk Drive 0 status: • Flashing green—Proportioned to read/write activity. • Solid amber—Hard disk drive failure. • Off—No hard disk drive present.
10	PS1	Indicates the status of the optional redundant power supply.
11	PS0	Indicates the status of the primary power supply that ships with the product.
12	Active	Indicates the status of the failover pair: • Solid green—Failover pair is operating normally. • Off—Failover pair is not operational.
13	Boot	Indicates power-up diagnostics: • Flashing green—Power-up diagnostics are running, or system is booting. • Solid green—System has passed power-up diagnostics. • Off—Power-up diagnostics are not operational.

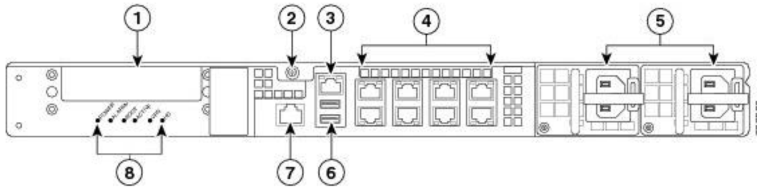
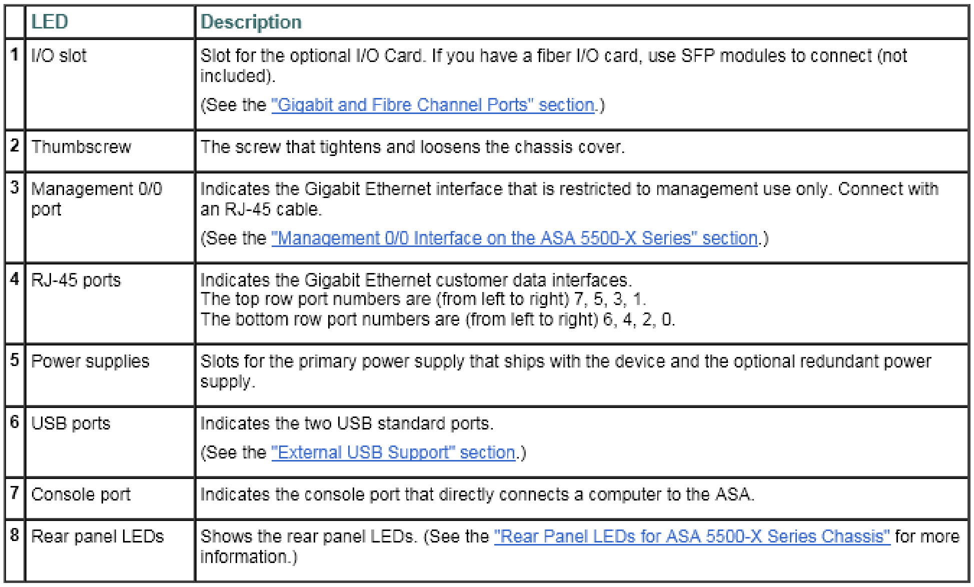


Figure 10 ASA 5545-X and ASA 5555-X Appliances Rear Panel



	LED	Description
1	I/O slot	Slot for the optional I/O Card. If you have a fiber I/O card, use SFP modules to connect (not included). (See the "Gigabit and Fibre Channel Ports" section.)
2	Thumbscrew	The screw that tightens and loosens the chassis cover.
3	Management 0/0 port	Indicates the Gigabit Ethernet interface that is restricted to management use only. Connect with an RJ-45 cable. (See the "Management 0/0 Interface on the ASA 5500-X Series" section.)
4	RJ-45 ports	Indicates the Gigabit Ethernet customer data interfaces. The top row port numbers are (from left to right) 7, 5, 3, 1. The bottom row port numbers are (from left to right) 6, 4, 2, 0.
5	Power supplies	Slots for the primary power supply that ships with the device and the optional redundant power supply.
6	USB ports	Indicates the two USB standard ports. (See the "External USB Support" section.)
7	Console port	Indicates the console port that directly connects a computer to the ASA.
8	Rear panel LEDs	Shows the rear panel LEDs. (See the "Rear Panel LEDs for ASA 5500-X Series Chassis" for more information.)

Notes:

1. The USB ports are disallowed in FIPS mode.
2. Please refer to Cisco ASA 5500-X Series Hardware Installation Guide for more information.

2.4 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/TLSv1.2

Authentication is identity-based. Each user is authenticated by the module upon initial access to the module. As required by FIPS 140-2, there are two roles in the security appliances that operators may assume: Crypto Officer role and User role. The administrator of the security appliances assumes the Crypto Officer role in order to configure and maintain the module using Crypto Officer services, while the Users exercise only the basic User services. The module also supports RADIUS and TACACS+ as another means of authentication, allowing the storage of usernames and passwords on an external server as opposed to using the module’s internal database for storage.

The User and Crypto Officer passwords and all shared secrets must each be at a minimum eight (8) characters long. There must be at least one special character and at least one number character (enforced procedurally) along with six additional characters taken from the 26 upper case, 26 lower case, 10 numbers and 32 special characters. See the Secure Operation section for more information. If six (6) special/alpha/number characters, one (1) special character and one (1) number are used without repetition for an eight (8) digit value, the probability of randomly guessing the correct sequence is one (1) in 187,595,543,116,800. This is calculated by performing 94 x 93 x 92 x 91 x 90 x 89 x 32 x 10. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the module.

Additionally, when using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength. Thus, an attacker would have a 1 in 2^{112} 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 8.6 x 10^{31} (5.2 x 10^{33} /60 = 8.6 x 10^{31}) attempts per second, which far exceeds the operational capabilities of the module to support.

2.5 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 an Ethernet port or ASDM via HTTPS/TLS. The module prompts the User for username and password. If the password is correct, the User is allowed entry to the module management functionality. The other means of accessing the console is via an IPsec session. This session is authenticated either using a shared secret or RSA digital signature authentication mechanism. The services available to the User role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below:

Services and Access	Description	Keys and CSPs
Status Functions	View state of interfaces and protocols, version of the firmware currently running.	Operator password (r)
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	Operator password (r)
Directory Services	Display directory of files kept in flash memory.	Operator password (r)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
IPsec VPN Functions	Negotiation and encrypted data transport via IPSec VPN.	Operator password, skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key, DRBG entropy input, DRBG seed, DRBG V, DRBG C and DRBG key (r, w, d)
SSHv2 Functions	Negotiation and encrypted data transport via SSHv2.	Operator password, SSHv2 Private Key, SSHv2 Public Key and SSHv2 session key, DRBG entropy input, DRBG seed, DRBG V, DRBG C and DRBG key (r, w, d)
HTTPS Functions (TLSv1.2)	Negotiation and encrypted data transport via HTTPS/TLS (TLSv1.2).	Operator password, ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master key, TLS encryption key, TLS integrity key, DRBG entropy input, DRBG seed, DRBG V, DRBG C and DRBG key (r, w, d)

Table 3 User Services

2.6 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 services available to the Crypto

Officer role accessing the CSPs, the type of access – read (r), write (w) and zeroized/delete (d) – and which role accesses the CSPs are listed below:

Services and Access	Description	Keys and CSPs
Configure the Security Blade	Define network interfaces and settings, create command aliases, set the protocols the module will support, enable interfaces and network services, set system date and time, and load authentication information.	ISAKMP preshared, Operator password, Enable password, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key, DRBG entropy input, DRBG seed, DRBG V, DRBG C and DRBG key (r. w, d)
Firmware Installation	Install the firmware during the System Initialization	Integrity test key (r. w, d)
Configure External Authentication Server	Configure Client/Server authentication	RADIUS secret, TACACS+ secret (r. w, d)
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.	Operator password, Enable password (r, w, d)
View Status Functions	View the module configuration, routing tables, active sessions health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	Operator password, Enable password (r, w, d)
Manage the Security Blade	Log off users, shutdown or reload the module, erase the flash memory, manually back up module configurations, view complete configurations, manager user rights, and restore module configurations.	Operator password, Enable password (r, w, d)
Configure Encryption/Bypass	Set up the configuration tables for IP tunneling. Set preshared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.	ISAKMP preshared, Operator password, Enable password, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key, DRBG entropy input, DRBG seed, DRBG V, DRBG C and DRBG key (r, w, d)
TLS VPN (TLSv1.2) Functions	Configure SSL VPN parameters, provide entry and output of CSPs.	ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master key, TLS encryption key, TLS integrity key, DRBG entropy input, DRBG seed, DRBG V, DRBG C and DRBG key (r, w, d)
SSH v2 Functions	Configure SSH v2 parameter, provide entry and output of CSPs.	SSHv2 private key, SSHv2 public key, SSHv2 encryption key, SSHv2 integrity key, DRBG entropy input, DRBG seed, DRBG V, DRBG C and DRBG key (r, w, d)
IPsec VPN Functions	Configure IPsec VPN parameters, provide entry and output of CSPs.	ISAKMP preshared, skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPsec encryption key, IPsec authentication key, DRBG entropy input, DRBG seed, DRBG V, DRBG C and DRBG key (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
User services	The Crypto Officer has access to all User services.	Operator password (r, w, d)
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.	N/A
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 6, Zeroization column.	All CSPs (d)

Table 4 Crypto Officer Services

2.7 Non-FIPS mode Services

The cryptographic module in addition to the above listed FIPS mode of operation can operate in a non-FIPS mode of operation. This is not a recommended operational mode but because the associated RFC's for the following protocols allow for non-approved algorithms and non-approved key sizes a non-approved mode of operation exist. So those services listed above with their FIPS approved algorithms in addition to the following services with their non-approved algorithms and non-approved keys sizes are available to the User and the Crypto Officer. Prior to using any of the Non-Approved services in Section 2.7, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

Services [1]	Non-Approved Algorithms
IPsec	Hashing: MD5 MACing: HMAC-SHA-1, MD5 Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
SSH	Hashing: MD5 MACing: HMAC MD5 Symmetric: DES Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
TLS	Symmetric: DES, RC4 Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman

Table 5 Non-approved algorithms in the Non-FIPS mode services

Neither the User nor the Crypto Officer are allowed to operate any of these services while in FIPS mode of operation.

All services available can be found at http://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html. This site lists all configuration guides for the ASA systems.

2.8 Unauthenticated Services

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

In addition, for details regarding the Roles, Services and Authentication provided by the embedded cryptographic module, please refer to certificate number 3261’s Security Policy.

2.9 Cryptographic Key/CSP Management

The module administers both cryptographic keys and other critical security parameters such as passwords. All keys and CSPs are protected by the password-protection of the Crypto Officer role and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory. Keys are both manually and electronically distributed but entered electronically. Persistent keys with manual distribution are used for pre-shared keys whereas protocols such as IKE, TLS and SSH are used for electronic distribution.

All pre-shared keys are associated with the CO role that created the keys, and the CO role is protected by a password. Therefore, the CO password is associated with all the pre-shared keys. The Crypto Officer needs to be authenticated to store keys. Only an authenticated Crypto Officer can view the keys. All Diffie-Hellman (DH) keys agreed upon for individual tunnels are directly associated with that specific tunnel only via the IKE protocol. RSA Public keys are entered into the module using digital certificates which contain relevant data such as the name of the public key's owner, which associates the key with the correct entity. All other keys are associated with the user/role that entered them. The entropy comes from a process of extracting bits from the

[1] These approved services become non-approved when using any of non-approved algorithms or non-approved key or curve sizes. When using approved algorithms and key sizes these services are approved.

entropy source and is fed into the DRBG. The module provides approximately 347 bits entropy to instantiate the DRBG.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG (AES-256) or HASH_DRBG (SHA-512)	384-bits/512-bits	This is the entropy for SP 800-90A CTR_DRBG and HASH_DRBG. HW based entropy source used to construct seed.	DRAM (plaintext)	Power cycle the device
DRBG seed	SP800-90A CTR_DRBG (AES-256) or HASH_DRBG (SHA-512)	384-bits/888-bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from hardware-based entropy source.	DRAM (plaintext)	Power cycle the device
DRBG V	SP800-90A CTR _DRBG (AES-256) or HASH_DRBG (SHA-512)	128-bits/888-bits	The DRBG V is one of the critical values of the internal state upon which the security of this DRBG mechanism depends. Generated first during DRBG instantiation and then subsequently updated using the DRBG update function.	DRAM (plaintext)	Power cycle the device
DRBG key	SP800-90A CTR_DRBG (using AES-256)	256-bits	Internal critical value used as part of SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Power cycle the device
DRBG C	SP800-90A HASH_DRBG (SHA-512)	888-bits	Internal critical value used as part of SP 800-90A HASH_DRBG. Established per SP 800-90A HASH_DRBG.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman Shared Secret	DH	2048 – 4096 bits	The shared secret used in Diffie-Hellman (DH) exchange. Established per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
Diffie Hellman private key	DH	224-384 bits	The private key used in Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90A DRBG.	DRAM (plaintext)	Power cycle the device
Diffie Hellman public key	DH	2048 – 4096 bits	The public key used in Diffie-Hellman (DH) exchange. This key is derived per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
skeyid	Keying material	160 bits	Keying material known only to IKE peers. It was established via key derivation function defined in SP800-135 KDF and it will be used for deriving other keys in IKE protocol implementation.	DRAM (plaintext)	Power cycle the device
skeyid_d	Keying material	160 bits	Keying material known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Power cycle the device

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
SKEYSEED	Keying material	160 bits	Keying material known only to IKE peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving IKE session authentication key.	DRAM (plaintext)	Power cycle the device
IKE session encrypt key	Triple-DES/AES	Triple-DES 192 bits or AES 128/192/256 bits	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Power cycle the device
IKE session authentication key	HMAC-SHA-1/256/384/512	160-512 bits	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Power cycle the device
ISAKMP preshared	Pre-shared secret	Variable 8 plus characters	The secret used to derive IKE skeyid when using preshared secret authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new secret
IKE authentication private Key	RSA/ECDSA	RSA 2048 bits or ECDSA Curves: P-256/P-384/512	RSA/ECDSA private key used in IKE authentication. This key is generated by calling SP800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IKE authentication public key	RSA/ECDSA	RSA 2048 bits or ECDSA Curves: P-256/P-384/512	RSA/ECDSA public key used in IKE authentication. This key is derived in compliance with FIPS 186-4 RSA/ECDSA key pair generation method in the module	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IPsec encryption key	Triple-DES, AES and AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	The IPsec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Power cycle the device
IPsec authentication key	HMAC-SHA-1/256/384/512	160-512 bits	The IPsec (IKE Phase II) authentication key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Power cycle the device
Operator password	Password	8 plus characters	The password of the User role. This CSP is entered by the User.	NVRAM (plaintext)	Overwrite with new password
Enable password	Password	8 plus characters	The password of the CO role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new password

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
RADIUS secret	Shared Secret	16 characters	The RADIUS shared secret. Used for RADIUS Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new secret
TACACS+ secret	Shared Secret	16 characters	The TACACS+ shared secret. Used for TACACS+ Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new secret
SSHv2 RSA private key	RSA	2048 bits modulus	The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 RSA public key	RSA	2048 bits modulus	The SSHv2 public key used in SSHv2 connection. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 encryption key	Triple-DES/AES	Triple-DES 192 bits or AES 128/192/256 bits	This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffics traversing between the SSHv2 Client and SSHv2 Server. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	Automatically when SSH session is terminated
SSHv2 integrity key	HMAC-SHA-1	160 bits	Used for SSH connections integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when SSH session is terminated
ECDSA private key	ECDSA	Curves: P-256, 384, 521	Key pair generation, signature generation/Verification. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by ECDSA keypair deletion command
ECDSA public key	ECDSA	Curves: P-256, 384, 521	Key pair generation, signature generation/Verification (used in IKE/IPSec and TLS). This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by ECDSA keypair deletion command
Enable secret	Shared Secret	At least eight characters	The obfuscated password of the CO role. However, the algorithm used to obfuscate 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. The Crypto Officer configures the module to obfuscate the Enable password. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Overwrite with new secret

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
TLS RSA private keys	RSA	2048 bits	Identity certificates for the security appliance itself and also used in IPSec, TLS, and SSH negotiations. This key was generated by calling FIPS approved DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS RSA public keys	RSA	2048 bits	Identity certificates for the security appliance itself and also used in IPSec, TLS, and SSH negotiations. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS pre-master secret	keying material	At least eight characters	Keying material used to derive TLS master key during the TLS session establishment. This key entered into the module in cipher text form, encrypted by RSA public key.	DRAM (plaintext)	Automatically when TLS secret is generated
TLS master secret	keying material	48 Bytes	Keying material used to derive other HTTPS/TLS keys. This key was derived from TLS pre-master secret during the TLS session establishment	DRAM (plaintext)	Automatically when TLS session is terminated
TLS encryption keys	Triple-DES/AES/AES-GCM 128/192/256	Triple-DES 192 bits or AES 128/192/256 bits	Used in HTTPS/TLS connections to protect the session traffic. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS Integrity Key	HMAC-SHA256/384	256-384 bits	Used for TLS integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
Integrity test key	RSA-2048 Public key	2048 bits	A hard coded key used for firmware power-up integrity verification.	Hard coded for firmware integrity testing	Zeroized by "#erase flash:" command, write to startup config, followed by a module reboot

Table 6 Cryptographic Keys and CSPs

In addition, for details regarding the cryptographic keys and CSPs used in the embedded cryptographic module, please refer to certificate number 3261's Security Policy.

2.10 Cryptographic Algorithms

The module implements a variety of approved and non-approved algorithms.

2.10.1 Approved Cryptographic Algorithms

The modules support the following FIPS 140-2 approved algorithm implementations:

Algorithm				
	Cisco Security Crypto (Firmware)	ASA On-board (Cavium Octeon III) (ASA 5506-X, 5506H-X, 5506W-X, 5508-X, 5516-X)	ASA On-board (Cavium Nitrox PX) (ASA 5525-X)	ASA On-board (Cavium Nitrox PX) (ASA 5545-X, 5555-X)
		ASA CN7020 or CN7130	ASA CN1610	ASA CN1620
AES (128/192/256 CBC, GCM)	4905	3301	2472	2050 & 2444
Triple-DES (CBC, 3-key)	2559	1881	1513	1321
SHS (SHA-1/256/384/512)	4012	2737	2091	1794
HMAC (SHA-1/256/384/512)	3272	2095	1514	1247
RSA (PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits PKCS1_V1_5; 2048 bits)	2678			
ECDSA (KeyGen, SigGen, SigVer; P-256, P-384, P-521)	1254			
CTR_DRBG (AES-256)	1735	819		
SHA_DRBG (SHA-512)			336	332
CVL Component (IKEv2, TLSv1.2 and SSHv2)	1521			
CKG (vendor affirmed)				

Table 7 Approved Cryptographic Algorithms and Associated Certificate Number

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.
- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS and RFC 7296 for IPSec/IKEv2. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established. The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
- Each of TLS, SSH and IPSec protocols governs the generation of the respective Triple-DES keys. Refer to RFC 5246 (TLS), RFC 4253 (SSH) and RFC 6071 (IPSec) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring the module limits the number of encryptions with the same key to 2^{20}.
- No parts of the SSH, TLS and IPSec protocols, other than the KDF, have been tested by the CAVP and CMVP.

- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 5 in SP800-133. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

2.10.2 Non-FIPS Approved Algorithms Allowed in FIPS Mode

The module supports the following non-FIPS approved algorithms which are permitted for use in the FIPS approved mode:

- Diffie-Hellman (CVL Cert. #1521, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- NDRNG

2.10.3 Non-Approved Cryptographic Algorithms

The module supports the following non-approved cryptographic algorithms that shall not be used in FIPS mode of operation:

- DES
- Diffie-Hellman (key agreement; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- HMAC MD5
- MD5
- RC4
- RSA (key wrapping; key establishment methodology less than 112 bits of encryption
- strength; non-compliant)
- HMAC-SHA1 is not allowed with key size under 112-bits

In addition, the embedded cryptographic module (FIPS 140-2 Cert. #3261) also provides the following FIPS approved algorithm certificates and non-approved algorithms:

2.10.4 Approved Cryptographic Algorithms from Embedded Module

The module supports the following FIPS 140-2 approved algorithm implementations:

Algorithms	Algorithm Implementations
AES (128/192/256 CBC, GCM)	4266
Triple-DES (CBC, 3-key)	2307
SHS (SHA-1/256/384/512)	3512
HMAC (SHA-1/256/384/512)	2811
RSA (PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits)	2297
DRBG (AES-256 CTR)	1337
CVL Component (TLSv1.2 and SSHv2)	1008
CKG (vendor affirmed)	

Table 8 Approved Cryptographic Algorithms and Associated Certificate Number for Embedded Module

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.

- The module’s AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The counter portion of the IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module’s power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
- No parts of SSH and TLS protocols, other than the KDFs, have been tested by the CAVP and CMVP.
- Each of TLS and SSH protocols governs the generation of the respective Triple-DES keys. Refer to RFC 5246 (TLS) and RFC 4253 (SSH) for details relevant to the generation of the individual Triple-DES encryption keys. The user is responsible for ensuring the module limits the number of encryptions with the same key to 2^{20}.
- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per scenario 1 of section 5 in SP800-133. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.

2.10.5 Non-FIPS Approved Algorithms Allowed in FIPS Mode from Embedded Module

The module supports the following non-FIPS approved algorithms which are permitted for use in the FIPS approved mode:

- Diffie-Hellman (CVL Cert. #1008, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- EC Diffie-Hellman (CVL Cert. #1008, key agreement; key establishment methodology provides between 128 and 256 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 of encryption strength)
- NDRNG

2.10.6 Non-Approved Cryptographic Algorithms from Embedded Module

The module supports the following non-approved cryptographic algorithms that shall not be used in FIPS mode of operation:

- Diffie-Hellman (key agreement; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- EC Diffie-Hellman (key agreement; key establishment methodology less than 112 bits of encryption strength
- RSA (key wrapping; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- DES
- HMAC MD5
- MD5
- RC4
- HMAC-SHA1 is not allowed with key size under 112-bits

2.11 Self-Tests

The module includes 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.

Self-tests performed

- ASA Self Tests
    - POSTs – Cisco Security Crypto (Firmware)
        - AES Encrypt/Decrypt KATs
        - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
        - ECDSA (sign and verify) Power On Self-Test
        - Firmware Integrity Test (using SHA-512 and RSA 2048)
        - HMAC-SHA-1 KAT
        - HMAC-SHA-256 KAT
        - HMAC-SHA-384 KAT
        - HMAC-SHA-512 KAT
        - RSA (sign/verify) KATs
        - SHA-1 KAT
        - SHA-256 KAT
        - SHA–384 KAT
        - SHA-512 KAT
        - Triple-DES Encrypt/Decrypt KATs
    - POSTs – ASA On-board (Hardware)
        - AES Encrypt/Decrypt KATs
        - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
        - HMAC-SHA-1 KAT
        - HMAC-SHA-256 KAT
        - HMAC-SHA-384 KAT
        - HMAC-SHA-512 KAT
        - SHA-1 KAT
        - SHA-256 KAT
        - SHA-384 KAT
        - SHA-512 KAT
        - Triple-DES Encrypt/Decrypt KATs
    - Conditional tests - Cisco Security Crypto (Firmware)
        - RSA pairwise consistency test (encrypt/decrypt and sign/verify)
        - ECDSA pairwise consistency test
        - Conditional IPSec Bypass test
        - Continuous Random Number Generator test for SP800-90A DRBG
        - Continuous Random Number Generator test for NDRNG
    - Conditional tests - ASA On-board (Hardware)
        - Continuous Random Number Generator test for SP800-90A DRBG

Note: DRBGs will not be available should the NDRNG become unavailable. This will in turn make the associated security service/CSP outlined above in Table 6 non-available.

The security appliances perform all power-on self-tests automatically when the power is applied. 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.

In addition, for details of the Self-Tests conducted by the embedded cryptographic module, please refer to certificate number 3261's Security Policy.

2.12 Physical Security

The FIPS 140-2 level 2 physical security requirements for the modules are met by the use of opacity shields covering the front panels of modules to provide the required opacity and tamper evident seals to provide the required tamper evidence.

2.12.1 Opacity Shield Security

The following table shows the tamper labels and opacity shields that shall be installed on the modules to operate in a FIPS approved mode of operation. The CO is responsible for using, securing and having control at all times of any unused tamper evident labels. Actions to be taken when any evidence of tampering should be addressed within site security program.

ASA Models	Number Tamper labels	Tamper Evident Labels	Number Opacity Shields	Opacity Shields
5506-X	4	AIR-AP-FIPSKIT=	1	ASA5506-FIPS-KIT=
5506H-X	4	AIR-AP-FIPSKIT=	1	ASA5506-FIPS-KIT=
5506W-X	4	AIR-AP-FIPSKIT=	1	ASA5506-FIPS-KIT=
5508-X	5	AIR-AP-FIPSKIT=	1	ASA5508-FIPS-KIT=
5516-X	5	AIR-AP-FIPSKIT=	1	ASA5516-FIPS-KIT=
5525-X, 5545-X, 5555-X	3	AIR-AP-FIPSKIT=	0	None

Table 9 Tamper Labels and Opacity Shield Quantities

ASA 5506-X, 5506H-X and 5506W-X Opacity Shield

To install an opacity shield on the ASA 5506-X, 5506H-X and 5506W-X, follow these steps:

Step 1: Remove the three screws from the bottom of the Cisco ASA 5506-X, 5506H-X and 5506W-X.
Step 2: Slide the ASA 5506-X, 5506H-X and 5506W-X into the FIPS enclosure.

Step 3: Turn the FIPS enclosure with the chassis securely inside and use the three screws removed in Step 1 to screw the FIPS enclosure to the Cisco ASA 5506-X, 5506H-X and 5506W-X.

Step 4: Apply the tamper evident label over the screw on the bottom. Please see Figure 18 for placement of the TEL.

Step 5: Apply another tamper evident label so that one half of the tamper evident label attaches to the enclosure and the other half attaches to the Cisco ASA 5506-X, 5506H-X and 5506W-X chassis. Please see Figure 24 for placement of the TEL.

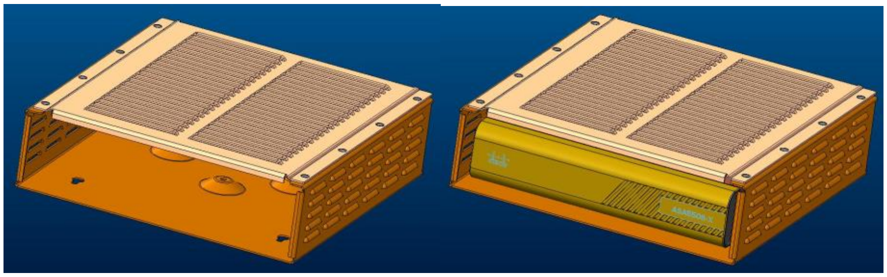


Figure 11 ASA 5506-X, ASA 5506H-X and ASA 5506W-X Opacity Shield Placement

ASA 5508-X and ASA 5516-X Opacity Shield

To install an opacity shield on the ASA 5508-X or ASA 5516-X rear, follow these steps:

Step 1: Power off the ASA.

Step 2: Remove the two screws.

Step 3: Place the shield over the vent areas and insert the screws.

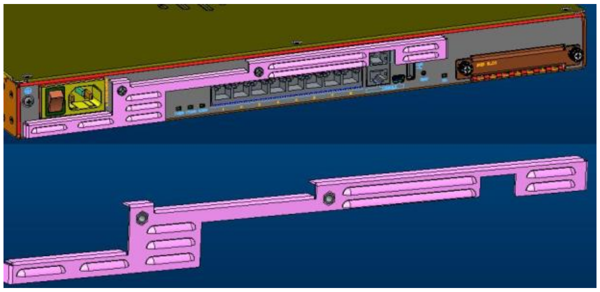


Figure 12 ASA 5508-X and ASA 5516-X Opacity Shield Placement

2.12.2 Tamper Evidence Labels (TELs)

The tamper evident seals (hereinafter referred to as tamper evident labels (TEL)) shall be installed on the security devices containing the module prior to operating in FIPS mode. TELs shall be applied as depicted in the figures below. Any unused TELs must be securely stored, accounted for, and maintained by the CO in a protected location.

Should the CO have to remove, change or replace TELs (tamper-evidence labels) for any reason, the CO must examine the location from which the TEL was removed and ensure that no residual debris is still remaining on the chassis or card. If residual debris remains, the CO must remove the debris using a damp cloth.

Any deviation of the TELs placement such as tearing, misconfiguration, removal, change, replacement or any other change in the TELs from its original configuration as depicted below by unauthorized operators shall mean the module is no longer in FIPS mode of operation. Returning the system back to FIPS mode of operation requires the replacement of the TEL as depicted below and any additional requirement per the site security policy which are out of scope of this Security Policy.

The Crypto Officer shall inspect the seals for evidence of tamper as determined by their deployment policies (every 30 days is recommended). If the seals show evidence of tamper, the

Crypto Officer shall assume that the module has been compromised and contact Cisco accordingly.

To seal the system, apply tamper-evidence labels as depicted in the figures below.

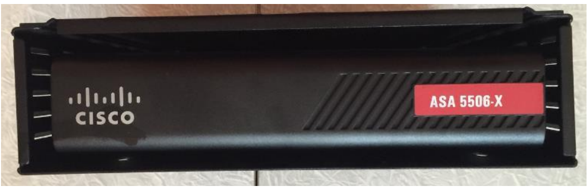


Figure 13 ASA 5506-X and ASA 5506W-X Front View

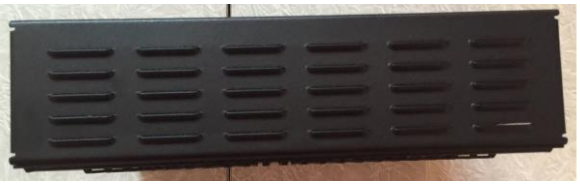


Figure 14 ASA 5506-X and ASA 5506W-X Right Side View

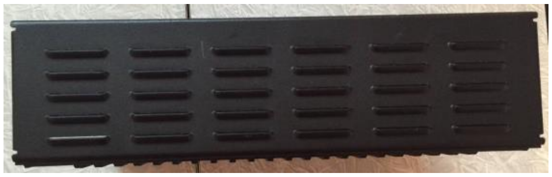


Figure 15 ASA 5506-X and ASA 5506W-X Left Side View

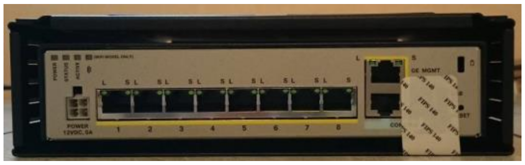


Figure 16 ASA 5506-X and ASA 5506W-X Rear TEL Placement

Figure 17 ASA 5506-X and ASA 5506W-X Top View

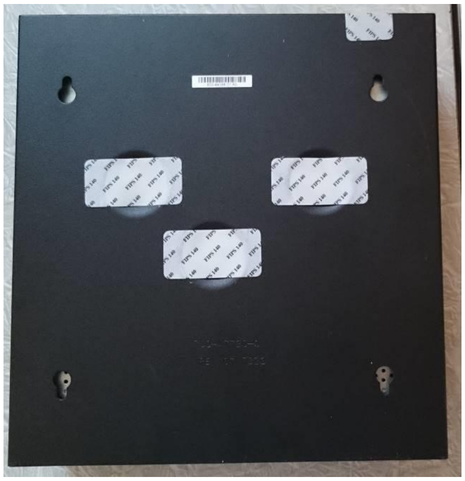


Figure 18 ASA 5506-X and ASA 5506W-X Bottom TEL Placement

Figure 19 ASA 5506H-X Front View

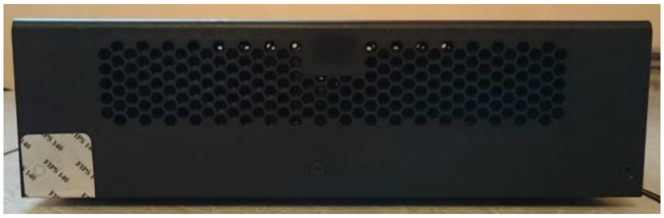


Figure 20 ASA 5506H-X Right Side TEL Placement

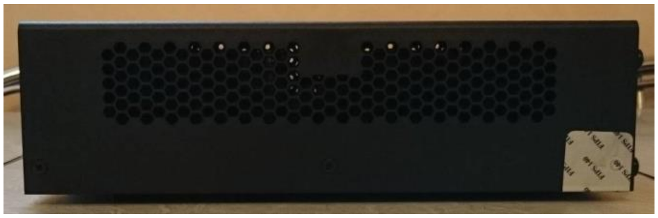


Figure 21 ASA 5506H-X Left Side TEL Placement

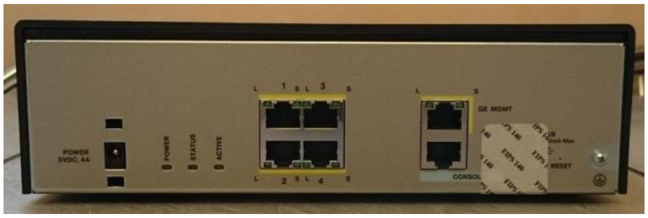


Figure 22 ASA 5506H-X Rear TEL Placement

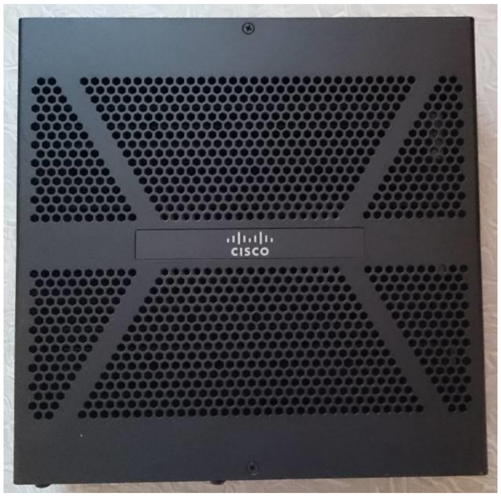


Figure 23 ASA 5506H-X Top View

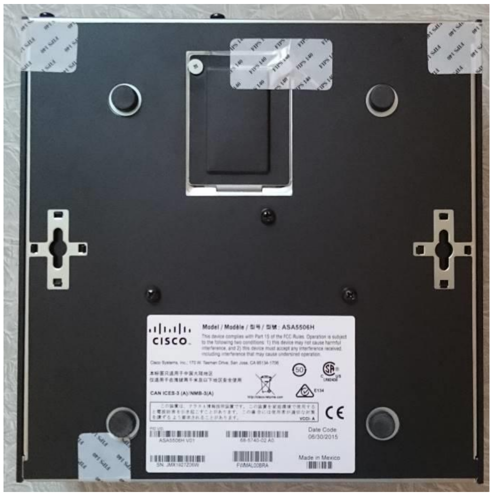


Figure 24 ASA 5506H-X Bottom TEL Placement

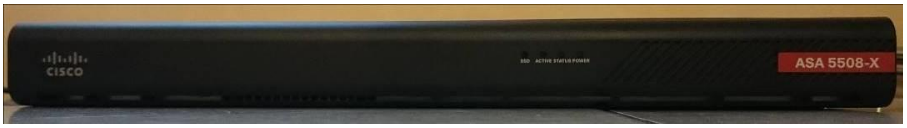


Figure 25 ASA 5508-X Front View

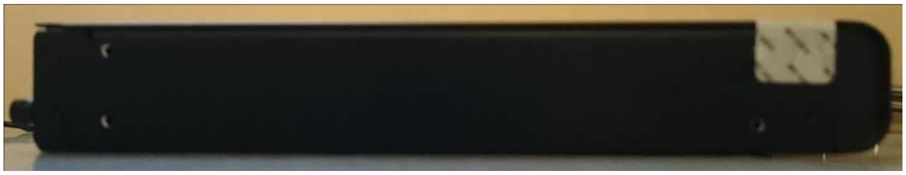


Figure 26 ASA 5508-X Right Side TEL Placement

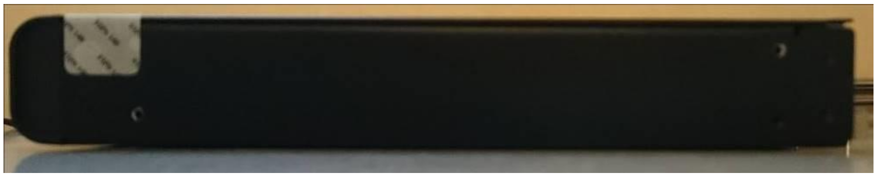


Figure 27 ASA 5508-X Left Side TEL Placement

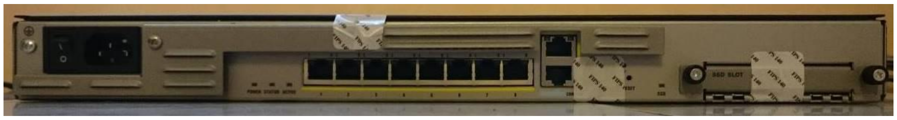


Figure 28 ASA 5508-X Rear TEL Placement

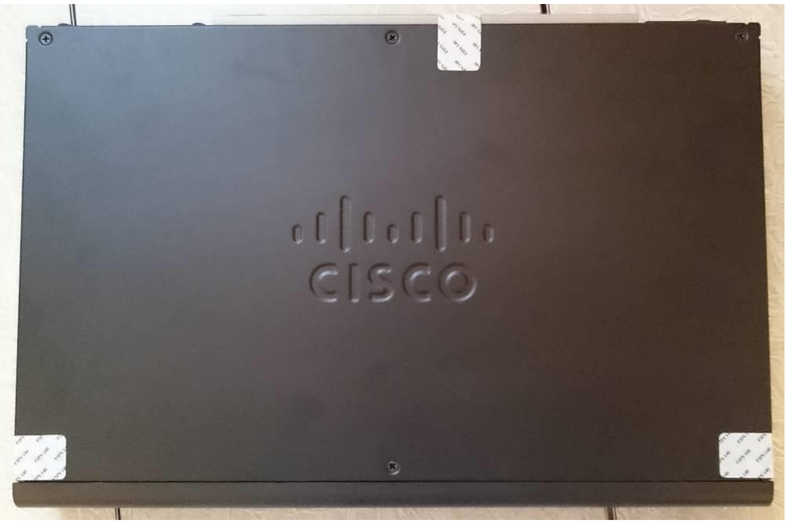


Figure 29 ASA 5508-X Top TEL Placement

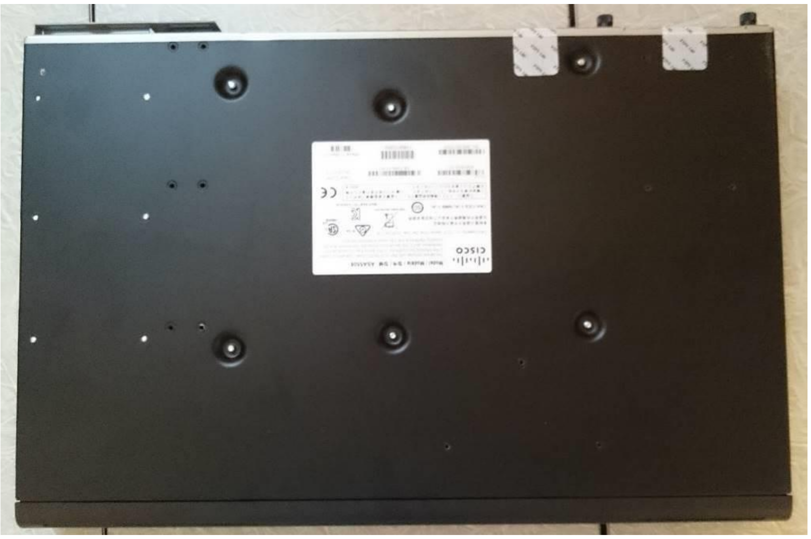


Figure 30 ASA 5508-X Bottom TEL Placement

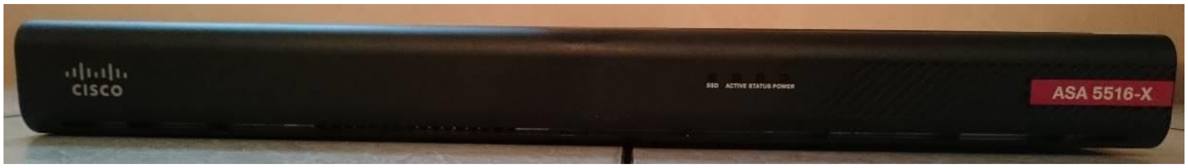


Figure 31 ASA 5516-X Front View

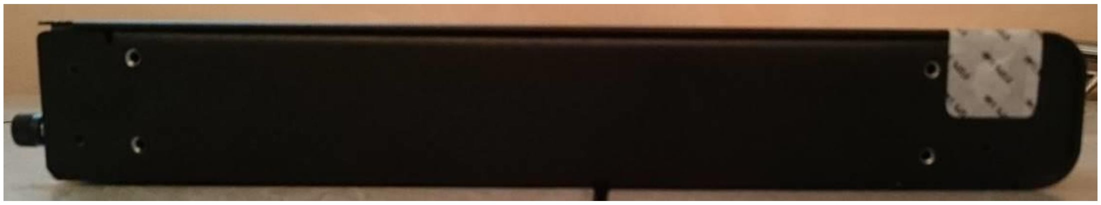


Figure 32 ASA 5516-X Right Side TEL Placement

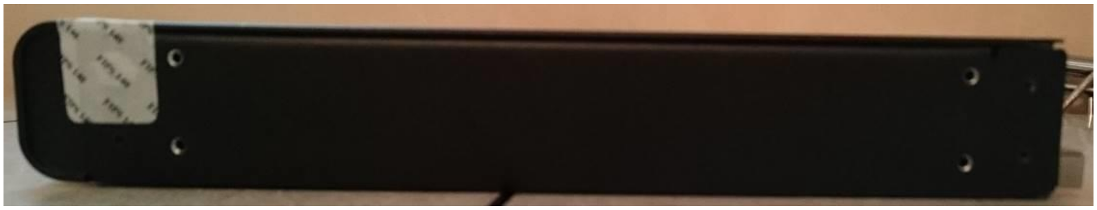


Figure 33 ASA 5516-X Left Side TEL Placement

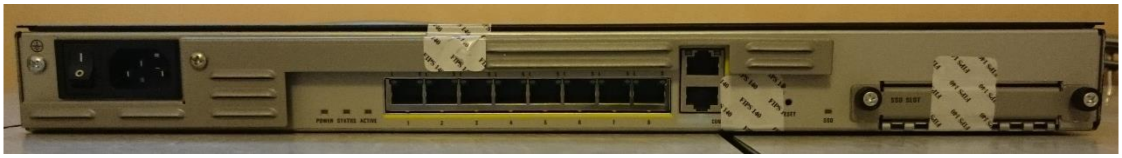


Figure 34 ASA 5516-X Rear TEL Placement

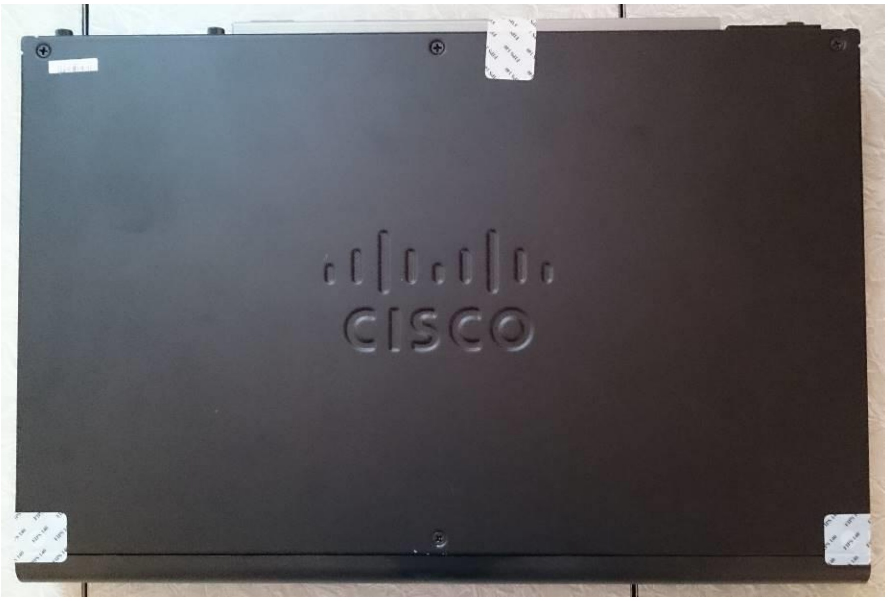


Figure 35 ASA 5516-X Top TEL Placement

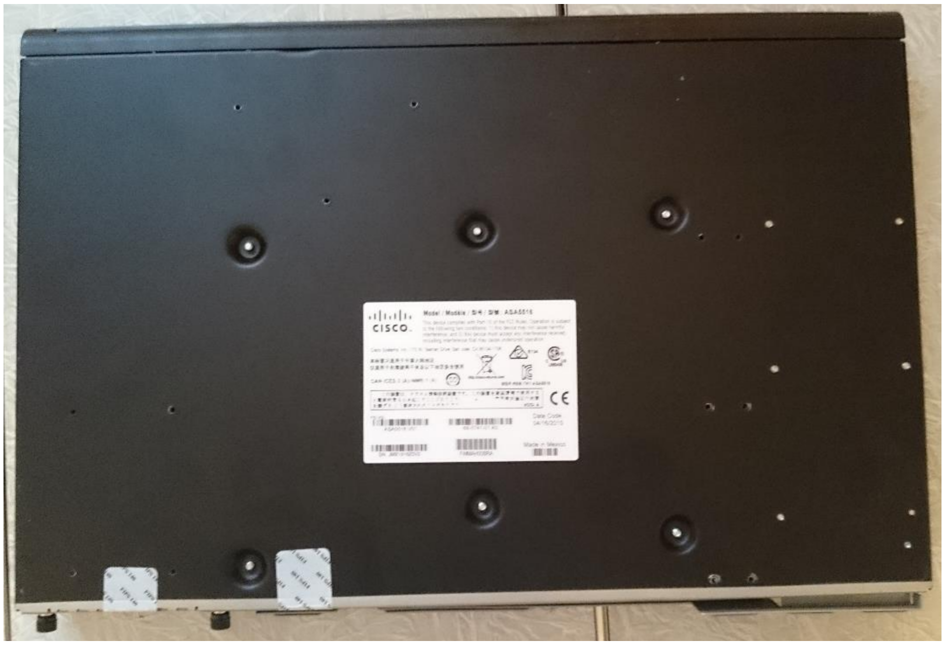


Figure 36 ASA 5516-X Bottom TEL Placement

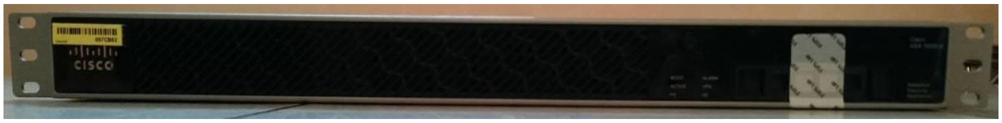


Figure 37   ASA 5525-X Front TEL Placement

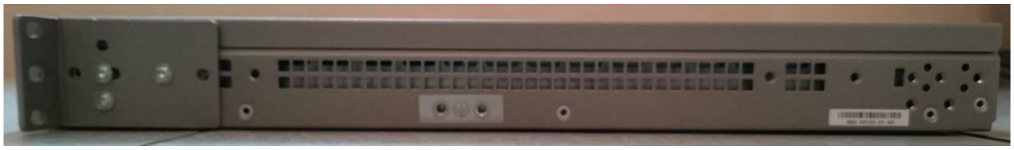


Figure 38 ASA 5525-X Right Side View

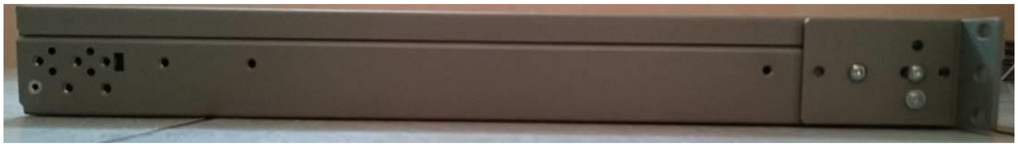


Figure 39 ASA 5525-X Left Side View

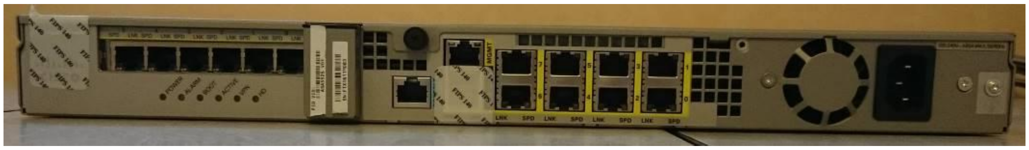


Figure 40 ASA 5525-X Rear TEL Placement

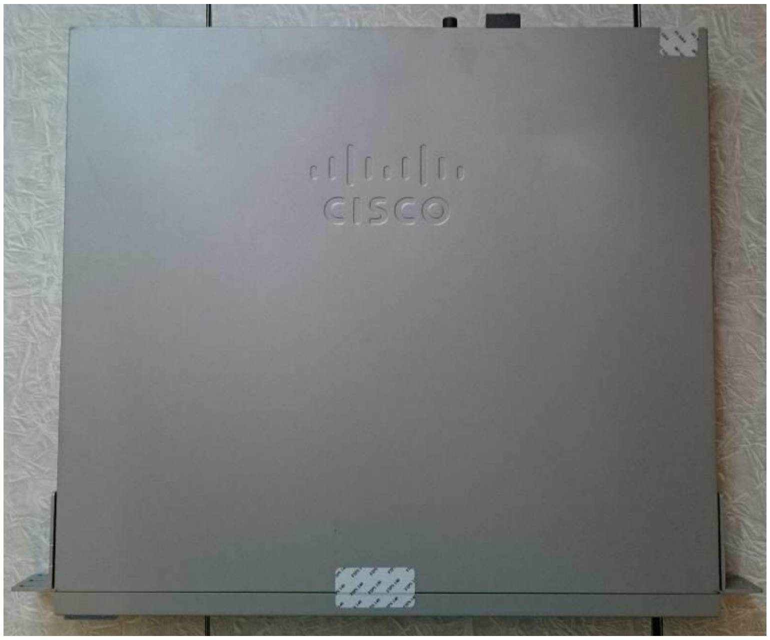


Figure 41 ASA 5525-X Top TEL Placement

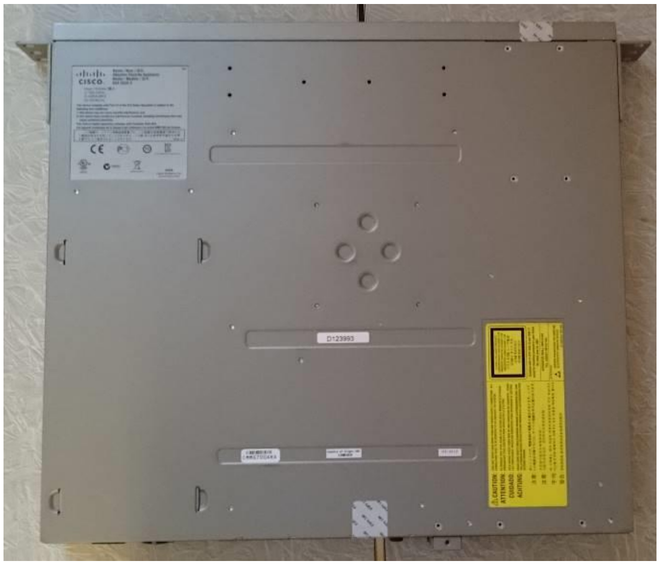


Figure 42 ASA 5525-X Bottom TEL Placement

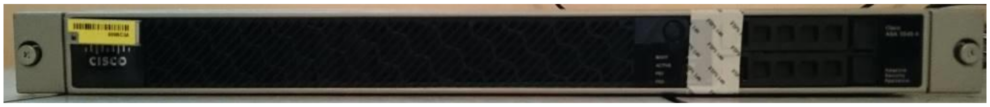


Figure 43 ASA 5545-X Front TEL Placement

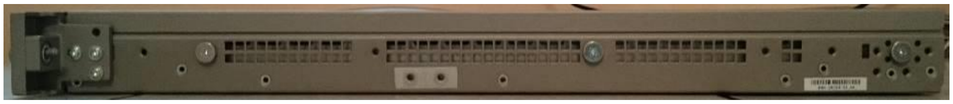


Figure 44 ASA 5545-X Right Side View

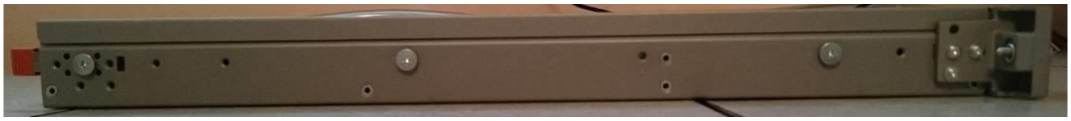


Figure 45 ASA 5545-X Left Side View

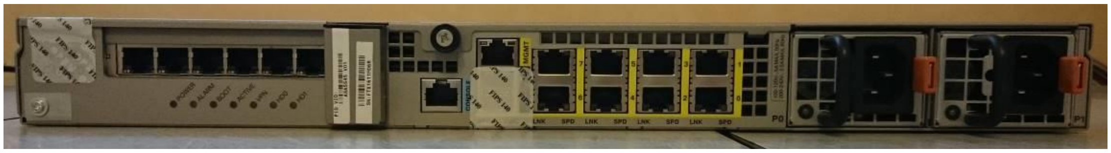


Figure 46 ASA 5545-X Rear TEL Placement

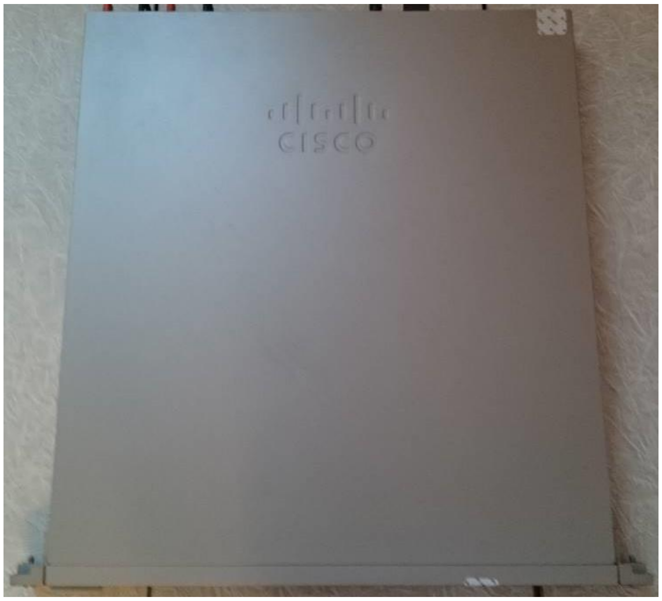


Figure 47 ASA 5545-X Top TEL Placement

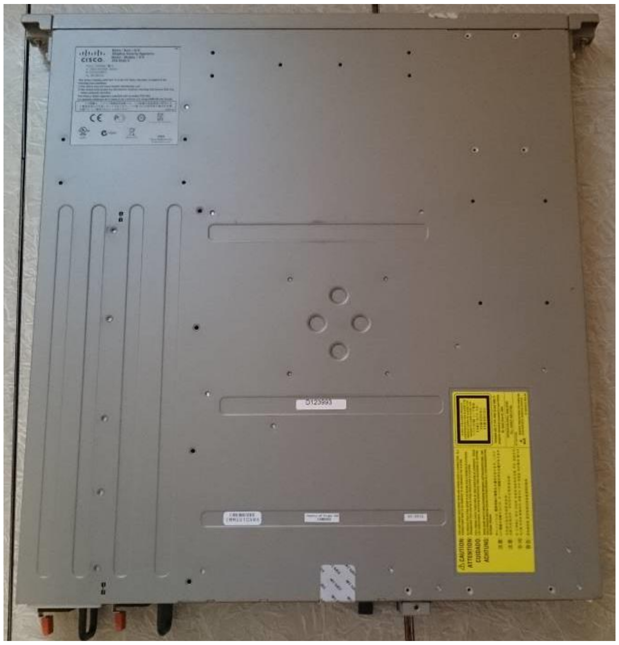


Figure 48 ASA 5545-X Bottom TEL Placement

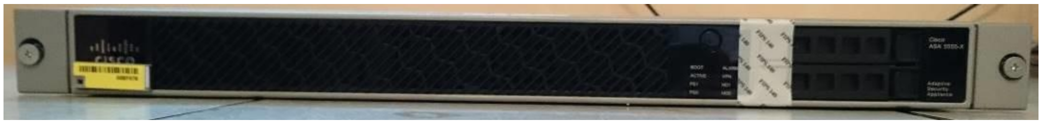


Figure 49 ASA 5555-X Front TEL Placement

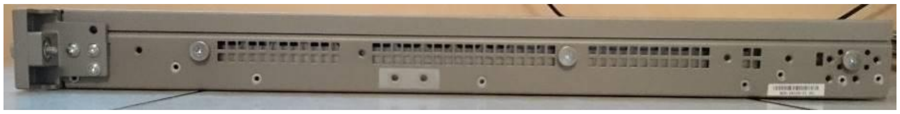


Figure 50 ASA 5555-X Right Side View

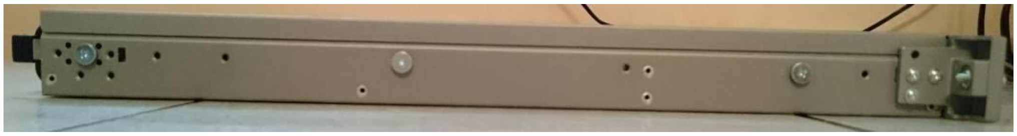


Figure 51 ASA 5555-X Left Side View

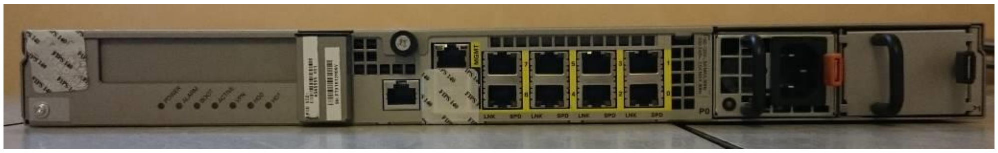


Figure 52 ASA 5555-X Rear TEL Placement

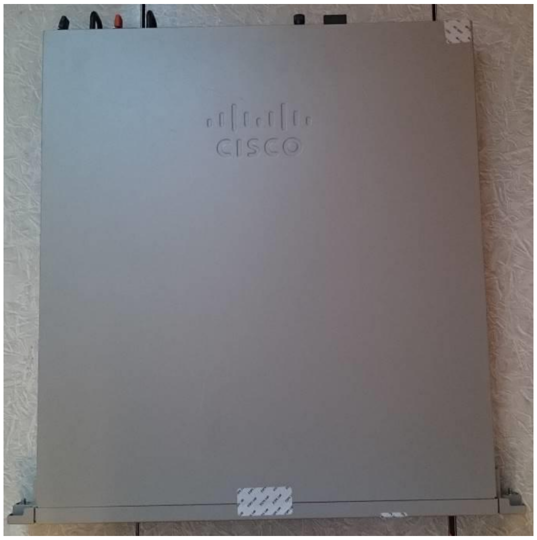


Figure 53 ASA 5555-X Top TEL Placement

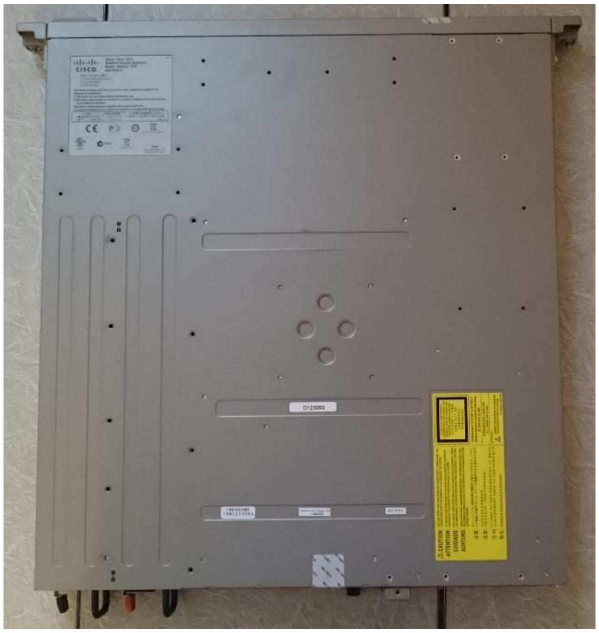


Figure 54 ASA 5555-X Bottom TEL Placement

Appling Tamper Evidence Labels

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 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.

3 Secure Operation

The module meets all the Level 2 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and modules are shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating the module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

3.1 Crypto Officer Guidance - System Initialization

The Cisco ASA 5500-X series security appliances were validated with adaptive security appliance firmware version 9.8 (file name: asa982-20-lfbff-k8.SPA and asa982-20-smp-k8.bin). The ASA 5506-X, ASA 5506H-X, ASA 5506W-X, ASA 5508-X, and ASA 5516-X run asa982-20-lfbff-k8.SPA. The ASA 5525-X, ASA 5545-X and ASA 5555-X run asa982-20-smp-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: Disable the console output of system crash information, using the following command:

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

Step 2: Install Triple-DES/AES licenses to require the security appliances to use Triple-DES and AES (for data traffic and SSH).

Step 3: 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
```

Note: If command fips disabled is entered, the module must be put back into factory setting (factory reset).

- Reboot system and while the system is booting, go into ROMMON
- Under the configuration mode, type admin-password erase, this will erase everything and bring the system back to factory defaults.

Step 4: Disable password recovery.

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

Step 5: Set the configuration register to bypass ROMMON prompt at boot.

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

Step 6: If using a Radius/TACACS+ server for authentication, perform the following steps (see Operator manual for specific TACACS+ commands). Otherwise, skip to step 7

```
(config)# aaa-server radius-server protocol radius
(config)# aaa-server radius-server host <IP-address>
```

Configure an IPsec tunnel to secure traffic between the ASA and the Radius server.
The pre-shared key must be at least 8 characters long.

Step 7: Enable AAA **authentication** for the console.

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

Step 8: Enable AAA **authentication** for SSH.

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

Step 9: Enable AAA **authentication** for Enable mode.

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

Step 10: Specify Privilege Level 15 for Crypto Officer and Privilege Level 1 for User and set up username/password for each role.

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

Step 11: Ensure passwords are at least 8 characters long.

Step 12: All default passwords, such as enable and telnet, must be replaced with new passwords.

Step 13: Apply tamper evident labels as described in the "Physical Security" section on page 17.

Step 14: Reboot the security appliances.

3.2 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/TACAS+ 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 TLS v1.2 packets using the following command:

```
(config)# ssl server-version tlsv1.2
(config)# ssl client-version tlsv1.2
```

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

c. Check TLS 1.2 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 Crypto Officer.

Step 8: Disable the TFTP server.

Step 9: Disable HTTP for performing system management in FIPS mode of operation. HTTPS with TLS should always be used for Web-based management.

Step 10: Ensure that installed digital certificates are signed using FIPS approved algorithms.

3.3 Identifying Module Operation in an Approved Mode

The following activities are required to verify that the module is operating in an Approved mode of operation:

1. Verify that the tamper evidence labels and FIPS opacity shields have been properly placed on the module based on the instructions specified in the “Physical Security” and “Secure Operation” sections of this document.
2. Verify that the length of User and Crypto Officer passwords and all shared secrets are at least eight (8) characters long, include at least one letter, and include at least one number character, as specified in the “Secure Operation” section of this document.
3. Issue the following commands: 'show crypto IPSec sa' and 'show crypto isakmp policy' to verify that only FIPS approved algorithms are used.

   In addition, for the Secure Operations steps required for the embedded cryptographic module, please refer to refer to certificate number 3261’s Security Policy.