Cisco ASA Service Module (SM)

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 1.0

June 21, 2016

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco ASA Security Module, hence forth referred to as ASA-SM, Blade running Firmware 9.1.7; referred to in this document as blade. This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 1 and how to run the modules 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	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	3
4	Finite State Model	1
5	Physical Security	1
6	Operational Environment	N/A
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

Table 1 Module Validation Level

1.3 References

This document deals only with the operations and capabilities of the Cisco ASA-SM blade listed above in section 1.2 in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the routers from the following sources:

The Cisco Systems website contains information on the full line of Cisco Systems security. Please refer to the following website:

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd802930c5.html

http://www.cisco.com/en/US/products/ps6120/index.html

http://www.cisco.com/en/US/products/ps11621/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 ASA SM identified above is referred to as ASA-SM Security Blades, Blades 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 ASA-SM Blades models identified in section 1.2 above 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 blades. 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 ASA-SM Blade

The ASA-SM, part number WS-SVC-ASA-SM1-K9, is a high performance security service module (SM) housed in the Catalyst 6500 with Sup2T chassis. It will serve as the next generation for the existing Firewall Service Module (FWSM).

As mentioned earlier, ASA-SM software is based on ASA code, the behavior and commands follow ASA as opposed to FWSM. The software version on ASA-SM is ASA 9.1.7. Cisco ASA-SM blades integrate world-class firewall and Secure Sockets Layer/IP Security (SSL/IPsec) VPN. These protocols are acceptable under FIPS 140-2 but are non-compliant for SP 800-135.

The following subsections describe the physical and security characteristics of the ASA-SM blade.

2.1 ASA SM and Cryptographic Module Physical Characteristics

ASA-SM Service Module is a high-speed, integrated network security module housed in Catalyst 6500 with Sup2T. Delivering industry-leading firewall data rates, this module provides exceptional scalability to meet the needs of today's dynamic organizations - in a single blade architecture.

The ASA-SM housed in the Catalyst 6500 with Sup2T provides enhanced security, reliability, and performance. With twice the performance and four times the session count of competitive network security modules, it supports up to:

- 20 Gbps maximum firewall throughput (max)

- 16 Gbps of maximum firewall throughput (multi-protocol)
- 300,000 connections per second
- 10 million concurrent connections
- 250 security contexts
- 1,000 VLANs

Its advanced features help reduce costs and operational complexity, while allowing management of multiple firewalls from the same platform. In addition, up to four ASA Services Module blades can be installed in the Catalyst 6500 with Sup2T, providing scalability to 64 Gbps.

The ASA Services Module makes it easy to add full firewall capabilities to an existing infrastructure by sliding a blade into an empty slot in an existing Catalyst 6500 with Sup2T - no additional rack space, cabling, power, or physical interface is required. It also works in tandem with other modules in the chassis to deliver robust security throughout the entire chassis, effectively making every port a security port. This is a multiple-chip embedded cryptographic module with the cryptographic boundary defined as just the blade. This module is used to support Remote Access VPN With TLSv1/ DTLSv1 and IKEv2/ ESPv3, Secure Shell SSHv2, Secure Sockets Layer (TLS/TLSv1), SNMPv3 and IKE v2 Site-to-Site VPN (with IKEv1 / ESPv1, IKEv2 / ESPv3 & manual keying) with Suite B. These protocols are acceptable under FIPS 140-2 but are non-compliant for SP 800-135.

2.2 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 provided 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 SM Physical Interface
Data Input Interface	VLAN
Data Output Interface	VLAN
Control Input Interface	VLAN Shutdown Button
Status Output Interface	VLAN Status LED ID LED

Table 2: Ports and Interfaces

2.3 Roles and Services

The security blades 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 by the module upon initial access to the module. As required by FIPS 140-2, there are two roles in the security blades that operators may assume: a Crypto Officer role and User role. The administrator of the security blades 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 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. 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. The probability of a random success in a one minute period is 187,595,543,116,800/100,000 = 1,875,955,431, which is less than 1 in 100,000.

User Services

Users can access the system in two ways:

1. By accessing the console port with a terminal program or via IPSec protected telnet or SSH session to an Ethernet port. The IOS prompts the User for username and password. If the password is correct, the User is allowed entry to the IOS executive program.

2. 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 consist of the following (r=read, w= write, x=execute, z=zeroize):

Services & Access	Description	Keys & CSPs
Status Functions (r)	Image version currently running, installed hardware components, and version of hardware installed.	User password
Network Functions (r, w, x)	Initiate diagnostic network services, such as ping.	User password
VPN functions (r, x)	Negotiation and encrypted data transport via VPN	ISAKMP pre-shared keys, IKE Authentication key, IKE Encryption Key, IPSec authentication keys, IPSec traffic keys, skeyid , skeyid _d, User passwords, Diffie-Hellman, ECDSA
Directory Services (r, x)	Display directory of files kept in flash memory.	User password
Perform Self-Tests (r, x)	Execute Known Answer Test on Algorithms within the cryptographic module.	N/A

Table 3 - User Services

Crypto Officer Services

The Crypto Officer role is responsible for the configuration and maintenance of the security blades and authenticates from the **enable** command (for local authentication) or the **login c**ommand (for AAA authentication) from the user services. The Crypto Officer services consist of the following:

The Crypto Officer services consist of the following:

Services & Access	Description	Keys & CSPs
Configure the Security Blade (r, w, z)	Define network interfaces and settings; provide for the entry and output of CSPs; set the protocols the security blades 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.	ISAKMP pre-shared secrets, IKE Authentication key, IKE Encryption Key, IPSec authentication keys, IPSec traffic keys, User passwords, skeyid, Enable password, Enable secret, Enable secret, Diffie-Hellman, ECDSA
Define Rules and Filters (r, w, z)	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.	Enable password
View Status Functions (r, x)	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.	Enable password
Manage the Security Blade (r, w, z)	Log off users, provide for the entry and output of CSPs, shutdown or reload the security blades, view complete configurations, view full status, manage user rights, and restore configurations.	Enable password
Set Encryption/Bypass (r, w, x, z)	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.	ISAKMP pre-shared secrets, IKE Authentication key, IKE Encryption Key, IPSec authentication keys, IPSec traffic keys, Enable secret, Diffie-Hellman, RSA, ECDSA
Perform Self-Tests (r, x)	Execute Known Answer Test on Algorithms within the cryptographic module.	N/A
SSL VPN (using TLSv1.0) (r, w, x, z)	Configure SSL VPN parameters, provide entry and output of CSPs.	TLS pre-master secret, TLS Traffic Keys, RSA, ECDSA
SSH (r, w, x, d)	Configure SSH	SSH v2 Authentication, SSH v2 session, RSA, Diffie-Hellman
Local Certificate Authority (r, w, z)	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

Table 4 - Crypto Officer Services

2.4 Unauthenticated Services

The services available to unauthenticated users are:

- Viewing the status output from the module's LEDs
- Powering the module on and off using the power switch
- Performing bypass service

2.5 Cryptographic Key Management

All keys and CSPs are protected by the password-protection on the Crypto Officer role login, 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.

The ASA-SM module securely administers both cryptographic keys and other critical security parameters such as passwords. 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 modules 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.

Key/CSP	Usage	Description	Storage	Zeroization
Diffie-Hellman private exponent	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. Please note that groups 1, 2 and 5 are not to be used in FIPS mode. This key was generated by calling FIPS approved SP800-90a DRBG	DRAM (plain text)	Automatically when session expires
Diffie-Hellman shared secret	Diffie-Hellman	This is the shared secret agreed upon as part of DH exchange. This key was generated by the module.	DRAM (plain text)	Automatically when session expires
Diffie-Hellman public key	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	DRAM (plain text)	Automatically when session expires

		(2048 bits) are supported. Please note that groups 1, 2 and 5 are not to be used in FIPS mode. This key was generated by calling FIPS approved SP800-90a DRBG		
RSA public keys	RSA 2048	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, 768 and 1024-bit key lengths are not to be used in FIPS mode). This key is generated by calling FIPS approved SP800-90a DRBG	Public Key - NVRAM (plain text)	Zeroized by "#crypto key zeroize rsa", write to startup config, followed by a module reboot
RSA private keys	RSA 2048	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, 768 and 1024-bit key lengths are not to be used in FIPS mode). This key was generated by calling FIPS approved SP800-90a DRBG	Private Key - NVRAM (plain text)	Zeroized by "# no crypto key generate rsa
skeyid	HMAC-SHA1/256/384/512	Value derived from the shared secret within IKE exchange.	DRAM (plain text)	Automatically after IKE session is terminated
skeyid_d	HMAC-SHA1/256/384/512	Value derived from the shared secret within IKE exchange.	DRAM (plain text)	Automatically after IKE session is terminated
ISAKMP pre-shared secret	Shared Secret	Used for authentication during IKE. This key was configured by Crypto Officer.	NVRAM (plain text)	Zeroized by "# no crypto isakmp key"
IKE authentication key	HMAC-SHA1/256/384/512	This key is used to authenticate IKE sessions. This key was derived in the module.	DRAM (plain text)	Automatically after IKE session is terminated
IKE encryption key	Triple-Des/AES	Used to encrypt IKE negotiations. This key was derived in the module.	DRAM (plain text)	Automatically after IKE session is terminated
IPSec authentication key	HMAC-SHA1/256/384/512	Exchanged using the IKE protocol and the public/private key pairs. These are Triple-DES or AES keys. This key was derived in the module.	DRAM (plain text)	Automatically after IPSec session is terminated
IPSec traffic keys	Triple-Des/AES/ HMAC-SHA1/256/384/512	Exchanged using the IKE protocol and the public/private key pairs. These are Triple-DES or AES keys. This key was derived in the module.	DRAM (plain text)	Automatically after IPSec session is terminated

RADIUS shared secret	Shared Secret	Used for authenticating the RADIUS server to the security appliances and vice versa. This key was configured by Crypto Officer.	NVRAM (plain text)	Zeroized by "# no radius-server key"
TACACS+ shared secret	Shared Secret	Used for authenticating the TACACS+ server to the security appliances and vice versa. This key was configured by Crypto Officer.	NVRAM (plain text)	Zeroized by "# no tacacs-server key"
User password	Shared Secret	Critical security parameters used to authenticate the User/Crypto-Officer login. This key was configured by Crypto Officer.	NVRAM (plaintext)	Overwrite with new password
Enable password	Shared Secret	Configured by Crypto Officer. It is used to authenticate Crypto officer.	NVRAM (plaintext)	Overwrite with new password
Enable secret	Shared Secret	Configured by Crypto Officer. It is used to authenticate Crypto officer role.	NVRAM (plaintext)	Overwrite with new password
TLS pre-master secret	Shared Secret	Shared secret created/derived using asymmetric cryptography from which new HTTPS session keys can be created. This key entered into the module in cipher text form, encrypted by RSA public key.	DRAM (plaintext)	Automatically when TLS session is terminated.
TLS traffic keys	Triple-DES/AES/ HMAC-SHA1/256/384/512	Used in HTTPS connections. Generated using TLS protocol. This key was derived in the module.	DRAM (plain text)	Automatically when TLS session is terminated
SSH v2 authentication keys	HMAC-SHA1/256/384/512	This key is used to perform the authentication between the SSH client and SSH server. This key was derived in the module.	DRAM (plain text)	Zeroized automatically when SSH sessions is closed
SSH v2 session encryption keys	Triple-Des/AES	This is the symmetric SSH key used to protect SSH session. This key was derived in the module.	DRAM (plain text)	Zeroized automatically when SSH sessions is closed
AES-GCM Encryption/decryption	AES-GCM 128/192/256	Symmetric Cipher Encrypts data blocks while performing decrypt-on-the-fly verification Decrypts data block	DRAM (plain text)	AES keys are dynamically generated IAW the RFCs and are not persistent, the new keys are regenerated for any AES-GCM connection after power is removed and restored.
ECDSA private key	ECDSA P-256,384,521	Key pair generation, signature generation/ verification	DRAM	Zeroized upon API call "#crypto key zeroize ecdsa"
ECDSA public key	ECDSA P-256,384,521	Key pair generation, signature generation/ verification	DRAM	Zeroized upon API call "#crypto key zeroize ecdsa"

DRBG Seed	SHA-512 Hash DRBG	This is the internal value generated by the module and used in the DRBG	DRAM	Power cycle the module
DRBG V value	SHA-512 Hash DRBG	This is the internal value generated by the module and used in the DRBG	DRAM	Power cycle the module
DRBG C value	SHA-512 Hash DRBG	This is the internal value generated by the module and used in the DRBG	DRAM	Power cycle the module
DRBG entropy1	SHA-512 Hash DRBG	This is the internal value generated by the module and used in the DRBG	DRAM	Power cycle the module

Table 5 Cryptographic Keys and CSPs

2.6 Cryptographic Algorithms

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

Approved Cryptographic Algorithms

The routers support the following FIPS-2 approved algorithm implementations:

	Adaptive Security Appliance OS(Firmware Algorithm Implementation)	CN1620
AES	2482	2050 & 2444
Triple-DES	1520	1321
SHS	2100	1794
HMAC	1524	1247
RSA	1271	1066
ECDSA	411	

[1]The entropy source is designed to produce jitter from free-running oscillators. Free-running oscillator jitter has been widely accepted in the academic community to provide a substantial amount of entropy. To go into more detail on the jitter: The time period of a ring oscillator output signal (wave form) vibrates in a random manner T=T+T' where T' is a random value. In high-quality circuits, like the Cavium source used, the range of T' is relatively small compared to T. This variation in oscillator period is called jitter. Local temperature effects cause the period of a ring oscillator to wander above and below the long-term average period. This is because the entropy accumulation from jitter tends to happen not linearly but as the square root of cycles. For more information on the relationship between thermal noise, jitter and signal period – "Jitter and Phase Noise in Ring Oscillators", IEEE J. Solid-State Circuits 34(6) (1999) 790-804. Note that the jitter of the 125 free-running oscillators are accumulated over 81 cycles into the 128-bit LFSR.
This product's entropy source is a hardware implementation that non-destructively combines noise from 125 free-running oscillators. Because each sample generated from a single oscillator offers less than a bit of entropy, all 125 oscillators are sampled 81 times as part of the LFSR accumulation. With the inherent hardware over-sampling, we are able to guarantee that the seed (seeding the DRBG) possesses at least 256 bits of entropy

DRBG	341	332

Table 6 Approved Cryptographic Algorithms

Note:

- RSA (Cert. #1066; non-compliant with the functions from the CAVP Historical RSA List).
  - FIPS186-2:
    ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1/256/384/512)), (2048 SHA(1))

- RSA (Cert. #1271; non-compliant with the functions from the CAVP Historical RSA List).
  - FIPS186-2:
    ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537
    ALG[RSASSA-PKCS1_V1_5] SIG(gen) (1024 SHA(1/256/384/512)), (2048/4096 SHA(1))

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 (key agreement; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength; non-compliant less than 112 bits of encryption strength)

Non-Approved Cryptographic Algorithms

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

- DES
- HMAC MD5
- MD5[2]
- NDRNG
- RC4
- HMAC-SHA1 is not allowed with key size under 112-bits

[2] Allowed in FIPS mode

2.7 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. The FIPS power-on self-tests are run regardless of the FIPS mode setting.

Self-tests performed

- ASA Self Tests
  - POSTs – Adaptive Security Blade OS (Firmware)
    - AES Encrypt/Decrypt KATs
    - DRBG KAT
    - ECDSA sign/verify
    - Firmware Integrity Test (using SHA-512)
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - HMAC-SHA-512 KAT
    - RSA KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - SHA–384 KAT
    - SHA-512 KAT
    - Triple-DES Encrypt/Decrypt KATs
  - POSTs – ASA On-board (Hardware)
    - AES GCM KAT
    - AES Encrypt/Decrypt KATs
    - DRBG KAT
    - HMAC-SHA-1 KAT
    - HMAC-SHA-256 KAT
    - HMAC-SHA-384 KAT
    - HMAC-SHA-512 KAT
    - RSA KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - SHA-384 KAT
    - SHA-512 KAT
    - Triple-DES Encrypt/Decrypt KATs
  - Conditional tests - Adaptive Security Blade OS (Firmware)
    - RSA pairwise consistency test (encrypt/decrypt and sign/verify)
    - ECDSA pairwise consistency test

        - Conditional Bypass test
        - Continuous random number generation test for FIPS approved and non-approved RNG
    - Conditional tests - ASA On-board (Hardware)
        - RSA pairwise consistency test (encrypt/decrypt and sign/verify)
        - Continuous random number generation test for FIPS approved SP800-90a DRBG

The security blades 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 blades 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 blade reboot.

3 Secure Operation of ASA-SM

The module meets all the Level 2 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the modules are shipped in Cisco boxes with Cisco adhesive. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating this router 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-SM is validated with adaptive security appliance firmware version 9.1.7, file names asa917-4-smp-k8.bin. This is 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: 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 3: Disable password recovery.
`(config)#`**`no service password-recovery`**

Step 4: Set the configuration register to bypass ROMMON prompt at boot.

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

Step 5: 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 6: Enable AAA **authentication** for the console.
(config)#**aaa authentication serial console LOCAL**
(config)#**username <name> password <password>**

Step 7: Enable AAA **authentication** for SSH.
(config)#**aaa authentication ssh console LOCAL**

Step 8: Enable AAA **authentication** for Enable mode.
(config)#**aaa authentication enable console LOCAL**

Step 9: 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 10: Ensure passwords are at least 8 characters long.

Step 11: All default passwords, such as enable and telnet, must be replaced with new passwords.

Step 12: Reboot the security appliances.