Cisco Firepower Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 0.4

August 8, 2018

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Firepower Cryptographic Module firmware 6.2 on the Cisco Adaptive Security Appliances. This security policy describes how the module meet the security requirements of FIPS 140-2 Level 1 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 Module*) details the U.S. Government requirements for cryptographic module. 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 is a non-proprietary Security Policy for the Cisco Firepower Cryptographic Module running on the Cisco Adaptive Security Appliances and additional rules imposed by Cisco Systems, Inc. More information is available on the module 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/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 Module 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 Firepower Cryptographic Module is referred to as Firepower Cryptographic Module, Module or the System.

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 Firepower Cryptographic Module running on the Cisco Adaptive Security Appliances models identified below along with 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 Firepower on Adaptive Security Appliances

Cisco® Firepower provides balanced security effectiveness with productivity. The module is designed to help handle network traffic in a way that complies with an organization's security policy—guidelines for protecting a network. A security policy may also include an acceptable use policy (AUP), which provides employees with guidelines of how they may use the organization's systems. The Firepower running on Cisco Adaptive Security Appliances (ASA) provides TLSv1.2 and SSHv2 security services.

2.1 Cryptographic Module Characteristics

The Firepower Cryptographic Module is defined as a multiple-chip standalone cryptographic module. The cryptographic logic boundary is defined as the area within the red dash box. Deployed inline, the system can affect the flow of traffic using access control, which allows specification, in a granular fashion, of how to handle the traffic entering, exiting, and traversing a network. The data that collected about network traffic and all the information gleaned from it can be used to filter and control that traffic.

The module was tested in the lab on the following platforms running non-modifiable Linux, Fire Linux OS 6.2:

1. Cisco ASA Hardware Platforms:

ASA 5506-X	ASA 5506H-X	ASA 5506W-X	ASA 5508-X
ASA 5516-X	ASA 5525-X	ASA 5545-X	ASA 5555-X

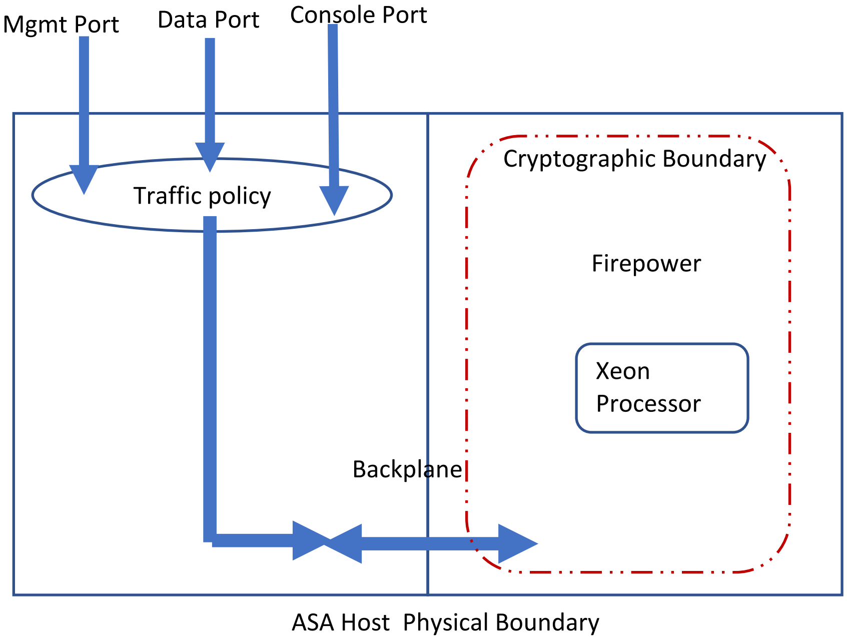

Diagram 1 Block Diagram

2.2 Module Interfaces

The physical interfaces provided by the Cisco ASA platforms are mapped to the following FIPS 140-2 defined logical interfaces: data input, data output, control input and status output. The logical interfaces and their mapping are described in the following table:

FIPS 140-2 Logical Interface	Logical Interface	Physical Interface
Data Input Interface	API input parameters	Mgmt port Console Port Data Ports
Data Output Interface	API output parameters	Mgmt port Console Port Data Ports
Control Input Interface	API function calls	Mgmt port Console Port Data Ports
Status Output Interface	API return codes	Mgmt port Console Port Data Ports

Table 2 Module Interfaces

2.3 Roles and Services

The module can be accessed via the API which connects to Console port, Data ports and Mgmt port by using one the following services:

- HTTPS/TLSv1.2
- SSHv2

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 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.

2.4 User Services

After entering the system via the API, the User is prompted for the username and password. If the password is correct, the User is allowed entry to the module management functionality. 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, protocols and firepower firmware version 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
SSH v2 Functions	Negotiation and encrypted data transport via SSH.	Operator password, DH private DH public key, DH Shared Secret, ECDH private ECDH public key, ECDH Shared Secret, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 encryption key, SSHv2 integrity key, DRBG Seed, DRBG entropy input, DRBG V, DRBG Key (r, w, d)
TLS v1.2 Functions	Negotiation and encrypted data transport via TLS.	TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption key, TLS integrity key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)

Table 3 User Services

2.5 Crypto Officer Services

The Crypto Officer role is responsible for the configuration of the module. After entering the system via the API, the CO is prompted for username and password. If the password is correct, the CO role is allowed entry to the module management functionality. 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	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.	TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption key, TLS integrity key, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 encryption key, SSHv2 integrity key, DRBG seed, DRBG entropy input, DRBG V, DRBG Key (r, w, d)
Firmware Installation	Install the firmware during the System Initialization	Integrity test key (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)
TLS v1.2 Functions	Configure TLS parameters, provide entry and output of CSPs.	TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption key, TLS integrity key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)
SSH v2 Functions	Configure SSH v2 parameter, provide entry and output of CSPs.	DH private DH public key, DH Shared Secret, ECDH private ECDH public key, ECDH Shared Secret, SSHv2 RSA private key, SSHv2 RSA public key, SSHv2 encryption key, SSHv2 integrity key, DRBG entropy input, DRBG seed, DRBG V, 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)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 6, Zeroization column.	All CSPs (d)

Table 4 Crypto Officer Services

2.6 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 2.6, the Crypto Officer must zeroize all CSPs which places the module into the non-FIPS mode of operation.

Services [1]	Non-Approved Algorithms
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.

2.7 Unauthenticated Services

The service for someone without an authorized role is to cycle power the module.

2.8 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 login and can be zeroized by the Crypto Officer. Zeroization consists of overwriting the memory that stored the key or refreshing the volatile memory.

The Crypto Officer needs to be authenticated to store keys. All Diffie-Hellman (DH)/ECDH keys agreed upon for individual sessions are directly associated with that specific session. The /dev/urandom device extracts bits from the urandom pool. This output is used directly to seed the NIST SP 800-90A CTR_DRBG.

The entropy comes from a process of extracting bits from /dev/urandom and is fed into the DRBG. The module provides approximately 277 bits entropy to instantiate the DRBG.

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

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG	384 bits	This is the entropy for SP 800-90A CTR_DRBG. Firmware based entropy source used to construct seed.	DRAM (plaintext)	Power cycle the device
DRBG seed	SP800-90A CTR_DRBG	384 bits	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from a firmware -based entropy source.	DRAM (plaintext)	Power cycle the device
DRBG V	SP800-90A CTR_DRBG	128 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	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
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
EC Diffie-Hellman shared secret	EC DH	Curves: P-256, P-384, P-521	The shared secret used in Elliptic Curve Diffie-Hellman (ECDH) exchange. Established per the Elliptic Curve Diffie-Hellman (ECDH) protocol.	DRAM (plaintext)	Power cycle the device
EC Diffie Hellman private key	EC DH	Curves: P-256, P-384, P-521	The private key used in EC Diffie-Hellman (DH) exchange. This key is generated by calling SP800-90A DRBG.	DRAM (plaintext)	Power cycle the device
EC Diffie Hellman public key	EC DH	Curves: P-256, P-384, P-521	The public key used in Elliptic Curve Diffie-Hellman (ECDH) exchange. This key is established per the EC Diffie-Hellman key agreement.	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
SSHv2 RSA Private Key	RSA	2048 bits	The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Uninstall the module
SSHv2 RSA Public Key	RSA	2048 bits	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)	Uninstall the module
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-1/256/384/512	160-512 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
TLS RSA private keys	RSA	2048 bits	Used for RSA signature verification in TLS connection This key was generated by calling FIPS approved DRBG.	NVRAM (plaintext)	Uninstall the module
TLS RSA public keys	RSA	2048 bits	Used for RSA signature verification in TLS connection. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module.	NVRAM (plain text)	Uninstall the module
TLS pre-master secret	keying material	8 plus 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 session is terminated.
TLS master secret	keying material	48 Bytes	Keying material used to derive other 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 key	Triple-DES/AES/AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	Used in 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-SHA-256/384	256-384 bits	Used for TLS connections integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
Integrity test key	HMAC-SHA-512	512 bits	A hard coded key used for firmware integrity test.	Hard coded for firmware integrity testing	Uninstall the module

Table 6 Cryptographic Keys and CSPs

2.9 Cryptographic Algorithms

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

Approved Cryptographic Algorithms

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 (TLS, SSH)	1008
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. 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.

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. #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

Non-Approved Cryptographic Algorithms

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

2.10 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

- POST tests
  - AES Known Answer Tests (Separate encrypt and decrypt)
  - AES-GCM Known Answer Tests (Separate encrypt and decrypt)
  - DRBG Known Answer Test (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
  - HMAC Known Answer Tests
    - HMAC-SHA1 Known Answer Test
    - HMAC-SHA256 Known Answer Test
    - HMAC-SHA384 Known Answer Test
    - HMAC-SHA512 Known Answer Test
  - RSA Known Answer Tests (Separate KAT for signing; Separate KAT for verification)
  - SHA-1 Known Answer Test
  - Firmware Integrity Test (HMAC-SHA512)
  - Triple-DES Known Answer Tests (Separate encrypt and decrypt)
- Conditional tests
  - RSA pairwise consistency test
  - CRNGT for SP800-90A DRBG
  - CRNGT for NDRNG

The module performs 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 module is initialized but prior to the initialization of the module’s interfaces; this prevents the security module 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 via the API and followed by a security module reboot.

3 Secure Operation

The module meets all the Level 1 requirements for FIPS 140-2. The module is shipped only to authorized operators by the vendor, and the module is 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 this 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 Firepower Cryptographic Module version 6.2 was validated using (File name: asasfr-5500x-boot-6.2.2-3.img and Cisco_Network_Sensor_Patch-6.2.2.2-109.sh.REL.tar). 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: Login to the device and accept the End User Agreement.
- Step 2: Change the default password.
- Step 3: Configure network settings, create default SSL policy. The CO shall only use FIPS approved/Allowed cryptographic algorithms listed above.
- Step 4: Log out the module by using “Ctrl^ x” to return to the ASA prompt. The module should be pingable from ASA.
- Step 5: Enter “show module” to see that module is up.