Cisco ASA Cryptographic Module

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Documentation Version 1.0

December 17, 2020

Table of Contents

1 Introduction

1.1 Purpose

This is the non-proprietary Security Policy for the Cisco ASA Cryptographic Module, henceforth referred to as ASA-CM, running firmware 9.12. This security policy describes how this module meets the security requirements of FIPS 140-2 Level 1 and how to run the module in a FIPS 140-2 mode of operation. This Security Policy 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 https://csrc.nist.gov/Projects/cryptographic-module-validation-program.

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-CM listed in section 1.1 above as it relates to the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available 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/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.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 (https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules) contains contact information for answers to technical or sales-related questions for the module.

1.4 Terminology

In this document, the Cisco ASA Cryptographic Module is referred to as Cisco ASA-CM, 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 ASA Cryptographic Module identified in section 1.1 above and explains the secure layout, configuration and operation of the module. This introduction section is followed by Section 2, which details the general features and functionality of the module. 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 Cryptographic Module

The Cisco ASA-CM is a cryptographic module that delivers enterprise-class firewall for businesses. Improving security at the Internet edge, high performance and throughput for demanding enterprise data centers. Now it's available in a blade form factor that can be integrated into the Cisco Firepower 4100 and 9300 Series.

The ASA 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 all using the ASA-CM.

Figure 1: Firepower 4110, 4115, 4120, 4125, 4140, 4145 and 4150

Cisco Firepower 4100 security appliance is a standalone modular security services platform with a one RU form factor. It is capable of running multiple security services simultaneously and so is targeted at the data center as a multi-service platform. It comprises a front-end "Management IO" (MIO) function and one Security Service card with x86 CPU complex. The MIO cards are the central place for all customer and management traffic as well as inter-card communications. The 4100 Series has dual multi-core processors, dual AC power supply modules, one 200 to 400-GB SSD, and 64 to 256-GB of DDR4 RAM depending on the model.

Figure 2: Firepower 9300

The modular standalone chassis offers high-performance and flexible I/O options that enables it to run multiple security services simultaneously. The Firepower 9300 security appliance contains a supervisor management I/O card called the Firepower 9300 Supervisor. The Supervisor provides chassis management.

Below is a list of part numbers for the ASA-CM module embedded in the Cisco Firmware 4100 or 9300 Security Appliances.

- FPR4110-ASA-K9
- FPR4115-ASA-K9
- FPR4120-ASA-K9
- FPR4125-ASA-K9
- FPR4140-ASA-K9
- FPR4145-ASA-K9
- FPR4150-ASA-K9
- FPR9K-SM-24
- FPR9K-SM-36
- FPR9K-SM-40
- FPR9K-SM-44
- FPR9K-SM-48
- FPR9K-SM-56

2.1 Cryptographic Module Physical Characteristics

The Cisco ASA-CM is an integrated network security module housed in a single blade architecture, which is designed to integrate into the Cisco Firepower 4100 or 9300 Series Appliances. Once integrated, the ASA-CM provides enhanced security, reliability, and performance. Delivering industry-leading firewall data rates, this module provides exceptional scalability to meet the needs of today's dynamic organizations.

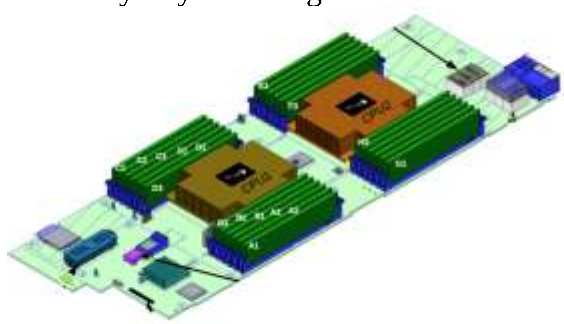

Figure 3: ASA-CM Blade

2.2 Cryptographic Boundary

The Cisco ASA-CM is a multiple-chip embedded cryptographic module with the cryptographic boundary defined as the physical perimeter of the blade as outlined in a red dashed line below.

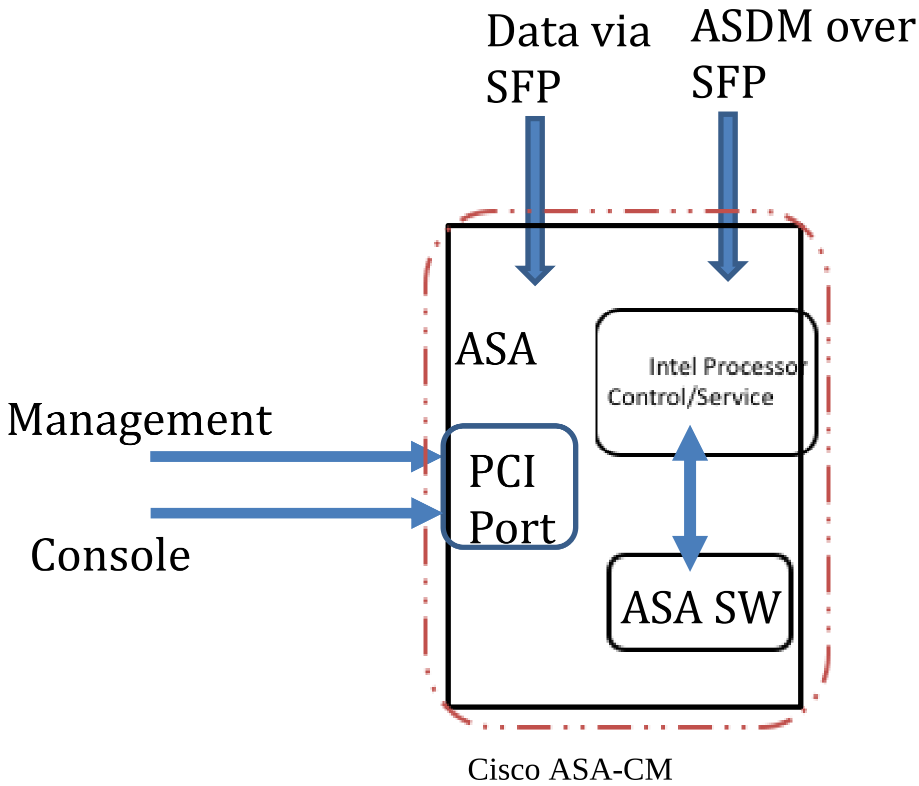

Diagram 1 Block Diagram

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 logical interfaces and their mapping are described in the following table:

FIPS 140-2 Logical Interfaces	Module Physical Interfaces
Data Input	SFP Ethernet Ports PCI port
Data Output	SFP Ethernet Ports PCI port
Control Input	SFP Ethernet Ports PCI port
Status Output	SFP Ethernet Ports PCI port LED

Table 2 Module's Physical/Logical Boundary Interfaces

2.4 Roles and Services

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

- SSHv2
- HTTPS/TLSv1.2
- IPSec/IKEv2

Authentication is identity-based. As required by FIPS 140-2, there are two roles that operators may assume: a Crypto Officer role and User role. The module upon initial access to the module authenticates both of these roles. 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 other shared secrets must each be at least eight (8) characters long, including at least one six (6) alphabetic characters, (1) integer number and one (1) special character in length (enforced procedurally). See the Secure Operation section for more information. Given these restrictions, the probability of randomly guessing the correct sequence is one (1) in 6,326,595,092,480 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total). The calculation should be 52x52x52x52x52x52x32x10 = 6,326,595,092,480. Therefore, the associated probability of a successful random attempt is approximately 1 in 6,326,595,092,480, which is less than the 1 in 1,000,000 required by FIPS 140-2.

In addition, for multiple attempts to use the authentication mechanism during a one-minute period, under the optimal modern network condition, if an attacker would only get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/ 6,326,595,092,480 = 1/105,443,251, which is less than 1 in 100,000 required by FIPS 140-2.

Additionally, when using RSA based authentication, RSA key pair has modulus size of 2048 bits, thus providing 112 bits of strength, which means 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 chances 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 8.65x10^31 (2^112 /60 = 8.65 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 either SSHv2 or HTTPS/TLSv1.2. The User role can be authenticated via either Username/Password or RSA based authentication method. 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/IKEv2 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	Description	Keys and CSPs Access
Status Functions	View state of interfaces and protocols, version of firmware currently running.	N/A
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	N/A
Directory Services	Display directory of files kept in flash memory.	N/A
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
IPSec VPN	Negotiation and encrypted data transport via IPSec VPN.	Operator password, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, skeyid, skeyid_d, SKEYSEED, IKE session encryption 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, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, SSHv2 Private Key, SSHv2 Public Key, SSHv2 integrity key, 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 secret, TLS encryption keys, 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

A Crypto Officer (CO) enters the system by accessing the Console port or SSH v2, HTTPS/TLSv1.2. The CO role can be authenticated via either Username/Password or RSA based authentication method. The other means of accessing the console is via an IPSec/IKEv2 session. This session is authenticated either using a shared secret or RSA digital signature authentication mechanism. A Crypto Officer may assign permission to access the Crypto Officer role to additional accounts, thereby creating additional Crypto Officers.

The Crypto Officer role is responsible for the configuration of the module. 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	Description	Keys and CSPs Access
Configure the Security	Define network interfaces and settings, create command aliases, set the protocols the router will support, enable interfaces and network services, set system date and time, and load authentication information.	DRBG entropy input, DRBG seed, DRBG V, DRBG C, DRBG key, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, SSHv2 private key, SSHv2 public key, SSHv2 session key, SSHv2 integrity key, ECDSA private key, ECDSA public key, TLS RSA private key, TLS RSA public key, TLS pre-master secret, TLS master secret, TLS encryption keys, TLS integrity key, ISAKMP preshared, skeyid, skeyid_d, SKEYSEED, IKE session encryption key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPSec encryption key and IPSec authentication key (r, w, d)
Firmware integrity	Execute firmware integrity verification	Integrity test key (r, w, d)
RADIUS / TACACS+ functions	Provide entry of shared secret CSP	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 router configuration, routing tables, active sessions health, temperature, memory status, voltage, packet statistics, review accounting logs, and view physical interface status.	N/A
Configure Encryption/Bypass	Configure Encryption or Bypass service.	ISAKMP preshared, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, Operator password, Enable password, IKE session encryption 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)	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 secret, TLS encryption keys, TLS 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, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, skeyid, skeyid_d, SKEYSEED, IKE session encryption 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)
SSHv2 Functions	Configure SSHv2 parameter, provide entry and output of CSPs.	Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, SSHv2 private key, SSHv2 public key, SSHv2 integrity key, SSHv2 session 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)
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
SSH	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES Asymmetric: 768-bit/1024-bit RSA (key transport), 1024-bit Diffie-Hellman
IPSec	Hashing: MD5, MACing: MD5 Symmetric: DES, RC4 Asymmetric: RSA (key transport), ECDSA, Diffie-Hellman

[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.

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.

To put the module back into the FIPS mode from the non-FIPS mode, the CO must zeroize all Keys/CSPs used in non-FIPS mode, and then strictly follow up the steps in section 3 of this document to put the module into the FIPS mode.

All services available can be found at CLI Book 1: Cisco ASA Series General Operations CLI Configuration Guide, 9.12. Updated: June 25, 2020. https://www.cisco.com/c/en/us/td/docs/security/asa/asa912/configuration/general/asa-912-general-config.html. This site lists all configuration guides.

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.

2.9 Operational Environment

The module is a hardware module. The module's operating system is non-modifiable. Thus, the requirements from FIPS 140-2 level 2, section 4.6.1, are not applicable to the module.

2.10 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. 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. The entropy source falls into IG 7.14, Scenario #1a: A hardware module with an entropy-generating NDRNG inside the module's cryptographic boundary. The entropy source provides at least 256 bits of entropy to seed SP800-90a DRBG for the use of key generation.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG (AES-256) or HASH_DRBG (SHA-512)	384 bits/512bits	This is the entropy input for SP 800-90A CTR_DRBG and HASH_DRBG, 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 the 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 (as part of SSH and IKE/IPSec). Established per the Diffie-Hellman key agreement.	DRAM (plaintext)	Power cycle the device
Diffie-Hellman private key	DH	224-379 bits	The private key used in Diffie-Hellman (DH) exchange (as part of SSH and IKE/IPSec). 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 (as part of SSH and IKE/IPSec). 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)	Automatically when IPSec session is terminated
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)	Automatically when IPSec session is terminated

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)	Automatically when IPSec session is terminated
IKE session encryption 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)	Automatically when IPSec session is terminated
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)	Automatically when IPSec session is terminated
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. Internally generated by the module.	NVRAM (plaintext)	Zeroized by RSA/ECDSA keypair deletion command
IPSec encryption key	Triple-DES/AES/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)	Automatically when IPSec session is terminated
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)	Automatically when IPSec session is terminated

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
Operator password	Password	8 plus characters	The password of the User role. This CSP is entered by the User.	NVRAM (plaintext)	Erase the password
Enable password	Password	8 plus characters	The password of the CO role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Erase the password
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)	Erase the 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)	Erase the secret
SSHv2 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 public key	RSA	2048 bits modulus	The SSHv2 public key used in SSHv2 connection. This key is internally generated by the module.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
SSHv2 integrity key	HMAC-SHA-1	160 bits	Used for SSHv2 connections integrity to assure the traffic integrity. This key is derived via key derivation function defined in SP800-135 KDF (SSH).	DRAM (plaintext)	Automatically when SSH session is terminated
SSHv2 session 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
ECDSA private key	ECDSA	Curves: P-256,384,521	Key pair generation, signature generation/Verification. The seed used in generating ECDSA parameters 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
TLS RSA private keys	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiation. The seed used in generating RSA parameters was	NVRAM (plaintext)	Zeroized by RSA keypair deletion command

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
			generated by calling FIPS approved DRBG.		
TLS RSA public keys	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiation. The seed used in generating RSA parameters was generated by calling FIPS approved DRBG.	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 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 keys	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 via key derivation function defined in SP800-135 KDF (TLSv1.2).	DRAM (plaintext)	Automatically when TLS session is terminated
TLS integrity key	HMAC-SHA-256/384	256-384 bits	Used for TLS integrity to assure the traffic integrity. This key was derived in the module via key derivation function defined in SP800-135 KDF (TLSv1.2).	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 erasing the firmware image

Table 6 Cryptographic Keys and CSPs

2.11 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:

	Cisco Security Crypto (Firmware) [2]	On-board Chip (Cavium Nitrox III)[3]	On-board Chip (Cavium Nitrox V)[4]
AES (128/192/256 CBC, GCM)	4905/C784	2035 (AES #2034 is the prerequisite algorithm under AES #2035)	C1026
Triple-DES (CBC, 3-key)	2559/C784	1311	C1026
SHS (SHA-1/256/384/512)	4012/C784	1780	C1026
HMAC (SHA-1/256/384/512)	3272/C784	1233	C1026
RSA (KeyGen, SigGen and SigVer; PKCS1_V1_5; 2048bits)	2678/C784		
ECDSA (PKG, SigGen and SigVer; P-256, P-384, P-521)	1254/C784		
CTR_DRBG (AES-256)	1735/C784		
HASH_DRBG (SHA-512)		197	C1026
CVL Component (IKEv2, TLS, SSH)	1521/C784		
CKG (vendor affirmed)			

Table 7 Approved Cryptographic Algorithms and Associated Certificate Numbers

Note:

- 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 operations of one of the two parties involved in the TLS key establishment scheme were performed entirely within the cryptographic boundary of the module being validated. 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

[2] Firmware algorithm implementation is available on each model.

[3] On-board Chip (Cavium Nitrox III) algorithm implementation is available on FPR 4110-ASA-K9, FPR 4120-ASA-K9, FPR 4140-ASA-K9, FPR 4150-ASA-K9, FPR9K-SM-24, FPR9K-SM-36, FPR9K-SM-44 and FPR9K-SM-40 models

[4] On-board Chip (Cavium Nitrox V) algorithm implementation is available on FPR 4115-ASA-K9, FPR 4125-ASA-K9, FPR 4145-ASA-K9, FPR9K-SM-48 and FPR9K-SM-56 models.

from which the AES GCM encryption keys are derived. The operations of one of the two parties involved in the IKE key establishment scheme shall be performed entirely within the cryptographic boundary of the module being validated. 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 the SSH, TLS and IPSec protocols, other than the KDFs, have been tested by the CAVP and CMVP.
- 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}.
- In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per section 6 in SP800-133. The resulting generated 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 Certs. #1521 and #C784, 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 (entropy source)

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)
- 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

2.12 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 ensure 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 – Cisco Security Crypto (Firmware)
        - AES-CBC Encrypt/Decrypt KATs
        - AES-GCM KAT
        - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
        - ECDSA (Sign and Verify) Pairwise Consistency Test
        - Firmware Integrity Test (RAS 2048 with SHA-512)
        - HMAC (SHA-1/256/384/512) KATs
        - RSA KATs (separate KAT for signing; separate KAT for verification)
        - SHA-1/256/384/512 KATs
        - Triple-DES-CBC Encrypt/Decrypt KATs
    - POSTs – ASA On-board (Hardware)
        - AES-CBC Encrypt/Decrypt KATs
        - AES-GCM KAT
        - DRBG KAT (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
        - HMAC (SHA-1/256/384/512) KATs
        - SHA-1/256/384/512 KATs
        - Triple-DES-CBC Encrypt/Decrypt KATs
    - Conditional tests - Cisco Security Crypto (Firmware)
        - RSA pairwise consistency test
        - ECDSA pairwise consistency test
        - Conditional Bypass test
        - CRNGT for SP800-90A DRBG
        - CRNGT for NDRNG
    - Conditional tests - ASA On-board (Hardware)
        - CRNGT for SP800-90A DRBG
        - CRNGT for NDRNG

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 module performs 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.

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 ASA Cryptographic Module was validated with ASA firmware version 9.12, which is the only allowable firmware for the current 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: 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.

Note: The use of an IPSec tunnel is only a suggested means. What is actually used is up to the user as long as the means provides a secure tunnel using only FIPS algorithms.

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.

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 TLSv1.2 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 V1.2 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.

