Cisco Adaptive Security Appliance (ASA) Virtual

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 0.5

Last Update: January 6, 2021

Table of Contents

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Adaptive Security Appliance (ASA) Virtual running software version 9.12, referred to in this document as ASAv. This security policy describes how the 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 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 https://csrc.nist.gov/groups/computer-security-division/security-testing-validation-and-measurement .

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	N/A
6	Operational Environment	1
7	Cryptographic Key management	1
8	Electromagnetic Interface/Electromagnetic Compatibility	1
9	Self-Tests	1
10	Design Assurance	1
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

Table 1 ASAv Module Validation Level

1.3 References

This document deals with the specification of the security rules listed in Table 1 above, under which the Cisco Adaptive Security Appliance (ASA) Virtual will operate, including the rules derived from the requirements of FIPS 140-2, FIPS 140-2IG and additional rules imposed by Cisco Systems, Inc. More information is available from the following Cisco Systems websites:

http://www.cisco.com/c/en/us/products/index.html

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

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

The NIST Validated Modules website (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 Adaptive Security Appliance (ASA) Virtual model identified is referred to as ASA virtual, ASAv, virtual, 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 Adaptive Security Appliance (ASA) Virtual 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 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 Adaptive Security Appliance (ASA) Virtual

Cisco® Adaptive Security Appliance (ASA) Virtual Series Next-Generation Firewalls provides balanced security effectiveness with productivity. This solution offers the combination of the industry's most deployed stateful firewall with a comprehensive range of next-generation network security services, intrusion prevention system (IPS), content security, secure unified communications, TLSv1.2, SSHv2, IPSec/IKEv2, and Cryptographic Cipher Suite B, all delivering enterprise-class security for business-to-enterprise networks in a virtual environment.

2.1 Cisco Servers

Cisco Adaptive Security Appliance (ASA) Virtual runs on many different UCS servers with various hypervisors.

For the purposes of this validation, the module was tested in the lab on the following servers:

OS	Platform	Hypervisor	Processor
FXOS version 2	Cisco UCS C220 M5	VMware ESXi 6.0	Intel Xeon Silver 4110
FXOS version 2	Cisco UCS C220 M5	VMware ESXi 6.5	Intel Xeon Silver 4110
FXOS version 2	ENCS-5412	NFVIS 3	Intel Xeon D-1528

Table 2 Testing Configuration

Cisco does not restrict the use of any hypervisor. Along with supporting ESXi and NFVIS listed above Cisco also supports the use of KVM’s and AWS (cloud service) on Cisco UCS and NFVIS on ENCS platforms.

Additionally, the CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

2.2 Cryptographic Boundary

The cryptographic module is defined as a multi-chip standalone software module, ASA virtual module (yellow box), while the physical boundary is defined as the hard case enclosure around the Server on which everything runs (blue box). Then the logical boundary is the ASA virtual module, hypervisor, API and processor (red dash box).

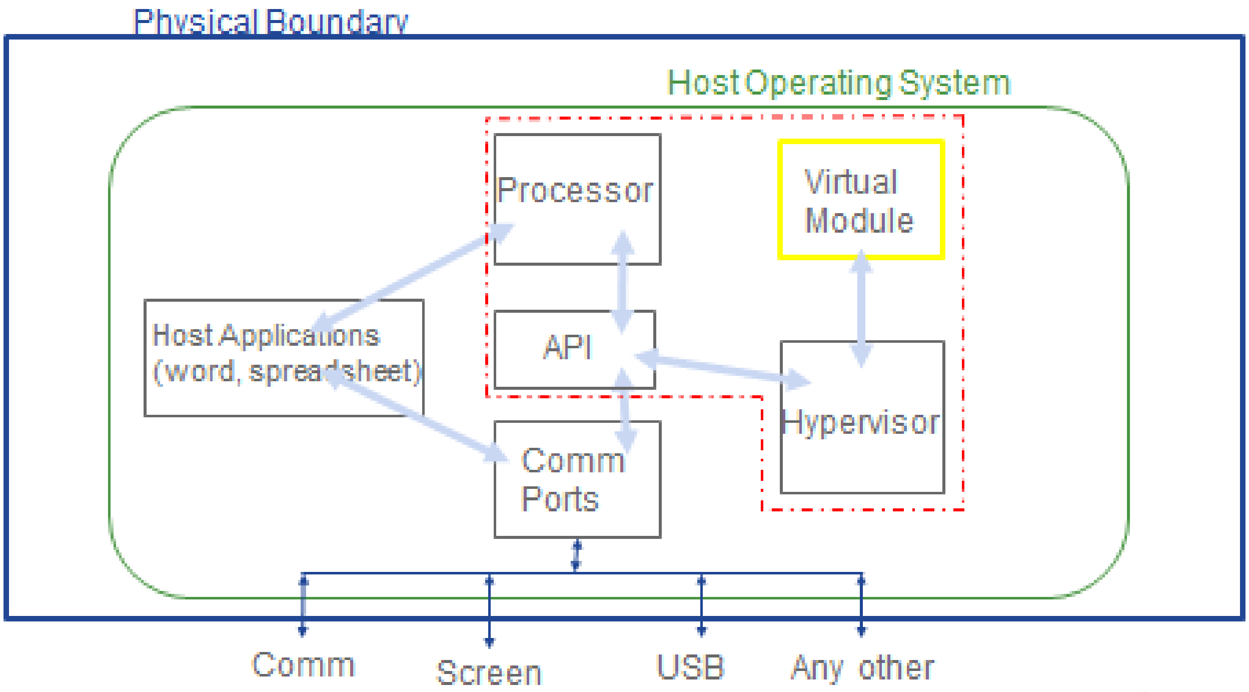

Figure 1 – Block diagram

The module makes use of the physical interfaces of the tested platform(s) hosting the virtual environment upon which the module is installed. The hypervisor controls and directs all interactions between the ASAv and the operator, and is responsible for mapping the module's virtual interfaces to the GPC's physical interfaces.

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 and status output. The module provides no power to external devices and takes in its power through normal power input/cord. The logical interfaces and their mapping are described in the following table:

Physical Port/Interface	ASA Virtual	FIPS 140-2 Interface
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Ports	**Data Input Interface**
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Ports	**Data Output Interface**
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Ports	**Control Input Interface**
Host System Ethernet (10/100/1000) Ports; Host System Serial Port	Virtual Ethernet Ports, Virtual Serial Ports	**Status Output Interface**

Table 3 Module Interfaces

2.4 Roles, Services, and Authentication

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

- Virtual Console Port
- IPSec/IKEv2
- SSH v2
- HTTPS/TLSv1.2

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

The User and Crypto Officer passwords and all 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. Similarly, for multiple attempts to use the authentication mechanism during a one-minute period, under the optimal modern network condition, an attacker would probably get 60,000 guesses per minute. Therefore, the associated probability of a successful random attempt during a one-minute period is 60,000/ 2^112 = 1/8.67x10^28, which is less than 1 in 100,000 required by FIPS 140-2.

User Services

A User enters the system by accessing either virtual console port, SSHv2, HTTPS/TLSv1.2 or IPSec/IKE via the virtual ethernet port. 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 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 software currently running.	Operator password (r)
Terminal Functions	Adjust the terminal session (e.g., lock the terminal, adjust flow control).	Operator password (r)
Directory Services	Display directory of files kept in flash memory.	Operator password (r)
Self-Tests	Execute the FIPS 140 start-up tests on demand	N/A
IPSec VPN Functions	Negotiation and encrypted data transport via IPSec VPN	Operator password, DRBG entropy input, DRBG seed, DRBG V, DRBG key, skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private Key, IKE authentication public key, IPSec encryption key and IPSec authentication key (r, w, d)
SSHv2 Functions	Negotiation and encrypted data transport via SSHv2	Operator password, DRBG entropy input, DRBG seed, DRBG V, DRBG key, SSHv2 private key, SSHv2 public key, SSHv2 integrity key and SSHv2 session key (r, w, d)
HTTPS/TLS (TLSv1.2) Functions	Negotiation and encrypted data transport via HTTPS/TLSv1.2	Operator password, DRBG entropy input, DRBG seed, DRBG V, DRBG 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 and TLS integrity key (r, w, d)

Table 4 - User Services

Crypto Officer Services

A Crypto Officer (CO) enters the system by accessing either virtual console port, SSHv2, HTTPS/TLSv1.2 or IPSec/IKE via the virtual ethernet port. 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. The Crypto Officer 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 module will support, enable interfaces and network services, set system date and time, and load authentication information.	DRBG entropy input, DRBG seed, DRBG V, DRBG key, Diffie-Hellman private key, Diffie-Hellman public key, Diffie-Hellman shared secret, ECDSA private key, ECDSA public key, SSHv2 private key, SSHv2 public key, SSHv2 integrity key, SSHv2 session 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)
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 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)
Software Integrity Verification	Execute software integrity verification.	Integrity test key (r, w, d)
Configure Encryption/Bypass	Set up the configuration tables for IP tunneling. Set preshared keys and algorithms to be used for each IP range or allow plaintext packets to be set from specified IP address.	Operator password, Enable password, ISAKMP preshared, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPSec encryption key, IPSec authentication key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
HTTPS/TLS (TLSv1.2) Functions	Configure HTTPS/TLS 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 and DRBG key (r, w, d)
SSHv2 Functions	Configure SSHv2 parameter, provide entry and output of CSPs.	SSHv2 private key, SSHv2 public key and SSHv2 session key, SSHv2 integrity key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
IPSec VPN Functions	Configure IPSec VPN parameters, provide entry and output of CSPs.	ISAKMP preshared, skeyid, skeyid_d, SKEYSEED, IKE session encrypt key, IKE session authentication key, IKE authentication private Key, IKE authentication public key, IPSec encryption key, IPSec authentication key, DRBG entropy input, DRBG seed, DRBG V and DRBG key (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
User services	The Crypto Officer has access to all User services.	Operator password (r, w, d)
Local Certificate Authority	Allows the ASA to be configured as a Root Certificate Authority and issue user certificates for SSL VPN use (AnyConnect and Clientless). The ASA can then be configured to require client certificates for authentication.	N/A
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 7, Zeroization column.	All CSPs (d)

Table 5 - Crypto Officer Services

2.5 Non-FIPS mode Services

The cryptographic module supports both FIPS mode and non-FIPS mode of operations. By selecting non-Approved services listed in Section 2.5, the Crypto Officer is placing the module into a non-FIPS mode of operation. The Keys/CSPs used in FIPS mode cannot be used in in non-approved FIPS mode, and vice versa. Prior to using any of the Non-Approved services in Table 6, the Crypto Officer must zeroize all CSPs used in FIPS mode of operation. Neither the User nor the Crypto Officer are allowed to operate any of these services in Table 6 while in FIPS mode of operation.

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

Table 6 – Non-approved algorithms in the Non-FIPS mode services

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.

Likewise, the complete services supported by the module are available at Cisco ASA Series General Operations CLI Configuration Guide, 9.12, Updated: June 25, 2020. https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640.html.

2.6 Unauthenticated Services

There are no unauthenticated services associated with a virtual module.

2.7 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. All other keys are associated with the User role that entered them.

[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.

The module is a software module that contains an approved DRBG that is seeded exclusively from one known entropy source located within the operational environment inside the module's physical boundary but the outside the logical boundary, which is complaint with FIPS 140-2 IG 7.14 #1 (b). The module provides at least 256 bits entropy to instantiate the DRBG.

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
DRBG entropy input	SP800-90A CTR_DRBG (AES-256)	384 bits	This is the entropy for SP 800-90A CTR_DRBG, used to construct seed.	DRAM (plaintext)	Power cycle the device
DRBG seed	SP800-90A CTR_DRBG (AES-256)	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 entropy source.	DRAM (plaintext)	Power cycle the device
DRBG V	SP800-90A CTR _DRBG (AES-256)	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 (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
Diffie-Hellman Shared Secret	DH	2048-4096 bits	The shared secret used in Diffie-Hellman (DH) exchange (as part of SSH, IKE/IPSec, and TLS). 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, IKE/IPSec, and TLS). 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, IKE/IPSec, and TLS). This key is derived per the Diffie-Hellman key agreement. Note that the public key is a cryptographic key, but not considered a CSP.	DRAM (plaintext)	Power cycle the device
skeyid	keying material	160 bits	keying material known only to IKE peers. It was established via key	DRAM (plaintext)	Automatically when IPSec

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
			derivation function defined in SP800-135 KDF and it will be used for deriving other keys in IKE protocol implementation.		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
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 encrypt key	Triple-DES/AES	Triple-DES 192 bits or AES 128/192/256 bits	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv2).	DRAM (plaintext)	Automatically when IPSec session is terminated
IKE session authentication key	HMAC-SHA-256/384/512	256-512 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)	Erase the 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. Note that the public key is a cryptographic key, but not considered a CSP.	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

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
IPSec authentication key	HMAC-SHA-256/384/512	256-512 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
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 derived in compliance with FIPS 186-4 RSA key pair generation method in the module. Note that the public key is a cryptographic key, but not considered a CSP.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
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
SSHv2 integrity key	HMAC-SHA-1	160 bits	Used for SSH 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
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	ECDSA	Curves: P-	Key pair generation, signature	NVRAM	Zeroized by

Name	CSP Type	Size	Description/Generation	Storage	Zeroization
key		256,384,521	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. Note that the public key is a cryptographic key, but not considered a CSP.	(plaintext)	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 generated by calling FIPS approved DRBG.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS RSA public keys	RSA	2048 bits	Identity certificates for the security appliance itself and also used in TLS negotiation. The seed used in generating RSA parameters was generated by calling FIPS approved DRBG. Note that the public key is a cryptographic key, but not considered a CSP.	NVRAM (plaintext)	Zeroized by RSA keypair deletion command
TLS pre-master secret	keying material	48 Bytes	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 HTTPS/TLS keys. This key was derived from TLS pre-master secret during the TLS session establishment	DRAM (plaintext)	Automatically when TLS session is terminated
TLS encryption keys	Triple-DES/AES/AES-GCM	Triple-DES 192 bits or AES 128/192/256 bits	Used in HTTPS/TLS connections to protect the session traffic. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
TLS integrity key	HMAC-SHA 256/384	256-384 bits	Used for TLS integrity to assure the traffic integrity. This key was derived in the module.	DRAM (plaintext)	Automatically when TLS session is terminated
Integrity test key	RSA-2048 Public key	2048 bits	A hard-coded key used for software power-up integrity verification.	Hard coded for software integrity testing	Zeroized by erasing the software image

Table 7 Cryptographic Keys and CSPs

2.8 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 certificates implemented by Adaptive Security Appliance Virtual (ASAv):

Algorithm	Certificate
AES (128/192/256 bits CBC, GCM)	5008
Triple-DES (CBC, 3-key)	2584
SHS (SHA-1/256/384/512)	4074
HMAC (SHA-1/256/384/512)	3329
RSA (PKCS1_V1_5; KeyGen, SigGen, SigVer; 2048 bits)	2703
ECDSA (KeyGen, SigGen, SigVer; P-256, P-384, P-521)	1277
DRBG (CTR_DRBG)	1828
CVL Component (IKEv2, TLSv1.2, SSHv2)	1561
CKG (vendor affirmed)	

Table 8 Approved Cryptographic Algorithms

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in this table.
- The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS and RFC 7296 for IPSec/IKEv2. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. The 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 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 scenario 1 of section 5 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 Cert. #1561, key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 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:

- DES
- Diffie-Hellman (key agreement; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- HMAC MD5
- MD5
- RC4
- RSA (key wrapping; key establishment methodology less than 112 bits of encryption strength; non-compliant)
- HMAC-SHA-1 is not allowed with key size under 112-bits

2.9 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

- POSTs – Cisco Security Crypto Virtual
    - 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) Power on Self-Test
    - HMAC-SHA-1/256/384/512 KATs
    - RSA KATs (separate KAT for signing; separate KAT for verification)

    - SHA-1/256/384/512 KATs
    - Software Integrity Test (RSA 2048 with SHA-512)
    - Triple-DES CBC Encrypt/Decrypt KATs

- Conditional tests - Cisco Security Crypto Virtual
    - RSA pairwise consistency test
    - ECDSA pairwise consistency test
    - Conditional Bypass test
    - CRNGT for SP800-90A DRBG
    - CRNGT for NDRNG

The module performs all power-on self-tests automatically at boot 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 virtual LAN's interfaces; this prevents the module from passing any data during a power-on self-test failure. In the unlikely event that a power-on or conditional self-test fails, an error message is displayed on the console followed by a 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. Follow the installation instructions found in the link above and the 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 ASAv module was validated with adaptive security appliance software version 9.12. This is the only allowable software image for FIPS-approved mode of operation.

The Crypto Officer must configure and enforce the following initialization steps:

Step 1: Power on.
Step 2: Change the factory default password. The new password should be a minimum of 8 alpha-numeric characters, see section 2.4 above for details.
Step 3: Disable the console output of system crash information, using the following command:

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

Step 4: Install Triple-DES/AES licenses to require the module to use Triple-DES and AES (for data traffic and SSH).

Step 5: Enable "FIPS Mode" to allow the module 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 6: Disable password recovery.
(config)#**no service password-recovery**

Step 7: Set the configuration register to bypass ROMMON prompt at boot.
(config)# **config-register 0x10011**

Step 8: 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 9: Enable AAA **authentication** for the console.
(config)#**aaa authentication serial console LOCAL**
(config)#**username <name> password <password>**

Step 10: Enable AAA **authentication** for SSH.
(config)#**aaa authentication ssh console LOCAL**

Step 11: Enable AAA **authentication** for Enable mode.
(config)#**aaa authentication enable console LOCAL**

Step 12: 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 13: Reboot the module.

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 module 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 module to use SSHv2. Note that all operators must still authenticate after remote access is granted.

```
(config)# ssh version 2
```

Step 5: Configure the module such that any remote connections via Telnet are secured through IPSec.

Step 6: Configure the module such that only FIPS-approved algorithms are used for IPSec tunnels.

Step 7: Configure the module such that error messages can only be viewed by a 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.

Step 11: Ensure that the 2048 bits RSA keys are used.

Step 12: Ensure that DH Group 1 (768-bits) and DH Group 2 (1024-bits) keys are not used.

3.3 Identifying Module Operation in an Approved Mode

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

1. Verify that the length of User and Crypto Officer passwords and all shared secrets are at least eight (8) characters long, include at least one letter, and include at least one number character, as specified in the “Secure Operation” section of this document.
2. Issue the following commands: 'show crypto IPSec sa' and 'show crypto isakmp policy' to verify that only FIPS approved algorithms are used.