Cisco Catalyst 9800 (40/80/L) Wireless Controllers running IOS-XE 16.12

Firmware Version: IOS-XE 16.12

FIPS 140-2 Non-Proprietary Security Policy
Level 1 Validation

Version 1.0

March 5, 2021

© Copyright 2021 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table of Contents

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

1 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the **Cisco Catalyst 9800 (40/80/L) Wireless Controllers running IOS-XE 16.12**; referred to in this document as controllers or the module. This security policy describes how the modules meet the security requirements of FIPS 140-2 Level 1 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

1.2 References

This document deals only with operations and capabilities of the Cisco Catalyst 9800 (40/80/L) Wireless Controllers, in the technical terms of a FIPS 140-2 cryptographic module security policy.

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

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

1.3 FIPS 140-2 Submission Package

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 Catalyst 9800 (40/80/L) Wireless Controllers and explains the secure configuration and operation of the module. This introduction section is followed by Section 2 through Section 10, which details the general features and functionality of the appliances. Section 11 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.

1.4 Terminology

In this document, the Cisco Catalyst 9800 (40/80/L) Wireless Controllers running IOS-XE 16.12 is referred to as controller or the module.

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2 Module Description

2.1 Cisco Systems Catalyst 9800 Wireless Controller

Cisco Catalyst 9800 Series Wireless Controllers (9800-80, 9800-40, and 9800-L) combine the best of RF excellence with IOS XE benefits. These are the industry's most reliable and highly secure controllers, ready to deploy anywhere--including the cloud of your choice. They provide operational ease and save time and money.

The Cisco Catalyst 9800-80 is our leading modular wireless controller, which supports up to 6000 access points and 64,000 clients and throughput up to 80 Gpbs, while the Cisco Catalyst 9800-40 is ideal for mid-sized organizations and campus deployments as it supports up to 2000 access points and 32,000 clients with throughput up to 40 Gbps. The 9800-L is designed for smaller network deployments while supporting 250 access points, 5000 clients, and a max throughput of 5Gbps. All devices fully inter-operable with AireOS controllers and 802.11ac Wave-1 and Wave-2 Access Points.

2.2 Models

- Catalyst 9800 Wireless Controller (HW: 9800-40)
- Catalyst 9800 Wireless Controller (HW: 9800-80)
- Catalyst 9800 Wireless Controller (HW: 9800-L)

2.3 FIPS and non-FIPS modes of operation

The Cisco Catalyst 9800 (40/80/L) Wireless Controllers support a FIPS and non-FIPS mode of operation. The non-FIPS mode of operation is not a recommended operational mode but because the module allows for non-approved algorithms and non-approved key sizes, a non-approved mode of operation exists. The following services are available in both a FIPS and a non-FIPS mode of operation:

- SSH
- TLS
- DTLS
- IPSec
- SNMPv3

When the services are used in non-FIPS mode they are considered to be non-compliant.

If the device is in the non-FIPS mode of operation, the Cryptographic Officer must follow the instructions in section 11.1 of this security policy to transition the module into a FIPS approved mode of operation. The FIPS Approved mode supports the approved and allowed algorithms, functions and protocols identified in Section 7 of this document. The FIPS Approved mode of operation is entered when the module is configured for FIPS mode (detailed in Section 11) and successfully passes all the power on self-tests (POST).

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

2.4 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	1
11	Mitigation of Other Attacks	N/A
	Overall module validation level	**1**

Table 1: Module Validation Level

3 Cryptographic Module Boundary

Each module is a multi-chip standalone security appliance, and the cryptographic boundary is defined as encompassing the "top," "front," "back," "left," "right," and "bottom" surfaces of the case. Included in this physical boundary is the ACT2Lite module (certificate #3637). ACT2Lite module is solely used as NDRNG (entropy source) and is neither used for directly generating any symmetric keys or seed for asymmetric keys nor used for any services implemented by the module.

4 Cryptographic Module Ports and 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 tables:

Module Physical Interface	FIPS 140-2 Logical Interface
• 5 ports 1/10 Gbps Ethernet (SFP+ or SFP) • 2 ports 10/100/1000 Ethernet (RJ-45) • Console ports (RJ-45 and mini USB) • 2 USB 3.0	Data Input Interface

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Module Physical Interface	FIPS 140-2 Logical Interface
• 5 ports 1/10 Gbps Ethernet (SFP+ or SFP) • 2 ports 10/100/1000 Ethernet (RJ-45) • Console ports (RJ-45 and mini USB) • 2 USB 3.0	Data Output Interface
• 5 ports 1/10 Gbps Ethernet (SFP+ or SFP) • 2 ports 10/100/1000 Ethernet (RJ-45) • Console ports (RJ-45 and mini USB) • 2 USB 3.0 • Power Switch	Control Input Interface
• 5 ports 1/10 Gbps Ethernet (SFP+ or SFP) • 2 ports 10/100/1000 Ethernet (RJ-45) • LEDs • Console ports (RJ-45 and mini USB)	Status Output Interface
• Power Connector	Power Interface

Table 2: Cisco Catalyst 9800-40 Physical Interface/Logical Interface Mapping

Figure 1: Front Cisco Catalyst 9800-40

Figure 2: Rear Cisco Catalyst 9800-40

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Module Physical Interface	FIPS 140-2 Logical Interface
• 9 ports 1/10 Gbps Ethernet (SFP+ or SFP) • 2 ports 10/100/1000 Ethernet (RJ-45) • 2 USB 3.0 • Console ports (RJ-45 or mini-B USB)	Data Input Interface
• 9 1/10 Gbps Ethernet (SFP+ or SFP) • 2 ports 10/100/1000 Ethernet (RJ-45) • 2 USB 3.0 • Console ports (RJ-45 or mini-B USB)	Data Output Interface
• 9 1/10 Gbps Ethernet (SFP+ or SFP) • 2 ports 10/100/1000 Ethernet (RJ-45) • Console ports (RJ-45 or mini-B USB) • 2 USB 3.0 • Power Switch	Control Input Interface
• 9 1/10 Gbps Ethernet (SFP+ or SFP) • 2 ports 10/100/1000 Ethernet (RJ-45) • LEDs • Console ports (RJ-45 or mini-B USB)	Status Output Interface
• Power Connector	Power Interface

Table 3: Cisco Catalyst 9800-80 Physical Interface/Logical Interface Mapping

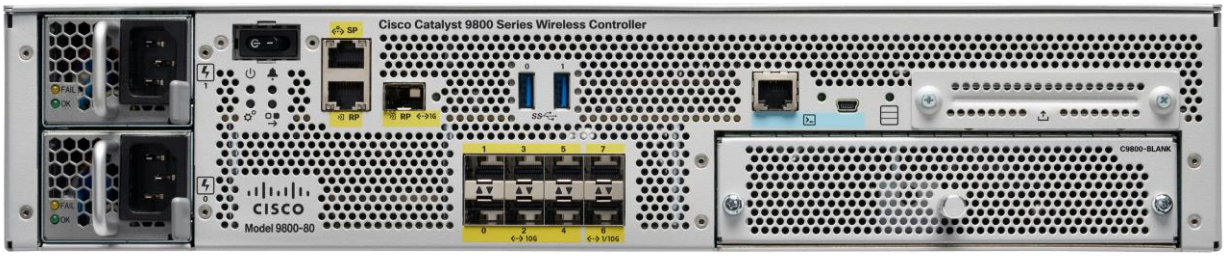

Figure 3: **Front Cisco Catalyst 9800-80**

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Figure 4: Rear Cisco Catalyst 9800-80

Module Physical Interface	FIPS 140-2 Logical Interface
• 2 ports 10 Gbps Ethernet (SFP+, RJ-45) • 4 ports 1000/2500 Gbps Ethernet (RJ-45) • 1 USB 3.0 • Console ports (RJ-45 and mini USB) • Service Port • Redundancy Port	Data Input Interface
• 2 ports 10 Gbps Ethernet (SFP+, RJ-45) • 4 ports 1000/2500 Gbps Ethernet (RJ-45) • 1 USB 3.0 • Console ports (RJ-45 and mini USB) • Service Port • Redundancy Port	Data Output Interface
• 5 ports 1/10 Gbps Ethernet (SFP+ or SFP) • 4 ports 1000/2500 Gbps Ethernet (RJ-45) • Console ports (RJ-45 and mini USB) • 1 USB 3.0 • Power Switch • Service Port	Control Input Interface
• 5 ports 1/10 Gbps Ethernet (SFP+ or SFP) • 4 ports 1000/2500 Gbps Ethernet (RJ-45) • LEDs • Console ports (RJ-45 and mini USB) • Service Port	Status Output Interface
• Power Connector	Power Interface

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Table 4: Cisco Catalyst 9800-L Physical Interface/Logical Interface Mapping

Figure 5: Front Cisco Catalyst 9800-L

Figure 6: Back Cisco Catalyst 9800-L

5 Roles, Services and Authentication

The module supports identity-based authentication. There are two roles in the module that the operators may assume in the FIPS mode:

- User Role -This role performs general security services including cryptographic operations and other approved security functions. The product documentation refers to this role as a management user with level 1 privilege.
- Crypto Officer (CO) Role -This role performs the cryptographic initialization and management operations. In particular, it performs the loading of optional certificates and key-pairs and the zeroization of the module. The product documentation refers to this role as a management user with level 15 privilege.

The Module does not support a Maintenance Role.

5.1 User Services

The services available to the User role consist of the following:

Services & Access	Description	Keys & CSPs
System Status	• The LEDs show the network activity (“Green” if the interfaces are up and running, “Flashing yellow” if the interfaces are coming up and no LED	N/A

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

	activity when there is no connection to the network interfaces), overall operational status ("Red" indicates module failure and "Green" indicates that module is operational).	
Random Number Generation	• Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG v, DRBG Key – r, w, d
Key Exchange	• Key exchange over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – w, d
Module Read-only Configuration	• Viewing of configuration settings	N/A

Table 5: User Services (r = read, w = write, d = delete)

5.2 Crypto Officer Services

The Crypto Officer services consist of the following:

Services & Access	Description	Keys & CSPs
Self Test and Initialization	• Cryptographic algorithm tests, firmware integrity tests, module initialization.	N/A (No keys are accessible)
System Status	• The LEDs show the network activity ("Green" if the interfaces are up and running, "Flashing yellow" if the interfaces are coming up and no LED activity when there is no connection to the network interfaces), overall operational status ("Red" indicates module failure and "Green" indicates that module is operational) and the command line "status commands" output system status ("show fips" command would result in indicating whether the module is in FIPS mode or not).	N/A (No keys are accessible)
Random Number Generation	• Key generation and seeds for asymmetric key generation	DRBG entropy input, DRBG seed, DRBG v, DRBG Key – r, w, d
Key Exchange	• Key exchange over Diffie-Hellman and EC Diffie-Hellman	Diffie-Hellman public key, Diffie-Hellman private key, Diffie-Hellman shared secret, EC Diffie-Hellman Public Key, EC Diffie-Hellman Private Key, EC Diffie-Hellman shared secret – w, d

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

IPSec	• Secure communications between module and a client.	skeyid, skeyid_d, IKE session encryption key, IKE session authentication key, IKE RSA private key, IKE RSA public key, IPSec session encryption key, IPSec session authentication key, IPSec authentication key, IPSec encryption key, ISAKMP preshared – r, w,d
Zeroization	• Zeroize CSPs and cryptographic keys by cycling power to zeroize all cryptographic keys stored in DRAM. The CSPs stored in Flash can be zeroized by overwriting with a new value.	All Keys and CSPs will be destroyed – d
Module Configuration	• Selection of non-cryptographic configuration settings	N/A
Power Cycle	• Reboot/reloading the module	All ephemeral Keys and CSPs will be destroyed - d
SNMPv3	• Non-security related monitoring by the CO using SNMPv3	snmpEngineID, SNMPv3 Password, SNMP session key – w, d
SSH	• Establishment and subsequent data transfer of a SSH session for use between the module and the CO.	SSH encryption key, SSH integrity key, SSH RSA private key – w, d
HTTPS/TLS	• Establishment and subsequent data transfer of a TLS session for use between the module and the CO. • Protection of syslog messages	HTTPS/TLS Pre-Master secret, HTTPS/TLS Master secret, HTTPS/TLS Encryption Key, HTTPS/TLS Integrity Key, HTTPS/TLS RSA/ECDSA private key – w, d
DTLS Data Encrypt	• Enabling optional DTLS data path encryption for Office Extended AP's	DTLS Pre-Master Secret, DTLS Master Secret, DTLS Encryption/Decryption Key (CAPWAP session keys), DTLS Integrity Keys, DTLS RSA/ECDSA private key – w, d

Table 6: Crypto Officer Services (r = read, w = write, d = delete)

User and CO Authentication

The Crypto Officer role is assumed by an authorized CO connecting to the module via CLI, SSH and GUI. The OS prompts the CO for their username and password, if the password is validated against the CO's password in memory, the operator is allowed entry to execute CO services. Each username is unique and configurable by Crypto-officer. The password feedback mechanism does not provide information that could be used to determine the authentication data. The User role monitors the module via CLI, SSH and GUI.

The Crypto Officer and User passwords and all shared secrets must each be at least eight (8) characters long, including at least one (1) special character and at least one (1) number, in length (enforced procedurally by policy) 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) alphabet are used without repetition for an eight (8) character long, the probability of randomly guessing the correct sequence is one (1) in 164,290,949,222,400 (this calculation is

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

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. Since it is claimed to be for 8 digits with no repetition, then the calculation should be 32x10x92x91x90x89x88x87). Therefore, for each attempt to use the authentication mechanism, the associated probability of a successful random attempt is approximately 1 in 164,290,949,222,400, which is less than the 1 in 1,000,000 required by FIPS 140-2.

The maximum number of possible attempts per minute is 5 for Password Authentication via console. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is 5/164,290,949,222,400 which is less than the 1 in 100,000 required by FIPS 140-2.

The module only supports sixteen (16) concurrent SSH sessions and maximum number of possible attempts per minute is 8 for each SSH session. Therefore, the probability of a success with multiple consecutive attempts in a one-minute period is (8*16)/ 164,290,949,222,400 which is less than the 1 in 100,000 required by FIPS 140-2.

SSH Public-key Authentication: The CO and User role also supports public key authentication for remotely accessing the module via SSH. RSA has modulus size of 2048 bit, thus providing 112 bits of strength. 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. The fastest network connection supported by the modules over management interfaces are 10 Gb/s. Hence, at most $10 \times 10^9 \times 60s = 6 \times 10^{11} = 600,000,000,000$ bits of data can be transmitted in one minute. Therefore, the probability that a random attempt will succeed, or a false acceptance will occur in one minute is:

$$1:(2^{112} \text{ possible keys}/(6 \times 10^{11} \text{ bits per minute})/112 \text{ bits per key}))$$
$$1:(2^{112} \text{ possible keys}/5,357,142,857 \text{ keys per minute})$$
$$1:9.7\times10^{23}$$

Therefore, the associated probability of a successful random attempt for a minute is approximately 1 in 9.7×10^{23}, which is less than the 1 in 100,000 required by FIPS 140-2.

6 Unauthenticated Services

The following are the list of services for Unauthenticated Operator:

System Status: An unauthenticated operator may observe the System Status by viewing the LEDs on the module, which show network activity and overall operational status. Unauthenticated operator can also view boot up/power on self test logs on console port which does not disclose any security relevant information.
Power Cycle: This operator can power cycle the module. A solid green LED indicates normal operation and the successful completion of self-tests.

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

The module does not support a bypass capability.

7 Cryptographic Algorithms

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

7.1 Approved Cryptographic Algorithms

The module supports many different cryptographic algorithms. However, only FIPS approved algorithms may be used while in the FIPS mode of operation. The following table identifies the approved algorithms included in the module for use in the FIPS mode of operation. The modules support the following FIPS 140-2 approved algorithm implementations:

1) CiscoSSL FOM 7.0a (9800-40, 9800-80 and 9800-L),
2) IOS Common Cryptographic Module Rel 5 (9800-40, 9800-80 and 9800-L), and
3) OCTEON II CN6700/CN6800 Series Die (Hardware version: CN6880) (9800-40 and 9800-80).

Algorithm	Supported Mode	Cert. #
CiscoSSL FOM 7.0a		
AES	ECB (128 , 192 , 256); CBC (128 , 192 , 256); CFB128 (128 , 192 , 256), CTR (128 , 192 , 256), GCM (128 , 192 , 256)	**C1279**
SHS	SHA-1, -256, -384, and -512 (Byte Oriented)	
HMAC SHS	SHA-1, -256, -384, and -512	
DRBG	CTR (using AES-256)	
ECDSA	Key Generation (P-256, P-384 and P-521) Key Verification (P-256, P-384 and P-521) Signature Generation (P-256 with SHA2-256, SHA2-384, SHA2-512, P-384 with SHA2-384, SHA2-512 and P-521 with SHA2-521) Signature Verification (P-256 with SHA2-256, SHA2-384, SHA2-512, P-384 with SHA2-384, SHA2-512 and P-521 with SHA2-521)	

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm	Supported Mode	Cert. #
RSA	FIPS186-4 RSA Key Generation**:** MOD 2048 with SHA2-256, MOD 3072 with SHA2-256 PKCS#1 v.1.5, 2048-3072 bit key SigGen, MOD: 2048, 3072 SigVer, MOD 1024 – 3072. 1024-bit keys allowed for signature verification only The following methods are non-approved: • Key Generation: MOD: 1024-bit keys and 1536-bit keys	
Triple-DES	TCBC (KO 1)	
CVL (SP800-135)	TLS KDF, IKEv2 KDF, SSH KDF, SNMP KDF Note: The TLS, IKEv2, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.	
CVL (SP800-56A)	FFC: FB: SHA2-256 FC: SHA2-256 ECC: EC: SHA2-256, P-256 ED: SHA2-384 , P-384 EE: SHA2-512, P-521	
CKG (SP800-133)	Vendor Affirmed	
IOS Common Cryptographic Module Rel 5		
AES	ECB (128 , 192 , 256); CBC (128 , 192 , 256); CFB128 (128 , 192 , 256), CTR (128 , 192 , 256), GCM (128 , 192 , 256), CMAC (128, 256).	C972
SP800-135 (CVL)	TLS KDF, IKEv2 KDF, SSH KDF, SNMP KDF Note: The TLS, IKEv2, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP.	

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Algorithm	Supported Mode	Cert. #
DRBG	CTR (using AES-256)	
ECDSA	Key Generation (P-256, P-384) Key Verification (P-256, P-384) Signature Generation (P-256, P-384 both with SHA2-256) Signature Verification (P-256, P-384, both with SHA2-256)	
HMAC	SHA-1, SHA2-256, SHA2-384, SHA2-512	
RSA	FIPS186-4 RSA Key Generation (2048 w/SHA2-256, 3072 w/SHA2-256) PKCS 1.5: 1024-3072 bit key RSA Signature Generation 2048 w/ SHA1, SHA2-256/384/512, 3072 w/ SHA1, SHA2-256/384/512) RSA Signature Verification (1024 w/SHA1, SHA2-256/384/512, 2048 w/ SHA1, SHA2-256/384/512, 3072 w/ SHA1, SHA2-256/384/512) 1024-bit keys allowed for signature verification only	
SHS	SHA-1, SHA2-256, SHA2-384, SHA2-512	
Triple-DES	TCBC (KO 1)	
CVL (SP800-56A	FFC: FC: SHA2-256 ECC: EC: SHA2-256, P-256 ED: SHA2-384, P-384	
CKG (SP800-133)	Vendor Affirmed	
CN6880		
AES	ECB (128/192/256), CBC (128/192/256), GCM (128/192/256)	2346
SHS	SHA-1, -224, -256, -384, and -512	2023

Table 7: Approved Cryptographic Algorithms

- KTS (AES Cert. #C972; key establishment methodology provides between 128 and 256 bits of encryption strength)
- KTS (AES Cert. #C972 and HMAC Cert. #C972; key establishment methodology provides between 128 and 256 bits of encryption strength)

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- KTS (Triple-DES Cert. #C972 and HMAC Cert. #C972; key establishment methodology provides 112 bits of encryption strength)
- KTS (AES Cert. #C1279 and HMAC Cert. #C1279; key establishment methodology provides between 128 and 256 bits of encryption strength)

Note 1**:** In accordance with CMVP IG A.13, when operating in a FIPS approved mode of operation, the same Triple-DES key shall not be used to encrypt more than 2^{20} 64-bit data blocks. The SSH protocols governs the generation of the respective Triple-DES keys. Please refer to IETF RFC 4253 (SSH) for details relevant to the generation of the individual Triple-DES encryption keys. IKEv2 generates the SKEYSEED according to RFC 7296, from which all keys are derived to include Triple-DES keys. The user is responsible for ensuring that the module limits the number of encrypted blocks with the same key to no more than 2^{20} when utilized as part of the recognized IETF protocols (SSH and IKEv2).
Note 2: The module's AES-GCM implementations conforms to IG A.5 Provision #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. Method ii) was used by the tester to demonstrate the module's compliance with the TLS provision for the AES GCM IV generation in IG A.5. The counter portion of the IV is set by the module within its cryptographic boundary. The restoration of the IV is in accordance with scenario 3 in IG A.5 in that a new AES GCM key is established. 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 which is in accordance with scenario 3 in IG A.5.
Note 3: The module's AES-GCM implementations conforms to IG A.5 Provision #1 following RFC 7296 for IPSec/IKEv2. The AES GCM IV is generated according to RFC5282 and RFC4106 and is used only in the context of the IPSec/IKEv2 protocol as allowed in IG A.5. The module uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived. Method ii) was used by the tester to demonstrate the module's compliance with the IPSec provision for the AES GCM IV generation in IG A.5. The restoration of the IV is in accordance with scenario 3 in IG A.5 in that a new AES GCM key is established. 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 which is in accordance with scenario 3 in IG A.5.
Note 4: CVL Certs. #C1279 and #C972 support the KDF (key derivation function) used in each of IKEv2, TLS, SSH and SNMPv3 protocols. IKEv2, TLS, SSH and SNMPv3 protocols have not been reviewed or tested by the CAVP and CMVP. Please refer IG D.11, bullet 2 for more information.
Note 5: CKG (vendor affirmed) Cryptographic Key Generation; SP 800-133. 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.

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

There are algorithms, modes, and keys that have been CAVs tested but not implemented by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are implemented by the module.
Note 6: There are algorithms, modes, and keys that have been CAVP tested but not implemented by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are implemented by the module.

7.2 Non-Approved Cryptographic Algorithms but Allowed in FIPS mode

The module supports the following non-approved, but allowed cryptographic algorithms:

- Diffie-Hellman (CVL Cert. #C972, key agreement; key establishment methodology provides 112 bits of encryption strength. Diffie-Hellman with less than 112-bit of security strength is non-compliant and may not be used)
- Diffie-Hellman (CVL Cert, #C1279, key agreement; key establishment methodology provides 112 bits of encryption strength. Diffie-Hellman with less than 112-bit of security strength is non-compliant and may not be used)
- EC Diffie-Hellman (CVL Cert. #C972 with CVL Cert. #C972, key agreement; key establishment methodology provides 128 or 192 bits of encryption strength. EC Diffie-Hellman with less than 128-bit of security strength is non-compliant and may not be used)
- EC Diffie-Hellman (CVL Cert. #C1279 with CVL Cert. #C1279, key agreement; key establishment methodology provides 128 or 192 bits of encryption strength. EC Diffie-Hellman with less than 128-bit of security strength is non-compliant and may not be used)
- RSA[1] (key wrapping; key establishment methodology provides 112 bits of encryption strength. RSA with less than 112-bit of security strength is non-compliant and may not be used).
- NDRNG

7.3 Non-Approved Cryptographic Algorithms

The cryptographic module implements the following non-approved algorithms that are not permitted for use in FIPS 140-2 mode of operations:

Service[2]	Non-Approved Algorithm
SSH (non-compliant)	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, Asymmetric: 512-bit RSA,1024-bit RSA, 1024-bit Diffie-Hellman

[1] As per IG D.9, the RSA Key Wrapping uses RSA modulus of 2048 bit long that uses PKCS#1-v1.5 scheme and is not complaint with any revision of SP800-56B.
[2] These non-approved algorithms are not to be used in FIPS mode.

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

TLS (non-compliant)	MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 512-bit RSA, 1024-bit RSA, 1024-bit Diffie-Hellman
IPsec (non-compliant)	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 512-bit RSA, 1024-bit RSA, 1024-bit Diffie-Hellman
SNMP (non-compliant)	Hashing: MD5, MACing: HMAC MD5 Symmetric: DES, RC4 Asymmetric: 512-bit RSA, 1024-bit RSA, 1024-bit Diffie-Hellman
Initialization	SHA-1 (non-compliant)

Table 8: Non-Approved Cryptographic Algorithms

7.4 Non-Approved Services

- SSHv1 with RC4 and HMAC-MD5,
- SNMP v1 and v2,
- IPSec/IKEv2 with Diffie-Hellman 768-bit/1024-bit modulus, EC Diffie-Hellman 163/192 curves,
- IKEv1,
- Telnet.

8 Cryptographic Key Management

Cryptographic keys are stored in plaintext form, in flash for long-term storage and in DRAM for active keys. The module securely 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 exchanged and entered electronically or via Internet Key Exchange (IKE).
Key generation and seeds for asymmetric key generation is performed as per SP 800-133 Scenario 1. The DRBG is seeded with a minimum of 256 bits of entropy strength prior to key generation.

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
DRBG entropy input	SP 800-90A CTR_DRBG	HW-based entropy source output used to construct seed.	256-bits	DRAM	Power cycle
DRBG seed	SP 800-90A CTR_DRBG	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from a hardware-based entropy source.	384 bits	DRAM	Power cycle
DRBG V	SP 800-90A CTR_DRBG	Internal V value used as part of SP 800-90A CTR_DRBG	128 bits	DRAM	Power cycle
DRBG Key	SP 800-90A CTR_DRBG	This is the 256-bit DRBG key used for SP 800-90A CTR_DRBG..	256 bits	DRAM	Power cycle
cscoCCDefaultMfgCaCert	rsa-pkcs1-sha2	Verification certificate, used with CAPWAP to validate the certificate that authenticates the access point presents when joining.	2048	Flash	N/A
Diffie-Hellman public key	Diffie-Hellman (Group 14)	The public key used in Diffie-Hellman (DH) Exchange.	2048 bits	DRAM	Power cycle
Diffie-Hellman private key	Diffie-Hellman (Group 14)	The private key used in Diffie-Hellman (DH) Exchange.	224 bits	DRAM	Power cycle
Diffie-Hellman shared secret	Diffie-Hellman (Group 14)	The shared key used in Diffie-Hellman (DH) Exchange. Created per the Diffie-Hellman Protocol.	2048 bits	DRAM	Power cycle
EC Diffie-Hellman public key	Diffie-Hellman (Groups 19 and 20)	P-256, P-384 public key used in EC Diffie-Hellman exchange. This key is derived per the Diffie-Hellman key agreement.	P-256 and P-384	DRAM (plaintext)	Power cycle
EC Diffie-Hellman private key	Diffie-Hellman (Groups 19 and 20)	P-256 and P-384 private key used in EC Diffie-Hellman exchange. Generated by calling the SP 800-90A CTR-DRBG.	P-256 and P-384	DRAM (plaintext)	Power cycle

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
EC Diffie-Hellman shared secret	Diffie-Hellman (Groups 19 and 20)	P-256 and P-384 shared secret derived in EC Diffie-Hellman exchange.	P-256 and P-384	DRAM (plaintext)	Power cycle
Operator password	Shared Secret, at least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer.	Variable (8+ characters)	Flash (plaintext)	Overwrite with new password
Enable Password	Shared Secret, at least eight characters	The password of the operator. This CSP is entered by the Cryptographic Officer.	Variable (8+ characters)	Flash (plaintext)	Overwrite with new password
Enable secret	Secret, at least eight characters	The obfuscated password of the CO role. However, the algorithm used to obfuscate this password is not FIPS approved. Therefore, this password is considered plaintext for FIPS purposes. This password is zeroized by overwriting it with a new password. The Cryptographic Operator optionally configures the module to obfuscate the Enable password. This CSP is entered by the Cryptographic Officer.	Variable (8+ characters)	Flash (plaintext)	Overwrite with new secret
SKEYSEED	HMAC	Shared secret known only to IKE peers. Used to derive IKE session keys. Derived by using key derivation function defined in SP800-135 KDF (IKEv2).	160-384 bits	DRAM (plaintext)	Power cycle
Skeyid	HMAC	It was derived by using 'IKE pre-shared' and other non-secret values through the key derivation function defined in SP800-135 KDF (IKEv2).	160-384 bits	DRAM (plaintext)	Power cycle
skeyid_d	HMAC	It was derived by using skeyid, Diffie-Hellman shared secret and other non-secret values through key derivation function defined in SP800-135 KDF (IKEv2).	160-384 bits	DRAM (plaintext)	Power cycle

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
IKE session encryption key	AES-CBC, AES-GCM, TDES-CBC.	The IKE session encrypt key is derived by using key derivation functions defined in SP800-135 KDF (IKEv2). Used for IKE payload protection.	AES-CBC (128-bit, 192-bit, 256-bit) AES-GCM (128-bit, 256-bit)	DRAM (plaintext)	Power cycle
IKE session authentication key	HMAC	The IKE session) authentication key is derived by using key derivation functions defined in SP800-135 KDF (IKEv2). Used for payload integrity verification.	160-512 bits	DRAM (plaintext)	Power cycle
IKE public key	RSA	This key generated by calling the SP 800-90A CTR-DRBG.	2048 bits	Flash (plaintext)	Overwrite with new key or use “crypto key zeroize rsa”
IKE private key	RSA	This key generated by calling the SP 800-90A CTR-DRBG.	2048 bits	Flash (plaintext)	Overwrite with new key or use “crypto key zeroize rsa”
IKE pre-shared	Shared secret	This shared secret was manually entered by CO for IKE pre-shared key-based authentication mechanism.	8 chars	Flash (plaintext)	Overwrite with new secret or use “no crypto isakmp key” command zeroizes it.
IPSec authentication key	HMAC	The IPsec authentication key is derived using the KDF defined in SP800-135 KDF (IKEv2). Used to authenticate the IPSec peer.	160 – 512 bits	DRAM (plaintext)	Automatically when IPsec session terminated or during Power Cycle.
IPSec encryption key	AES-CBC, AES-GCM, TDES-CBC. .	The IPsec encryption key is derived using key derivation function defined in SP800-135 KDF (IKEv2). Used to Secure IPSec traffic.	AES-CBC (128-bit, 192-bit, 256-bit) AES-GCM (128-bit, 256-bit)	DRAM (plaintext)	Automatically when IPsec session terminated or during power cycle.
DTLS Pre-Master Secret	Shared Secret	Generated by approved DRBG for generating the DTLS Master Secret.	48 bytes	DRAM (plaintext)	Power cycle

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
DTLS Master Secret	Shared Secret	Derived from DTLS Pre-Master Secret. Used to create the DTLS encryption and integrity keys.	48 bytes	DRAM (plaintext)	Power cycle
DTLS Encryption/Decryption Key (CAPWAP session keys)	AES-CBC, AES-GCM	Session Keys used to e/d CAPWAP control messages.	128-256 bits	DRAM (plaintext)	Power cycle
DTLS Integrity Keys	HMAC-	Session keys used for integrity checks on CAPWAP control messages.	160-384 bits	DRAM (plaintext)	Power cycle
DTLS public/private key	RSA and ECDSA	PKCS#1 v.1.5, P-256 and P-384 generated by calling the SP 800-90A CTR-DRBG.	ECDSA (P-256 and P-384) RSA (MOD 2048)	Flash (plaintext)	Overwrite with new key or use “crypto key zeroize rsa” or “crypto key zeroize ec “ to zeroize rsa and ecdsa keys
snmpEngineID	Shared secret	Unique string to identify the SNMP engine.	32-bits	Flash (plaintext)	Overwrite with new engine ID
SNMPv3 Password	Shared Secret	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication.	32 bytes	Flash (plaintext)	Overwrite with new password
SNMPv3 session key	AES-CFB	Encrypts SNMPv3 traffic.	128-bit	DRAM (plaintext)	Power cycle
HTTPS/TLS Pre-Master secret	Shared secret	Internal generation by FIPS-approved DRBG. Used to establish HTTPS/TLS Master Secret .	48 bytes	DRAM (plaintext)	Power cycle
HTTPS/TLS Master secret	Shared secret	Derived from the HTTPS/TLS Pre-Master Secret. Used for computing the Encryption and Integrity Keys.	48 bytes	DRAM (plaintext)	Power cycle
HTTPS/TLS Encryption Key	AES-CBC, AES-GCM.	AES key used to encrypt TLS data.	128 and 256 bits	DRAM (plaintext)	Power cycle
HTTPS/TLS Integrity Key	HMAC	HMAC key used for HTTPS integrity protection.	160-384 bits	DRAM (plaintext)	Power cycle

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Key/CSP Name	Algorithm	Description	Key Size	Storage	zeroization
HTTPS/TLS public/private key	ECDSA, RSA	PKCS#1 v.1.5, P-256 and P-384 generated by calling the SP 800-90A CTR-DRBG.	ECDSA (P-256 and P-384) RSA (MOD 2048)	Flash (plaintext)	HTTPS/TLS Server RSA private/public key is zeroized by either deletion (via # crypto key zeroize rsa or crypto key zeroize ec) or by overwriting with new value of the key.
Infrastructure MFP MIC Key	AES-CMAC, AES-GMAC	This key is generated in the module by calling FIPS approved DRBG and then is transported to the Access Point (AP) protected by DTLS Encryption/Decryption Key. The Access Point (AP) uses this key with sign management frames when infrastructure MFP is enabled.	128 and 256 bits	DRAM (plaintext)	Power cycle
SSH Encryption Key	AES-CBC, TDES-CBC, AES-CTR	Symmetric AES key for encrypting SSH.	128-256 bits AES and TDES-CBC	DRAM (plaintext)	Power cycle
SSH Integrity Key	HMAC	Used for SSH integrity protection.	160-512 bits	DRAM (plaintext)	Power cycle
SSH Public/Private Key Pair	RSA	PKCS#1 v.1.5 generated by calling the SP 800-90A CTR-DRBG.	MOD 2048	Flash (plaintext)	SSH private/public key is zeroized by either deletion (via # crypto key zeroize rsa) or by overwriting with a new value of the key

Table 9: Cryptographic Keys and CSPs

Note 1 to table: The KDF infrastructure used in DTLS v1.2 is identical to the ones used in TLS v1.2, which was certified by CVL Cert. #C1279.

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Note 2 to table: No parts of the SSH, TLS and IPSec protocols, other than the KDFs, have been tested by the CAVP and CMVP.

9 -Self-Tests

The modules include an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

Power On Self-Tests Performed:

- Firmware Integrity Test 2048-bit/SHA-512 RSA

CiscoSSL FOM algorithm implementation (9800-40, 9800-80 and 9800-L)

- AES CBC (128) encryption KAT
- AES CBC (128) decryption KAT
- AES GCM (256) encryption KAT
- AES GCM (256) decryption KAT
- TripleDES-CBC Encryption KAT
- TripleDES-CBC Decryption KAT
- HMAC SHA-1 KAT
- HMAC SHA2-256 KAT
- HMAC SHA2-384 KAT
- HMAC SHA2-512 KAT
- ECDSA P-256 sign and verify KATs
- RSA 2048 sign and verify KATs
- SP 800-90A AES-CTR DRBG KAT
- SP 800-90A Section 11 Health Tests

IOS Common Cryptographic Module (9800-40, 9800-80 and 9800-L)

- AES CBC (128) encryption KAT
- AES CBC (128) decryption KAT
- AES GCM encryption KAT
- AES GCM decryption KAT
- TripleDES-CBC Encryption KAT
- TripleDES-CBC Decryption KAT
- Diffie-Hellman “Z” primitive KAT
- EC Diffie-Hellman “Z” primitive KAT
- ECDSA (P-256 and P-384) Sign and Verify KATs
- HMAC SHA-1 KAT
- HMAC SHA2-256 KAT
- HMAC SHA2-384 KAT
- HMAC SHA2-512 KAT
- RSA 2048 Sign and Verify KATs

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- SP 800-90A AES-CTR DRBG KAT
- SP 800-90A Section 11 Health Tests

Hardware Crypto (CN6880) (9800-40 and 9800-80)
- AES GCM (128) encryption KAT
- AES GCM (128) decryption KAT
- AES CBC (128) encryption KAT
- AES CBC (128) decryption KAT
- SHA-1 KAT
- SHA2-256 KAT
- SHA2-384 KAT
- SHA2-512 KAT

As per IG 9.1 and IG 9.2, the module performs the HMAC SHA selftests and these tests pass, thus assuring the health of underlying SHS implementations for CiscoSSL FOM algorithm implementation and IOS Common Cryptographic Module.

The module performs all power-on self-tests automatically at boot. All power-on self-tests must be passed before a role 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 module from passing any data during a power-on self-test failure.

Conditional Tests Performed:
- Continuous Random Number Generator Test for the FIPS-approved DRBG
- Continuous Random Number Generator Test for the non-approved NDRNG
- ECDSA pairwise consistency test
- RSA pairwise consistency test
- Firmware Load test using a 2048-bit/SHA-512 RSA-Based integrity test to verify firmware to be loaded into the module.

10 Physical Security

The modules are production grade multi-chip standalone cryptographic modules that meet level 1 physical security requirements.

11 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 modules are shipped in Cisco boxes with Cisco adhesive, so if tampered with the recipient will notice. Follow the setting instructions provided below to place the module in a FIPS-approved mode. Operating this module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

It should also be noted that the module is shipped to the customer site without the firmware pre-installed on the device. This means that the module arrives at the customer in a non-compliant state until such time as the Crypto Officer has performed the following steps:

- Downloaded the module's correct FIPS firmware image (via a secure method from https://software.cisco.com/)
- Verified the integrity of the firmware image file (by calculating an MD5 or a SHA512 checksum value of the downloaded image file and comparing it with values provided on the Cisco download page),
- Installed the firmware onto the module, and
- Has performed all of the correct initialization steps (see below) after which time the module will then be in a FIPS compliant state.

Only after a successful completion of all required FIPS POSTs in the FIPS compliant state, will the module be considered to be in a FIPS-approved mode of operation.

The modules are validated with IOS-XE Firmware version 16.12 with Cisco FOM 7.0a (9800-40, 9800-80 and 9800-L), IOS Common Cryptographic Module (9800-40, 9800-80 and 9800-L) and Cavium Octeon II Datapath (9800-40 and 9800-80). Any firmware versions other than IOS-XE 16.12, loaded into the modules are out of the scope of this validation and require a separate FIPS 140-2 validation. Follow the setting instructions provided below to place the module in FIPS-approved mode. Operating the module without maintaining the following settings will remove the module from the FIPS approved mode of operation.

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

11.1 System Initialization and Configuration

Step1 - The value of the boot field must be 0x2102. This setting disables break from the console to the ROM monitor and automatically boots. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

```
>config-register 0x2102
```

Step 2 - The Crypto Officer must set up the operators of the module. Procedurally, the password must be at least 8 characters (procedurally enforced by policy), including at least one letter and at least one number, and is entered when the Crypto Officer first engages the "configure terminal" command. The Crypto Officer enters the following syntax at the "#" prompt:

```
>configure terminal
>username [USERNAME] privilege 15 password [PASSWORD]
```

Step 3 – For the created operators, identification and authentication on the console/auxiliary port is required for Users. From the "configure terminal" command line, the Crypto Officer enters the following syntax:

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

>line con 0
>login local

Step 4 - Enable FIPS Mode of Operations
The following CLI command places the controller in FIPS mode of operations, enabling all necessary self-tests and algorithm restriction

>configure terminal
>fips-authorization key <32-bit Hex Value>
>platform ipsec fips-mode
>write memory

Save the configuration then reload. At the next boot, FIPS Mode will be set.

11.2 Transition of module from FIPS mode to non-FIPS mode

The keys and CSPs generated in the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs shall be zeroized by the Crypto Officer.

For transition from FIPS to non-FIPS mode, the Crypto Officer has to zeroize the module to delete all plaintext secret and private cryptographic keys and CSPs as defined in the Table 9 of this non-proprietary FIPS 140-2 Security Policy document and the Crypto Officer has to issue "no fips authorization key <128-bits (16 octet) key to be used>" command in addition to those defined in Table 9 of this document.

11.3 Protocol Configuration

1. Enable CAPWAP data encryption

   >sh ap sum

   >config t

   > ap profile default-ap-profile

   > link-encryption
   Enabling link-encryption globally will reboot the APs with no link-encryption.
   Are you sure you want to continue? (y/n)[y]: y

2. Enable SSH

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

>config t

>ip ssh version 2

>ip ssh server aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc

>ip ssh server algorithm mac hmac-sha1

>ip ssh server algorithm hostkey ssh-rsa

>show ip ssh

(replace “server” with “client” to configure the client protocols.

3. Enable HTTPS

   >config t

   >ip http secure-server

   >ip http secure-trustpoint CA-trust-local

   >ip https tls-version tlsv1.1 tlsv1.2

   >show ip http server secure status

4. Add SNMPv3 Config

   >snmp-server group SnmpAuthPrivGroup v3 priv

   >snmp-server group SnmpAuthNoPrivGroup v3 auth

   >snmp-server group SnmpNoAuthNoPrivGroup v3 noauth

   >snmp-server community snmp RO

   >snmp-server host <IPaddress> snmp

12 Related Documentation

This document deals only with operations and capabilities of the security appliances in the technical terms of a FIPS 140-2 cryptographic device security policy. More information is available on the security appliances from the sources listed in this section and from the following source:

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- The NIST Cryptographic Module Validation Program website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains contact information for answers to technical or sales-related questions for the security appliances.
- Software Configuration Guide (https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/16-12/config-guide/b_wl_16_12_cg.html)

13 Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

13.1 Cisco.com

You can access the most current Cisco documentation at this URL:
http://www.cisco.com/techsupport

You can access the Cisco website at this URL:
http://www.cisco.com

You can access international Cisco websites at this URL:
http://www.cisco.com/public/countries_languages.shtml

13.2 Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.
The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.
The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:
http://www.cisco.com/go/marketplace/

13.3 Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:
http://www.cisco.com/go/marketplace/
Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

14 Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.
You can send comments about Cisco documentation to bug-doc@cisco.com.
You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

15 Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:
http://www.cisco.com/go/psirt
If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:
http://tools.cisco.com/security/center/rss.x?i=44

15.1 Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified vulnerability in a Cisco product, contact PSIRT:

- Emergencies — security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- Nonemergencies — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*. Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:
http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html
The link on this page has the current PGP key ID in use.

16 Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

16.1 Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:
http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:
http://tools.cisco.com/RPF/register/register.do

Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

16.2 Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:
http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:
http://www.cisco.com/techsupport/contacts

16.3 Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.
Severity 1 (S1) – Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.
Severity 2 (S2) – Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
Severity 3 (S3) – Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.
Severity 4 (S4) – You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

17 Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

http://www.cisco.com/go/marketplace/

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

http://www.cisco.com/packet

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

http://www.cisco.com/en/US/learning/index.html

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

Definitions List

ACL	Access Control List
AES	Advanced Encryption Standard
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameter
DRAM	Dynamic RAM
DRBG	Deterministic random bit generator
ESP	Embedded Services Processor
FIPS	Federal Information Processing Standard
Gbps	Gigabits per second
GigE	Gigabit Ethernet
HMAC	Hash Message Authentication Code
HTTP	Hyper Text Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
ISAKMP	Internet Security Association and Key Management Protocol
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random Access Memory
PIN	Personal Identification Number
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman method for asymmetric encryption
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell

© Copyright 2020 Cisco Systems, Inc.

This document may be freely reproduced and distributed whole and intact including this Copyright Notice.

TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
USB	Universal Serial Bus
VPN	Virtual Private Network

© Copyright 2020 Cisco Systems, Inc.
This document may be freely reproduced and distributed whole and intact including this Copyright Notice.