Cisco Catalyst 3560-CX Switch

FIPS 140-2 Non Proprietary Security Policy
Level 1 Validation

Version 0.4

August 24, 2016

Table of Contents

1 Introduction

1.1 Purpose

This document is the non-proprietary Cryptographic Module Security Policy for the Cisco Catalyst 3560-CX Switch. This security policy describes how the modules listed below meet the security requirements of FIPS 140-2, and how to operate the switch with on-board crypto enabled in a secure FIPS 140-2 mode. Modules covered in this document are listed below:

Cisco Catalyst WS-3560CX-8TC-S running IOS Firmware Version - 15.2(3)E1

This policy was prepared as part of the Level 1 FIPS 140-2 validation of the Catalyst 3560-CX Switch.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 — *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website at http://csrc.nist.gov/groups/STM/index.html.

1.2 Module Validation Level

The following table lists the level of validation for each area in the FIPS PUB 140-2.

No.	Area Title	Level
1	Cryptographic Module Specification	1
2	Cryptographic Module Ports and Interfaces	1
3	Roles, Services, and Authentication	2
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

1.3 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the switch from the following sources:

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

Catalyst 3560-CX switch - http://www.cisco.com/c/en/us/products/switches/catalyst-3560-cx-series-switches/index.html
For answers to technical or sales related questions, please refer to the contacts listed on the Cisco Systems website at www.cisco.com.

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

1.4 Terminology

In this document, the Catalyst 3560-CX switch is referred to as C3560-CX, the switch or the module.

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 Catalyst 3560-CX switch 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 switch. 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 Catalyst 3560-CX Switch

The compact Cisco® Catalyst® 3560-CX Switch easily extends an intelligent, fully managed Cisco Catalyst wired switching infrastructure, including end-to-end IP and Borderless Network services, with a single Ethernet cable or fiber from the wiring closet. These attractive, small form-factor Gigabit and Fast Ethernet switches are ideal for connecting multiple devices: wherever space is at a premium and multiple cable runs could be challenging. This switch delivers advanced Layer 2 switching with intelligent Layer 2 through 4 services for the network edge, such as voice, video, and wireless LAN services, including support for routed access, Cisco TrustSec®, and other Cisco Borderless Network services. Catalyst 3560-CX implements MACsec, but the feature is not available in FIPS mode of operation. The Catalyst 3560-CX Switch meets FIPS 140-2 overall Level 1 requirements as a multi-chip standalone module.

2.1 Cryptographic Module Physical Characteristics

The C3560-CX switch is a small form factor, fixed chassis switch. This fanless, small form-factor switch is ideal for space-constrained deployments where multiple cable runs would be challenging. C3560-CX is a Gigabit Ethernet (GbE) managed switch, which is ideal for high-speed data connectivity and Wi-Fi backhaul. With a single copper or fiber cable from the wiring closet, this Cisco Catalyst compact switch enables IP connectivity for devices such as IP phones, wireless access points, surveillance cameras, PCs, and video endpoints.

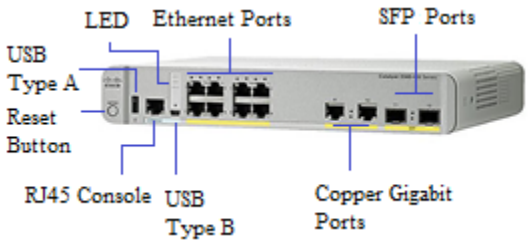

Figure 1- Cisco C3560-CX Switch

2.2 Cryptographic Boundary

The cryptographic boundary is defined as being the physical enclosure of the chassis. All of the functionality described in this publication is provided by components within this cryptographic boundary.

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 four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The module also supports a power interface.

The following table identifies the features on the module covered by this Security Policy:

Model	Ethernet Ports	PoE Output Ports	Available PoE Power	Uplinks
3560CX-8TC-S	8 x 10/100/1000 Gigabit Ethernet	N/A		2x1G copper plus 2x1G SFP

Table 2 - C3560-CX Interface Information

Note: Cisco Catalyst 3560-CX includes hardware for IEEE 802.1AE MACsec for Layer 2, line-rate Ethernet data confidentiality and integrity on host-facing ports. But the capability has not been tested for FIPS 140-2.

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 Table 3 below:

Physical Interface	Logical Interface
Ethernet Ports (RJ45) Copper Gigabit Ports SFP Ports Type A USB port Console Port (RJ45 and USB Type B)	Data Input Interface
Ethernet Ports (RJ45) Copper Gigabit Ports SFP Ports Type A USB port Console Port (RJ45 and USB Type B)	Data Output Interface
Ethernet Ports (RJ45) Copper Gigabit Ports SFP Ports Console Port (RJ45 and USB Type B) Reset Button	Control Input Interface
Copper Gigabit Ports SFP Ports Console Port (RJ45 and USB Type B) LEDs	Status Output Interface
Power Plug	Power Interface

Table 3 - Module Interfaces

3 Roles, Services, and Authentication

Authentication is role-based. Each user is authenticated upon initial access to the module. There are two roles in the switch that may be assumed: the Crypto Officer (CO) role and the User role. The administrator of the switch assumes the CO role in order to configure and maintain the switch using CO services, while the Users exercise security services over the network.

3.1 User Role

The role is assumed by users obtaining general security services. From a logical view, user activity exists in the data-plane. Users are authenticated using a password and their data is protected with secure communication protocol such as IPsec. The user passwords must be at least eight (8) characters long, including at least one letter and at least one number character (enforced procedurally). If six (6) special/alpha/number characters, one (1) special character and one (1) number are used without repetition for an eight (8) digit value, the probability of randomly guessing the correct sequence is one (1) in 187,595,543,116,800. This is calculated by performing 94 x 93 x 92 x 91 x 90 x 89 x 32 x 10. Therefore, the associated probability of a successful random attempt is approximately 1 in 187,595,543,116,800, which is less than 1 in 1,000,000 required by FIPS 140-2. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the module.

The User role can also be authenticated via certificate credentials by using 2048 bit RSA keys – in such a case the security strength is 112 bits, so the associated probability of a successful random attempt is 1 in 2^{112}, which is less than 1 in 1,000,000 required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be

capable of approximately $8.65x10^{31}$ attempts per second, which far exceeds the operational capabilities of the module to support.

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
IPsec VPN	Negotiation and encrypted data transport via IPSec VPN	User password, 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, IPsec authentication key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)

Table 4 - User Services

3.2 Crypto Officer Role

This role is assumed by an authorized CO connecting to the switch via CLI through the console port and performing management functions and module configuration. From a logical view, CO activity exists only in the control plane. IOS prompts the CO for their username and password, and, if the password is validated against the CO's password in IOS memory, the CO is allowed entry to the IOS executive program. The module supports RADIUS and TACACS+ for authentication of CO.

CO passwords must be at least eight (8) characters long, including at least one letter and at least one number character (enforced procedurally). If six (6) special/alpha/number characters, one (1) special character and one (1) number are used without repetition for an eight (8) digit value, the probability of randomly guessing the correct sequence is one (1) in 187,595,543,116,800. This is calculated by performing 94 x 93 x 92 x 91 x 90 x 89 x 32 x 10. Therefore, the associated probability of a successful random attempt is approximately 1 in 187,595,543,116,800, which is less than 1 in 1,000,000 required by FIPS 140-2. In order to successfully guess the sequence in one minute would require the ability to make over 3,126,592,385,280 guesses per second, which far exceeds the operational capabilities of the module.

The Crypto Officer role is responsible for the configuration of the switch. 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	Define network interfaces and settings, create command aliases, set the protocols the switch will support, enable interfaces and network services, set system date and time, and load authentication information.	Enable password (r, w, d)
Manage	Log off users, shutdown or reload the switch, manually back up switch configurations, view complete configurations, manage user rights, and restore switch configurations.	Enable password (r, w, d)

Services	Description	Keys and CSPs Access
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.	Enable password (r, w, d)
View Status Functions	View the switch configuration, routing tables, active sessions, health, temperature, memory status, voltage, packet statistics; review accounting logs; and view physical interface status.	Enable password (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.	IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE authentication private Key, IKE authentication public key, skeyid, skeyid_d, SKEYSEED, IPsec encryption key, IPsec authentication key (r, w, d)
Configure Remote Authentication	Set up authentication account for users and devices using RADIUS or TACACS+.	RADIUS secret, RADIUS Key wrap key, TACACS+ secret (r, w, d)
HTTPs	HTTP server over TLS (1.0).	TLS Server RSA private key, TLS Server RSA public key, TLS pre-master secret, TLS session keys, TLS authentication keys, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)
SSH v2	Configure SSH v2 parameter, provide entry and output of CSPs.	DH private DH public key, DH Shared Secret, SSH RSA private key, SSH RSA public key, SSH session key, SSH session authentication key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)
SNMPv3	Configure SNMPv3 MIB and monitor status.	SNMPv3 Password, snmpEngineID, SNMP session key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)
IPsec VPN	Configure IPsec VPN parameters, provide entry and output of CSPs.	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, IPsec authentication key, DRBG entropy input, DRBG Seed, DRBG V, DRBG Key (r, w, d)
Self-Tests	Execute the FIPS 140 start-up tests on demand.	N/A
User services	The Crypto Officer has access to all User services.	User Password (r, w, d)
Zeroization	Zeroize cryptographic keys/CSPs by running the zeroization methods classified in table 8, Zeroization column.	All CSPs (d)

Table 5 - Crypto Officer Services

3.3 Unauthorized Role

The services for someone without an authorized role are: passing traffic through the device, view the status output from the module's LED pins, and cycle power.

3.4 Services Available in Non-FIPS Mode of Operation

The cryptographic module in addition to FIPS mode of operation can operate in a non-FIPS mode of operation. This is not a recommended operational mode but because the associated RFC's for the following protocols allow for non-approved algorithms and non-approved key sizes a non-approved mode of operation exist. The module is considered to be in a non-FIPS mode of operation when it is not configured per section 7. The FIPS approved services listed in table 6 become non-approved services when using any non-approved algorithms or non-approved key or curve sizes.

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
SNMP v1/v2	Hashing: MD5 Symmetric: DES
MACsec	AES GCM

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

Note: The AES GCM supporting MACsec service is a non-compliant algorithm.

Neither the User nor the Crypto Officer are allowed to operate any of these services while in FIPS mode of operation.

4 Physical Security

The module is a multi-chip standalone cryptographic module. The module meets FIPS 140-2 level 1 physical security requirements as production grade equipment.

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

5 Cryptographic Algorithms

5.1 Approved Cryptographic Algorithms

The switch supports many different cryptographic algorithms. However, only FIPS approved algorithms may be used while in the FIPS mode of operation. Table 7 below identifies the approved algorithms included in the module for use in the FIPS mode of operation.

Algorithm	Algorithm Implementation Name
	IOS Common Cryptographic Module (IC2M) Algorithm Module (Firmware)
AES (CBC, GCM; 128, 192, 256 bits)	#3984 and #4016
Triple-DES (CBC, 3-key, 192 bits)	#2187
SHS (SHA-1/256/384/512)	#3289
HMAC (SHA-1)	#2600
RSA (FIPS 186-4 KeyGen; PKCS1_V1_5; 2048 bits; Signature Generation/Verification)	#2045
DRBG (SP 800-90A AES CTR-256)	#1177
CVL Component (SP800-135 KDF for IKEv2, TLSv1.0, SSH, SNMPv3)	#813

Table 7- Approved Cryptographic Algorithms and Associated Certificate Number

Notes:

- There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in Table 7.
- The AES-GCM IV generation method from AES #4016 is in compliance with IG A.5, scenario #1. The module is in compliance with the RFC 6071 (IPSec Protocol). The module generates new AES-GCM keys if the module loses power.
- The SSH, TLSv1.0, SNMPv3 and IKEv2 protocols have not been reviewed or tested by the CAVP and CMVP.

5.2 Non-FIPS Approved, but Allowed Cryptographic Algorithms

The cryptographic module implements the following non-approved algorithms, but they are allowed to be used in a FIPS 140-2 mode of operation.

- Diffie-Hellman (key agreement; key establishment methodology provides between 112 and 150 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- AES (Cert. #3984, key wrapping; key establishment methodology provides 128 or 256 bits of encryption strength)
- NDRNG (entropy source for DRBG; at minimum 256 bits can be obtained)
- HMAC-MD5 is allowed in FIPS mode strictly for TLS
- MD5 is allowed in FIPS mode strictly for TLS

Notes:

- The AES key wrapping method is not compliant with SP 800-38F.

5.3 Non-FIPS Approved and not Allowed Cryptographic Algorithms

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

- AES GCM (non-compliant)
- DES
- Diffie-Hellman (key agreement; non-compliant less than 112 bits of encryption strength)
- HMAC-MD5
- MD5
- RC4
- RSA (key wrapping; non-compliant less than 112 bits of encryption strength)

5.4 Self-Tests

The module includes an array of self-tests that are run during startup and periodically during operations to prevent any secure data from being released and to ensure all components are functioning correctly. The module implements the following power-on self-tests:

- IOS Power-On Self-Tests Known Answer Tests (KATs):
    - AES (encryption and decryption) KATs
    - AES-CMAC KAT
    - AES-GCM (encryption and decryption) KATs
    - AES-256 CTR DRBG KAT
    - HMAC-SHA-1 KAT
    - DRBG health test (Note: DRBG Health Tests as specified in SP800-90A Section 11.3 are performed)
    - SHA-1 KAT
    - SHA-256 KAT
    - SHA-512 KAT
    - RSA (sign and verify) KATs
    - Triple-DES (encryption and decryption) KATs
- Firmware Integrity Test
    - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256

The module performs all power-on self-tests automatically at boot. All power-on self-tests must be passed before any operator can perform cryptographic services. The power-on self-tests are performed after the cryptographic systems are initialized but prior to any other operations; this prevents the module from passing any data during a power-on self-test failure.

In addition, the modules also provide the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for SP800-90A DRBG
- CRNGT for the NDRNG
- Pairwise Consistency Test for RSA
- Conditional IPSec Bypass Test

6 Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. All keys are also protected by the password-protection on the CO role login, and can be zeroized by the CO. Keys are exchanged and entered electronically. Persistent keys are entered by the CO via the console port CLI, transient keys are generated or established and stored in DRAM.

Note that the command **fips zeroize all** will zeroize a large majority of the listed CSPs.

The module supports the following cryptographic keys and critical security parameters (CSPs):

ID	Algorithm	Description	Storage	Zeroization Method
General Keys/CSPs				
Enable password	Password	Variable (8+ characters). The password used to authenticate the CO role. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Zeroized by overwriting with new password
User password	Password	Variable (8+ characters). The password used to authenticate the User role. This CSP is created by the CO role and entered by the User role.	NVRAM (plaintext)	Zeroized by overwriting with new password
RADIUS secret	Shared Secret	Variable (8+ characters). The RADIUS shared secret is used for RADIUS Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Zeroized by "# no radius-server key" command
RADIUS Key wrap key	AES-CBC	128/256 bits. Secures communication with RADIUS authentication server. This CSP is derived from the RADIUS secret.	DRAM (plaintext)	Zeroized when data structure is freed
TACACS+ secret	Shared Secret	Variable (8+ characters). The TACACS+ shared secret is used for TACACS+ Client/Server authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Zeroized by "# no tacacs-server key" command
DRBG entropy input	SP 800-90A CTR_DRBG	256-bits. HW based entropy source output used to construct the seed.	DRAM (plaintext)	Automatically when the switch is power cycled
DRBG Seed	SP 800-90A CTR_DRBG	384-bits. Generated using DRBG derivation function that includes the entropy input from hardware-based entropy source.	DRAM (plaintext)	Automatically when the switch is power cycled
DRBG V	SP 800-90A CTR_DRBG	128-bits. Generated by entropy source via the CTR_DRBG derivation function. It is stored in DRAM with plaintext form	DRAM (plaintext)	Automatically when the switch is power cycled
DRBG Key	SP 800-90A CTR_DRBG	256-bits. This is the 256-bit DRBG key used for SP 800-90A CTR_DRBG. Established per SP 800-90A CTR_DRBG.	DRAM (plaintext)	Automatically when the switch is power cycled
Diffie-Hellman private key	Diffie-Hellman	224-379 bits DH private key used in Diffie-Hellman (DH) exchange. Generated by calling the SP 800-90A CTR-DRBG.	DRAM (plaintext)	Automatically after shared secret generated.

Diffie-Hellman public key	Diffie-Hellman	2048-4096 bits DH private key used in Diffie-Hellman (DH) exchange. Generated by calling the SP 800-90A CTR-DRBG.	DRAM (plaintext)	Automatically after shared secret generated.
Diffie-Hellman Shared Secret	Diffie-Hellman	2048-4096 bits. DH shared secret derived in Diffie-Hellman (DH) exchange.	DRAM (plaintext)	Zeroized upon deletion
SSH				
SSH RSA private key	RSA	2048 bits. The SSHv2 private key used in SSHv2 connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
SSH RSA public key	RSA	2048 bits. The SSHv2 public key used in SSHv2 connection. This key is internally generated by the module.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
SSH session key	Triple-DES/AES	192-bits/256-bits. This is the SSHv2 session key. It is used to encrypt all SSHv2 data traffic 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 terminated
SSH session authentication key	HMAC SHA	160-bits. It is used to authenticate all SSHv2 data traffic traversing between the SSHv2 Client and SSHv2 Server. This key is internally derived by the module.	DRAM (plaintext)	Automatically when SSH session terminated
TLS				
TLS Server RSA private key	RSA	2048 bits. The TLS server private key used in TLS connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
TLS Server RSA public key	RSA	2048 bits. The TLS server public key used in TLS connection. This key is generated by calling SP 800-90A DRBG.	NVRAM (plaintext)	Zeroized by "# fips zeroize all" command
TLS pre-master secret	Shared Secret	384-bits. Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	DRAM (plaintext)	Automatically when session terminated.
TLS session keys	Triple-DES/AES	192-bits/256-bits. This is the TLS session key. It is used to encrypt all TLS data traffic traversing between the TLS client and server. This key is derived via key derivation function defined in SP800-135 KDF (TLS).	DRAM (plaintext)	Automatically when session terminated.

TLS authentication keys	HMAC SHA	160-bit. This is the TLS authentication key. It is used to authenticate all TLS data traffic traversing between the TLS client and server. This key is internally generated by the module.	DRAM (plaintext)	Automatically when session terminated.
IPSec				
Skeyid	Shared Secret	160 bits. A shared secret known only to IKE peers. It is established via key derivation function defined in SP800-135 KDF and it will be used for deriving other keys in IKE protocol implementation.	DRAM (plaintext)	Automatically when session expires
skeyid_d	Shared Secret	160 bits. A shared secret known only to IKE peers. It is 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 session expires
SKEYSEED	Shared Secret	160 bits. A shared secret known only to IKE peers. It is 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 session expires
IKE session encryption key	TRIPLE-DES/AES	192-bit Triple-DES or a 256-bit AES. 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 session expires
IKE session authentication key	HMAC-SHA1	160 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 session expires
ISAKMP preshared	pre-shared secret	The secret used to derive IKE skeyid when using preshared secret authentication. This CSP is entered by the Crypto Officer.	NVRAM (plaintext)	Zeroized by overwriting with new secret
IKE Authentication private Key	RSA	2048 bits. RSA private key used in IKE authentication. This key is generated by calling SP800-90A DRBG.	NVRAM (plaintext)	Zeroized by “# fips zeroize all” command
IKE Authentication public Key	RSA	2048 bits. RSA public key used in IKE authentication. Internally generated by the module.	NVRAM (plaintext)	Zeroized by “# fips zeroize all” command

IPSec Authentication key	HMAC-SHA-1	160 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 session expires
IPSec encryption key	TRIPLE-DES/AES/AES-GCM	192 bits Triple-DES or 128/192/256 bits AES. 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 session expires
SNMPv3				
SNMPv3 Password	Secret	256 bits. This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication.	NVRAM (plaintext)	Zeroized by overwriting with new secret
snmpEngineID	Shared secret	32 bits. Unique string to identify the SNMP engine.	NVRAM (plaintext)	Overwritten with new engine ID
SNMP session key	AES	128 bits. Encrypts SNMP traffic.	DRAM (plaintext)	Automatically when session expires

Table 8 - Cryptographic Keys and CSPs

7 Secure Operation of the C3560-CX Switch

The switch meets all the overall Level 1 requirements for FIPS 140-2. Follow the setup instructions provided below to place the module in FIPS-approved mode. Operating this Switch without maintaining the following settings will remove the module from the FIPS approved mode of operation.

7.1 System Initialization and Configuration

1. The value of the boot field must be 0x0102. This setting disables break from the console to the ROM monitor and automatically boots. From the "configure terminal" command line, the CO enters the following syntax:

   config-register 0x0F

2. The CO must create the "enable" password for the CO role. Procedurally, the password must be at least 8 characters, including at least one letter and at least one number, and is entered when the CO first engages the "enable" command. The CO enters the following syntax at the "#" prompt:

   Switch(config)# enable secret [PASSWORD]

3. The CO must always assign passwords (of at least 8 characters, including at least one letter and at least one number) to users. Identification and authentication on the console/auxiliary port is required for Users. From the "configure terminal" command line, the CO enters the following syntax:

Switch(config)# line con 0
Switch(config)# password [PASSWORD]
Switch(config)# login local

4. To ensure all FIPS 140-2 logging is received, set the log level:

   Switch(config)# logging console errors

5. The CO may configure the module to use RADIUS or TACACS+ for authentication. If the module is configured to use RADIUS, the CO must define RADIUS or shared secret keys that are at least 8 characters long, including at least one letter and at least one number. The RADIUS or TACACS+ traffic must be protected by an IPSec tunnel.
6. The CO shall only assign users to a privilege level 1 (the default).
7. The CO shall not assign a command to any privilege level other than its default.

7.2 Remote Access

1. Remote access is permitted via SSHv2, TLS and SNMPv3. While in FIPS 140-2 Mode of Operation the module will enforce use of Approved algorithms for the management protocols.

8 Definition List

AES – Advanced Encryption Standard
CMVP – Cryptographic Module Validation Program
CSE – Communications Security Establishment
CSP – Critical Security Parameter
DRBG – Deterministic Random Bit Generator
FIPS – Federal Information Processing Standard
HMAC – Hash Message Authentication Code
HTTP – Hyper Text Transfer Protocol
KAT – Known Answer Test
LED – Light Emitting Diode
MAC – Message Authentication Code
MACsec – IEEE MAC Security protocol 802.1AE
NDRNG – Non-Deterministic Random Number Generator
NIST – National Institute of Standards and Technology
NVRAM – Non-Volatile Random Access Memory
PoE+ – Power over Ethernet Plus
RAM – Random Access Memory
SHA – Secure Hash Algorithm
SHS – Secure Hashing Standard
Triple-DES – Triple Data Encryption Standard