Cisco Catalyst 4503-E, Catalyst 4506-E, Catalyst 4507R-E, Catalyst 4507R+E, Catalyst 4510R-E, Catalyst 4510R+E with Supervisor Cards (WS-X45-SUP7-E and WS-X45-Sup7L-E) and Line Cards (WS-X4748-RJ45V+E, WS-X4712-SFP+E, WS-X4640-CSFP-E, WS-X4748-NGPOE+E, and WS-X4748-RJ45-E)

FIPS 140-2 Level 2
Non-Proprietary Security Policy

Overall Level 2 (Sections 3 and 10 Level 3) Validation

Version 0.11

May 2013

Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Cisco Catalyst 4503-E, Catalyst 4506-E, Catalyst 4507R-E, Catalyst 4507R+E, Catalyst 4510R-E, Catalyst 4510R+E with Supervisor Cards (WS-X45-SUP7-E and WS-X45-Sup7L-E) and Line Cards (WS-X4748-RJ45V+E, WS-X4712-SFP+E, WS-X4640-CSFP-E, WS-X4748-NGPOE+E, and WS-X4748-RJ45-E), referred to in this document as the modules or switches. This security policy describes how modules meet the security requirements of FIPS 140-2 and how to run the modules in a FIPS 140-2 mode of operation and may be freely distributed.

Versions:

- Catalyst 4503-E
- Catalyst 4506-E
- Catalyst 4507R+E
- Catalyst 4507R-E
- Catalyst 4510R+E
- Catalyst 4510R-E
- Supervisor Card WS-X45-SUP7-E
- Supervisor Card WS-X45-Sup7L-E
- Line Card WS-X4748-RJ45V+E
- Line Card WS-X4712-SFP+E
- Line Card WS-X4640-CSFP-E
- Line Card WS-X4748-NGPOE+E
- Line Card WS-X4748-RJ45-E
- Catalyst 4503 FIPS kit packaging (WS-C4503-FIPS-KIT=)
- Catalyst 4506 FIPS kit packaging (WS-C4506-FIPS-KIT=)
- Catalyst 4507 FIPS kit packaging (WS-C4507-FIPS-KIT=)
- Catalyst 4510 FIPS kit packaging (WS-C4510-FIPS-KIT=)
- Filler Plate (C4K-SLOT-CVR-E)
- IOS-XE version 3.3.1SG

Configuration

The switches included as part of the FIPS validation may be configured in the following configurations.

Chassis	Supervisor Cards	Line Cards
Catalyst 4503-E	Single supervisor card WS-X45-SUP7-E	**Up to Two (2) of the following line cards in any configuration.**
		Single line card WS-X4748-RJ45V+E
		Single line card WS-X4712-SFP+E
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-NGPOE+E
	Single supervisor card WS-X45-Sup7L-E	**Up to Two (2) of the following line cards in any configuration.**

Chassis	Supervisor Cards	Line Cards
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-RJ45-E
Catalyst 4506-E	Single supervisor card WS-X45-SUP7-E	**Up to Five (5) of the following line cards in any combination.**
		Single line card WS-X4748-RJ45V+E
		Single line card WS-X4712-SFP+E
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-NGPOE+E
		Single line card WS-X4748-RJ45-E
	Single supervisor card WS-X45-Sup7L-E	**Up to Five (5) of the following line cards in any combination.**
		Single line card WS-X4748-RJ45V+E
		Single line card WS-X4712-SFP+E
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-NGPOE+E
		Single line card WS-X4748-RJ45-E
Catalyst 4507R+E	Dual supervisor card WS-X45-SUP7-E	**Up to Five (5) of the following line cards in any combination.**
		Single line card WS-X4748-RJ45V+E
		Single line card WS-X4712-SFP+E
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-NGPOE+E
		Single line card WS-X4748-RJ45-E
	Dual supervisor card WS-X45-Sup7L-E	**Up to Five (5) of the following line cards in any combination.**
		Single line card WS-X4748-RJ45V+E
		Single line card WS-X4712-SFP+E
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-NGPOE+E
		Single line card WS-X4748-RJ45-E
Catalyst 4507R-E	Dual supervisor card WS-X45-SUP7-E	**Up to Five (5) of the following line cards in any combination.**
		Single line card WS-X4748-RJ45V+E
		Single line card WS-X4712-SFP+E
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-NGPOE+E
		Single line card WS-X4748-RJ45-E
	Dual supervisor card WS-X45-Sup7L-E	**Up to Five (5) of the following line cards in any combination.**
		Single line card WS-X4748-RJ45V+E
		Single line card WS-X4712-SFP+E

Chassis	Supervisor Cards	Line Cards
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-NGPOE+E
		Single line card WS-X4748-RJ45-E
Catalyst 4510R+E	Dual supervisor card WS-X45-SUP7-E	**Up to Eight (8) of the following line cards in any combination.**
		Single line card WS-X4748-RJ45V+E
		Single line card WS-X4712-SFP+E
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-NGPOE+E
		Single line card WS-X4748-RJ45-E
Catalyst 4510R-E	Dual supervisor card WS-X45-SUP7-E	**Up to Eight (8) of the following line cards in any combination.**
		Single line card WS-X4748-RJ45V+E
		Single line card WS-X4712-SFP+E
		Single line card WS-X4640-CSFP-E
		Single line card WS-X4748-NGPOE+E
		Single line card WS-X4748-RJ45-E

Table 1: Module Hardware Configurations

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 module from the following sources:

- The Cisco Systems website (http://www.cisco.com) contains information on the full line of products from Cisco Systems.
- 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 module.
- 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/cmvp/index.html.

FIPS 140-2 Submission Package

The security policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the submission package includes:

- Vendor Evidence
- Finite State Machine

- Other supporting documentation as additional references

With the exception of this non-proprietary security policy, the FIPS 140-2 validation documentation is proprietary to Cisco Systems, Inc. and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Cisco Systems, Inc. See “Obtaining Technical Assistance” section for more information.

Module Description

Branch office networking requirements are dramatically evolving, driven by web and e-commerce applications to enhance productivity and merging the voice and data infrastructure to reduce costs. The Catalyst 4500 series switches with the VPN Services Port Adapter offer versatility, integration, and security to branch offices. The Catalyst 4500 series switches provide a scalable, secure, manageable remote access server that meets FIPS 140-2 Level 2 requirements, as a multi-chip standalone module.

The switches include cryptographic algorithms implemented in IOS-XE software, IOS-XE Image Signing software, and hardware ASICs. The line card ASICs implement CTS (Cisco proprietary TrustSec protocol) supporting IEEE 802.1AE for Layer 2 CTS and contain hardware implementations of the GCM and ECB modes of the AES algorithm.

The switches support the Cisco TrustSec protocol which provides policy-based access control, identity-aware networking, and data confidentiality and integrity; and Virtual Switching System which is a system virtualization technology that allows the pooling of multiple Catalyst 4500 switches into a single virtual switch.

The switches also support SSH and TLS to provide remote administrative access to the module.

The following pictures are representative each of the switch modules:

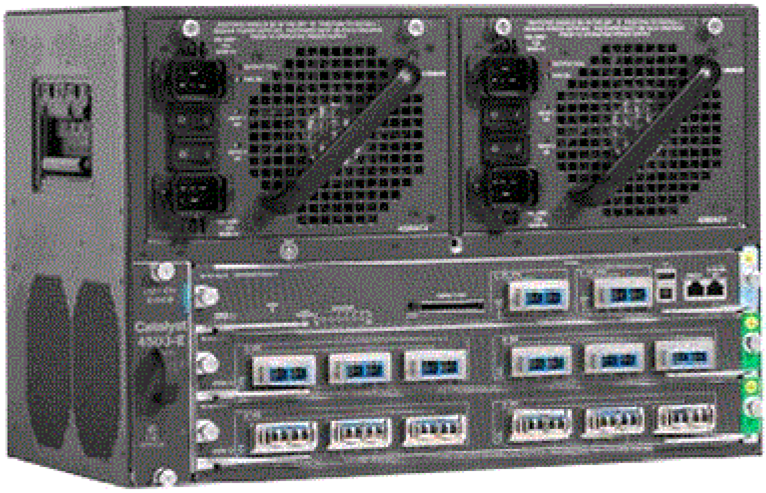

Figure 1: Catalyst 4503-E Switch

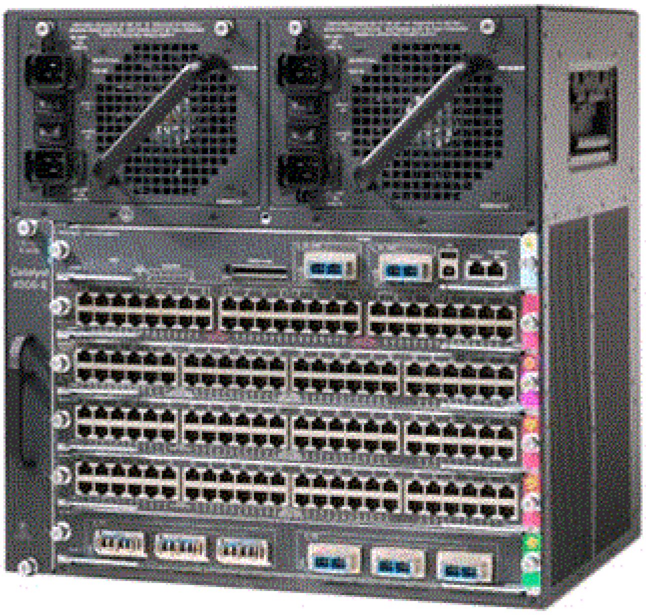

Figure 2: Catalyst 4506-E Switch

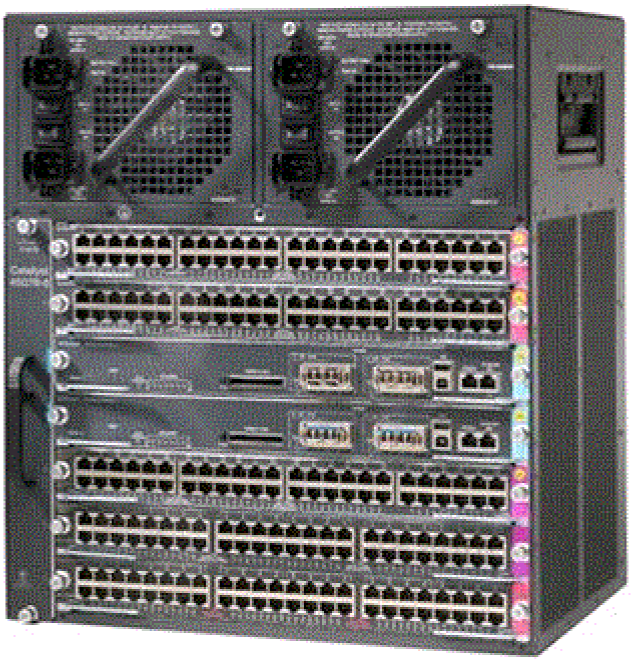

Figure 3: Catalyst 4507R+E/4507R-E Switch

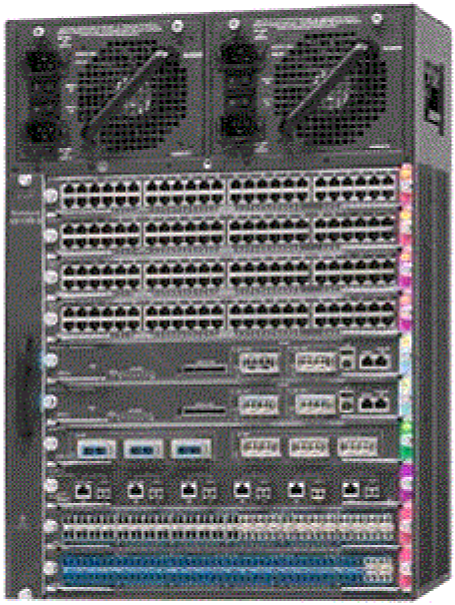

Figure 4: Catalyst 4510R+E/ 4510R-E Switch

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	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key management	2
8	Electromagnetic Interface/Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
Overall	**Overall module validation level**	**2**

Table 2: Module Validation Level

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. The module incorporates one or two supervisor cards and one or more line cards in a single configuration.

Cryptographic Module Ports and Interfaces

Each 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 logical interfaces and their mapping are described in the following tables:

Physical Interface	Logical Interface
Supervisor Card WS-X45-SUP7-E Management Port USB Ports Secure Digital Slot Console Port Supervisor card WS-X45-SUP7L-E Management Port USB Ports Secure Digital Slot Console Port Line Card WS-X4748-RJ45V+E 10/100/1000Mbps Line Card WS-X4712-SFP+E 10GE (SFP+) Line Card WS-X4640-CSFP-E SFP/CSFP Line Card WS-X4748-NGPOE+E 10/100/1000Mbps Line Card WS-X4748-RJ45-E 10/100/1000Mbps	**Data Input Interface**
Supervisor Card WS-X45-SUP7-E Management Port USB Ports Secure Digital Slot Console Port Supervisor card WS-X45-SUP7L-E Management Port USB Ports Secure Digital Slot Console Port Line Card WS-X4748-RJ45V+E 10/100/1000Mbps Line Card WS-X4712-SFP+E 10/100/1000Mbps	**Data Output Interface**

Physical Interface	Logical Interface
Line Card WS-X4640-CSFP-E 10/100/1000Mbps Line Card WS-X4748-NGPOE+E 10/100/1000Mbps Line Card WS-X4748-RJ45-E 10/100/1000Mbps	
Supervisor Card WS-X45-SUP7-E Management Port Console Port Supervisor card WS-X45-SUP7L-E Management Port Console Port	**Control Input Interface**
Supervisor Card WS-X45-SUP7-E Management Port USB Ports Secure Digital Slot Console Port Supervisor card WS-X45-SUP7L-E Management Port USB Ports Secure Digital Slot Console Port LEDs	**Status Output Interface**
Power Plug	**Power Interface**

Table 3: Physical To Logical Interfaces

Note: USB ports and Secure Digital slot on each Supervisor card are disabled by TELs in FIPS mode

Roles, Services, and Authentication

Authentication is identity-based. Each user is authenticated upon initial access to the module. There are two roles in the Switch that operators may assume: 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. The module supports RADIUS for authentication.

User Role

The role assumed by users obtaining general security services. From a logical view, user activity exists in the data-plane. Users access via network ports using the CTS (CTS uses 802.1X and EAP-FAST for authentication), IPSec, SSH, or TLS protocols.

CTS, IPSec and SSH can use password based credentials – in such a case the user credentials must be at least eight (8) characters long (max characters for the password is twenty-five (25)),, including at least one letter and at least one number character, in length (enforced procedurally). If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 832,000,000. In order to successfully guess the sequence in one minute would require the ability to make over

13,000,000 guesses per second, which far exceeds the operational capability of the console port. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

In addition, CTS, IPSec, SSH, and TLS can also use certificate credentials using 1024 bit RSA keys and SHA-1 – in such a case the security strength is 80 bits, so an attacker would have a 1 in 2^{80} chance of a successful authentication which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 1.8 x 10^{21} attempts per minute, which vastly exceeds the operational capabilities of the module to support.

CO Role

The role 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, if the password is validated against the CO's password in IOS memory, the user is allowed entry to the IOS executive program. A CO can assign permission to access the CO role to additional accounts, thereby creating additional COs.

CO passwords must be at least eight (8) characters long (max characters for the password is twenty-five (25)), including at least one letter and at least one number character, in length (enforced procedurally). If six (6) integers, one (1) special character and one (1) alphabet are used without repetition for an eight (8) digit PIN, the probability of randomly guessing the correct sequence is one (1) in 832,000,000. In order to successfully guess the sequence in one minute would require the ability to make over 13,000,000 guesses per second, which far exceeds the operational capability of the console port. Including the rest of the alphanumeric characters drastically decreases the odds of guessing the correct sequence.

Services

Role	Authentication Method	Services
User	CTS/IPsec/SSH/TLS Authentication	**Status Functions:** view state of interfaces, view state of connection, version of IOS currently running. **Network Functions:** connect to other network devices through outgoing telnet or PPP, and initiate diagnostic network services (for example, ping or mtrace). **Terminal Functions:** adjust the terminal session (that is, lock the terminal and adjust flow control). **Directory Services:** display directory of files kept in flash memory. **- Perform Self Tests:** occurs upon system startup.
Cryptographic	Console login	**Configure the switch:** define network interfaces and

Role	Authentication Method	Services
Officer		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. **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. **Status functions:** view the switch configuration, routing tables, and active sessions; view health, temperature, memory status, voltage, and packet statistics; review accounting logs, and view physical interface status. **Manage the switch:** log off users, shut down or reload the switch, manually back up switch configurations, view complete configurations, manager user rights, and restore switch configurations. **Set Encryption/Bypass** - Place module into Encryption or Bypass state. - **Perform Self-Tests** - Perform the FIPS 140 start-up tests on demand.
Unauthenticated	N/A	Show status (viewing LEDs), passing traffic through the device and power-cycling the device.

Table 4: Module Roles/Service

Cryptographic Key/CSP Management

The module securely administers both cryptographic keys and other critical security parameters such as passwords. The tamper evidence seals provide physical protection for all keys. All keys are also protected by the password-protection on the CO role login, and can be zeroized by the CO. All zeroization consists of overwriting the memory that stored the key. 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.

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

ID	Algorithm/ Size/Mode	Size	Description	Origin	Storage	Zeroization Method
RNG Seed	ANSI X9.31 Appendix A.2.4 Using the 2-Key Triple-DES Algorithm	64-bits	This is the seed for X9.31 RNG.	Generated by the module	DRAM (plaintext)	Power cycle the device
RNG Seed Key	ANSI X9.31 Appendix A.2.4 Using the 2-Key Triple-DES Algorithm	128-bits	This is the seed key for X9.31 RNG.	Generated by the module	DRAM (plaintext)	power cycle the device
DRBG V	SP 800-90 CTR_DRBG	128-bits	Internal V value used as part of SP 800-90 CTR_DRBG	Generated by entropy source via the CTR_DRBG derivation function.	DRAM (plaintext)	power cycle the device
DRBG Key	SP 800-90 CTR_DRBG	256-bits	Internal Key value used as part of SP 800-90 CTR_DRBG	Generated from entropy source via CTR_DRBG derivation function	DRAM (plaintext)	power cycle the device
Diffie-Hellman private exponent	Diffe-Hellman	1024-2048 bits	The private exponent used in Diffie-Hellman (DH) exchange.	Generated using ANSI X9.31 RNG	DRAM (plaintext)	Automatically after shared secret generated
Diffie-Hellman shared secret	Diffe-Hellman	256 bits	Shared secret generated by the Diffie-Hellman Key exchange	Shared secret derived by the Diffie-Hellman Key exchange	DRAM (plaintext)	Automatically when session expires

ID	Algorithm/ Size/Mode	Size	Description	Origin	Storage	Zeroization Method
SAP Pairwise Master Key (PMK)	Shared Secret	64 byte key used to derive PTK which is used to generate CTS session MAC and Encryption keys. Only the first 32 bytes are used by CTS.	64 byte key used to derive PTK which is used to generate CTS session MAC and Encryption keys. Only the first 32 bytes are used by CTS.	Generated by ACS server and sent to Authenticator encrypted by RADIUS AES KEK WRAP KEY	DRAM (plaintext)	Unconfigure the PMK in CTS manual mode or unconfigure cts dot1x in CTS dot1x mode.
SAP Pairwise Transient Key (PTK)	Shared Secret	256-bit	Concatenation of KCK and KEK.	Concatenation of KCK and KEK.	DRAM (plaintext)	Automatically when session expires
SAP Key Encryption Key (KEK)	AES	128-bit	Used to encrypt SAP payloads during SAP protocol implementations.	Derived by SAP	DRAM (plaintext)	Automatically when session expires
SAP Key Confirmation Key (KCK)	HMAC-SHA-1	160-bit	Used to protect SAP payloads integrity during SAP protocol implementations.	Derived by SAP	DRAM (plaintext)	Automatically when session expires
802.1ae Session Keys	AES-GCM	128-bit	Used for bulk encryption of data	Derived by SAP	XgStub2 ASIC (plaintext)	Automatically when session expires
CTS password	Shared Secret	Up to 256 bytes	This is CTS credential. Used for CTS device to authenticate itself. The maximum size is 256 bytes.	CO configured	NVRAM (plaintext)	"#clear cts credentials"
CTS PAC secret	Shared Secret	256-bits	CTS PAC is a Protected Access Credential that is mutually and uniquely shared between the peer and ACS. It is used to secure EAP-FAST tunnel.	Generated and sent by ACS to the CTS device	NVRAM (plaintext)	"#clear cts pacs"
RADIUS AES KEK WRAP KEY	AES key wrap KEK	256-bits	Used to protect SAP Pairwise Master Key (PMK)	CO configured	DRAM (plaintext)	Resetting or rebooting the module
RADIUS AES KEK WRAP MACK	AES key wrap MACK	160-bits	Used to protect SAP Pairwise Master Key (PMK)	CO configured	DRAM (plaintext)	Resetting or rebooting the module

ID	Algorithm/ Size/Mode	Size	Description	Origin	Storage	Zeroization Method
Skeyid	HMAC-SHA-1	160-bits	Used to derive skey_d.	Value derived from the shared secret within IKE exchange. Zeroized when IKE session is terminated.	DRAM (plaintext)	Automatically after IKE session terminated.
skeyid_d	HMAC-SHA-1	160-bits	Derived as part of the IKE process.	The IKE key derivation key for non ISAKMP security associations.	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session encrypt key	Triple-DES/AES	Triple-DES (168-bits)/AES (128/192/256-bits)	The IKE session encrypt key.	Value derived from the shared secret within IKE exchange	DRAM (plaintext)	Automatically after IKE session terminated.
IKE session authentication key	HMAC-SHA-1	160-bits	The IKE session authentication key.	Value derived from the shared secret within IKE exchange	DRAM (plaintext)	Automatically after IKE session terminated.
ISAKMP preshared	Shared Secret	At least eight characters	The key used to generate IKE skeyid during preshared-key authentication.. This key can have two forms based on whether the key is related to the hostname or the IP address.	Configured by CO	NVRAM (plaintext)	“# no crypto isakmp key”
IKE RSA Authentication private Key	RSA	1024 - 2048 bits	RSA private key for IKE authentication.	Generated by using FIPS approved DRBG	NVRAM (plaintext)	“# crypto key zeroize rsa"
IPSec encryption key	Triple-DES/AES	Triple-DES (168-bits)/AES (128/192/256 bits AES keys)	The IPSec encryption key. Zeroized when IPSec session is terminated.	Derived using the IKE key derivation function	DRAM (plaintext)	Automatically when IPSec session terminated.
IPSec authentication key	HMAC-SHA-1	160-bits	The IPSec authentication key. The zeroization is the same as above.	Derived using the IKE key derivation function	DRAM (plaintext)	Automatically when IPSec session terminated.
RSA private key (SSH)	RSA	1024 - 2048 bits	Private key used in SSH protocol	Generated by using FIPS approved DRBG	NVRAM (plaintext)	“#crypto key zeroize rsa”

ID	Algorithm/ Size/Mode	Size	Description	Origin	Storage	Zeroization Method
SSH session key	TDES / AES	128, 256 bits (AES) 168 bits (TDES)	This is the SSH session key. It is used to encrypt all SSH data traffics traversing between the SSH client and SSH server.	Derived as part of SSH session set-up	DRAM (plaintext)	Zeroized when SSH session is terminated
SSH session authentication key	HMAC-SHA-1	160-bits	This key is used to perform the authentication between the SSH client and SSH server.	Derived as part of SSH session set-up	DRAM (plaintext)	Zeroized when SSH session is terminated
RSA private key (TLS)	RSA	1024 - 2048 bits	Identity certificates for module itself and also used in TLS negotiations. This CSP is used for both SSL VPN and SIP Gateway Signaling Over TLS Transport.	Generated by using FIPS approved DRBG	NVRAM (plaintext)	"#crypto key zeroize rsa"
TLS pre-master secret	Shared Secret	384-bits	Shared secret created using asymmetric cryptography from which new HTTPS session keys can be created.	Created as part of TLS session establishment	DRAM (plaintext)	Zeroized when TLS session is terminated
TLS Session Key	Triple-DES/AES	Triple-DES (168-bits)/AES (128/192/256-bits)	Derived using the TLS protocol.	Derived as part of TLS session establishment	DRAM (plaintext)	Zeroized when TLS session is terminated
TLS Session Authentication Key	HMAC-SHA-1	160-bits	Derived using the TLS protocol.	Derived as part of TLS session establishment	DRAM (plaintext)	Zeroized when TLS session is terminated
User password	Shared Secret	8-25 characters long, including at least one letter and at least one number character	Password of the user role	CO configured	NVRAM (plaintext)	Set new password
Enable password	Shared Secret	8-25 characters long	CO password	CO configured	NVRAM (plaintext)	Set new password

ID	Algorithm/ Size/Mode	Size	Description	Origin	Storage	Zeroization Method
Enable secret	Shared Secret	8-25 characters long, including at least one letter and at least one number character	Obfuscated password of the CO role.	CO configured	NVRAM (plaintext)	Set new password
RADIUS secret	Shared Secret	At least eight (8) characters long, including at least one letter and at least one number character	The RADIUS Shared Secret	CO configured	NVRAM (plaintext)	# no radius-server key"
TACACS+ secret	Shared Secret	At least eight (8) characters long, including at least one letter and at least one number character	The TACACS+ shared secret	CO configured	NVRAM (plaintext)	# no tacacs-server key"

Table 5: CSP Table

The services accessing the CSPs, the type of access and which role accesses the CSPs are listed below.

Role	Service	Critical Security Parameters
User Role	Network Functions	RNG Seed, RNG Seed, RNG Seed Key Diffie-Hellman private exponent, Diffie-Hellman shared secret, 802.11x-REV PMK, CTS Password, CTS PAC secret, Secure RADIUS KEK, Secure RADIUS MACK, Skeyid, skeyid_d, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE RSA Authentication private Key, IPSec encryption key, IPSec authentication key (R), User password (W)
Crypto-Officer Role	Configure the Switch	802.11x-REV PMK, Secure RADIUS KEK, Secure RADIUS MACK, CTS Password, Enable Password, Skeyid, skeyid_d, IKE session encrypt key, IKE session authentication key, ISAKMP preshared, IKE RSA Authentication private Key, IPSec encryption key, IPSec authentication key (R/W/D)

Table 6: Role CSP Access

Cryptographic Algorithms

Approved Cryptographic Algorithms

The Cisco Switches support 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 Switches for use in the FIPS mode of operation.

Algorithm	Implementation	CAVP Certificate
AES	IOS-XE Firmware	#1977
	Hardware	#2057
Triple-DES	IOS-XE Firmware	#1282
SHS	IOS-XE Firmware	#1730
	IOS-XE Image Signing Implementations	#1731
HMAC	IOS-XE Firmware	#1190
RSA	IOS-XE Firmware	#1023
	IOS-XE Image Signing Implementations	#1024
ANSI X9.31 RNG	IOS-XE Firmware	#1072
SP 800-90A CTR_DRBG	IOS-XE Firmware	#179

Table 7: FIPS-Approved Algorithms for use in FIPS Mode

Non-Approved Algorithms

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

- NDRNG
- MD4
- MD5

In addition, the modules support the following key establishment/derivation schemes:

- Diffie-Hellman (key establishment methodology provides between 80 and 112 bits of encryption strength)
- RSA key transport (key establishment methodology provides between 80 and 112 bits of encryption strength)
- AES (Cert. #1977, key wrapping; key establishment methodology provides 256 bits of encryption strength)

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. The modules implement the following power-on self-tests:

- IOS-XE Firmware Implementation Known Answer Tests:
  - Firmware Integrity Test
  - AES KAT
  - AES-CMAC KAT
  - CTR_DRBG KAT
  - HMAC SHA-1 KAT
  - X9.31 RNG KAT
  - FIPS 186-2 RSA KAT
  - SHA-1 KAT
  - SHA-512 KAT
  - Triple-DES KAT
- IOS-XE Image Signing Implementation Known Answer Tests:
  - FIPS 186-3 RSA KAT
  - SHA-512 KAT
- Cat4k ASIC Algorithm Implementation (Hardware)Known Answer Tests:
  - AES-GCM KAT

The modules perform 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 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:

- IOS-XE Firmware Implementation Conditional Self-Tests
  - Continuous Random Number Generator test for ANSI X9.31 RNG
  - Continuous Random Number Generator test for SP800-90A CTR_DRBG
  - Continuous Random Number Generator test for the non-approved RNGs
  - Bypass Test (IPSec Bypass Test)
  - Bypass Test (TrustSec Bypass Test)
  - FIPS 186-2 RSA Pairwise Consistency Test
  - Firmware Load Test
- IOS-XE Image Signing Implementation Conditional Self-Tests
  - FIPS 186-3 RSA Pairwise Consistency Test

Physical Security

This module is a multi-chip standalone cryptographic module.

The FIPS 140-2 level 2 physical security requirements for the modules are met by the use of opacity shields covering the front panels of modules to provide the required opacity and tamper evident seals to provide the required tamper evidence. The following sections illustrate the physical security provided by the module.

Module Opacity

To install an opacity shield on the Catalyst 4500 series switches, follow these steps:

1. The opacity shield is designed to be installed on a Catalyst 4500 series switch chassis that is already rack-mounted. If your Catalyst 4500 series switch chassis is not rack-mounted, install the chassis in the rack using the procedures contained in the Catalyst 4500 Series Switches Installation Guide. If your Catalyst 4500 series switch chassis is already rack-mounted, proceed to step 2.

2. Open the FIPS kit packagings. The kits contain the following items:

   - WS-C4503-FIPS-KIT=: A packaged opacity shield assembly with installation hardware for the Catalyst 4503-E switch chassis.

   - WS-C4506-FIPS-KIT=: A packaged opacity shield assembly with installation hardware for the Catalyst 4506-E switch chassis.

   - WS-C4507-FIPS-KIT=: A packaged opacity shield assembly with installation hardware for the Catalyst 4507R+E/4507R-E switch chassis.

   - WS-C4510-FIPS-KIT=: A packaged opacity shield assembly with installation hardware for the Catalyst 4510R+E/4510R-E switch chassis.

   - All Kits: An envelope with 60 FIPS tamper evidence labels.

   - All Kits: An envelope containing a disposable ESD wrist strap.

3. Select the appropriate opacity shield kit for your system. Set the other opacity shield kit aside.

4. Open the protective packaging and remove the opacity shield and the two bags of installation hardware. The bag with the part number 69-1497 contains the installation hardware for -E chassis. Select the bag of installation hardware appropriate for your installation. Set the second bag of fasteners aside; you will not need them for this installation.

5. Open the bag of installation hardware (Bag with part number 69-1497) and remove the following: Two M4 thumbscrews, four M4 snap rivet fastener sleeves, and four M4 snap rivet pins.

6. Ensure that any open slots are covered using the provided slot cover (C4K-SLOT-CVR-E).

Note: Extra snap fasteners are included in the bags of installation hardware in case of loss or damage.

Note: Installation hardware from one bag is not interchangeable with the installation hardware from the second bag.

The following figures illustrate the installation of the opacity shields for each platform.

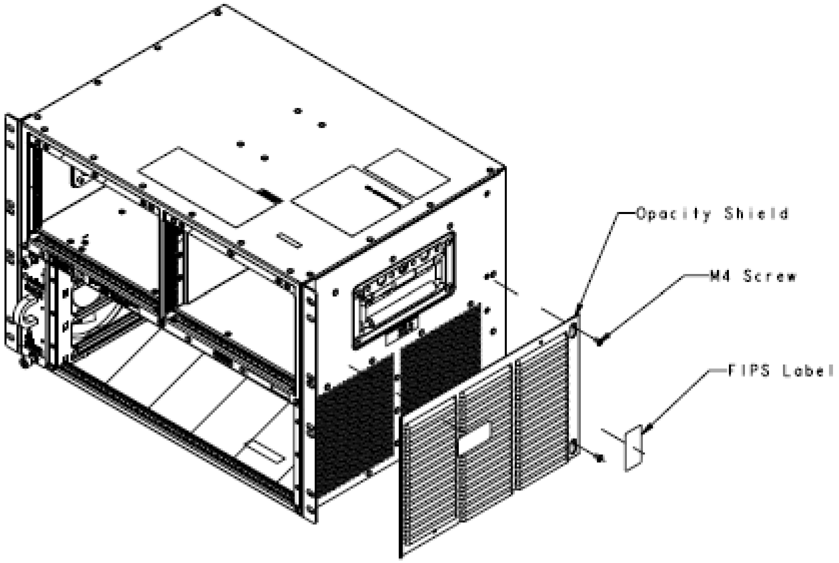

Figure 5: Catalyst 4503-E Opacity Shield Installation

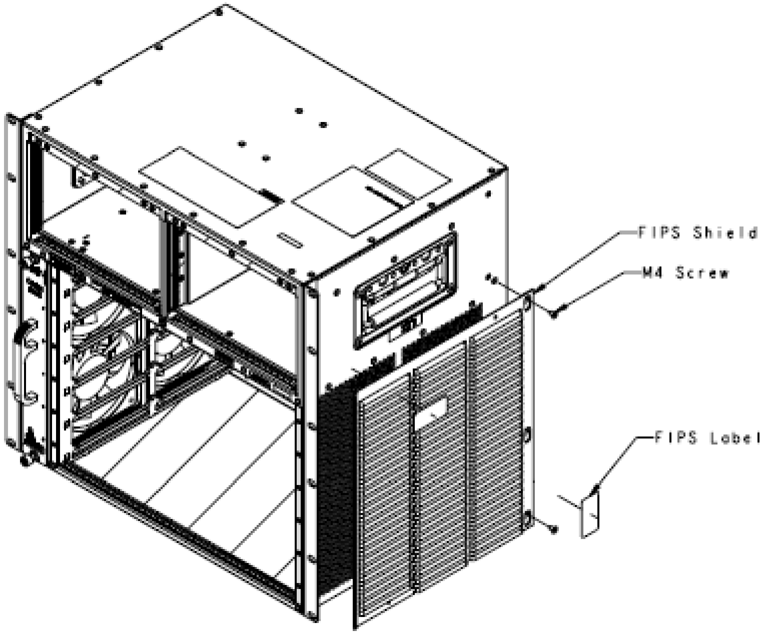

Figure 6: Catalyst 4506-E Opacity Shield Installation

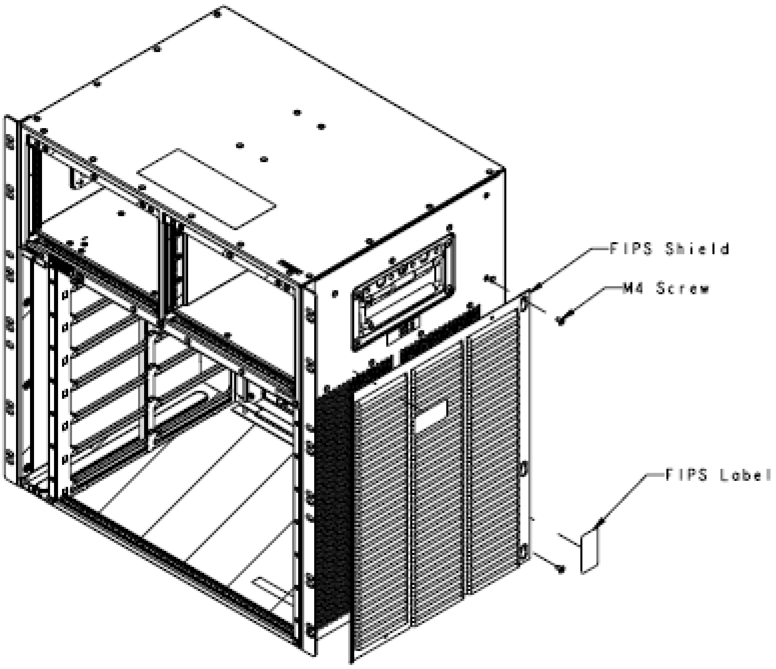

Figure 7: Catalyst 4507R+E/ 4507R-E Opacity Shield Installation

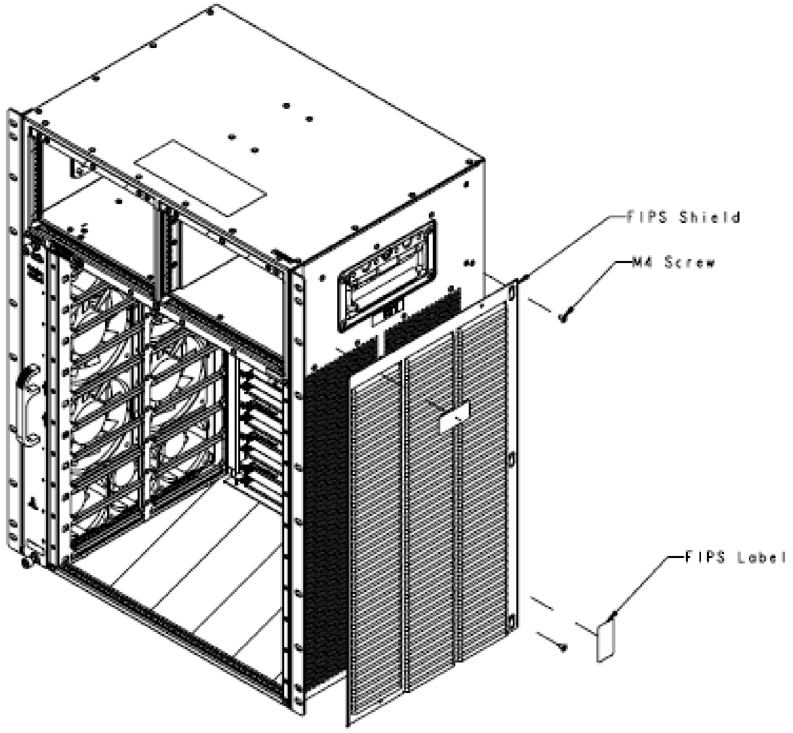

Figure 8: Catalyst 4510R+E/ 4510R-E Opacity Shield Installation

Tamper Evidence

The module is validated when tamper evident labels and security devices are installed on the initially built configuration as indicated. Any changes, modifications or repairs performed after the initially built configuration that requires the removal of any TEL will invalidate the module.

The total number of tamper evident labels required for the configuration is dependent on the cards installed in the chasis.

Once the module has been configured to meet overall FIPS 140-2 Level 2 requirements, the module cannot be accessed without signs of tampering. The CO shall inspect for signs of tampering periodically. Any extra TELs must remain in the CO control and must be securely stored in a monitored location.

If the CO must remove or change TELs (tamper-evidence labels) for any reason, the CO must examine the location from which the TEL was removed and ensure that no residual debris is still remaining on the chassis or card. If residual debris remains, the CO must remove the debris using a damp cloth.

To seal the system, CO should apply TELs as depicted in the figures below. The following table identifies the number of TELs required for each chassis.

Number of Slots	Model	TELs
Three (3)	4503-E	Eight (8)
Six (6)	4506-E	Eleven (11)
Seven (7)	4507R-E 4507R+E	Fifteen (15)
Ten (10)	4510R-E 4510R+E	Eighteen (18)

Table 8: Tamper Evident Labels

Please notice that the numbers of TELs listed in table 8 are applied to all possible hardware configurations specified in Table 1in this document.

The following figures illustrate the installation of the TELs for each platform.

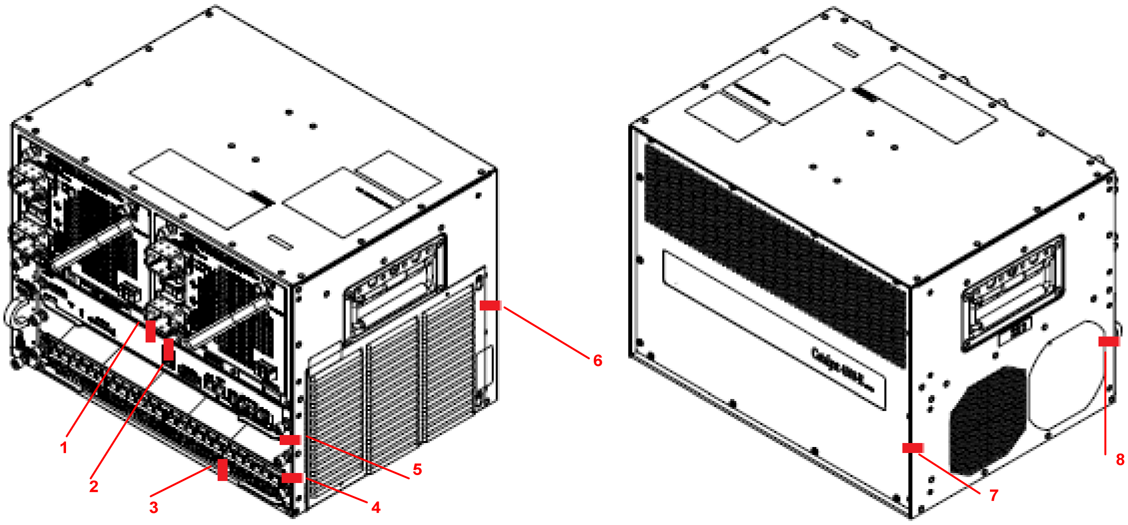

Figure 9: Catalyst 4503-E TEL Installation

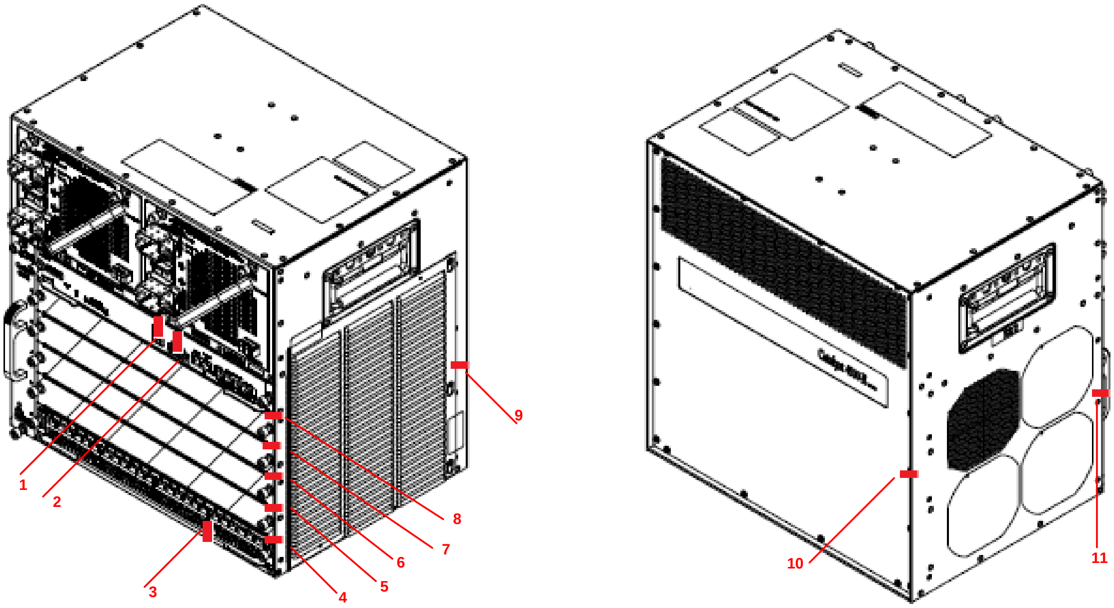

Figure 10: Catalyst 4506-E TEL Installation

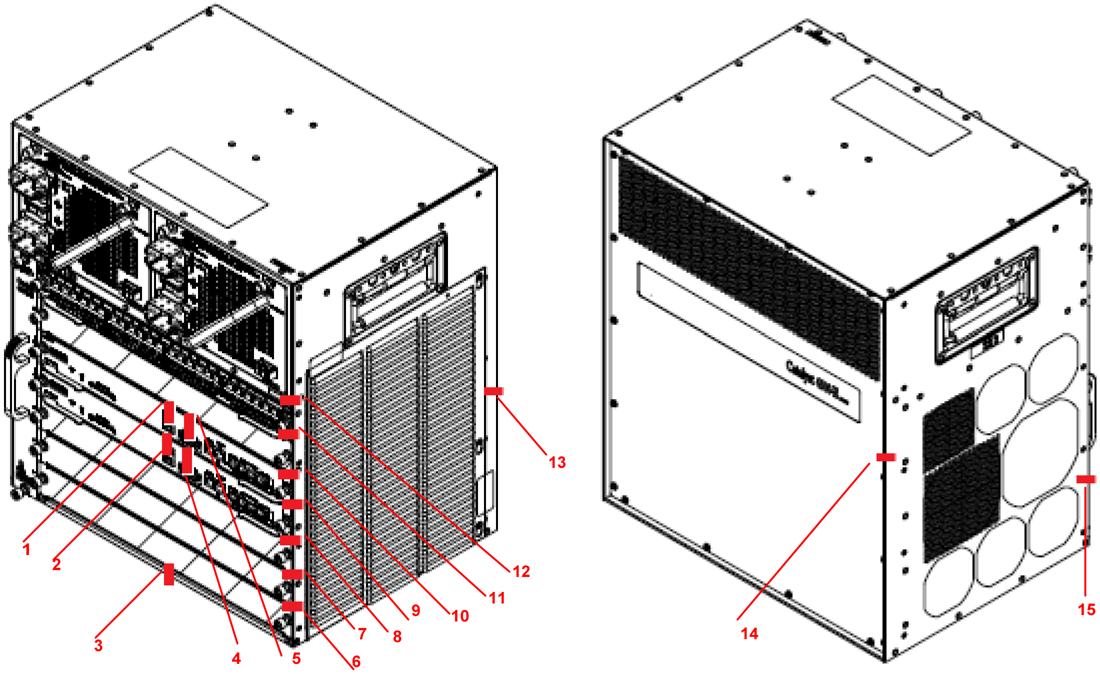

Figure 11: Catalyst 4507R+E/ 4507R-E TEL Installation

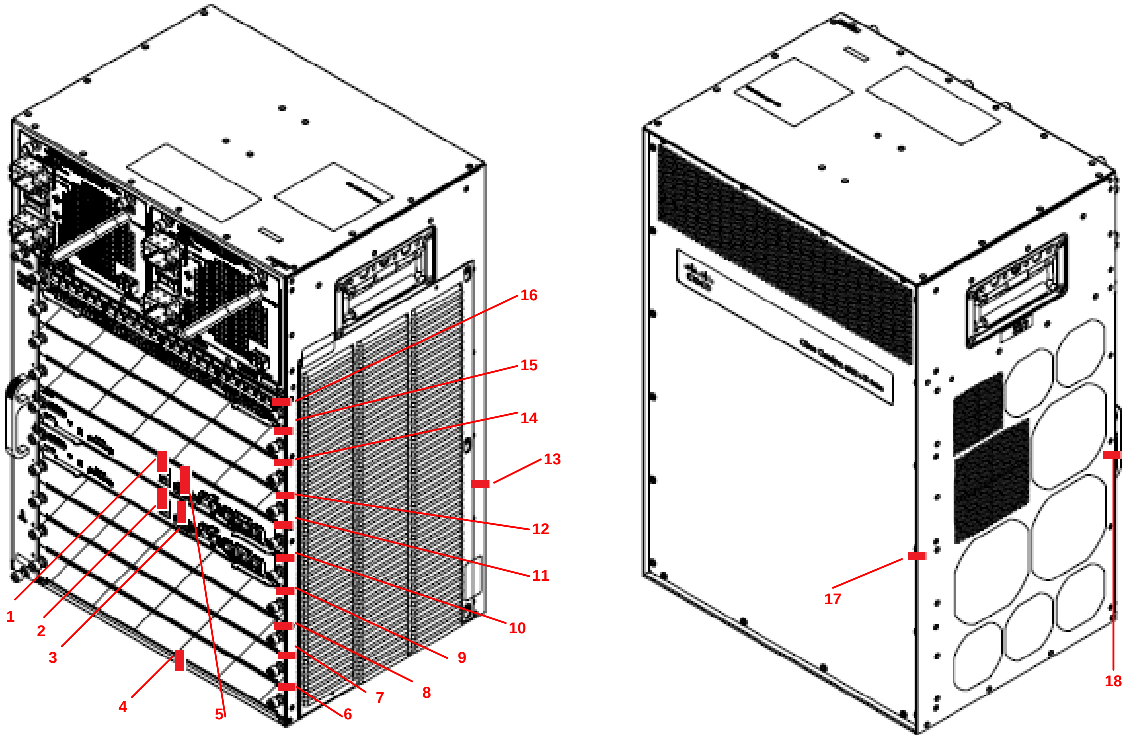

Figure 12: Catalyst 4510R+E/ 4510R-E TEL Installation

Secure Operation

The Switches meet all the overall Level 2 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.

Initial Setup

1. The CO must apply opacity shield and tamper evidence labels as described above.

System Initialization and Configuration

1. 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:

   ```
   enable secret [PASSWORD]
   ```

2. The CO must always assign passwords (8-25 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:

   ```
   line con 0
   password [PASSWORD]
   login local
   ```

3. The CO enables FIPS mode using the following command:

   ```
   Switch(config)# fips
   ```

4. The CO may configure the module to use RADIUS or TACACS+ for authentication. If the module is configured to use RADIUS, the Crypto-Officer must define RADIUS or shared secret keys that are at least 8 characters long, including at least one letter and at least one number.

5. The CO shall only assign users to a privilege level 1 (the default).

6. The CO shall not assign a command to any privilege level other than its default.

Remote Access

1. SSH access to the module is allowed in FIPS approved mode of operation, using SSH v2 and a FIPS approved algorithm.

2. HTTPS/TLS access to the module is allowed in FIPS approved mode of operation, using SSLv3.1/TLSv1.0 and the associated FIPS approved algorithms.

Identifying Switch Operation in an Approved Mode

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

1. Verify that the tamper evidence labels and FIPS opacity shields have been properly placed on the module based on the instructions specified in the “Physical Security” and “Secure Operation” sections of this document.
2. Verify that the length of User and Crypto Officer passwords and all shared secrets are at least eight (8) characters long, include at least one letter, and include at least one number character, as specified in the “Secure Operation” section of this document.
3. Verified that the output of "The FIPS mode is on" was shown on the Command Line Interface after login Crypto Officer role.

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:

- 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.

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.

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

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/

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-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.

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.

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://www.cisco.com/en/US/products/products_psirt_rss_feed.html

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 a 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.

- 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.

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.

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.

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 55USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

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.

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/

- *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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

- or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *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

Definition List

AES – Advanced Encryption Standard

ACS – Access Control Server

CMVP – Cryptographic Module Validation Program

CSEC – Communications Security Establishment Canada

CSP – Critical Security Parameter

CSFP – Compact Small Form-Factor Pluggable Transceiver

CTS – Cisco proprietary TrustSec protocol

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

NIST – National Institute of Standards and Technology

NVRAM – Non-Volatile Random Access Memory

RAM – Random Access Memory

RNG – Random Number Generator

SHA – Secure Hash Algorithm

SFP - Small Form-Factor Pluggable Transceiver

SFP+ - Enhanced Small Form-Factor Pluggable

Triple-DES – Triple Data Encryption Standard