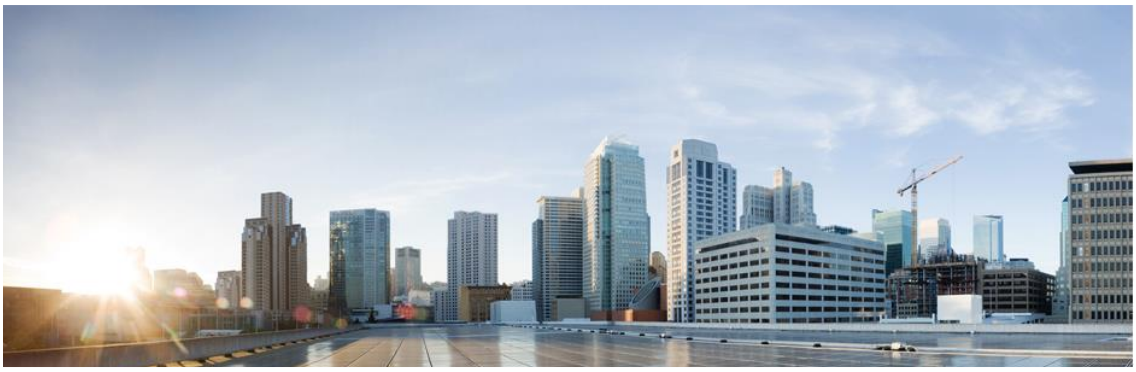

Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6

Common Criteria Configuration Guide

Version: 0.7
Date: 31 May 2022

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Table of Contents

List of Tables

DOCUMENT INTRODUCTION

Prepared By:
Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6, hereafter referred to as the Catalyst 9300/9300L/9500 Series Switches, Cat 9K Switches, or the TOE. This Configuration Guide addresses the administration of the TOE software and hardware and describes how to install, configure, and maintain the TOE in the Common Criteria evaluated configuration. In this document, administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged administrators, and privileged administrators.

1. Introduction

This Configuration Guide documents the administration of the Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 certified under Common Criteria (CC). The TOE may be referenced below as the Cat 9K Switches, TOE, or switch.

1.1 Audience

This document is written for administrators configuring the TOE. This document assumes familiarity with basic networking concepts and terminology, understanding of network protocols, and working knowledge of the internal network topology. This document assumes that the administrator is a trusted individual, trained to use IOS software and the various operating systems run within the network. The administrator configuring the TOE must review this Configuration Guide and the documents identified in Table 1 below.

In this document, users of the TOE are referred to as "users" or "administrators". A user with privilege level 15, access to all TOE commands, is referred to as an Authorized Administrator or privileged administrator.

1.2 Purpose

This document is the Configuration Guide for the CC evaluation, fulfilling the AGD security assurance requirement. The purpose of this document is to highlight the administrator functions and interfaces necessary to configure and maintain the TOE in the evaluated configuration. The evaluated configuration is the configuration of the TOE that satisfies the requirements as defined in the *Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Common Criteria Security Target* (ST). This document covers all the security functional requirements specified in the ST. This document does not mandate configuration settings for features of the TOE that are outside the evaluation scope, such as information flow and access control policies.

This document is not meant to be a comprehensive guide for configuring the TOE. This is a road map of the steps necessary to install, configure, and manage the TOE. This Configuration Guide, used in conjunction with the documents in Table 1 below, will allow the administrator to place and operate the TOE in the evaluated configuration. It is recommended that all instructions in this document and any references herein be read before performing any actions on the TOE.

1.3 Document References

This Configuration Guide refers to several Cisco documents. The documents used are shown in Table 1 below Throughout this document, the guides will be referred to by the "#", such as **[1]**.

Table 1 Reference Documents

Reference number	Document Name	Link
[1]	Release Notes for Cisco Catalyst 9300 Series Switches, Cisco IOS-XE Bengaluru 17.6.x	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/release_notes/ol-17-6-9300.html?dtid=osscdc000283
[2]	Cisco Catalyst 9300 Switches Hardware Installation Guide)	https://www.cisco.com/c/en/us/td/docs/switches/lan/cata

Reference number	Document Name	Link
		lyst9300/hardware/install/b_c9300_hig.html?dtid=osscdc000283
[3]	Software Configuration Guide, Cisco IOS-XE Bengaluru 17.6.x (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/b-176-9300-cg.html?dtid=osscdc000283
[4]	Security Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/sec/b_176_sec_9300_cg.html?dtid=osscdc000283
[5]	Network Management Configuration Guide, Cisco IOS-XE Bengaluru 17.6 (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/nmgmt/b_176_nmgmt_9300_cg/configuring_cisco___plug_and_play.html
[6]	Cisco IOS Security Command Reference: A to C D to L M to R S to Z	A – C: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html D – L: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book.htmlhttps://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-

Reference number	Document Name	Link
		cr-book.htmlhttps://www.cisco.com/c/en/us/td/enabledocs/ios-xml/ios/security/d1/sec-d1-cr-book.html M - R: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/m1/sec-m1-cr-book.html S – Z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book.html
	Cisco IOS Master Command List, All Releases	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mcl/allreleasemcl/all-book.html
	Command Reference, Cisco IOS-XE Bengaluru 17.6 (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/command_reference/b_176_9300_cr.html?dtid=osscdc000283
[7]	IP Routing Configuration Guide, Cisco IOS-XE Bengaluru 17.6 (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/rtng/b_176_rtng_9300_cg.html?dtid=osscdc000283
[8]	Internet Key Exchange for IPsec VPNs Configuration Guide, Cisco IOS-XE Amsterdam 17.x	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_ikevpn/conf

Reference number	Document Name	Link
		iguration/xe-17/sec-ike-for-ipsec-vpns-xe-17-book.html?dtid=osscdc000283
[9]	Cisco IOS Configuration Fundamentals Command Reference	https://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html
[10]	Configuration Fundamentals Configuration Guide, Cisco IOS-XE 17.6	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/fundamentals/configuration/xe-17-6/fundamentals-xe-17-6-book.html
[11]	Security Configuration Guide, Cisco IOS-XE Bengaluru 17.6.x (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/sec/b_176_sec_9300_cg.htmlhttps://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/sec/b_176_sec_9300_cg.html
[12]	System Message Guide for Cisco IOS-XE Bengaluru 17.6.x	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/17_xe/syslogs/17-6-x/b-system-message-guide-17-6-x.html
[13]	Public Key Infrastructure Configuration Guide, Cisco IOS-XE 17	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_pki/configuration/xe-17/sec-pki-xe-17-book.html?dtid=osscdc000283
[14]	Loading and Managing System Images Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sys-image-

Reference number	Document Name	Link
		mgmt/configuration/xe-16/sysimgmgmt-xe-16-book.html
[15]	Software Configuration Guide, Cisco IOS-XE Bengaluru 17.6.x (Catalyst 9300 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-6/configuration_guide/b-176-9300-cg.html?dtid=osscdc000283
[16]	Embedded Event Manager Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/eem/configuration/xe-16/eem-xe-16-book/eem-overview.html
[17]	Security Configuration Guide, Cisco IOS-XE Bengaluru 17.6.x (Catalyst 9500 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-6/configuration_guide/sec/b_176_sec_9500_cg.html?dtid=osscdc000283
[18]	Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Bengaluru 17.6.x	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-6/release_notes/ol-17-6-9500.html?dtid=osscdc000283
[19]	Cisco Catalyst 9500 Series Switches Hardware Installation Guide	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/hardware/install/b_catalyst_9500_hig.html?dtid=osscdc000283
[20]	Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9500 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-6/configuration_guide/b-176-9500-cg.html?dtid=osscdc000283

Reference number	Document Name	Link
[21]	Network Management Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9500 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-6/configuration_guide/nmgmt/b_176_nmgmt_9500_cg.html?dtid=osscdc000283
[22]	Command Reference, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9500 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-6/command_reference/b_176_9500_cr.html?dtid=osscdc000283
[23]	IP Routing Configuration Guide, Cisco IOS XE Bengaluru 17.6.x (Catalyst 9500 Switches)	https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/17-6/configuration_guide/rtng/b_176_rtng_9500_cg.html?dtid=osscdc000283

1.4 Supported Hardware and Software

Only the hardware and software listed in this Configuration Guide may be used in the evaluated configuration. Using hardware not specified invalidates the secure configuration. Likewise, using a software version, other than the evaluated software listed below, will invalidate the secure configuration.

1.4.1 Supported Configurations

The TOE is comprised of both software and hardware. The hardware is comprised of the following: Catalyst 9300/9300L/9500 Series Switches. The software is comprised of the Universal Cisco Internet Operating System (IOS) software image Release IOS-XE 17.6.

The Catalyst 9300/9300L/9500 Series Switches that comprises the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions, such as throughput and storage. Therefore, security equivalency of the switches between hardware models is supported.

The Catalyst 9300/9300L/9500 Series Switches primary features include the following:

- Central processor that supports all system operations
- Dynamic memory, used by the central processor for all system operation
- Central Processing Unit (CPU) complex with 8-GigaBytes (GB) memory, 16-GB of flash, and an external Universal Serial Bus (USB) 3.0 Solid State Drive (SSD) pluggable storage slot (delivering 120-GB of storage with an optional SSD drive)
- Serial Advanced Technology Attachment (SATA) SSD local storage

- Flash memory Electrically Erasable Programmable Read-Only Memory (EEPROM), used to store the Cisco IOS-XE image (binary program)
- Non-volatile Read Only Memory (ROM) is used to store the bootstrap program and power-on diagnostic programs
- Non-volatile Random-Access Memory (NVRAM) is used to store switch configuration parameters that are used to initialize the system at start-up.
- Physical network interfaces (minimally two) (e.g., Registered Jack (RJ-45) serial and standard 10/100/1000 Ethernet ports). The number of network interface ports varies by model
- Dedicated management port on the switch, RJ-45 console port, and a USB mini-Type B console connection
- Resiliency with Field Replaceable Units (FRU) and redundant power supply, fans, and modular uplinks

Cisco IOS-XE is a Cisco-developed, highly configurable proprietary operating system that provides efficient and effective routing and switching. Although IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in this document.

1.5 Operational Environment

Table 2 below identifies the hardware and software components in the TOE operational environment. Each component is identified as being required or optional based on claims made in the ST.

Table 2 Required non-TOE Hardware/ Software/ Firmware

Component	Required	Usage/Purpose Description for TOE performance
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE transmits syslog messages over a secure Internet Protocol security (IPsec) trusted channel either directly or connected to a TOE Peer that also supports a secure IPsec trusted channel
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Management Workstation with Secure Shell v2 (SSHv2) client	Yes	This includes any IT Environment Management workstation that is used by the TOE administrator to support TOE administration using SSHv2 protected channels. Any SSH client that supports SSHv2 may be used.
Remote Authentication Dial-In User Service (RADIUS) Authentication, Authorization, and Accounting (AAA) Server	Yes	This includes any IT environment RADIUS AAA server that provides authentication services to TOE administrators over a secure IPsec trusted channel either directly or connected to a TOE Peer that also supports a secure IPsec trusted channel.
Media Access Control security (MACsec) Peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications.
Certification Authority (CA)	Yes	This includes any IT Environment CA on the TOE network. The CA can be used to provide the TOE with a valid certificate during certificate enrolment as well as validating a certificate.
TOE Peer	Optional	The TOE Peer is required if the remote syslog server and/or the remote authentication server is attached to the TOE Peer and used by the TOE If the remote syslog server and/or the remote authentication server is directly connected to the TOE for the TOE's use, then the TOE Peer is not required.

1.6 Excluded Functionality

Functionality listed in Table 3 below is excluded from the evaluated configuration. The exclusion of this functionality does not affect compliance to the collaborative Protection Profile for Network Devices, version 2.2e (NDcPP v2.2e) and the NDcPP Extended Package (EP) MACsec Ethernet Encryption (MACsec EP), version 1.2 (MACsec EP v1.2).

Table 3 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	Operational mode that supports non-FIPS allowed functions and algorithms.

2. Secure Acceptance of the TOE

The following steps must be performed to confirm that the correct TOE is received:

1 Before unpacking the TOE, inspect the physical packaging the equipment was delivered in. Verify that the external cardboard packing is printed with the Cisco Systems, Inc. logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems, Inc. or an authorized Cisco distributor/partner).

2 Verify that the packaging tape has not been opened and resealed. If the package appears to have been resealed, contact the supplier of the equipment (Cisco Systems, Inc. or an authorized Cisco distributor/partner).

3 Verify that a white tamper-resistant, tamper-evident Cisco Systems, Inc. bar coded label is applied to the external cardboard box. This label provides information regarding contents of the box, including product number and serial number. If the label is not applied, contact the supplier of the equipment (Cisco Systems, Inc. or an authorized Cisco distributor/partner).

4 Verify the serial number of the TOE provided on the separately mailed invoice matches the serial number on the shipping documentation and the white label affixed to the outside of the box. If the serial numbers do not match, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

5 Verify that the box was shipped from the expected equipment supplier (Cisco Systems, Inc. or an authorized Cisco distributor/partner). This can be done by verifying with the supplier that they shipped the box with the courier company that delivered the box and that the consignment number for the shipment, matches that used on the delivery. Verification of the courier should be performed by a mechanism that does not involve the equipment delivery, such as verification of the phone/FAX number or other online tracking service.

6 Once the TOE is unpacked, inspect the unit. Verify that the serial number displayed on the unit matches the serial number on the shipping documentation and invoice. If the serial numbers do not match, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

7 Download the evaluated version of the CC software image from Cisco.com.

NOTE: The TOE ships with a software images installed; however, this may not be the evaluated version so updating the software is recommended.

8 Verify that the software image has not been tampered with. Use a hash generation utility to compute a SHA-512 hash. Compare the generated hash with the SHA_512 has associated with the downloaded file, see Table 4 below for this hash value. If the SHA-512 hashes do not match, contact Cisco Technical Assistance Center (TAC), https://www.cisco.com/c/en/us/support/index.html. If the hash values match, proceed with the installation and configuration of the TOE, section 3 below.

Table 4: Software Image Hash Value

Software Version	Image Name / Description	Checksum Hash
17.6	cat9k_liosxe.17.6.1.SPA.bin	ca8282223835e06065e2ca3c0c300ad52665ae783ac7773535b831fe9463cb1264f14bdcb18a2e35526cde38241abd805b0ccea28bb4a1b05de518078ce50e3c

9 Power-on the TOE **[11], [17]**. Confirm the image loads correctly, all internal power-on self-tests complete successfully, and the cryptographic export warning is displayed.

10 Validate that the TOE is running the CC evaluated version of software by executing the `show version` command. Use the `showmon` command to display the currently running system image filename and the system software release version **[9]**.

11 Validate and activate the software license **[1], [18]**. The software license determines available TOE functionality. It is assumed the end-user has acquired a permanent license.

NOTE: A permanent license is recommended as it is valid for the lifetime of the system on which it is installed.

NOTE: Periodically updates to address psirts (bug fixes) to the evaluated imagine are posted and customers are notified that updates are available (if continuing support was purchased). Follow the above steps to download and verify all software updates.

3. Secure Installation and Configuration

The following sections outline configuration settings that must be applied to place the TOE in the evaluated configuration. The evaluated configuration includes the following security features as outlined in the *Cisco Catalyst 9300/9300L/9500 Series Switches running IOS-XE 17.6 Common Criteria Security Target*.

- **Security audit** – ensure audit records are generated for the relevant events and are securely transmitted to a remote syslog server

- **Cryptographic support** – ensure cryptography support for secure communications. The TOE also authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers. The TOE supports zeroization of all cryptographic keys and secrets

- **Identification and authentication** – ensure all users are successfully identified and authenticated prior to gaining access to the TOE, the users can only perform functions in which they have privileges, and terminates users after a configured period of inactivity

- **Secure Management** – provide secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection

- **Protection of the TSF** - protect against interference and tampering by untrusted subjects by implementing identification, authentication, access controls to limit configuration to Authorized Administrators, and software integrity checks. The TOE performs testing to verify correct operation of the switch itself and that of the cryptographic module. The TOE is able to detect replay of information received via secure channels (MACsec). The TOE maintains date and time information

- **TOE access** - terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The TOE can be configured to lock a user account after a specified number of failed logon attempts. The account will remain locked until an Authorized Administrator enables the user account. The Authorized Administrator can configure a security banner to be displayed on the CLI management interface prior to allowing any administrative access to the TOE

- **Trusted Path/Channel** - allow trusted channels to be established from the TOE to a remote administrative session via SSHv2 and initiate outbound IPsec tunnels to transmit audit messages to remote syslog servers. IPsec is used to secure the session between the TOE and the authentication servers

3.1 Physical Installation

Prior to receiving the TOE, prepare the site and gather all necessary tools. Follow all Cisco recommendations for preparing and installing the physical hardware **[2], [19].**

3.2 Initial Setup via Direct Console Connection

Basic configuration of the TOE via console connection must be performed prior to connecting to the network.

NOTE: All CLI commands that can be entered into the TOE by the administrator are indicated with the `courier new` font.

3.2.1 Initial Setup

The TOE comes with Cisco IOS Setup mode enabled **[10]** and a privileged Authorized Administrator (privilege level 15). Setup starts automatically when a device has no configuration file in NVRAM. When setup completes, the System Configuration Dialog is displayed. The dialog guides the Authorized Administrator through the initial configuration of the TOE and network. Once all required information is provided, the TOE prompts the Authorized Administrator to accept the generated configuration file. Enter `Yes` to accept the configuration file. The configuration file is saved in NVRAM. Additional configuration may be made using TOE CLI commands **[6], [22]**. The following parameters are configured in the System Configuration Dialog:

1 **Enter host name** – the **host name** is the name given to the device. The **host name** should comply with the organization's device naming policies

2 **Enter enable secret** – the **secret** must adhere to the password complexity requirements. The **secret** is used to protect access to the privileged (15) Authorized Administrator and configuration modes. Once created the **secret** is stored encrypted in the configuration file

3 **Enter virtual terminal password** – The **virtual terminal password** must adhere to the password complexity requirements. Securing the virtual terminal (or vty) lines with a password in the evaluated configuration is suggested. The **virtual terminal password** allows access to the device through the console port

NOTE: Section 3.3.2 below provides steps to allow ssh into the vty lines.

4 **Configure SNMP Network Management** – NO (this is the default). This setting can be confirmed after "setup" is complete by examining the configuration file to ensure that there is no "snmp-server" entry. To ensure there is no snmp server agent running, use the "**no snmp-server**' command **[5], [21]**. SNMP was not tested during this evaluation and is not a part of the evaluated configuration

5 **Enter interface name used to connect to the management network from the above interface summary** – a list of current interfaces is displayed. Select the interface to be used to connect to the network. Following the organization's networking policies, provide the following information:

- Configure IP on this interface: **Yes**
- IP address for this interface
- Subnet mask for this interface

3.2.2 Saving Configuration

The IOS-XE software uses a running configuration and a startup configuration. Configuration changes made by the Authorized Administrator affect the running configuration. To save the configuration for use on future restarts, the running configuration (held in memory) must be copied to the startup configuration. Use the `write memory` CLI command or the `copy system:running-config nvram:startup-config` CLI command **[6], [22]** to copy the configuration file to the startup configuration. These commands should be used frequently when making changes to the configuration of the TOE. If the TOE power cycles without having copied the running configuration to the startup configuration, then all changes will be lost, and the TOE will revert to the previous saved configuration**.**

3.2.3 FIPS Mode

The TOE must be run in the FIPS-Approved mode of operation. The Authorized Administrator enables FIPS-Approved mode by entering the `fips authorization-key key` CLI command to configure the Authorization key **[4], [17]**. Optional logging may be turned on by entering the `logging console errors` CLI command **[4], [17]**. FIPS status can be vied by entering the `show-fips status` CLI command **[4],[17] .**

The use of the cryptographic engine in any other mode is not allowed and is not tested as part of the CC evaluated configuration.

The CC evaluated configuration supports the following cryptographic functions:

- SSHv2 with RSA keys (minimum 2048-bits)

  NOTE: SSHv1 is not supported

- IPsec must be used to secure connections to AAA servers and may be used to secure other traffic that originates or terminates at the TOE

  NOTE: The evaluated configuration does not require using IPsec to secure traffic flows through the TOE

- IKEv1
- ESP

The following cryptographic functions may be used in the CC evaluated configuration, but were not included in the evaluation effort:

- MD5 for authentication of routing protocols in features of the TOE that are outside the evaluation scope, such as in authentication of routing protocols
- RADIUS may be used, but only when tunneled in IPsec
- AH may be used in IPsec but use of ESP is mandatory

3.2.4 Administration of Cryptographic Self-Tests

The TOE provides self-tests consistent with FIPS 140-2 requirements. The following self-tests are run automatically during power-on:

- AES Known Answer Test
- HMAC Known Answer Test
- RNG/DRBG Known Answer Test
- SHA-1/256/512 Known Answer Test
- RSA Signature Known Answer Test (both signature/verification)
- Software Integrity Test

During the system bootup process (power on or reboot), all the Power On Self-Tests (POSTs) are performed for all cryptographic modules (hardware or software). During initialization and execution of the POSTs, all cryptographic functions are prohibited.

The POSTs are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces. This prevents the security appliances from passing any data before completing the POSTs and entering FIPS mode. In the event of a POST failure, the cryptographic module will force the software to reload, reinitializing the operating system and cryptographic modules. Execution prior to being operational ensures no cryptographic algorithms are accessed unless all POSTs are successful.

Following are descriptions of each of the POSTs:

AES Known Answer Test
For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value. If the encrypted texts match, the test passes; otherwise, the test fails. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The

resulting plaintext value is compared to a known plaintext value. If the decrypted texts match, the test passes; otherwise, the test fails.

RSA Signature Known Answer Test (both signature/verification)
This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value. If the encrypted values, the test passes; otherwise, the test fails. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value. If the decrypted values match, the test passes; otherwise, the test fails.

RNG/DRBG Known Answer Test
For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits. If the random bits match, the test passes; otherwise, the test fails.

HMAC Known Answer Test
For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC. If the MAC values match, the test passes; otherwise, the test fails.

SHA-1/256/512 Known Answer Test
For each of the values listed, the SHA implementation is fed known data and a key. These values are used to generate a hash. This hash is compared to a known value. If the hash values match, the test passes; otherwise, the test fails.

Software Integrity Test
The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity. The software contains a SHA-512 hash and RSA digital signature. If the hash and digital signature match, , the test passes; otherwise, the test fails.

If any self-tests fail, the TOE transitions into a critical error state. In the critical error state, all secure data transmission is halted and the TOE outputs status information indicating the failure. If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated:

Example Error Message

```
_FIPS-2-SELF_TEST_IOS_FAILURE: "IOS crypto FIPS self test failed at %s."
Explanation  FIPS self test on IOS crypto routine failed.
```

These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are performing as expected. Any deviation in the TSF behavior will be identified as a self-test failure.

If a self-test fails, the device will automatically reboot and attempt to execute the tests again. If the error persists, the Authorized Administrator must contact Cisco.

Once operational, the Authorized Administrator executes the power-on self-tests on demand by running the following command:

```
TOE-common-criteria(config)# test crypto self-test
```

3.2.5 Administration of Non-Cryptographic Self-Tests

The TOE provides self-tests to verify the correct image is running on the TOE. The Authorized Administrator can run these tests on demand by entering the `reload/verify` command **[6], [22]**. The following output is displayed:

```
Calculating SHA-1 hash...done
validate_package: SHA-1 hash:
    calculated [hash value]
    expected [same hash value as above]
Image validated
```

The Authorized Administrator can run the `show diagnostic` command to display the online diagnostic test results and the supported test suites **[6], [22]**. This command allows the Authorized Administrator to set diagnostics for various levels, set schedules, and set the diagnostic log size. Diagnostic and error messages received while running tests aid with troubleshooting **[12].**

3.2.6 User Setup

Prior to creating user accounts (administrators) on the TOE, see section 4.2 below for configuring strong passwords. Once a strong password policy is established, perform the following steps to create administrators of the TOE and an enable command **[4], [17]**:

1. Ensure all passwords are stored encrypted: `service password-encryption`

2. Configures administrators using local AAA authentication

   ```
   aaa authentication login default local
   aaa authorization exec default local
   ```

3. Configure local accounts will a privilege level of 1:

   `Username <username> privilege 1 password <password>`

4. When creating administrator accounts, all individual accounts are to be set to a privilege level of one. This is done by using the following commands:

   `username <name> privilege 1 password <password>`

Verify new accounts by logging in via SSH or local console using the new username and password.

3.2.7 Session Termination

The Authorized Administrator configures inactivity settings for session termination for remote and local console connections. Configuration is performed using the following CLI commands **[6], [22]:**

Remote Connection Timeout:

```
line vty <first> <last>
exec-timeout <time>
```

- first and last - range of vty lines on the box (i.e., “0 4”)

- time - period of inactivity after which the session should be terminated

Local Console Timeout:

```
Line console
Exec-timeout <time>
```

- time - period of inactivity after which the session should be terminated

NOTE: The line console setting is not immediately activated for the current session. The current console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session.

In addition to session timeouts, an administrator can manually logout from the TOE using the `exit` CLI command.

3.2.8 User Lockout

The Authorized Administrator configures the TOE to lock a user account after a specified number of failed authentication attempts. Configuration is performed using the following CLI command **[6], [22]:**

```
aaa local authentication attempts max-fail <number of failures>
```

- number of failures - the number of consecutive failures that will trigger locking of the account.

Only the Authorized Administrator can view the list of locked accounts and take actions to unlock them. Following are CLI commands used to view and unlock accounts **[6], [22]:**

Clear unsuccessful login attempts:

```
clear aaa local user fail-attempts
```

Unlock the account:

```
clear aaa local user lockout
```

Display a list of all locked out accounts:

```
show aaa local user lockout
```

This applies to consecutive failures on the TOE during a given session and is not affected by the SSH session disconnections after their default number of failures.

NOTE: The user lockout mechanism is not applicable to the local console.

3.3 Network Protocols and Cryptographic Settings

The TOE provides secure transmission of TSF data when transmitted between separate parts of the TOE (encrypted sessions for remote administration (via SSHv2)).

If the SSH connection between the TOE and the remote Management Workstation is unintentionally broken, the connection will need to be re-established as described section 3.3.1 below.

The TOE supports connection to a remote AAA server (RADIUS) via IPsec. The RADIUS server is used to identify and authenticate users, including login and password, challenge and response, and messaging support. Encryption of the packet body is provided using RADIUS (RADIUS only encrypts the password within the packet body). It is recommended that the AAA server be on an internally protected network, such as a network isolated behind a VPN gateway.

If the IPsec connection between the TOE and the remote authentication server is unintentionally broken, the connection will need to be re-established as described in section 3.3.2 below.

The TOE supports connection to a remote syslog server for the storage of audit data. Audit data is sent securely via IPsec.

If the IPsec connection between the TOE and the remote syslog server is unintentionally broken, the connection will need to be re-established as described in section 3.3.2 below.

The TOE supports the following routing protocols:

- EIGRP
- EIGRPv6 for IPv6
- PIMv2
- PIM-SMv2
- PIM-SSMv2
- OSPFv2
- OSPFv3 for IPv6

3.3.1 Remote Administration Protocols

The TOE supports SSHv2 remote administration. However, prior to configuring SSHv2, the Authorized Administrator must disable Telnet on all vty ports. Telnet provides no protection of transmitted date, so it is not allowed in the evaluated configuration **[6], [22]**:

```
line vty 0 10
transport input ssh
```

The Authorized Administrator must configure SSHv2 using the following commands **[6], [12], [22]**:

Enable SSHv2:

```
ip ssh version 2
```

Generate 2048-bit RSA key pair:

```
crypto key generate rsa {modulus 2048}
```

RSA keys are generated in pairs, one public and one private. The generated keys are saved to the private configuration in NVRAM, which is never displayed to the user or backed up to another device. Only one set of keys is generated at a time. Repeating the command overwrites the old keys.

NOTE: If the configuration is not saved to NVRAM by executing the `copy run start` CLI command, the generated keys are lost on the next reload of the switch.

NOTE: If the error "% Please define a domain-name first" is received, execute the `ip domain-name {domain name}` CLI command.

Configure key exchange method (Diffie-Hellman (DH) group 14) – Server Side:

```
ip ssh dh min size 2048
```

NOTE: The default DH modulus size is 1024-bits (DH Group 1). This Group Size is not allowed in the CC evaluated configuration.

Configure key exchange method (DH group 14) – Client Side:

1. Open Putty on the Management Workstation
2. On the Putty Graphical User Interface (GUI) select **Connection > SSH > Kex**
3. Under **Algorithm selection policy,** use the **Up** button to move DH group 14 to the top of the list
4. Use the **Up** button to move "warn below here" directly below DH group 14
5. Close Putty to save the updated configuration

Configure encryption algorithms (AES-CBC-128 and AES-CBC-256):

```
ip ssh server algorithm encryption aes128-cbc aes256-cbc
```

Configure message authentication code (MAC) algorithms (hmac-sha256, and hmac-sha512):

```
ip ssh server algorithm mac hmac-sha256 hmac-sha512
```

NOTE: The 'none' MAC algorithm is not allowed in the evaluated configuration.

Configure failed login attempts allowed before lockout:

```
ip ssh authentication-retires <integer>
```

NOTE: In the evaluated configuration, the number of failed login attempts is **3**.

Configure inactivity period before session termination:

```
ip ssh timeout <seconds>
```

NOTE: In the evaluated configuration, the timeout time is set to 120 seconds. The default and maximum value allowed by the TOE is 120 seconds.

Configure rekey time and size:

```
ip ssh rekey {time <time> | volume <volume> }
```

NOTE: In the evaluated configuration, the time is no greater than one hour (60 minutes) and the volume is no greater than 1-GB.

Verify encryption algorithms used in an SSH session:

```
show ssh sessions
```

Disconnect an SSH session:

```
ssh disconnect
```

NOTE: The Authorized Administrator can zeroize all RSA key pairs by entering the following command:

```
Crypto key zeroize rsa
```

The TOE, acting as the SSH server, supports the following user authentication methods, it sends to the SSH client in the following predefined order:

- Public-key
- Keyboard-interactive (note this method is not included nor allowed in the evaluated configuration and must be disabled using the following command no ip ssh server authenticate user keyboard
- Password

NOTE: The "Keyboard-interactive" authentication method is not supported in the evaluated configuration and must be disabled by entering the `no ip ssh server authenticate user {keyboard}` CLI command **[6], [22]**. Once disabled, this authentication method will not be offered to the client.

The following remote authentication protocols were not tested in the evaluated configuration and must be disabled **[6], [22]**:

HTTP:

```
no ip http server
```

HTTPS:

```
no ip http secure-server
```

SNMP:

```
no snmp-server
```

Smart Install:

```
no vstack
```

3.3.2 Authentication Server Protocols

RADIUS (outbound) for authentication of TOE administrators to remote authentication servers is disabled by default but can be enabled by the Authorized Administrator in the evaluated configuration. Use best practices for selection and protection of a key to ensure that the key is not easily guessable and is not shared with unauthorized users.

For further information about configuring RADIUS, refer to the following documentation:

- Securing User Services Overview **[4], [17]**
  - RADIUS Attributes
  - RADIUS and TACACS+

- Cisco IOS Security Command Reference: Commands M to R **[6], [22]**
  - radius attributes nas-port-type through rd -> radius server

If using RADIUS for remote authentication, the connection must be secured using IPsec. Additional information regarding configuring IPsec is provided in sections 3.3.6 through 3.3.8 below.

3.3.3 Routing Protocols

The TOE provides MD5 hashing for authentication of neighbor switches via EIGRP, EIGRPv6 for IPv6, PIMv2, PIM-SMv2, PIM-SSMv2, OSPFv2, OSPFv3 for IPv6, RIP for IPv6, and RIPv2 with shared passwords. The hash mechanism is implemented as specified in MD5 RFC 1321 and applied as specified in the related routing protocol RFCs and EIGRP (Cisco proprietary).

Routing tables can be created and maintained manually using static routes configured by the Authorized Administrator. Use of routing protocols is not required to support or enforce any TOE security functionality, including filtering of IPv6 traffic.

The routing protocols are used to maintain routing tables; however, as with any IP routing protocol, the routing process must be created, networks associated with the routing process, and the routing protocols customized for the organization's network. Some combination of these tasks must be performed before routing activities can begin, such as specifying interior (routing networks that are under a common network administration) and exterior (used to exchange routing information between networks that do not share a common administration) gateway protocols. There are other routing configurations, such as multiple routing protocols in a single switch to connect networks that use different routing protocols; however, by default the internal and external (if applicable) need to be configured. Refer to the applicable sections in **[8]** for configuration of the routing protocol.

NOTE: When FIPS-Approved mode is enabled on the TOE (which is required in the evaluated configuration), then MD5 is not permitted unless all neighbor switch authentication routing protocols are being transmitted through IPsec tunnels.

3.3.4 MACSEC and MKA Configuration

The TOE authenticates and encrypts packets between itself and a MACsec peer. The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys to protect data exchanged by the peers.

By default, MACsec is disabled and there are no MKA policies configured on the TOE. Following is an example of an MKA policy:

```
Switch(config)# mka policy mka_policy
Switch(config-mka-policy)# key-server priority 200
Switch(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Switch(config-mka-policy)# confidentiality-offset 30
Switch(config-mka-policy)# end
```

Detailed steps to configure MACsec and an MKA policy on the TOE can be found here:

- Security Configuration Guide, Cisco IOS-XE Bengaluru 17.6.x (Catalyst 9300 Series Switches) **[11]** and Security Configuration Guide, Cisco IOS-XE Bengaluru 17.6.x (Catalyst 9500 Series Switches) **[17]**

- MACsec Encryption -> How to Configure MACsec Encryption -> Configuring MKA MACsec using PSK
- MACsec Encryption -> Configuring Examples for MACsec Encryption

3.3.5 X.509 Certificates

The TOE supports the use of X.509v3 certificates to authenticate IPsec peers using RSA certificates. The validity of the configured certificates is checked both on load of the certificate and during the authentication process. Generation of the RSA key pair is covered in section 3.3.1 above. Creation of the certificates and loading them on the TOE is covered in **[13]** and the sections below.

3.3.5.1 Creation of the Certificate Signing Request

The certificate signing request for the TOE will be created using an RSA key pair and the domain name, as configured in section 3.3.1 above. The Authorized Administrator will use the following CLI commands to generate the certificate signing request **[6], [22]**:

1. In configuration mode, specify the hostname for the peer in the IKE keying exchange

   ```
   hostname <host_name>
   ```

   <host_name> is the identifier assigned to the peer

2. In configuration mode, declare the trustpoint that the TOE should use

   ```
   crypto pki trustpoint <trustpoint_name>
   ```

   <trustpont_name> is the identifier assigned to the trustpoint

3. In ca-trustpoint configuration mode, specify the enrollment parameters of a certification authority (CA).

   ```
   enrollment url <url>
   ```

   <**url**> specifies the URL of the file system where the TOE should send certificate requests (**enrollment url** http://192.168.2.137:80)

4. In ca-trustpoint configuration mode, specify the subject name settings in the certificate request

   ```
   Subject-name <x 500-name>
   ```

   <x.500-name> specifies the subject name used in the certificate request. If the **<x.500-name>** argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used **(subject-name CN=catTOE.cisco.com,OU=TAC)**.

All certificates include the following information:

- public key
- Common Name
- Organization
- Organizational Unit
- Country

Example: <subject-name> CN=catTOE.cisco.com,O=cisco,OU=TAC,C=U

In global configuration mode, create the certificate signing request
.

```
crypto pki enroll <name>
```

"**<name>"** is the CA that was set above using the **crypto pki trustpoint** command (**crypto pki enroll ciscotest**)

3.3.5.2 Securely Connecting to a Certificate Authority for Certificate Signing

The TOE must communicate with the CA for Certificate Signing over IPSEC. This authentication will use pre-shared keys.

Following are sample instructions to configure the TOE to support an IPsec tunnel with AES encryption, with 10.10.10.102 as the IPsec peer IP on the CA, 10.10.10.110 as the local TOE IP.

```
TOE-common-criteria#configure terminal
TOE-common-criteria(config)#crypto isakmp policy 1
TOE-common-criteria(config-isakmp)#encryption aes
TOE-common-criteria(config-isakmp)#authentication pre-share
TOE-common-criteria(config-isakmp)#group 14
TOE-common-criteria(config-isakmp)#lifetime 86400
TOE-common-criteria(config)#crypto isakmp key [insert 22 character preshared key] address 10.10.10.101
TOE-common-criteria(config)#crypto ipsec transform-set sampleset esp-aes esp-sha-hmac
TOE-common-criteria(cfg-crypto-trans)#mode tunnel
TOE-common-criteria(config)#crypto map sample 19 ipsec-isakmp
TOE-common-criteria(config-crypto-map)#set peer 10.10.10.102
TOE-common-criteria(config-crypto-map)#set transform-set sampleset
TOE-common-criteria(config-crypto-map)#set pfs group14
TOE-common-criteria(config-crypto-map)#match address 170
TOE-common-criteria(config-crypto-map)#exit
TOE-common-criteria(config)#interface g0/0
TOE-common-criteria(config-if)#ip address 10.10.10.110 255.255.255.0
TOE-common-criteria(config-if)#crypto map sample
TOE-common-criteria(config-if)#exit
TOE-common-criteria(config)#access-list 170 permit ip 10.10.10.0 0.255.255.255 10.10.10.0 0.255.255.255
```

3.3.5.3 Authenticating the Certificate Authority

The TOE must authenticate the CA by acknowledging its attributes match the publicly posted fingerprint.

1. In global configuration mode, retrieve the CA certificate

   ```
   Crypto ca authenticate <trustpoint_name>
   ```

   <trustpoint_name> is the name of the CA set above using the **crypto pki trustpoint** command (**crypto ca authenticate ciscotest)**

2. Verify the command output matches the fingerprint on the CA public site

```
crypto ca authenticate ciscotest
```

Certificate has the following attributes:

```
Fingerprint MD5: 8DE88FE5 78FF27DF 97BA7CCA 57DC1217
Fingerprint SHA1: 271E80EC 30304CC1 624EEE32 99F43AF8 DB9D0280
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

3.3.5.4 Storing Certificates to a Local Storage Location

Certificates are stored to NVRAM by default; however, storage space is dependent on the platform and storage options. The Authorized Administrator may verify NVRAM storage space by entering the `dir flash` or `boot flash` command **[6], [22]**.

All Cisco platforms support NVRAM and flash local storage; however, other options may be available, including bootflash, slot, disk, USB flash, or USB token. During run time, an Authorized Administrator can specify the active local storage device to be used for certificate storage by performing the following steps **[13]**:

1. Enter configure terminal mode

```
configure terminal
```

2. Specify certificate local storage location

```
crypto pki certificate storage /location-name
crypto pki certificate storage flash:/certs
```

3. Exit configure terminal mode

```
exit
```

4. Save the configuration changes

```
copy system:running-config nvram:startup-config
```

5. Display the certificate storage location

```
show crypto pki certificates storage
```

The following is sample output from the show crypto pki certificates storage command, which shows that the certificates are stored in the certs subdirectory of disk0:

```
Device# show crypto pki certificates storage
Certificates will be stored in disk0:/certs/
```

3.3.5.5 Configuring a Revocation Mechanism for PKI Certificate Status Checking

The Authorized Administrator must monitor the revocation status of all certificates and remove them once expired. The TOE supports the following methods to check the revocation status of certificates:

- crl--Certificate checking is performed by a certificate revocation list (CRL). This is the default behavior
- ocsp--Certificate checking is performed by an online certificate status protocol (OCSP) server

The Authorized Administrator configures the revocation check method in the ca-trustpool configuration mode:

```
revocation-check <method1> [ method2 method3 ]
```

"**<method1>"** specifies the method used by the TOE to check the revocation status of the certificate. If a second and third method is specified, each method is used only if the previous method returns an error, such as a server being down.

Once operational, if the TOE does not have the applicable CRL and is unable to obtain one, or if the OCSP server returns an error, the TOE will reject the peer certificate.

When using OCSP, nonces, unique identifiers for OCSP requests, are sent by default during peer communications with an OCSP server. The use of nonces offers a more secure and reliable communication channel between the peer and OCSP server. If the OCSP server does not support nonces, an authorized administrator may disable the sending of nonces.

3.3.5.6 Configuring Certificate Chain Validation

The TOE supports certificate chaining. The following prerequisites must be met:

- The device must be enrolled in the PKI hierarchy.
- The appropriate key pair must be associated with the certificate.

The Authorized Administrator must perform the following steps to setup certificate chaining **[13]**:

1. Enter configure terminal mode

   ```
   configure terminal
   ```

2. Set the crypto pki trustpoint name

   ```
   crypto pki trustpoint <name>
   ```

   <name> is the name of the trustpoint configured in section 3.3.5.1 above

3. Configure the level to which a certificate chain is processed on all certificates, including subordinate CA certificates

   ```
   chain-validation [{stop | continue } [parent-trustpoint ]]
   ```

   stop - the certificate is already trusted (this is the default setting)
   continue –the subordinate CA certificate associated with the trustpoint must be validated
   parent-trustpoint - the name of the parent trustpoint the certificate must be validated against

NOTE: A trustpoint associated with the root CA cannot be configured to be validated to the next level. The **chain-validation** command is configured with the continue keyword for the trust point associated with the root CA, an error message will be displayed, and the chain validation will revert to the default **chain-validation** command setting.

4. Exit configure terminal mode

```
exit
```

3.3.5.7 Setting X.509 for use with IKE

Once X.509v3 certificates are installed on the TOE, the certificates can be set for use with IKEv1 or IKE2 using the following commands:

```
crypto isakmp policy 1
authentication rsa-sig
```

If an invalid certificate is loaded, authentication will not succeed.

3.3.6 IPsec Overview

The Authorized Administrator configures IKE and IPsec policies on the TOE. IPsec provides the following network security services:

- **Data confidentiality** - the IPsec sender can encrypt packets before transmitting them across a network
- **Data integrity** - the IPsec receiver can authenticate packets sent by the IPsec sender to ensure that the data has not been altered during transmission
- **Data origin authentication** - the IPsec receiver can authenticate the source of the sent IPsec packets. This service is dependent upon the data integrity service
- **Anti-replay** - the IPsec receiver can detect and reject replayed packets

IPsec provides secure tunnels between two peers, such as two switches. The Authorized Administrator defines which packets are considered sensitive and should be sent through secure tunnels. The Authorized Administrator configures the parameters used to protect sensitive packets by specifying tunnel characteristics. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer.

More accurately, these tunnels are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used by the two peers. SAs are unidirectional and are established per security protocol (AH or ESP).

With IPsec, Authorized Administrators can define the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. Traffic is selected based on the source and destination address, and optionally the Layer 4 protocol and port. (The access lists used for IPsec are only used to determine the traffic that needs to be protected by IPsec, not the traffic that should be blocked or permitted through the interface. Separate access lists define blocking and permitting at the interface.)

A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in sequence--the switch attempts to match the packet to the access list specified in that entry. For example:

- The 'discard' option is accomplished using access lists with deny entries, which are applied to interfaces within access-groups.
- The 'bypassing' option is accomplished using access lists with deny entries, which are applied to interfaces within crypto maps for IPsec.
- The 'protecting' option is accomplished using access lists with permit entries, which are applied to interfaces within crypto maps for IPsec.

When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged as cisco, connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.
Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the switch. "Applicable" packets are packets that match the same access list criteria that the original packet matched.

The corresponding inbound SAs are used when processing the incoming traffic from that peer.
Access lists associated with IPsec crypto map entries also represent the traffic that the switch needs protected by IPsec. Inbound traffic is processed against crypto map entries. If an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto map entry, that packet is dropped because it was not sent as an IPsec-protected packet.

Crypto map entries also include transform sets. A transform set is an acceptable combination of security protocols, algorithms, and other settings that can be applied to IPsec-protected traffic. During the IPsec SA negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

3.3.7 Configuration of IPsec

IPsec tunnels must be used for remote administration, transmission of audit records, and whenever connecting to AAA servers (RADIUS). If an IPsec tunnel terminates in a switch (rather than a syslog or RADIUS server) then the connection from the server to the switch must be physically secure. Refer to **[8]** for detailed guidance on configuring IPsec tunnels. To ensure the IPsec tunnels will be consistent with the evaluated configuration, use parameters as described in this section. Configuring IPsec tunnels requires configuration of the following elements:

- **Layer-3 Interfaces:** IP-enabled interfaces that can be local tunnel endpoints
- **Crypto Access Lists:** Any access lists that will be applied to Crypto Maps
- **Crypto Maps:** An association of a crypto access list (a "match address"), one or more IPsec peers (accessible from a valid local layer-3 interface), and with one or more transforms or transform sets
- **IKEv1 Transforms:** Administratively-specified parameters to be permitted during IKE SA negotiation (see tables below for permitted parameters)
- **IKEv1 Transform Sets:** Administratively named sets of IKEv1 Transforms that can be applied within crypto maps instead of assigning parameters individually
- **IPsec Transforms:** Administratively-specified parameters to be permitted during IPsec SA negotiation (see tables below for permitted parameters)

3.3.7.1 Configure Reference Identifier

This section describes configuration of the peer reference identifier, which is achieved through a certificate map.

NOTE: SAN extension is not supported in the evaluated configuration.

Certificate maps provide the ability for a certificate to be matched with a given set of criteria. The Authorized Administrator can specify which fields within a certificate should be checked and which values those fields may or may not have. Following are logical tests for comparing the field with the value:

- equal
- not equal
- contains
- does not contain
- less than
- greater than or equal

ISAKMP and ikev2 profiles can bind themselves to certificate maps, and the TOE will determine if they are valid during IKE authentication. Table 5 below provides information for configuring the reference identifier.

Table 5 Reference Identifier Configuration

Sequence	Command	Action
Step 1	(config)# **crypto pki certificate map** *label sequence-number*	Starts certificate-map mode
Step 2	(ca-certificate-map)# field-name match-criteria match-value	In ca-certificate-map mode, specify one or more certificate fields together with their matching criteria and the value to match. *field-name*—Specifies one of the following case-insensitive name strings or a date: –subject-name –issuer-name –unstructured-subject-name –name –valid-start –expires-on Note Date field format is dd mm yyyy hh:mm:ss or mm dd yyyy hh:mm:ss. *match-criteria*—Specifies one of the following logical operators: –eq—Equal (valid for name and date fields) –ne—Not equal (valid for name and date fields) –co—Contains (valid only for name fields) –nc—Does not contain (valid only for name fields) –lt —Less than (valid only for date fields) –ge —Greater than or equal (valid only for date fields) *match-value*—Specifies the name or date to test with the logical operator assigned by match-criteria.
Step 3	(ca-certificate-map)# **exit**	Exits ca-certificate-map mode.
Step 4	For IKEv1: crypto isakmp profile ikev1-profile1 match certificate *label* For IKEv2: crypto ikev2 profile ikev2-profile1 match certificate *label*	Associates the certificate-based ACL defined with the crypto pki certificate map command to the profile.

Following is an example of how to create a certificate map for IKEv1 to match four subject-name values of the peer:

```
# conf t
(config)# crypto pki certificate map cert-map-match-all 99
(ca-certificate-map)# subject-name co cn=CC_PEER
(ca-certificate-map)# subject-name co o=ACME
(ca-certificate-map)# subject-name co ou=North America
(ca-certificate-map)# subject-name co c=US
(ca-certificate-map)#exit
(config)# crypto isakmp profile ike1-profile-match-cert
match certificate cert-map-match-all
```

3.3.7.2 IKEv1 Transform Sets

An IKEv1 transform set represents a certain combination of security protocols and algorithms. During the IPsec SA negotiation, the peers agree to use a particular transform set for protecting a particular data flow.

Authorized Administrators can specify multiple transform sets and then specify one or more of these transform sets in a crypto map entry. The transform set defined in the crypto map entry is used in the IPsec SA negotiation to protect the data flows specified by that crypto map entry's access list.

During IPsec security association negotiations with IKE, peers search for a transform set that is the same at both peers. When such a transform set is found, it is selected and applied to the protected traffic as part of both IPsec SAs. (With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.)

If a transform set definition is changed during operation the change is not applied to existing security associations but is used in subsequent negotiations to establish new SAs. To apply settings immediately, clear all or part of the SA database by using the `clear crypto sa command` **[6], [22]**.

Following are steps for configuring an IKEv1 transform set **[8]**.

1. Enter configure terminal mode

   ```
   configure terminal
   ```

2. Define the IKE policy and enter config-isakmp configuration mode

   ```
   crypto isakmp policy <priority>
   ```

   <priority> uniquely identifies the IKE policy and assigns a priority to the policy. Valid values: 1 to 10,000; 1 is the highest priority.

3. Set the encryption algorithm(s)

   ```
   encryption <encryption algorithm>
   ```

   <encryption algorithm> denotes the encryption algorithm(s) to be used. In the evaluated configuration, the TOE supports AES-CBC-128 and AES-CBC-256.

4. Set the hash algorithm(s)

   ```
   hash <hash algorithm>
   ```

<hash algorithm> denotes the hash algorithm(s) to be used. In the evaluated configuration, the TOE supports HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512.

5. Specify the authentication mechanism

```
authentication pre-share
```

IKEv1 uses pre-shared keys for authentication. Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")").

The TOE supports pre-shared keys up to 128 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.

For additional information on configuring pre-shared keys, see section 3.3.7.6 below.

6. Specify the Diffie-Hellman key exchange group

```
group 14
```

7. Specify the IKE SA lifetime

```
lifetime <seconds>, <bytes>
```

<seconds> is set from 60 to 86,400 seconds. The shorter the lifetime, the more secure the connection.
<bytes> is the amount of traffic allowed to flow for a given SA. The default value is 2560KB, with a maximum value of 4GB.

8. Disable Aggressive mode, ensure the TOE operates in the default Main mode

```
crypto isakmp aggressive-mode disable
```

9. Exit config-isakmp configuration mode

```
exit
```

10. Exit configure terminal mode

```
exit
```

In IKEv1 only one value may be set per parameter. Therefore, repeat the steps above to create additional IKEv1 transform sets for additional encryption and hash algorithms.

Additional information on configuring IKEv1 transforms can be found in **[8]**.

3.3.7.3 IKEv2 Transform Sets

An IKEv2 proposal is a set of transforms used in the negotiation of the IKEv2 SA as part of the IKE_SA_INIT exchange. An IKEv2 proposal is regarded as complete only when it has an encryption algorithm, an integrity algorithm, and a DH group configured. If no proposal is configured and attached to an IKEv2 policy, then

the default proposal is used. The default proposal contains values that are not valid for the TOE in the CC evaluated configuration. Therefore, the following settings must be set in configuring the IPsec with IKEv2 functionality for the TOE:

Following are steps for configuring an IKEv2 transform set **[8]**.

1. Enter configure terminal mode

```
configure terminal
```

2. Define the IKE policy and enter config-isakmp configuration mode

```
crypto isakmp policy <priority>
```

<priority> uniquely identifies the IKE policy and assigns a priority to the policy. Valid values: 1 to 10,000; 1 is the highest priority.

3. Set the integrity algorithm

```
integrity sha-1
```

The integrity setting specifies the hash algorithm used to ensure data integrity. It ensures that a packet comes from where it says it comes from and that it has not been modified in transit. The default value is sha-1. The TOE can also be configured to use sha-256 or sha-512.

4. Set the encryption algorithm(s)

```
encryption <encryption algorithm1 | encryption algorithm2>
```

<encryption algorithm> denotes the encryption algorithms to be used. In the evaluated configuration, the TOE supports AES-CBC-128 and AES-CBC-256. In IKEv2, multiple encryption algorithms can be specified.

5. Set the hash algorithm(s)

```
hash <hash algorithm1 | hash algorithm2 | hash algorithm3>
```

<hash algorithm> denotes the hash algorithm(s) to be used. In the evaluated configuration, the TOE supports HMAC-SHA-1, HMAC-SHA-256, and HMAC-SHA-512. In IKEv2, multiple hash algorithms can be specified.

6. Specify the authentication mechanism

```
authentication pre-share
```

IKEv1 uses pre-shared keys for authentication. Pre-shared keys on the TOE must be at least 22 characters in length and can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”).

The TOE supports pre-shared keys up to 128 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.

For additional information on configuring pre-shared keys, see section 3.3.7.6 below.

HEX keys generated outside the TOE can be used instead of pre-shared keys for IKEv2. To use HEX keys, instead of pre-shared keys, enter the "`pre-shared-key hex [hex key]`" command **[8]**.

7. Specify the Diffie-Hellman key exchange group

```
group 14
```

8. Specify the IKE SA lifetime

```
lifetime <seconds>, <bytes>
```

<seconds> is set from 60 to 86,400 seconds. The shorter the lifetime, the more secure the connection.
<bytes> is the amount of traffic allowed to flow for a given SA. The default value is 2560KB, with a maximum value of 4GB.

9. Disable Aggressive mode, ensure the TOE operates in the default Main mode

```
crypto isakmp aggressive-mode disable
```

10. Exit config-isakmp configuration mode

```
exit
```

11. Exit configure terminal mode

```
exit
```

Additional information on configuring IKEv2 transforms can be found in **[8]**.

3.3.7.4 IPsec Transform and Lifetimes

Regardless of the IKE version selected, the TOE must be configured with the proper transform for IPsec ESP encryption and integrity as well as IPsec lifetimes.

To configure IPsec ESP to use HMAC-SHA-1 and AES-CBC-128 use the following command:

```
crypto ipsec transform-set example esp-aes 128 esp-sha-hmac
```

To configure IPsec ESP to the other allowed algorithms the following command:

```
crypto ipsec transform-set example esp-aes 256 esp-sha-hmac-256
crypto ipsec transform-set example esp-aes 256 esp-sha-hmac-512
```

The default time value for Phase 2 SAs is 1 hour. There is no configuration required for this setting since the default is acceptable. However, to change the setting to 8 hours as claimed in the Security Target execute the following command:

```
crypto ipsec security-association lifetime seconds 28800
```

Configuring the lifetime based on 100 MB of traffic for Phase 2 SAs is done by entering the following command:

```
crypto ipsec security-association lifetime kilobytes 100000
```

The default amount for this setting is 2560KB. The security association lifetime range is 2560KB - 4GB (100,000 to 4,000,000 Kilobytes).

3.3.7.5 Main Mode vs. Aggressive Mode for IKEv1

By default, the IOS action will initiate IKE authentication negotiations in Main mode. The TOE is not to be operated in Aggressive mode. Aggressive mode can be disabled by entering the following command:

```
crypto isakmp aggressive-mode disable
```

The following commands are not to be used in the evaluated configuration:

- `set aggressive-mode password`
- `set aggressive-mode client-endpoint`
- `initiate mode aggressive`

3.3.7.6 Using Pre-Shared Keys for Authentication

When using pre-shared keys to secure IPsec tunnels, the keys must be entered by an administrator via the CLI. If the remote VPN peer is not administered by the same organization, the pre-shared keys must be exchanged securely, ensuring the keys are never stored or transmitted in unencrypted form. Pre-shared keys can be composed of any combination of upper and lower case letters, numbers, and special characters (including: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”). Pre-shared keys can be from 1 to to 127 characters, with a recommended minimum length of 22 characters from all character sets. The password complexity is not automatically enforced by the TOE and must be mandated in a policy. Execute the following command to set a policy for the pre-shared keys **[6], [22]**:

```
crypto isakmp key {enc-type-digit | keystring} address {peer-
address}
```

To ensure the pre-shared key is stored in encrypted form (AES encrypted) in the configuration file, enable the storing of encrypted keys **[6], [22]**:

```
key config-key password-encryption [text]
password encryption aes
```

If an encryption key is not present, a prompt for the following information will be displayed:

```
New key and Confirm key
```

If an encrypted key already exists, a prompt for the following information will be displayed:

```
Old key, New key, and Confirm key
```

To remove the password that is already encrypted, respond “`yes`” at the following prompt:

```
WARNING: All type 6 encrypted keys will become unusable. Continue
with master key deletion? [yes/no]:
```

To set the key for a tunnel, use the following command **[6], [22]**:

```
crypto isakmp key <enc-type-digit> <keystring>
```

To enter the keystring in encrypted form (AES encrypted), specify "6" as the **<enc-type-digit**>

3.3.7.7 Tunnel Mode vs. Transport Mode

Tunnel mode is the default mode for all IKE connections. The mode setting is applicable only to traffic whose source and destination addresses are IPsec peer addresses. The mode setting is ignored for all other traffic. This mode ensures secure connectivity between the TOE and the authorized remote entity (i.e., syslog server).

Tunnel mode can be specified by entering the following command in crypto ipsec transform set mode **[6], [22]**:

```
mode tunnel
```

However, in the evaluated configuration transport mode is required. Transport mode provides end-to-end communications between a client and server.

Transport mode can be specified by entering the following command in crypto ipsec transform set mode **[6], [22]**:

```
mode transport
```

3.3.7.8 IKEv1 and IKEv2 Parameters Permitted in the Evaluated Configuration

Table 6 below identifies all IKEv1 and IKEv2 parameters permitted in the TOE evaluated configuration.

Table 6 Permitted IKEv1/IKEv2 Parameters

IKEv1 and IKEv2 Transform Types	IKEv1 and IKEv2 Transform Options	Permitted in the Evaluated Configuration	Required in the Evaluated Configuration
Authentication	rsa-sig (default) (RSA signature) rsa-encr (RSA encrypted nonces) pre-share	rsa-sig (default) (RSA signature) pre-share	Yes. While rsa-encr (RSA encrypted nonces) may be offered for use, it is known for weakness and is not allowed for use in the evaluated configuration
Encryption	des (default) 3des aes 128 aes 256	aes 128 aes 256	Yes.
Group	1, 2, 5, 14, 15, 16, 19, 20, 24	14	Yes.
Hash	sha (default sha 1) sha256 sha512	sha (default sha 1) sha256 sha512	Yes.
Lifetime	number of seconds	Yes.	Any time limit is acceptable. The recommended limit for IKEv1 and IKEv2 SA (IKE Phase 1 SA) lifetimes is 24 hours (86,400 seconds).

Table 7 below identifies all IPsec parameters permitted in the TOE evaluated configuration.

Table 7 Permitted IPsec Parameters

IPsec Transform Types	IPsec Transform Options	Permitted in the Evaluated Configuration	Required in the Evaluated Configuration
AH Transform	ah-md5-hmac ah-sha-hmac	No	No. Use of AH is irrelevant to evaluated security functionality.
ESP Encryption Transform	esp-3des esp-aes esp-des esp-null esp-seal	esp-aes	Yes. AES must be used in the evaluated configuration. IPsec protocol ESP is implemented using the cryptographic algorithms AES-CBC-128 and AES-CBC-256 together with HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512
ESP Authentication Transform	esp-md5-hmac esp-sha-hmac	esp-sha-hmac	Yes, IPsec protocol ESP is implemented using the cryptographic algorithms AES-CBC-128 and AES-CBC-256 together with HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512 Not specifying an ESP Authentication Transform would equate to using ESP in "confidentiality only" mode, which is not permitted in the evaluated configuration.
IP Compression Transform	comp-lzs	Yes.	No.
Mode	tunnel (default) transport	Yes.	Tunnel mode is always preferred.
Lifetime	Seconds and/or kilobytes	Yes.	IPsec SAs (IKEv1 and IKEv2 Phase 2 SAs) can be restricted within the range of 2560KB - 4GB (100,000 to 4,000,000 Kilobytes). The recommended time limit for IKEv1 and IKEv2 Phase 2 SAs is no more than 8 hours (28,800 seconds).

3.3.8 Session Protection

TOE communications with the AAA server (RADIUS) and the syslog server must be secured using IPsec. If an Authorized Administrator wants to authenticate using a RADIUS server, then the session between the TOE and AAA server must be protected to ensure the authentication data is not passed in the clear. If an Authorized Administrator wants to back-up the logs to a syslog server, then protection must be provided for the syslog server communications so that audit data is protected.

Following are ways these sessions are protected:

- With a syslog/AAA server acting as an IPsec peer of the TOE and the records tunneled over the IPsec connection
- With a syslog/AAA server that is not an IPsec peer of the TOE but is physically co-located with an IPsec peer of the TOE within a trusted facility, and the records are tunneled over the connection to that IPsec peer.

The syslog/AAA servers will need to act as an IPsec peer or as an IPsec endpoint where there would be a direct connection from the TOE to the syslog/AAA servers.

If the syslog/AAA server is not capable of acting as an IPsec peer or as an IPsec endpoint, then the syslog/AAA server must be in a physically protected facility and connected to a switch capable of establishing an IPsec tunnel with the TOE.

The following sections look at how a syslog sever would be configured in each scenario.

3.3.8.1 Scenario 1 - Syslog Server Running on an IPsec Endpoint

For deployments where the syslog/AAA server operates as an IPsec peer of the TOE, the IPsec tunnel will protect events as they are sent to the server. Examples of free VPN endpoint products that can be installed on a syslog server to allow it to be an IPsec peer include:

- Racoon tool that is part of the IPsec Tools on many Linux systems
- strongSwan
- Openswan
- FreeS/WAN

Below are examples instructions needed to configure the TOE to support an IPsec tunnel with the following parameters:

- aes encryption
- 10.10.10.101 as the IPsec peer IP on the syslog server
- 10.10.10.110 and 30.0.0.1 as the local TOE IPs
- syslog server running on 40.0.0.1 (a separate interface on the syslog server)

For additional information on these commands see **[6], [22]**.

NOTE: This is just an example. Changes to these parameters may be needed to support

```
Switch#configure terminal
Switch(config)#crypto isakmp policy 1
Switch(config)#encryption aes
Switch(config)#authentication pre-share
Switch(config)#group 14
Switch(config)#lifetime 86400
Switch(config)#crypto isakmp key {keystring} address 10.10.10.101
Switch(config)#crypto isakmp key {keystring} address 40.0.0.1
Switch(config)#crypto ipsec transform-set sampleset esp-aes esp-sha-
hmac
Switch(config)#mode tunnel
Switch(config)#crypto map sample 19 ipsec-isakmp
Switch(config-crypto-map)#set peer 10.10.10.101
Switch (config-crypto-map)#set transform-set sampleset
Switch (config-crypto-map)#set pfs group14
Switch (config-crypto-map)#match address 170
Switch (config-crypto-map)#exit
Switch (config)#interface g0/0
Switch (config-if)#ip address 10.10.10.110 255.255.255.0
```

```
Switch (config-if)#crypto map sample
Switch(config-if)#interface Loopback1
Switch(config-if)#ip address 30.0.0.1 255.0.0.0
Switch(config-if)#exit
Switch(config)#ip route 40.0.0.0 255.0.0.0 10.10.10.101
Switch(config)#access-list 170 permit ip 30.0.0.0 0.255.255.255 40.0.0.0
0.255.255.255
Switch(config)#logging source-interface Loopback1
Switch(config)#logging host 40.0.0.1
```

3.3.8.2 Syslog Server Adjacent to an IPsec Peer

If the syslog server is not directly co-located with the TOE, then the syslog server must be in a physically protected facility and connected to a switch capable of establishing an IPsec tunnel with the TOE. This will protect the syslog records as they traverse the public network.

Below are examples instructions needed to configure the TOE to support an IPsec tunnel with the following parameters:

- aes encryption
- 11.1.1.4 as the IPsec peer IP
- 10.1.1.7 and 11.1.1.6 as the local IPs
- syslog server on the 12.1.1.0/28 subnet

For additional information on these commands see **[6], [22]**.

NOTE: This is just an example. Changes to these parameters may be needed to support

```
Switch#configure terminal
Switch#crypto isakmp policy 1
Switch(config-isakmp)#encryption aes
Switch(config-isakmp)#authentication pre-share
Switch(config-isakmp)#group 14
Switch(config-isakmp)#lifetime 28800
Switch(config)#crypto isakmp key {keystring} address 10.10.10.101
Switch(config)#crypto ipsec transform-set sampleset esp-aes esp-sha-
hmac
Switch(cfg-crypto-trans)#mode tunnel
Switch(config)#crypto map sample 1 ipsec-isakmp
Switch(config-crypto-map)#set peer 11.1.1.4
Switch(config-crypto-map)#set transform-set sampleset
Switch(config-crypto-map)#match address 115
Switch(config-crypto-map)#exit
Switch(config)#interface g0/1
Switch(config-if)#ip address 10.1.1.7 255.255.255.0
Switch(config-if)#no ip route-cache
Switch(config-if)#crypto map sample
Switch(config-if)#interface g0/0
Switch(config-if)#ip address 11.1.1.6 255.255.255.0
Switch(config-if)#crypto map sample
Switch(config-if)#exit
```

```
Switch(config)#ip route 12.1.1.0 255.255.255.0 11.1.1.4
Switch(config)#access-list 115 permit ip 10.1.1.0 0.0.0.255 12.1.1.0
0.0.0.255 log
Switch(config)#logging host 12.1.1.1
```

3.4 Logging Configuration

The TOE can be configured to generate an audit record whenever an auditable event occurs. The following events are audited in the evaluated configuration:

- startup and shutdown of the audit function
- starting and stopping services
- identification and authentication related events
- administrative events
    - Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).
    - Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).
    - Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
    - Resetting passwords (name of related user account shall be logged).

A complete list of available audit messages within the TOE is available in [9].

The Authorized Administrator must configure the TOE to capture auditable events. If the command "no logging on" is entered, no audit events are captured, and the TOE is not operating in the evaluated configuration. The Authorized Administrator must perform the following steps to enable audit event logging on the TOEE **[6], [9], [22]**:

1. Enter the Global Configuration Mode

```
enable
```

2. Enter configuration change logger configuration mode

```
log config
```

3. Enable logging of configuration changes

```
logging enable
```

4. Ensure keys and passwords are not displayed in plaintext

```
hidekeys
```

5. Enter the number of entries to be retained in the audit log

```
logging size <entities>
```

NOTE: The range of entries to be saved in the configuration log is from 1 to 1000; the default is 100.

6. Set timestamps on the audit records

```
service timestamps log datetime year
service timestamps debug datetime year
```

7. To ensure audit records are not lost if the TOE fails, enable saving audit records to flash

```
logging file flash <filename>
```

8. Set the logging file size

```
logging file <filesystem/filename> max-file-size
```

NOTE: File size can be 4,096 to 2,147,483,647 characters

9. Turn-on logging of success and failure login attempts

```
logging buffer information
login on-failure log
login on-success log
```

10. Enable RADIUS and SSH debugging

```
debug radius authentication
debug ip ssh authentication
```

11. Enable IPsec related debugging

```
debug crypto isakmp
debug crypto ipsec
debug crypto ikev1 or ikev2
```

12. Enable logging of SSH session establishment, authentication request, terminations and timeouts

```
debug ip ssh detail
```

13. Enable logging of a reboot

```
logging trap debugging
```

14. Enable sending of audit records to a syslog server

```
logging host <ip address of syslog server>
```

NOTE: Direction for configuring remote logging to the syslog server are provided in section 3.4.2 below

15. Specify the severity level for logging to the syslog host

```
logging trap 7
```

NOTE: Level 7 will send all logs required in the evaluation, including debug level logs, to the syslog server.

WARNING: This setting can generate a large number of events that could affect the performance of the device, network, and syslog host.

16. End the configuration session

```
end
```

17. Exit the configuration session

```
exit
```

Debug level auditing is required for specific protocols and events to ensure the audit records with the level of information are generated to meet the requirements in the Security Target. When the debug level of auditing is required, it is annotated as such throughout this Configuration Guide.

NOTE: Before entering a debug command, consider the output of this command and the amount of time it will take to execute. Verify CPU availability by running the "`show processes cpu`" command **[6], [22]**. Always use debug commands with caution.

3.4.1 Usage of Embedded Event Manager

To ensure all commands executed by a privilege level 15 administrator are captured in a syslog record, perform the following **[16]**:

```
event manager applet cli_log
event cli pattern "." *mode exec enter
action 1.0 info type switchname
action 2.0 syslog msg "User:$_cli_username via Port:$_cli_tty
Executed[$_cli_msg]"
action 3.0 set _exit_status "1"
end
```

3.4.2 IPsec Protection for Remote Logging

To protect against audit data loss the TOE must be configured to send audit records securely (through an IPsec tunnel) to an external TCP syslog server. In the evaluated configuration, all audit records are stored locally and simultaneously sent to the external TCP syslog server. The IPsec tunnel ensures the confidentiality and integrity of audit data during transit. Following are various configurations of the syslog server within the TOE operational environment:

- A syslog server operating as an IPsec peer of the TOE and the records tunneled over an IPsec peer-to-peer connection
- A syslog server is not directly co-located with the TOE but is adjacent to an IPsec peer within a trusted facility, and the records are tunneled over the public network

In either configuration the IPsec peer must, at a minimum, support peer authentication using RSA with pre-shared keys and the following algorithms:

- AES-CBC-128 (as specified by RFC 3602) or AES-CBC-256 (as specified by RFC 3602)
- SHA-based HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512)
- DH Group 14 (2048-bit MODP).

For guidance on IPsec configuration of either scenario, refer to section 3.3.7 above.

When connection to the remote audit server is down (either because the IPsec tunnel is down, or the syslog server is unavailable), the TOE will continue to log messages to the logging buffer. Messages in the logging buffer can be viewed with the "`show logging buffer`" command **[6], [22]**.

When the buffer is full, the oldest messages will be overwritten with new messages. The buffer size can be increased using the "`logging buffered <buffer size in bytes>`" command **[6], [22]**.

Set the "`logging buffer debug`" command to ensure an audit record is generated if there is an issue with the logging buffer.

4. Secure Management

4.1 User Roles

The TOE supports privileged, semi-privileged, and non-administrative roles. Non-administrative access is granted to authenticated neighbor switches to allow for the receipt of updated routing tables. This role has no other access and cannot perform any other functions of the TOE.

Administrators with privileged and semi-privileged access are configured in section 3.2.6 above. Privilege levels are set by associating a number, 0-15, to an account. Privilege levels do not have to be hierarchical. The Authorized Administrator is a privileged administrator with privilege level 15 and is automatically configured at installation. Privilege level 15 has access to all commands on the TOE. Privilege levels 0 and 1 are defined by default, while levels 2 - 14 are configured by the Authorized Administrator. Levels 2 – 14 can be configured to include any commands available to privilege level 15. Administrators associated with privilege level 2 – 14 are considered semi-privileged administrators for purposes of this evaluation **[3], [4], [6], [10], [17], [20], [22]**. All administrators access the TOE by logging in with a valid username and password. Successful login is noted by a "#switch" prompt and access to all TOE security functions.

4.2 Passwords

Password complexity is not enforced by default but is required as part of the evaluated configuration to ensure administrators select secure passwords. The Authorized Administrator must configure the password policy using the authentication, authorization, and accounting (AAA) CC policy. The Authorized Administrator must perform the following steps to set the AAA CC policy **[6], [22]:**

1. Enable the new AAA CC policy:

```
enable
configure terminal
aaa new-model
aaa common-criteria policy <policy name>
end
```

2. Set minimum password length:

```
security passwords min-length <length>
```

NOTE: When operating in the CC evaluated configuration, the minimum password length should be set to 15 characters.

3. Set password complexity rules:

```
aaa password restriction
```

NOTE: The following rules will be applied:

- The new password must contain characters from at least three of the following classes: lowercase letters (a – z), uppercase letters (A - Z), digits (0 – 9), and special characters ("!", "@", "#", "$", "%", "^", "&", "*", "(","))").
- The new password should not have a character repeated more than three times consecutively.
- The new password should not be the same as the associated username. The password obtained by capitalization of the username or username reversed is not accepted.
- The new password should not be "cisco", "ocsic", or any variant obtained by changing the capitalization of letters therein, or by substituting "1", "|", or "!" for I; or by substituting "0" for "o" or substituting "$" for "s".

The AAA CC policy and password must be assigned to an administrator account using the "**username**" command **[6], [22]:**

```
username <username> common-criteria-policy <policy> password
<password>
```

Passwords can be stored in encrypted form using the "**service password-encryption**" command **[6], [22]:**

```
service password-encryption
```

Passwords can be stored as a SHA-256 value using the "**username**" command.**[6], [22]:**

```
username <username> secret {0 <password>| 4 <secret-string>
| 5 SHA256 <secret-string>}
```

- <username> - name of the account
- *<password>* - password associated with the user account
- 0 - specifies an unencrypted clear-text password. The password is converted to a SHA-256 secret and gets stored in the switch
- 4 - specifies a SHA-256 encrypted secret string. The SHA 256 secret string is copied from the switch configuration
- 5 - specifies a message digest alogrithm5 (MD5) encrypted secret

NOTE: In previous versions of the TOE evaluated configurations, Cisco required the use of the **enable password** command. This is no longer recommended. With this validation, Cisco recommends the use of the **enable secret** command. The secret generated with the **enable secret** command is stored in the configuration file as a SHA-256 hash value **[6], [22]**.

The IKE preshared keys can be stored in encrypted form (Advanced Encryption Standard (AES)) using the **password encryption aes** and the **key config-key password-encrypt** CLI commands **[6], [22].** These commands must be used in conjunction to set the master password that is used to encrypt the preshared keys.

4.3 System Clock Management

Time and date information is derived from the system clock. The clock is initialized at start-up and is based on Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT). The Authorized Administrator can configure the local time zone and daylight saving time to ensure that time displays correctly regardless of location or season **[6], [22]**.

Configure time zone:

```
clock timezone <zone> <hours-offset> <minute offset>
```

- zone – name of the time zone to be displayed when standard time is in effect
- hours-offset – hours different from UTC
- minute offset – minutes different from UTC

Configure summer-time:

```
clock summer-time zone { date start-date start-month start-year hh : mm end-date end-month end-year hh : mm [offset] | recurring [ week | first | last ] start-date start-month hh : mm { end-week | first | last } end-day end-month hh : mm [offset] }
```

- zone – name of the time zone to be displayed when summer-time is in effect
- date – configure summer-time based on a date range
    - start-date – start day of the week (Sunday, Monday, etc.)
    - start-month – month to start summer timing
    - start-year – year to start summer timing
    - hh:mm – (optional) hour and minute to start summer timing (in military time)
    - end-date – day of the month to end summer timing (integer from 1 to 31)
    - end-month – (optional) month to end summer timing
    - end-year – year to end summer timing (1993 to 2035)
    - offset – (optional) number of minutes to add during summertime (default is 60, with a range of 1 to 1440)
- recurring – configure start and end time for summer timing
    - week – (optional) week of the month (1 to 4)
        - first – (optional) specify the first week of the month
        - last – (optional) specify the last week of the month
        - end day – (optional) day of the week on which summer timing will end (Sunday, Monday, etc.)

4.4 Identification and Authentication

An administrator can connectto the TOE locally through a direct console connection or remotely via SSHv2 or a RADIUS authentication server connected securely through IPsec. Configuration of Identification and Authentication settings is performed through the CLI by the Authorized Administrator **[4], [6], [17], [22]**. Configuration of a user account through RADIUS is available in **[11], [17], [22]**.

4.5 Administrative Banner Configuration

A TOE access banner is displayed to all administrators logging in via the CLI. The Authorized Administrator configures the banner by performing the following steps **[11], [17]**:

```
enable
configure terminal
aaa new-model
aaa authentication banner <delimiter> <text> <delimiter>
end
```

NOTE: Before and after the <text> string, a delineating character or characters must be defined. These character(s) cannot be used in the <text> string.

4.6 Use of Administrative Session Lockout and Termination

The Authorized Administrator configures the length of time that an inactive administrative session may remain open. After the allowed time has elapsed, the administrative session is locked, and the screen is

flushed. All further action is prohibited until the administrator has successfully re-authenticated to the TOE. Following is an example of the CLI commands used to configure the administrative session lockout **[6], [22]**.

```
Line console
Exec-timeout 0 10
```

This example sets the time interval to 10 seconds. If the "no" form of the command is used (`no exec-timeout`) then the timeout configuration is removed, and the TOE will no longer be operating in the evaluated configuration.

4.7 Product Updates

Periodically updates will be made to the TOE. Prior to acceptance the TOE must be verified. Follow the steps outlined in section 2 above for verification and acceptance of the TOE.

5. Security Relevant Events

The TOE generates audit records whenever an auditable event occurs. Audit records are stored locally within the TOE; and if connected, sent securely via IPsec tunnel to an external syslog server. Information about configuring audit event logging is provided in section 3.4 above. The following sections provide information on audit events captured by the TOE, reviewing audit records, and deleting audit records.

5.1 Audit Records

The TOE captures audit events related to TOE security functional requirements (SFRs). Table 8 below provides a list of all SFRs and information related to any applicable audit event captured in the TOE evaluated configuration.

Table 8 SFR to Audit Event Mapping

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_STG_EXT.1	None	None
FCS_CKM.1	None	None
FCS_CKM.2	None	None
FCS_CKM.4	None	None
FCS_COP.1/DataEncryption	None	None
FCS_COP.1/SigGen	None	None
FCS_COP.1/Hash	None	None
FCS_COP.1/KeyedHash	None	None
FCS_COP.1(1)/KeyedHashCMAC	None	None
FCS_COP.1(5) Cryptographic Operation (MACsec Data Encryption/Decryption)	None	None
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)
FCS_MACSEC_EXT.4.4	Creation of Connectivity Association	Connectivity Association Key Names
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key	Creation and update times
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
FCS_RBG_EXT.1	None	None
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).

SFR	Auditable Event	Additional Audit Record Contents
	Administrator lockout due to excessive authentication failures	None
FIA_PMG_EXT.1	None	None
FIA_PSK_EXT.1	None	None
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None	None
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None	None
FIA_X509_EXT.3	None	None
FMT_MOF.1/Services	None	None
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update.	None
FMT_MTD.1/CoreData	None	None
FMT_MTD.1_CryptoKeys	None	None
FMT_SMF.1	All management activities of TSF data.	None
FMT_SMR.2	None	None
FPT_FLS.1	None	None
FPT_SKP_EXT.1	None	None
FPT_APW_EXT.1	None	None
FPT_RPL.1	Detected replay attempt	None
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None	None
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success and failure)	None
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
FTA_SSL.4	The termination of an interactive session.	None
FTA_TAB.1	None	None
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1/Admin	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	None

5.2 Reviewing Audited Events

Authorized Administrators must review audit records on a regular basis. Audit records can be viewed locally or from the remote syslog server. Audit records contain up to 80 characters and a percent sign (%), which follows the optional sequence number or time-stamp information. Audit records include the following information:

- sequence number – unique number assigned to an audit record
- timestamp - date and time of the message or event (format mm/dd hh:mm:ss or hh:mm:ss (short uptime or d h
- facility - the facility to which the message refers (for example, SNMP, SYS, and so forth)
- severity - single-digit code indicating the severity of the event, range from 0 - 7
- MNEMONIC - text string that uniquely describes the message
- description - text string containing detailed information about the event
- hostname-n - hostname of a stack member and its switch number in the stack. Though the stack master is a stack member, it does not append its hostname to system messages

The Authorized Administrator can view audit records by entering the "`show logging`" CLI command **[6], [22]**.

Table 9 below provides sample audit records for the required auditable events; these records are a sample and not meant as an exact record for the event. In addition, for some cryptographic failures producing an audit record would require extensive manipulation and therefore snippets of source code are provided to illustrate what would be displayed in an audit record. The indication that the TSF self-test was completed successful is indicated by reaching a log-in prompt. If TSF self-test did not complete successfully, a system failure error message would be displayed.

Table 9 Audit Records (sample)

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)	**Session Establishment** Mar 15 2016 12:49:11.891 IST: %MKA-5-SESSION_START: (Te1/2 : 22) MKA Session started for RxSCI 188b.9d3c.c83f/0000, AuditSessionID 092B033C0000000E000C08B8, AuthMgr-Handle 45000002 Mar 15 2016 12:49:11.891 IST: MKA-EVENT: Started a new MKA Session on interface TenGigabitEthernet1/2 for Peer MAC 188b.9d3c.c83f with SCI80E0.1DC6.3E7F/0016 successfully
FCS_MACSEC_EXT.4.4	Creation of Connectivity Association	Connectivity Association Key Names	**Creation of Connectivity Associatio** Mar 15 2016 <Gi1/0/2 : 9> 14:38:53.326 IST: %MKA-5-SESSION_SECURED: (Gi1/0/2 : 9) MKA Session was secured for RxSCI 90e2.ba12.a00d/0000, AuditSessionID 000000000000000D001C2D92, CKN 24AA15376050334AE1EA9BE8A1D0894B000000000000000000000000000000000
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key	Creation and update times	**For SAK (Security Association Key) creation**- Mar 15 2016 12:54:49.937 IST: MKA-EVENT 80e0.1dc6.3e7f/0016 C7000003: Generation of new Latest SAK succeeded (Latest AN=0, KN=1)... **For SAK (Security Association Key) update** – Mar 15 2016 <tel:2016> 14:38:53.326 IST: %MKA-6-SAK_REKEY: (Gi0/1/0 : 10) MKA Session is beginning a SAK Rekey (current Latest AN/KN 0/1, Old AN/KN 0/1) for RxSCI f4cf.e298.ccb8/000a, AuditSessionID CKN 100000000000000000000000000000000000000000000000000000000000000000

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.	**Attempted aggressive mode:** Jan 22 2013 13:17:19 UTC: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Aggressive mode failed with peer at 21.0.0.3 Feb 1 2013 10:15:36.555: %CRYPTO-5-IKMP_AG_MODE_DISABLED: Unable to initiate or respond to Aggressive Mode while disabled Unsupported algorithms: [debug - similar to] Jan 21 2013 09:28:02.468: IPSEC(ipsec_process_proposal): transform proposal not supported for identity: {esp-aes } **Termination of IPSEC session (outbound-initiated):** .Jun 19 21:09:49.619: IPSEC(delete_sa): deleting SA, (sa) sa_dest= 100.1.1.5, sa_proto= 50, sa_spi= 0x3C81B171(1015132529), sa_trans= esp-aes esp-sha-hmac , sa_conn_id= 62 sa_lifetime(k/sec)= (4608000/28800), (identity) local= 100.1.1.1:0, remote= 100.1.1.5:0, local_proxy= 10.1.1.0/255.255.255.0/256/0, remote_proxy= 12.1.1.0/255.255.255.0/256/0 **<u>Administrator Action</u>** **Configure IPsec Settings:** Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto isakmp policy 1
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	**Failure to establish an SSH Session.** IP address of remote host Reason for failure. Jun 18 2012 11:19:06 UTC: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: anonymous] [Source: 100.1.1.5] [localport: 22] [Reason: Login Authentication Failed] at 11:19:06 UTC Mon Jun 18 2012 **Establishment of an SSH session** **IP address of remote host** Jun 18 2012 11:31:35 UTC: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ranger] [Source: 100.1.1.5] [localport: 22] at 11:31:35 UTC Mon Jun 18 2012 Feb 8 06:47:17.041: %SSH-5-SSH2_CLOSE: SSH2 Session from 1.1.1.1 (tty = 0) for user 'cisco' using crypto cipher 'aes256-cbc', hmac 'hmac-sha1-96' closed **<u>Administrative action:</u>** **Configure SSH Settings:** Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: ip ssh version 2

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	**Unsuccessful login attempts limit is met or exceeded:** Nov 25 2017 10:52:47.652: \%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user:] [Source: 10.21.0.101] [localport: 22] [Reason: Login Authentication Failed] at 10:52:47 EST Sat Nov 25 2017 Nov 25 2017 10:52:49.655: \%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user:] [Source: 10.21.0.101] [localport: 22] [Reason: Login Authentication Failed] at 10:52:49 EST Sat Nov 25 2017 Nov 25 2017 10:53:05.678: \%SEC_LOGIN-4-LOGIN_FAILED: Login failed [user:] [Source: 10.21.0.101] [localport: 22] [Reason: Login Authentication Failed] at 10:53:05 EST Sat Nov 25 2017 Nov 25 2017 10:53:26.693: \%AAA-5-USER_LOCKED: User testuser locked out on authentication failure **<u>Administrative Actions:</u>** **Configurng number of failures:** Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: aaa local authentication attempts max-fail [number of failures] **Unlock a user** Feb 7 2013 02:05:41.953: %AAA-5-USER_UNLOCKED: User user unlocked by admin on vty0 (21.0.0.1)
FIA_UIA_EXT.1	All use of the identification and authentication mechanism. Administrative Actions: Logging into TOE.	Provided user identity, origin of the attempt (e.g., IP address).	**Login failed:** Jan 17 2013 05:15:14.912: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: anonymous] [Source: 21.0.0.3] [localport: 22] [Reason: Login Authentication Failed] at 00:15:14 EST Thu Jan 17 2013 **Login successful:** Jan 17 2013 05:05:49.460: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ranger] [Source: 21.0.0.3] [localport: 22] at 00:05:49 EST Thu Jan 17 2013 **<u>Administrator Action:</u>** **Administrator login successful:** Jan 21 2013 04:00:57 UTC: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 0.0.0.0] [localport: 0] at 23:00:57 EST Sun Jan 20 2013
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).	**Login failed:** Jan 17 2013 05:15:14.912: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: anonymous] [Source: 21.0.0.3] [localport: 22] [Reason: Login Authentication Failed] at 00:15:14 EST Thu Jan 17 2013 **Login successful:** Jan 17 2013 05:05:49.460: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: ranger] [Source: 21.0.0.3] [localport: 22] at 00:05:49 EST Thu Jan 17 2013

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.	**Unsuccessful attempt to validate a certificate:** Jan 22 2014 13:17:19 UTC: * Jan 22 2014 13:17:19: %CRYPTO-5-IKMP_INVAL_CERT: Certificate received from 10.100.100.2 is bad: certificate invalid
FMT_MOF.1(1)/Manual Update	Any attempt to initiate a manual update	None	See FPT_TUD_EXT.1
FMT_SMF.1	All management activities of TSF data.	None	**Resetting of passwords:** Nov 21 2017 15:06:53.679: \%PARSER-5CFGLOG_LOGGEDCMD: User:admin logged command:no enable password Nov 21 2017 15:06:53.724: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no username script privilege 15 password 0 password Nov 21 2017 15:08:54.042: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username script privilege 15 password 0 secret Nov 21 2017 15:08:54.070: \%PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:enable password secret **Services:** Jul 19 12:10:00 toe-loopback 289: *Jul 19 2018 12:10:00.678: \%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 started - CLI initiated Jul 19 12:09:51 toe-loopback 282: *Jul 19 2018 12:09:51.963: \%SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.24.0.1 port 514 stopped - CLI initiated See all records with 'Administrator Actions'
FPT_RPL.1	Detected replay attempt	None	**Detected replay attempt:** *Jul 7 18:43:14.595: %MKA-3-MKPDU_VALIDATE_FAILURE: (Gi0/0/1 : 11) Validation of a MKPDU failed for RxSCI 6412.25a1.a409/0009, AuditSessionID , CKN 1234000000000000000000000000000000000000000000000000000000000000

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FPT_STM.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	**Local Clock Update:** Feb 5 2013 06:28:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 11:27:52 UTC Tue Feb 5 2013 to 06:28:00 UTC Tue Feb 5 2013, configured from console by admin on console. **Administrator Actions:** **Manual changes to the system time:** Feb 5 2013 06:28:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 11:27:52 UTC Tue Feb 5 2013 to 06:28:00 UTC Tue Feb 5 2013, configured from console by admin on console.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure) Administrative Actions: Software updates	No additional information.	**Administrator Actions:** **Software update:** *Jul 10 2013 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade *Jul 10 2013 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:copy tftp …. *Jul 10 2013 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:reload (if Embedded Event Manager is used) Aug 30 2013 00:33:13 30.0.0.1 239: Aug 30 2013 00:33:12.452: \%HA_EM-6-LOG: cli_log: host[CC_TOE] user[script] port[0] exec_lvl[15] command[upgrade] Executed Aug 30 2013 00:33:13 30.0.0.1 239: Aug 30 2013 00:33:12.452: \%HA_EM-6-LOG: cli_log: host[CC_TOE] user[script] port[0] exec_lvl[15] command[copy tftp] Executed Aug 30 2013 00:33:13 30.0.0.1 239: Aug 30 2013 00:33:12.452: \%HA_EM-6-LOG: cli_log: host[CC_TOE] user[script] port[0] exec_lvl[15] command[reload] Executed
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism. Administrative Actions: Specifying the inactivity time period.	No additional information.	In the TOE this is represented by login attempts that occur after the timeout of an administrative user. Feb 6 2013 04:37:59.190: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 0.0.0.0] [localport: 0] at 04:37:59 UTC Wed Feb 6 2013 **Administrator Action:** **Configure inactivity time period:** Feb 6 2013 04:32:07.609: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FTA_SSL.3	The termination of a remote session by the session locking mechanism. Administrative Actions: Specifying the inactivity time period.	No additional information.	**Tremination of a remote session:** Feb 6 2013 04:32:07.609: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin **<u>Administrator Action:</u>** **Configure inactivity time limit:** Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exec-timeout 60
FTA_SSL.4	The termination of an interactive session.	No additional information.	\ **Admin console log out:** Feb 15 2013 16:29:09: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:exit Or (if Embedded Event Manager is used) Aug 30 2013 00:33:13 30.0.0.1 239: Aug 30 2013 00:33:12.452: \%HA_EM-6-LOG: cli_log: host[CC_TOE] user[script] port[0] exec_lvl[15] command[logout] Executed \ **Admin SSH logout:** Jun 18 2013 11:17:36.653: SSH0: Session terminated normally **<u>Administrator Action:</u>** **Admiinistrator logout:** Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exit
FTA_TAB.1	Administrative Action: Configuring the banner displayed prior to authentication	None	**<u>Administrator Action:</u>** **Configure login banner:** Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: banner login d This is a banner d
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	See events for FCS_IPSEC_EXT.1 above.
FTP_TRP.1	I Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.	See events for FCS_SSH_EXT.1 above.

5.3 Deleting Audit Records

An Authorized Administrator may delete audit records both locally and on the remote syslog server. To delete audit records, the Authorized Administrator must enter the "`clear logging`" CLI command **[6], [22].**

6. Network Services and Protocols

The table below lists the network services/protocols available on the TOE as a client (initiated outbound) and/or server (listening for inbound connections). All services run as system-level processes. The table indicates whether each service or protocol is allowed in the evaluated configuration.

Table 10 Protocols and Services

Service/ Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the evaluated configuration
AH	Authentication Header (part of IPsec)	Yes	No	Yes	No	No, ESP must be used in all IPsec connections.
DHCP	Dynamic Host Configuration Protocol	Yes	Yes	Yes	Yes	No restrictions.
DNS	Domain Name Service	Yes	Yes	No	n/a	No restrictions.
ESP	Encapsulating Security Payload (part of IPsec)	Yes	Yes	Yes	Yes	Configure ESP as described in relevant section of this document.
FTP	File Transfer Protocol	Yes	No	No	n/a	Use tunneling through IPsec
HTTP	Hypertext Transfer Protocol	Yes	No	Yes	No	Use tunneling through IPsec
HTTPS	Hypertext Transfer Protocol Secure	Yes	No	Yes	No	Use tunneling through IPsec
ICMP	Internet Control Message Protocol	Yes	Yes	Yes	Yes	No restrictions.
IKE	Internet Key Exchange	Yes	Yes	Yes	Yes	As described in the relevant sections of this document.
IMAP4S	Internet Message Access Protocol Secure version 4	Yes	Over IPsec	No	n/a	No restrictions.
IPsec	Internet Protocol Security (suite of protocols including IKE, ESP and AH)	Yes	Yes	Yes	Yes	Only to be used for securing traffic that originates from or terminates at the TOE, not for "VPN Gateway" functionality to secure traffic through the TOE. See IKE and ESP for other usage restrictions.
Kerberos	A ticket-based authentication protocol	Yes	Over IPsec	No	n/a	If used for authentication of TOE administrators, tunnel this authentication protocol secure with IPsec.
LDAP	Lightweight Directory Access Protocol	Yes	No, use RADIUS	No	n/a	Use RADIUS instead

Service/ Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the evaluated configuration
LDAP-over-SSL	LDAP over Secure Sockets Layer	Yes	No, use RADIUS	No	n/a	Use RADIUS instead
NTP	Network Time Protocol	Yes	Yes	No	n/a	Any configuration. Use of key-based authentication is recommended.
RADIUS	Remote Authentication Dial In User Service	Yes	Yes	No	n/a	If used for authentication of TOE administrators, secure through IPsec.
SNMP	Simple Network Management Protocol	Yes (snmp-trap)	Yes	Yes	No	Outbound (traps) only. Recommended to tunnel through IPsec.
SSH	Secure Shell	Yes	Over IPsec secured connectio n	Yes	Yes	As described in the relevant section of this document.
SSL (not TLS)	Secure Sockets Layer	Yes	No	Yes	No	Use IPsec instead.
TACACS+	Terminal Access Controller Access-Control System Plus	Yes	No, use RADIUS	No	n/a	Use RADIUS instead
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	Use SSH instead.
TLS	Transport Layer Security	Yes	No	Yes	No	Not claimed; use IPsec instead
TFTP	Trivial File Transfer Protocol	Yes	Yes	No	n/a	Recommend using SCP or HTTPS instead or tunneling through IPsec.

The table above does not include the following protocols and services:

- OSI Layer 2 protocols such as CDP, VLAN protocols (802.11q), Ethernet encapsulation protocols (PPPoE), etc. The evaluated configuration places no restrictions on the use of these protocols; however, evaluation of these protocols was beyond the scope of the CC evaluation. Follow best practices for the secure use of these services.
- Routing protocols such as EIGRP, OSPF, and RIP. The evaluated configuration places no restrictions on the use of these protocols; however, evaluation of these protocols was beyond the scope of the CC evaluation. Follow best practices for the secure use of these services.
- Protocol inspection engines, used for filtering traffic, can be enabled with “inspect” commands. These engines are not used for initiating or terminating sessions, so they are not considered network “services” or “processes’ as defined in Table 10 above. The evaluated configuration places no restrictions on the use of the protocol inspection engines; however, evaluation of this functionality was beyond the scope of the CC evaluation. Follow best practices for the secure usage of these services.
- Network protocols that can be proxied through/by the TOE. Proxying of services by the TOE does not result in running said service on the TOE in any way that would allow the TOE itself to be accessible via that service, nor does it allow the TOE to initiate a connection to a remote server independent of the remote client that has initiated the connection. The evaluated configuration places no restrictions on enabling of proxy functionality; however, evaluation of this functionality

was beyond the scope of the CC evaluation. Follow best practices for the secure usage of these services.

7. Modes of Operation

Following are modes of operation for the TOE:

- **Bootup** – while in Bootup mode, all network traffic is dropped until the software image and configuration is loaded. If This mode of operation automatically progresses to the Normal mode of operation. During Bootup, an administrator may press the **Break** key on a console connection within the first 60 seconds of startup to enter the ROM Monitor mode of operation. This mode is referred to in the guidance documentation as "ROM Monitor Initialization". In Bootup mode, if the TOE does not find a valid operating system image it will enter ROM Monitor mode, and not initiate Normal mode. The transition to ROM Monitor mode protects the TOE from Bootup into an insecure state.

- **Normal (EXEC)** - the IOS-XE image and configuration is loaded, and the TOE is operating as configured. All levels of administrative access occur in this mode and all TOE security functions are available. In Normal mode there is little interaction between the TOE and the administrator. However, the configuration of the TOE can have a detrimental effect on security; therefore, guidance in this document must be followed. Misconfiguration of the TOE could result in inadvertent access to the internal/protected network

- **ROM Monitor** – ROM Monitor mode is a maintenance, debugging, and disaster recovery mode. While the TOE is in this mode, no network traffic is routed between the network interfaces. The TOE may be configured to upload a new boot image from a specified TFTP server, perform configuration tasks, and run various debugging commands.

  When a reload is needed, if NVRAM is empty, IOS-XE will try to boot automatically from an image that is in the flash directory, Images are loaded from top to bottom, so ensure a valid image is listed above all other images in flash by executing the following CLI command **[6], [22]**:

  ```
  #boot system flash:<image filename>
  ```

  To return to Normal (EXEC) mode from ROM Monitor mode, use the following CLI command **[6], [22]**:

  ```
  continue
  ```

  While no administrator password is required to enter ROM Monitor mode, physical access to the TOE is required; therefore, the TOE should be stored in a physically secure location to avoid unauthorized access which may lead to the TOE being placed in an insecure state.

7.1 Power-On Self-Tests Run During Bootup and Normal Operation

Following an operational error, the TOE reboots (once power supply is available) and enters Bootup mode. However, if a power-on self-test (POST) fails during Bootup or Normal operation, then the system crashes, information is displayed on the console, and an error is logged in the "crashinfo" file. POSTs are run automatically during Bootup mode or on-demand by the administrator during Normal mode.

All ports are blocked during execution of the POST. Only when all components of all modules pass the POST is the system placed in a "FIPS PASS" state and ports can forward data traffic.

If any of the POST fail, an error is logged and the system reboots to attempt to re-execute the tests. If the tests continue to fail, the TOE loads into a ROM Monitor state where an administrator can review the crashinfo file to gather additional information on the cause of the crash.

If the problem persists, contact Cisco Technical Assistance via http://www.cisco.com/techsupport or 1 800 553-2447. If necessary, return the TOE to Cisco under guidance of Cisco Technical Assistance.

The TOE performs a software load test whenever a software upgrade is attempted. If the software upgrade load test fails, the system reboots, an error is displayed, and the TOE transitions to a ROM Monitor state.

7.2 Network Processes Available During Normal Operation

The following network-based processes may be running, or can be run, in the evaluated configuration, except where explicitly stated:

- ICMP is supported inbound and outbound for detection and troubleshooting of network connectivity
- IPsec including ESP and IKE is supported for encryption of syslog traffic to an external audit server, and potentially to secure other traffic to/from external entities
- RADIUS is supported for authentication of administrative connections to the console and/or via SSH
- Routing protocols: The evaluated configuration supports use of BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 and RIPv2. The routing protocols, BGPv4, EIGRP, EIGRPv6 for IPv6, PIM-SMv2, and OSPFv2, OSPFv3 for IPv6 supports routing updates with IPv4 or IPv6, while RIPv2 routing protocol support routing updates for IPv4 only. All routing protocols support authentication of neighbor switches using MD5. Neither the authentication functions of those protocols, nor the use of MD5 were tested in the CC evaluated configuration
- Secured SSHv2 sessions are supported inbound and outbound for remote administrative access to the TOE, or to initiate administrative access to an external network device or other device/server running SSHv2
- Syslog is supported outbound for transmission of audit records to a remote syslog server (syslog connections must be tunneled through IPsec)
- Cisco IOS software; to be configured for use as described in this document
- Redundant components, such as power supplies and fans
- SSL (not TLS) may be running; no claims are made in the evaluated configuration
- TLS to secure communications may be running; no claims are made in the evaluated configuration
- Infrastructure services
- Automation through Embedded Event Manager (EEM); no claims are made in the evaluated configuration. This may not be supported on all TOE models due to limited space
- AutoQoS (quality of services responding to traffic flows); no claims are made in the evaluated configuration
- Borderless services
- Rich layer 2/3/4 information (MAC, VLAN, TCP flags); no claims are made in the evaluated configuration

8. Security Measures for the Operational Environment

Proper operation of the TOE requires support from additional components in the TOE operational environment. It is the responsibility of the TOE administrators to ensure all components are available and operational. Table 11 below identifies the security objective for the operational environment and actions to be taken by an administrator to ensure the objective is addressed.

NOTE: The operational environment security objective, OE.NO_THRU_TRAFFIC_PROTECTION is strike-through since the TOE does provide protection against the traffic that does traverse the TOE.

Table 11 Security Objective for the Operational Environment

Security Objective for the Operational Environment	Definition of the Security Objective	Responsibility of the Administrators
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	The TOE must be installed in a physically secured location that only allows physical access to authorized personnel.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	None IOS-XE is a purpose-built operating system that does not allow installation of additional software.
~~OE.NO_THRU_TRAFFIC_PROTECTION~~	~~The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.~~	~~Administrators will ensure protection of any critical network traffic (administration traffic, authentication traffic, audit traffic, etc.) and ensure appropriate operational environment measures and policies are in place for all other types of traffic.~~
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.	Administrators must read, understand, and follow the guidance in this document to securely install and operate the TOE and maintain secure communications with components of the operational environment.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.	Administrators must download updates, including psirts (bug fixes) to the evaluated image, to ensure that the security functionality of the TOE is maintained
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.	Administrators must securely store and appropriately restrict access to credentials that are used to access the TOE (i.e., private keys and passwords)
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.	Administrators must securely wipe the TOE of all sensitive information prior to removing from the operational environment.

9. Acronyms

Table 12 below provides a list of acronyms and abbreviations that are common and may be used in this Configuration Guidance.

Table 12 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AC	Alternating Current
ACL (acl)	Access Control Lists
AES	Advanced Encryption Standard
AGD	Guidance Document
APT	Adaptive Proportion Test
ASCII	American Standard Code for Information Interchange
ASIC	Application Specific Integrated Circuit
CA	Connectivity Association
CAK	(Secure) Connectivity Association Key
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CC	Common Criteria for Information Technology Security Evaluation
CDP	CRL Distribution Point
CEM	Common Evaluation Methodology for Information Technology Security
CKN	Secure Connectivity Association Key Name
CLI	Command Line Interface
CM	Configuration Management
CMAC	Cipher Based Message Authentication Code
CPU	Central Processing Unit
CRL	Certificate Revocation List
CS	Certificate Server
CSP	Critical Security Parameter
CSR	Certificate Signing Request
CTR	Counter
CVL	Component Validation List
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DM	Division Multiplexing
DN	Distinguished Name
DRAM	Dynamic Random-Access Memory
DRBG	Deterministic Random Bit Generator
DW	Dense Wavelength
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	EAP Transport Layer Security
EAPOL	EAP over LANs
EEPROM	Electronically Erasable Programmable Read-Only Memory
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
FFC	Finite Field Cryptography
FQDN	Fully Qualified Domain Name
FRU	Field Replaceable Unit
GB	Giga Byte
GCM	Galois Counter Mode
GE	Gigabit Ethernet port
GUI	Graphical User Interface
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure

Acronyms / Abbreviations	Definition
IC2M	IOS Common Cryptographic Module
ICK	Integrity Check Key
ICMP	*Internet Control Message Protocol*
ICV	Integrity Check Value
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IFS	IOS-XE File System
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IOS	Internetworking Operating System
IP	Internet Protocol
IPsec	IP Security
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	*Integrated Services Digital Network*
ISO	*International Organization of Standardization*
IT	Information Technology
KDF	Key Derivation Function
KEK	Key Encryption Key
LC	Lucent Connector
KAS	Key Agreement Scheme
KAS-SSC	KAS-Shared Secret Computation
KW	Key Wrap
MAC	Media Access Control
MACsec	MAC Security
MKA	MACsec Key Agreement protocol
MKPDU	MACsec Key Agreement Protocol Data Unit
MN	Member Number
MPDU	MAC Protocol Data Unit
MSAP	MAC Service Access Point
MSC	MACsec Controller
MSDU	MAC Service Data Unit
MSK	Master Session Key
NDcPP	collaborative Network Device Protection Profile
NIST	National Institute of Standards and Technology
NVRAM	Non-Volatile Random-Access Memory
OCSP	Online Certificate Status Protocol
OS	Operating System
OSI	Open System Interconnection
OSP	Organizational Security Policies
PAE	Physical Address Extension
PC	Personal Computer
PKCS	Public Key Cryptography Standard
PoE	Power over Ethernet
POST	Power-on Self-Test
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PSK	Pre-Shared Key
PUB	Publication
RA	Registration Authority
RADIUS	Remote Authentication Dial-In User Service
RCT	Repetition Count Test
RFC	Request for Comment
RJ	Registered Jack
RNG	Random Number Generator
ROM	Read-Only Memory
RSA	Rivest, Shamir and Adleman
SA	Security Association
SAK	Secure Association Key

Acronyms / Abbreviations	Definition
SAR	Security Assurance Requirement
SATA	Serial Advanced Technology Attachment
SC	Secure Channel
SCI	Secure Channel Identifier
SCEP	Simple Certificate Enrollment Protocol
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SFP	Small–Form-Factor Pluggable Port
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SM	Service Module
SNMP	Simple Network Management Protocol
SP	Special Publication
SPD	Security Policy Definition
SSD	Solid State Drive
SSHv2	Secure Shell (version 2)
ST	Security Target
TAC	Technical Assistance Center
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UADP	Unified Access Data Plane
UDP	User Datagram Protocol
U.S.	United States
USB	Universal Serial Bus
UTP	Universal Twisted Pair
VAC	Volts of Alternating Current
VPN	Virtual Private Network
WAN	Wide Area Network
WIC	WAN Interface Card

10.Terminology

Table 13 below provides a list of terms that are common and may be used in this Security Target.

Table 13 Terminology

Term	Definition
Authorized Administrator	Any user that has been assigned to a privilege level that is permitted to perform all TSF-related functions.
IOS-XE	Proprietary operating system developed by Cisco Systems.
Peer	Another switch on the network that the TOE interfaces.
MACsec Peer	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
Remote VPN Gateway/Peer	A remote VPN Gateway/Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another switch.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term).
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

11.Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation at:

With CCO login:
http://www.cisco.com/en/US/partner/docs/general/whatsnew/whatsnew.html

Without CCO login:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Documentation is available based on geographic location. Access the most current Cisco documentation at the following sites:

http://www.cisco.com

11.1 Documentation Feedback

We at Cisco appreciate your feedback! Following are ways to provide feedback to Cisco:

Directly through online documentation:

1. Click **Feedback** in the document toolbar
2. Select **Documentation**
3. Once the form is completed, click **Submit**

E-mail comments to **bug-doc@cisco.com**.

Mail comments to:

Cisco Systems, Inc., Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

NOTE: For convenience, a comment card is included in the shipping materials of the TOE.

11.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all product support. Cisco.com is a suite of interactive, networked services that provide immediate, open access to Cisco information and resources from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco. Customers and partners have access to a wide range of features to help streamline business processes and improve productivity:

- View information about Cisco and our networking solutions, services, and programs

- Resolve technical issues with online technical support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Obtain valuable online skill assessment, training, and certification programs

Customers and partners can self-register on Cisco.com to receive personalized information and services. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website (https://mycase.cloudapps.cisco.com/case).

To access or register with Cisco.com, go to the following website:

http://www.cisco.com