Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500)

CC Configuration Guide

Version: 1.0
Date: March 28, 2023

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

Table of Contents

List of Tables

List of Acronyms

The following acronyms and abbreviations are used in this document:

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
FIPS	Federal Information Processing Standards
EAL	Evaluation Assurance Level
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
RADIUS	Remote Authentication Dial In User Service
SFP	Security Function Policy
SSHv2	Secure Shell (version 2)
TCP	Transport Control Protocol
TOE	Target of Evaluation

Document Introduction

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

This document provides supporting evidence for an evaluation of a specific Target of Evaluation (TOE), the Cisco Catalyst 8200 and 8500 Series Edge Routers. This Operational User Guidance with Preparative Procedures 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. Administrators of the TOE will be referred to as administrators, authorized administrators, TOE administrators, semi-privileged administrators, and privileged administrators in this document.

1. Introduction

This Operational User Guidance with Preparative Procedures documents the administration of the Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500), the TOE, as it was certified under Common Criteria. The Cisco Catalyst 8200 and 8500 Series Edge Routers (Cat8200, Cat8500) may be referenced below as the TOE or simply router.

1.1 Audience

This document is written for administrators configuring the TOE. This document assumes that you are familiar with the basic concepts and terminologies used in internetworking, understand your network topology and the protocols that the devices in your network can use, that you are a trusted individual, and that you are trained to use the operating systems on which you are running your network.

1.2 Purpose

This document is the Operational User Guidance with Preparative Procedures for the Common Criteria evaluation. It was written to highlight the specific TOE configuration and administrator functions and interfaces that are necessary to configure and maintain the TOE in the evaluated configuration. This document is not meant to detail specific actions performed by the administrator but rather is a road map for identifying the appropriate locations within Cisco documentation to get the specific details for configuring and maintaining router operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3 Document References

This document refers to several Cisco Systems documents. The documents used are shown below in Table 2. Throughout this document, the guides will be referred to by the "#", such as **[1]**.

Table 2 Cisco Documentation

#	Title	Link
[1]	MACsec and MKA Configuration Guide	https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html

1.4 Supported Hardware and Software

Only the hardware and software listed in section 1.5 of the Security Target (ST) is compliant with the Common Criteria evaluation. Using hardware not specified in the ST invalidates the secure configuration. Likewise, using any software version other than the evaluated software listed in the ST will invalidate the secure configuration. The TOE is a hardware and software solution that makes up the Cat8200 and Cat8500. The network, on which they reside, is considered part of the environment.

1.5 Operational Environment

1.5.1 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports (in some cases optionally) the following hardware, software, and firmware in its environment:

Table 3 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides single-use authentication mechanisms. This can be any RADIUS AAA server that provides single-use authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide single-use authentication to administrators.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
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.
Certification Authority (CA)	Yes	This includes any IT Environment Certification Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
MACSec Peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. It may be any device that supports MACsec communications.
Remote VPN Gateway/Peer	Yes	This includes any VPN Peer (Gateway, Endpoint, another instance of the TOE) with which the TOE participates in VPN communications. Remote VPN Peers may be any device that supports IPsec VPN communications. Another instance of the TOE used as a VPN Peer would be installed in the evaluated configuration, and likely administered by the same personnel.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST

1.6 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 4 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.

These services will be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect compliance to the NDcPP v2.2e, MOD_VPNGW v1.1 and MACSECEP v1.2.

2. Secure Acceptance of the TOE

In order to ensure the correct TOE is received, the TOE should be examined to ensure that that is has not been tampered with during delivery.

Verify that the TOE software and hardware were not tampered with during delivery by performing the following actions:

Step 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 logo and motifs. If it is not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

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

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

Step 4 Note the serial number of the TOE on the shipping documentation. The serial number displayed on the white label affixed to the outer box will be that of the device. Verify the serial number on the shipping documentation matches the serial number on the separately mailed invoice for the equipment. If it does not, contact the supplier of the equipment (Cisco Systems or an authorized Cisco distributor/partner).

Step 5 Verify that the box was indeed shipped from the expected supplier of the equipment (Cisco Systems 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 note number for the shipment matches that used on the delivery. Also verify that the serial numbers of the items shipped match the serial numbers of the items delivered. This verification should be performed by some mechanism that was not involved in the actual equipment delivery, for example, phone/FAX or other online tracking service.

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

Step 7 Approved methods for obtaining a Common Criteria evaluated software images:

- Download the Common Criteria evaluated software image file from Cisco.com onto a trusted computer system.
- Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html.
- The TOE ships with the correct software images installed, however this may not be the evaluated version.

Step 8 Once the file is downloaded, verify that it was not tampered with by using a SHA-512

utility to compute a SHA-512 hash for the downloaded file and comparing this with the SHA-512 hash for the image listed in Table 5 below. If the SHA-512 hashes do not match, contact Cisco Technical Assistance Center (TAC), https://www.cisco.com/c/en/us/support/index.html.

Once the file has been copied, it is recommended that you read and familiarize yourself with the *Configuration Fundamentals Configuration Guide*, *Cisco Catalyst 8300 and 8200 Series Edge Platforms Software Configuration Guide*, and *Cisco Catalyst 8500 Series Edge Platforms Software Configuration Guide* before proceeding with the installation and configuration of the TOE.

Step 9 To verify the digital signature prior to installation, the show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The command handler will extract the signature envelope and its fields from the image file and dump the required information. The show software authenticity file command allows you to display software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. The command handler will extract the signature envelope and its fields from the image file and dump the required information. To display the software public keys that are in the storage with the key types, use the **show software authenticity keys** command in privileged EXEC mode.

TOE-common-criteria# **show software authenticity file** {**bootflash0:***filename* | **bootflash1:***filename* | **bootflash:***filename* | **nvram:***filename* | **usbflash0:***filename* | **usbflash1:***filename*}

To display information related to software authentication for the current ROM monitor (ROMMON), monitor library (monlib), and Cisco IOS image used for booting, use the **show software authenticity running** command in privileged EXEC mode

If the output from the **show software authenticity file** command does not provide expected output, contact Cisco Technical Assistance Center (TAC)
https://tools.cisco.com/ServiceRequestTool/create/launch.do.

After verifying the digital signature with the **show software authenticity file** command, an upgrade and reboot should be configured on the router. The router will not boot if the digital signature is not valid, and an error will be displayed on the console:

autoboot: boot failed, restarting...

Step 10 To install and configure the router follow the instructions as described in *the Configuration Fundamentals Configuration Guide*.

After powering on your router, confirm that the TOE loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

Step 11 The end-user must confirm once the TOE has booted that they are indeed running the evaluated version. Use the **"show version"** command to display the currently running system image

filename and the system software release version. It is also recommended the license level be verified and activated. It is assumed the end-user has acquired a permanent license is valid for the lifetime of the system on which it is installed.

Table 5 Evaluated Software Images

Platform	Image Name	Hash
C8200	c8000be-universalk9.17.06.01a.SPA.bin	SHA512 Checksum : 657ecc86c725a9de35f324f5dbabbdb67d4a4e35ba3a068ec3094e6cf8685f8122e9574e728808df28d3cfc3acb1d0269167cd0921d9c584f670918d5118785e
C8500L	c8000aes-universalk9.17.06.01a.SPA.bin	SHA512 Checksum : 43c0ab85967e9a13b9bbbcef44f1949820369 9fe5885c9aa3e928bd5a1db346b85f4fdd7c2 6a98c0c82a3496c8cefedb94cb9c1dd96c2b1 c83004f7677276a27

When updates, including PSIRTS (bug fixes) to the evaluated image are posted, customers are notified that updates are available (if they have purchased continuing support), information provided how to download updates and how to verify the updates. This information is the same as described above for installing the software image.

3. Secure Installation and Configuration

3.1 Physical Installation

For installation instructions, follow the Cisco Hardware Installation Guide for Catalyst 8200 Series Edge Platforms and Catalyst 8500 Series Edge Platforms.

3.2 Initial Setup via Direct Console Connection

The router must be given basic configuration via console connection prior to being connected to any network.

3.2.1 Options to be chosen during initial setup

The setup starts automatically when a device has no configuration file in NVRAM. When setup completes, it presents the System Configuration Dialog. This dialog guides the administrator through the initial configuration with prompts for basic information about the TOE and network and then creates an initial configuration file. After the file is created, an authorized administrator can use the CLI to perform additional configuration. Use Setup Mode to build a basic configuration and to make configuration changes. The following items must be noted during setup:

It should be noted that the account created during the initial installation of the TOE is considered the privileged administrator and has been granted access to all commands on the TOE.

The term "authorized administrator" is used in this document to refer to any administrator that has successfully authenticated to the router and has access to the appropriate privileges to perform the requested functions.

1 – Enable Secret – The password must adhere to the password complexity requirements as described in the relevant section below in this document. This command ensures that the enable password is not stored in plain text. To configure, use the **enable secret 5** command. Note that this setting can be confirmed after initial configuration is complete by examining the configuration file and looking for "enable secret 5".

2 – Enable Password – The password must adhere to the password complexity requirements as described in the relevant section below in this document. This command is used to control access to various privilege levels. See above how access is controlled when this command has been configured. Note that this password should be set to something different than the enable secret password.

3 – Virtual Terminal Password - Must adhere to the password complexity requirements. Note that securing the virtual terminal (or vty) lines with a password in the evaluated configuration is suggested, though not a requirement for the evaluated configuration. This password allows access to the device through only the console port. Later in this guide, steps will be given to allow ssh into the vty lines.

4 – Configure SNMP Network Management – Note that this setting can be confirmed after configuration 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. Note, in the evaluated configuration, SNMP should remain disabled.

3.2.2 Saving Configuration

IOS-XE uses both a running configuration and a starting configuration. Configuration changes affect the running configuration. In order to save that configuration, the running configuration (held in memory) must be copied to the startup configuration. This may be achieved by either using the **write memory** command or the **copy system:running-config nvram:startup-config** command. These commands should be used frequently when making changes to the configuration of the Router. If the Router reboots and resumes operation when uncommitted changes have been made, these changes will be lost, and the router will revert to the last configuration saved.

3.2.3 Enabling FIPS Mode

The TOE must be run in the FIPS mode of operation. The use of the cryptographic engine in any other mode was not evaluated nor tested during the CC evaluation of the TOE. This is done by setting the following in the configuration:

TOE-common-criteria(config)# **platform ipsec fips-mode**

The self-tests for the cryptographic functions in the TOE are run automatically during power-on as part of the POST. The same POST self-tests for the cryptographic operations can also be executed manually at any time by the privileged administrator using the command:

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

If any of the self-tests fail, the TOE transitions into an error state. In the error state, all secure data transmission is halted and the TOE outputs status information indicating the failure.

3.2.4 Administrator Configuration and Credentials

The router must be configured to use a username and password for each administrator and one password for the enable command. Ensure all passwords are stored encrypted by using the following command:

TOE-common-criteria(config)# **service password-encryption**

Configures local AAA authentication:

TOE-common-criteria(config)# **aaa authentication login default local**

TOE-common-criteria(config)# **aaa authorization exec default local**

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:

TOE-common-criteria(config)# **username <name> password <password>**

to create a new username and password combination, and

TOE-common-criteria(config)# **username <name> privilege 1**

to set the privilege level of <name> to 1.

To login to the router, connect via SSH or local console. Enter the username and password when prompted.

User Access Verification

Username: <enter configured username>

Password: <enter configured password>

3.2.5 Session Termination

Inactivity settings must trigger termination of the administrator session. These settings are configurable by setting

TOE-common-criteria(config)# **line vty <first> <last>** TOE-

common-criteria(config-line)# **exec-timeout <time>** TOE-

common-criteria(config-line)# **line console**

TOE-common-criteria(config)# **exec-timeout <time>**

To save these configuration settings to the startup configuration:

copy run start

where first and last are the range of vty lines on the box (i.e. "0 15"), and time is the period of inactivity after which the session should be terminated. Configuration of these settings is limited to the privileged administrator (see Section 4.1).

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.

3.2.6 User Lockout

User accounts must be configured to lockout after a specified number of authentication failures

TOE-common-criteria(config)# **aaa local authentication attempts max-fail [*number of failures*]**

where number of failures is the number of consecutive failures that will trigger locking of the account. Configuration of these settings is limited to the privileged administrator (see Section 4.1).

Related commands:

clear aaa local user fail-attempts [username *username* | all]	Clears the unsuccessful login attempts of the user.
clear aaa local user lockout username [username]	Unlocks the locked-out user.

show aaa local user lockout	Displays a list of all locked-out users.

Note: *this lockout only applies to privilege 14 users and below.*

Note: Administrator lockouts are not applicable to the local console. Local administrators cannot be locked out and have the ability to unlock other users by using the local console.

3.3 Network Protocols and Cryptographic Settings

Telnet for management purposes is enabled by default and must be disabled in the evaluated configuration. To only allow ssh for remote administrator sessions, use the **transport input ssh** command. This command disables telnet by only allowing ssh connections for remote administrator access.

3.3.1 Remote Administration Protocols

3.3.1.1 Steps to configure SSH on router

1. Configure a hostname:
   TOE-common-criteria# **hostname TOE-common-criteria**

2. Configure a domain name:
   TOE-common-criteria# **ip domain-name cisco.com**

3. Generate RSA – choose a longer modulus length for the evaluated configuration (i.e., 3072):
   TOE-common-criteria(config)# **crypto key generate rsa**
   How many bits in the modulus [512]: **3072**

   RSA keys are generated in pairs—one public key and one private key. This command is not saved in the router configuration; however, the keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.
   Note: *Only one set of keys can be configured using the* ***crypto key generate*** *command at a time. Repeating the command overwrites the old keys.*
   Note: *If the configuration is not saved to NVRAM with a "****copy run start****", the generated keys are lost on the next reload of the router.*

4. Enable SSH v2:
   TOE-common-criteria# **ip ssh version 2**

5. Configure –SSH timeout:
   TOE-common-criteria# **ip ssh time-out 60**

6. Configure SSH retries:
   TOE-common-criteria# **ip ssh authentication-retries 2**

7. Ensure that the product is configured to support diffie-hellman-group14-sha1 key exchange using the following command 'ip ssh dh min size 2048':
   TOE-common-criteria(config)# **ip ssh dh min size 2048**

8. Configure vty lines to accept 'ssh' login services:
   TOE-common-criteria(config-line)# **transport input ssh**

   Note: *To only allow SSH for remote administrator sessions, use the* ***transport input ssh*** *command. This command disables telnet by only allowing SSH connections for remote administrator access.*

9. To secure and control SSH sessions, the evaluated configuration requires SSHv2 session to only use AES-CBC-128 and AES-CBC-256 encryption key algorithms. To set, use the following command:

   TOE-common-criteria(config)# **ip ssh server algorithm encryption aes128-cbc aes256-cbc**

10. The TOE also needs to be configured to only support HMAC-SHA2-256 and HMAC-SHA2-512 MAC algorithms using the following:

    TOE-common-criteria(config)# **ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512**

11. Configure the SSH rekey time-based rekey (in minutes) and volume-based rekey values (in kilobytes) (values can be configured to be lower than the default values if a shorter interval is desired):
    a. **ip ssh rekey time 60**
    b. **ip ssh rekey volume 1000000**

    Note: *When configuring an SSH rekey time or volume interval, the TOE will begin re-key based upon the first threshold reached*

12. To verify the proper encryption algorithms are used for established SSHv2 connections; use the "**show ssh**" command. To disconnect SSH sessions, use the **disconnect ssh** command.

13. To terminate a remote or local session to the router, use the "**exit**" or "**logout**" command at the User or Privilege EXEC prompt to terminate the session.

    Router# **exit**
    or
    Router# **logout**

14. The TOE acting as the SSH server supports three types of user authentication methods and sends these authentication methods to the SSH client in the following predefined order:
    - Public-key authentication method
    - Keyboard-interactive authentication method (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 authentication method

    By default, all the user authentication methods are enabled. Use the **no ip ssh server authenticate user {publickey | keyboard | pasword }** command to disable any specific user authentication method so that the disabled method is not negotiated in the SSH user authentication protocol. This feature helps the SSH server offer any preferred user authentication method in an order different from the predefined order. The disabled user authentication method can be enabled using the **ip ssh server authenticate user {publickey | keyboard | pasword }** command. Refer to Cisco's *Secure Shell Configuration Guide*.

15. HTTP and HTTPS servers were not evaluated and must be disabled:
    TOE-common-criteria(config)# **no ip http server**
    TOE-common-criteria(config)# **no ip http secure-server**

16. SNMP server was not evaluated and must be disabled:

    TOE-common-criteria(config)# **no snmp-server**

Recovery from an event where the connection is unintentionally broken is to follow the steps to establish a connection as listed above.

3.3.2 Authentication Server Protocols

RADIUS (outbound) for authentication of TOE administrators to remote authentication servers are disabled by default but should be enabled by administrators in the evaluated configuration.

To configure RADIUS, refer to the *RADIUS Configuration Guide*. Use best practices for the selection and protection of a key to ensure that the key is not easily guessable and is not shared with unauthorized users.

These protocols are to be tunneled over an IPSec connection in the evaluated configuration. The instructions for setting up this communication are the same as those for protecting communications with a syslog server, detailed in Section 3.3.5below.

3.3.3 Logging Configuration

1. Logging of command execution must be enabled:

    TOE-common-criteria(config)#**archive**
    TOE-common-criteria(config)#**no logging console**
    TOE-common-criteria(config-archive)#**log config**

```
TOE-common-criteria(config-archive-log-cfg)#logging enable
TOE-common-criteria(config-archive-log-cfg)#hidekeys
TOE-common-criteria(config-archive-log-cfg)#notify syslog
TOE-common-criteria(config-archive-log-cfg)#exit
TOE-common-criteria(config-archive)#exit
```

2. Add year to the timestamp:

```
TOE-common-criteria(config)# service timestamps log datetime year
```

3. Enable any required debugging. Debugging is needed for radius (if used), isakmp (if using ikev1), ipsec, and ikev2 (if using ikev2) to generate the events required in the Security Target, however administrators should use discretion when enabling a large number of debugs on an on-going basis:

```
TOE-common-criteria# debug radius authentication
TOE-common-criteria# debug crypto isakmp
TOE-common-criteria# debug crypto ipsec
TOE-common-criteria# debug crypto ikev2
TOE-common-criteria# debug crypto pki server
```

4. Set the size of the logging buffer. It is recommended to set it to at least 150000000:

```
TOE-common-criteria(config)# logging buffer 150000000
```

5. To generate logging messages for failed and successful login attempts in the evaluated configuration, issue the login on-failure and login on-success commands:

```
TOE-common-criteria(config)#login on-failure log
TOE-common-criteria(config)#login on-success log
```

6. To configure the logs to be sent to a syslog server:

```
TOE-common-criteria(config)#logging host<ip address of syslog server>
```

Ex. TOE-common-criteria(config)#logging host192.168.202.169

7. To specify the severity level for logging to the syslog host, use the **logging trap** command. Level 7 will send all logs required in the evaluation up to the debug level logs (as enabled in step 3 above) to the syslog server:

```
TOE-common-criteria(config)# logging trap 7
```

WARNING: this setting has the ability to generate a large number of events that could affect the performance of your device, network, and syslog host.

8. To configure the syslog history table use the **logging history** command. The severity level are numbered 0 through 7, with 0 being the highest severity level and 7 being the lowest severity level (that is, the lower the number, the more critical the message). Specifying a level causes messages at that severity level and numerically lower levels to be stored in the router's history table. To change the number of syslog messages stored in the router's history table, use the logging history size global configuration command. The range of messages that can be stored is 1-500. When the history table is full (that is, it contains the maximum number of

message entries specified with the logging history size command), the oldest message entry is deleted from the table to allow the new message entry to be stored.

TOE-common-criteria(config)# **logging history <level>**

TOE-common-criteria(config)# **logging history size <number>**

3.3.4 Usage of Embedded Event Manager

In order to ensure that all commands executed by a level 15 user are captured in a syslog record, the following Cisco Embedded Event Manager script can be used. Enter it at the CLI as follows:

(config)**#event manager applet cli_log**

(config-applet)**#event cli pattern ".*" sync yes**

(config-applet)**#action 1.0 info type routername**

(config-applet)**#action 2.0 if $_cli_privilege gt "0"**

(config-applet)**#action 3.0 syslog msg "host[$_info_routername] user[$_cli_username] port[$_cli_tty] exec_lvl[$_cli_privilege] command[$_cli_msg] Executed"**

(config-applet)**#action 4.0 end**

(config-applet)**#action 5.0 set _exit_status "1"**

(config-applet)**#end**

See https://supportforums.cisco.com/community/netpro/network-infrastructure/eem for more information on EEM scripting.

3.3.5 Logging Protection

If an authorized administrator wants to backup the logs to a syslog server, then protection must be provided for the syslog server communications. This can be provided in one of two ways:

1. With a syslog server operating as an IPsec peer of the TOE and the records tunneled over that connection, or
2. With a syslog server 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.

When a Syslog server is configured on the TOE, generated audit events are simultaneously sent to the external server and the local logging buffer.

3.3.5.1 Syslog Server Running on an IPsec Endpoint

For deployments where the syslog server is able to operate as an IPsec peer of the TOE, the IPsec tunnel will protect events as they are sent to the server. Examples of products that can be installed on a syslog server to allow it to be an IPsec peer include the Racoon tool that is part of the IPsec Tools on many Linux systems, strongSwan, Openswan, and FreeS/WAN.

Following are sample instructions to configure the TOE to support an IPsec tunnel with aes encryption, with 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, and the syslog server running on 40.0.0.1 (a separate interface on the syslog server).

```
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 28800
TOE-common-criteria(config-isakmp)#exit
TOE-common-criteria(config)#crypto isakmp key [insert 22 character preshared key]
address 10.10.10.101
TOE-common-criteria(config)#crypto isakmp key [insert 22 character preshared key]
address 40.0.0.1
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 10.10.10.101
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)#interface Loopback1
TOE-common-criteria(config-if)#ip address 30.0.0.1 255.0.0.0
TOE-common-criteria(config-if)#exit
TOE-common-criteria(config)# ip route 40.0.0.0 255.0.0.0 10.10.10.101
TOE-common-criteria(config)# access-list extended 170
TOE-common-criteria (config-ext-nacl)# permit ip 30.0.0.0 0.255.255.255 40.0.0.0
0.255.255.255
TOE-common-criteria (config-ext-nacl)# exit
TOE-common-criteria(config)#logging source-interface Loopback1
TOE-common-criteria(config)#logging host 40.0.0.1
```

3.3.5.2 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 located in a physically protected facility and connected to a router capable of establishing an IPsec tunnel with the TOE. This will protect the syslog records as they traverse the public network.

Following are sample instructions to configure the TOE to support an IPsec tunnel with aes encryption, with 11.1.1.4 as the IPsec peer, 10.1.1.7 and 11.1.1.6 as the local IPs, and the syslog server on the 12.1.1.0 /28 subnet:

```
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 28800
TOE-common-criteria (config- isakmp)# exit
TOE-common-criteria(config)#crypto isakmp key [insert 22 character preshared key]
address 10.10.10.101
TOE-common-criteria(config)#crypto isakmp key [insert 22 character preshared key]
address 40.0.0.1
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 1 ipsec-isakmp
TOE-common-criteria(config-crypto-map)#set peer 11.1.1.4
TOE-common-criteria(config-crypto-map)#set transform-set sampleset
TOE-common-criteria(config-crypto-map)#match address 115
TOE-common-criteria(config-crypto-map)#exit
TOE-common-criteria(config)#interface g0/1
TOE-common-criteria(config-if)#ip address 10.1.1.7 255.255.255.0
TOE-common-criteria(config-if)#no ip route-cache
TOE-common-criteria(config-if)#crypto map sample
TOE-common-criteria(config-if)#interface g0/0
TOE-common-criteria(config-if)#ip address 11.1.1.6 255.255.255.0
TOE-common-criteria(config-if)#crypto map sample
TOE-common-criteria(config-if)#exit
TOE-common-criteria(config)#ip route 12.1.1.0 255.255.255.0 11.1.1.4
TOE-common-criteria(config)#access-list extended 115
TOE-common-criteria (config-ext-nacl)# permit ip 10.1.1.0 0.0.0.255 12.1.1.0 0.0.0.255 log
TOE-common-criteria (config-ext-nacl)# exit
TOE-common-criteria(config)#logging host 12.1.1.1
```

Recovery from an event where the connection is unintentionally broken is to follow the steps to establish a connection as listed above.

3.3.6 Base Firewall Rule Set Configuration

The PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW) contains requirements for the TOE basic packet filtering. Packet filtering is able to be done on many protocols by the TOE, including but not limited to (although the evaluation only covers IPv4, IPv6, TCP and UDP):

- IPv4 (RFC 791)

- IPv6 (RFC 2460)
- TCP (RFC 793)
- UDP (RFC 768)
- IKEv1 (RFCs 2407, 2408, 2409, RFC 4109)
- IKEv2 (RFC 5996)
- IPsec ESP (RFCs 4301, 4303)
- SSH (RFCs 4251, 4252, 4253, 4254, 6668, 8308 section 3.1, 8332)

The following attributes, at a minimum, are configurable within Packet filtering rules for the associated protocols:

- IPv4
  - Source address
  - Destination Address
  - Protocol
- IPv6
  - Source address
  - Destination Address
  - Next Header (Protocol)
- TCP
  - Source Port
  - Destination Port
- UDP
  - Source Port
  - Destination Port

The following protocols are not supported and will be dropped ***before*** the packet is matched to an ACL; therefore, any "permit" or "deny" entries in an ACL will not show matches in the output of the 'show ip access-list' command.

- IPv4 - Protocol 2 (IGMP)
  Protocol 2 is configuration dependent and is not supported when the device is not participating in an IGMP routing group.
- IPv6 - Protocols 43 (IPv6-Route), 44 (IPv6-Frag), 51 (AH), 60 (IPv6-Opts), 135 (Mobility Header)

Traffic matching is done based on a top-down approach in the access list. The first entry that a packet matches will be the one applied to it. The MOD_VPNGW requires that the TOE Access control

lists (ACLs) are to be configured to drop all packet flows as the default rule and that traffic matching the acl be able to be logged. The drop all default rule can be achieved by including an ACL rule to drop all packets as the last rule in the ACL configuration. The logging of matching traffic is done by appending the key word "log-input" per the command reference at the end of the acl statements, as done below.

A privileged authorized administrator may manipulate the ACLs using the commands ip inspect, access-list, crypto map, and access-group.

Access lists must be configured on the TOE to meet the requirements of the MOD_VPNGW.

Note: *These access lists must be integrated with the defined security policy for your TOE router. Enabling just these access lists with no permits will result in traffic being dropped. Ensure that your access list entries are inserted above the default deny acl.*

In this example, we are assuming that interface GigabitEthernet0/0 is the external interface and is assigned an IP address of 10.200.1.1. Interface GigabitEthernet0/1 is the internal interface and is assigned an IP address of 10.100.1.1.

If remote administration is required, ssh has to be explicitly allowed through either the internal or external interfaces.

TOE-common-criteria# **configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

TOE-common-criteria(config)# **access-list 199 permit tcp host 10.200.0.1 host 10.200.0.1 eq 22 log-input**

To log connections to the Certificate Authority, implement the following acl:

TOE-common-criteria(config)# **access-list 100 permit ip any host [IP of CA] log- input**

TOE-common-criteria(config)# **access-list 199 permit ip any host [IP of CA] log- input**

To close ports that don't need to be open and may introduce additional vulnerabilities, implement the following acl:

TOE-common-criteria(config)# **access-list 100 deny 132 any any log-input**

TOE-common-criteria(config)# **access-list 199 deny 132 any any log-input**

To explicitly create the default deny acl for traffic with no other match, implement the following acl:

TOE-common-criteria(config)# **access-list 100 deny any any log-input**

TOE-common-criteria(config)# **access-list 199 deny any any log-input**

Note: *Logging of all traffic hitting the default deny acl can generate a large number of logs, and a determination should be made whether it is necessary prior to entering this at the end of all access lists.*

To apply the acls to the interfaces:

TOE-common-criteria(config)# **interface GigabitEthernet0/0**

TOE-common-criteria(config-if)# **ip access-group 199 in** TOE-

common-criteria(config)# **interface GigabitEthernet0/1** TOE-

```
common-criteria(config-if)# ip access-group 100 in
```

Additional information on creation of packet filtering and VPN information flow policies is given in Section 4.6.5 below.

3.3.7 Routing Protocols

The routing protocols are used to maintain routing tables. The routing tables can also be configured and maintained manually. Refer to the *Cisco Catalyst 8300 and 8200 Series Edge Platforms Software Configuration Guide* and the *Cisco Catalyst 8500 Series Edge Platforms Software Configuration Guide* for configuration of the routing protocols.

3.3.8 MACsec and MKA Configuration

The detailed steps to configure MKA, configure MACsec and MKA on interfaces are listed in **[1]**:

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/macsec/configuration/xe-17/macsec-xe-17-book.html

Note: MACsec supports pre-shared keys of 32 and 64 characters in length only.

4. Secure Management

4.1 User Roles

The router has both privileged and semi-privileged administrator roles as well as non-administrative access. Non-administrative access is granted to authenticated neighbor routers for the ability to receive updated routing tables per the information flow rules. There is no other access or functions associated with non-administrative access. These privileged and semi- privileged roles are configured in the Access Control and Session Termination section above. The TOE also allows for customization of other levels. Privileged access is defined by any privilege level entering an 'enable secret 5' after their individual login. Note: The command 'enable secret' is a replacement for the 'enable password' command since the 'enable secret' creates the password and stores it in encrypted. Privilege levels are number 0-15 that specifies the various levels for the user. The privilege levels are not necessarily hierarchical. 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 undefined by default. Levels 0-14 can be set to include any of the commands available to the level 15 administrator and are considered the semi-privileged administrator for purposes of this evaluation. The privilege level determines the functions the user can perform; hence the authorized administrator with the appropriate privileges.

To establish a username-based authentication system, use the username command in global configuration mode.

TOE-common-criteria(config)# **username** *name* [privilege level]

When a user no longer requires access to the TOE, the user account can be removed. To remove an established username-based authentication account, use the "no" form of the command.

TOE-common-criteria(config)# **no username** *name*

Refer to the IOS Command Reference Guide for available commands and associated roles and privilege levels.

4.2 Passwords

The password complexity is not enforced by the router by default and must be administratively set in the configuration. To prevent administrators from choosing insecure passwords, each password must be:

1. At least 15 characters long. Use the following command to set the minimum length to 15 or greater. Password length is configurable up to 127 characters.

   TOE-common-criteria (config)#security passwords min-length *length*

   Example: TOE-common-criteria (config)# **security passwords min-length 15**

2. Composed of any combination of characters that includes characters for at least 3 of these

four character sets: upper case letters, lower case letters, numerals, and the following special characters: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")". Configure the router to enforce that complexity requirement by using enabling "**aaa password restriction**".

Example: TOE-common-criteria (config)# **aaa password restriction**

Enabling **aaa password restriction** will also enforce the following restrictions:

1. The new password cannot have any character repeated more than three times consecutively.
2. The new password cannot be the same as the associated username.
3. The password obtained by capitalization of the username or username reversed is not accepted.
4. The new password cannot 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".

Note: The **aaa password restriction** command can only be used after the **aaa new-model** command is configured.

The following configuration steps are optional but recommended for good password complexity. The below items are recommended but are not enforced by the TOE:

1. Does not contain more than three sequential characters, such as abcd
2. Does not contain dictionary words
3. Does not contain common proper names

Administrative passwords, including any "enable" password that may be set for any privilege level, must be stored in non-plaintext form. To have passwords stored as a SHA-256 hash, use the "**service password-encryption**" command in config mode.

TOE-common-criteria (config)#**service password-encryption**

Once that service has been enabled, passwords can be entered in plaintext, or has SHA-256 hash values, and will be stored as SHA-256 hash values in the configuration file when using the "username" command.

TOE-common-criteria (config)#**username** *name* {**password** *password* | **password** *encryption- type encrypted-password*}

Whether or not "service password-encryption" has been enabled, a password for an individual username can be entered in either plaintext or as a SHA-256 hash value, and be stored as a SHA-256 hash value by using the following command:

TOE-common-criteria(config)#**username** *name* **secret** {**0** *password* | **4** *secret-string* | *5 SHA256 secret-string*}

To store the enable password in non-plaintext form, use the '**enable secret**' command when setting the enable password. Example:

TOE-common-criteria(config)#**enable secret** [**level** *level*] {*password* | **0** | **4** [*encryption-type*] *encrypted-password* }

level – (Optional) Specifies the level for which the password applies. You can specify up to sixteen privilege levels, using the numerals 0 through 15.

password – password that will be entered

0 – Specifies an unencrypted clear-text password. The password is converted to a SHA256 secret and gets stored in the router.

4 – Specifies an SHA256 encrypted secret string. The SHA256 secret string is copied from the router configuration.

encryption-type – (Optional) Cisco-proprietary algorithm used to encrypt the password. If you specify a value for *encryption- type* argument, the next argument you supply must be an encrypted password (a password encrypted by a Cisco router).

encrypted-password – Encrypted password that is copied from another router configuration.

Use of enable passwords are not necessary, so all administrative passwords can be stored as SHA-256 if enable passwords are not used.

Note: *Cisco no longer recommends that the 'enable password' command be used to configure a password for privileged EXEC mode. The password that is entered with the 'enable password' command is stored as plain text in the configuration file of the networking device. If passwords were created with the 'enable password' command, it can be hashed by using the 'service password-encryption' command. Instead of using the 'enable password' command, Cisco recommends using the 'enable secret' command because it stores a SHA-256 hash value of the password.*

To have IKE preshared keys stored in encrypted form, use the **password encryption aes** command to enable the functionality and the **key config-key password-encrypt** command to set the master password to be used to encrypt the preshared keys. The preshared keys will be stored encrypted with symmetric cipher Advanced Encryption Standard [AES].

TOE-common-criteria (config)# **password encryption aes**

TOE-common-criteria (config)# **key config-key password-encryption** [*text*]

4.3 Clock Management

Clock management is restricted to the privileged administrator. Use the commands below to configuring the time and date:

```
router(config)# clock timezone zone hours-offset [minutes-offset]
router(config)# clock summer-time zone recurring [week day month hh:mm week day month
hh:mm [offset]]
router(config)# clock summer-time zone date date month year hh:mm:ss date month year
hh:mm:ss [offset]
router(config)# exit
router# clock set hh:mm:ss date month year
```

4.4 Identification and Authentication

Configuration of Identification and Authentication settings is restricted to the privileged administrator.

The router can be configured to use any of the following authentication methods:

- Remote authentication (RADIUS)
  - Refer to "Authentication Server Protocols" elsewhere in this document for more details.
- Local authentication (password or SSH public key authentication);
  - Note: this should only be configured for local fallback if the remote authentication server is not available.
- X.509v3 certificates
  - Refer to "X.509 Certificates" in Section 4.6.4 below for more details.

4.5 Login Banners

The TOE may be configured by the privileged administrators with banners using the **banner login** command. This banner is displayed before the username and password prompts. To create a banner of text "This is a banner" use the command

banner login d This is a banner d

where d is the delimiting character. The delimiting character may be any character except '?', and it must not be part of the banner message.

4.6 Virtual Private Networks (VPN)

4.6.1 IPsec Overview

The TOE allows all privileged administrators to configure Internet Key Exchange (IKE) and IPSEC policies. 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 routers. The privileged administrator defines which packets are considered sensitive and should be sent through these secure tunnels and specifies the parameters that should be used to protect these sensitive packets by specifying the characteristics of these tunnels. 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, privileged 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. Therefore, traffic may be selected on the basis of 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 a sequence--the router attempts to match the packet to the access list specified in that entry.

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 router. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted before being forwarded to the remote peer. 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 router 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.

4.6.1.1 IKEv1 Transform Sets

An Internet Key Exchange version 1 (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.

Privileged 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 peers' IPsec SAs. (With manually established SAs, there is no negotiation with the peer, so both sides must specify the same transform set.)

Note: *If a transform set definition is changed during operation that the change is not applied to existing security associations but is used in subsequent negotiations to establish new SAs. If you want the new settings to take effect sooner, you can clear all or part of the SA database by using the* ***clear crypto sa command.***

The following settings must be set in configuring the IPsec with IKEv1 functionality for the TOE:

TOE-common-criteria # **conf t**

TOE-common-criteria (config)#**crypto isakmp policy 1**

TOE-common-criteria (config-isakmp)# **hash sha**

This configures IPsec IKEv1 to use SHA-1 cryptographic hashing. SHA-256 and SHA-512 can be configured with the hash command, **hash <sha | sha256 | sha512>.**

TOE-common-criteria (config-isakmp)# **encryption aes**

This configures IPsec IKEv1 to use AES-CBC-128 for payload encryption. AES-CBC_192 and AES-CBC-256 can be selected with the encryption command, **encryption <aes | aes-192 | aes-256>.**

Note: *the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128.*

Note: *Both confidentiality and integrity are configured with the hash and encryption commands respectively. As a result, confidentiality-only mode is disabled.*

TOE-common-criteria (config-isakmp)# **authentication pre-share**

This configures IPsec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPsec peers. See Section 4.6.4 below for additional information.

TOE-common-criteria(config-isakmp)# **Crypto isakmp key cisco123!cisco123!CISC address 11.1.1.4**

Note: *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 127 bytes in length. While longer keys increase the difficulty of brute-force attacks, longer keys increase processing time.

TOE-common-criteria (config-isakmp)# **group 14**

This selects DH Group 14 (2048-bit MODP) for IKE, but 19 (256-bit Random ECP), 24

(2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP) and 15 (3072 bit MODP) are also allowed and supported.

TOE-common-criteria (config-isakmp)# **lifetime 86400**

The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values.

TOE-common-criteria (config-isakmp)# **crypto isakmp aggressive-mode disable**

Main mode is the default mode and the **crypto isakmp aggressive-mode disable** ensures all IKEv1 Phase 1 exchanges will be handled in the default main mode.

TOE-common-criteria(config-isakmp)#**exit**

4.6.1.2 IKEv2 Transform Sets

An Internet Key Exchange version 2 (IKEv2) proposal is a set of transforms used in the negotiation of IKEv2 SA as part of the IKE_SA_INIT exchange. An IKEv2 proposal is regarded as complete only when it has at least an encryption algorithm, an integrity algorithm, and a Diffie-Hellman (DH) group configured. If no proposal is configured and attached to an IKEv2 policy, then the default proposal is used in the negotiation, and it contains selections that are not valid for the TOE. Thus, the following settings must be set in configuring the IPsec with IKEv2 functionality for the TOE:

TOE-common-criteria # **conf t**

TOE-common-criteria (config)#**crypto ikev2 proposal sample**

TOE-common-criteria (config-ikev2-proposal)# **integrity sha1**

This configures IPsec IKEv2 to use SHA-1 cryptographic hashing. SHA 256 and SHA-512 can be configured with the integrity command, **integrity <sha1 | sha256 | sha512>**.

TOE-common-criteria (config-ikev2-proposal)# **encryption aes-cbc-128**

This configures IPsec IKEv2 to use AES-CBC-128 for payload encryption. AES-CBC-192, AES-CBC-256, AES-GCM-128, and AES-GCM-256 can be selected with the encryption command, **encryption <aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | aes-gcm-128 | aes-gcm-256>**.

Note: *the authorized administrator must ensure that the keysize for this setting is greater than or equal to the keysize selected for ESP in Section 4.6.2 below. If AES 128 is selected here, then the highest keysize that can be selected on the TOE for ESP is AES 128 (either CBC or GCM).*

Note: *Both confidentiality and integrity are configured with the hash and encryption commands respectively. As a result, confidentiality-only mode is disabled.*

TOE-common-criteria (config-ikev2-proposal)# **authentication local pre-share**

This configures IPsec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPsec peers. See Section 4.6.4 below for additional information.

TOE-common-criteria (config-ikev2-proposal)# **group 14**

This selects DH Group 14 (2048-bit MODP) for IKE, but 19 (256-bit Random ECP), 24 (2048-bit MODP with 256-bit POS), 20 (384-bit Random ECP), and15 (3072 bit MODP) are also allowed and supported.

TOE-common-criteria (config-ikev2-proposal)# **lifetime 86400**

The default time value for Phase 1 SAs is 24 hours (86400 seconds), but this setting can be changed using the command above with different values.

TOE-common-criteria (config)#**crypto ikev2 keyring keyring-1**

TOE-common-criteria (config-ikev2-keyring)# **peer peer1**

TOE-common-criteria (config-ikev2-keyring-peer)# **address 0.0.0.0 0.0.0.0**

TOE-common-criteria (config-ikev2-keyring-peer)# **pre-shared-key cisco123!cisco123!CISC**

This section creates a keyring to hold the pre-shared keys referenced in the steps above. In IKEv2 these pre-shared keys are specific to the peer.

Note: *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 127 bytes in length. While longer keys increase the difficulty of brute-force attacks, but longer keys increase processing time.

HEX keys generated off system can also be input for IKEv2 using the following instead of the pre-shared-key command above: '**pre-shared-key hex [hex key]**'.

For example: **pre-shared-key hex 0x6A6B6C**.

This configures IPsec to use pre-shared keys. X.509 v3 certificates are also supported for authentication of IPsec peers. See Section 4.6.4 below for additional information.

TOE-common-criteria (config)#**crypto logging ikev2**

This setting enables IKEv2 syslog messages.

4.6.2 IPsec Transforms 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.

Router(config)# **crypto ipsec transform-set NAME <esp-aes 128 | esp-aes 192 | esp-aes 256> <esp-sha-hmac | esp-sha256-hmac | esp-sha512-hmac>**

or

Router(config)# **crypto ipsec transform-set NAME <esp-gcm 128 | esp-gcm 192 | esp-gcm 256>**

Example command:

TOE-common-criteria(config)# **crypto ipsec transform-set EXAMPLE esp-aes 128 esp-sha-hmac**

Note: *The size of the key selected here must be less than or equal to the key size selected for the IKE encryption setting in 4.6.1.1 and 4.6.1.2 above. If AES-CBC- 128 was selected there for use with IKE encryption, then only AES-CBC-128 or AES-GCM-128 may be selected here.*

TOE-common-criteria(config-crypto)#**mode tunnel**

This configures tunnel mode for IPsec. Tunnel is the default, but by explicitly specifying tunnel mode, the router will request tunnel mode and will accept only tunnel mode.

TOE-common-criteria(config-crypto)#**mode transport**

This configures transport mode for IPsec.

TOE-common-criteria (config)#**crypto ipsec security-association lifetime seconds 28800**

The default time value for Phase 1 SAs is 24 hours. The default time value for Phase 2 SAs is 1 hour. There is no configuration required for these since the defaults are acceptable. However, to change the setting to 8 hours as claimed in the Security Target the crypto ipsec security-association lifetime command can be used as specified above.

TOE-common-criteria (config)#**crypto ipsec security-association lifetime kilobytes 100000**

This configures a lifetime of 100 MB of traffic for Phase 2 SAs. The default amount for this setting is 2560KB, which is the minimum configurable value for this command. The maximum configurable value for this command is 4GB.

This functionality is available to the Privileged Administrator. Configuration of VPN settings is restricted to the privileged administrator.

4.6.3 NAT Traversal

For successful NAT traversal over an IOS-XE NAT device for an IPsec connection between two IOS-XE peers, the following configuration needs to be used. For more information, refer to the *IP Addressing: NAT Configuration Guide*.

On an IOS NAT device (router between the IPsec endpoints):

config terminal

ip nat service list <ACL-number> ESP spi-match

access-list <ACL-number> permit <protocol> <local-range> <remote-

range> end

On each IOS peer (IPsec router endpoints):

config terminal

crypto ipsec nat-transparency spi-

matching end

4.6.4 X.509 Certificates

The TOE may be configured by the privileged administrators to use X.509v3 certificates to authenticate IPsec peers. Both RSA and ECDSA certificates are supported.

Creation of these certificates and loading them on the TOE is covered in the *Public Key Infrastructure Configuration Guide*.

4.6.4.1 Generate a Key Pair

RSA and ECDSA keys are generated in pairs—one public key and one private key:

(config)# crypto key generate rsa modulus 3072

- or -

(config)# crypto key generate ec keysize <256 | 384> exportable

The keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device) the next time the configuration is written to NVRAM.

Note: Only one set of keys can be configured using the crypto key generate command at a time. Repeating the command overwrites the old keys.

Note: If the configuration is not saved to NVRAM with a "copy run start", the generated keys are lost on the next reload of the router.

Note: If the error "% Please define a domain-name first" is received, enter the command 'ip domain-name [domain name].

4.6.4.2 Creation of the Certificate Signing Request

The certificate signing request for the TOE will be created using the RSA or ECDSA key pair and the domain name configured in Section 4.6.4.1 above.

In order for a certificate signing request to be generated, the TOE must be configured with a hostname, trustpoint, enrollment method and revocation checking. This is done by using the following commands:

- To specify the hostname for the peer in the IKE keyring exchange, use the **hostname** *name* in configuration mode

  Hostname <name>
  Where the **<name>** is the name of the peer (**hostname catTOE**)

- To declare the trustpoint that the TOE should use, use the **crypto pki trustpoint** *name* command in configuration mode

  crypto pki trustpoint <name>
  Where the **<name>** creates the name of the trustpoint (**crypto pki trustpoint ciscotest**)

- To specify the enrollment parameters of a certification authority (CA), use the enrollment [terminal or url] command in ca-trustpoint configuration mode

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

- To specify the subject name settings in the certificate request, use the subject-name command in ca-trustpoint configuration mode.

  subject-name <x.500-name>
  Where the **<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 of the certificates include at least the following information:

  public key and (Common Name, Organization, Organizational Unit, Country) **<subject-name> CN=catTOE.cisco.com,O=cisco,OU=TAC,C=U**

- To specify the revocation check method, use the revocation-check command in ca-trustpool configuration mode.

  revocation-check *crl*

  (ca-trustpoint)**#revocation-check crl**

  This will set up the certificate revocation mechanism to CRL, which is to be used to ensure that the certificate of a peer has not been revoked. If the TOE is unable to obtain a CRL, the TOE will reject the peer's certificate.

- To create the certificate signing request, use the crypto pki enroll command in global configuration mode.

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

4.6.4.3 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**

4.6.4.4 Authenticating the Certificate Authority

The TOE must authenticate the CA by acknowledging its attributes match the publicly posted fingerprint. The TOE administrator must verify that the output of the command below matches the fingerprint of the CA on its public site.

Authenticate the CA: **crypto ca authenticate** ***trustpoint-name***
Device (config)**#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.

4.6.4.5 Storing Certificates to a Local Storage Location

Certificates are stored to NVRAM by default; however, some routers do not have the required amount of NVRAM to successfully store certificates. All Cisco platforms support NVRAM and flash local storage. Depending on the platform, an authorized administrator may have other supported local storage options including bootflash, slot, disk, USB flash, or USB token. During run time, an authorized administrator can specify what active local storage device will be used to store certificates.

How to Specify a Local Storage Location for Certificates -

The summary steps for storing certificates locally to the TOE are as follows:

Enter configure terminal mode:
TOE-common-criteria# **configure terminal**

Specify the local storage location for certificates: **crypto pki certificate storage** ***location-name***
Device(config)# **crypto pki certificate storage bootflash:/certs**

Exit: Device(config)#
exit

Save the changes made:
Device# **copy system:running-config nvram:startup-config**

Display the current setting for the PKI certificate storage location:
Device# **show crypto pki certificates storage**

4.6.4.6 Configuring a Revocation Mechanism for PKI Certificate Status Checking

Perform this task to set up the certificate revocation mechanism--CRLs--that is used to check the status of certificates in a PKI.

Use the **revocation-check** command to specify at least one method (CRL or skip the revocation check) that is to be used to ensure that the certificate of a peer has not been revoked. For multiple methods, the order in which the methods are applied is determined by the order specified via this command.

(ca-trustpoint)#**revocation-check crl**

If the TOE does not have the applicable CRL and is unable to obtain one, the TOE will reject the peer's certificate.

4.6.4.7 Configuring Certificate Chain Validation

Perform this task to configure the processing level for the certificate chain path of peer certificates.

Prerequisites:

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

1. **Enter configure terminal mode:**
   TOE-common-criteria# **configure terminal**
2. **Set the crypto pki trustpoint name:**
   TOE-common-criteria(config)# **crypto pki trustpoint ca-sub1**
3. **Configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates using the chain-validation [{stop | continue} [parent- trustpoint]] command:**
   TOE-common-criteria(ca-trustpoint)# **chain-validation continue ca-sub1**
   - **Use the stop keyword to specify that the certificate is already trusted. This is the default setting.**
   - **Use the continue keyword to specify that the subordinate CA certificate associated with the trustpoint must be validated.**
   - **The parent-trustpoint argument specifies 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:**

   TOE-common-criteria(ca-trustpoint)# **exit**

4.6.4.8 Setting X.509 for use with IKE

Once X.509v3 keys are installed on the TOE, they can be set for use with IKEv1 with the commands:

TOE-common-criteria (config)#**crypto isakmp policy 1**

TOE-common-criteria (config-isakmp)# **authentication rsa-sig**

or

TOE-common-criteria (config-isakmp)# **authentication ecdsa-sig**

And for IKEv2 with the commands:

TOE-common-criteria (config)#**crypto ikev2 profile sample**

TOE-common-criteria(config-ikev2-profile)#**authentication [remote | local] rsa-sig**

or

TOE-common-criteria(config-ikev2-profile)#**authentication [remote | local] ecdsa-sig**

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

4.6.4.9 Deleting Certificates

If the need arises, certificates that are saved on the router can be deleted. The router saves its own certificates and the certificate of the CA.

To delete the router's certificate from the router's configuration, the following commands can be used in global configuration mode:

Router# **show crypto ca certificates** [*Displays the certificates stored on router*]

Router(config)# **crypto ca certificate chain** *name* [*Enters certificate chain configuration mode*

Router(config-cert-cha)# **no certificate** *certificate-serial-number* [*deletes the certificate*]

To delete the CA's certificate, the entire CA identity must be removed, which also removes all certificates associated with the CA—router's certificate and the CA certificate. To remove a CA identity, the following command in global configuration mode can be used:

Router(config)# **no crypto ca identity** *name* [*Deletes all identity information and certificates associated with the CA*]

4.6.5 Information Flow Policies

The TOE may be configured by the privileged administrators for information flow control/ firewall rules as well as VPN capabilities using the access control functionality. Configuration of information flow policies is restricted to the privileged administrator.

The MOD_VPNGW requires that the TOE be able to support options for information flow policies that include discarding, bypassing, and protecting. On the TOE, an authorized administrator can define the traffic rules on the box by configuring access lists (with permit, deny, and/or log actions) and applying these access lists to interfaces using access and crypto map sets:

- The 'discard' option is accomplished using access lists with deny entries, which are applied to interfaces within access-groups. Guidance for configuration of Access Control Lists is in the *Security Configuration Guide: Access Control Lists.*
- The 'bypassing' option is accomplished using access lists, which are applied to interfaces within crypto maps for IPsec and the 'filter tunnel' command for SSL VPN. If no explicit 'permit' exists within the crypto map, but there is no explicit or implicit deny, then the packet is allowed to bypass the tunnel in plaintext.
- The 'protecting' option is accomplished using access lists with permit entries, which are

applied to interfaces within crypto maps for IPsec and the 'filter tunnel' command for SSL VPN.

The criteria used in matching traffic in all of these access lists includes the source and destination address, and optionally the Layer 4 protocol and port.

The TOE enforces information flow policies on network packets that are receive by TOE interfaces and leave the TOE through other TOE interfaces. When network packets are received on a TOE interface, the TOE verifies whether the network traffic is allowed or not and performs one of the following actions, pass/not pass information, as well as optional logging.

Create an ACL:

```
Router(config)# access-list 100 < deny | permit> ip <source address> <source wildcard bits>
<destination address> <destination wildcard bits>
```

Create crypto map:

```
Router(config)# crypto map <MAP_NAME> isakmp-profile
Router(config-crypto-map)#  set peer 10.0.0.1
Router(config-crypto-map)#  set transform-set SAMPLE_SET
Router(config-crypto-map)#  match address 100
```

Apply the crypto map to an interface:

```
Router(config)# interface GigabitEthernet0/0
Router(config-if)#  crypto map <MAP_NAME>
```

Please refer to the "Cisco IOS Security Command Reference: Commands A to C" for additional information on configuring crypto maps, https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/a1/sec-a1-cr-book.html.

4.6.6 IPsec Session Interruption/Recovery

If an IPsec session with a peer is unexpectedly interrupted, the connection will be broken. In these cases, no administrative interaction is required. The IPsec session will be reestablished (a new SA set up) once the peer is back online.

4.7 Product Updates

Verification of authenticity of updated software is done in the same manner as ensuring that the TOE is running a valid image. See Section 2, steps 7 and 9 above for the method to download and verify an image prior to running it on the TOE.

4.8 Configure Reference Identifier

When certificates are used for authentication, the distinguished name (DN) is verified to ensure the certificate is valid and is from a valid entity. The DN naming attributes in the certificate is compared with the expected DN naming attributes and deemed valid if the attribute types are the same and the values are the same and as expected. The fully qualified domain name (FQDN) can also be used

as verification where the attributes in the certificate are compared with the expected CN: FQDN, CN: user FQDN and CN: IP Address.

This section describes configuration of the peer reference identifier which is achieved through configuring the DN attributes with a certificate map. Certificate maps provide the ability for a certificate to be matched with a given set of criteria. You can specify which fields within a certificate should be checked and which values those fields may or may not have. There are six logical tests for comparing the field with the value: equal, not equal, contains, does not contain, less than, and 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.

Note: SAN is not supported for reference identifiers.

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, you 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 –alt-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.

For example: To create a certificate map for IKEv1 to match four subject-name values of the peer enter:

```
# 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
```

FQDN attributes include the hostname, domain name and IP address:

Configure a hostname:

TOE-common-criteria# **hostname TOE-common-criteria**

Configure a domain name:

TOE-common-criteria# **ip domain-name cisco.com**

Configure an IP address:

TOE-common-criteria(config)#**interface g0/0**
TOE-common-criteria(config-if)#**ip address 10.10.10.110 255.255.255.0**

5. Security Relevant Events

The TOE is able to generate audit records that are stored internally within the TOE whenever an audited event occurs, as well as simultaneously offloaded to an external syslog server. Thedetails for protection of that communication are covered in section 3.3.5 above.

The administrator can set the level of the audit records to be stored in a local buffer, displayed on the console, sent to the syslog server, or all of the above. The details for configuration of these settings are covered in Section 3.3.3 above.

The local log buffer is circular. Newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer.

When configured for a syslog backup the TOE will simultaneously offload events from a separate buffer to the external syslog server. This buffer is used to queue events to be sent to the syslog server if the connection to the server is lost. It is a circular buffer, so when the events overrun the storage space overwrites older events.

The tables below include the security relevant events that are applicable to the TOE. Table 7 General Auditable Events includes general applicable events, and Table 8 Auditable Administrative Events includes auditable events for administrator actions.

Note: *In Table 7, if Embedded Event Manager is used, as outlined in Section 3.3.4, that |%HA_EM-6-LOG logs will be created for each command executed, in addition to the %PARSER- 5-CFGLOG_LOGGEDCMD syslog.*

The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table below). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Additionally, the startup and shutdown of the audit functionality is audited.

The local audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. The audit fields in each audit event will contain at a minimum the following:

Example Audit Event: Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encryption/decryption ... passed)

Date: Nov 19

Time: 13:55:59

Type of event: %CRYPTO-6-SELF_TEST_RESULT

Subject identity: Available when the command is run by an authorized TOE administrator user such as “user: lab”. In cases where the audit event is not associated with an authorized user, an IP address may be provided for the Non-TOE endpoint and/ or TO

Outcome (Success or Failure): Success may be explicitly stated with "success" or "passed" contained within the audit event or is implicit in that there is not a failure or error message.

As noted above, the information includes at least all of the required information. Example audit events are included below:

Additional Audit Information: As described in Column 3 of Table 7 below:

Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test activated by user: lab)

Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software checksum passed)

Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encryption/decryption ... passed)

Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (3DES encryption/decryption ... passed)

Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA hashing ... passed)

Nov 19 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (AES encryption/decryption ... passed)

Table 6 General Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA. Session establishment with peer	Reason for failure. Entire packet contents of packets transmitted/received during session establishment	**Initiation of IPSEC session (outbound):** Jun 20 07:42:26.823: ISAKMP (0): received packet from 100.1.1.5 dport 500 sport 500 Global (N) NEW SA Jun 20 07:42:26.823: ISAKMP: Created a peer struct for 100.1.1.5, peer port 500 Jun 20 07:42:26.823: ISAKMP: New peer created peer = 0x89C3879C peer_handle = 0x8000000C Jun 20 07:42:26.823: ISAKMP: Locking peer struct 0x89C3879C, refcount 1 for crypto_isakmp_process_block Jun 20 07:42:26.823: ISAKMP: local port 500, remote port 500 Jun 20 07:42:26.823: ISAKMP:(0):insert sa successfully sa = 8C1C1FD4 Jun 20 07:42:26.823: ISAKMP:(0):Input = IKE_MESG_FROM_PEER,

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			IKE_MM_EXCH Jun 20 07:42:26.823: ISAKMP:(0):Old State = IKE_READY New State = IKE_R_MM1 ... Jun 20 07:42:26.823: ISAKMP:(0):found peer pre-shared key matching 100.1.1.5 Jun 20 07:42:26.823: ISAKMP:(0): local preshared key found Jun 20 07:42:26.823: ISAKMP : Scanning profiles for xauth ... Jun 20 07:42:26.823: ISAKMP:(0):Checking ISAKMP transform 1 against priority 1 policy Jun 20 07:42:26.827: ISAKMP: encryption AES-CBC Jun 20 07:42:26.827: ISAKMP: keylength of 128 Jun 20 07:42:26.827: ISAKMP: hash SHA Jun 20 07:42:26.827: ISAKMP: default group 14 Jun 20 07:42:26.827: ISAKMP: auth pre-share... Jun 20 07:42:26.843: ISAKMP (0): received packet from 100.1.1.5 dport 500 sport 500 Global (R) MM_SA_SETUP Jun 20 07:42:26.843: ISAKMP:(0):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH Jun 20 07:42:26.843: ISAKMP:(0):Old State = IKE_R_MM2 New State = IKE_R_MM3 Jun 20 07:42:26.843: ISAKMP:(0): processing KE payload. message ID = 0 Jun 20 07:42:27.055: ISAKMP:(0): processing NONCE payload. message ID = 0 Jun 20 07:42:27.059: ISAKMP:(0):found peer pre-shared key matching 100.1.1.5 **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,

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			remote_proxy= 12.1.1.0/255.255.255.0/256/0 Jun 19 21:10:37.575: ISAKMP:(2034):purging node -506111676 .Jun 19 21:10:39.615: ISAKMP:(2034):purging node -22679511 .Jun 20 04:46:14.789: IPSEC(lifetime_expiry): SA lifetime threshold reached, expiring in 1412 seconds **Failure to establish an IPSEC session (outbound-initiated)** Jun 19 11:12:33.905: %CRYPTO-5-IKMP_AG_MODE_DISABLED: Unable to initiate or respond to Aggressive Mode while disabled **IPSEC Failures:** Apr 20 2021 14:02:01.563: IKEv2:(SESSION ID = 4,SA ID = 1):Verify cert failed Apr 20 2021 14:02:01.563: IKEv2:(SESSION ID = 4,SA ID = 1):Auth exchange failed Apr 20 2021 14:02:01.564: IKEv2-ERROR:(SESSION ID = 4,SA ID = 1):: Auth exchange failed
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.3.1	Creation and update of Secure Association Key	Creation and update times	**For SAK (Security Association Key) creation-**

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			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 10000000000000000000000000000000000000000000000000000000000000000
FCS_MACSEC_EXT.4.4	Creation of Connectivity Association	Connectivity Association Key Names	**Creation of Connectivity Association** 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 24AA15376050334AE1EA9BE8A1D0894B00000000000000000000000000000000
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.** GENERIC EXAMPLE: 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

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			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 **SSH initiation** Dec 8 2020 09:57:14.048: %SSH-5-SSH2_USERAUTH: User 'cisco' authentication for SSH2 Session from 192.168.137.3 (tty = 1) using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' Succeeded **SSH termination** Dec 8 2020 09:59:28.155: %SSH-5-SSH2_CLOSE: SSH2 Session from 192.168.137.3 (tty = 1) for user '' using crypto cipher 'aes128-cbc', hmac 'hmac-sha2-256' closed
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
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	See Audit events in FIA_UAU_EXT.2

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).	**Login as an administrative user at the console:** Username: auditperson Password: 000278: *Apr 23 07:11:56: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: auditperson] [Source: 0.0.0.0] [localport: 0] at 07:11:56 UTC Thu Apr 23 2009? **Failed login via the console does not allow any actions:** Username: auditperson Password: % Authentication failed Username: 000254: *Apr 26 00:45:43.340: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: auditperson] [Source: 0.0.0.0] [localport: 0] [Reason: Login Authentication Failed] at 23:45:43 a Sat Apr 25 2009 See FCS_SSH_EXT.1 for remote login audit events.
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 Session establishment with CA	Reason for failure Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store Entire packet contents of packets transmitted/r	**Session establishment with CA:** 42479: Initiator SPI : 6038B31E75BFF128 - Responder SPI : ECB6C134F5652076 Message id: 1 42478: *Feb 5 11:10:18.749: IKEv2:(SA ID = 1):Sending Packet [To 210.1.1.1:500/From 110.1.1.1:500/VRF i0:f0]42442: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):[PKI -> IKEv2] Getting of cert chain for the trustpoint PASSED 42441: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Getting cert chain for the trustpoint rahul 42440: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):[PKI -> IKEv2] Retrieved trustpoint(s): 'rahul' 42439: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):[IKEv2 -> PKI] Retrieving trustpoint(s) from received certificate hash(es) 42438: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message 42437: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):Verify SA init message

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
		eceived during session establishment	42436: *Feb 5 11:10:18.747: IKEv2:(SA ID = 1):Processing IKE_SA_INIT message 42435: SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED) **Unsuccessful attempt to validate a certificate:** Aug 3 19:10:18.621: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 04) is revoked **Replacement of trust anchors:** Sep 18 11:38:06.256: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named cryptokeytest has been generated or imported by crypto-engine
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.	Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade
FMT_MOF.1/Services	Starting and stopping of Services	None.	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
FMT_SMF.1	All management activities of TSF data	None.	**Resetting of passwords:** Nov 21 2017 15:06:53.679: \%PARSER-5-CFGLOG_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

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			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 **Crypto keys (generating and deleting):** Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto key generate Feb 17 2013 16:37:27: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key zeroize See all other records in Table 8 “Auditable Administrative Events”.
FPF_RUL_EXT.1	Application of rules configured with the ‘log’ operation	Source and destination addresses Source and destination ports Transport Layer Protocol TOE Interface	**ACL Configuration:** Aug 6 10:53:48 toe-loopback 327: *Aug 6 2018 10:53:47.403: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:ip access-list extended FPF_RUL_EXT.1-deny Aug 6 10:53:48 toe-loopback 328: *Aug 6 2018 10:53:47.572: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:deny icmp 10.22.0.203 0.0.0.0 10.21.0.101 0.0.0.0 log Aug 6 10:53:48 toe-loopback 329: *Aug 6 2018 10:53:47.748: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:permit icmp 10.22.0.203 0.0.0.0 10.21.0.101 0.0.0.0 log Aug 6 10:53:48 toe-loopback 330: *Aug 6 2018 10:53:47.878: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:interface GigabitEthernet0/0/1 Aug 6 10:53:48 toe-loopback 331: *Aug 6 2018 10:53:48.010: \%PARSER-5-CFGLOG_LOGGEDCMD: User:script logged command:ip

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			access-group FPF_RUL_EXT.1-deny in **Packets denied by ACL:** Aug 6 10:53:54 toe-loopback 335: *Aug 6 2018 10:53:53.601: \%FMANFP-6-IPACCESSLOGDP: R0/0: fman_fp_image: list FPF_RUL_EXT.1-deny denied icmp 10.22.0.203 -> 10.21.0.101 (0/0), 1 packet Aug 6 10:53:54 toe-loopback 336: *Aug 6 2018 10:53:53.853: \%FMANFP-6-IPACCESSLOGDP: R0/0: fman_fp_image: list FPF_RUL_EXT.1-deny denied icmp 10.22.0.203 -> 10.21.0.101 (0/0), 1 packet Aug 6 10:53:54 toe-loopback 337: *Aug 6 2018 10:53:54.104: \%FMANFP-6-IPACCESSLOGDP: R0/0: fman_fp_image: list FPF_RUL_EXT.1-deny denied icmp 10.22.0.203 -> 10.21.0.101 (0/0), 1 packet
	Indication of packets dropped due to too much network traffic	TOE interface that is unable to process packets	*May 6 04:04:28.279: %HA_EM-6-LOG: test2: value GigabitEthernet0/2 output_packets_dropped increased from 1058406890 to 1061078215
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success	**Local Clock Update:** CLOCKUPDATE: System clock has been updated from 06:11:37 EDT Mon Dec 20 2010 to 06:10:00 EDT Tue Dec 20 2011, configured from console by user on console.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
		and failure (e.g., IP address).	
FPT_RPL.1	Detected replay attempt	None.	*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
FPT_TST_EXT.3	Failure of self-test Indication that TSF self-test was completed	Reason for failure (including identifier of invalid certificate)	Validating dev_mode signature dev_mode validation failed for token 0006F66C59BF dev_mode is PRIV Unsupported package header version (0) Failed to boot file bootflash:images/c2960s-universalk9-mz.152-1.E1.bin ..... autoboot: boot failed, restarting...
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.	**Use of the "upgrade" command:** *Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade *Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:copy tftp .... *Jul 10 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:reload **Update Failure:** autoboot: boot failed, restarting...
FTA_SSL_EXT.1	The termination of a local session by the session locking	None.	001383: May 10 18:06:34.091: %SYS-6-EXEC_EXPIRE_TIMER: (tty 0 (0.0.0.0)) exec-timeout timer expired for user securityperson 001384: May 10 18:06:34.091: %SYS-6-EXIT_CONFIG: User securityperson has exited tty session 0(0.0.0.0)

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	mechanism.		
FTA_SSL.3	The termination of a *remote* session by the session locking mechanism.	None.	**Audit record generated when SSH session is terminated because of idle timeout:** May 29 2012 15:18:00 UTC: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin
FTA_SSL.4	The termination of an interactive session.	None.	**Audit record generate when admin logs out of CONSOLE:** May 17 2011 16:29:09: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:exit **Audit record generated when the admin logs out of SSH:** Jun 18 11:17:36.653: SSH0: Session terminated normally
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 logs provided by FCS_IPSEC_EXT.1.
FTP_TRP.1/Admin	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	None.	See logs provided by FCS_SSH_EXT.1

Table 7 Auditable Administrative Events

Requirement	Management Action to Log	Sample Log
FAU_GEN.1: Audit data generation	Changing logging settings. Clearing logs.	Feb 17 2013 16:29:07: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:logging enable Feb 17 2013 16:34:02: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:logging informational Feb 17 2013 17:05:16: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:clear logging
FAU_GEN.2: User identity association	None	N/A
FAU_STG_EXT.1: External audit trail storage	Configuration of syslog export settings	Feb 17 2013 17:05:16: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:logging host
FCS_CKM.1: Cryptographic key generation (for asymmetric keys)	Manual key generation	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key ***** Jan 24 2013 03:10:08.878: %GDOI-5-KS_REKEY_TRANS_2_UNI: Group getvpn transitioned to Unicast Rekey.ip
FCS_CKM_EXT.4: Cryptographic key zeroization	Manual key zeroization	Feb 17 2013 16:37:27: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command:crypto key zeroize

Requirement	Management Action to Log	Sample Log
FCS_COP.1/DataEncryption: Cryptographic operation (for data encryption/decryption)	None	N/A
FCS_COP.1/SigGen: Cryptographic operation (for cryptographic signature)	None	N/A
FCS_COP.1/Hash: Cryptographic operation (for cryptographic hashing)	None	N/A
FCS_COP.1/KeyedHash: Cryptographic operation (for keyed-hash message authentication)	None	N/A
FCS_RBG_EXT.1: Cryptographic operation (random bit generation)	None	N/A
FCS_IPSEC_EXT.1	Configuration of IPsec settings: including mode, security policy, IKE version, algorithms, lifetimes, DH group, and certificates.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto isakmp policy 1
FCS_SSH_EXT.1	Configuration of SSH settings: including certificates or passwords, algorithms, host names, users.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: ip ssh version 2

Requirement	Management Action to Log	Sample Log
FIA_AFL.1	Configuring number of failures. Unlocking the user. Administrator lockout due to excessive authentication 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] Feb 7 2013 02:05:41.953: %AAA-5-USER_UNLOCKED: User user unlocked by admin on vty0 (21.0.0.1)
FIA_PMG_EXT.1: Password management	Setting length requirement for passwords.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: security passwords min-length 15
FIA_PSK_EXT.1: Pre-Shared Key Composition	Creation of a pre-shared key.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: crypto isakmp key *****
FIA_UIA_EXT.1: User identification and authentication	Logging into TOE.	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
FIA_UAU_EXT.2: Password-based authentication mechanism	None	N/A
FIA_UAU.7: Protected authentication feedback	None	N/A

Requirement	Management Action to Log	Sample Log
FIA_X509_EXT.1/Rev: X.509 Certificates	Generating a certificate.	Feb 17 2013 16:14:47: %PARSER-5-CFGLOG_LOGGEDCMD: User:test_admin logged command: crypto key generate
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate: Management of Security Functions Behavior	See all other rows in table.	N/A
FMT_MTD.1/CoreData: Management of TSF data (for general TSF data)	See all other rows in table.	N/A
FMT_SMF.1: Specification of management functions	See all other rows in table.	N/A
FMT_SMR.2: Restrictions on Security roles	Configuring administrative users with specified roles.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: username admin 15
FPT_RUL_EXT.1: Packet Filtering	Configuring packet filtering rules.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: access-list 199 deny ip 10.100.0.0 0.0.255.255 any log-input
FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)	None	N/A

Requirement	Management Action to Log	Sample Log
FPT_APW_EXT.1: Protection of Administrator Passwords	None	N/A
FPT_STM_EXT.1: Reliable time stamps	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: Trusted update	Software updates	Jul 10 2013 11:04:09.179: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command:upgrade
FPT_TST_EXT.1: TSF testing	None	N/A
FTA_SSL_EXT.1: TSF-initiated session locking	Specifying the inactivity time period.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exec-timeout 60
FTA_SSL.3: TSF-initiated termination	Specifying the inactivity time period.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exec-timeout 60
FTA_SSL.4: User-initiated termination	Logging out of TOE.	Feb 15 2013 13:12:25.055: %PARSER-5-CFGLOG_LOGGEDCMD: User:cisco logged command: exit

Requirement	Management Action to Log	Sample Log
FTA_TAB.1: Default TOE access banners	Configuring the banner displayed prior to authentication.	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: Inter-TSF trusted channel	None	N/A
FTP_ITC.1/VPN: Inter-TSF trusted channel	None	None
FTP_TRP.1/Admin: Trusted path	Connecting to the TOE with SSH.	Jan 17 05:05:49.460: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: Cisco] [Source: 21.0.0.3] [localport: 22] at 00:05:49 EST Thu Jan 17 2013

5.1 Managing Audit Records

The TOE provides the privileged Administrator the ability to manage local audit records stored within the TOE. Audit logging is enabled by default on the TOE.

Configuring the audit log severity level is done with the **logging buffered** command.

Router(config)# **logging buffered <0-7>**

Severity levels:

1 – Alerts
2 – Critical
3 – Errors
4 – Warnings
5 – Notifications
6 – Informational
7 – Debugging

Viewing the audit log is done with the **show logging** command.

```
Router# show logging
```

Clearing the audit log is done with the **clear logging** command.

```
Router# clear logging
```

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 of which run as system-level processes. The table indicates whether each service or protocol is allowed to be used in the certified configuration.

For more detail about each service, including whether the service is limited by firewall mode (routed or transparent), or by context (single, multiple, system), refer to the ***Command Reference*** guides listed in Table 2.

Table 8 Protocols and Services

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
AH	Authentication Header (part of IPsec)	Yes	Yes	Yes	Yes	No restrictions. ESP must be used in all IPsec connections. Use of AH in addition to ESP is optional. Protocol is not considered part of the evaluation.
DHCP	Dynamic Host Configuration Protocol	Yes	Yes	Yes	Yes	No restrictions. Protocol is not considered part of the evaluation.
DNS	Domain Name Service	Yes	Yes	No	n/a	No restrictions. Protocol is not considered part of the evaluation.
ESP	Encapsulating Security Payload (part of IPsec)	Yes	Yes	Yes	Yes	Configure ESP as described in the section 4.6.1 of this document.
FTP	File Transfer Protocol	Yes	No	No	n/a	Use tunneling through IPsec
ICMP	Internet Control Message Protocol	Yes	Yes	Yes	Yes	No restrictions. Protocol is not considered part of the evaluation.
IKE	Internet Key Exchange	Yes	Yes	Yes	Yes	As described in section 4.6.1 of this document.

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
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 ASA, not for "VPN Gateway" functionality to secure traffic through the ASA. 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 ASA administrators, tunnel this authentication protocol secure with IPsec.
RADIUS	Remote Authentication Dial In User Service	Yes	Yes	No	n/a	If used for authentication of ASA administrators, secure through IPsec.
SDI (RSA SecureID)	RSA SecurID authentication	Yes	Over IPsec	No	n/a	If used for authentication of ASA 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	Yes	Yes	Yes	As described in the section 3.3.1 of this document.
Telnet	A protocol used for terminal emulation	Yes	No	Yes	No	Use of SSH is recommended.
TFTP	Trivial File Transfer Protocol	Yes	Yes	No	n/a	Recommend using SC instead or tunneling through IPsec. Protocol is not considered part of the evaluation.
CDP	Cisco Discovery Protocol	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
DTP	Dynamic Trunking Protocol	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
Frame Relay	Standardized wide area network technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
HDLC	High-Level Data Link Control	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
L2F	Layer 2 Forwarding	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
L2TP	Layer 2 Tunneling Protocol	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
STP	Spanning Tree Protocol	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
VTP	VLAN Trunking Protocol	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
PPPoE	Point-to-point protocol over Ethernet	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
Token Ring	Data Link layer Protocol	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
BGP	Border Gateway Protocol	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
MP-BGP	Multiprotocol BGP	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
OSP	Open Shortest Path First	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
EIGRP	Enhanced Interior Gateway Routing Protocol	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
RIP	Routing Information Protocol	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols
IS-IS	Intermediate system to intermediate system	n/a	n/a	n/a	n/a	Follow best practices for the secure usage as there are no restrictions on use of these protocols

Note: The table above does not include the types of protocols and services listed here:

- OSI Layer 2 protocols such as CDP, VLAN protocols like 802.11q, Ethernet encapsulation protocols like PPPoE, etc. The certified configuration places no restrictions on the use of these protocols; however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation. Follow best practices for the secure usage of these services.
- Routing protocols such as EIGRP, OSPF, and RIP. The certified configuration places no restrictions on the use of these protocols, however evaluation of these protocols was beyond the scope of the Common Criteria product evaluation, so follow best practices for the secure usage of these protocols.

7. Modes of Operation

An IOS-XE router has several modes of operation, these modes are as follows:

Booting – while booting, the routers drop all network traffic until the router image and configuration has loaded. This mode of operation automatically progresses to the Normal mode of operation. During booting, 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 Booting mode is referred to in the IOS guidance documentation as "ROM Monitor Initialization". Additionally if the Router does not find a valid operating system image it will enter ROM Monitor mode and not normal mode therefore protecting the router from booting into an insecure state.

Normal – The IOS router image and configuration is loaded, and the router is operating as configured. It should be noted that all levels of administrative access occur in this mode and that all router based security functions are operating. While operating the router have little interaction with the administrator. However, the configuration of the router can have a detrimental effect on security. Misconfiguration of the router could result in the unprotected network having access to the internal/protected network.

ROM Monitor – This mode of operation is a maintenance, debugging, and disaster recovery mode. While the router is in this mode, no network traffic is routed between the network interfaces. In this state the router may be configured to upload a new boot image from a specified TFTP server, perform configuration tasks and run various debugging commands. It should be noted that while no administrator password is required to enter ROM monitor mode, physical access to the router is required; therefore, the router should be stored in a physically secure location to avoid unauthorized access which may lead to the router being placed in an insecure state.

Following operational error, the TOE reboots (once power supply is available) and enters booting mode. The only exception to this is if there is an error during the Power on Startup Test (POST) during bootup, then the TOE will shut down. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen and saved in the crashinfo file. Within the POST, self-tests for the cryptographic operations are performed. The same cryptographic POSTs can also be run on-demand as described in section 3.2.3, and when the tests are run on-demand after system startup has completed (and the syslog daemon has started), error messages will be written to the log.

All ports are blocked from moving to forwarding state during the POST. Only when all components of all modules pass the POST is the system placed in FIPS PASS state and ports are allowed to forward data traffic.

POST tests include:

- 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 to ensure that the encrypt operation is working correctly. 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 to ensure that the decrypt operation is working correctly.

- 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 to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.

- 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 to ensure that the DRBG is operating correctly.

- 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 to verify that the HMAC and hash operations are operating correctly.

- SHA-1/256/384/512 Known Answer Test –

For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match, and the hash operations are operating correctly.

- ECDSA self-test –

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 to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly.

- 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 integrity of stored TSF executable code when it is loaded for execution can be verified through the use of RSA and Elliptic Curve Digital Signature algorithms.

If any of the POST fails, the following actions should be taken:

- If possible, review the crashinfo file. This will provide additional information on the cause of the crash.
- Restart the TOE to perform POST and determine if normal operation can be resumed.
- 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.

If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated.

Example Error Message:
*Nov 26 16:28:23.629: %CRYPTO-0-SELF_TEST_FAILURE: Encryption self-test failed

If a software upgrade fails, the router will display an error when an authorized administrator tries to boot the system. The router will then boot into the rommon prompt.

```
Directory an_image.bin not  found
Unable to locate an_image.bin  directory
Unable to load an_image.bin
boot: error executing "boot  harddisk:an_image.bin"
autoboot: boot failed,  restarting
```

Autoboot has been enabled by using the **config-register 0x2102** command. The following error message is displayed when the router restarts automatically:

```
no valid BOOT image found
Final autoboot attempt from  default boot device...
Located l2tp_rmcd_alg
Image size 10271 inode num 12,  bks cnt 3 blk size 8*512
#
Boot image size = 10271  (0x281f) bytes
.
.
.
Boot image size = 11262  (0x2bfe) bytes
Unknown image structure
Located test
Image size 11506 inode num 63,  bks cnt 3 blk size 8*512
```

Pressing the Break key or running the “break” command will cause the router to enter rommon mode.

8. Security Measures for the Operational Environment

Proper operation of the TOE requires functionality from the environment. It is the responsibility of the authorized administrator of the TOE to ensure that the Operational Environment provides the necessary functions and adheres to the environment security objectives listed below. The environment security objective identifiers map to the environment security objectives as defined in the Security Target.

Table 9 Operational Environment Security Measures

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
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. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
~~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.~~
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
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.
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.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual

Environment Security Objective	IT Environment Security Objective Definition
	information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.CONNECTIONS	TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

9. 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.

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com.

9.1 Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click Feedback in the toolbar and select Documentation. After you complete the form, click Submit to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

9.2 Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at any time, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

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

http://www.cisco.com