Cisco Embedded Services Router (ESR) 6300 v17.12

Common Criteria Configuration Guide

Version: 1.0
Date: May 30, 2024

Table of Contents

List of Tables

List of Figures

List of Acronyms

The following acronyms and abbreviations are used in this document:

Table 1 Acronyms

Acronyms/Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
AGD	Guidance Document
AH	Authentication Header
BGP	Border Gateway Protocol
BTB	Board-to-Board
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CLI	Command-Line Interface
CM	Configuration Management
CN	Common Name
CS	Certificate Server
CSfC	Commercial Solutions for Classified
CON	Conduction Cooled
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DRAM	Dynamic random access memory
DSS	Digital Signature Standard
eMMC	Embedded MultiMediaCard
ESP	Encapsulating Security Payload
ESR	Embedded Services Router
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure

IC2M	IOS Common Cryptographic Module
IEC	International Electrotechnical Commission
IKE	Internet Key Exchange
IOS	Internetwork Operating System
IPsec	Internet Protocol (IP) secure (sec)
ISO	International Organization for Standardization
IT	Information Technology
LAN	Local Area Network
NCP	No Cooling Plater
NDcPP	Network Device collaborative Protection Profile
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NIT	Network Device iTC Interpretation Team
NTP	Network Time Protocol
NVRAM	Non-Volatile Random-Access Memory
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OSP	Organizational Security Policies
OSPF	Open Shortest Path First
PoE	Power over Ethernet
POST	Power on Startup
PKI	Public Key Infrastructure
PP	Protection Profile
PPK	Post-Quantum Preshared Keys
RBG	Random Bit Generator
RFC	Request For Comments
SA	Security Association
SAR	Security Assurance Requirements
SCEP	Simple Certificate Enrollment Protocol
SFP	Small–Form-factor Pluggable port
SFR	Security Functional Requirement
SHS	Secure Hash Standard
SKP	Signing Key Pair
SPD	Security Policy Definition
SSH	Secure Shell

SSL	Secure Sockets Layer
ST	Security Target
TAC	Technical Assistance Center
TCP	Transmission Control Protocol
TD	Technical Decision
TOE	Target of Evaluation
TSC	Target of Evaluation Security Function Scope of Control
TSF	Target of Evaluation Security Function
TSP	Target of Evaluation Security Policy
UART	Universal Asynchronous Receiver Transmitter
UDP	User Datagram Protocol
WAN	Wide Area Network
VM	Virtual Machine
vND	virtual Network Device
VPN	Virtual Private Network
VS	Virtualisation System
VTI	Virtual Tunnel Interface

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 Embedded Services Router (ESR) 6300. 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 Embedded Services Router (ESR) 6300), the TOE, as it was certified under Common Criteria. The Cisco Embedded Services Router (ESR) 6300 may be referenced below as the ESR6300, 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 ESR6300 operations. All security relevant commands to manage the TSF data are provided within this documentation within each functional section.

1.3 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 ESR6300. The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 17.12. In addition, the software image is also downloadable from the Cisco web site.

The ESR6300 can be inserted into an optional enclosure to provide physical protection for the TOE itself if required by the end user. The TOE is self-contained and does not rely on the ESR6300 enclosure for any ports or connections. The TOE includes a fully integrated multi-pin BTB interface connector that provides pins dedicated for power input, ethernet ports, and console ports which enable the connections to external devices. The enclosure needs to accommodate the TOE's size (3.0 x 3.775 in.) and provides no computational services. In addition, the ESR6300 enclosure does not provide any access points that would interfere with the security functions provided by the TOE in the evaluated configuration.

1.4 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 2 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.
Remote VPN 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.
NTP Server	Yes	The TOE supports communications with an NTP Server in order to synchronize the date and time for a reliable timestamp on the TOE.
Router Enclosure	No	The end user can opt to use an enclosure that can accommodate the TOE's size (3.0 x 3.775 in.) and provides no compute capabilities. The ND functionality is implemented inside the ESR 6300 physical chassis, as the chassis includes the underlying board (with or without a cooling plate) and all electronic components attached to it; therefore, no computational capabilities outside of the TOE boundary are required to secure the TOE. During testing, the TOE was enclosed within a Cisco developed hardened enclosure. It is a specially designed enclosure used for Cisco internal testing purposes only. It has no compute capabilities and is not a commercially available product. The enclosure passes network connections directly to the TOE interfaces and does not change or modify TSF functionality. In the evaluated configuration, the enclosure used for testing contains the ESR6300 board including the integrated multi-pin BTB interface connector with pins dedicated for power input, ethernet ports, and console ports (two combo Gigabit Ethernet WAN ports, four Gigabit Ethernet LAN ports, and one UART RS232 RJ-45 console port). Refer to Annex A in the Guidance Document (AGD) for hardware technical guidance including ESR6300 board layout, dimensions, and multi-pin BTB interface connector details with pinout mappings and descriptions for network interfaces and power inputs.

1.5 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 3 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 and MOD_VPNGW_v1.3.

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. Ifit 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 The TOE must be deployed in a manner consistent with the CC evaluated configuration in which the TOE's BTB connector is attached to a compatible interface as described in Annex A: Technical Hardware Guidance.

Step 8 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 http://www.cisco.com/techsupport.
- The TOE ships with the correct software images installed, however this may not be the evaluated version.

Step 9 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 4 below. If the SHA-512 hashes do not match, contact Cisco Technical Assistance Center (TAC), http://www.cisco.com/techsupport.

Once the file has been copied, it is recommended that you read and familiarize yourself with the *Configuration Fundamentals Configuration Guide, Cisco ESR6300 Series Router Software Configuration Guide*, and the *Release Notes for the Cisco ESR6300* before proceeding with the installation and configuration of the TOE.

Step 10 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.

CC-TOE# 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), http://www.cisco.com/techsupport.

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...
```

For additional information about the 'show software authenticity' commands, refer to the Loading and Managing System Images Configuration Guide.

Step 11 To install and configure the ESR6300 follow the instructions as described in the *Configuration Fundamentals Configuration Guide*.

After powering on your ESR6300, confirm that the TOE loads the image correctly, completes internal self-checks and displays the cryptographic export warning on the console.

Step 12 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 4 Evaluated Software Images

Platform	Image Name
ESR6300	c6300-universalk9.17.12.2.SPA.bin

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

Follow the Cisco Embedded Service 6300 Series Router Hardware Technical Guide for hardware installation instructions.

3.2 Initial Setup via Direct Console Connection

The ESR6300 must be given basic configuration via console connection prior to being connected to any network.

3.2.1 Options to be chosen during the 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. The *Configuration Fundamentals Configuration Guide* describes how to use Setup Mode to build a basic configuration and to make configurationchanges. 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 switch 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.

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:

```
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:

```
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 ESR6300 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:

```
CC-TOE(config)# service password-encryption
```

Configures local AAA authentication:

```
CC-TOE(config)# aaa authentication login default local
CC-TOE(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:

```
CC-TOE(config)# username <name> password <password>
```

to create a new username and password combination, and

```
CC-TOE(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

```
CC-TOE(config)# line vty <first> <last>

CC-TOE(config-line)# exec-timeout <time>

CC-TOE(config-line)# line console
CC-TOE(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 CC-TOE(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

The TOE provides remote administration using SSH. The steps below provide instructions to configure SSH Server for the CC evaluated configuration.

3.3.1 Remote Administration Protocols

3.3.1.1 Steps to configure SSH on router

1. Configure a hostname:
   ```
   CC-TOE# hostname CC-TOE
   ```

2. Configure a domain name:
   ```
   CC-TOE# ip domain-name cisco.com
   ```

3. Generate RSA – choose a longer modulus length for the evaluated configuration (i.e., 2048):

```
CC-TOE(config)# crypto key generate rsa
        How many bits in the modulus [2048]: 2048

CSfC configuration requires 3072 bits:
CSfC-TOE(config)# crypto key generate rsa
        How many bits in the modulus [2048]: 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 (this will also deny use of SSHv1):

```
CC-TOE(config)# ip ssh version 2
```

5. Configure –SSH timeout:

```
CC-TOE(config)# # ip ssh time-out < time in minutes >
```

6. Configure SSH retries:

```
CC-TOE(config)# # ip ssh authentication-retries 2
```

7. Configured SSH server key exchange using the following commands:

```
CC-TOE(config)# ip ssh dh min size 2048
CC-TOE(config)# ip ssh server algorithm kex <diffie-hellman-group14-sha1 | ecdh-sha2-nistp384 >

CSfC configuration requires 4096 bits and ecdh-sha2-nistp384
CSfC-TOE(config)# ip ssh dh min size 4096
CSfC-TOE(config)# ip ssh server algorithm kex ecdh-sha2-nistp384
```

8. Configure vty lines to accept 'ssh' login services:

```
CC-TOE(config-line)# line vty 0 15
CC-TOE(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, AES-CBC-256 and aes256-gcm@openssh.com encryption key algorithms. To set, use the following command:

   ```
   CC-TOE(config)# ip ssh server algorithm encryption aes128-cbc aes256-cbc aes256-gcm@openssh.com
   ```

   CSfC configuration requires only aes256-gcm@openssh.com:

   ```
   CSfC-TOE(config)# ip ssh server algorithm encryption aes256-gcm@openssh.com
   ```

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

```
CC-TOE(config)# ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512 implicit
```

CSfC configuration requires only implicit for aes256-gcm@openssh.com:

```
CC-TOE(config)# ip ssh server algorithm mac implicit
```

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 ip 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 for more information*.

15. Configure Host Key Algorithms

```
ROUTER(config)# ip ssh server algorithm hostkey < rsa-sha2-256 | rsa-sha2-512>
```

16. The administrator needs to configure the Router for SSH public key authentication. This is necessary to avoid a potential situation where password failures by remote Administrators lead to no Administrator access for a temporary period of time. During the defined lockout period, the Router provides the ability for the Administrator account to login remotely using SSH public key authentication.

    Before proceeding, please have the SSH public key ready for use. The public key is generated from your SSH client on the Management workstation.

    a. Configure Algorithm for SSH public-key based authentication

    ```
    ROUTER(config)# ip ssh server algorithm publickey < rsa-sha2-256 | rsa-sha2-512>
    ```

    b. Enter public-key configuration mode

    ```
    ROUTER(config)# ip ssh pubkey-chain
    ```

    c. Specify the admin user account to configure for SSH public key authentication

    ```
    ROUTER(conf-ssh-pubkey-user)# username admin
    ```

    d. Enter public-key data configuration mode

    ```
    ROUTER(conf-ssh-pubkey-user)# key-string
    ```

    e. Paste the data portion of the public key generated from the SSH client. **Note:** If necessary, you may split the key into multiple lines.

    ```
    ROUTER(conf-ssh-pubkey-data)# <paste your public key>
    ```

    f. Return to configuration mode by entering exit 3 times:

    ```
    ROUTER(conf-ssh-pubkey-data)# exit
    ROUTER(conf-ssh-pubkey-user)# exit
    ROUTER(conf-ssh-pubkey)# exit
    ```

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 Disable Unused Protocols

The following remote management protocols (HTTP, HTTPS, SNMP) were not tested in the evaluated configuration and must be disabled:

```
ROUTER(config)# no ip http server
```

```
ROUTER(config)# no ip http secure-server

ROUTER(config)# no snmp-server
```

3.3.3 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.

Example configuration:

```
CC-TOE(config)#radius server <server name>

CC-TOE(config-radius-server)#address ipv4 <ip-address> auth-port 1812 acct-port 1813

CC-TOE(config-radius-server)#key 7 <hidden key>

CC-TOE(config-radius-server)#aaa authentication login default group radius local

CC-TOE(config-radius-server)#aaa authorization exec default group radius local

CC-TOE(config)#ip radius source-interface Loopback1
```

Refer to the *RADIUS Configuration Guide* for more information.

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 3.3.5 below.

3.3.4 Logging Configuration

1. Logging of command execution must be enabled:

```
CC-TOE(config)#archive
CC-TOE(config)#no logging console
CC-TOE(config-archive)#log config
CC-TOE(config-archive-log-cfg)#logging enable
CC-TOE(config-archive-log-cfg)#hidekeys
CC-TOE(config-archive-log-cfg)#notify syslog
CC-TOE(config-archive-log-cfg)#exit
CC-TOE(config-archive)#exit
```

2. Add year to the timestamp:

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

3. Enable any required debugging. Debugging is needed for radius (if used), isakmp (if using ikev1) 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:

```
CC-TOE# debug radius authentication
CC-TOE# debug crypto ipsec
```

```
CC-TOE# debug crypto ikev2
CC-TOE# debug crypto pki server
```

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

```
CC-TOE(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:

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

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

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

Ex. CC-TOE(config)#logging host 192.168.202.169
```

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:

```
CC-TOE(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.

```
CC-TOE(config)# logging history <level>

CC-TOE(config)# logging history size <number>
```

3.3.5 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.

3.3.6 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 co 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.

Note: CSfC configuration requires the use of IKEv2. See section 4.6.1 IPSec Overview.

3.3.6.1 Syslog over IPsec

IPsec is used by the TOE to securely transmit generated audit data to an external syslog server. The steps below provide instructions to configure an IPsec Virtual Tunnel Interface (VTI).

1. Enable priviledged EXEC mode:

```
Router> enable
```

2. enter global configuration mode:

```
Router# configure terminal
```

3. Configure transform set:

```
Router(config)# crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
   mode tunnel
```

4. Configure IPsec profile:

```
Router(config)# crypto ikev2 profile PROF
   match identity remote address 192.0.2.2 255.255.255.255
   authentication remote pre-share key <KEY>
   authentication local pre-share key <KEY>
  lifetime 86400
!
Router(config)# crypto ipsec profile PROF
   set transform-set TSET
   set ikev2-profile PROF
```

5. Configure interface:

```
Router(config)# interface GigabitEthernet0/0/0
   ip address 192.0.2.1 255.255.255.
```

6. Configure IPsec VTI:

   ```
   Router(config)# interface Tunnel0
     ip address 100.0.2.1 255.255.255.252
     tunnel source GigabitEthernet0/0/0
     tunnel mode ipsec ipv4
     tunnel destination 192.0.2.2
     tunnel protection ipsec profile PROF
   ```

7. Configure logging with the syslog server IP address and subnet mask:

   ```
   Router(config)# logging host 192.3.3.3
   Router(config)# logging source-interface Tunnel0
   ```

8. Configure route to the Syslog server:

   ```
   Router(config)# ip route 192.0.2.0 255.255.255.0 Tunnel0
   ```

Verify IPsec VTI with the following commands:

```
Router# show crypto session
Router# show interface tunnel0
Router# show ip route
```

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

3.3.7 Base Firewall Rule Set Configuration

The Network Device PP VPN Gateway Module 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 8200)
- TCP (RFC 793)
- UDP (RFC 768)
- IKEv1(RFCs2407,2408,2409,RFC4109)
- IKEv2 (RFC 5996)
- IPsec ESP (RFCs 4301, 4303)
- SSH(RFCs4251,4252,4253,,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 VPN GW Module 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, tunnel protection ipsec policy, and access-group.

Access lists must be configured on the TOE to meet the requirements of the VPN Gateway Module.

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.

```
CC-TOE# configure terminal

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

CC-TOE(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:

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

CC-TOE(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:

```
CC-TOE(config)# access-list 100 deny 132 any any log-input

CC-TOE(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:

```
CC-TOE(config)# access-list 100 deny any any log-input

CC-TOE(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:

```
CC-TOE(config)# interface GigabitEthernet0/0
CC-TOE(config-if)# ip access-group 199 in

CC-TOE(config)# interface GigabitEthernet0/1
```

```
CC-TOE(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.

3.3.8 Routing Protocols

The routing protocols are used to maintain routing tables. The routing tables can also be configured and maintained manually. Refer to the applicable sections for configuration of the routing protocols in the *Cisco ESR6300 Series Router Software Configuration Guide*.

4. Secure Management

4.1 User Roles

The ESR6300 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.

```
CC-TOE(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.

```
CC-TOE(config)# no username name
```

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

It is recommended to create a unique username and password for each user who will be accessing the TOE. This is also recommended for administrative accounts, rather than using one shared administrator account.

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.

   ```
   CC-TOE (config)#security passwords min-length length
   ```

   Example: CC-TOE (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: CC-TOE (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.

CC-TOE (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.

CC-TOE (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:

CC-TOE(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:

CC-TOE(config)#enable secret [level *level*] {*password* | 0 | 4 | 5 [*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.

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].

```
CC-TOE (config)# password encryption aes
CC-TOE (config)# key config-key password-encryption [text]
```

4.3 Clock Management

In the evaluated configuration, the TOE must support time synchronization with an NTP server. In addition, the TOE must be able to support configuration with at least three (3) NTP servers.

The following NTP commands are used to ensure logging of the NTP services are generated, the NTP server is identified and that NTP version 4 is being used.

```
router(config)# ntp logging
router(config)# ntp server 192.168.10010 version 4
```

By default, NTP broadcast is disabled. Clock management is restricted to the privileged administrator. Note that the TOE will not respond to broadcast & multicast NTP traffic.

NTP does not rely on a persistent connection with the time server. It does rely on an IPSec session with the time server, which is persistent. Recovery from an event where the IPSec connection is unintentionally broken is the same as that described in section 3.3.5.2 Syslog Server Adjacent to an IPsec Peer.

4.4 Identification and Authentication

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

The ESR6300 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:

```
CC-TOE (config)# 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.

These tunnels are sets of security associations (SAs) that are establishedbetween 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 (ESP).

With IPsec, privileged administrators can define the traffic that needs to be protected between two IPsec peers by configuring an IPsec VTI, an access lists and then applying the access list to the IPsec VTI. 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.)

The access list entries are searched in a sequence--the router attempts to match the packet to the access list specified in that entry, for example:

- The ‘discard’ option is accomplished using access lists with deny entries, which are applied to interfaces within access-groups.
- The ‘bypassing’ option is accomplished using access lists with deny entries, which are applied to interfaces.
- The ‘protecting’ option is accomplished using access lists with permit entries, which are applied to interfaces.

When a packet matches a permit entry in a particular access list, and the corresponding VTI, connections are established, if necessary. If the access list entry is tagged in the IPsec VTI, 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 IPsec VTI 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 the IPsec VTI also represent the traffic that the router needs protected by IPsec. Inbound traffic is processed against an access list--if an unprotected packet matches a permit entry in a particular access list associated with an IPsec VTI, that packet is dropped because it was not sent as an IPsec-protected packet.

The IPsec VTI also includes a specified transform set. 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 an IPsec VTI. The transform set defined in the IPsec VTI is used in the IPsec SA negotiation to protect the data flows specified by that IPsec VTI'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:

```
CC-TOE # conf t
CC-TOE (config)# crypto isakmp policy 1
CC-TOE (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>.

```
CC-TOE (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.*

```
CC-TOE (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.

```
CC-TOE(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.

```
CC-TOE (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), 16 (4096-bit MODP), and 15 (3072 bit MODP) are also allowed and supported.

```
CC-TOE (config-isakmp)# lifetime 85500
```

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. **Note:** A value of 85500 should not be exceeded.

```
CC-TOE (config-isakmp)# crypto isakmp aggressive-mode disable
```

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

```
CC-TOE(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:

```
CC-TOE # conf t

CC-TOE (config)# crypto ikev2 proposal sample

CC-TOE (config-ikev2-proposal)# integrity sha1
```

CSfC configuration requires sha512:

```
CSfC-TOE (config-ikev2-proposal)# integrity sha512
```

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>.

```
CC-TOE (config-ikev2-proposal)# encryption aes-cbc-128
```

CSfC configuration requires AES-CBC-256 or AES-GCM-256:

```
CSfC-TOE (config-ikev2-proposal)# encryption <aes-cbc-256 | aes-gcm-256>
```

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 for additional information

```
CC-TOE (config-ikev2-proposal)# group 14
```

CSfC configuration requires groups 19, 20, 15 or 16:

```
CC-TOE (config-ikev2-proposal)# group 16
```

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), 15 (3072 bit MODP), and 16 (4096 bit MODP) are also allowed and supported.

```
CC-TOE (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.

```
CC-TOE (config)# crypto ikev2 keyring keyring-1

CC-TOE (config-ikev2-keyring)# peer peer1

CC-TOE (config-ikev2-keyring-peer)# address 0.0.0.0 0.0.0.0

CC-TOE (config-ikev2-keyring-peer)# pre-shared-key hex < hex-string >
```

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*: Hexadecimal pre-shared key length on the TOE must be exactly 64 characters.*

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.

1. Configure transform set:

```
Router(config)# crypto ipsec transform-set TSET esp-aes 256 esp-sha256-hmac
   mode tunnel
```

2. Configure IPsec profile:

```
Router(config)# crypto ikev2 profile PROF
   match identity remote address 192.0.2.2 255.255.255.255
   authentication remote pre-share key <KEY>
   authentication local pre-share key <KEY>
  lifetime 86400
```

```
!
Router(config)# crypto ipsec profile PROF
   set transform-set TSET
   set ikev2-profile PROF
```

3. Configure interface:

```
Router(config)# interface GigabitEthernet0/0/0
   ip address 192.0.2.1 255.255.255.
```

4. Configure IPsec VTI:

```
Router(config)# interface Tunnel0
  ip address 100.0.2.1 255.255.255.252
  tunnel source GigabitEthernet0/0/0
  tunnel mode ipsec ipv4
  tunnel destination 192.0.2.2
  tunnel protection ipsec profile PROF
```

5. Enable IKEv2 syslog messages:

```
Router(config)# crypto logging ikev2
```

6. Verify IPsec VTI with the following commands:

```
Router# show crypto session
Router# show interface tunnel0
Router# show ip route
```

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:

```
CC-TOE(config)# crypto ipsec transform-set EXAMPLE esp-aes 128 esp- sha-hmac
```

CSfC configuration requires AES-GCM-256 and HMAC-SHA-512:

```
CSfC-TOE(config)# crypto ipsec transform-set EXAMPLE esp-gcm 256 esp-sha512-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.*

```
CC-TOE(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.

```
CC-TOE (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.

```
CC-TOE (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. RSA certificates are supported.

CRL is configurable and may be used for certificate revocation. The authorized administrator executes the "revocation-check" command to specify at least one method of revocation checking; CRL is the default method and must be selected in the evaluated configuration as the 'none' option is not allowed. The authorized administer sets the trust point and its name and the revocation-check method.

The extendedKeyUsage field is validated according to the following rules:

- Certificates used for trusted updates and executable code integrity verification have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3)
- Server certificates have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field
- Client certificates have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2)
- OCSP certificates presented for OCSP responses have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9)

in the extendedKeyUsage field.

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 keys are generated in pairs with one public key and one private key:

```
(config)# crypto key generate rsa modulus 2048
```

CSfC configuration requires 3072 bits:

```
(config)# crypto key generate rsa modulus 3072
```

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 the ‘copy run start’ command, 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 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)

  crypto pki import <trustpoint name> certificate
  crypto ikev2 profile ikev2_profile

pki trustpoint <trustpoint name>

- 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 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.

  (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(cfg-crypto-trans)# crypto ipsec profile sampleprofile
TOE-common-criteria(cfg-crypto-trans)# set transform-set sampleset
TOE-common-criteria(cfg-crypto-trans)# 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)#exit
TOE-common-criteria(config-if)# interface Tunnel0
TOE-common-criteria(config-if)# ip address 10.10.10.101 255.255.255.252
TOE-common-criteria(config-if)# tunnel source GigabitEthernet0/0
TOE-common-criteria(config-if)# tunnel mode ipsec ipv4
TOE-common-criteria(config-if)# tunnel destination 10.10.10.102
TOE-common-criteria(config-if)# tunnel protection ipsec profile sampleprofile
```

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.

1. Authenticate the CA: crypto ca authenticate *trustpoint-name*

```
Device (config)#crypto ca authenticate ciscotest
Certificate has the following attributes:
    Fingerprint: 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:

1. Enter configure terminal mode:
2. CC-TOE# configure terminal
3. Specify the local storage location for certificates: crypto pki certificate storage *location-name*
   Device(config)# crypto pki certificate storage flash:/certs
4. Exit: Device(config)# exit
5. Save the changes made:
6. Device# copy system:running-config nvram:startup-config

7. Display the current setting for the PKI certificate storage location:

   Device# show crypto pki certificates storage

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

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

4.6.4.6 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:

   CC-TOE# configure terminal

2. Set the crypto pki trustpoint name:

   CC-TOE(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:

   CC-TOE(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. 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.

   CC-TOE(ca-trustpoint)# (ca-trustpoint)# revocation-check crl

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

5. Use the 'match key-usage crlsign' command to enforces checking for the CRLSign bit in certificates.

   CC-TOE(ca-trustpoint)# match key-usage crlsign

6. Exit:

   CC-TOE(ca-trustpoint)# **exit**

4.6.4.7 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:

```
CC-TOE (config)# crypto isakmp policy 1
CC-TOE (config-isakmp)# authentication rsa-sig
```

And for IKEv2 with the commands:

```
CC-TOE (config)#crypto ikev2 profile sample
CC-TOE(config-ikev2-profile)#authentication [remote | local] rsa-sig
```

4.6.4.8 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 VPNGW Module 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:

- The ‘discard’ option is accomplished using access lists with deny entries, which are applied to interfaces.
- The ‘bypassing’ option is accomplished using access lists, whichare applied to IPsec VTI interfaces. If no explicit ‘permit’ exists within the access list, 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 IPsec VTI interfaces.

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 extended <ACL_NAME>
< deny | permit> ip <source address> <source wildcard bits> <destination address> <destination wildcard bits>
```

Apply the ACL to an IPsec VTI:

```
Router(config)# interface Tunnel0
Router(config-if)#  Tunnel protection ipsec policy ipv4 <ACL_NAME>
```

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.

4.6.7 Configuring Quantum-Safe Encryption Using Postquantum Preshared Keys

NOTE: Required for CSfC

RFC 8784 (Mixing Preshared Keys in IKEv2 for Postquantum Security) describes an extension to the IKEv2 protocol to allow it to be resistant to a quantum computer by using preshared keys known as PPKs. The RFC defines negotiation of PPK capability, communication of PPK ID, mixing of PPK as an additional input in the session key derivation, and optional fallback to non-PPK-based session.

Perform the following tasks to configure the manual PPK:

- Configuring Manual Post-Quantum Preshared Keys in IKEv2 Keyring
- Configuring IKEv2 Keyring in IKEv2 Profile

Configuring Manual Post-Quantum Preshared Keys in IKEv2 Keyring

Follow these steps to configure the manual PPK for one or more peers or groups of peers, in the IKEv2 keyring:

1. Enable privileged EXEC mode,

   ```
   TOE-common-criteria> enable
   ```

2. Enter global configuration mode,

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

3. Define an IKEv2 keyring and enters IKEv2 keyring configuration mode,

   TOE-common-criteria(config)# **crypto ikev2 keyring <keyring-name**>

4. Define the peer or peer group and enters IKEv2 keyring peer configuration mode,

   TOE-common-criteria(config-ikev2-keyring)# **peer <name**>

5. Specify the remote IKEv2 peers based on WAN IP address,

   TOE-common-criteria(config-ikev2-keyring-peer)# **address <ipv4-address mask | ipv6-address prefix>**

6. Configure PPK ID and PPK for the identified peers,

   TOE-common-criteria(config-ikev2-keyring-peer)# **ppk manual id ppk-id key <KEY>**

Configuring IKEv2 Keyring in IKEv2 Profile

1. Define an IKEv2 profile and enters the IKEv2 profile configuration mode,

   TOE-common-criteria(config-ikev2-keyring-peer)# **crypto ikev2 profile <profile-name**>

2. Specify the keyring that has either manual or dynamic PPK configured,

   TOE-common-criteria(config-ikev2-profile)# **keyring ppk <keyring-name**>

3. Exits IKEv2profile configuration mode,

   TOE-common-criteria(config-ikev2-profile)# **exit**
   TOE-common-criteria(config)# **exit**

Verifying the Post-Quantum Preshared Keys Configuration

Use the “show crypto ikev2 sa detailed” command to display information about the current IKEv2 security associations. The “**Quantum Resistance Enabled**” message displayed in the output indicates that PPK-based quantum-safe encryption is enabled.

The following is a sample output from the “show crypto ikev2 sa detailed” command:

```
IPv4 Crypto IKEv2  SA
Tunnel-id       Local               Remote                   fvrf/ivrf          Status
   3        <src IP>/SrcPort     <Dst IP>/DstPort              none/none        READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19,
Auth sign:
.
.
```

```
.
Initiator of SA : No
Quantum Resistance Enabled
```

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

This section describes configuration of the peer reference identifier which is achieved through 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: *CN is not supported for reference identifiers. The accepted identifiers are Distinguished Name (DN), SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), and SAN: user FQDN.*

Step1	(config)# **crypto pki certificate map** *label sequence-number*	Starts certificate-map mode

Step2	*(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.
Step3	(ca-certificate-map)# **exit**	Exits ca-certificate-map mode.
Step4	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
```

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 3.3.6 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 3.3.4 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' 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 5 General Auditable Events includes general applicable events.

***Note**: In Table 5, if Embedded Event Manager is used, as outlined in Section 3.3.5, 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 2023 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encryption/decryption ... passed)

Date: Nov 19 2023

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 TOE.

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 Table 5 below:

Nov 19 2023 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test activated by user: lab)

Nov 19 2023 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software checksum passed)

Nov 19 2023 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encryption/decryption ... passed)

Nov 19 2023 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (3DES encryption/decryption ... passed)

Nov 19 2023 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA hashing ... passed)

Nov 19 2023 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (AES encryption/decryption ... passed)

Table 5 General Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FAU_GEN.1	Startup and Shutdown of the Audit Function	None.	Enable Auditing 2023-09-20T11:29:04.067675-04:00 esr6300 894: *Sep 20 2023 16:29:34: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:logging host 192.168.144.254 Disable Auditing 2023-09-20T11:29:04.067675-04:00 esr6300 895: *Sep 20 2023 16:29:34: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.144.254 port 514 started - CLI initiated Administrative login and logout 2023-09-20T09:27:21.076072-04:00 esr6300 4665: Sep 20 2023 14:27:51: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 192.168.144.254 port 514 stopped -

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			CLI initiated For login audits, see FIA_UIA_EXT.1 For logout audits, see FTA_SSL_EXT.4 For changes to TSF data related to configuration changes, see FMT_SMF.1 Generate/Import 2023-09-28T08:35:20.166754-04:00 esr6300_outside 2791: *Sep 28 2023 13:35:50: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named ESR6300.example.com has been generated or imported by crypto-engine Delete 2023-09-28T08:35:19.153759-04:00 esr6300_outside 2790: *Sep 28 2023 13:35:49: %CRYPTO_ENGINE-5-KEY_DELETED: A key named ESR6300.example.com has been removed from key storage Changes to TSF data related to configuration changes 2024-02-12T16:54:15.565418-05:00 esr6300 504: *Feb 12 2024 22:50:37: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:username AntonioTonerson password * See audits above in Enable/Disable auditing for an example of the Administrator Starting & Stopping the logging services.
FAU_GEN.1/VPN	No events specified	None.	Start-up and shut-down of the audit functions See NDcPP22e FAU_GEN.1 for starup and shutdown of the audit functions. Indication that TSF self-test was completed *Sep 28 2023 16:41:30.507: %CRYPTO-5-SELF_TEST_START: Crypto algorithms release (Rel5a), Entropy release (3.4.1) begin self-test *Sep 28 2023 16:41:31.134: %CRYPTO-5-SELF_TEST_END: Crypto algorithms self-test completed successfully

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			All tests passed. Failure of self-test *Nov 6 2023 19:32:02.128: %CRYPTO-0-SELF_TEST_FAILURE: Crypto algorithms self-test failed (Software self-integrity test)
FAU_GEN.2	None.	None.	
FAU_STG.1	None.	None.	
FAU_STG_EXT.1	None.	None.	
FCS_CKM.1	None.	None.	
FCS_CKM.1/IKE	None.	N/A	
FCS_CKM.2	None.	None.	
FCS_CKM.4	None.	None.	
FCS_COP.1/ DataEncryption	None.	None.	
FCS_COP.1/SigGen	None.	None.	
FCS_COP.1/Hash	None.	None.	
FCS_COP.1/KeyedHash	None.	None.	
FCS_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	No Matching Proposal 2023-09-27T13:56:23.888255-04:00 esr6300_outside 22837: Sep 27 18:56:55.802: IKEv2-ERROR:(SESSION ID = 110,SA ID = 1):: Failed to find a matching policy Reference Identifier Match failed 2023-10-05T10:02:24.542880-04:00 esr6300_outside 197: *Oct 5 2023 15:02:42: %IKEV2-3-NEG_ABORT: Negotiation aborted due to ERROR: Auth exchange failed Invalid Chain 2023-10-06T08:40:06.288367-04:00 esr6300_outside 33847: *Oct 6 2023 13:40:22: %IKEV2-3-NEG_ABORT: Negotiation aborted due to ERROR: Failed to locate an item in the database Expired Cert 2023-09-29T13:45:15.800307-04:00 esr6300_outside 30320: *Sep 29 18:45:46.367: IKEv2-ERROR:Current time is more than cert validity time Revoked Cert (CRL)

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			2023-09-29T14:08:30.697230-04:00 esr6300_outside 600: *Sep 29 2023 19:09:00: %PKI-3-CERTIFICATE_REVOKED: Certificate chain validation has failed. The certificate (SN: 00D5) is revoked Invalid Key Usage (missing cRLSign) 2023-09-29T14:11:53.700791-04:00 esr6300_outside 739: Reason : failed to verify CRL signature Invalid Signature / Corrupt ASN.1 2023-09-29T14:55:14.967260-04:00 esr6300_outside 208: *Sep 29 2023 19:55:45: %PKI-3-CERTIFICATE_INVALID: Certificate chain validation has failed. Missing basicConstraints / False CA Flag 2023-09-29T14:25:39.714250-04:00 esr6300_outside 1092: *Sep 29 2023 19:26:09: %IKEV2-3-NEG_ABORT: Negotiation aborted due to ERROR: Platform errors Unreachable Revocation Server 2023-09-29T14:22:16.008184-04:00 esr6300_outside 1032: *Sep 29 2023 19:22:45: %PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint rootca-rsa failed
FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity if new/removed time server	Configuration of new time server 2023-09-26T11:25:31.594952-04:00 esr6300_outside 413: *Sep 28 2023 16:45:22: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:ntp server 172.16.16.254 Removal of configured time server 2023-09-23T16:10:51.105263-04:00 esr6300_outside 4413: .Sep 23 2023 20:10:50: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no ntp server 192.168.144.254
FCS_RBG_EXT.1	None.	None.	
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.	No matching kex 2023-09-25T20:42:16.155694-04:00 esr6300_outside 16343: *Sep 28 2023 02:02:09: %SSH-3-NO_MATCH: No matching kex algorithm found: client diffie-

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			hellman-group1-sha1,ext-info-c server diffie-hellman-group14-sha1,ecdh-sha2-nistp384 No matching cipher 2023-09-25T20:37:24.771615-04:00 esr6300_outside 16066: *Sep 28 2023 01:57:17: %SSH-3-NO_MATCH: No matching cipher found: client aes128-gcm@openssh.com server aes128-cbc,aes256-cbc,aes256-gcm@openssh.com No matching host key alg 2023-09-21T10:00:24.295701-04:00 esr6300_outside 3465: *Sep 21 2023 15:00:53: %SSH-3-NO_MATCH: No matching hostkey algorithm found: client ecdsa-sha2-nistp384 server rsa-sha2-512,rsa-sha2-256,ssh-rsa No matching MAC 2023-09-25T20:38:03.117252-04:00 esr6300_outside 16079: *Sep 28 2023 01:57:56: %SSH-3-NO_MATCH: No matching mac found: client hmac-md5 server hmac-sha2-256,hmac-sha2-512
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	2023-09-19T14:28:28.862928-04:00 esr6300 3829: Aug 31 2023 20:28:31: %AAA-5-USER_LOCKED: User testuser1 locked out on authentication failure
FIA_PMG_EXT.1	None.	None.	
FIA_PSK_EXT.1	None.	N/A	
FIA_PSK_EXT.2	None.	N/A	
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).	Successful Console Login 2023-09-28T08:51:25.915646-04:00 esr6300_outside 3582: *Sep 28 2023 13:51:56: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: LOCAL] [localport: 0] at 08:51:56 EST Thu Sep 28 2023 Failed Console login 2023-09-28T08:51:19.710923-04:00 esr6300_outside 3579: *Sep 28 2023 13:51:50: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 172.16.16.254] [localport: 22] [Reason: Login Authentication Failed] at 08:51:50 EST Thu Sep 28 2023 Successful RADIUS SSH login

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
			2023-09-28T08:49:03.229788-04:00 esr6300_outside 3436: *Sep 28 2023 13:49:33: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: wilma] [Source: 172.16.16.254] [localport: 22] at 08:49:33 EST Thu Sep 28 2023 Failed RADIUS SSH login 2023-09-28T08:49:01.319399-04:00 esr6300_outside 3406: *Sep 28 2023 13:49:31: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: wilma] [Source: 172.16.16.254] [localport: 22] [Reason: Login Authentication Failed] at 08:49:31 EST Thu Sep 28 2023 Successful SSH login 2023-09-28T08:51:21.151480-04:00 esr6300_outside 3580: *Sep 28 2023 13:51:51: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 172.16.16.254] [localport: 22] at 08:51:51 EST Thu Sep 28 2023 Failed SSH login 2023-09-28T08:51:19.710923-04:00 esr6300_outside 3579: *Sep 28 2023 13:51:50: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: admin] [Source: 172.16.16.254] [localport: 22] [Reason: Login Authentication Failed] at 08:51:50 EST Thu Sep 28 2023
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).	Refer to audits for FIA_UIA_EXT.1
FIA_UAU.7	None.	None.	
FIA_X509_EXT.1/REV	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	See FCS_IPSEC_EXT.1 where these X509 failure cases are covered. Addition/replacement 2023-09-27T11:59:58.641076-04:00 esr6300_outside 6913: Sep 27 17:00:30.738: %HA_EM-6-LOG: cli_log: host[ESR6300] user[admin] port[146] exec_lvl[15] command[crypto pki import rootca-ecdsa certificate] Executed Removal 2023-09-27T11:57:34.122949-04:00 esr6300_outside 6735: Sep 27 2023 16:58:06: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:no crypto pki trustpoint rootca-ecdsa

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FIA_X509_EXT.2	None.	None.	
FIA_X509_EXT.3	None.	None.	
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.	Refer to audits for FPT_TUD_EXT.1
FMT_MOF.1/Services	Starting and stopping of Services	None.	Refer to audits for starting and stopping auditing in FAU_GEN.1
FMT_MOF.1/Functions	None.	None.	
FMT_SMF.1	All management activities of TSF data.	None.	Samples of audits showing the commands executed by an administrator: 2023-09-28T08:49:06.297906-04:00 esr6300_outside 3438: *Sep 28 13:49:36.928: %HA_EM-6-LOG: cli_log: host[ESR6300] user[wilma] port[146] exec_lvl[1] command[enable] Executed 2023-09-27T14:40:47.439167-04:00 esr6300_outside 333: *Sep 27 19:41:18.992: %HA_EM-6-LOG: cli_log: host[ESR6300] user[callhome] port[147] exec_lvl[15] command[show version] Executed 2023-09-28T08:51:00.995733-04:00 esr6300_outside 3564: *Sep 28 13:51:31.627: %HA_EM-6-LOG: cli_log: host[ESR6300] user[wilma] port[146] exec_lvl[15] command[configure terminal] Executed 2023-10-05T09:43:14.193840-04:00 esr6300_outside 13976: *Oct 5 14:43:32.029: %HA_EM-6-LOG: cli_log: host[ESR6300] user[admin] port[146] exec_lvl[15] command[ip access-group ipsec_acl out] Executed
FMT_MTD.1/CryptoKeys	Management of Cryptographic keys	None.	**Refer to cryptographic key audits for FAU_GEN.1.**
FMT_MTD.1/CoreData	None.	None.	
FMT_SMR.2	None.	None.	
FPT_FLS.1/SelfTest	None.	N/A	
FPF_RUL_EXT.1	Application of rules	Source and	ICMP deny

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	configured with the 'log' operation	destination addresses Source and destination ports Transport Layer Protocol TOE Interface	2023-09-27T10:29:23.213537-04:00 esr6300_outside 3934: Sep 27 2023 15:29:56: %FMANFP-6-IPACCESSLOGDP: F0/0: fman_fp_image: list FPF_RUL_EXT.1.1 denied icmp 0015.5d00.3b0a 192.168.144.254 -> 10.1.1.1 (2048/0), 4 packets ICMPv6 deny 2023-09-27T11:28:53.088764-04:00 esr6300_outside 5692: Sep 27 2023 16:29:23: %FMANFP-6-IPV6ACCESSLOGDP: F0/0: fman_fp_image: list FPF_RUL_EXT.1.6_ipv6 denied icmpv6 0015.5d00.3b0a fe80::215:5dff:fe00:3b0a -> ff02::16 (0/143), 1 packet ICMP permit 2023-09-27T16:43:59.268925-04:00 esr6300_outside 875: *Sep 27 2023 21:44:29: %FMANFP-6-IPACCESSLOGDP: F0/0: fman_fp_image: list 160 permitted icmp 0015.5d00.3b0a 100.100.100.90 -> 100.100.100.100 (2048/0), 1 packet ICMPv6 permit 2023-09-27T11:41:31.605640-04:00 esr6300_outside 6174: Sep 27 2023 16:42:03: %FMANFP-6-IPV6ACCESSLOGDP: F0/0: fman_fp_image: list FPF_RUL_EXT.1.6_ipv6 permitted icmpv6 0015.5d00.3b0a 2620:2:2a03:2a:1f3::25 -> 2001:db8:1:9::11 (0/128), 1 packet
FPT_SKP_EXT.1	None.	None.	
FPT_APW_EXT.1	None.	None.	
FPT_TST_EXT.1	None.	None.	
FPT_TST_EXT.3	None.	N/A	
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 and failure (e.g., IP address).	Set Clock Manually 2023-09-19T14:21:28.648135-04:00 esr6300 3799: Aug 31 2023 20:21:31: %SYS-6-CLOCKUPDATE: System clock has been updated from 16:21:13 EST Thu Aug 31 2023 to 15:21:31 EST Thu Aug 31 2023, configured from console by admin on vty0 (172.16.16.254).

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	No additional information.	Initiate Update 2023-10-10T10:39:03.267231-04:00 esr6300 491: *Oct 10 2023 15:39:13: %PARSER-5-CFGLOG_LOGGEDCMD: User:admin logged command:boot system flash:c6300-zero-signature.SSA.bin 2023-10-10T10:39:08.034249-04:00 esr6300 494: *Oct 10 15:39:17.938: %HA_EM-6-LOG: cli_log: host[ESR6300] user[admin] port[146] exec_lvl[15] command[reload /verify] Executed No signature update 2023-10-10T10:34:12.556276-04:00 esr6300 460: *Oct 10 2023 15:34:22: %SIGNATURE-3-NOT_VALID: %ERROR: Signature not valid for file bootflash:/c6300-zero-signature.SSA.bin. Invalid signature update 2023-10-10T10:29:46.264319-04:00 esr6300 454: *Oct 10 2023 15:29:56: %SIGNATURE-3-NOT_ABLE_TO_PROCESS: %ERROR: Not able to process Signature in bootflash:/c6300-invalid-signature.SSA.bin. Modified update 2023-10-10T10:32:17.042084-04:00 esr6300 457: *Oct 10 2023 15:32:26: %SIGNATURE-3-NOT_VALID: %ERROR: Signature not valid for file bootflash:/c6300-modified-signature.SPA.bin.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.	Termination of Console session 2023-09-28T08:52:26.550051-04:00 esr6300_outside 3586: *Sep 28 2023 13:52:57: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 0 (0.0.0.0)), user admin
FTA_SSL.3	The termination of a *remote* session by the session locking mechanism.	None.	Termination of SSH session 2023-09-26T17:55:56.050449-04:00 esr6300_outside 3414: Sep 26 2023 22:56:31: %SYS-6-TTY_EXPIRE_TIMER: (exec timer expired, tty 146 (172.16.16.254)), user admin
FTA_SSL.4	The termination of an interactive	None.	Termination of Console session 2023-09-28T08:52:26.550051-04:00 esr6300_outside 3587: *Sep 28 2023

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
	session.		13:52:57: %SYS-6-LOGOUT: User admin has exited tty session 0() Termination of SSH session 2023-09-19T14:29:41.119794-04:00 esr6300 3848: Aug 31 2023 20:29:44: %SYS-6-LOGOUT: User admin has exited tty session 146(172.16.16.254)
FTA_TAB.1	None.	None.	
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	Initiation of an IPSec channel 2023-09-26T09:44:08.178633-04:00 esr6300_outside 56906: *Sep 28 2023 15:04:00: %IKEV2-5-OSAL_INITIATE_TUNNEL: Received request to establish an IPsec tunnel; local traffic selector = Address Range: 0.0.0.0-255.255.255.255 Protocol: 256 Port Range: 0-65535 ; remote traffic selector = Address Range: 0.0.0.0-255.255.255.255 Protocol: 256 Port Range: 0-65535 Termination of an IPsec Channel (audit located only on switch) 2023-09-27T16:44:08.856558-04:00 esr6300_outside 876: *Sep 27 2023 21:44:40: %IKEV2-5-SA_DOWN: SA DOWN Failure to Establish an IPsec SA Refer to audits for FCS_IPSEC_EXT.1
FTP_ITC.1/VPN	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	Refer to NDcPP22e FTP_ITC.1 and FCS_IPSEC_EXT.1 for audits pertaining to initiation and failure respectively for the IPsec channel.

Requirement	Auditable Events	Additional Audit Record Contents	Sample Record
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.	Initiation, Termination and Failure of a IPsec channel Audits for IPSec channel initiations can be found under FTP_ITC.1 as the audit of IPSec are the same regardless of the usage of the channel Initiation of an SSH channel 2023-09-19T14:30:03.921523-04:00 esr6300 3852: Aug 31 2023 20:30:06: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: testuser1] [Source: 172.16.16.254] [localport: 22] at 15:30:06 EST Thu Aug 31 2023 Termination of an SSH channel 2023-09-19T14:29:41.119794-04:00 esr6300 3848: Aug 31 2023 20:29:44: %SYS-6-LOGOUT: User admin has exited tty session 146(172.16.16.254) Failures of an SSH Channnel Refer to audits for FCS_SSHS_EXT.1

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.

Table 6 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.
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.

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
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
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

Service or Protocol	Description	Client (initiating)	Allowed	Server (terminating)	Allowed	Allowed use in the certified configuration
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
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 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-1/256/512 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.

- 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.

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 2023 16:28:23.629: %CRYPTO-0-SELF_TEST_FAILURE: Encryption self-test failed

If a software upgrade fails, the ESR6300 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 7 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.
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	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
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 information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

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

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

10. ANNEX A: TECHNICAL HARDWARE GUIDANCE

10.1 BTB Interface Connector Details

The board-to-board (BTB) connector provides the power input and the interface to external devices. Figure 7 above shows the BTB interface connector pictured on the top left of the board and is fully integrated on each ESR6300 hardware model. In the CC evaluated configuration, the following interfaces were used during testing:

- Console: 1 UART RS232 RJ45 console port
- WAN Interfaces: 2 Combo Layer 3 GE WAN ports
- LAN Interfaces: 4 Layer 2 GE LAN ports

The tables below show TSF relevance, CC lab tested interfaces, and which pins work together for each interface. This information is also provided in the “Board-To-Board (BTB) Interface Connector” section of Cisco Embedded Service 6300 Series Router Hardware Technical Guide.

Table 8 BTB Connector Pin Relevance

External Connectivity	TSF Relevance	Tested by CC Lab
USB A	Non-interfering	No
RS232 Console	Console	Yes
RS232 DTE	Console	No
SFP 0/0	Network	No
SFP 0/1	Network	No
GE0/0	Network	Yes
GE 0/1	Network	Yes
GE 1/0	Network	No
GE 1/1	Network	No
GE 1/2	Network	No
GE 1/3	Network	No
Power	Non-interfering	Yes
SATA	Non-interfering	No
System LEDs	Non-interfering	No
System Button	Non-interfering	No
Unused	Unused	NA

Table 9 BTB Connector External Connectivity Details

PIN	Row A	Row B	Row C	Row D	Row E	Row F
1	Power	Power	Power	Power	Power	Power
2	Power	Power	Power	Power	Power	Power
3	GND	GND	GND	GND	GND	GND
4	GND	GND	GND	GND	GND	GND
5	Power	Power	Power	Power	Power	Power
6	GND	GND	GND	GND	GND	GND
7	GE 1/3	GND	GE 1/3	GND	unused	unused
8	GE 1/3	GND	GE 1/3	GND	unused	GND

9	GND	GE 1/3	GND	GE 1/3	GND	System LED
10	GND	GE 1/3	GND	GE 1/3	GND	System Button
11	GE 1/2	GND	GE 1/2	GND	unused	Power
12	GE 1/2	GND	GE 1/2	GND	unused	unused
13	GND	GE 1/2	GND	GE 1/2	GND	USB A
14	GND	GE 1/2	GND	GE 1/2	GND	USB A
15	GE 1/1	GND	GE 1/1	GND	unused	GND
16	GE 1/1	GND	GE 1/1	GND	unused	RS232 DTE
17	GND	GE 1/1	GND	GE 1/1	GND	RS232 DTE
18	GND	GE 1/1	GND	GE 1/1	GND	RS232 DTE
19	GE 1/0	GND	GE 1/0	GND	USB A	RS232 DTE
20	GE 1/0	GND	GE 1/0	GND	USB A	GND
21	GND	GE 1/0	GND	GE 1/0	GND	RS232 DTE
22	GND	GE 1/0	GND	GE 1/0	GND	RS232 DTE
23	unused	GND	unused	GND	unused	System LED
24	unused	GND	unused	GND	unused	System LED
25	GND	USB A	GND	USB A	GND	System LED
26	GND	USB A	GND	USB A	GND	System LED
27	SATA	GND	SATA	GND	unused	GND
28	SATA	GND	SATA	GND	unused	System LED
29	GND	SFP 0/1	GND	SFP 0/1	GND	System LED
30	GND	SFP 0/1	GND	SFP 0/1	GND	System LED
31	GE 0/1	GND	GE 0/1	GND	unused	System LED
32	GE 0/1	GND	GE 0/1	GND	System LED	GND
33	GND	GE 0/1	GND	GE 0/1	GND	RS232 Console
34	GND	GE 0/1	GND	GE 0/1	GND	RS232 Console
35	GE0/0	GND	GE0/0	GND	System LED	GND
36	GE0/0	GND	GE0/0	GND	unused	unused
37	GND	GE0/0	GND	GE0/0	GND	unused
38	GND	GE0/0	GND	GE0/0	GND	unused
39	SFP 0/0	GND	SFP 0/0	GND	unused	System LED
40	SFP 0/0	GND	SFP 0/0	Power	unused	System LED

Table 10 BTB Connector Pin Mapping Details

PIN	Row A	Row B	Row C	Row D	Row E	Row F
1	+5V	+5V	+5V	+5V	+5V	+5V
2	+5V	+5V	+5V	+5V	+5V	+5V
3	GND	GND	GND	GND	GND	GND
4	GND	GND	GND	GND	GND	GND
5	+3.3V	+3.3V	+3.3V	+3.3V	+3.3V	RTC_3.0V
6	GND	GND	GND	GND	GND	GND
7	P4_MDI3_N	GND	P4_MDI2_N	GND	PCIE_REFCLK_P	P3V3_TRIM
8	P4_MDI3_P	GND	P4_MDI2_P	GND	PCIE_REFCLK_N	GND
9	GND	P4_MDI1_N	GND	P4_MDI0_N	GND	ALM_IN_L

10	GND	P4_MDI1_P	GND	P4_MDI0_P	GND	PUSHBUTTON_L
11	P3_MDI3_N	GND	P3_MDI2_N	GND	PIM_SGMII_RX_P	DCIN_PWR_GOOD
12	P3_MDI3_P	GND	P3_MDI2_P	GND	PIM_SGMII_RX_N	PIM_PWR_EN
13	GND	P3_MDI1_N	GND	P3_MDI0_N	GND	USBA_5V_EN
14	GND	P3_MDI1_P	GND	P3_MDI0_P	GND	USBA_OC_L
15	P2_MDI3_N	GND	P2_MDI2_N	GND	PIM_SGMII_TX_P	GND
16	P2_MDI3_P	GND	P2_MDI2_P	GND	PIM_SGMII_TX_N	CP_UA0_DTR
17	GND	P2_MDI1_N	GND	P2_MDI0_N	GND	CP_UA0_DSR
18	GND	P2_MDI1_P	GND	P2_MDI0_P	GND	CP_UA0_RTS
19	P1_MDI3_N	GND	P1_MDI2_N	GND	USBA_DP	CP_UA0_CTS
20	P1_MDI3_P	GND	P1_MDI2_P	GND	USBA_DN	GND
21	GND	P1_MDI1_N	GND	P1_MDI0_N	GND	CP_UA0_TXD
22	GND	P1_MDI1_P	GND	P1_MDI0_P	GND	CP_UA0_RXD
23	PIM_USB3_TX_N	GND	PIM_USB3_RX_P	GND	PIM_USB2_DP	R0_LED
24	PIM_USB3_TX_P	GND	PIM_USB3_RX_N	GND	PIM_USB2_DN	R1_LED
25	GND	USB3A_TX_N	GND	USB3A_RX_P	GND	C0_LED
26	GND	USB3A_TX_P	GND	USB3A_RX_N	GND	C1_LED
27	SSD_TX_SERDES_P	GND	SSD_RX_SERDES_P	GND	PIM_UA2_TXD	GND
28	SSD_TX_SERDES_N	GND	SSD_RX_SERDES_N	GND	PIM_UA2_RXD	P5_LED_GRN
29	GND	SFP_2_TXD_P	GND	SFP_2_RXD_P	GND	SFP1_LED_YEL
30	GND	SFP_2_TXD_N	GND	SFP_2_RXD_N	GND	P6_LED_GRN
31	P6_MDI3_N	GND	P6_MDI2_N	GND	PIM_GPS	SFP2_LED_YEL
32	P6_MDI3_P	GND	P6_MDI2_P	GND	ALM_LED_RED	GND
33	GND	P6_MDI1_P	GND	P6_MDI0_N	GND	AP_UA0_TXD
34	GND	P6_MDI1_N	GND	P6_MDI0_P	GND	AP_UA0_RXD
35	P5_MDI2_N	GND	P5_MDI1_N	GND	VPN_LED_GRN	GND
36	P5_MDI2_P	GND	P5_MDI1_P	GND	EVK_INT_L	I2C3_SCL
37	GND	P5_MDI3_N	GND	P5_MDI0_P	GND	I2C3_SDA
38	GND	P5_MDI3_P	GND	P5_MDI0_N	GND	GND
39	SFP_1_TXD_P	GND	SFP_1_RXD_P	GND	I2C2_SCL	SYS_LED_GRN_L
40	SFP_1_TXD_N	GND	SFP_1_RXD_N	+1.8V_OUT	I2C2_SDA	SYS_LED_YEL_L

***Note:** Table 12 can be found in the "ESR-6300 Board-To-Board Connector (J1)" section of the Cisco Embedded Service 6300 Series Router Hardware Technical Guide along with a description for each pin mapping in the "Power and I/O Signals at the ESR BTB Connector" sections.*

10.2 ESR6300 Board Layout and Dimensions

The TOE must be deployed in a manner consistent with the CC evaluated configuration in which the TOE's BTB connector is attached to a compatible interface as described in the "Board-To-Board (BTB) Interface Connector" section of *the Cisco Embedded Service 6300 Series Router Hardware Technical Guide*, and the TOE's board is affixed using screw holes noted in the diagrams below as described in the "ESR Board Layout and Dimensions" section of Cisco Embedded Service 6300 Series Router Hardware Technical Guide.

Figure 1 shows the ESR Board (left) with the cooling plate (right). The board dimensions are 3.0" x 3.775" inches (76.2mm x 95.885mm). All information provide below is also provided in the Cisco Embedded Service

6300 Series Router Hardware Technical Guide.

Note: *Dimensions are in inches. Tolerances (unless otherwise stated):.XX +/- 0.010,.XXX +/- 0.005.*

Figure 1 ESR6300 Board Images

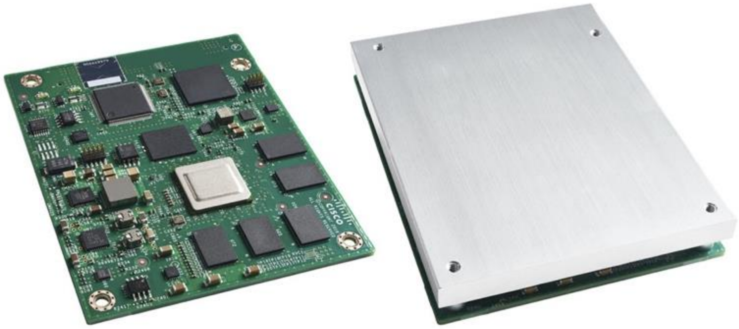


Figure 2 Board Without Cooling Plate (ESR-6300-NCP-K9) Top View

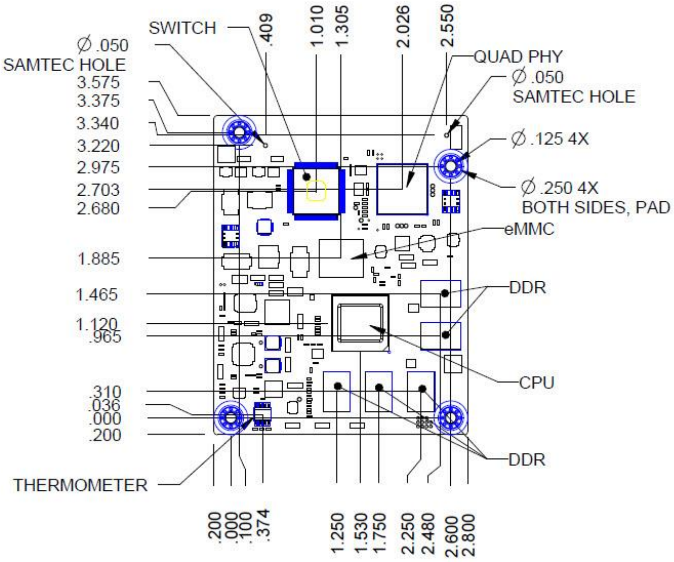


Figure 3 Board Without Cooling Plate (ESR-6300-NCP-K9) Side View

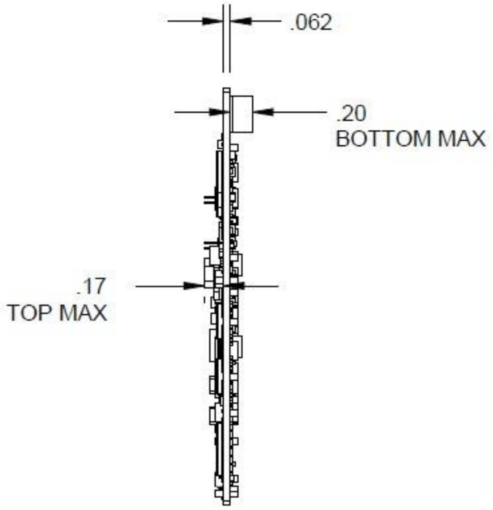


Figure 4 Board Without Cooling Plate (ESR-6300-NCP-K9) Bottom View

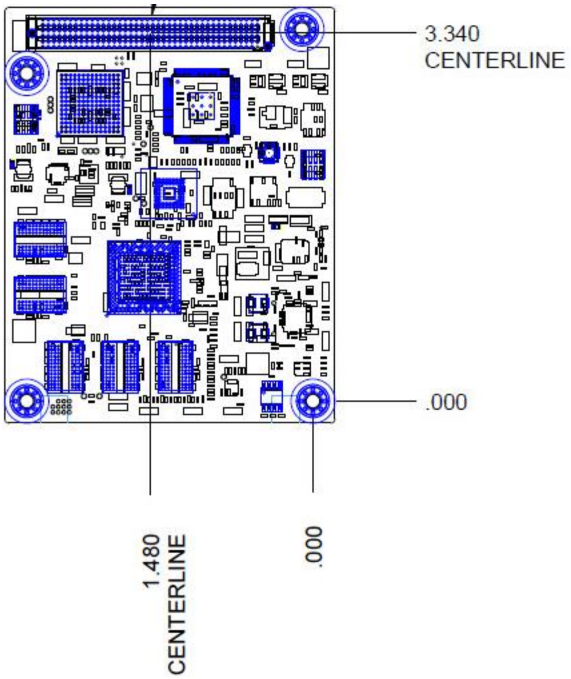


Figure 5 Board Without Cooling Plate (ESR-6300-CON-K9) Top View

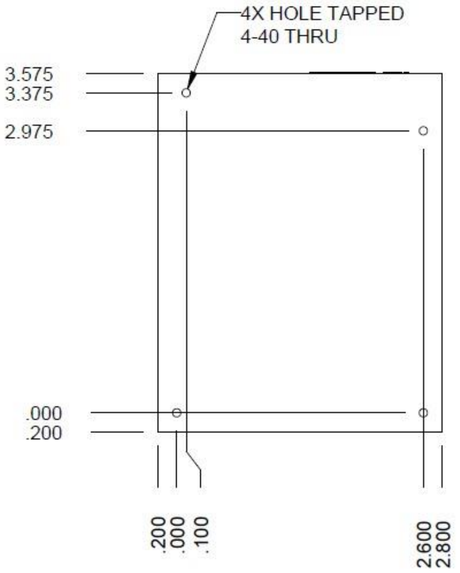


Figure 6 Board Without Cooling Plate (ESR-6300-CON-K9) Side View

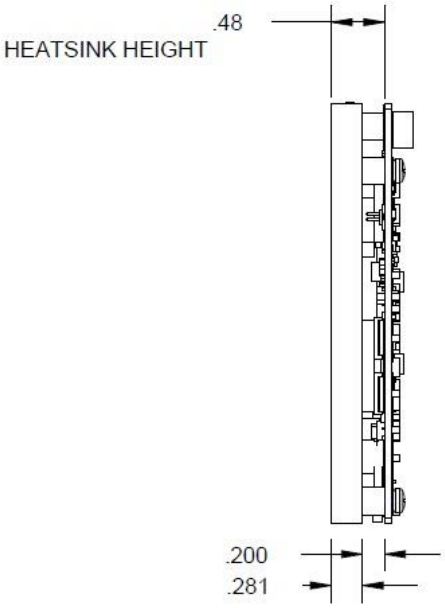
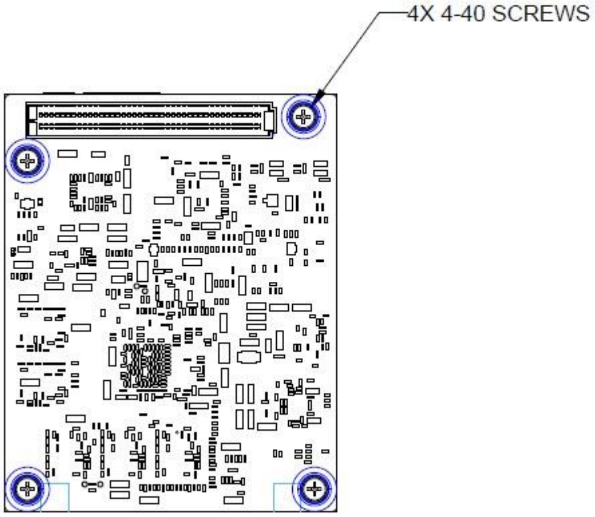


Figure 7 Board Without Cooling Plate (ESR-6300-CON-K9) Bottom View


4X 4-40 SCREWS