Cisco Embedded Services Router (ESR) 6300 v17.18 Common Criteria Security Target

Version: 2.2
Date: July 7, 2026

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

Table of Contents

Document Introduction 7

1 Security Target Introduction 8

1.1 ST and TOE Reference 8
1.2 TOE Overview 8
1.3 TOE Product Type 8
1.4 Supported non-TOE Hardware/ Software/ Firmware 9
1.5 TOE Description 9
1.5.1 Embedded Services Router (ESR) 6300 v17.18 (ESR6300) 10
1.6 TOE Evaluated Configuration 10
1.7 Physical Scope of the TOE 13
1.8 Logical Scope of the TOE 14
1.8.1 Security Audit 14
1.8.2 Cryptographic Support 14
1.8.3 Identification and authentication 16
1.8.4 Security Management 16
1.8.5 Packet Filtering 17
1.8.6 Protection of the TSF 17
1.8.7 TOE Access 17
1.8.8 Trusted path/Channels 17
1.9 Excluded Functionality 18

2 Conformance Claims 19

2.1 Common Criteria Conformance Claim 19
2.2 Protection Profile Conformance 19
2.3 Protection Profile Conformance Claim Rationale 20
2.3.1 TOE Appropriateness 20
2.3.2 TOE Security Problem Definition Consistency 20
2.3.3 Statement of Security Requirements Consistency 20

3 Security Problem Definition 21

3.1 Assumptions 21
3.2 Threats 22
3.3 Organizational Security Policies 24

4 Security Objectives 25

4.1 Security Objectives for the TOE 25
4.2 Security Objectives for the Environment 26

5 Security Requirements 27

5.1 Conventions 27
5.2 TOE Security Functional Requirements 27
5.3 SFRs from NDcPP and MOD_VPNGW 29
5.3.1 Security audit (FAU) 29
5.3.2 Cryptographic Support (FCS) 32
5.3.3 Identification and authentication (FIA) 37
5.3.4 Security management (FMT) 39
5.3.5 Packet Filtering (FPF) 40
5.3.6 Protection of the TSF (FPT) 41
5.3.7 Trusted Path/Channels (FTP) 43

5.4 TOE SFR Dependencies Rationale for SFRs Found in PP 44
5.5 Security Assurance Requirements 44
5.5.3 SAR Requirements 44
5.5.4 Security Assurance Requirements Rationale 44
5.6 Assurance Measures 45
6 TOE Summary Specification 46
6.3 TOE Security Functional Requirement Measures 46
7 Annex A: Key Zeroization 61
8 Annex B: References 63
9 Annex C: Obtaining Documentation and Submitting a Service Request 64
10.1 Document Feedback 64
10.2 Obtaining Technical Assistance 64

List of Tables

TABLE 1 ACRONYMS 5
TABLE 2 ST AND TOE IDENTIFICATION 8
TABLE 3 IT ENVIRONMENT COMPONENTS 9
TABLE 4: HARDWARE MODELS AND SPECIFICATIONS 13
TABLE 5 FIPS REFERENCES 15
TABLE 6 TOE PROVIDED CRYPTOGRAPHY 15
TABLE 7 EXCLUDED FUNCTIONALITY 18
TABLE 8: NIAP TECHNICAL DECISIONS 19
TABLE 9 TOE ASSUMPTIONS 21
TABLE 10 THREATS 22
TABLE 11 ORGANIZATIONAL SECURITY POLICIES 24
TABLE 12 SECURITY OBJECTIVES FOR THE TOE 25
TABLE 13 SECURITY OBJECTIVES FOR THE ENVIRONMENT 26
TABLE 14 SECURITY FUNCTIONAL REQUIREMENTS 27
TABLE 15 AUDITABLE EVENTS 29
TABLE 16 ASSURANCE MEASURES 44
TABLE 17 ASSURANCE MEASURES 45
TABLE 18 HOW TOE SFRS MEASURES 46
TABLE 19 TOE KEY ZEROIZATION 61
TABLE 20 REFERENCES 63

List of Figures

FIGURE 1 TOE EXAMPLE DEPLOYMENT FOR ESR6300 11
FIGURE 2: TOE EVALUATED LAN/WAN INTERFACES 12
FIGURE 3: TOE EVALUATED RS232 CONSOLE PORT 12

Acronyms

The following acronyms and abbreviations are common and may be used in this Security Target:

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
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
CRL	Certificate Revocation List
CSfC	Commercial Solutions for Classified
CSR	Certificate Signing Request
DN	Distinguished Name
DRAM	Dynamic random access memory
DSS	Digital Signature Standard
ESP	Encapsulating Security Payload
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
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
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
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
UDP	User Datagram Protocol
WAN	Wide Area Network
VPN	Virtual Private Network
VTI	Virtual Tunnel Interface

Document Introduction

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Embedded Services Router (ESR) 6300 v17.18. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1 Security Target Introduction

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]
- Annex A: Key Zeroization [Section 7]
- Annex B: References [Section 8]
- Annex C: Obtaining Documentation [Section 10]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A, and Part 2.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its TOE.

Table 2 ST and TOE Identification

Name	Description
ST Title	Cisco Embedded Services Router (ESR) 6300 v17.18 Common Criteria Security Target
ST Version	2.2
Publication Date	July 7, 2026
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Embedded Service Router 6300 (ESR)
TOE Hardware Models	ESR-6300-NCP-K9 ESR-6300-CON-K9
TOE Software Version	IOS-XE 17.18
Keywords	Router, Network Appliance, Data Protection, Authentication, Cryptography, Secure Administration, Network Device, Virtual Private Network (VPN), VPN Gateway

1.2 TOE Overview

The Cisco Embedded Services Routers 6300 (herein after referred to as the ESR6300) is a purpose-built, routing platform that includes VPN functionality provided by the Cisco IOS-XE software. The TOE includes the hardware models as defined in Table 5. This Security Target only addresses the functions that provide for the security of the TOE itself as described in Section 1.8 Logical Scope of the TOE. Functionality not described in the Protection Profile is outside the scope of the evaluation. The TOE must be configured per the Guidance Document in order to operate in the evaluated configuration. Once operating in the evaluated configuration, all other functionality provided by the TOE is out of scope of this validation.

1.3 TOE Product Type

The TOE is a Network Device that includes VPN functionality as defined in NDcPPv3.0e, PKG_SSH_V1.0, and MOD_VPNGW v1.3. The TOE comprises both software and hardware comprises the Cisco Internet Operating System (IOS) XE software image Release IOS-XE 17.18.

The ESR6300 is an embedded router module with a compact form factor of 3.0 by 3.775 inches. Its compact, modular, ruggedized design allows Cisco partners and integrators to build a wide variety of custom embedded solutions. The TOE can be inserted into an enclosure that can accommodate the TOE's size (3.0 x 3.775 in) and provides no compute capabilities. The ESR6300 is available with a custom-designed cooling plate, as well as without the cooling plate. Both versions of the ESR6300 board include an integrated multi-pin Board-to-Board (BTB) interface connector with pins dedicated for power input, ethernet ports, and console ports. The TOE 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. Refer to Annex A in the Guidance Document (AGD) for hardware technical guidance on the ESR6300 board layout and dimensions and Multi-pin BTB Interface Connector description that includes pinout mapping descriptions for network interfaces and power inputs.

1.4 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 3 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
RADIUS AAA Server	Yes	This includes any IT environment RADIUS AAA server that provides remote authentication mechanisms. This can be any RADIUS AAA server that provides remote authentication. The TOE correctly leverages the services provided by this RADIUS AAA server to provide remote 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.
Certificate 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 Gateway/Peer	Yes	This includes any VPN Peer (Gateway, Endpoint, another instance of the TOE) with which the TOE participates in VPN communications. Remote VPN Peers may be any device that supports IPsec VPN communications. Another instance of the TOE used as a VPN Peer would be installed in the evaluated configuration and likely administered by the same personnel.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST.
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. The NTP server should support NTPv4.
Router Enclosure	No	The end user can opt to use an enclosure that accommodates the TOE's size (3.0 x 3.775 in.) and provides no compute capabilities. The TOE 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 on the ESR6300 board layout and dimensions and Multi-pin BTB Interface Connector description that includes pinout mapping descriptions for network interfaces and power inputs.

1.5 TOE Description

This section provides an overview of the ESR6300 Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE comprises both software and hardware. The hardware models included in the evaluation are the ESR-6300-NCP-K9 and ESR-6300-CON-K9 which are further described in Section 1.7

Physical Scope of the TOE. The TOE software for each platform comprises Cisco IOS-XE version 17.18. The Cisco IOS-XE version 17.18 software is used to meet all of the requirements as specified in this document regardless of the hardware platform.

1.5.1 Embedded Services Router (ESR) 6300 v17.18 (ESR6300)

- Compact 3" x 3.75" form factor board optimized for custom solutions
- DRAM: 4-GB DDR4 memory capacity
- Flash Memory: 4-GB usable eMMC flash
- Optional router enclosure as described in Table 4
- Integrated multi-pin BTB Interface Connector - provides pins dedicated for power input, ethernet ports, and console ports. 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

1.6 TOE Evaluated Configuration

The TOE consists of one physical device as specified in section 1.5 below and includes the Cisco IOS-XE software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XE configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

The following figures provide a visual depiction of an example TOE deployment, a LAN/WAN interface diagram, and console port options:

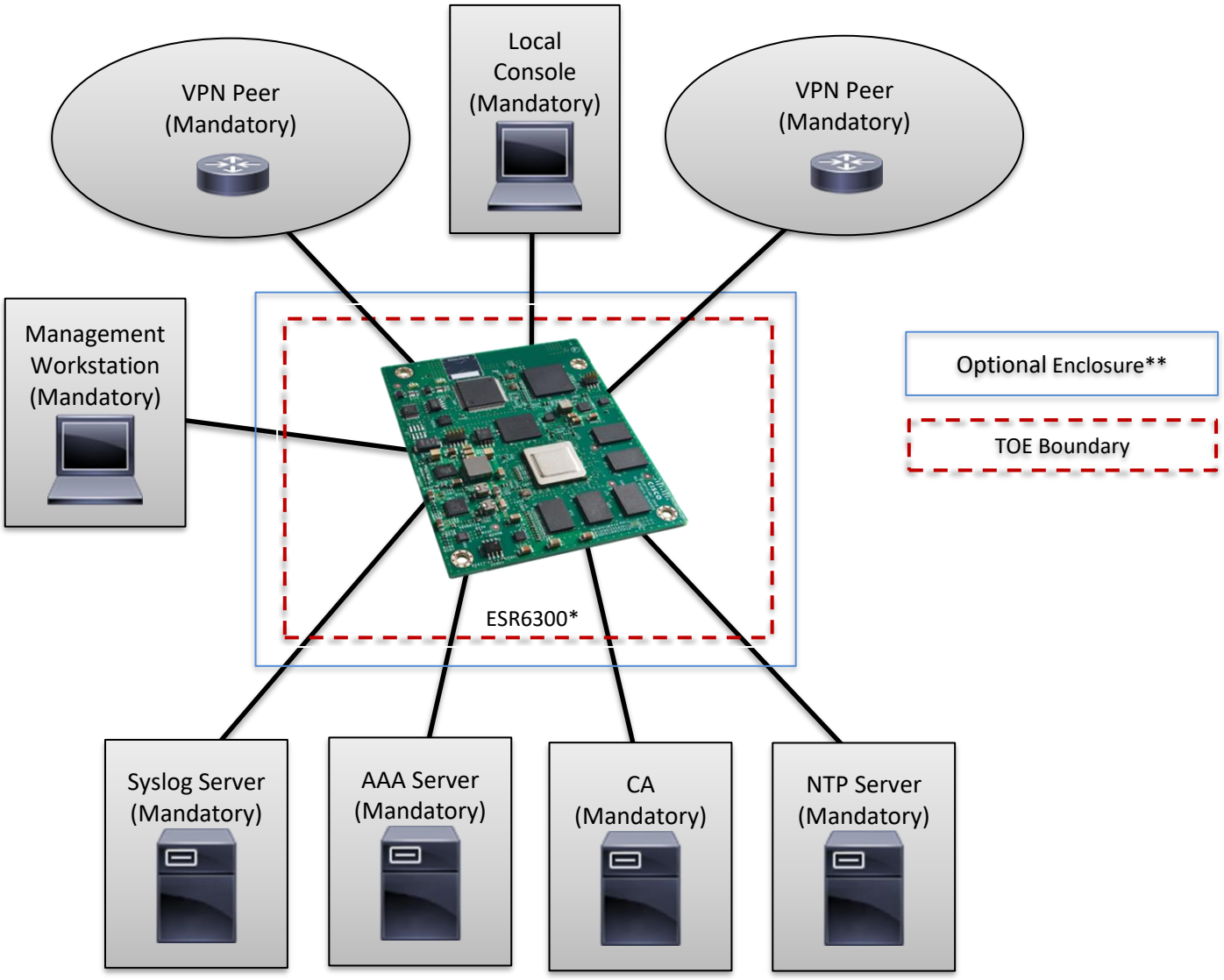


Figure 1 TOE Example Deployment for ESR6300

*** The ESR6300 physical chassis pictured includes a multi-pin BTB interface connector on the underside of the board that is fully integrated when purchased. See Table 5 for further information and images.**
**** 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 computational services. The enclosure used during testing is described above.**

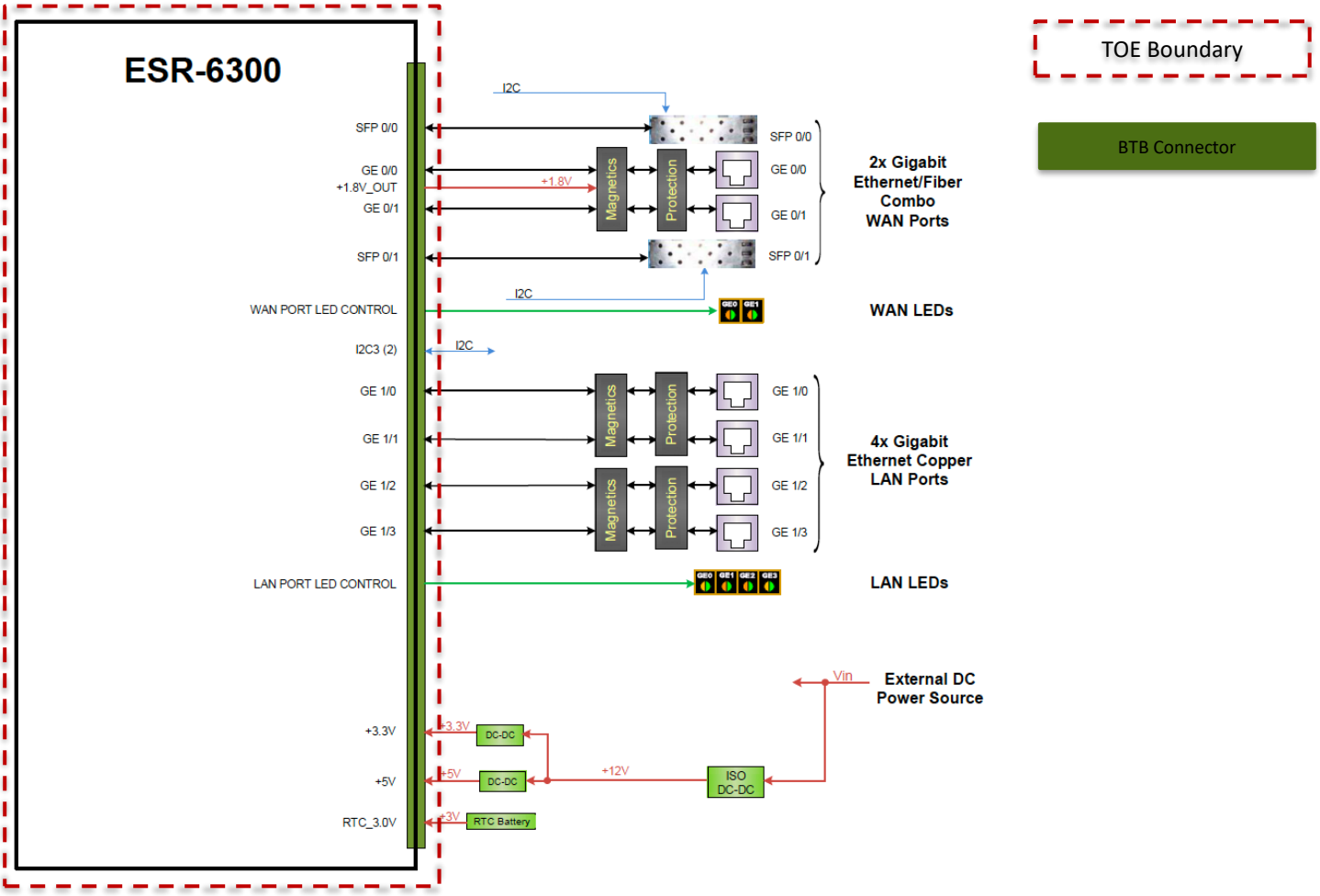


Figure 2: TOE Evaluated LAN/WAN Interfaces

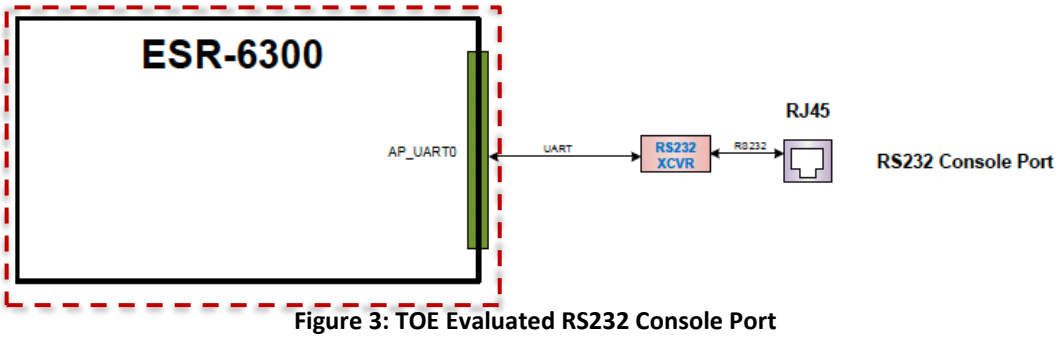


Figure 3: TOE Evaluated RS232 Console Port

The TOE example deployment in Figure 1 includes the following:

- The following are considered to be in the IT Environment:
  - VPN Peers
  - Management Workstation
  - RADIUS AAA (Authentication) Server
  - Audit (Syslog) Server
  - Local Console

- Certification Authority (CA)
- NTP Server

NOTE: While Figure 1 includes several non-TOE IT environment devices, the TOE is only the ESR6300 device. Only one TOE device is required for deployment in an evaluated configuration.

The certification only covers functionality when the TOE is in FIPS mode.

1.7 Physical Scope of the TOE

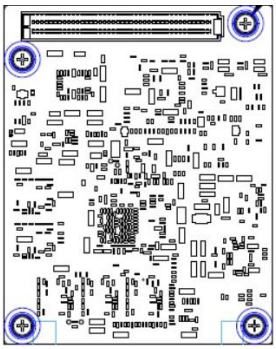
The TOE is a hardware and software solution that makes up the router models as follows:

- ESR-6300-NCP-K9
  Embedded Router Board without a cooling plate, (NCP = No Cooling Plate)
  Includes an integrated multi-pin BTB interface connector
- ESR-6300-CON-K9
  Embedded Router Board with cooling plate, (CON = Conduction cooled)
  Includes an integrated multi-pin BTB interface connector

The network, on which they reside, is considered part of the environment. The software is pre-installed and consists of the Cisco OS-XE software image Release 17.18. In addition, the software image is downloadable from the Cisco web site. A login ID and password is required to download the software image. The TOE consists of the following physical specifications as described in Table 4 below.

Table 4: Hardware Models and Specifications

Hardware	Picture	Features
Cisco Embedded Services Router (ESR6300) ESR-6300-NCP-K9 Embedded Router Board without a cooling plate, (NCP = No Cooling Plate) ESR-6300-CON-K9 Embedded Router Board with cooling plate, (CON = Conduction cooled)	 	**Processor** Marvell Armada 88F7040 **Physical dimensions** (H x W) 3.0 x 3.775 in. (76.2 x 95.885 mm) **Memory** • 4-GB DDR4 memory capacity (32-bit plus 4-bit ECC) • 4-GB usable (pSLC mode) eMMC flash **Interfaces** • 1 UART RS232 RJ45 console port • WAN Interfaces: 2 Combo Layer 3 GE WAN ports** • LAN Interfaces: 4 Layer 2 GE LAN ports **Power** • 3.3V and 5V power inputs ** A Combo port is a GE port and a SFP port that share the same switch fabric and port number. Each combo port uses different pins and are two different physical ports that can only be used one at a time.

Hardware	Picture	Features
Multi-pin BTB interface connector – Pictured on the top left of the board and is fully integrated on each hardware model listed above and provides pins dedicated for power input, ethernet ports, and console ports.		Refer to Annex A in the Guidance Document (AGD) for hardware technical guidance on the ESR6300 board layout and dimensions and Multi-pin BTB Interface Connector description that includes pinout mapping descriptions for network interfaces and power inputs.

Note: 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.

1.8 Logical Scope of the TOE

The TOE is comprised of several security features. Each of the security features identified above consists of several security functionalities, as identified below.

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Packet Filtering
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v3.0e, PKG_SSH_V1.0, and MOD_VPNGW v1.3 as necessary to satisfy testing/assurance measures prescribed therein.

1.8.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations and manages audit data storage. The TOE provides the administrator with a circular audit trail. The TOE is configured to transmit its audit messages to an external syslog server over an encrypted channel.

1.8.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operational Environment = Marvell Armada 88F7040). The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5b (see Table 5 for certificate references).

Table 5 FIPS References

SFR	Selection	Algorithm	Implementation	Standard	Certificate Number
FCS_CKM.1 – Cryptographic Key Generation	2048 3072	RSA	IC2M	FIPS PUB 186-4	A4354
FCS_CKM.1 – Cryptographic Key Generation and Verification	P-256 P-384	ECDSA	IC2M	FIPS PUB 186-4	A4354
FCS_CKM.1 – Cryptographic Key Generation	DH-14, DH-15, DH-16	FFC with safe-primes	IC2M	NIST SP 800-56A Rev 3	Tested with a known good implementation
FCS_CKM.2 – Cryptographic Key Establishment	P-256 P-384	KAS-ECC	IC2M	NIST SP 800-56A Rev 3	A4354
FCS_CKM.2 – Cryptographic Key Establishment	DH-14, DH-15, DH-16	FFC with safe-primes	IC2M	NIST SP 800-56A Rev 3	Tested with a known good implementation
FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CBC-128 AES-CBC-192 AES-CBC-256 AES-GCM-128 AES-GCM-192 AES-GCM-256	AES	IC2M	ISO/IEC 18033-3 (AES) ISO/IEC 10116 (CBC) ISO/IEC 19772 (GCM)	A4354
FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)	2048 3072	RSA	IC2M	FIPS PUB 186-4	A4354
FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)	P-384	ECDSA	IC2M	FIPS PUB 186-4	A4354
FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)	SHA-1 SHA-256 SHA-384 SHA-512	SHS	IC2M	ISO/IEC 10118-3:2004	A4354
FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256 HMAC-SHA-384	HMAC	IC2M	ISO/IEC 9797-2:2011	A4354
FCS_RBG_EXT.1– Random Bit Generation	CTR_DRBG (AES) 256 bits	DRBG	IC2M	ISO/IEC 18031:2011	A4354

The TOE provides cryptography in support of VPN connections and remote administrative management via SSHv2 and IPsec to secure the transmission of audit records to the remote syslog server. In addition, IPsec is used to secure the session between the TOE and the authentication servers.

The cryptographic services provided by the TOE are described in Table 6 below:

Table 6 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Internet Key Exchange	Used to establish initial IPsec session.
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in IPsec session establishment. Used in SSH session establishment. X.509 certificate signing

Cryptographic Method	Use within the TOE
SP 800-90 RBG	Used in IPsec session establishment. Used in SSH session establishment. Used for random number generation, key generation and seeds to asymmetric key generation
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
AES	Used to encrypt IPsec session traffic. Used to encrypt SSH session traffic.
HMAC	Used for keyed hash, integrity services in IPsec and SSH session establishment.
RSA	Used in IKE protocols peer authentication Used to provide cryptographic signature services
ECDSA	Used to provide cryptographic signature services Used in Cryptographic Key Generation Used as the Key exchange method for IPsec
FFC DH	Used as the Key exchange method for SSH and IPsec
ECC DH	Used as the Key exchange method for IPsec

1.8.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The TOE supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE supports the use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections.

The TOE provides an automatic lockout when a user attempts to authenticate and enters invalid information. After a defined number of authentication attempts fail exceeding the configured allowable attempts, the user is locked out until an authorized administrator can enable the user account.

1.8.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage:

- Administration of the TOE locally and remotely;

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- NTP configurations;
- The timestamps maintained by the TOE;
- Update to the TOE and verification of the updates;
- Configuration of IPsec functionality.

The TOE supports two separate administrator roles: non-privileged administrator and privileged administrator. Only the privileged administrator can perform the above security relevant management functions. Management of the TSF data is restricted to Security Administrators. The ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE is restricted to authorized administrators.

Administrators can create configurable login banners to be displayed at time of login and can also define an inactivity timeout for each admin interface to terminate sessions after a set period of inactivity.

1.8.5 Packet Filtering

The TOE provides packet filtering and secure IPsec tunneling. The tunnels can be established between two trusted VPN peers and the TOE. More accurately, these tunnels are sets of security associations (SAs). The SAs define the protocols and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per the ESP security protocol. An authorized administrator can define the traffic that needs to be protected via IPsec by configuring access lists (permit, deny, log) and applying these access lists to interfaces using crypto map sets.

1.8.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords. Additionally, Cisco IOS-XE is not a general-purpose operating system and access to Cisco IOS-XE memory space is restricted to only Cisco IOS-XE functions.

The TOE has an internal clock; the TOE, however, synchronizes time with an NTP server and then internally maintains the date and time. This date and time are used as the timestamp that is applied to audit records generated by the TOE.

The TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software. Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads.

Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

1.8.7 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. Sessions can also be terminated if an Authorized Administrator enters the “exit” command.

The TOE can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

1.8.8 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers. The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog

server, as well as to protect communications with a CA or remote administrative console. In addition, IPsec is used to secure the session between the TOE and the remote authentication servers and uses NTPv4 to secure the connection to the NTP server.

1.9 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 7 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 Document (AGD). The exclusion of this functionality does not affect compliance to the NDcPP v3.0e and MOD_VPNGW v1.3.

In addition to the explicitly stated exclusion above, it must be noted that any functionality not discussed in the Logical Scope of the TOE, Section 1.8, has not been covered by this evaluation effort. The evaluation is limited only to the capabilities described in the NDcPP v3.0e and MOD_VPNGW v1.3.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

2.2 Protection Profile Conformance

The TOE and ST demonstrate exact conformance with the protection Profiles, Functional Packages, and Modules as listed below. This ST applies the NIAP Technical Decisions as described in the table below.

- PP Configuration Document for NDcPP-VPNGW v2.0:
  - collaborative Protection Profile for Network Devices, Version 3.0e (CPP_ND_V3.0E)
  - PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_V1.3)
- Functional Package for Secure Shell (SSH), Version 1.0 (PKG_SSH_V1.0)

Table 8: NIAP Technical Decisions

TD Identifier	TD Name	Protection Profiles	Publication Date	Applicable?
TD0923	NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2	CPP_ND_V3.0E	06/25/2025	Yes
TD0921	NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment	CPP_ND_V3.0E	06/25/2025	Yes
TD0909	Updates to FCS_SSH_EXT.1.1 App Note in SSH FP 1.0	PKG_SSH_V1.0	04/16/2025	Yes
TD0900	NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	CPP_ND_V3.0E	02/27/2025	Yes
TD0899	NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	CPP_ND_V3.0E	03/06/2025	No, SFR not claimed
TD0886	Clarification to FAU_STG_EXT.1 Test 6	CPP_ND_V3.0E	2024.10.16	Yes
TD0880	NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	CPP_ND_V3.0E	2024.09.17	Yes
TD0879	NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	CPP_ND_V3.0E	2024.09.17	No – SFR not claimed
TD0878	Updating FIPS 186-4 to 186-5 in MOD_VPNGW_V1.3	MOD_VPNGW_v1.3	2025.01.30	Yes
TD0868	NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	CPP_ND_V3.0E	2024.09.17	Yes
TD0838	PPK Configurability in FIA_PSK_EXT.1.1	MOD_VPNGW_v1.3	2024.06.28	Yes
TD0836	NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	CPP_ND_V3.0E	2024.04.25	Yes

TD Identifier	TD Name	Protection Profiles	Publication Date	Applicable?
TD0824	Aligning MOD_VPNGW 1.3 with NDcPP 3.0E	MOD_VPNGW_v1.3	2024.04.25	Yes
TD0811	Correction to Referenced SFR in FIA_PSK_EXT.3 Test	MOD_VPNGW_v1.3	2024.01.02	Yes
TD0781	Correction to FIA_PSK_EXT.3 EA for MOD_VPNGW_v1.3	MOD_VPNGW_v1.3	2023.09.11	No, SFR not claimed
TD0777	Clarification to Selections for Auditable Events for FCS_SSH_EXT.1	PKG_SSH_V1.0	2023.08.23	Yes
TD0732	FCS_SSHS_EXT.1.3 Test 2 Update	PKG_SSH_V1.0	2023.05.19	Yes
TD0695	Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package	PKG_SSH_V1.0	2022.12.14	Yes
TD0682	Addressing Ambiguity in FCS_SSHS_EXT.1 Tests	PKG_SSH_V1.0	2022.12.13	Yes

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profile, PP-Module and Extended Package:

- collaborative Protection Profile for Network Devices (NDcPP) Version 3.0e
- Functional Package for Secure Shell (SSH), Version 1.0
- PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.3

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organizational Security Policies included in the Security Target represent the Assumptions, Threats, and Organizational Security Policies specified in the collaborative Protection Profile for Network Devices (NDcPP) Version 3.0e, Functional Package for Secure Shell (SSH), Version 1.0, and PP-Module for Virtual Private Network (VPN) Gateway (MOD_VPNGW), Version 1.3 for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the NDcPP Version 3.0e, PKG_SSH_V1.0, and MOD_VPNGW v1.3 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the NDcPP v3.0e, PKG_SSH_V1.0, and MOD_VPNGW v1.3 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in the NDcPP Version 3.0e, PKG_SSH_V1.0, and MOD_VPNGW v1.3.

3 Security Problem Definition

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Organizational security policies for the TOE as appropriate.

This document identifies assumptions as A.assumption with "assumption" specifying a unique name. Threats are identified as T.threat with "threat" specifying a unique name. Organizational Security Policies (OSPs) are identified as P.osp with "osp" specifying a unique name.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 9 TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

Assumption	Assumption Definition
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure 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.
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

3.2Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

Table 10 Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between Network Devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the Network Device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Nonvalidated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This

Threat	Threat Definition
	could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.DATA_INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network that may attempt to modify the data without authorization. If known malicious external devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices then the data contained in the communications may be susceptible to a loss of integrity.
T.NETWORK_ACCESS	Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network. From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network. From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled email servers, or, that access to the mail server must be done over an encrypted link.
T.NETWORK_DISCLOSURE	Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information. From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically configured ports on identified network nodes (e.g., web pages from a

Threat	Threat Definition
	designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information. From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.
T.NETWORK_MISUSE	Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network. From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services. From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.
T.REPLAY_ATTACK	If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions: • Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate • segment of the communications to replay as well in order to cause the desired outcome • No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured • traffic and replay it to cause the desired outcome if the recipient has no means to detect these

3.3 Organizational Security Policies

The following table lists the Organizational Security Policies imposed by an organization to address its security needs.

Table 11 Organizational Security Policies

Policy Name	Policy Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which Administrators consent by accessing the TOE.

4 Security Objectives

This section identifies the security objectives of the TOE and the IT Environment. The security objectives identify the responsibilities of the TOE and the TOE's IT environment in meeting the security needs.

This document identifies objectives of the TOE as O.objective with objective specifying a unique name. Objectives that apply to the IT environment are designated as OE.objective with objective specifying a unique name.

4.1 Security Objectives for the TOE

The following table, Security Objectives for the TOE, identifies the security objectives of the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies. The security objectives below have been drawn verbatim from [NDcPPv3.0e].

Table 12 Security Objectives for the TOE

TOE Objective	TOE Security Objective Definition
O.ADDRESS_FILTERING	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption or denial of services, and network-based reconnaissance, compliant TOE's will implement packet filtering capability. That capability will restrict the flow of network traffic between protected networks and other attached networks based on network addresses of the network nodes originating (source) or receiving (destination) applicable network traffic as well as on established connection information.
O.AUTHENTICATION	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (IPSec) will allow a VPN peer to establish VPN connectivity with another VPN peer and ensure that any such connection attempt is both authenticated and authorized. VPN endpoints authenticate each other to ensure they are communicating with an authorized external IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	To address the issues associated with unauthorized disclosure of information, inappropriate access to services, misuse of services, disruption of services, and network-based reconnaissance, compliant TOE's will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE.
O.FAIL_SECURE	There may be instances where the TOE's hardware malfunctions or the integrity of the TOE's software is compromised, the latter being due to malicious or non-malicious intent. To address the concern of the TOE operating outside of its hardware or software specification, the TOE will shut down upon discovery of a problem reported via the self-test mechanism and provide signature-based validation of updates to the TSF.
O.PORT_FILTERING	To further address the issues associated with unauthorized disclosure of information, etc., a compliant TOE's port filtering capability will restrict the flow of network traffic between protected networks and other attached networks based on the originating (source) or receiving (destination) port (or service) identified in the network traffic as well as on established connection information.
O.SYSTEM_MONITORING	To address the issues of administrators being able to monitor the operations of the VPN gateway, it is necessary to provide a capability to monitor system activity. Compliant TOEs will implement the ability to log the flow of network traffic. Specifically, the TOE will provide the means for administrators to configure packet filtering rules to 'log' when network traffic is found to match the configured rule. As a result, matching a rule configured to 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security associations (SAs) is auditable, not only between peer VPN gateways, but also with certification authorities (CAs).
O.TOE_ADMINISTRATION	TOEs will provide the functions necessary for an administrator to configure the packet filtering rules, as well as the cryptographic aspects of the IPsec protocol that are enforced by the TOE.

4.2 Security Objectives for the Environment

All of the assumptions stated in section 3.1 are considered to be security objectives for the environment. The following are the Protection Profile non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 13 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.CONNECTIONS	The TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, dated: April 2017* and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Assignment completed within a selection in the cPP: the completed assignment text is indicated with *italicized and underlined text*
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by adding a string starting with "/" (e.g., "FCS_COP.1/Hash") or appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the NDcPP itself, the formatting used in the NDcPP has been retained.

The following conventions were used to resolve conflicting SFRs between the NDcPP and MOD_VPNGW:

- All SFRs from MOD_VPNGW reproduced as-is
- SFRs that appear in both NDcPP and MOD_VPNGW are modified based on instructions specified in MOD_VPNGW

5.2TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 14 Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.1/VPN	VPN Audit data generation
	FAU_GEN.2	User identity association
	FAU_STG.1	Protected Audit Trail Storage
	FAU_STG_EXT.1	Protected Audit Event Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation
	FCS_CKM.1/IKE	Cryptographic Key Generation (for IKE peer authentication)
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (for cryptographic signature)
	FCS_COP.1/Hash	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1KeyedHash	Cryptographic Operation (for keyed-hash message authentication)
	FCS_COP.1/CMAC	Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)
	FCS_IPSEC_EXT.1	Extended: IPsec
	FCS_NTP_EXT.1	NTP Protocol
	FCS_SSH_EXT.1	SSH Protocol

Class Name	Component Identification	Component Name
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_RBG_EXT.1	Random Bit Generation
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_PSK_EXT.1	Pre-Shared Key Composition
	FIA_PSK_EXT.2	Generated Pre-Shared Keys
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
	FMT_MOF.1/ManualUpdate	Trusted Update - Management of security functions behaviour
	FMT_MOF.1/Services	Trusted Update - Management of TSF Data
	FMT_MOF.1/Functions	Management of Security Functions Behavior
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMF.1/VPN	Specification of Management Functions (VPN Gateway)
	FMT_SMR.2	Restrictions on security roles
FPF: Packet Filtering	FPF_RUL_EXT.1	Packet Filtering
FPT: Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_FLS.1/SelfTest	Failure with Preservation of Secure State (Self-Test Failures)
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	Extended: TSF Testing
	FPT_TST_EXT.3	Extended: TSF Testing
	FPT_TUD_EXT.1	Extended: Trusted Update
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_ITC.1/VPN	Inter-TSF Trusted Channel (VPN Communications)
	FTP_TRP.1/Admin	Trusted Path

5.3 SFRs from NDcPP and MOD_VPNGW

5.3.1 Security audit (FAU)

5.3.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;
b) All auditable events for the not specified level of audit; and
c) All administrative actions comprising:
    - o *Administrative login and logout (name of Administrator account shall be logged if individual accounts are required for Administrators).*
    - o *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
    - o *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
    - o *[Resetting passwords (name of related Administrator account shall be logged), no other actions, [Starting and stopping services]];*
d) Specifically defined auditable events listed in Table 15.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity ~~(if applicable),~~ and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the **c**PP/ST, *information specified in column three of Table 15*.

5.3.1.2 FAU_GEN.1/VPN Audit Data Generation (VPN Gateway)

FAU_GEN.1.1/VPN The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions
b) Indication that TSF self-test was completed
c) Failure of self-test
d) All auditable events for the [*not specified*] level of audit; and
e) *[auditable events defined in the Auditable Events for Mandatory Requirements Table 15]*.

FAU_GEN.1.2/VPN The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*additional information defined in the Auditable Events for Mandatory Requirements Table 15 for each auditable event, where applicable*].

Table 15 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.1/VPN	None.	None.
FAU_GEN.2	None.	None.
FAU_STG.1	None.	None.
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.

SFR	Auditable Event	Additional Audit Record Contents
FCS_CKM.1	None.	None.
FCS_CKM.1/IKE	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
FCS_NTP_EXT.1	• Configuration of a new time server. • Removal of configured time server.	Identity of new/removed time server.
FCS_SSH_EXT.1	Failure to establish an SSH session.	Reason for failure.
FCS_SSHS_EXT.1	No events specified.	N/A
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address)
FIA_PMG_EXT.1	None.	None.
FIA_PSK_EXT.1	None.	None.
FIA_PSK_EXT.2	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanisms.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	• Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store	• Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MOF.1/Services	None.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMF.1/VPN	All administrative actions	No additional information.
FMT_SMR.2	None.	None.
FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	• Source and destination addresses • Source and destination ports • Transport Layer Protocol
FPT_APW_EXT.1	None.	None.
FPT_FLS.1/SelfTest	No events specified	N/A
FPT_SKP_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).

SFR	Auditable Event	Additional Audit Record Contents
FPT_TST_EXT.1	None.	None.
FPT_TST_EXT.3	No events specified	N/A
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.
FPT_CAK_EXT.1	None.	None.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	• None • None • Reason for failure
FTP_ITC.1/VPN	• Initiation of the trusted channel. • Termination of the trusted channel. • Failure of the trusted channel functions.	• No additional information • No additional information • Identification of the initiator and target of failed trusted channel establishment attempt
FTP_TRP.1/Admin	• Initiation of the trusted path • Termination of the trusted path. • Failure of the trusted path functions.	• None. • None. • Reason for Failure

5.3.1.3 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.3.1.4 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2
The TSF shall be able to prevent unauthorised modifications to the stored audit records in the audit trail.

5.3.1.5 FAU_STG_EXT.1 Protected Audit Event Storage

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP_ITC.1.

FAU_STG_EXT.1.2 The TSF shall be able to store generated audit data on the TOE itself. In addition
[

- The TOE shall consist of a single standalone component that stores audit data locally,]

FAU_STG_EXT.1.3 The TSF shall maintain a [buffer] of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store [persistent] audit records locally with a minimum storage size of [*4096 to 2147483647 buffer size(s)*].

FAU_STG_EXT.1.5 The TSF shall [overwrite previous audit records according to the following rule*:[the newest audit record will overwrite the oldest audit record]],* when the local storage space for audit data is full.

FAU_STG_EXT.1.6 The TSF shall provide the following mechanisms for administrative access to locally stored audit records [ability to view locally].

5.3.2 Cryptographic Support (FCS)

5.3.2.1 FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: [

- RSA schemes using cryptographic key sizes of [*2048-bit, 3072-bit*] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", A.1;
- ECC schemes using 'NIST curves' [P-256, P-384] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2, or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.;
- FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]

] ~~and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: list of standards]~~.

5.3.2.2 FCS_CKM.1/IKE Cryptographic Key Generation (for IKE peer authentication)

FCS_CKM.1.1/IKE The TSF shall generate **asymmetric** cryptographic keys **used for IKE peer authentication** in accordance with a specified cryptographic key generation algorithm:
[

- **FIPS PUB 186-5 "Digital Signature Standard (DSS)," Appendix B.3 for RSA schemes**
- **FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix B.4 for ECDSA schemes and implementing "NIST curves" P-384 and [P-256]]**
  ] and[
- **FFC Schemes using "safe-prime" groups that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]**

] and specified cryptographic key sizes [*equivalent to, or greater than, a symmetric key strength of 112 bits*].

5.3.2.3 FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method: [

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";

- FFC Schemes using “safe-prime” groups that meet the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [groups listed in RFC 3526];

] ~~that meets the following: [assignment: list of standards]~~.

5.3.2.4 FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method

- *For plaintext keys in volatile storage, the destruction shall be executed by a* [single overwrite consisting of [zeroes]];
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that* [
  - logically addresses the storage location of the key and performs a [single] overwrite consisting of [zeroes]];

that meets the following: *No Standard*.

5.3.2.5 FCS_COP.1/DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)

FCS_COP.1.1/DataEncryption The TSF shall perform encryption/decryption in accordance with a specified cryptographic algorithm *AES* used in **[CBC, GCM] and [no other]** mode and cryptographic key sizes ***[*128 bits, 256 bits*]* and [192 bits]** that meet the following: AES as specified in ISO 18033-3, **[CBC as specified in ISO 10116, GCM as specified in ISO 19772] and [no other standards]**.

5.3.2.6 FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)

FCS_COP.1.1/SigGen The TSF shall perform *cryptographic signature services (generation and verification)* in accordance with a specified cryptographic algorithm

[

- RSA Digital Signature Algorithm,
- Elliptic Curve Digital Signature Algorithm

]

and cryptographic key sizes [

- For RSA: [2048 or 3072 bits]
- For ECDSA: [384 bits]

]

that meet the following: [

- For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

- For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST curves” [P-384]; ISO/IEC 14888-3, Section 6.4

].

5.3.2.7 FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)

FCS_COP.1.1/Hash The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ and **message digest sizes [160, 256, 384, 512] bits** that meet the following: *ISO/IEC 10118-3:2004*.

5.3.2.8 FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)

FCS_COP.1.1/KeyedHash The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-256, HMAC-SHA-384] ~~and cryptographic key sizes [*160-bit, 256-bit, 512-bit*]~~ and **message digest sizes [256, 384] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 'MAC Algorithm 2'.*

5.3.2.9 FCS_IPSEC_EXT.1 IPSEC Protocol

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC 4301.

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [tunnel mode, transport mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [**AES-CBC-128, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-256 (specified in RFC 4106)] and [AES-CBC-192 (specified in RFC 3602), AES-GCM-192 (specified in RFC 4106**)] together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA-256, HMAC-SHA-384].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [no other RFCs for extended sequence numbers], and [RFC 4868 for hash functions]].
- IKEv2 as defined in RFC 5996 and [with mandatory support for NAT traversal as specified in RFC 5996, section 2.23)], and [RFC 4868 for hash functions]

].

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the [IKEv1, IKEv2] protocol uses the cryptographic algorithms [AES-CBC-128, AES-CBC-192, AES-CBC-256 (specified in RFC 3602), AES-GCM-128, AES-GCM-256 (specified in RFC 5282)].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- IKEv1 Phase 1 SA lifetimes can be configured by ana Security Administrator based on [
  - length of time, where the time values can be configured between *[1 hour] and [24 hours]*;

  ].
- IKEv2 SA lifetimes can be configured by a Security Administrator based on [
  - length of time, where the time values can be configured between *[1 hour] and [24 hours]*;

  ].

]

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- IKEv1 Phase 2 SA lifetimes can be configured by a Security Administrator based on [
  - number of bytes
  - length of time, where the time values can be configured between *[1 hour] and [8 hours]*;

  ];
- IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [
  - number of bytes
  - length of time, where the time values can be configured between *[1 hour] and [8 hours]*;

  ]

]

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [*224 (for DH Group 14), 256 (for DH Group 19), 384 (for DH Group 20), 256 (for DH Group 15), and 384 (for DH Group 16)*] bits.

FCS_IPSEC_EXT.1.10 The TSF shall generate nonces used in [IKEv1, IKEv2] exchanges of length [

- according to the security strength associated with the negotiated DH group;
- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Groups

- **19 (256-bit Random ECP), 20 (384-bit Random ECP) according to RFC 5114 and**
  [
- [14 (2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP)] according to RFC 3526
  ].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 1, IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 2, IKEv2 CHILD_SA] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that **[IKEv1, IKEv2**] protocols perform peer authentication using [RSA] that use X.509v3 certificates that conform to RFC 4945 and [Pre-shared Keys that conform to RFC 8784].

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following fields and types: **Distinguished Name (DN),** [SAN: IP address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN, **no other reference identifier types**.].

5.3.2.16 FCS_NTP_EXT.1 NTP Protocol

FCS_NTP_EXT.1.1 The TSF shall use only the following NTP version(s) [NTP v4 (RFC 5905)].

FCS_NTP_EXT.1.2 The TSF shall update its system time using [

- [IPsec] to provide trusted communication between itself and an NTP time source.

].

FCS_NTP_EXT.1.3 The TSF shall not update NTP timestamp from broadcast and/or multicast addresses.

FCS_NTP_EXT.1.4 The TSF shall support configuration of at least three (3) NTP time sources in the Operational Environment.

5.3.2.17 FCS_SSHS_EXT.1 SSH Protocol

FCS_SSH_EXT.1.1 The TOE shall implement *SSH* acting as a [server] in accordance with that complies with RFCs 4251, 4252, 4253, 4254*,* [5647, 8308, 8332] and [*no other standard*].

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods: [

- *"*password" (RFC 4252*),*
- *"*publickey" (RFC 4252): *[*

  - rsa-sha2-256 (RFC 8332),
  - rsa-sha2-512 (RFC 8332),
  - ecdsa-sha2-nistp384 (RFC 5656),

]

] and no other methods.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*65,806 bytes*] in an SSH transport connection are dropped.

FCS_SSH_EXT.1.4 The TSF shall protect data in transit from unauthorised disclosure using the following mechanisms: [

- aes128-cbc (RFC 4253),
- aes256-cbc (RFC 4253),
- aes256-gcm@openssh.com (RFC 5647)

] and no other mechanisms.

FCS_SSH_EXT.1.5 The TSF shall protect data in transit from modification, deletion, and insertion using: [

- *hmac-sha2-256 (RFC 6668)*,
- *implicit*

] and no other mechanisms.

FCS_SSH_EXT.1.6 The TSF shall establish a shared secret with its peer using: [

diffie-hellman-group14-sha256 (RFC 8268), ecdh-sha2-nistp384 (RFC 5656)
] and no other mechanisms.

FCS_SSH_EXT.1.7 The TSF shall use *SSH KDF* as defined in [

- RFC 4253 (Section 7.2),

] to derive the following cryptographic keys from a shared secret: *session keys*.

FCS_SSH_EXT.1.8 The TSF shall ensure that [

- a rekey of the session keys,

] occurs when any of the following thresholds are met:

- one hour connection time
- no more than one gigabyte of transmitted data, or
- no more than one gigabyte of received data.

5.3.2.18 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall authenticate itself to its peer (SSH Client) using: [

- rsa-sha2-256 (RFC 8332),
- rsa-sha2-512 (RFC 8332),
- ecdsa-sha2-nistp384 (RFC 5656)].

5.3.2.19 FCS_RBG_EXT.1 Random Bit Generation

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [CTR_DRBG (AES)].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [[*1*] platform based noise source] with a minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.

5.3.3 Identification and authentication (FIA)

5.3.3.1 FIA_AFL.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1 to 25*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [*an authorized Administrator unlocks the locked user account]* is taken by an Administrator].

5.3.3.2 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“,”)”, *[“ “, “,”, “.”, “”””, “‘”, “|”, “+”, “-“. “=”, “.”. “,”, “/”, “\”. “<”, “>”, “ ”, “`”. “~”. “{“, “}”*]];

b) Minimum password length shall be *configurable to between* [*1*] and [*127*] characters.

5.3.3.3 FIA_ PSK_EXT.1 (2): Pre-Shared Key Composition

FIA_PSK_EXT.1.1 (2) The TSF shall be able to use pre-shared keys for IPsec and *[*IKEv2].

FIA_PSK_EXT.1.2 (2) The TSF shall be able to accept the following as pre-shared keys: [generate bit-based] keys.

5.3.3.4 FIA_ PSK_EXT.1: Generated Pre-Shared Keys

FIA_PSK_EXT.2.1 The TSF shall be able to [

- *accept externally generated pre-shared keys*
- *generate [256] bit-based pre-shared keys via FCS_RBG_EXT.1*.

]

5.3.3.5 FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [no other actions].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

FIA_UIA_EXT.1.3 The TSF shall provide the following remote authentication mechanisms [SSH password, SSH public key,] and [*external authentication server*]. The TSF shall provide the following local authentication mechanisms [*password-based, [no other authentication mechanism]]*.

FIA_UIA_EXT.1.4 The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.

5.3.3.6 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the **administrative** user while the authentication is in progress **at the local console**.

5.3.3.7 FIA_X509_EXT.1/Rev – X.509 Certificate Validation

FIA_X509_EXT.1.1/Rev The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates.**
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
    - *Server certificates presented for DTLS/TLS shall 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 presented for DTLS/TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
    - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/Rev The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

5.3.3.8 FIA_ X509_EXT.2 – X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for **IPsec and [no other protocols],** and [no additional uses].

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

5.3.3.9 FIA_ X509_EXT.3 – X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit, Country].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.3.4 Security management (FMT)

5.3.4.1 FMT_MOF.1/ManualUpdate Management of Security Functions Behaviour

FMT_MOF.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual updates to Security Administrators*.

5.3.4.2 FMT_MOF. 1/ Services Management of Security Functions Behaviour

FMT_MOF.1/Services The TSF shall restrict the ability to **start and stop** ~~the functions~~ **services** to *Security Administrators*.

5.3.4.3 FMT_MOF. 1/Functions Management of Security Functions Behaviour

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [modify the behaviour of] the functions [transmission of audit data to an external IT entity] to *Security Administrators*.

5.3.4.4 FMT_MTD.1/CoreData Management of TSF Data

FMT_MTD.1/CoreData The TSF shall restrict the ability to *manage* the *TSF data* to *Security Administrators*.

5.3.4.5 FMT_MTD.1/CryptoKeys Management of TSF Data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to [[*manage*]] the [*cryptographic keys* ***and certificates used for VPN operation]*** *to [Security Administrators]*.

5.3.4.6 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the remote session inactivity time before session termination;*
- *Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;*

[

- Ability to start and stop services;
- Ability to configure local audit behavior (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size);
- Ability to modify the behaviour of the transmission of audit data to an external IT entity;
- Ability to manage the cryptographic keys;
- Ability to configure the cryptographic functionality;
- Ability to configure thresholds for SSH rekeying;
- Ability to configure the lifetime for IPsec SAs;
- Ability to re-enable an Administrator account;
- Ability to configure NTP;
- Ability to configure the reference identifier for the peer;
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
- Ability to administer the TOE locally;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to manage the trusted public keys database;
- No other capabilities].

5.3.4.7 FMT_SMF.1/VPN Specification of Management Functions (VPN Gateway)

FMT_SMF.1.1/VPN The TSF shall be capable of performing the following management functions [

- *Definition of packet filtering rules*
- *Association of packet filtering rules to network interfaces*
- *Ordering of packet filtering rules by priority*

  [
- No other capabilities]].

5.3.4.8 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator.*

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE remotely*

are satisfied.

5.3.5 Packet Filtering (FPF)

5.3.5.1 FPF_RUL_EXT.1 Packet Filtering

FPF_RUL_EXT.1.1 The TSF shall perform packet filtering on network packets processed by the TOE.

FPF_RUL_EXT.1.2 The TSF shall allow the definition of packet filtering rules using the following network protocols and protocols fields: [

- *IPv4 (RFC 791)*

    - *source address*
    - *destination address*
    - *protocol*
- *IPv6 (RFC 8200)*
    - *source address*
    - *destination address*
    - *next header (protocol)*
- *TCP (RFC 793)*
    - *source port*
    - *destination port*
- *UDP (RFC 768)*
    - *source port*
    - *destination port*

]

FPF_RUL_EXT.1.3 The TSF shall allow the following operations to be associated with packet filtering rules: permit and drop with the capability to log the operation.

FPF_RUL_EXT.1.4 The TSF shall allow the packet filtering rules to be assigned to each distinct network interface.

FPF_RUL_EXT.1.5 The TSF shall process the applicable packet filtering rules (as determined in accordance with FPF_RUL_EXT.1.4) in the following order: [*Administrator-defined*.]

FPF_RUL_EXT.1.6 The TSF shall drop traffic if a matching rule is not identified.

5.3.6 Protection of the TSF (FPT)

5.3.6.1 FPT_APW_EXT.1 Extended: Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store administrative passwords in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext administrative passwords.

5.3.6.2 FPT_FLS.1/SelfTest Failure with Preservation of Secure State (Self-Test Failures)

FPT_FLS.1.1/SelfTest The TSF shall **shut down** when the following types of failures occur: [*failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests.]*

5.3.6.3 FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.3.6.4 FPT_STM_EXT.1 Reliable Time Stamps

FPT_STM_EXT.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_STM_EXT.1.2 The TSF shall [synchronise time with an NTP server].

5.3.6.5 FPT_TST_EXT.1: TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests [during initial start-up (on power on), periodically during normal operation] to demonstrate the correct operation of the TSF: **noise-source health tests**, [

- *AES Known Answer Test*
- *RSA Signature Known Answer Test (both signature/verification)*
- *RNG/DRBG Known Answer Test*
- *HMAC Known Answer Test*
- *SHA-1/256/384/512 Known Answer Test*
- *ECDSA Self Test (both signature/verification)*
- *Software Integrity Test*

].

5.3.6.6 FPT_TST_EXT.3: Self-Test with Defined Methods

FPT_TST_EXT.3.1 The TSF shall run a suite of the following self-tests [*[when loaded for execution]*] to demonstrate the correct operation of the TSF: [*integrity verification of stored executable code*].

FPT_TST_EXT.3.2 The TSF shall execute the self-testing through [*a TSF-provided cryptographic service specified in FCS_COP.1/**SigGen***].

5.3.6.7 FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software and [no other TOE firmware/software version].

FPT_TUD_EXT.1.2 The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [no other update mechanism].

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a **digital signature mechanism and** [***no other mechanisms***] prior to installing those updates.

5.3.6.8 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [

- terminate the session]

after a Security Administrator-specified time period of inactivity.

5.3.6.9 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1: The TSF shall terminate **a remote** interactive session after a *Security Administrator-configurable time interval of session inactivity*.

5.3.6.10 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow ~~user~~ **Administrator**-initiated termination of the ~~user's~~ **Administrator**'s own interactive session.

5.3.6.11 FTA_TAB.1 Default TOE Access Banners

FTA_TAB.1.1: Before establishing ~~a~~ **an administrative** user session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding ~~unauthorized~~ use of the TOE.

5.3.7 Trusted Path/Channels (FTP)

5.3.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1: The TSF shall **be capable of using** [***IPSEC***] **to** provide a **trusted** communication channel between itself and ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, [authentication server *[NTP Server]*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure **and detection of modification of the channel data**.

FTP_ITC.1.2 The TSF shall permit [*the TSF, **the authorized IT entities***] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for *[communications with the following:*

- *external audit servers using IPsec,*
- *remote AAA servers using IPsec,*
- *NTP server using IPSec*

]

5.3.7.2 FTP_ITC.1/VPN Inter-TSF Trusted Channel (VPN Communications)

FTP_ITC.1.1/VPN The TSF shall **be capable of using IPSEC to** provide a communication channel between itself and **authorized IT entities supporting VPN communications** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

FTP_ITC.1.2/VPN The TSF shall permit [*the authorized IT entities*] to initiate communication via the trusted channel.

FTP_ITC.1.3/VPN The TSF shall initiate communication via the trusted channel for [remote VPN gateways or peers].

5.3.7.3 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin The TSF shall **be capable of using [IPsec, SSH] to** provide a communication path between itself and **authorized** remote **Administrators** ~~users~~ that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure **and provides detection of modification of the channel data**.

FTP_TRP.1.2/Admin The TSF shall permit remote **Administrators** ~~users~~ to initiate communication via the trusted path.

FTP_TRP.1.3/Admin The TSF shall require the use of the trusted path for *initial Administrator authentication and all remote administration actions*.

5.4 TOE SFR Dependencies Rationale for SFRs Found in PP

The NDcPP v3.0e, PKG_SSH_V1.0 and MOD_VPNGW v1.3 contain all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PP and EP have been approved.

5.5 Security Assurance Requirements

5.5.3 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPP which are derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below:

Table 16 Assurance Measures

Assurance Class	Components	Components Description
Security Target (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.1	Security objectives for the operational environment
	ASE_REQ.1	Stated security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE summary specification
Development (ADV)	ADV_FSP.1	Basic Functional Specification
Guidance documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
	ALC_FLR.2	Flaw reporting procedures
Tests (ATE)	ATE_IND.1	Independent testing - conformance
Vulnerability assessment (AVA)	AVA_VAN.1	Cisco will provide a list of TOE hardware and software components. The lab will conduct the additional vulnerability testing as prescribed by the MOD_VPNGW_v1.3.

5.5.4 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPPv3.0e, PKG_SSH_V1.0 and MOD_VPNGW v1.3. As such, the NDcPP SAR rationale is deemed acceptable since the PPs have been validated.

5.6 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. The table below lists the details.

Table 17 Assurance Measures

Component	How requirement will be met
ADV_FSP.1	There are no specific assurance activities associated with ADV_FSP.1. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other assurance activities being performed. The functional specification is comprised of the information contained in the AGD_OPE and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ALC_CMC.1 ALC_CMS.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error. The TOE will also be provided along with the appropriate administrative guidance.
ALC_FLR.2	Cisco documents the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

6 TOE Summary Specification

6.3 TOE Security Functional Requirement Measures

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 18 How TOE SFRs Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record whenever any of the audited events identified in Table 15 or additional events from FAU_GEN.1.1 or FAU_GEN.1.1/VPN occurs. The types of events that cause audit records to be generated include: startup and shutdown of the audit mechanism, 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 within the FAU_GEN.1 SFR, "Auditable Events Table"). 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 such as generating keys, including the type of key and a key reference. Additionally, the startup and shutdown of the audit functionality is audited. The 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. As noted above, the information includes at least all of the required information. Example audit events are included below: Nov 19 2022 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test activated by user: lab) Nov 19 2022 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software checksum ... passed) Nov 19 2022 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encryption/decryption ... passed) Nov 19 2022 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (3DES encryption/decryption ... passed) Nov 19 2022 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA hashing ... passed) Nov 19 2022 13:55:59: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (AES encryption/decryption ... passed) In the above log events a date and timestamp is displayed as well as an event description "CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test)". The subject identity where a command is directly run by a user is displayed "user: lab." The outcome of the command is displayed: "passed". The logging buffer size can be configured from a range of 4096 (default) to 4,294,967,295 bytes. It is noted to not make the buffer size too large because the TOE could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the TOE. However, this value is the maximum available, and the buffer size should not be set to this amount. The administrator can also configure a 'configuration logger' to keep track of configuration changes made with the command-line interface (CLI). The administrator can configure the size of the configuration log from 1 to 1000 entries (the default is 100). The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc. The logs can be saved to flash memory, so records are not lost in case of failures or restarts. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The administrator can set the level of the audit records to be displayed on the console or sent to the syslog server. For instance, all emergency, alerts, critical, errors, and warning messages can be sent to the console alerting the administrator that some action needs to be taken as these types of messages

TOE SFRs	How the SFR is Met
	mean that the functionality of the TOE is affected. All notifications and information type message can be sent to the syslog server. The audit records are transmitted using IPSec tunnel to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record, and all permit traffic is denied until the communications is re-established. When the FIPS crypto tests are performed during startup, the messages are displayed only on the console. Once the box is up and operational and the crypto self test command is entered, then the result messages would be displayed on the console and will also be logged. For the TSF self-test, successful completion of the self-test is indicated by reaching the log-on prompt. If there are issues, the applicable audit record is generated and displayed on the console. When the incoming traffic to the TOE exceeds what the interface can handle, the packets are dropped at the input queue itself and there are no error messages generated.
FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. A sample audit record is below: Jun 18 2022 11:17:20.769: AAA/BIND(0000004B): Bind i/f Jun 18 2022 11:17:20.769: AAA/AUTHEN/LOGIN (0000004B): Pick method list 'default' Jun 18 2022 11:17:26 UTC: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 100.1.1.5] [localport: 22] at 11:17:26 UTC Mon Jun 18 2012
FAU_STG_EXT.1	The TOE is configured to export syslog records to a specified, external syslog server in real-time. The TOE protects communications with an external syslog server via IPsec. If the IPsec connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents when connected to the syslog server. For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 4096 (default) to 2147483647 bytes of available disk space Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.
FCS_CKM.1 FCS_CKM.1/IKE FCS_CKM.2	The TOE implements DH-14, DH-15, and DH-16 establishment schemes that NIST Special Publication 800-56A Revision 3 and RFC 3526 and RFC 3526 and DH-19 (256-bit Random ECP), and DH-20 (384-bit Random ECP) according to RFC 5114. The TOE acts as both a sender and receiver for Diffie-Helman based key establishment schemes. The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP 800-56A and with section 6. Asymmetric cryptographic keys used for IKE peer authentication are generated according to FIPS PUB 186-4, Appendix B.3 for RSA schemes and Appendix B.4 for ECDSA schemes, and NIST Special Publication 800-56A Revision 3 for FCC Schemes using ‘safe-prime’ groups. The TOE can create an RSA public-private key pair, with a minimum RSA key size of 2048-bits (for CSfC purposes, the TOE is capable of a minimum RSA key size of 3072-bit) and ECDSA key pairs using NIST curves P-256 and P-384, and FFC key pairs. RSA schemes can be used to generate a Certificate Signing Request (CSR). Through use of Simple Certificate Enrollment Protocol (SCEP), the TOE can: send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its X.509v3 certificate from the CA. Integrity of the CSR and certificate during transit are assured through use of digitally signatures (encrypting the hash of the TOE’s public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>IOS-XE Software supports embedded PKI client functions that provide secure mechanisms for distributing, managing, and revoking certificates. In addition, the IOS-XE Software includes an embedded certificate server, allowing the router to act as a certification authority on the network.

The TOE can also use the X.509v3 certificate for securing IPsec sessions. The TOE provides cryptographic signature services using ECDSA that meets FIPS 186-4, “Digital Signature Standard” with NIST curves P-256, P-384, and RSA that meets FIPS PUB 186-4, “Digital Signature Standard”.
<table>
<tr><th>Scheme</th><th>SFR</th><th>Service</th></tr>
<tr><td rowspan="3">RSA
Key generation</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
<tr><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
<tr><td>FIA_X509_EXT.1/Rev
FIA_X509_EXT.2
FIA_X509_EXT.3</td><td>RSA certificate based authentication</td></tr>
<tr><td rowspan="2">ECC
Key generation
Key establishment</td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity

Support for protecting VPN traffic</td></tr>
<tr><td>FIA_X509_EXT.1/Rev
FIA_X509_EXT.2
FIA_X509_EXT.3</td><td>ECDSA signature based authentication</td></tr>
<tr><td rowspan="2">FFC
Key generation
Key establishment</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
<tr><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
</table></td></tr>
<tr><td>FCS_CKM.4</td><td>See Table 19: TOE Key Zeroization in Section 7 Key Zeroization. The information provided in the table includes all of the all secrets, keys and associated values, the description, and the method used to zeroization when no longer required for use.

The information is provided in the reference section for ease and readability of all of the all secrets, keys and associated values, their description and zeroization methods.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TOE provides symmetric encryption and decryption capabilities using AES in GCM and CBC mode (128, 192 and 256 bits) as described in ISO 18033-3, ISO 19772 and ISO 10116 respectively. Please see CAVP certificate in Table 5 for validation details. AES is implemented in the IPSec and SSH protocols. The TOE provides AES encryption and decryption in support of IPSec and SSHv2 for secure communications.</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater as specified in ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3.

In addition, the TOE will provide cryptographic signature services using ECDSA with key size of 256 and 384 bits as specified in FIPS PUB 186-4, “Digital Signature Standard”. The TOE provides cryptographic signature services using ECDSA that meets ISO/IEC 14888-3, Section 6.4 with NIST curves P-256 and P-384.

Please refer to Table 5 for all the CAVP references.</td></tr>
<tr><td>FCS_COP.1/Hash
FCS_COP.1/KeyedHash</td><td>The TOE provides cryptographic hashing services using SHA-1, SHA-256, and SHA-384 and SHA-512 as specified in ISO/IEC 10118-3:2004.</td></tr>
</table>

TOE SFRs	How the SFR is Met
	The TOE provides keyed-hashing message authentication services using HMAC-SHA-256, which operates on 512-bit blocks, and HMAC-SHA-384, which operates on 1024-bit blocks of data, with key sizes and message digest sizes 256 bits and 384 bits respectively) as specified in ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". For IKE (ISAKMP) hashing, administrators can select either of HMAC-SHA-256 and/or HMAC-SHA-384 (with message digest sizes of 256 and 384 bits respectively) to be used with remote IPsec endpoints. SHA-512 hashing is used for verification of software image integrity. Cisco provides a SHA512 checksum to validate images downloaded at www.cisco.com. The TOE provides Secure Hash Standard (SHS) hashing in support of SSH for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands. For IPsec SA authentication integrity options administrators can select either of esp-sha256-hmac, or esp-sha384-hmac (with message digest sizes of 256 and 384 bits respectively) to be part of the IPsec SA transform-set to be used with remote IPsec endpoints. Please see CAVP certificate in Table 5 for validation details.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in ISO/IEC 18031:2011 seeded by an entropy source that accumulates entropy from a TSF-platform based noise source (for CSfC purposes, AES-256). The deterministic RBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.
FCS_IPSEC_EXT.1	The TOE implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network as specified in RFC 4301. The IPsec implementation provides both VPN peer-to-peer TOE capabilities. The VPN peer-to-peer tunnel allows the TOE and another router to establish an IPsec tunnel to secure the passing of route tables (user data). Another configuration in the peer-to-peer configuration is to have the TOE be set up with an IPsec tunnel with a VPN peer to secure the session between the TOE and syslog server. In addition to tunnel mode, which is the default IPsec mode, the TOE also supports transport mode, allowing for only the payload of the packet to be encrypted. If tunnel mode is explicitly specified, the router will request tunnel mode and will accept only tunnel mode. The TOE implements IPsec to provide both certificates and pre-shared key-based authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the external network. The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services. The IPsec protocol ESP, as defined by RFC 4303, is implemented using the cryptographic algorithms AES-CBC-128 (RFC 3602), AES-CBC-256 (RFC 3602), AES-GCM-128 (RFC 4106), AES-GCM-256 (RFC 4106) and AES-CBC-192 (RFC 3602), AES-GCM-192 (RFC 4106) together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA-256, HMAC-SHA-384. Preshared keys can be configured using the 'crypto isakmp key' key command and may be proposed by each of the peers negotiating the IKE establishment. IPsec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPsec Security Association (SA). The strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 1 and IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 2 or IKEv2 CHILD_SA connection. The IKE protocols implement Peer Authentication using RSA and ECDSA along with X.509v3 certificates, or pre-shared keys. When certificates are used for authentication, the distinguished name (DN) is verified to ensure the certificate is valid and is from a valid entity. The DN naming attributes in the certificate is compared with the expected DN naming attributes and deemed valid if the attribute types are the same and the values are the same and as expected. The fully qualified domain name (FQDN) can also be used as

TOE SFRs	How the SFR is Met
	verification where the attributes in the certificate are compared with the expected SAN: IPv4 address, SAN: Fully Qualified Domain Name (FQDN), SAN: user FQDN. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including: • The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based), • The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and • The agreement of secure bulk data encryption AES keys for use with ESP. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation. The TOE supports both IKEv1 and IKEv2 session establishment. As part of this support, the TOE can be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode using the 'crypto ISAKMP aggressive-mode disable' command. The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using the following command, lifetime. The time values for Phase 1 SAs can be limited up to 24 hours and for Phase 2 SAs up to 8 hours. The Phase 2 SA lifetimes can also be configured by an Administrator based on number of packets. The TOE supports Diffie-Hellman Group 14, 16, 19, 20 and 15. Group 14 (2048-bit keys) can be set by using the "group 14" command in the config mode. The nonces used in IKE exchanges are generated in a manner such that the probability that a specific nonce value will be repeated during the life a specific IPsec SA is less than 1 in 2^[128]. The secret value 'x' used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) is generated using a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG). Preshared keys can be configured using the 'crypto isakmp key' or 'crypto ikev2 keyring' commands and may be proposed by each of the peers negotiating the IKE establishment. The TOE supports configuring the maximum amount of traffic that is allowed to flow for a given IPsec SA using the following command, 'crypto ipsec security-association lifetime'. The default amount is 2560KB, which is the minimum configurable value. The maximum configurable value is 4GB. The TOE provides AES-CBC-128, AES-CBC-192 and AES-CBC-256 for encrypting the IKEv1 payloads, and AES-CBC-128, AES-CBC-192, AES-CBC-256, AES-GCM-128and AES-GCM-256 for IKEv2 payloads. The administrator is instructed in the AGD to ensure that the size of key used for ESP must be greater than or equal to the key size used to protect the IKE payload. The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 19 (256-bit Random ECP), 20 (384-bit Random ECP), 15 (3072-bit MODP), and 16 (4096-bit MODP) in support of IKE Key Establishment. These keys are generated using the AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90, Table 2 in NIST SP 800-57 "Recommendation for Key Management –Part 1: General" and the following corresponding key sizes (in bits) are used: 224 (for DH Group 14), 256 (for DH Group 19), 384 (for DH Group 20), 256 (for DH Group 15), and 384 (for DH Group 16) bits. The DH group can be configured by issuing the following command during the configuration of IPsec: TOE-common-criteria (config)# group 14 This command selects DH Group 14 (2048-bit MODP) for IKE and this sets the DH group offered during negotiations. IPsec provides secure tunnels between two peers, such as two routers. An authorized administrator defines which packets are considered sensitive and should be sent through these secure tunnels. When the IPsec peer recognizes a sensitive packet, the peer sets up the appropriate secure tunnel and sends the packet through the tunnel to the remote peer. More accurately, these tunnels are sets of security associations (SAs) that are established between two IPsec peers. The SAs define the protocols

TOE SFRs	How the SFR is Met
	and algorithms to be applied to sensitive packets and specify the keying material to be used. SAs are unidirectional and are established per security protocol (AH or ESP). In the evaluated configuration only ESP will be configured for use. A crypto map (the Security Policy Definition (SPD)) set can contain multiple entries, each with a different access list.. The access list entries are searched in a sequence - the router attempts to match the packet to the access list (acl) specified in that entry. Separate access lists define blocking and permitting at the interface). For example: Router# access-list extended TEST permit ip 192.168.3.0 0.0.0.255 10.3.2.0 0.0.0.255 When a packet matches a permit entry in a particular access list, the method of security in the corresponding crypto map is applied. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. For example: Router# Tunnel protection ipsec policy ipv4 TEST The 'tunnel protection ipsec policy ipv4 TEST' command means to use extended access list named TEST in order to determine which traffic is relevant. The traffic matching the permit acls would then flow through the IPSec tunnel and be classified as "PROTECTED". Traffic that does not match a permit acl and is also blocked by other non-crypto acls on the interface would be DISCARDED. Traffic that does not match a permit acl in the crypto map, but that is not disallowed by other acls on the interface is allowed to BYPASS the tunnel. For example, a non-crypto permit acl for icmp would allow ping traffic to flow unencrypted if a permit access list entry was not configured that matches the ping traffic. 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 access list entry as well as the data flow information from the specific access list entry. The command "fqdn name" can be configured within a crypto identity and applied to a access list in order to perform validation of the peer device during authentication. 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. 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.
FCS_SSH_EXT.1 FCS_SSHS_EXT.1	The TOE implementation of SSHv2 complies with RFCs 4251, 4252, 4253, 4254, 5647, 5656, 8308 section 3.1, 8332 and supports the following: • Public key algorithms for authentication: RSA Signature Verification. • The TOE's implementation of SSH public-key based authentication supports rsa-sha2-256, rsa-sha2-512, and ecdsa-sha2-nistp384. • When an SSH client presents a public key, the TOE establishes a user identity by verifying that the SSH client's presented public key matches one that is stored within an authorized keys file. • Local password-based authentication for administrative users accessing the TOE through SSHv2 and optionally supports deferring authentication to a remote AAA server. • Encryption algorithms, AES-CBC-128, AES-CBC-256 and aes256-gcm@openssh.com to ensure confidentiality of the session.

TOE SFRs	How the SFR is Met
	• The TOE's implementation of SSHv2 supports hashing algorithms hmac-sha2-256, hmac-sha2-384 and implicit to ensure the integrity of the session. • The TOE's implementation of SSHv2 can be configured to allow Diffie-Hellman Group 14 (2048-bit keys) and ecdh-sha2-nistp384 Key Establishment. • The TOE supports Key Derivation Functions (KDFs) as specified in RFC 4253, which includes the use of KDFs derived from the specified RFCs to ensure secure key establishment. • Packets greater than 65,806 bytes in an SSH transport connection are dropped. Large packets are detected by the SSH implementation and dropped internal to the SSH process. • The TOE can also be configured to ensure that SSH re-key of no longer than one hour and no more than one gigabyte of transmitted data for the session key. Rekeying is performed upon reaching the threshold that is hit first. Please refer to Table 5 for all the CAVP references.
FIA_AFL.1	The TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentication attempts before privileged administrator or non-privileged administrator is locked out through the administrative CLI using a privileged CLI command. While the TOE supports a range from 1-25, in the evaluated configuration, the maximum number of failed attempts is recommended to be set to 3. All successive unsuccessful authentication attempts are logged on the router. When a privileged administrator or non-privileged administrator attempting to log into the administrative CLI reaches the administratively set maximum number of failed authentication attempts, the user will not be granted access to the administrative functionality of the TOE until a privileged administrator resets the user's number of failed login attempts through the administrative CLI. Administrator lockouts are not applicable to the local console.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")", and other special characters listed in the SFR. Minimum password length is settable by the Authorized Administrator and supports passwords of 1 to 127 characters. A minimum password length of 15 is recommended.
FIA_PSK_EXT.1 (1) FIA_PSK_EXT.1 (2) FIA_PSK_EXT.2	Through the implementation of the CLI, the TOE supports use of IKEv1 (ISAKMP) and IKEv2 pre-shared keys for authentication of IPsec tunnels. Preshared keys can be entered as ASCII character strings, or HEX values. The TOE supports keys that are from 22 characters in length up to 127 bytes in length and composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")",and other special characters listed in the SFR. The data that is input is conditioned by the cryptographic module prior to use via SHA-1.
FIA_UIA_EXT.1 FIA_UAU_EXT.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login warning banner that is displayed prior to user authentication. Administrative access to the TOE is facilitated through the TOE's CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 secured connection, the TOE prompts the user for a username and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE provides a local password based authentication mechanism as well as RADIUS AAA server for remote authentication. The administrator authentication policies include authentication to the local user database or redirection to a remote authentication server. Interfaces can be configured to try one or more remote

TOE SFRs	How the SFR is Met
	authentication servers and then fail back to the local user database if the remote authentication servers are inaccessible. The TOE can invoke an external authentication server to provide a remote authentication mechanism by forwarding the authentication requests to the external authentication server (when configured by the TOE to provide single-use authentication). The process for authentication is the same for administrative access whether administration is occurring via a directly connected console or remotely via SSHv2 secured connection. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE displays only '*' characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3	The TOE uses X.509v3 certificates as defined by RFC 5280 (and RFC 8603 for CSfC purposes) to support authentication for IPsec connections. The TOE supports the following methods to obtain a certificate from a CA: • Simple Certificate Enrollment Protocol (SCEP)—A Cisco-developed enrollment protocol that uses HTTP to communicate with the CA or registration authority (RA). • Imports certificates in PKCS12 format from an external server • IOS-XE File System (IFS)—The router uses any file system that is supported by Cisco IOS-XE software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. • Manual cut-and-paste—The router displays the certificate request on the console terminal, allowing the administrator to enter the issued certificate on the console terminal; manually cut-and-paste certificate requests and certificates when there is no network connection between the router and CA • Enrollment profiles—The router sends HTTP-based enrollment requests directly to the CA server instead of to the RA-mode certificate server (CS). • Self-signed certificate enrollment for a trust point Regardless off the method used to obtain a certificate, the TOE validates the certificate the same, verifying that the certificate chains to a trusted root CA certificate or subordinate CA. All the certificates include at least the following information: public key, Common Name, Organization, Organizational Unit and Country. Public key infrastructure (PKI) credentials, such as Rivest, Shamir, and Adelman (RSA) and Elliptical Curve Digital Signature Algorithm (ECDSA) keys and certificates can be stored in a specific location on the TOE. Certificates are stored to NVRAM by default. The certificates themselves provide protection in that they are digitally signed. If a certificate were modified in any way, it would be invalidated. The digital signature verifications process would show that the certificate has been tampered with, and the hash value would then be invalid. The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. The administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates. To verify, the authorized administrator could 'show' the pki certificates and the pki trust points.

TOE SFRs	How the SFR is Met
	The authorized administrator can also configure one or more certificate fields together with their matching criteria to match. Such as: • alt-subject-name • expires-on • issuer-name • name • serial-number • subject-name • unstructured-subject-name • valid-start This allows for installing more than one certificate from one or more CAs on the TOE. For example, one certificate from one CA could be used for one IPsec connection, while another certificate from another CA could be used for a different IPsec connection. However, the default configuration is a single certificate from one CA that is used for all authenticated connections. The physical security of the TOE (A.PHYSICAL_PROTECTION) protects the router and the certificates from being tampered with or deleted. Only authorized administrators with the necessary privilege level can access the certificate storage and add/delete them. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE. CRL is configurable and may be used for certificate revocation. The authorized administrator could use 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. Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted. The certificate chain path validation is configured on the TOE by first setting crypto pki trustpoint name and then configuring the level to which a certificate chain is processed on all certificates including subordinate CA certificates using the chain-validation command. If the connection to determine the certificate validity cannot be established, the certificate is not accepted, and the connection will not be established.
FMT_MOF.1/ManualUpdate FMT_MOF.1/Services	The TOE provides the ability for Security Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds, to securely manage certificates in the TOE's trust store, and to perform manual updates to the TOE. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS-XE privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable.

TOE SFRs	How the SFR is Met
FMT_MOF.1/Functions FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys	See FMT_SMF.1 for services the Security Administrator is able to start and stop. Management functionality of the TOE is provided through the TOE CLI. The TOE contains a trust store of X.509v3 certificates. The trust store contains certificates for the local TOE and certificates for the remote syslog server. Access to trust store data on each component is restricted to authorized administrators only. The term "Security Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges can also modify TOE data based on if granted the privilege. No administrative functionality is available prior to administrative login. The TOE provides the ability for Security Administrators to generate, import, modify or delete cryptographic keys and certificates used for VPN operation through the TOE CLI as described in Section 7 Key Zeroization and in the CC Configuration Guide.
FMT_SMF.1 FMT_SMF.1/VPN	The TOE provides all the capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE include - • Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above; • The ability to manage the warning banner message and content – allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users • The ability to manage the time limits of session inactivity which allows the Authorized Administrator the ability to set and modify the inactivity time threshold. • The ability to update the IOS-XE software. The validity of the image is provided using SHA-512 and digital signature prior to installing the update • The ability to manage audit behavior and the audit logs which allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs • The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2 • The ability to manage cryptographic keys • The ability to configure the authentication failure parameters for FIA_AFL.1. • The ability to import the X.509v3 certificates to the TOE's trusted store. • The ability to configure the reference identifier for the peer. • The ability to manually unlock a locked administrator account. • The ability to start and stop services. • The ability to modify the behaviour of the transmission of audit data to an external IT entity. • The ability to configure NTP. • The ability to configure thresholds for SSH rekeying. • The ability to configure the lifetime for IPsec SAs. • The ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors. • The ability to manage the trusted public keys database. • The ability to define packet filtering rules; • The ability to associate packet filtering rules to network interfaces; • The ability to order packet filtering rules by priority. Information about TSF-initiated Termination is covered in the TSS under FTA_SSL_EXT.1 or FTA_SSL.3.
FMT_SMR.2	The TOE platform maintains privileged and semi-privileged administrator roles. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS-XE privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level

TOE SFRs	How the SFR is Met
	15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and are also customizable. Note: the levels are not hierarchical. The term "Security Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. The privilege level determines the functions the user can perform, hence the Security Administrator with the appropriate privileges. Refer to the Guidance documentation and IOS-XE Command Reference Guide for available commands and associated roles and privilege levels. The TOE can and shall be configured to authenticate all access to the command line interface using a username and password. The TOE supports both local administration via a directly connected console cable and remote administration via SSH or IPSec over SSH.
FPF_RUL_EXT.1	An authorized administrator can define the traffic that needs to be protected by configuring access lists (permit, deny, log) and applying these access lists to interfaces using the 'ip access-group' command. 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 can be applied to all the network interfaces. The TOE enforces information flow policies on network packets that are received 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. By implementing rules that defines the permitted flow of traffic between interfaces of the TOE for unauthenticated traffic. These rules control whether a packet is transferred from one interface to another based on: 1. presumed address of source 2. presumed address of destination 3. transport layer protocol (or next header in IPv6) 4. Service used (UDP or TCP ports, both source and destination) 5. Network interface on which the connection request occurs These rules are supported for the following protocols: RFC 791(IPv4); RFC 8200 (IPv6); RFC 793 (TCP); RFC 768 (UDP). TOE compliance with these protocols is verified via regular quality assurance, regression, and interoperability testing. 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) The TOE is capable of inspecting network packet header fields to determine if a packet is part of an established session or not. ACL rules still apply to packets that are part of an ongoing session. Packets will be dropped unless a specific rule has been set up to allow the packet to pass (where the attributes of the packet match the attributes in the rule and the action associated with the rule is to pass traffic). This is the default action that occurs on an interface if no ACL rule is found. If a packet arrives that does not meet any rule, it is expected to be dropped. Rules are enforced on a first match basis from the top down. As soon as a match is found the action associated with the rule is applied. These rules are entered in the form of access lists at the CLI (via 'access list' and 'access group' commands). These interfaces reject traffic when the traffic arrives on an external TOE interface, and the source address is an external IT entity on an internal network;

TOE SFRs	How the SFR is Met
	These interfaces reject traffic when the traffic arrives on an internal TOE interface, and the source address is an external IT entity on the external network; These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on a broadcast network; These interfaces reject traffic when the traffic arrives on either an internal or external TOE interface, and the source address is an external IT entity on the loopback network; These interfaces reject requests in which the subject specifies the route for information to flow when it is in route to its destination. Otherwise, these interfaces pass traffic only when its source address matches the network interface originating the traffic through another network interface corresponding to the traffic's destination address. These rules are operational as soon as interfaces are operational following startup of the TOE. There is no state during initialization/startup that the access lists are not enforced on an interface. The initialization process first initializes the operating system, and then the networking daemons including the access list enforcement, prior to any daemons or user applications that potentially send network traffic. No incoming network traffic can be received before the access list functionality is operational. During initialization/startup (while the TOE is booting) the configuration has yet to be loaded, and no traffic can flow through any of its interfaces. No traffic can flow through the TOE interfaces until the POST has completed, and the configuration has been loaded. If any aspect of the POST fails during boot, the TOE will reload without forwarding traffic. If a critical component of the TOE, such as the clock or cryptographic modules, fails while the TOE is in an operational state, the TOE will reload, which stops the flow of traffic. Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE.
FPT_FLS.1	Whenever a failure occurs within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE. The TOE shuts down by reloading and will continue to reload as long as the failures persist. This functionally prevents any failure of power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests from causing an unauthorized information flow. There are no failures that circumvent this protection.
FPT_SKP_EXT.1 FPT_APW_EXT.1	The TOE stores all private keys in a secure directory protected from access as there is no interface in which the keys can be accessed. The TOE includes CLI command features that can be used to configure the TOE to encrypt all locally defined user passwords. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. The password is encrypted by using the command "password encryption aes" used in global configuration mode. The "password encryption aes" command enables the functionality and the "key config-key password-encrypt" command is used to set the master password to be used to encrypt the preshared keys. The command *service password-encryption* applies encryption to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords. Additionally, enabling the 'hidekeys' command in the logging configuration ensures that and passwords are not displayed in plaintext. The TOE includes a Master Passphrase feature that can be used to configure the TOE to encrypt all locally defined user passwords using AES. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. Password encryption is configured using the 'service password-encryption' command. There are no administrative interfaces available that allow passwords to be viewed as they are encrypted via the password-encryption service.

TOE SFRs	How the SFR is Met
FPT_STM_EXT.1 FCS_NTP_EXT.1	The TOE provides a source of date and time information used in audit event timestamps, and for certificate validity checking. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time information is also used in various routing protocols such as, OSPF and BGP; Calculate IKE stats (including limiting SAs based on times); determining AAA timeout, administrative session timeout, and SSH rekey. The TOE synchronizes with an NTP server for its reliable and accurate timestamp. The TOE can be configured to support at least three (3) NTP servers. The TOE supports NTPv4 and validates the integrity of the time-source using IPsec to provide trusted communication between itself and an NTP time source. In addition, the TOE does not allow the timestamp to be updated from broadcast addresses. NTP use UTC to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.
FPT_TUD_EXT.1	An Authorized Administrator can query the software version running on the TOE and can initiate updates to software images. The current active version can be verified by executing the “show version” command from the TOE’s CLI. When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from the software.cisco.com. Digital signatures are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to actually update the applicable TOE components. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded. 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. If the output from the “show software authenticity file” command does not provide the expected output, contact Cisco Technical Assistance Center (TAC) https://tools.cisco.com/ServiceRequestTool/create/launch.do. Further instructions for how to do this verification are provided in the administrator guidance for this evaluation. Software images are available from Cisco.com at the following: http://www.cisco.com/cisco/software/navigator.html
FPT_TST_EXT.1 FPT_TST_EXT.3	The TOE runs a suite of self-tests during initial start-up to verify its correct operation. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. For testing of the TSF, the TOE automatically runs checks and tests at startup and during resets and periodically during normal operation to ensure the TOE is operating correctly, including checks of image integrity and all cryptographic functionality. During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include: • Noise Source Health Tests – The Noise Source Health Tests check the functioning of the Noise Source that supplies randomness to the Entropy Source. The tests are designed to detect failure of the Noise Source. These tests are run at startup and continuously during normal operation. • 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) –

TOE SFRs	How the SFR is Met
	This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly. • RNG/DRBG Known Answer Test – For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly. • HMAC Known Answer Test – For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly. • SHA-1/256/384/512 Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match, and the hash operations are operating correctly. • ECDSA self-test (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. • Software Integrity Test – The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity. The integrity of stored TSF executable code when it is loaded for execution can be verified through the use of RSA and Elliptic Curve Digital Signature algorithms. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen and saved in the crashinfo file. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated. Example Error: *Nov 26 2022 16:28:23.629: %CRYPTO-0-SELF_TEST_FAILURE: Encryption self-test failed These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behavior will be identified by the failure of a self-test. The integrity of stored TSF executable code when it is loaded for execution can be verified through the use of RSA Digital Signature algorithms.
FTA_SSL_EXT.1	

TOE SFRs	How the SFR is Met
FTA_SSL.3	An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the "session-timeout" setting applied to the console. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session. The allowable inactivity timeout range is from 1 to 65535 seconds. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the "exec-timeout" setting.
FTA_SSL.4	An administrator can exit out of both local and remote administrative sessions. Each administrator logged onto the TOE can manually terminate their session using the "exit" or "logout" command.
FTA_TAB.1	The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. This interface is applicable for both local (via console) and remote (via SSH) TOE administration.
FTP_ITC.1 FTP_ITC.1/VPN	The TOE protects communications with peer or neighbor routers using keyed hash as defined in FCS_COP.1/KeyedHash and cryptographic hashing functions FCS_COP.1/Hash. This protects the data from modification of data by hashing that verify that data has not been modified in transit. In addition, encryption of the data as defined in FCS_COP.1/DataEncryption is provided to ensure the data is not disclosed in transit. The TSF allows the TSF, or the authorized IT entities to initiate communication via the trusted channel. The TOE requires that peers and other TOE instances establish an IKE/IPSec connection in order to forward routing tables used by the TOE. The TOE protects communications between the TOE and the remote audit server using IPsec. This provides a secure channel to transmit the log events. Likewise, communications between the TOE and AAA servers are secured using IPsec. The TOE protects communications between itself and the NTP server using NTPv4, IPsec. The distinction between "remote VPN gateway" and "another instance of the TOE" is that "another instance of the TOE" would be installed in the evaluated configuration, and likely administered by the same personnel, whereas a "remote VPN gateway/peer" could be any interoperable IPsec gateway/peer that is expected to be administered by personnel who are not administrators of the TOE, and who share necessary IPsec tunnel configuration and authentication credentials with the TOE administrators. For example, the exchange of X.509 certificates for certificate based authentication.
FTP_TRP.1/Admin	All remote administrative communications take place over a secure encrypted SSHv2 session which has the ability to be encrypted further using IPsec. The SSHv2 session is encrypted using AES encryption. The remote users can initiate SSHv2 communications with the TOE.

7 Annex A: Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM.4 provided by the TOE.

Table 19 TOE Key Zeroization

Name	Description of Key	Zeroization
Diffie-Hellman Shared Secret	This is the shared secret used as part of the Diffie-Hellman key exchange. This key is stored in SDRAM.	Automatically after completion of DH exchange. Overwritten with: 0x00
Diffie Hellman private exponent	This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in SDRAM.	Zeroized upon completion of DH exchange. Overwritten with: 0x00
Skeyid	This is the IKE intermittent value used to create skeyid_d. This key is stored in SDRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
skeyid_d	This is the IKE intermittent value used to derive keying data for IPsec. This key is stored in SDRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session encrypt key	This is the IPsec key used for encrypting the traffic in an IPsec connection. This key is stored in SDRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session authentication key	This is the IPsec key used for authenticating the traffic in an IPsec connection. This key is stored in SDRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
ISAKMP preshared key	This is the configured preshared key for ISAKMP negotiation. This key is stored in NVRAM.	Zeroized using the following command: **# no crypto isakmp key** Overwritten with: 0x0d
IKE ECDSA Private Key	The ECDSA private-public key pair is created by the device itself using the key generation CLI command. Afterwards, the device's public key must be put into the device certificate. The device's certificate is created by creating a trustpoint on the device. This trustpoint authenticates with the CA server to get the CA certificate and also enrolls with the CA server to generate the device certificate. In the IKE authentication step, the device's certificate is firstly sent to another device to be authenticated. The other device verifies that the certificate is signed by CA's signing key, then sends back a random secret encrypted by the device's public key in the valid device certificate. Only the device with the matching device private key can decrypt the message and obtain the random secret. This key is stored in NVRAM.	Zeroized using the following command: **# crypto key zeroize ecdsa**[1] Overwritten with: 0x0d
IKE RSA Private Key	The RSA private-public key pair is created by the device itself using the key generation CLI described below.	Zeroized using the following command:

[1] Issuing this command will zeroize/delete all ECDSA keys on the TOE.

Name	Description of Key	Zeroization
	Afterwards, the device's public key must be put into the device certificate. The device's certificate is created by creating a trustpoint on the device. This trustpoint authenticates with the CA server to get the CA certificate and also enrolls with the CA server to generate the device certificate. In the IKE authentication step, the device's certificate is firstly sent to another device to be authenticated. The other device verifies that the certificate is signed by CA's signing key, then sends back a random secret encrypted by the device's public key in the valid device certificate. . Only the device with the matching device private key can decrypt the message and obtain the random secret. This key is stored in NVRAM.	**# crypto key zeroize rsa** Overwritten with: 0x0d
IPSec encryption key	This is the key used to encrypt IPsec sessions. This key is stored in SDRAM.	Automatically when IPSec session terminated. Overwritten with: 0x00
IPSec authentication key	This is the key used to authenticate IPsec sessions. This key is stored in SDRAM.	Automatically when IPSec session terminated. Overwritten with: 0x00
RADIUS secret	Shared secret used as part of the Radius authentication method. This key is stored in NVRAM.	Zeroized using the following command: **# no radius-server key** Overwritten with: 0x0d
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents) using memset. This overwrites the key with all 0's. This key is stored in NVRAM.	Zeroized using the following command: **# crypto key zeroize rsa** Overwritten with: 0x00
SSH Session Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents). This is called by the ssh_close function when a session is ended. This key is stored in SDRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00
NTP Keys	This is the key that is used for encryption and decryption of authentication of NTP packets. This key is stored in NVRAM.	Zeroized by overwriting with new key

8 Annex B: References

The following documentation was used to prepare this ST:

Table 20 References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, April 2017, version 3.1, Revision 5
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, April 2017, version 3.1, Revision 5
[NDcPP]	collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023
[MOD_VPNGW]	PP-Module for Virtual Private Network (VPN) Gateways (MOD_VPNGW), Version 1.3, August 16, 2023
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009 Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 186-4]	FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS) July 2013
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[NIST SP 800-90A Rev 1]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2015
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008

9 Annex C: 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 the following sites:

http://www.cisco.com

10.1 Document 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.

10.2 Obtaining Technical Assistance

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

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

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

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

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

http://www.cisco.com