Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3

Common Criteria Security Target

Version 1.0
3 August 2021

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

Table of Contents

List of Tables

List of Figures

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
BRI	Basic Rate Interface
CAK	Secure Connectivity Association Key
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CKN	Secure Connectivity Association Key Name
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAP-TLS	EAP Transport Layer Security
EAPOL	EAP over LANs
EHWIC	Ethernet High-Speed WIC
ESP	Encapsulating Security Payload
GCM	Galois Counter Mode
GE	Gigabit Ethernet port
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IOS-XE	The proprietary operating system developed by Cisco Systems
IP	Internet Protocol
IPsec	IP Security
ISDN	Integrated Services Digital Network
IT	Information Technology
MAC	Media Access Control
MSK	Master Session Key
NDcPP	collaborative Network Device Protection Profile
NVRAM	Non-volatile random access memory, specifically the memory in the switch where the configuration parameters are stored
OS	Operating System

Acronyms / Abbreviations	Definition
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message
PBKDF2	Password-Based Key Derivation Function version 2
PoE	Power over Ethernet
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SA	Security Association
SAK	Secure Association Key
SC	Secure Channel
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SCI	Secure Channel Identifier
SecTAG	MAC Security TAG
SecY	MAC Security Entity
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SM	Service Module
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
WAN	Wide Area Network
WIC	WAN Interface Card

Terminology

The following terms are common and may be used in this Security Target.

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user that has been assigned to a privilege level that is permitted to perform all TSF-related functions.
Peer	Another switch on the network that the TOE interfaces.
Remote VPN Gateway/Peer	A remote VPN Gateway/Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another switch.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
vty	vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term).
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

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), Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3 . 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.

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]
- Key Zeroization [Annex A]
- NIAP Technical Decisions [Annex B]
- References [Annex C]

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 3 ST and TOE Identification

Name	Description
ST Title	Cisco Catalyst Industrial Ethernet 3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running IOS-XE 17.3 Common Criteria Security Target
ST Version	1.0
Publication Date	3 August 2021
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches
TOE Hardware Models	IE3200, IE3300, IE3400 and IE3400H Rugged Series
TOE Software Version	IOS-XE 17.3
Keywords	Audit, Authentication, Encryption, Network Device, Secure Administration

1.2 TOE Overview

The Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches (here after referred to as Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches), all running IOS-XE 17.3. The TOE is a purpose-built, switching and routing platform with OSI Layer2 and Layer3 traffic filtering capabilities. The TOE includes the hardware models as defined in Table 3 in Section 1.1.

1.2.1 TOE Product Type

The Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches are switching and routing platforms that provide connectivity and security services. These switches offer broadband speeds and simplified management to small businesses, and enterprise small branch and teleworkers.

The Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches is a single-device security and switching solutions for protecting the network.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this Security Target. All the following environment components are supported by all TOE evaluated configurations.

Table 4 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE transmits syslog messages over a secure IPsec trusted channel either directly or connected to a TOE Peer that also supports a secure IPsec trusted channel.
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Management Workstation with SSHv2 client	Yes	This includes any IT Environment Management workstation that is used by the TOE administrator to support TOE administration using SSHv2 protected channels. Any SSH client that supports SSHv2 may be used.
Certification Authority (CA)	Yes	This includes any IT Environment Certification Authority (CA) on the TOE network. The CA can be used to provide the TOE with a valid certificate during certificate enrollment as well as validating a certificate.
TOE Peer	Conditional	The TOE Peer is required if the remote syslog server is attached for the TOE’s use. If the remote syslog server is directly connected to the TOE for the TOE’s use, then the TOE Peer is not required.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following hardware models as described in 1.5 Physical Scope of the TOE. The software is comprised of the Universal Cisco Internet Operating System (IOS) XE software image Release IOS-XE 17.3 .

The Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches that comprises the TOE has common hardware characteristics as described in Table 5 Hardware Models and Specifications. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware.

The Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches primary features include the following:

- Central processor that supports all system operations;
- Dynamic memory, used by the central processor for all system operation;
- x86 CPU complex with minimum, based on model of 2 GB memory, 1.5 GB of flash and external USB 4GB SD pluggable storage slot (optional);
- Flash memory (EEPROM), used to store the Cisco IOS-XE image (binary program);
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs and
- Non-volatile random-access memory (NVRAM) is used to store switch configuration parameters that are used to initialize the system at start-up.
- Physical network interfaces (minimally two) (e.g. RJ45 serial and standard 10/100/1000 Ethernet ports). Some models have a fixed number and/or type of interfaces; some models have slots that accept additional network interfaces;
- Dedicated management port on the switch, RJ-45 console port and a USB mini-Type B console connection and
- Built for harsh environments and temperature ranges, fanless, convection-cooled with no moving parts for extended durability and hardened for vibration, shock and surge, and electrical noise immunity.

Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.6 Logical Scope of the TOE below.

The following figure provides a visual depiction of an example TOE deployment.

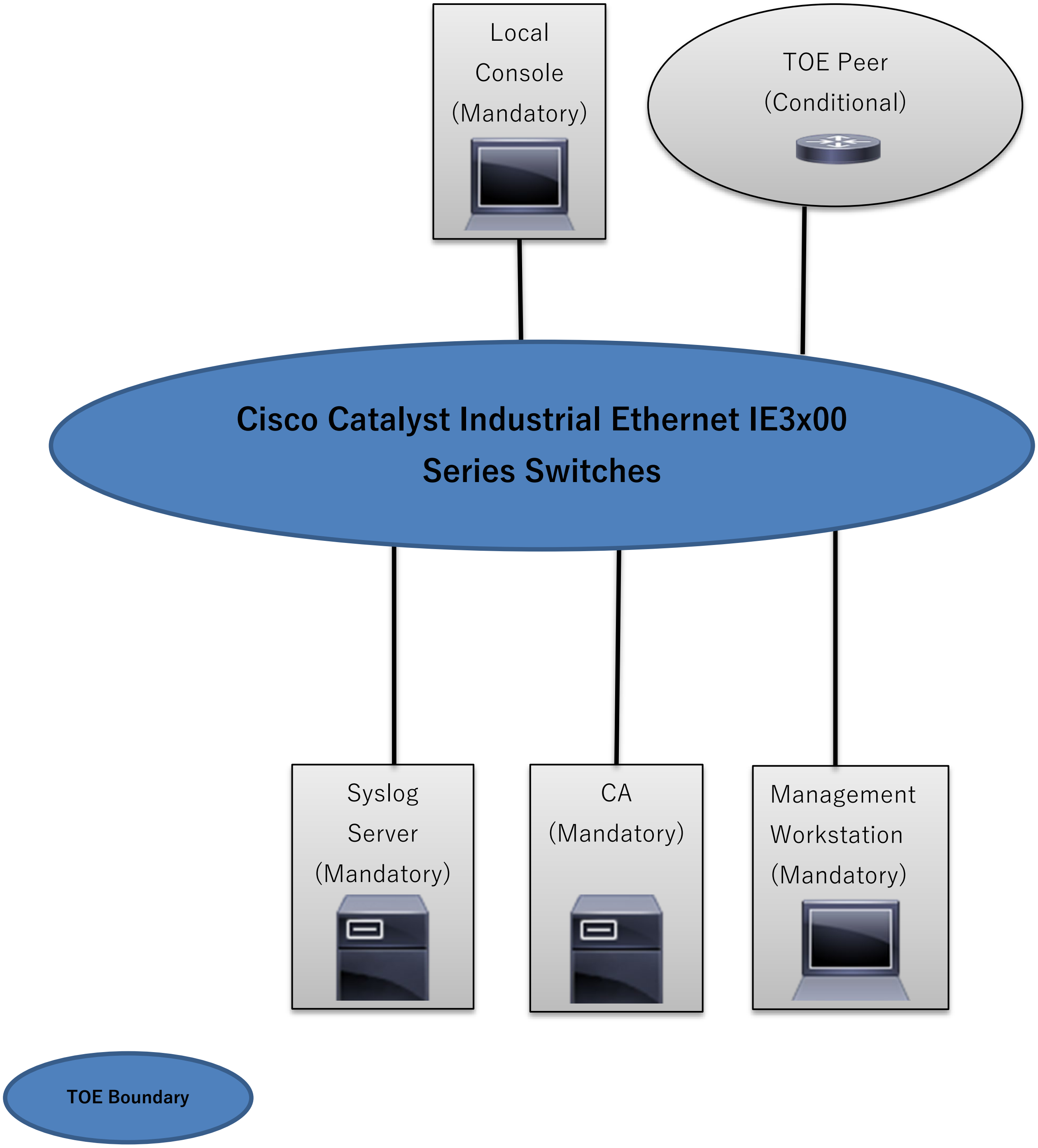

Figure 1 TOE Example Deployment

The previous figure includes the following devices, noting the TOE is only the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches and only one TOE device is required for the deployment of the TOE in the evaluated configuration.

- Identifies the TOE Models
  - Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series (IE3200, IE3300, IE3400, IE3400H) Switches running Cisco IOS-XE 17.3
- Identifies the following IT entities that are considered to be in the IT Environment:
  - Syslog (audit) Server with a secure connection using IPsec
  - Local Console to support local Administration (direct connection)
  - Management Workstation to support remote Administration with a secure connection using SSHv2 Client
  - Certificate Authority (CA) for X509 certificate validation with a secure connection using IPsec
  - TOE Peer (Conditional) with a secure connection using IPsec

1.4 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.5 below and includes the Cisco IOS-XE 17.3 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 switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internet working device and forwarded to their configured destination.

In addition, if the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches are to be remotely administered, then the management workstation must be connected to an internal network. SSHv2 is used to securely connect to the switch. An external syslog server is used to store audit records, where IPsec is used to secure the transmission of the records. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic, one that is in a controlled environment where implementation of security policies can be enforced.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switch models as follows: IE3200, IE3300, IE3400 and IE3400H running Cisco IOS-XE 17.3 . The network, on which they reside is considered part of the operational environment. The TOE deployment and operational guidance documentation that is considered to be part of the TOE can be found in the Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches Common Criteria Operational User Guidance and Preparative Procedures document and is downloadable from the http://cisco.com web site. The TOE is comprised of the following physical specifications as described in Table 5 below. The hardware, size and the interfaces are based on the number of ports.

Table 5 Hardware Models and Specifications

Hardware	Processor	Software	Picture	Size	Power	Interfaces
Cisco Catalyst Industrial Ethernet Series IE3200 Switch	Xilinx ZU3EG (ARM Cortex-A53)	Cisco IOS-XE 17.3		6 in. X 3.6 in. X 5.3 in. 3.8lbs	Supports up to 8 PoE/PoE+ ports [Power budget - 240W]	8 -10/100/1000 RJ45 Copper ports, 2 - 100/1000 SFP Ports, 1 RS-232 (via RJ-45), 1 USB Mini Type B
Cisco Catalyst Industrial Ethernet Series IE3300 Switch	Xilinx ZU3EG (ARM Cortex-A53)	Cisco IOS-XE 17.3		6 in. X 3.6 in. X 5.3 in. 3.8 lbs	up to 24x PoE/PoE+ ports or 4x 802.3bt type 4 ports (with 2.5G expansion module) with the all GE PoE enabled base [Power budget - 360W] OR up to 24x PoE/PoE+ ports or 4x 802.3bt type 3 ports (on PoE base system) or 4x 802.3bt type 4 ports (with 2.5G expansion module) with the 10G PoE enabled base	8 -10/100/1000 RJ45 Copper ports, 2 - 100/1000 SFP Ports, 4 1GE/2.5G RJ45 Copper ports 2 1GE/10G SFP+ ports 1 RS-232 (via RJ-45), 1 USB Mini Type B
Cisco Catalyst Industrial Ethernet IE3400 Series Switch	Xilinx ZU3EG (ARM Cortex-A53)	Cisco IOS-XE 17.3		6 in. X 3.6 in. X 5.3 in. 3.8 lbs to 6 in. X 4.4 in. X 5.3 in. 5.0 lbs	Supports up to 24 PoE/PoE+ ports or up to 8 PoE/PoE+ Ports and 4 “802.3bt type 4” Ports with the 2.5G expansion module 2 [System Power budget - 480W]	8 up to 1610/100/1000 RJ45 Copper ports, 2 up t0 8 100/1000 SFP Ports, 4 1GE/2.5G RJ45 Copper Ports

Hardware	Processor	Software	Picture	Size	Power	Interfaces
Cisco Catalyst Industrial Ethernet IE3400H Series Switch	Xilinx ZU3EG (ARM Cortex-A53)	Cisco IOS-XE 17.3		9.58 x 7.90 x 3.15 in. 8.45 lbs to 9.58 x 10.90 x 3.15 in.	IP67-rated PoE DC-DC power supply, Input:18V-60V Output: 54V, 3.1A max 160W OR IP67-rated PoE AC-DC power supply, input 85-264VAC/88-300VDC, Output 54V, 3.1A max, 180Watts	8 up to 24 - 10/100 Fast Ethernet ports, 8 up to 24 - 10/100/1000 Gigabit Ethernet ports

1.6 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
- 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 v2.2e as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco Catalyst Industrial Ethernet IE3x00 Rugged Series Switches provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event.

Auditable events include:

- failure on invoking cryptographic functionality such as establishment, termination and failure of cryptographic session establishments and connections;
- creation and update of Secure Association Key
- modifications to the group of users that are part of the Authorized Administrator roles;
- all use of the user identification mechanism;
- any use of the authentication mechanism;
- Administrator lockout due to excessive authentication failures;
- any change in the configuration of the TOE;
- changes to time;
- initiation of TOE update;
- indication of completion of TSF self-test;
- maximum sessions being exceeded;
- termination of a remote session;
- attempts to unlock a termination session and
- initiation and termination of a trusted channel

The TOE is configured to transmit its audit messages to an external syslog server. Communication with the syslog server is protected using IPsec and the TOE can determine when communication with the syslog server fails. If that should occur, the TOE will store all audit records locally and when the connection to the remote syslog server is restored, all stored audit records will be transmitted to the remote syslog server.

The audit logs can be viewed on the TOE using the appropriate IOS-XE commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the Authorized Administrator to clear audit data stored locally on the TOE.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operation Environment – Xilinx ZU3EG processors).

The TOE leverages the IOS Common Cryptographic Module (IC2M) Rel5 as identified in the table below. The IOS software calls the IOS Common Cryptographic Module (IC2M) Rel5 (Firmware Version: Rel 5) that has been validated for conformance to the requirements of FIPS 140-2 Level 1.

Refer to Table 6 for algorithm certificate references.

Table 6 CAVP References

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
AES	Used for symmetric encryption/decryption, keyed hashing	CBC and GCM (128 and 256 bits)	A1462	IC2M	FCS_COP.1/ DataEncryption
SHS (SHA-1, SHA-256)	Cryptographic hashing services	Byte Oriented	A1462	IC2M	FCS_COP.1/Hash
HMAC (HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	A1462	IC2M	FCS_COP.1/KeydHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	A1462	IC2M	FCS_RBG_EXT.1
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation PKCS #1 v2.1 2048 bit key	C1411	IC2M	FCS_CKM.1 FCS_COP.1/SigGen
CVL-KAS-ECC	Key Agreement	NIST Special Publication 800-56A	A1462	IC2M	FCS_CKM.2
ECDSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	A1462	IC2M	FCS_CKM.1

The TOE provides cryptography in support of secure connections that includes 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.

The cryptographic services provided by the TOE are described in Table 7 below.

Table 7 TOE Provided Cryptography

Cryptographic Method	Use within the TOE
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
FFC DH	Used as the Key exchange method for IPsec and SSH
Internet Key Exchange	Used to establish initial IPsec session
RSA Signature Services	Used in IPsec session establishment Used in SSH session establishment X.509 certificate signing.
RSA	Used in IKE protocols peer authentication Used to provide cryptographic signature services Used in Cryptographic Key Generation and Key Establishment
Secure Shell Establishment	Used to establish initial SSH session.
SHS	Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
SP 800-90 RBG	Used for random number generation, key generation and seeds to asymmetric key generation Used in IPsec session establishment Used in SSH session establishment
ECDSA	Used to provide cryptographic signature services
ECC DH	Used as the Key exchange method for IPsec

The IE 3000 Series Switches platforms contain the following processors as listed in Table 5 Hardware Models and Specifications.

1.6.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (TOE 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 IKE phase authentication for the IPsec communication channel 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 as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the local serial console or SSHv2 interfaces. The SSHv2 interface also supports authentication using SSH keys.

The TOE also provides an automatic lockout when a user attempts to authenticate and enters invalid information. When the threshold for a defined number of failed authentication attempts has exceeded the configured allowable attempts, the user is locked out until an Authorized Administrator can reenable the user account.

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

1.6.4 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 serial console connection. The TOE provides the ability to securely manage:

- Administration of the TOE locally and remotely;
- Configuration of warning and consent access banners;
- Configuration of session inactivity thresholds;
- Updates of the TOE software;
- Configuration of authentication failures;
- Configuration of the audit functions of the TOE;
- Configuration of the TOE provided services;
- Configuration of the cryptographic functionality of the TOE.

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. The privileged administrator is the Authorized Administrator of the TOE and has the ability to enable, disable, determine and modify the behavior of all of the security functions of the TOE as described in this document.

1.6.5 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 is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

The TOE 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 provides the Authorized Administrators the capability to update the TOE’s clock manually to maintain a reliable timestamp.

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

1.6.6 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 Authorized Administrator 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 an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

1.6.7 Trusted path/Channels

The TOE allows trusted path to be established to itself from remote administrators over SSHv2 and initiates outbound IPsec trusted channels to transmit audit messages to remote syslog servers. In addition, IPsec is used as a trusted channel to protect the communications with the CA server.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 8 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
SNMP:The Simple Network Management Protocol is an application layer protocol, facilitates the exchange of management information among network devices	SNMP is not associated with Security Functional Requirements claimed in [NDcPP].
Telnet	Telnet sends authentication data in plain text. This feature must remain disabled in the evaluated configuration. SSHv2 must be used to secure the trusted path for remote administration for all SSHv2 sessions.
TLS Transport layer Security	TLS is not associated with Security Functional Requirements claimed in [NDcPP] IPsec is used instead.
SSL Secure Socket Layer	SSL is not associated with Security Functional Requirements claimed in [NDcPP] IPsec is used instead.
HTTP Hypertext Transfer Protocol	Hypertext Transfer Protocol is not associated with Security Functional Requirements claimed in [NDcPP] Use tunnelling through IPSEC.
HHTPS Hypertext Transfer Protocol Secure	Hypertext Transfer Protocol Secure is not associated with Security Functional Requirements claimed in [NDcPP] Use tunnelling through IPSEC.
AH Authentication Header (part of IPsec)	Encapsulating Security Payload (part of IPsec) must be used in all IPsec connections.

These services can be disabled by configuration settings as described in the Guidance documents (AGD). The (AGD) Table 14 provides a list of the services and protocols allowed in the evaluated configuration.

The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices Version 2.2e.

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. For a listing of Assurance Requirements claimed, see section 5.4.

The TOE and ST are CC Part 2 extended and CC Part 3 conformant.

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 9 Protection Profiles below. This ST applies the NIAP Technical Decisions as described in Table 20 in Annex B. Each posted TD was reviewed and considered based on the TOE product type, the PP claims and the security functional requirements claimed in this document.

Table 9 Protection Profiles

Protection Profile	Version	Date
collaborative Protection Profile for Network Devices (NDcPP)	2.2e	23 March 2020

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The TOE provides all the functionality at a level of security commensurate with that identified in the:

- collaborative Protection Profile for Network Devices, Version 2.2e

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the collaborative Protection Profile for Network Devices, Version 2.2e for which conformance is claimed verbatim. All concepts covered in the Protection Profile and Extended Package Security Problem Definition is 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 collaborative Protection Profile for Network Devices, Version 2.2e for which conformance is claimed verbatim. All concepts covered in the Protection Profile and Extended Package Statement of Security Objectives is 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 collaborative Protection Profile for Network Devices, Version 2.2e for which conformance is claimed verbatim. All concepts covered in the Protection Profile and Extended Package Statement of Security Requirements is 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 collaborative Protection Profile for Network Devices, Version 2.2e.

3 SECURITY PROBLEM DEFINITION

This section identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- 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. Note, the assumption, A.NO_THRU_TRAFFIC_PROTECTION is strike-through since the TOE does provide protection against the traffic that does traverse the TOE, which is countered by the TOE objectives defined in 4.1 Security Objectives for the TOE.

Table 10 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 and/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 will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will 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).

Assumption	Assumption Definition
	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 being 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).
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.

3.2 Threats

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 11 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 tunneling 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. An attacker may acquire sensitive TOE or user data that is transmitted to or from the TOE because an untrusted communication channel causes a disclosure of data in transit.

Threat	Threat Definition
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., 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. Non-validated 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 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.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
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.

3.3 Organizational Security Policies

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

Table 12 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 users 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.

4.1 Security Objectives for the TOE

The collaborative Protection Profile for Network Devices v2.2e does not define any security objectives for the TOE.

4.2 Security Objectives for the Environment

All 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. Note, the environment security objective, OE.NO_THRU_TRAFFIC_PROTECTION is strike-through since the TOE does provide protection against the traffic that does traverse the TOE, which is countered by the TOE objectives defined in 4.1 Security Objectives for the TOE.

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 the its own VM, and does not include other VMs or the VS
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality.

Environment Security Objective	IT Environment Security Objective Definition
	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.

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 and claimed PP/EP:

- Unaltered SFRs are stated in the form used in [CC2] or their extended component definition (ECD);
- Refinement made by PP author: Indicated with **bold text** and ~~strikethroughs~~;
- Selection wholly or partially completed in the PP: the selection values (i.e. the selection values adopted in the PP or the remaining selection values available for the ST) are indicated with underlined text
    - e.g. "[selection: *disclosure, modification, loss of use*]" in [CC2] or an ECD might become "disclosure" (completion) or "[selection: disclosure, modification]" (partial completion) in the PP;
- Assignment wholly or partially completed in the PP: indicated with *italicized text*
- Assignment completed within a selection in the PP: the completed assignment text is indicated with italicized and underlined text
    - e.g. "[selection: *change_default*, *query*, *modify*, *delete*, [*assignment: other operations*]]" in [CC2] or an ECD might become "change_default, select_tag" (completion of both selection and assignment) or "[selection: change_default, *select_tag*, *select_value*]" (partial completion of selection, and completion of assignment) in the PP;
- Iteration: indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").
- Extended SFRs are identified by having a label "EXT" at the end of the SFR name.

Formatting conventions outside of operations and iterations matches the formatting specified within the NDcPPv2.2e.

5.2 TOE 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.2	User Identity Association
	FAU_STG_EXT.1	Protected Audit Event Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/ Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_IPSEC_EXT.1	IPsec Protocol
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_RBG_EXT.1	Random Bit Generation
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Handling
	FIA_PMG_EXT.1	Password Management
	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
FMT: Security management	FMT_MOF.1/Services	Management of security functions behaviour
	FMT_MOF.1/ManualUpdate	Management of security functions behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	FPT_STM.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	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_ITC.1	Inter-TSF trusted channel

Class Name	Component Identification	Component Name
FTP: Trusted path/channels	FTP_TRP.1/Admin	Trusted Path

5.2.1 Security audit (FAU)

5.2.1.1 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:

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

d) *Specifically defined auditable events listed in Table 16*.

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, 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, *information specified in column three of Table 15*.

Table 15 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
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_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/Services	None	None.
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_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	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for

SFR	Auditable Event	Additional Audit Record Contents
	to be logged. See also application note on FPT_STM_EXT.1)	success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success and failure)	None.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None.

5.2.1.2 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.

5.2.1.3 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 [TOE shall consist of a single standalone component that stores audit data locally].

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [*when allotted space has reached its threshold*]] when the local storage space for audit data is full.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 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 or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;
- ECC schemes using "NIST curves" [P-256, P-384] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;
- 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]~~.

5.2.2.2 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: [

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1;
- Elliptic curve-based key establishment schemes that meets 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]~~.

5.2.2.3 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*.

5.2.2.4 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] *mode* and cryptographic key sizes [128 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3,* [CBC as specified in ISO 10116].

5.2.2.5 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 and cryptographic key sizes (*modulus*) [*2048 bits or greater*],

]

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,

].

5.2.2.6 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] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ and **message digest sizes** [160, 256] **bits** that meet the following: *ISO/IEC 10118-3:2004*.

5.2.2.7 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-1, HMAC-SHA-256, HMAC-SHA-512] and cryptographic key sizes [*160-bit, 256-bit, 512-bit used in HMAC*] **and message digest sizes** [160, 256, 512] **bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"*.

5.2.2.8 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 by RFC 3602)] together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-512].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- IKEv2 as defined in RFCs 5996 and [with no support for NAT traversal], and [RFC 4868 for hash functions]

].

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

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- IKEv2 SA lifetimes can be configured by a Security Administrator based on

[

  - length of time, where the time values can be configured within [*1-24*] hours;

]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- 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 within [*1-8*] 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 [*112 (for DH Group 14)*] bits.

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

- [according to the security strength associated with the negotiated Diffie-Hellman 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 Group(s) [14 (2048-bit MODP)].

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [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 [IKEv2 CHILD_SA] connection.

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

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: [SAN: Fully Qualified Domain Name (FQDN)] and *[no other reference identifier type]*].

5.2.2.9 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*] hardware based] 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.

5.2.2.10FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs [4251, 4252, 4253, 4254].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [password based].

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*65,535*] bytes in an SSH transport connection are dropped.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [aes128-cbc, aes256-cbc].

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [ssh-rsa, rsa-sha2-256, rsa-sha2-512] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha2-256, hmac-sha2-512] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1, ecdh-sha2-nistp256] and [ecdh-sha2-nistp384, ecdh-sha2-nistp384] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHS_EXT.1.8 The TSF shall ensure that within SSH connections, the same session keys are used for a threshold of no longer than one hour, and each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

5.2.3 Identification and authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*1-3*] 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 a local Administrator].

5.2.3.2 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 [minimum *1*] and [*maximum 127*] characters.

5.2.3.3 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 action on behalf of that administrative user.

5.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local [password-based, SSH public key-based [*no other*]] authentication mechanism to perform local administrative user authentication.

5.2.3.5 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**.

5.2.3.6 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 certification 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 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 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.*

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.

Application Note
NIAP TD0527 has been applied to FIA_X509_EXT.1/Rev, though it impacts only the tests, not the text of the SFR

5.2.3.7 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 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].

Application Note
NIAP TD0537 has been applied to FIA_X509_EXT.2.

5.2.3.8 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.

5.2.4 Security management (FMT)

5.2.4.1 FMT_MOF.1/Services Management of security functions behavior

FMT_MOF.1.1/Services The TSF shall restrict the ability to start and stop **services** to *Security Administrators*.

5.2.4.2 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 update to Security Administrators*.

5.2.4.3 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*.

5.2.4.4 FMT_MTD.1/CryptoKeys Management of TSF data

FMT_MTD.1.1/CryptoKeys The TSF shall restrict the ability to *manage* the *cryptographic keys to Security Administrators*.

5.2.4.5 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 locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [*hash comparison*] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*

- [
    - *Manually unlock a locked administrator account,*
    - Ability to start and stop services;
    - Ability to configure audit behaviour;
    - 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 set the time which is used for time-stamps;
    - Ability to configure the reference identifier for the peer;

    ]

  ].

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

are satisfied.

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_APW_EXT.1: 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.

5.2.5.2 FPT_SKP_EXT.1 Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

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

5.2.5.3 FPT_STM.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 [allow the Security Administrator to set the time].

5.2.5.4 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: [

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

].

5.2.5.5 FPT_TUD_EXT.1 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 [published hash] prior to installing those updates.

5.2.6 TOE Access (FTA)

5.2.6.1 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.

5.2.6.2 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*.

5.2.6.3 FTA_SSL.4 User-initiated Termination

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

5.2.6.4 FTA_TAB.1 Default TOE Access Banners

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

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 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 **authorized IT entities supporting the following capabilities: audit server,** [no other capabilities] 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 or 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 [

- *external audit server using IPsec*

  ].

5.2.7.2 FTP_TRP.1 Trusted Path/Admin Trusted Path (Refinement)

FTP_TRP.1.1/Admin: The TSF shall **be capable of using** [SSH] **to** provide a communication path between itself and **authorized** remote **Administrators** 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** 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*.

5.3 TOE SFR Dependencies Rationale for SFRs Found in NDcPPv2.2e

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPPv2.2e. As such, the NDcPPv2.2e SFR dependency rationale is deemed acceptable since the PP itself has been validated.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPPv2.2e which are derived from Common Criteria Version 3.1, Revision 5, dated April 2017. 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
Tests (ATE)	ATE_IND.1	Independent testing - conformance
Vulnerability Assessment (AVA)	AVA_VAN.1	Vulnerability analysis

5.4.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPPv2.2e. As such, the NDcPPv2.2e SAR rationale is deemed acceptable since the PP itself has been validated.

5.5 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
Security Target (ASE) / ASE_CCL.1 / ASE_ECD.1 / ASE_INT.1 / ASE_OBJ.1 / ASE_REQ.1 / ASE_SPD.1 / ASE_TSS.1	Section 2 of this ST includes the TOE and ST conformance claim to CC Version 3.1, Revision 5, dated: April 2017, CC Part 2 extended and CC Part 3 conformant, NDcPPv2.2e and the rationale of how TOE provides all of the functionality at a level of security commensurate with that identified in NDcPPv2.2e. Section 2 also includes the consistency rationale for the TOE Security Problem Definition and the Security Requirements to include the extended components definition.
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their: • purpose (general goal of the interface); • method of use (how the interface is to be used); • parameters (explicit inputs to and outputs from an interface that control the behaviour of that interface); • parameter descriptions (tells what the parameter is in some meaningful way); and • error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
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 ST.
AGD_PRE.1	The Installation Guide describes the installation, generation and startup procedures so that the users of the TOE can setup the components of the TOE in the evaluated configuration.
ALC_CMC.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.
ALC_CMS.1	
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

This section 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 an audited event occurs. The types of events that cause audit records to be generated include cryptography related events such as, generating keys (e.g. RSA), and deletion of cryptographic keys, importing of X509 certificates, and management of the cryptographic algorithms is provided through the CLI with auditing of those commands. Audit records are also generated for 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 specified in the audit record is in enough detail to identify the user for which the event is associated (e.g. user identity, MAC address, IP address), 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. 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. Additional information can be configured and included if desired. Following is the audit record format: seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n) Following is an example of an audit record: Dec 8 2020 10:59:19.394: ¥%PARSER-5-CFGLOG_LOGGEDCMD: User:lab logged command:line console 0 Dec 8 2020 10:59:19.441: ¥%SYS-5-CONFIG_I: Configured from console by lab on console The logging buffer size can be configured from a range of 4096 (default) to 2147483647 bytes. It is noted, not make the buffer size too large because the switch could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the switch. However, this value is the maximum available, and the buffer size should not be set to this amount. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.

TOE SFRs	How the SFR is Met
	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). Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. 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.; all of which are described in the Guidance documents and IOS-XE CLI. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. 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 message can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the functionality of the switch is affected. All notifications and information type message can be sent to the syslog server, whereas message is only for information; switch functionality is not affected. To configure the TOE to send audit records to a syslog server, the 'set logging server' command is used. A maximum of three syslog servers can be configured. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. 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 will store all audit records locally and when the connection to the remote syslog server is restored, all stored audit records will be transmitted to the remote syslog server. The FIPS crypto tests 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 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.
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. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.

TOE SFRs	How the SFR is Met
FAU_STG_EXT.1	The TOE is a standalone TOE that 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. The TOE can optionally be configured to export syslog records to a specified, external syslog server. Once the configuration is complete, the audit records are automatically sent to the external syslog server at the same time as they are written to the logging buffer. 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 connectivity to the syslog server
FCS_CKM.1	The TOE implements Diffie-Hellman based key establishment schemes that meets RFC 3526, Section 3. The TOE implements and uses the prime and generator specified in RFC 3526 Section 3 when generating parameters for the key exchange. 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. The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation in the NIST SP 800-56A and with section 6 and all subsections regarding RSA key pair generation. The TOE employs RSA-based key establishment, RSAES-PKCS1-v1_5 used in cryptographic operations as specified in Section 7.2 of RFC 8017. The TOE can create an RSA public-private key pair using key sizes of 2048-bit or larger that 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 X509v3 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 key pair generation portions of "The RSA Validation System" for FIPS 186-4 were used as a guide in testing the FCS_CKM.1 during the FIPS validation. The TOE employs RSA-based key establishment used in cryptographic operations. The TOE also implements ECC key generation for SSH key exchanges.
FCS_CKM.2	

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<p>The TOE implements Diffie-Hellman (DH) group 14 (2048) bit key establishment schemes in SSH and IPsec. The DH key generation meets RFC3526, Section 3.</p>
<p>The TOE acts as a receiver for SSH communications (remote administration) and as both a sender and receiver for IPsec communications (transmit generated audit records to an external IT entity (syslog server).</p>
<table>
<tr><th>Scheme</th><th>SFR</th><th>Service</th></tr>
<tr><td rowspan="2">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 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>
<tr><td>ECC
Key generation
Key establishment</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
</table>
<p>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 digital 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 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 RSA that meets FIPS PUB 186-4, “Digital Signature Standard”.</p>
<p>For details on each protocol, see the related SFR.</p>
</td></tr>
<tr><td>FCS_CKM.4</td><td>
<p>The TOE meets all requirements as specified by the cryptographic key destruction method of the keys and the Critical Security Parameters (CSPs) when no longer required for use.</p>
<p>See Table 21: TOE Key Zeroization in Section 7.1 Key Zeroization. The information provided in the table includes all of the secrets, keys and associated values, the description, and the method used to zeroization when no longer required for use.</p>
<p>The information is provided in the reference section for ease and readability of all of the secrets, keys and associated values, their description and zeroization methods.</p>
</td></tr>
</table>

TOE SFRs	How the SFR is Met
FCS_COP.1/DataEncryption	The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 256 bits) as described in ISO 10116. AES is implemented in the following protocols: IPsec and SSH. Through the implementation of the cryptographic module, the TOE also provides AES encryption and decryption in support of SSH for secure communications. The configuration and management of the cryptographic algorithms is provided through the CLI, to include the auditing of configuring the options by the Authorized Administrator. The relevant CAVP certificate numbers are listed in Table 6 FIPS References.
FCS_COP.1/SigGen	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. The TOE also supports RSA key size of 3072-bit, and it is recommended to use the stronger key size. Through the implementation of the cryptographic module, the TOE provides cryptographic signatures in support IPsec for secure communications. The configuration and management of the cryptographic algorithms is provided through the CLI, to include the auditing of configuring the options by the Authorized Administrator. The relevant CAVP certificate numbers are listed in Table 6 FIPS References.
FCS_COP.1/Hash FCS_COP.1/KeyedHash	The TOE provides cryptographic hashing services using SHA-1 and SHA-256 as specified in ISO/IEC 10118-3:2004 (with key sizes and message digest sizes of 160 and 256, respectively). The TOE provides keyed-hashing message authentication services using HMAC-SHA-1 and HMAC-SHA-256 that operates on 512-bit blocks and HMAC-SHA-512 operating on 1024-bit blocks of data, with key sizes and message digest sizes of 160-bits, 256 bits and 512 bits respectively as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. For IKE (ISAKMP) hashing, administrators can select any of SHA-1 and/or SHA-256 (with message digest sizes of 160 and 256 respectively) to be used with remote IPsec endpoints. For IPsec SA authentication integrity options Authorized Administrators can select any of esp-sha-hmac (HMAC-SHA-1), esp-sha256-hmac (HMAC-SHA-256), or esp-sha512-hmac (HMAC_SHA-512) with message digest sizes of 160 and 256 and 512 bits respectively to be part of the IPsec SA transform-set to be used with remote IPsec endpoints. Through the implementation of the cryptographic module, the TOE provides SHS hashing and HMAC message authentication in support of SSH and IPsec for secure communications. The configuration steps, commands and algorithms for the supported keys, key sizes and hashing are provided in the Operational User Guidance And Preparative Procedures. The relevant CAVP certificate numbers are listed in Table 6 FIPS References.

TOE SFRs	How the SFR is Met
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. The IPsec implementation provides VPN peer-to-peer capabilities. The VPN peer-to-peer tunnel allows for example the TOE and another switch 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 switch 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 is implemented using the cryptographic algorithms AES-CBC-128 and AES-CBC-256 together with HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512. 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 IKE protocols implement Peer Authentication using the RSA algorithm with X.509v3 certificates or preshared keys. When certificates are used for authentication, the SAN: fully qualified domain name (FQDN) is verified to ensure the certificate is valid and is from a valid entity. The attributes in the certificate are compared with the expected SAN: 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 a SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation.

TOE SFRs	How the SFR is Met
	The TOE can be configured to not allow "confidentiality only" ESP mode by ensuring the IKE Policies configured include ESP-encryption. The TOE supports configuration lifetimes of both Phase 1 SAs and Phase 2 SAs using "lifetime" command. The default time value for Phase 1 SAs is 24 hours, though is configurable from 1 to 24 hours. The default time value for Phase 2 SAs is 1 hour, though is configurable up to 8 hours. The TOE also 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 and AES-CBC-256 for encrypting the IKEv2 payloads. The Authorized 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), 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, and the following corresponding key sizes (in bits) are used: 112 (for DH Group 14) bits. The DH group can be configured by issuing the following command during the configuration of IPsec: TOE-common-criteria (config-isakmp)# group 14 This selects DH Group 14 (2048-bit MODP) for IKE and this sets the DH group offered during negotiations. The TOE generates the secret value 'x' used in the IKEv2 Diffie-Hellman key exchange ('x' in gx mod p) using the NIST approved AES-CTR Deterministic Random Bit Generator (DRBG) specified in FCS_RBG_EXT.1 and having possible lengths of 112 bits. When a random number is needed for a nonce, 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 nonce is likewise generated using the AES-CTR DRBG, is at least 128-bits and is at least half the output size of the negotiated pseudorandom function. IPsec provides secure tunnels between two peers, such as two switches. 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 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.

TOE SFRs	How the SFR is Met
	A crypto map (the Security Policy Definition (SPD)) set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence - the switch 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 170 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# crypto map MAP_NAME 19 ipsec-isakmp The match address 170 command means to use access list 101 in order to determine which traffic is relevant. For example: Router# (config-crypto-map)#match address 170 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 crypto map acl and does not match a non-crypto permit acl on the interface would be DISCARDED. Traffic that does not match a permit acl in the crypto map, though does match a non-crypto permit acl would be allowed to BYPASS the tunnel. For example, a non-crypto permit acl for icmp would allow ping traffic to flow unencrypted if a permit crypto map 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 crypto map entry as well as the data flow information from the specific access list entry. In IOS-XE the negotiations of the IKE SA adhere to configuration settings for IPsec applied by the administrator. For example, in the first SA, the encryption, hash and DH group is identified, for the Child SA the encryption and the hash are identified. The administrator configures the first SA to be as strong as or stronger than the child SA; meaning if the first SA is set at AES 128, then the Child SA can only be AES128. If the first SA is AES256, then the Child SA could be AES128 or AES256. During the negotiations, if a non-match is encountered, the process stops, and an error message is received.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in ISO/IEC 18031:2011seeded by an entropy source that accumulates entropy from a TSF-hardware based noise source. 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.

TOE SFRs	How the SFR is Met
FCS_SSHS_EXT.1	The TOE implementation of SSHv2 supports the following: • Compliance with RFCs 4251, 4252, 4253, and 4254; • Dropping packets greater than 65,535 bytes, as such packets would violate the IP packet size limitations; • Enforcement to only allow the encryption algorithms AES-CBC-128, and AES-CBC-256 to ensure confidentiality of the session; • Enforcement to only use of the SSH_RSA, RSA-SHA2-256, RSA-SHA2-512 public key algorithms for authentication; • Local password-based and public key authentication for administrative users accessing the TOE through SSHv2; The TOE provides a command that allows a user to upload a public key for SSHv2 public key authentication and to specify the user identity associated that key. • Enforcement to only allow the hashing algorithms hmac-sha2-256 and hmac-sha2-512-96 to ensure the integrity of the session and • The TOE's implementation of SSHv2 can be configured to only allow Diffie-Hellman Group 14 (2048-bit keys), ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384 and ECDH-SHA2-NISTP512 Key Establishment, as required by the cPP to which conformance is claimed. 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. Re-key occurs on the limit that is reached first.
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. 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. To ensure the privileged administrator account does not get locked out by the number of failed attempts it is essential that an additional Administrator account be created to only be used in an emergency at the local console to unlock the locked Administrator account. Although, it is noted that the lockout is not applicable to the local console administrators.
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 “)”. Minimum password length from 1 – 127 characters is settable by the Authorized Administrator and can be configured for minimum password lengths of 15 characters.

TOE SFRs	How the SFR is Met
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 and any network packets as configured by the Authorized Administrator may flow through the switch. 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 user name 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. The TOE also performs remote authentication using SSH public key to login authorized administrative users. 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 does not echo any characters as they are entered. For remote session authentication, the TOE does not echo any characters as they are entered.
FIA_X509_EXT.1/Rev FIA_X509_EXT.2 FIA_X509_EXT.3	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for IPsec connections. The Certificate Authority (CA) server in the IT Environment acts as a CRL distribution point. 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 switch 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 switch 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 switch and CA. • Enrollment profiles—The switch sends HTTP-based enrollment requests directly to the CA server instead of to the RA-mode certificate server (CS).

TOE SFRs	How the SFR is Met
	• Self-signed certificate enrollment for a trust point. When the CA issues a certificate, the CA can include in the certificate the CRL distribution point (CDP) for that certificate. The TOE will use the CDPs to locate and load the correct CRL. If a CDP is not specified in the certificate, the TOE will use the default Simple Certificate Enrollment Protocol (SCEP) method to retrieve the CRL. 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) keys and certificates can be stored in a specific location on the TOE. Certificates are stored to NVRAM by default; however, some switches do not have the required amount of NVRAM to successfully store certificates. All Cisco platforms support NVRAM and flash local storage. Depending on the platform, an authorized administrator may have other supported local storage options including bootflash, slot, disk or USB flash. The other supported storage options were not tested in the evaluated configuration. During run time, an authorized administrator can specify what active local storage device will be used to store certificates. 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 had been tampered with when the hash value would 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. 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

TOE SFRs	How the SFR is Met
	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 switch 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. The use of CRL is configurable and may be used for certificate revocation. The authorized administrator uses the revocation-check command to specify at least one method of revocation checking; CRL is the default method. The authorized administer sets the trust point and its name and the revocation-check method • crl --Certificate checking is performed by a CRL. This is the default option. 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. If the connection to determine the certificate validity cannot be established, the connection is rejected.
FMT_MOF.1/Services FMT_MOF./ManualUpdate FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys	The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged levels. For the purposes of this evaluation, the privileged level is equivalent to full administrative access to the CLI, which is the default access for IOS-XE privilege level 15; and the semi-privileged level 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. The term "Authorized 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 may also manage and modify TOE data based on the privileges assigned. The TOE provides the ability for Security Administrators (a.k.a Authorized Administrators) to access TOE data, such as audit data, configuration data, security attributes, session thresholds, cryptographic keys and updates. Each of the predefined and administratively configured privilege level has a set of permissions that will grant them access to the TOE data, though with some privilege levels, the access is limited.

TOE SFRs	How the SFR is Met
	The TOE does not provide automatic updates to the software version running on the TOE. The Security Administrators (a.k.a Authorized Administrators) can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates. In addition, network packets are permitted to flow, as configured by the Authorized Administrator, through the switch prior to the identification and authentication of an Authorized Administrator. The warning and access banner may also be displayed prior to the identification and authentication of an Authorized Administrator. No administrative functionality is available prior to administrative login. 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.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The Security Administrators (a.k.a Authorized Administrators) user can connect to the TOE using the CLI to perform these functions via SSHv2 secured connection, a terminal server, or at the local console. 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 which 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 allow any network packets as configured by the Authorized Administrator may flow through the switch prior to the identification and authentication process; • 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 configure the number of failed administrator logon attempts that will cause the account to be locked until it is reset; • The ability to update the IOS-XE software. The validity of the image is provided using SHA-256 and/or 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 configure the IPsec functionality which supports the secure connections to the audit server;

TOE SFRs	How the SFR is Met
	• The ability to import the X.509v3 certificates and validate for use in authentication and secure connections; • The ability to configure and set the time clock. • The ability to configure the reference identifiers for peers, which can be FQDN identifier. • The ability to *manually unlock a locked administrator account.*
FMT_SMR.2	The TOE maintains Authorizer Administrators that include privileged and semi-privileged administrator roles to administer the TOE locally and remotely. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-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 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. Note: the levels are not theoretically hierarchical. The term “Authorized 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 Authorized Administrator with the appropriate privileges. 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 SSHv2 secure connection.
FPT_SKP_EXT.1 and FPT_APW_EXT.1	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 command is the *password encryption aes* command used in global configuration mode. 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. During the setup and configuration of the TOE and the generation of keys, the TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. Additionally, all pre-shared and symmetric keys are stored in encrypted form to prevent access. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.

TOE SFRs	How the SFR is Met
FPT_STM.1	The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock provided by the underlying hardware. This date and time are used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. This system clock is also used for cryptographic functions such as SA lifetimes that are configured based on length of time values configured within 1-24 hours and for certificate validity.
FPT_TUD_EXT.1	Authorized Administrator can query the software version running on the TOE and can initiate updates to (replacements of) software images. The software version information for the TOE specific image can be displayed using the following commands. The administrator in privileged EXEC mode enters: Switch# show version (this displays information about the Cisco IOS software version running on the TOE the ROM Monitor and Bootflash software versions, and the hardware configuration, including the amount of system memory When updates are made available by Cisco, an Authorized Administrator can obtain and install those updates. The Authorized Administrator can download the approved image file from Cisco.com onto a trusted computer system for usage in the trusted update functionality. Software images are available from Cisco.com at the following: https://www.cisco.com/cisco/web/download/index.html. Published hash mechanisms 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 update the TOE. Once the Authorized Administrator has verified the TOE image, the Authorized Administrator can install the file on the TOE after they have logged in and have been successfully identified and authenticated. Once the image is loaded into bootflash, the Authorized Administrator can display information related to software authenticity for a specific image file, using the verify command. The image name and hash can be verified on the [TOE] download page on Cisco.com (https://software.cisco.com/download/home/286314016/type/282046477/release/Gibraltar-17.3 .1). If the there is an issue with the verification of the SHA512 checksum, the software should not be installed and contact Cisco for assistance. Once the Authorized Administrator has verified the TOE image, the file can be installed. For full details, refer to the (AGD) for assistance.
FPT_TST_EXT.1	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). Also, during the initialization and self-tests, the module inhibits all access to the cryptographic algorithms.

TOE SFRs	How the SFR is Met
	Additionally, the power-on self-tests are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before completing self-tests and entering FIPS mode. In the event of a power-on self-test failure, the cryptographic module will force the IOS platform to reload and reinitialize the operating system and cryptographic module. This operation ensures no cryptographic algorithms can be accessed unless all power on self-tests are successful. The tests include: • AES Known Answer Test – For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. • RSA Signature Known Answer Test (both signature/verification) – This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly. • RNG/DRBG Known Answer Test – For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly. • HMAC Known Answer Test – For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly. • SHA-1/256/512 Known Answer Test – For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match and the hash operations are operating correctly. Prior to installing the image, the Authorized Administrator can verify the public hash to ensure the files has not been tampered with prior to installing. In addition, the Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity. If any self-tests fail, the TOE transitions into an error state. In the error state, all secure data transmission is halted and the TOE outputs status information indicating the failure.

TOE SFRs	How the SFR is Met
	If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated. Following is an example: Example Error Message _FIPS-2-SELF_TEST_IOS_FAILURE: "IOS crypto FIPS self test failed at %s." Explanation FIPS self test on IOS crypto routine failed. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behaviour will be identified by the failure of a self-test.
FTA_SSL_EXT.1 and FTA_SSL.3	An Authorized 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 and virtual terminal (vty) lines. The configuration of the vty lines sets the configuration for the remote console access. The line console settings are not immediately activated for the current session. The current line console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session. If a local user session is inactive for a configured period of time, the session will be terminated and will require re-identification and authentication to login. If a remote user session is inactive for a configured period of time, the session will be terminated and will require re- identification and authentication to establish a new session. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the "exec-timeout" setting. The allowable inactivity timeout range is from 1 to 65535 seconds. A session (local or remote) that is inactive (i.e., no commands issuing from the local or remote client) for the defined timeout value will be terminated.
FTA_SSL.4	An Authorized Administrator is able to exit out of both local and remote administrative sessions by issuing the 'exit' command.
FTA_TAB.1	Authorized administrators define a custom login banner that will be displayed at the CLI for both local and remote access configurations prior to allowing Authorized Administrator access through those interfaces. A local console 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. Whereas a remote console is one that 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.
FTP_ITC.1	The TOE protects communications with authorized IT entities such as the remote audit server with IPsec. This protects the data from disclosure by encryption and by checksums that verify that data has not been modified.

TOE SFRs	How the SFR is Met
	The TOE protects communications with peer or neighbour switches using keyed hash as defined in FCS_COP.1.1/keyedhash and cryptographic hashing functions FCS_COP.1.1/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.1.1/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.
FTP_TRP.1/Admin	All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption. The remote users (Authorized Administrators) are able to initiate SSHv2 communications with the TOE.

7 ANNEX A: KEY ZEROIZATION

7.1 Key Zeroization

The following table describes the key zeroization referenced by FCS_CKM.4 provided by the TOE. As described below in the table, the TOE zeroize all secrets, keys and associated values when they are no longer required. The process in which the TOE zeroizes, meets FIPS 140 validation.

Table 19: TOE Key Zeroization

Name	Description	Zeroization
Diffie-Hellman Shared Secret	The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0's. This key is stored in DRAM.	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 DRAM.	Zeroized upon completion of DH exchange. Overwritten with: 0x00
skeyid	This is an IKE intermittent value used to create skeyid_d. This information is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
skeyid_d	This is an IKE intermittent value used to derive keying data for IPsec. This information is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session encrypt key	This the key IPsec key used for encrypting the traffic in an IPsec connection. This key is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
IKE session authentication key	This the key IPsec key used for authenticating the traffic in an IPsec connection. This key is stored in DRAM.	Automatically after IKE session terminated. Overwritten with: 0x00
ISAKMP preshared	This is the configured pre-shared key for ISAKMP negotiation. This key is stored in NVRAM.	Zeroized using the following command: # no crypto isakmp key[1] Overwritten with: 0x0d

[1] Using this command will zeroized all isakmp keys.

Name	Description	Zeroization
IKE RSA Private Key	The RSA private-public key pair is created by the device itself using the key generation CLI described below. The device's public key must be added 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 to enrol with the CA server to generate the device certificate. In the IKE authentication step, the device's certificate is first sent to another device so that it can be authenticated. The other device verifies the certificate is signed by CA's signing key, and then the device sends a random secret encrypted by the device's public key in the valid device certificate. Thus, establishing the trusted connection since 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 rsa[2] Overwritten with: 0x0d
IPsec encryption key	This is the key used to encrypt IPsec sessions. This key is stored in DRAM.	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 DRAM.	Automatically when IPsec session terminated. Overwritten with: 0x00
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents). This key is stored in NVRAM	Zeroized using the following command: # crypto key zeroize rsa [3] Overwritten with: 0x00
SSH Session Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents). This key is stored in DRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00
User Password	This is a variable 15+ character password that is used to authenticate local users. The password is stored in NVRAM.	Zeroized by overwriting with new password

[2] Using this command will zeroize all RSA keys.

[3] Using this command will zeroized all RSA keys

Name	Description	Zeroization
Enable Password (if used)	This is a variable 15+ character password that is used to authenticate local users at a higher privilege level. The password is stored in NVRAM.	Zeroized by overwriting with new password
RNG Seed	This seed is for the RNG. The seed is stored in DRAM.	Zeroized upon power cycle the device
RNG Seed Key	This is the seed key for the RNG. The seed key is stored in DRAM.	Zeroized upon power cycle the device

8 ANNEX B: NIAP TECHNICAL DECISIONS

This ST applies the following NIAP Technical Decisions:

Table 20 NIAP Technical Decisions (TD)

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0592	NIT Technical Decision for Local Storage of Audit Records	CPP_ND_V2.2E	FAU_STG	2021.05.21	Yes- TD has been applied
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	CPP_ND_V2.2E	A.LIMITED_FUNCTIONALITY, ACRONYMS	2021.05.21	Yes- TD has been applied
TD0581	The NIT has issued a technical decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3.	CPP_ND_V2.2E	FCS_CKM.2	2021.04.09	Yes- TD has been applied
TD0580	The NIT has issued a technical decision for clarification about use of DH14 in NDcPPv2.2e.	CPP_ND_V2.2E	FCS_CKM.1.1, FCS_CKM.2.1	2021.04.09	Yes- TD has been applied
TD0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	CPP_ND_V2.1, CPP_ND_V2.2E	FTP_ITC.1	2021.01.29	Yes- TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1	CPP_ND_V2.1, CPP_ND_V2.2E	FIA_UAU.1, FIA_PMG_EXT.1	2021.01.29	Yes- TD has been applied
TD0570	NiT Technical Decision for Clarification about FIA_AFL.1	CPP_ND_V2.1, CPP_ND_V2.2E	FIA_AFL.1	2021.01.29	Yes- TD has been applied
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	CPP_ND_V2.2E	ND SD v2.2, FCS_DTLSS_EXT.1.7, FCS_TLSS_EXT.1.4	2021.01.28	No, SFR not claimed
TD0564	NiT Technical Decision for Vulnerability Analysis Search Criteria	CPP_ND_V2.2E	NDSDv2.2, AVA_VAN.1	2021.01.28	Yes- TD has been applied
TD0563	NiT Technical Decision for Clarification of audit date information	CPP_ND_V2.2E	NDcPPv2.2e, FAU_GEN.1.2	2021.01.28	Yes- TD has been applied
TD0556	NIT Technical Decision for RFC 5077 question	CPP_ND_V2.2E	NDSDv2.2, FCS_TLSS_EXT.1.4, Test 3	2020.11.06	No, SFR not claimed
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	CPP_ND_V2.2E	NDSDv2.2, FCS_TLSS_EXT.1.4, Test 3	2020.11.06	No, SFR not claimed
TD0547	NIT Technical Decision for Clarification on developer	CPP_ND_V2.1, CPP_ND_V2.2E	ND SDv2.1, ND SDv2.2, AVA_VAN.1	2020.10.15	Yes- TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
	disclosure of AVA_VAN				
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	CPP_ND_V2.2E	FCS_DTLSC_EXT.1.1	2020.10.15	No, SFR not claimed
TD0538	The NIT has issued a technical decision for Outdated link to allowed-with list	CPP_ND_V2.1, CPP_ND_V2.2E	Section 2	2020.07.13	Yes- TD has been applied
TD0537	The NIT has issued a technical decision for Incorrect reference to FCS_TLSC_EXT.2.3	CPP_ND_V2.2E	FIA_X509_EXT.2.2	2020.07.13	Yes- TD has been applied
TD0536	The NIT has issued a technical decision for Update Verification Inconsistency	CPP_ND_V2.1, CPP_ND_V2.2E	AGD_OPE.1, ND SDv2.1, ND SDv2.2	2020.07.13	Yes - TD has been applied
TD0528	The NIT has issued a technical decision for Missing EAs for FCS_NTP_EXT.1.4	CPP_ND_V2.1, CPP_ND_V2.2E	FCS_NTP_EXT.1.4, ND SD v2.1, ND SD v2.2	2020.07.13	No, SFR not claimed

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	CPP_ND_V2.2E	FIA_X509_EXT.1/REV, FIA_X509_EXT.1/ITT	2020.07.01	Yes - TD has been applied

9 ANNEX C: REFERENCES

The following documentation was used to prepare this ST:

Table 21: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 5, dated: April 2017
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 5, dated: April 2017
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 5, dated: April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Version 3.1, Revision 5, dated: April 2017
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020
[800-56A]	NIST Special Publication 800-56A, March 2007
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication
[FIPS PUB 186-4]	FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS) October, 2015
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008