Cisco Catalyst 3650 and 3850 Series Switches running IOS-XE 16.12

Common Criteria Security Target

Version 2.0

4 December 2019

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

Table of Contents

1 SECURITY TARGET INTRODUCTION 9
1.1 ST and TOE Reference 9
1.2 TOE Overview 9
1.2.1 TOE Product Type 9
1.2.2 Supported non-TOE Hardware/ Software/ Firmware 10
1.3 TOE DESCRIPTION 10
1.4 TOE Evaluated Configuration 13
1.5 Physical Scope of the TOE 13
1.6 Logical Scope of the TOE 15
1.6.1 Security Audit 15
1.6.2 Cryptographic Support 16
1.6.3 Identification and authentication 18
1.6.4 Security Management 19
1.6.5 Protection of the TSF 19
1.6.6 TOE Access 20
1.6.7 Trusted path/Channels 20
1.7 Excluded Functionality 20
2 Conformance Claims 22
2.1 Common Criteria Conformance Claim 22
2.2 Protection Profile Conformance 22
2.3 Protection Profile Conformance Claim Rationale 26
2.3.1 TOE Appropriateness 26
2.3.2 TOE Security Problem Definition Consistency 26
2.3.3 Statement of Security Requirements Consistency 26
3 SECURITY PROBLEM DEFINITION 27
3.1 Assumptions 27
3.2 Threats 28
3.3 Organizational Security Policies 30
4 SECURITY OBJECTIVES 31
4.1 Security Objectives for the TOE 31
4.2 Security Objectives for the Environment 32
5 SECURITY REQUIREMENTS 33
5.1 Conventions 33
5.2 TOE Security Functional Requirements 33
5.2.1 Security audit (FAU) 35
5.2.2 Cryptographic Support (FCS) 37
5.2.3 Identification and authentication (FIA) 44
5.2.4 Security management (FMT) 46
5.2.5 Protection of the TSF (FPT) 48
5.2.6 TOE Access (FTA) 49
5.2.7 Trusted Path/Channels (FTP) 50
5.3 TOE SFR Dependencies Rationale for SFRs Found in NDcPPv2.0 50
5.4 Security Assurance Requirements 50

5.4.1 SAR Requirements....50
5.4.2 Security Assurance Requirements Rationale....51
5.5 Assurance Measures....51
6 TOE Summary Specification....53
6.1 TOE Security Functional Requirement Measures....53
7 Annex A: Key Zeroization....71
7.1 Key Zeroization....71
8 Annex B: References....74

List of Tables

TABLE 1 ACRONYMS 5
TABLE 2 TERMINOLOGY 6
TABLE 3 ST AND TOE IDENTIFICATION 9
TABLE 4 IT ENVIRONMENT COMPONENTS 10
TABLE 5 HARDWARE MODELS AND SPECIFICATIONS 14
TABLE 6 FIPS REFERENCES 17
TABLE 7 TOE PROVIDED CRYPTOGRAPHY 17
TABLE 8 CATALYST 3650 AND 3850 SERIES SWITCHES PLATFORM PROCESSORS 18
TABLE 9 EXCLUDED FUNCTIONALITY 20
TABLE 10 NIAP TECHNICAL DECISIONS (TD) 22
TABLE 11 PROTECTION PROFILES 26
TABLE 12 TOE ASSUMPTIONS 27
TABLE 13 THREATS 28
TABLE 14 ORGANIZATIONAL SECURITY POLICIES 30
TABLE 15 SECURITY OBJECTIVES FOR THE TOE 31
TABLE 16 SECURITY OBJECTIVES FOR THE ENVIRONMENT 32
TABLE 17 SECURITY FUNCTIONAL REQUIREMENTS 34
TABLE 18 AUDITABLE EVENTS 35
TABLE 19: ASSURANCE MEASURES 51
TABLE 20 ASSURANCE MEASURES 51
TABLE 21 HOW TOE SFRS MEASURES 53
TABLE 22: TOE KEY ZEROIZATION 71
TABLE 23: REFERENCES 74

List of Figures

FIGURE 1 TOE EXAMPLE DEPLOYMENT 12

Acronyms

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

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
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
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IOS	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
MKA	MACsec Key Agreement protocol
MKPDU	MACsec Key Agreement Protocol Data Unit
MPDU	MAC Protocol Data Unit
MSAP	MAC Service Access Point
MSDU	MAC Service Data Unit
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
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

Acronyms / Abbreviations	Definition
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.
MACsec Peer	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications
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.

Term	Definition
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), the Catalyst 3650 and 3850 Series Switches (Cat 3K Series) running IOS-XE 16.12. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE, which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]

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 3650 and 3850 Series Switches running IOS-XE 16.12
ST Version	2.0
Publication Date	4 December 2019
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Catalyst 3650 and 3850 Series Switches
TOE Hardware Models	3650 Series and 3850 Series
TOE Software Version	IOS-XE 16.12
Keywords	Audit, Authentication, Encryption, MACsec, Network Device, Secure Administration

1.2 TOE Overview

The Cisco Catalyst Switches 3650 Series and 3850 Series running IOS XE 16.12 (herein after referred to as Cat3K Series). The TOE is a purpose-built, switching and routing platform with OSI Layer2 and Layer3 traffic filtering capabilities. The TOE also supports MACsec encryption for switch-to-switch (inter-network device) security. The TOE includes the hardware models as defined in Table 3 in Section 1.1.

Cisco IOS software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective switching and routing. Although IOS performs many networking functions, this Security Target 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.

1.2.1 TOE Product Type

The Cisco Cat 3K Series are switching and routing platforms that provide connectivity and security services, including MACsec encryption onto a single, secure device. These switches offer broadband speeds and simplified management to small businesses, and enterprise small branch and teleworkers.

The Cisco Cat 3K Series are 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 of 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.
RADIUS Authentication (AAA) Server	Yes	This includes any IT environment RADIUS AAA server that provides authentication services to TOE administrators over a secure IPsec trusted channel either directly or connected to a TOE Peer that also supports a secure IPsec trusted channel.
MACsec Peer	Yes	This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications.
Certification Authority (CA)	Yes	This includes any IT Environment 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 and/or the remote authentication is attached for the TOE's use. If the remote syslog server and/or the remote authentication 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 Catalyst 3650 and 3850 Series Switches Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following: 3650 Series and 3850 Series Switches. The software is comprised of the Universal Cisco Internet Operating System (IOS) XE software image Release IOS XE 16.12

The Catalyst 3650 and 3850 Series Switches that comprises the TOE has common hardware characteristics. 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 Catalyst 3650 and 3850 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.
- Flash memory (EEPROM), used to store the Cisco IOS image (binary program).
- USB port (v2.0) (note, none of the USB devices are included in the TOE).
    - Type A for Storage, all Cisco supported USB flash drives.
    - Type mini-B as console port in the front.
- Non-volatile read-only memory (ROM) is used to store the bootstrap program and power-on diagnostic programs.
- Non-volatile random-access memory (NVRAM) is used to store switch configuration parameters that are used to initialize the system at start-up.
- Management is through a 10/100/1000 Ethernet port or an RJ-45 console port
- 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.

Cisco IOS 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 1.7 Logical Scope of the TOE below.

The following figure provides a visual depiction of an example TOE deployment. The TOE boundary is surrounded with a hashed red line.

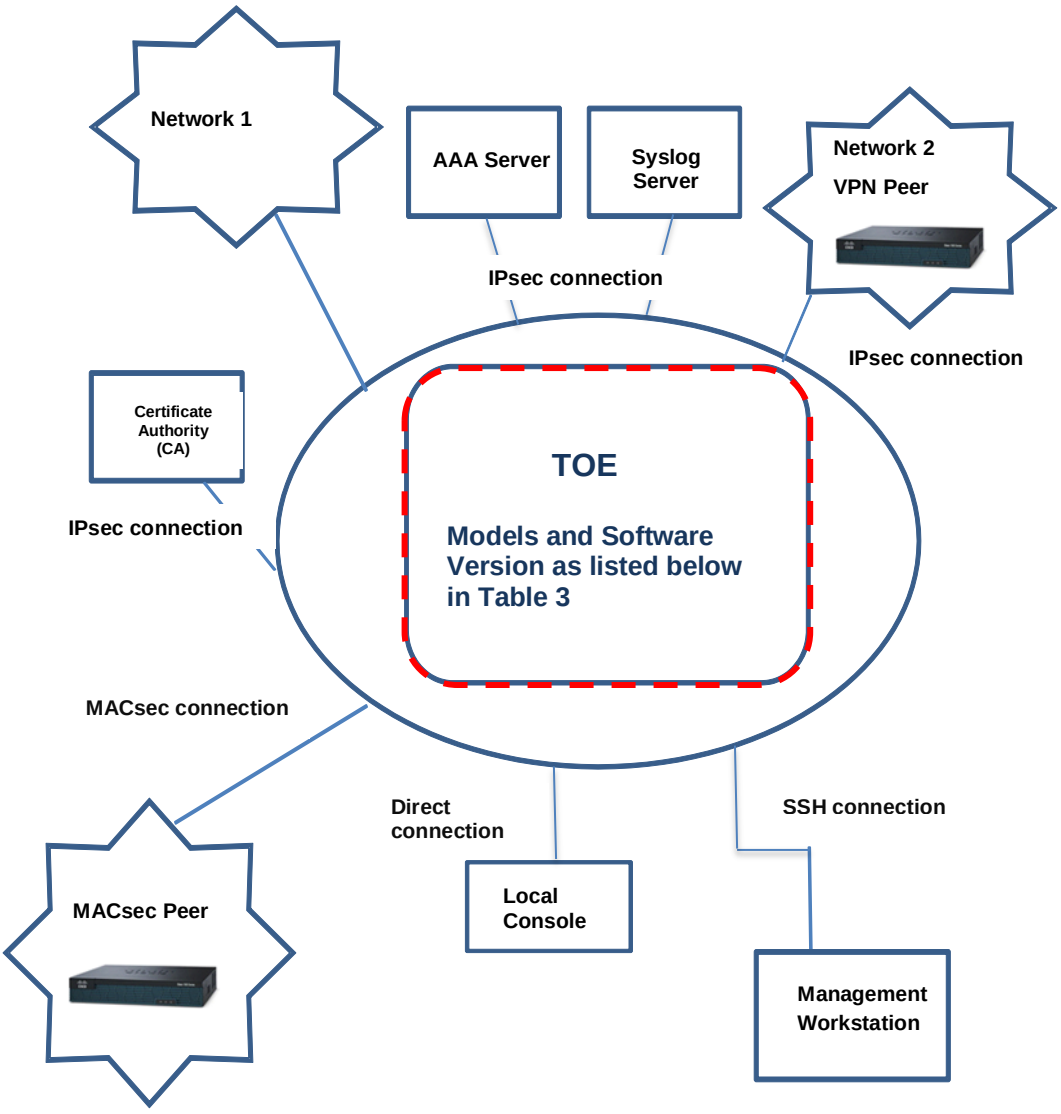

Figure 1 TOE Example Deployment

The previous figure includes the following devices, noting the TOE is only the 3650 Series and 3850 Series Catalyst Switches and only one TOE device is required for the deployment of the TOE in the evaluated configuration.

- Identifies the TOE Models
  - Catalyst Switches 3650 Series and 3850 Series running Cisco IOS-XE 16.12
- Identifies the following IT entities that are considered to be in the IT Environment:
  - Audit (syslog) Server
  - Local Console
  - Management Workstation with SSHv2 Client
  - RADIUS Authentication (AAA) Server
  - MACsec Peer

- Certificate Authority (CA)
- TOE Peer (Conditional)

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 16.12 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 Catalyst 3650 and 3850 Series Switches is to be remotely administered, then the management workstation must be connected to an internal network, SSHv2 is used to securely connect to the switch. A 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 switch models as follows: 3650 Series and 3850 Series running Cisco IOS-XE 16.12. The network, on which they reside, is considered part of the environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco Catalyst 3650 and 3850 Series Switches Common Criteria Operational User Guidance and Preparative Procedures document and are 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 on a particular model. For example, the 3650, WS-C3650-24TS measures 1.73 x 17.5 x 19.125 and has 24 ports (10M/100M/1000M (10 Gigabit Ethernet SFP+ Ports and Gigabit Ethernet SFP Ports). The USB, RJ-45, StackWise, power, software and processors are the same on all hardware series listed.

Table 5 Hardware Models and Specifications

Hardware	Processor	Software	Picture	Size	Power	Interfaces
Cisco Catalyst 3650 Series (WS-C3650-24TS WS-C3650-48TS WS-C3650-24PS WS-C3650-48PS WS-C3650-48FS WS-C3650-24TD WS-C3650-48TD WS-C3650-24PD WS-C3650-48PD WS-C3650-48FD WS-C3650-48TQ WS-C3650-48PQ WS-C3650-48FQ) WS-C3650-48FQM	Cavium Octeon CN6230, a MIPS64 processor	Cisco IOS-XE 16.12		1.73 x 17.5 x 17.625 1.73 x 17.5 x 19.125 1.73 x 17.5 x 11.625	The Cisco Catalyst 3650 Series support full IEEE 802.3at Power over Ethernet Plus (PoE+), Cisco Universal Power over Ethernet (Cisco UPOE®), and modular and field-replaceable redundant fans and power supplies.	24- and 48-port 10M/100M/1000M (10 Gigabit Ethernet SFP+ Ports and Gigabit Ethernet SFP Ports) USB connection and USB mini-Type B console connections Ethernet management is a 10/100/1000 port VPN routing/forwarding (VRF)) interface to which you can connect a PC Console port (RJ-45 Serial) is used to connect the TOE to a PC or a terminal server Cisco StackWise-160 technology stacking ports using the StackPower cables

Hardware	Processor	Software	Picture	Size	Power	Interfaces
Cisco Catalyst 3850 Series (WS-C3850-24T WS-C3850-48T WS-C3850-24P WS-C3850-48P WS-C3850-48F WS-C3850-24U WS-C3850-48U WS-C3850-12S WS-C3850-24S WS-C3850-12XS WS-C3850-24XS WS-C3850-24XU WS-C3850-48XS)	Cavium Octeon CN6230, a MIPS64 processor	Cisco IOS-XE 16.12		1.75 x 17.5 x 17.7 1.75 x 17.5 x 19.2 1.75 x 17.5 x 17.7 1.75 x 17.5 x 20.1	The Cisco Catalyst 3850 Series Switches support full IEEE 802.3at Power over Ethernet Plus (PoE+), Cisco Universal Power over Ethernet (Cisco UPOE), modular and field-replaceable network modules, RJ45 and fiber-based downlink interfaces, and redundant fans and power supplies.	12, 24- and 48-port 10M/100M/1000M (10 Gigabit Ethernet SFP+ Ports and Gigabit Ethernet SFP Ports) USB host port and USB mini-Type B console port Ethernet management is a 10/100/1000 port is a VPN routing/forwarding (VRF) interface to which you can connect a PC Console port (RJ-45 Serial) is used to connect the TOE to a PC or a terminal server Cisco StackWise-480 technology stacking ports using the StackPower cables

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 v2.0e and MACsec EP v1.2 as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco Catalyst 3650 and 3850 Series Switches provides 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 can be configured to block new permit actions.

The audit logs can be viewed on the TOE using the appropriate IOS 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 TOE security functionality. All the algorithms claimed have CAVP certificates (Operation Environment - Cavium Octeon CN6230, a MIPS64 processor).

The TOE leverages the IOS Common Criteria Module (IC2M) Rel5 as identified in the table below. The IOS software calls the IOS Common Cryptographic Module (IC2M) Rel5 (Firmware Version: Rel 5) certificate 2388 and has been validated for conformance to the requirements of FIPS 140-2 Level 1.

In addition, the TOE supports MACsec using proprietary Unified Access Data Plane (UADP) ASIC. The MACsec Controller (MSC) is embedded within the ASICs that are utilized within Cisco hardware platforms.

Refer to Table 6 for algorithm certificate references.

Table 6 FIPS References

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
AES	Used for symmetric encryption/decryption	AES Key Wrap in CMAC, CBC and GCM (128 and 256 bits)	4583	IC2M	FCS_COP.1/DataEncryption
			4769	UADP MSC	
SHS (SHA-1, SHA-256 and SHA-512)	Cryptographic hashing services	Byte Oriented	3760	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	3034	IC2M	FCS_COP.1/KeydHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	1529	IC2M	FCS_RBG_EXT.1
RSA	Key Generation and Signature Verification	FIPS PUB 186-4 Key Generation PKCS #1 v2.1 2048 bit key	2500	IC2M	FCS_CKM.1 FCS_COP.1/SigGen

The TOE provides cryptography in support of VPN 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 and the authentication servers.

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

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. Used to encrypt MACsec traffic.

Cryptographic Method	Use within the TOE
HMAC	Used for keyed hash, integrity services in IPsec and SSH session establishment.
DH	Used as the Key exchange method for SSH and IPsec
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 Used in MACsec session establishment

The Cisco Catalyst 3650 and 3850 Series Switches platforms contain the following processors as listed in Table 8 Catalyst 3650 and 3850 Series Switches Platform Processors

Table 8 Catalyst 3650 and 3850 Series Switches Platform Processors

Chassis	CPU Designation
3650	Cavium Octeon CN6230, a MIPS64 processor
3850	Cavium Octeon CN6230, a MIPS64 processor

1.6.3 Identification and authentication

The TOE performs two types of authentication: device-level authentication of the remote device (VPN peers) and user authentication for the Authorized Administrator of the TOE. Device-level authentication allows the TOE to establish a secure channel with a trusted peer. The secure channel is established only after each device authenticates the other. Device-level authentication is performed via IKE/IPsec mutual authentication. The IKE phase authentication for the IPsec communication channel between the TOE and authentication server and between the TOE and syslog server is considered part of the Identification and Authentication security functionality of the TOE.

The TOE provides authentication services for administrative users to connect to the TOEs 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 serial console or SSHv2 interfaces. The SSHv2 interface also supports authentication using SSH keys. The TOE supports use of a RADIUS AAA server (part of the IT Environment) for authentication of administrative users attempting to connect to the TOE's CLI.

The TOE also provides an automatic lockout when a user attempts to authenticate and enters invalid information. When the threshold for a defined number of authentication attempts fail has exceeded the configured allowable attempts, the user is locked out until an authorized administrator re-enables 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 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;
- Generate, install and manage PSK;
- Manage the Key Server, CAK and MKA participants and
- Configure lockout time interval for excessive authentication failures

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 who 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 is not a general-purpose operating system and access to Cisco IOS memory space is restricted to only Cisco IOS 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 is also able to detect replay of information received via secure channels (MACsec). The detection applied to network packets that terminate at the TOE, such as trusted communications between the TOE and an IT entity (e.g., MACsec peer). If replay is detected, the packets are discarded.

The TOE internally maintains the date and time. This date and time is 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 user to re-authenticate to establish a new session. The TOE can also be configured to lock the Authorized Administrator account after a specified number of failed logon attempts until an authorized administrator can enable the user account.

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 channels to be established to itself from remote administrators over SSHv2 and initiates outbound IPsec tunnels to transmit audit messages to remote syslog servers. In addition, IPsec is used to secure the session between the TOE and the authentication servers.

The TOE can also establish trusted paths of peer-to-peer IPsec sessions. The peer-to-peer IPsec sessions can be used for securing the communications between the TOE and authentication server/syslog server, as well as to protect the communications with the CA server.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 9 Excluded Functionality

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

These services can be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect the compliance to the collaborative

Protection Profile for Network Devices Version 2.0 + Errata 20180314 or the Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption v1.2.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. 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 11 Protection Profiles below. The following NIAP Technical Decisions (TD) have also been applied to the claims in this document. 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 10 **NIAP Technical Decisions (TD)**

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0357	AES Modes for the MACsec EP	PP_NDCPP_MACSEC_EP_V1.2	FCS_COP.1	2018.10.01	Yes - TD has been applied
TD0343	NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests	CPP_FW_V2.0E, CPP_ND_V2.0E	ND SD V2.0, FCS_IPSEC_EXT.1.14	2018.08.02	Yes - TD has been applied
TD0342	NIT Technical Decision for TLS and DTLS Server Tests	CPP_ND_V2.0E	ND SD V2.0, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2	08/02/18	No - Referenced SFR is not being claimed.
TD0341	NIT Technical Decision for TLS wildcard checking	CPP_ND_V2.0E	ND SD V2.0, FCS_TLSC_EXT.1.2, FCS_TLSC_EXT.2.2, FCS_DTLSC_EXT.1.2, FCS_DTLSC_EXT.2.2,	08/02/18	No, Referenced SFR is not being claimed.
TD0340	NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	CPP_FW_V2.0E, CPP_ND_V2.0E	FIA_X509_EXT.1.1	2018.08.02	Yes - TD has been applied
TD0339	NIT Technical Decision for Making password-	CPP_FW_V2.0E, CPP_ND_V2.0E	ND SD V2.0, FCS_SSHS_EXT.1.2	2018.08.02	Yes - TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
	based authentication optional in FCS_SSHS_EXT.1.2				
TD0338	NIT Technical Decision for Access Banner Verification	CPP_ND_V2.0E	ND SD V2.0, FTA_TAB.1	08/02/18	Yes - TD has been applied
TD0337	NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	CPP_FW_V2.0E, CPP_ND_V2.0E	ND SD V2.0, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1	2018.08.02	Yes - TD has been applied
TD0336	NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8	CPP_ND_V2.0E	ND SD V2.0, FCS_SSHC_EXT.1.8, FCS_SSHS_EXT.1.8	08/01/18	Yes - TD has been applied
TD0335	NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites	CPP_FW_V2.0E, CPP_ND_V2.0E	FCS_DTLSC_EXT.1.1, FCS_DTLSC_EXT.2.1, FCS_DTLSS_EXT.1.1, FCS_DTLSS_EXT.2.1, FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1, FCS_TLSS_EXT.1.1, FCS_TLSS_EXT.2.1	2018.08.01	No, Referenced SFR is not being claimed.
TD0334	NIT Technical Decision for Testing SSH when password-based authentication is not supported	CPP_ND_V2.0E	ND SD V2.0, FCS_SSHC_EXT.1.9	08/01/18	No, Referenced SFR is not being claimed.
TD0333	NIT Technical Decision for Applicability of FIA_X509_EXT.3	CPP_FW_V2.0E, CPP_ND_V2.0E	ND SD V2.0, FIA_X509_EXT	2018.08.01	Yes - TD has been applied
TD0324	NIT Technical Decision for Correction of section numbers in SD Table 1	CPP_ND_V2.0E	Table 1	05/18/18	Yes - TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0323	NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list	CPP_ND_V2.0E	ND SD V2.0, FCS_DTLSS_EXT.2.7, FCS_DTLSS_EXT.2.8	05/18/18	No, Referenced SFR is not being claimed.
TD0322	NIT Technical Decision for TLS server testing - Empty Certificate Authorities list	CPP_ND_V2.0E	ND SD V.1.0, ND SD V2.0, FCS_TLSS_EXT.2.4, FCS_TLSS_EXT.2.5	05/18/18	No, Referenced SFR is not being claimed.
TD0321	Protection of NTP communications	CPP_FW_V2.0E, CPP_ND_V2.0E	FTP_ITC.1, FPT_STM_EXT.1	05/21/18	Yes - TD has been applied
TD0291	NIT technical decision for DH14 and FCS_CKM.1	CPP_FW_V1.0, CPP_FW_v2.0, CPP_FW_V2.0E, CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	FCS_CKM.1.1, ND SD V1.0, ND SD V2.0	02/03/18	Yes - TD has been applied
TD0290	NIT technical decision for physical interruption of trusted path/channel.	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	FTP_ITC.1, FTP_TRP.1, FPT_ITT.1, ND SD V1.0, ND SD V2.0	02/03/18	Yes - TD has been applied
TD0289	NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1, FCS_DTLSC_EXT.1.1 (only ND SD V2.0), FCS_DTLSC_EXT.2.1 (only ND SD V2.0)	02/03/18	No, Referenced SFR is not being claimed.
TD0281	NIT Technical Decision for Testing both thresholds for SSH rekey	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	FCS_SSHC_EXT.1.8, FCS_SSHS_EXT.1.8, ND SD V1.0, ND SD V2.0	01/05/18	Yes - TD has been applied
TD0273	Rekey after CAK expiration	PP_NDCPP_MACSEC_EP_V1.2	FCS_MACSEC_EXT.4	12/20/17	Yes - TD has been applied
TD0272	Update to FMT_SMF.1	PP_NDCPP_MACSEC_EP_V1.2	FMT.SMF.1	12/20/17	Yes - TD has been applied
TD0259	NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	CPP_FW_v2.0, CPP_FW_V2.0E, CPP_ND_V2.0, CPP_ND_V2.0E	FCS_SSHC_EXT.1.5/FCS_SSHS_EXT.1.5	11/13/17	Yes - TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0257	NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	ND SD V1.0, ND SD V2.0, FCS_DTLSC_EXT.1.2/FCS_DTLSC_EXT.2.2 Tests 1-4 (ND SD V2.0), FCS_TLSC_EXT.1.2/FCS_TLSC_EXT.2.2, Tests 1-4 (ND SD V1.0, ND SD V2.0)	11/13/17	No, Referenced SFR is not being claimed.
TD0256	NIT Technical Decision for Handling of TLS connections with and without mutual authentication	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	ND SD V1.0, ND SD V2.0, FCS_DTLSC_EXT.2.5 (ND SD V2.0), FCS_TLSC_EXT.2 (ND SD V1.0, ND SD V2.0)	11/13/17	No, Referenced SFR is not being claimed.
TD0228	NIT Technical Decision for CA certificates - basicConstraints validation	CPP_FW_V1.0, CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	ND SD V1.0, ND SD V2.0, FIA_X509_EXT.1.2	06/15/18	Yes - TD has been applied
TD0190	FPT_FLS.1(2)/ SelfTest Failure with Preservation of Secure State and Modular Network Devices	PP_NDCPP_MACSEC_EP_V1.2	FPT_FLS.1(2)/SelfTest	04/11/17	Yes - TD has been applied
TD0135	SNMP in NDcPP MACsec EP v1.2	PP_NDCPP_MACSEC_EP_V1.2	FMT_SNMP_EXT.1.1, FCS_SNMP_EXT.1.1	01/25/17	No, Referenced SFR is not being claimed.
TD0134	AES Data Encryption/Decryption in NDcPP MACsec EP v1.2	PP_NDCPP_MACSEC_EP_V1.2	FCS_COP.1	12/21/16	Yes - TD has been applied
TD0105	MACsec Key Agreement	PP_NDCPP_MACSEC_EP_V1.2	FCS_MKA_EXT.1.2, FCS_MKA_EXT.1.5, FCS_MKA.1.8,	09/13/16	Yes - TD has been applied

Table 11 Protection Profiles

Protection Profile	Version	Date
Network Device Collaborative Protection Profile (NDcPP) + Errata 20180314	2.0e	14 March 2018
Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption (MACsec EP)	1.2	10 May 2016

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

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

- collaborative Protection Profile for Network Devices + Errata 20180314, Version 2.0e
- Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption (MACsec EP), version 1.2

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 + Errata 20180314, Version 2.0e and the Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption (MACsec EP), version 1.2 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 NDcPP v2.0e and MACsec EP v1.2, 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 NDcPP v2.0e and MACsec EP v1.2, 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 NDcPP v2.0e and MACsec EP v1.2.

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.

Table 12 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.
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 computing platform for general purpose applications (unrelated to networking functionality).
~~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 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.

Assumption	Assumption Definition
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.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.

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 13 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.

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 include 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.
T.DATA_INTEGRITY	An attacker may modify data transmitted over the MACsec channel in a way that is not detected by the recipient.
T.NETWORK_ACCESS	An attacker may send traffic through the TOE that enables them to access devices in the TOE's Operational Environment without authorization.
T.UNTRUSTED_COMMUNICATION_CHANNELS	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.

3.3 Organizational Security Policies

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

Table 14 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 +Errata 2018314 v2.0e does not define any security objectives for the TOE, however the Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption (MACsec EP), version 1.2 includes the following security objectives specific to MACsec devices.

Table 15 Security Objectives for the TOE

Security Objective and SFR mapping	Security Objective Definition
O.CRYPTOGRAPHIC_FUNCTIONS (FCS_COP.1/DataEncryption, FCS_MACSEC_EXT.2, FCS_MACSEC_EXT.3, FTP_ITC.1, FTP_TRP.1)	The TOE will provide cryptographic functions that are used to establish secure communications channels between the TOE and the Operational Environment.
O.AUTHENTICATION (FCS_MACSEC_EXT.4, FCS_MKA_EXT.1, FIA_PSK_EXT.1)	The TOE will provide the ability to establish connectivity associations with other MACsec peers.
O.PORT_FILTERING (FCS_MACSEC_EXT.1, FCS_EAP-TLS_EXT.1 (selection-based), FCS_DEVID_EXT.1 (selection-based), FIA_PSK_EXT.1)	The TOE will provide the ability to restrict the flow of traffic between networks based on originating port and established connection information.
O.SYSTEM_MONITORING (FAU_GEN.1)	The TOE will provide the means to detect when security-relevant events occur and generate audit events in response to this detection.
O.AUTHORIZED_ADMINISTRATION (FIA_AFL.1, FIA_AFL_EXT.1 (optional), FMT_SNMP_EXT.1 (selection-based), FMT_SMF.1, FPT_CAK_EXT.1, FTP_TRP.1)	The TOE will provide management functions that can be used to securely manage the TSF.
O.TSF_INTEGRITY (FPT_FLS.1(2)/SelfTest)	The TOE will provide mechanisms to ensure that it only operates when its integrity is verified.
O.REPLAY_DETECTION (FPT_RPL.1, FPT_RPL_EXT.1(optional))	The TOE will provide the means to detect attempted replay of MACsec traffic by inspection of packet header information.
O.VERIFIABLE_UPDATES (FPT_TUD_EXT.1)	The TOE will provide a mechanism to verify the authenticity and integrity of product updates before they are applied.

4.2 Security Objectives for the Environment

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

Table 16 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.
~~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 Administrator are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

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 4, dated: September 2012* 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:

- 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 NDcPPv2.0e and MACsec EP v1.2.

The following conventions were used to resolve conflicting SFRs between NDcPPv2.0e and MACsec Ep v1.2:

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

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 17 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_COP.1(1)	KeyedHashCMAC Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)
	FCS_COP.1(2)	Cryptographic Operation (MACsec Data Encryption/Decryption)
	FCS_IPSEC_EXT.1	IPsec Protocol
	FCS_MACSEC_EXT.1	MACsec
	FCS_MACSEC_EXT.2	MACsec Integrity and Confidentiality
	FCS_MACSEC_EXT.3	MACsec Randomness
	FCS_MACSEC_EXT.4	MACsec Key Usage
	FCS_MKA_EXT.1	MACsec Key Agreement
	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_PSK_EXT.1 Extended	Pre-Shared Key Composition
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
FMT: 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_CAK_EXT.1	Protection of CAK Data
	FPT_FLS.1	SelfTest Failure with Preservation of Secure State
	FPT_RPL.1	Replay Detection
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	FPT_STM_EXT.1	Reliable Time Stamps

Class Name	Component Identification	Component Name
	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: Trusted path/channels	FTP_ITC.1	Trusted Channel
	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 administrator 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 18.*

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 18.*

Table 18 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.
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.

SFR	Auditable Event	Additional Audit Record Contents
FCS_COP.1(1)/KeyedHashCMAC Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)	None	None
FCS_COP.1(2) Cryptographic Operation (MACsec Data Encryption/Decryption)	None.	None.
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)
FCS_MACSEC_EXT.1.7	Creation of Connectivity Association	Connectivity Association Key Names
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key	Creation and update times
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FIA_AFL.1	Administrator lockout due to excessive authentication failures	None.
FIA_PMG_EXT.1	None.	None.
FIA_PSK_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the 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	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/Service	Starting and stopping of services	None.
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	All management activities of TSF data.	None.
FMT_MTD.1_CryptoKeys	Management of cryptographic keys	None
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_RPL.1	Detected replay attempt	None.
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	No additional information.

SFR	Auditable Event	Additional Audit Record Contents
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.

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [*when allotted space has reached its threshold*], [*no other action*]] 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 Refinement: 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;
- FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3

] ~~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 meets the following: NIST Special Publication 800-56B Revision 1, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"**;**
- Key establishment scheme using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3;

] ~~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-pass]* 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, GCM] *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, GCM as specified in ISO 19772].

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, SHA-512] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ and message digest sizes [160, 256, 512] 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] **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_COP.1(1)/KeyedHashCMAC Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)

FCS_COP.1.1(1)/KeyedHash:CMAC Refinement: The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm **[AES-CMAC]** and cryptographic key sizes [**128, 256 bits]** and message digest size **of 128** bits that meets **NIST SP 800-38B.**

5.2.2.9 FCS_COP.1(2) Cryptographic Operation (MACsec Data Encryption/Decryption)

FCS_COP.1.1(2) Refinement: The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm AES used in **AES Key Wrap, GCM** and cryptographic key sizes **128 bits, 256 bits** that meet the following: **AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F, GCM as specified in ISO 19772**.

5.2.2.10 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 [transport mode, tunnel 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 (specified by RFC 3602, 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] and [*no other algorithm*].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- IKEv1, using Main Mode for Phase 1 exchanges, as defined in RFCs 2407, 2408, 2409, RFC 4109, [no other RFCs for extended sequence numbers], and [RFC 4868 for hash functions]].
- IKEv2 as defined in RFCs 5996 [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 [IKEv1, 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 [

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

  ];
- IKEv2 SA lifetimes can be configured by an Security Administrator based on *[*
    - length of time, where the time values can configured within *[1-24*] hours*;*

  ]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that

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

  ];
- IKEv2 Child SA lifetimes can be configured by an Security Administrator based on *[*
    - number of bytes
    - length of time, where the time values can 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 [*320 (for DH Group 14)*] bits.

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

- [according to the security strength associated with the negotiated Diffie-Hellman group

].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that all 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 [IKEv1 Phase 1, IKEv2 IKE_SA] connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the [IKEv1 Phase 2, IKEv2 CHILD_SA] connection.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that 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: [CN: Fully Qualified Domain Name (FQDN), Distinguished Name (DN)] and [no other reference identifier type].

5.2.2.11 FCS_MACSEC_EXT.1 MACsec

FCS_MACSEC_EXT.1.1 The TSF shall implement MACsec in accordance with IEEE Standard 802.1AE-2006.

FCS_MACSEC_EXT.1.2 The TSF shall derive a Secure Channel Identifier (SCI) from a peer's MAC address and port to uniquely identify the originator of a MACsec Protocol Data Unit (MPDU).

FCS_MACSEC_EXT.1.3 The TSF shall reject any MPDUs during a given session that contain an SCI other than the one used to establish that session.

FCS_MACSEC_EXT.1.4 The TSF shall permit only EAPOL (PAE EtherType 88-8E) and MACsec frames (EtherType 88-E5) and discard others.

5.2.2.12 FCS_MACSEC_EXT.2 MACsec Integrity and Confidentiality

FCS_MACSEC _EXT.2.1 The TOE shall implement MACsec with support for integrity protection with a confidentiality offset of [0, 30, 50].

FCS_MACSEC_ EXT.2.2 The TSF shall provide assurance of the integrity of protocol data units (MPDUs) using an Integrity Check Value (ICV) derived with the Secure Association Key (SAK).

FCS_MACSEC_EXT.2.3 The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF.

5.2.2.13 FCS_MACSEC_EXT.3 MACsec Randomness

FCS_ MACSEC_EXT.3.1 The TSF shall generate unique Secure Association Keys (SAKs) using [key derivation from Connectivity Association Key (CAK) per section 9.8.1 of IEEE 802.1X-

2010] such that the likelihood of a repeating SAK is no less than 1 in 2 to the power of the size of the generated key.

FCS_ MACSEC_EXT.3.2 The TSF shall generate unique nonce for the derivation of SAKs using the TOE's random bit generator as specified by FCS_RBG_EXT.1.

5.2.2.14 FCS_MACSEC_EXT.4 MACsec Key Usage

FCS_MACSEC_EXT.4.1 The TSF shall support peer authentication using pre-shared keys, [no other methods].

FCS_MACSEC_EXT.4.2 The TSF shall distribute SAKs between MACsec peers using AES key wrap as specified in FCS_COP.1(2).

FCS_MACSEC_EXT.4.3 The TSF shall support specifying a lifetime for CAKs.

FCS_MACSEC_EXT.4.4 The TSF shall associate Connectivity Association Key Names (CKNs) with CAKs that are defined by the key derivation function using the CAK as input data (per 802.1X, section 9.8.1).

FCS_MACSEC_EXT.4.5 The TSF shall associate Connectivity Association Key Names (CKNs) with CAKs. The length of the CKN shall be an integer number of octets, between 1 and 32 (inclusive).

5.2.2.15 FCS_MKA_EXT.1 MACsec Key Agreement

FCS_MKA_EXT.1.1 The TSF shall implement Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014.

FCS_MKA_EXT.1.2 The TSF shall enable data delay protection for MKA that ensures data frames protected by MACsec are not delayed by more than 2 seconds.

FCS_MKA_ EXT.1.3 The TSF shall provide assurance of the integrity of MKA protocol data units (MKPDUs) using an Integrity Check Value (ICV) derived from an Integrity Check Value Key (ICK).

FCS_MKA_EXT.1.4 The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF.

FCS_ MKA_EXT.1.5 The TSF shall enforce an MKA Lifetime Timeout limit of 6.0 seconds and MKA Bounded Hello Time limit of 0.5 seconds.

FCS_MKA_EXT.1.6 The Key Server shall refresh a SAK when it expires. The Key Server shall distribute a SAK by [pairwise CAKs]. ~~If group CAK is selected, then the Key Server shall distribute a group CAK by [selection: a group CAK, pairwise CAKs, pre-shared key].~~ If pairwise

CAK is selected, then the pairwise CAK shall be [pre-shared key]. The Key Server shall refresh a CAK when it expires.

FCS_MKA_EXT.1.7 The Key Server shall distribute a fresh SAK whenever a member is added to or removed from the live membership of the CA.

FCS_MKA_EXT.1.8 The TSF shall validate MKPDUs according to 802.1X, Section 11.11.2. In particular, the TSF shall discard without further processing any MKPDUs to which any of the following conditions apply:

a) The destination address of the MKPDU was an individual address.
b) The MKPDU is less than 32 octets long.
c) The MKPDU is not a multiple of 4 octets long.
d) The MKPDU comprises fewer octets than indicated by the Basic Parameter Set body length, as encoded in bits 4 through 1 of octet 3 and bits 8 through 1 of octet 4, plus 16 octets of ICV.
e) The CAK Name is not recognized.

If an MKPDU passes these tests, then the TSF will begin processing it as follows:

a) If the Algorithm Agility parameter identifies an algorithm that has been implemented by the receiver, the ICV shall be verified as specified in IEEE 802.1x Section 9.4.1.
b) If the Algorithm Agility parameter is unrecognized or not implemented by the receiver, its value can be recorded for diagnosis but the received MKPDU shall be discarded without further processing.

Each received MKPDU that is validated as specified in this clause and verified as specified in 802.1X, section 9.4.1 shall be decoded as specified in 802.1X, section 11.11.4.

5.2.2.16 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 noise source*] with 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.

5.2.2.17 FCS_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*] 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] 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-sha1, hmac-sha1-96] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1] and [no other methods] 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 no more than one gigabyte of transmitted data. After either 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 Refinement: The TSF shall detect when an Administrator configurable positive integer within [1-3] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met], the TSF shall [prevent the offending remote Administrator from successfully authenticating 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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“,”)”, *[no other characters]*];
b) Minimum password length shall be configurable to [15] and [15].

5.2.3.3 FIA_PSK_EXT.1 Extended: Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall use pre-shared keys for MKA as defined by IEEE 802.1X, [IPsec protocols].

FIA_PSK_EXT.1.2 The TSF shall be able to [accept] bit-based pre-shared keys.

5.2.3.4 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;
- [*any network packets as configured by the authorized administrator may flow through the switch*].

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.

5.2.3.5 FIA_UAU_EXT.2 Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [*remote password-based authentication via RADIUS*] to perform administrative user authentication.

5.2.3.6 IA_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**.

5.2.3.7 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates.**
- The certificate path must terminate with a trusted CA certificate.
- 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, Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *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.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

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

5.2.3.8 FIA_X509_EXT.2 X.509 Certificate Authentication

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

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [allow the administrator to choose whether to accept the certificate in these cases].

5.2.3.9 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and [Common Name, Organization, Organizational Unit and 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 enable and disable the functions **and services** to *Security Administrators*.

5.2.4.2 FMT_MOF.1/ManualUpdate Management of security functions behaviour

FMT_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual update* to *Security Administrators*.

5.2.4.1 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*.

5.2.4.2 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*.

5.2.4.3 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;*
- *Generate a PSK-based CAK and install it in the device*
- *Manage the Key Server to create, delete, and activate MKA participants* [as specified in 802.1X, sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipantEntry) and section 12.2 (cf. function createMKA())]
- *Specify a lifetime of a CAK*
- *Enable, disable, or delete a PSK-based CAK using* [CLI management commands]
- *Cause Key Server to generate a new group CAK (i.e., rekey the CA) using* [CLI management commands]
- *Configure the number of failed administrator authentication attempts that will cause an account to be locked out* [*Manually unlock a locked administrator account*]
- [
    - Ability to configure audit behaviour;
    - Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;
    - 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;

    ]

].

5.2.4.4 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 passwords in non-plaintext form.

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

5.2.5.2 FPT_CAK_EXT.1 Protection of CAK Data

FPT_CAK_EXT.1.1 The TSF shall prevent reading of CAK values by administrators.

5.2.5.3 FPT_FLS.1(2)/ SelfTest Failure with Preservation of Secure State

FPT_FLS.1.1(2)/SelfTest Refinement: The TSF shall **shut down** when any of the following types of failures occur: **failure of the power-on self-tests, failure of integrity check of the TSF executable image, failure of noise source health tests**.

5.2.5.4 FPT_RPL.1 Replay Detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: [MPDUs, MKA frames].

FPT_RPL.1.2 The TSF shall perform [*discarding of the replayed data, logging of the detected replay attempt*] when replay is detected.

5.2.5.5 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.

5.2.5.6 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*].

5.2.5.7 FPT_TST_EXT.1: TSF Testing (Extended)

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 operations*] 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*

].

5.2.5.8 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 a 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, MACsec**] to provide** a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, [**authentication server, *[MACsec peers]***]** 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 [communications with the following:

- *remote AAA servers using IPsec*
- *external audit server using IPsec*
- *MACsec peers using MACsec*].

5.2.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin Refinement: The TSF shall **be capable of using** [SSH] **to** provide a communication path between itself **and authorized** remote **administrators** that provides confidentiality and integrity, 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 **Aadministrators** 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 NDcPPv2.0

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPPv2.0e and MACsec EPv1.2. As such, the NDcPPv2.0e and MACsec EPv1.2 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 NDcPPv2.0e and MACsec EPv1.2 which are derived from Common Criteria Version 3.1, Revision 4, September 2012. The assurance requirements are summarized in the table below.

Table 19: 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 NDcPPv2.0e and MACsec EP v1.2. As such, the NDcPPv2.0e and MACsec EP v1.2 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 20 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 4, dated: September 2012, CC Part 2 extended and CC Part 3 conformant and NDcPPv2.0e and the rationale of how TOE provides all of the functionality at a level of security commensurate with that identified in NDcPPv2.0e. Section 2 also includes the consistency rationale for the TOE Security Problem Definition and the Security Requirements to include the extended components definition.

Component	How requirement will be met
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 ALC_CMS.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s) identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
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 21 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 identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the events is specified in 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. Additionally, the startup and shutdown of the audit functionality is audited. The audit trail consist 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: *Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) 18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) *Mar 1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) 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. 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 CLI. 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 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 all permit traffic is denied until the communications is re-established. 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.
FAU_STG_EXT.1	The TOE is 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 For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 4096 (default) to 2147483647 bytes of available disk space Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.. Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.
FCS_CKM.1 and FCS_CKM.2	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 also implements RSA key establishment schemes that is conformant to NIST SP 800-56B. The TOE complies with section 6 and all subsections regarding RSA key pair generation and key establishment in the NIST SP 800-56B. Asymmetric cryptographic

TOE SFRs	How the SFR is Met
	keys used for IKE peer authentication are generated according to FIPS PUB 186-4, Appendix B.3 for RSA schemes. The TOE can create a RSA public-private key pair 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 TOE can store and distribute the certificate to external entities including Registration Authorities (RA). 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 implements Diffie-Hellman (DH) group 14 (2048) bit key establishment schemes in SSH. The DH key generation meets RFC3526, Section 3. The TOE acts as a receiver for SSH communications and as both a sender and receiver for IPsec communications. For details on each protocol, see the related SFR.
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) when no longer required for use. See Table 22: TOE Key Zeroization in Section 7.1 Key Zeroization. The information provided in the table includes all of the all secrets, keys and associated values, the description, and the method used to zeroization when no longer required for use. The information is provided in the reference section for ease and readability of all of the all secrets, keys and associated values, their description and zeroization methods.
FCS_COP.1/DataEncryption	The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode (128, 256 bits) as described in ISO 18033-3 and ISO 10116. AES is implemented in the following protocols: IPsec and SSH. The relevant FIPS 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 FIPS PUB 186-4, "Digital Signature Standard". The relevant FIPS 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, SHA-256 and SHA-512 as specified in ISO/IEC 10118-3:2004. 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".

TOE SFRs	How the SFR is Met
	For IKE (ISAKMP) hashing, administrators can select any of SHA-1, SHA-256 and/or SHA-512 (with message digest sizes of 160, 256 and 512 bits respectively) to be used with remote IPsec endpoints. SHA-256 hashing is used for verification of software image integrity. The TOE uses HMAC-SHA1 message authentication as part of the RADIUS Key Wrap functionality. For IPsec SA authentication integrity options administrators can select any of esp-sha-hmac (HMAC-SHA-1), esp-sha256-hmac, or esp-sha512-hmac (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. The relevant FIPS certificate numbers are listed in Table 6 FIPS References. The configuration steps, commands and algorithms for the supported keys, key sizes and hashing are provided in the Operational User Guidance And Preparative Procedures
FCS_COP.1(1)/KeyedHashCMAC Cryptographic Operation (AES-CMAC Keyed Hash Algorithm) FCS_COP.1(2) Cryptographic Operation (MACsec Data Encryption/Decryption)	The TOE implements AES-CMAC keyed hash function for message authentication as described in NIST SP 800-38B. The key length, hash function used, block size, and output MAC length used are as follows: AES-128 (hash function and key length) Block Sizes: Full (block size) Message Length: 0-256 bits (output MAC length) AES-256 (hash function and key length) Block Sizes: Full (block size) Message Length: 0-256 bits (output MAC length) The TOE provides symmetric encryption and decryption capabilities using AES in AES Key Wrap and GCM mode (128 and 256 bits) as described in AES as specified in ISO 18033-3, AES Key Wrap in CMAC mode as specified in NIST SP 800-38F, GCM as specified in ISO 19772. AES is implemented in MACsec protocol. The relevant FIPS certificate numbers are listed in Table 6 FIPS References.
FCS_IPSEC_EXT.1	The IPsec implementation provides both VPN peer-to-peer and VPN client to TOE 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. The VPN client to TOE configuration would be where a remote VPN client connects into the TOE in order to gain access to an authorized private network. Authenticating with the TOE would give the VPN client a secure IPsec tunnel to connect over the internet into their private network. 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

TOE SFRs	How the SFR is Met
	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 distinguished name (DN) is verified to ensure the certificate is valid and is from a valid entity. The DN naming attributes in the certificate is compared with the expected DN naming attributes and deemed valid if the attribute types are the same and the values are the same and as expected. The fully qualified domain name (FQDN) can also be used as verification where the attributes in the certificate are compared with the expected FQDN. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including: • The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters, either signature based or pre-shared key based), • The establishment of additional Security Associations to protect packets flows using Encapsulating Security Payload (ESP), and • The agreement of secure bulk data encryption AES keys for use with ESP. After the two peers agree upon a policy, the security parameters of the policy are identified by an SA established at each peer, and these IKE SAs apply to all subsequent IKE traffic during the negotiation. The TOE supports both IKEv1 and IKEv2 session establishment. As part of this support, the TOE can be configured to not support aggressive mode for IKEv1 exchanges and to only use main mode using the 'crypto isakmp aggressive-mode disable' command. The TOE 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

TOE SFRs	How the SFR is Met
	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 IKEv1 payloads and IKEv2. The administrator is instructed in the AGD to ensure that the size of key used for ESP must be greater than or equal to the key size used to protect the IKE payload. The TOE supports Diffie-Hellman Group 14 (2048-bit keys), 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: 320 (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 IKEv1 and 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 320 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. IPsec provides secure tunnels between two peers, such as two switches and remote VPN clients. 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 or between the TOE and remote VPN client. 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. 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. 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 ipsecisakmp, IPsec is triggered. 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, but 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. The TOE implementation of the IPsec standard (in accordance with the RFCs noted in the SFR and using cryptographic algorithms AES-CBC-128 and AES-CBC-256 together with HMAC-SHA1, HMAC-SHA-256, and HMAC-SHA-512) uses the Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services.

TOE SFRs	How the SFR is Met
	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 adheres 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_MACSEC_EXT.1	The TOE implements MACsec in compliance with IEEE Standard 802.1AE-2006. The MACsec connections maintain confidentiality of transmitted data and takes measures against frames transmitted or modified by unauthorized devices. In addition, the TOE implementation provides configuration options and management of the MACsec functionality, The SCI is composed of a globally unique 48-bit MAC Address and the Secure System Address (port). The SCI is part of the SecTAG if the SC bit is set and will be at the end of the tag. Any MPDUs during a given session that contain an SCI other than the one used to establish that session is rejected. Only EAPOL (PAE EtherType 88-8E) and MACsec frames (EtherType 88-E5) are permitted and others are rejected.
FCS_MACSEC_EXT.2	The TOE implements the MACsec requirement for integrity protection with the confidentiality offsets of 0, 30 and 50 through the CLI command of “mka-policy confidentiality-offset command”. An offset value of 0 does not offset the encryption and offset values of 30 and 50 offset the encryption by 30 and 50 characters respectively. An Integrity Check Value (ICV) derived with the Secure Association Key (SAK) is used to provide assurance of the integrity of MPDUs. The TOE derives the ICV from a CAK using KDF, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV.
FCS_MACSEC_EXT.3	Each SAK is generated using the KDF specified in SP800-108 (KDF Validation System), clause 6.2.1 using the following transform - KS-nonce = a nonce of the same size as the required SAK, obtained from an RNG each time an SAK is generated. The CAK is based on AES cipher in CMAC mode, with key sizes of 128 and 256 bits. Each of the keys used by MKA is derived from the CAK. The key string is the CAK that is used for ICV validation by the MKA protocol. The CAK is not used directly, but derives two further keys from the CAK using the AES cipher in CMAC mode. The derived keys, which are derived via key derivation function as defined in SP800-108 KDF (CMAC) are tied to the identity of the CAK, and thus restricted to use with that

TOE SFRs	How the SFR is Met
	particular CAK. These are the ICV Key (ICK) used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, and the Key Encrypting Key (KEK) used by the Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a CA. The size of the key is based on the configured AES key sized used. If using AES 128-bit CMAC mode encryption, the key string will be 32-bit hexadecimal in length. If using 256-bit encryption, the key string will be 64-bit hexadecimal in length. The TOE's random bit generator is used for creating these unique nonces.
FCS_MACSEC_EXT.4	MACsec peer authentication is achieved by only using pre-shared keys. The SAKs are distributed between these peers using AES Key Wrap. Prior to distribution of the SAKs between these peers, the TOE uses AES Key Wrap GCM with a key size of 128 or 256 bits in accordance with AES as specified in ISO 18033-3, AES Key Wrap in CMAC mode as specified in NIST SP 800-38F, and GCM as specified in ISO 19772. The "Key-chain macsec lifetime" key configuration command is used to specify the lifetime for CAKs. The "MACSEC Key-chain key" configuration command is used to specify the length of the CKN that is allowed to be between 1 and 32 octets.
FCS_MKA_EXT.1	The TOE implements Key Agreement Protocol (MKA) in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014. The data delay protection is enabled for MKA as a protection guard against an attack on the configuration protocols that MACsec is designed to protect by alternately delaying and delivering their PDUs. The Delay protection does not operate if and when MKA operation is suspended. An MKA Lifetime Timeout limit of 6.0 seconds and Hello Timeout limit of 0.5 seconds is enforced by the TOE. The TOE discards MKPDUs that do not satisfy the requirements listed under FCS_MKA_EXT.1.8 in Section 5.2.2.15. All valid MKPDUs that meet the requirements as defined under FCS_MKA_EXT.1.8 are decoded in a manner conformant to IEEE 802.1x-2010 Section 11.11.4. On successful peer authentication, a connectivity association is formed between the peers and a secure Connectivity Association Key Name (CKN) is exchanged. After the exchange, the MKA ICV is validated with a Connectivity Association Key (CAK), which is effectively a secret key. For the Data Integrity Check, MACsec uses MKA to generate an Integrity Check Value (ICV) for the frame arriving on the port. If the generated ICV is the same as the ICV in the frame, then the frame is accepted; otherwise it is dropped. The key string is the Connectivity Association Key (CAK) that is used for ICV validation by the MKA protocol.
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;

TOE SFRs	How the SFR is Met
	• 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 public key algorithms for authentication; • Password-based authentication; • Enforcement to only allow the hashing algorithms hmac-sha1 and hmac-sha1-96 to ensure the integrity of the session and • Enforcement of DH Group 14 (diffie-hellman-group-14-sha1) as defined by the NDcPPv2.0e. 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.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90 seeded 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.
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.
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 is settable by the Authorized Administrator, and can be configured for minimum password lengths of 15 characters.
FIA_PSK_EXT.1	The TOE supports use of pre-shared keys for MACsec key agreement protocols as defined by IEEE 802.1X. The pre-shared keys are not generated by the TOE, though the TOE accepts the keys in the form of HEX strings. This is done via the CLI configuration command – "key chain test_key macsec" The pre-shared keys for IPsec, the keys can be configured using the 'crypto isakmp key' key command and may be proposed by each of the peers negotiating the IKE establishment.
FIA_UIA_EXT.1 and 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

TOE SFRs	How the SFR is Met
	allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE provides a local password based authentication mechanism as well as RADIUS AAA server for remote authentication. The administrator authentication policies include authentication to the local user database or redirection to a remote authentication server. Interfaces can be configured to try one or more remote authentication servers, and then fail back to the local user database if the remote authentication servers are inaccessible. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console or remotely via SSHv2 secured connection. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE displays only '*' characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
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 an OCSP server and/or 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). • 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.

TOE SFRs	How the SFR is Met
	For OCSP, the OCSP server provides real-time certificate status checking. The OCSP server validation is based on the root CA certificate or a valid subordinate CA certificate. All of 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, USB flash, or USB token. 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 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.

TOE SFRs	How the SFR is Met
	USB tokens provide for secure configuration distribution of the digital certificates and private keys. RSA operations such as on-token key generation, signing, and authentication, and the storage of Virtual Private Network (VPN) credentials for deployment can be implemented using the USB tokens. The use of CRL and OCSP 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, though OCSP may also be used. 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. • ocsp --Certificate checking is performed by an OCSP server There is also an option of 'none', where certificate checking is ignored, however this cannot be selected in the evaluated configuration. 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 administrator is able to choose whether or not to accept the certificate.

TOE SFRs	How the SFR is Met
FMT_MOF.1/Services FMT_MOF.1/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. 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.
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;

TOE SFRs	How the SFR is Met
	• 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 unlocked; • 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 and the remote authentication server; • The ability to import the X.509v3 certificates and validate for use in authentication and secure connections; • The ability to manage the Key Server and associated MKA participants and • The ability to generate a PSK and in the install in the CAK cache • The ability to specify the lifetime of a CAK and to enable, disable or delete a PSK in the CAK cache of a device • The ability to configure and set the time clock. • The ability to configure the reference identifiers for peers, which can be IP address, FQDN identifier or can be the same as the peer's name.
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 authentication via SSHv2 secure connection.
FPT_CAK_EXT.1	During the setup and configuration of the TOE and the MACsec functionality, the Authorized Administrator issues the command – "service password –encryption. This prevents the CAK value to be shown in clear text to the administrators on the CLI when the "show run" output is displayed.

TOE SFRs	How the SFR is Met
	In addition, CAK data is stored in secure directory that is not readily accessible to administrators.
FPT_FLS.1.1(2)/SelfTest	Whenever a failure occurs (power-on self-tests, integrity check of the TSF executable image and/or the noise source health-tests) within the TOE that results in the TOE ceasing operation, the TOE securely disables its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads. So long as the failures persist, the TOE will continue to reload in an attempt to correct the failure. This functionally prevents any failure from causing an unauthorized information flow. There are no failures that circumvent this protection. If the rebooting continues, the Administrator should contact Cisco TAC as described in the Cisco Catalyst 3650 and 3850 Series Switches running IOS 16.12 Common Criteria Operational User Guidance And Preparative Procedures for assistance.
FPT_RPL.1	Replayed data is discarded by the TOE and the attempt to replay data is logged. MPDUs are also replay protected in the TOE. The MKA frames are guarded against replay such as if a MKPDU with duplicate MN (member number) and not latest MN, then this MKPDU will be dropped and not processed further. Also, the attempt to replay data is logged.
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.
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 is 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. When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The TOE image updates can be downloaded from Cisco.com website. The TOE image files include a published hash so their integrity can be verified after the files are download onto a trusted system. An image that fails an integrity check should not be loaded on the TOE. The TOE will automatically display the hash verification on boot or by using the reload command. The successful hash verification message will display on

TOE SFRs	How the SFR is Met
	the successful verification of the boot image. If the image was tampered with in any way, an error would display, and the image will not boot. Once the image is loaded into bootflash, to display information related to software authenticity for a specific image file, use the verify command. For example: <3650># verify <image name> FileName: cat3k_caa-universalk9.16.12.01.SPA.bin / CAT3850/3650 UNIVERSAL SHA512 Checksum: 5800720c79f217e150e50397006f199c…...… The image name and hash can be verified on the [TOE] download page on Cisco.com (https://software.cisco.com/download/home/284846001/type/282046477/release/Gibraltar-16.12.1) 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 Switch# show software authenticity running (displays software authenticity-related information for the current ROMmon and the Cisco IOS image file used for booting) Switch# show software authenticity file {flash0:*filename* | flash1:*filename* | flash:*filename* | nvram:*filename* | usbflash0:*filename* | usbflash1:*filename*} (displays software authenticity-related information for a specific image file.) For full details, refer to the Cisco Catalyst 3650 and 3850 Series Switches running IOS 16.12 Common Criteria Operational User Guidance And Preparative Procedures for assistance.
FPT_TST_EXT.1	The TOE runs a suite of self-tests during initial start-up to verify its correct operation. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. For testing of the TSF, the TOE automatically runs checks and tests at startup and during resets to ensure the TOE is operating correctly, including checks of image integrity and all cryptographic functionality. During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). In the event of a power-on self-test failure, the cryptographic module will force the IOS-XE 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: • Software Integrity Test - The firmware integrity test ensures the correct operation of the device and its components

TOE SFRs	How the SFR is Met
	• 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. • 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. • 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. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen and saved in the crashinfo file. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. 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. The integrity of stored TSF executable code when it is loaded for execution can be verified through the use of digital signature.
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 establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require 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.
FTA_SSL.4	An Authorized Administrator is able to exit out of both local and remote administrative sessions by issuing the ‘exit’ command.

TOE SFRs	How the SFR is Met
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 and remote authentication servers with IPsec. This protects the data from disclosure by encryption and by checksums that verify that data has not been modified. 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/SigGen. 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. MACsec is also used to secure communication channels between MACsec peers at Layer 2. 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 zeroizes all secrets, keys and associated values when they are no longer required. The process in which the TOE zeroizes, meets FIPS 140 validation.

Table 22: 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 DRAM.	Zeroized using the following command: # no crypto isakmp key Overwritten with: 0x0d
IKE RSA Private Key	The RSA private-public key pair is created by the device itself using the key generation CLI described below. 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	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x0d

Name	Description	Zeroization
	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.	
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
MACsec Security Association Key (SAK)	The SAK is used to secure the control plane traffic. This key is stored in internal ASIC register.	Automatically when MACsec session terminated. Overwritten with: 0x00.
MACsec Connectivity Association Key (CAK)	The CAK secures the control plane traffic. This key is stored in internal ASIC register.	Automatically when MACsec session terminated. Overwritten with: 0x00.
MACsec Key Encryption Key (KEK)	The Key Encrypting Key (KEK) is used by Key Server, elected by MKA, to transport a succession of SAKs, for use by MACsec, to the other member(s) of a Secure Connectivity Association (CA). This key is stored in internal ASIC register.	Automatically when MACsec session terminated. Overwritten with: 0x00.
MACsec Integrity Check Key (ICK)	The ICK is used to verify the integrity of MPDUs and to prove that the transmitter of the MKPDU possesses the CAK, this key is stored in internal ASIC register.	Automatically when MACsec session terminated. Overwritten with: 0x00.
RADIUS secret	Shared secret used as part of the Radius authentication method. The password is stored in NVRAM.	Zeroized using the following command: # no radius-server key Overwritten with: 0x0d

Name	Description	Zeroization
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 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
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: REFERENCES

The following documentation was used to prepare this ST:

Table 23: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 4, dated: September 2012
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 4, dated: September 2012
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 4, dated: September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Version 3.1, Revision 4, dated: September 2012
[NDcPP]	collaborative Protection Profile for Network Devices + Errata 20180314, Version 2.0e, 14 March 2018
[MACsec EP]	Network Device Collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption (MACsec EP), Version 1.2, 10 May 2016
[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 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[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