Cisco Catalyst 9200/9200L Series Switches 17.12

Security Target

Version: 0.7
Date: July 16, 2024

Table of Contents

Table of Tables

Table of Figures

Document Introduction

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Catalyst 9200/9200L Series Switches 17.12. 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.

Revision History

Version	Date	Change
0.1	October 4, 2023	Initial Version
0.2	October 12, 2023	Updates to revert to IPsec
0.3	November 27, 2023	Updates to add CSfC requirements
0.4	March 14, 2024	Updates to address CCTL comments
0.5	April 4, 2024	Updates to address Check-In Comments
0.6	July 1, 2024	Updates to address Check-Out Comments
0.7	July 16, 2024	Updates to address Check-Out Comments

1. Security Target Introduction

This Security Target contains the following sections:

- Security Target Introduction
- Conformance Claims
- Security Problem Definition
- Security Objectives
- Security Requirements
- TOE Summary Specification
- References

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 1. ST and TOE Identification

Name	Description
ST Title	Cisco Catalyst 9200/9200L Series Switches 17.12 Security Target
ST Version	0.7
Publication Date	July 16, 2024
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Catalyst 9200/9200L Series Switches 17.12
TOE Hardware Models	Catalyst 9200 and Catalyst 9200L Series Switches
TOE Software Version	IOS-XE 17.12.03
Keywords	Audit, Authentication, Encryption, MACsec, Network Device, Secure Administration

1.2. TOE Overview

The Cisco Catalyst 9200/9200L Series Switches 17.12 TOE is an enterprise access-layer switch for branch office deployments. Switches are used to connect multiple devices, such as computers, wireless access points, printers, and servers; on the same network within a building or campus. A switch enables connected devices to share information and talk to each other and are key building blocks for any network.

1.3.TOE Product Type

The Cisco Catalyst 9200/9200L Series Switches 17.12 TOE is a layer 2 and 3 network device comprised of both hardware and software. The hardware is the Catalyst 9200 and Catalyst 9200L switches as described below in Table 3 of section 1.7.

1.4.Required non-TOE Hardware/Software/Firmware

The TOE requires the following hardware/software/firmware in the IT environment when the TOE is configured in its evaluated configuration.

Table 2. Required IT Environment Components

Component	Usage/Purpose/Description
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.
Syslog Server	This includes any syslog server to which the TOE would transmit syslog messages over IPsec.
Certificate Authority	The Certification Authority is used to provide the TOE with valid certificates. The CA also provides the TOE with a method to check the peer certificate revocation status of devices the TOE communicates with.
Management Workstation	This includes any IT Environment Management workstation with a TLS web browser client or SSH client installed that is used by the Security Administrator for remote administration over SSH trusted paths.
Local Console	This includes any IT Environment Console that is directly connected to the TOE component via the console port and is used by the Security Administrator for local TOE administration.

1.5.TOE Description

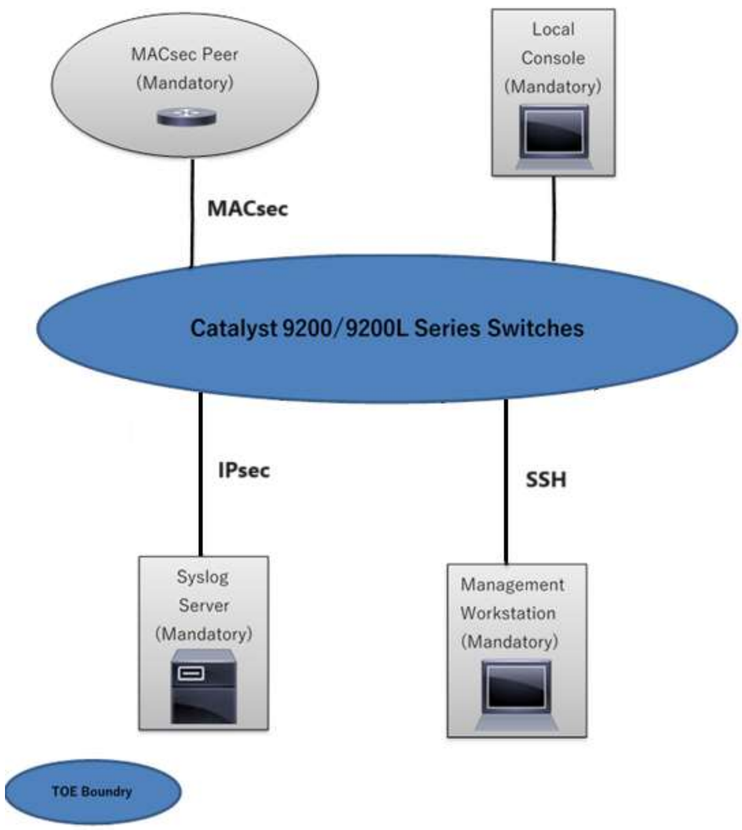
The Cisco Catalyst 9200/9200L Series Switches 17.12 Target of Evaluation (TOE) is a purpose-built, switching and routing platform enabling connected devices to communicate over a network at layer 2 or 3. The TOE provides Administrative control and management of the network. For communicating with other network devices, the TOE provides AES-128 MACsec encryption. The TOE also provides Layer 3 capabilities, including OSPF, EIGRP, ISIS, RIP, and routed access.

1.6. TOE Evaluated Configuration

Deployment of the TOE in its evaluated configuration consists of at least one TOE switch model following the CC installation and configuration guidance document (AGD). 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.

A typical deployment with a single instance of the TOE is depicted in in figure 1 below.

Figure 1. TOE and Environment



The TOE can be administered interactively using a CLI over a local console connection or remotely over SSH.

The operational environment of the TOE will include at least one MACsec peer. The environment will also include an audit (syslog) server and a Management Workstation. The syslog server is used to store audit records, where the TOE uses IPsec to secure the transmission of the records.

1.7. Physical Scope of the TOE

The Cisco Catalyst 9200 and Catalyst 9200L Series Switches TOE is composed of hardware and software with the following specifications:

Table 3. Hardware Models and Specifications

Hardware Model	Picture	Specifications
9200 models: C9200-24T C9200-48T C9200-24P C9200-48P C9200-48PL C9200-24PB C9200-48P C9200-24PXG C9200-48PXG ***With the following network modules:*** C9200-NM-4G C9200-NM-4X C9200-NM-2Y C9200-NM-2Q		**ASIC**: Cisco UADP 2.0 **Processor**: Xilinx ZU3EG (ARM Cortex-A53) **Modular Uplinks** **Ports**: 24 or 48 **Management Ports:** ■ Ethernet management port: RJ-45 connectors, 4-pair Cat 5 UTP cabling ■ Management console port: RJ45 or mini USB connectors.-RJ-45-to-DB9 cable for PC connections, USB-C adaptor, USB adaptor
9200L models: C9200L-24P-4G C9200L-24P-4X C9200L-24T-4G C9200L-24T-4X C9200L-48P-4G C9200L-48P-4X C9200L-48T-4G C9200L-48T-4X C9200L-48PL-4G C9200L-48PL-4X C9200L-24PXG-2Y C9200L-48PXG-2Y C9200L-24PXG-4X C9200L-48PXG-4X		**ASIC**: Cisco UADP 2.0 **Processor**: Xilinx ZU3EG (ARM Cortex-A53) **Fixed Uplinks** **Ports**: 24 or 48 **Management Ports:** ■ Ethernet management port: RJ-45 connectors, 4-pair Cat 5 UTP cabling ■ Management console port: RJ45 or mini USB connectors.-RJ-45-to-DB9 cable for PC connections, USB-C adaptor, USB adaptor

The TOE includes the **cat9k_lite_iosxe.17.12.03.SPA.bin** software image available for download on Cisco Software Central at https://software.cisco.com/. Customers can use their Cisco Care Online (CCO) or SMART account to download the software in a binary image format.

1.8. Logical Scope of the TOE

The TOE is comprised of several security features including:

- 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 following subsections.

Security Audit

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE) of a suspicious nature.

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The TOE stores audit messages in a circular audit trail configurable by the Security Administrator. All audit logs are transmitted to an external audit server over a trusted channel protected with IPsec.

Cryptographic Support

The TOE provides cryptographic functions to implement SSH, IPsec, and MACsec protocols. The cryptographic algorithm implementation has been validated for CAVP conformance. This includes key generation and random bit generation, key establishment methods, key destruction, and the various types of cryptographic operations to provide AES encryption/decryption, signature verification, hash generation, and keyed hash generation.

The TOE supports MACsec using the proprietary Unified Access Data Plane (UADP) 2.0 Application-Specific Integrated Circuit (ASIC). The MACsec Controller (MSC) v1.0 is embedded within the ASICs that are utilized within Cisco hardware platforms.

SSH and IPsec protocols are implemented using the IOS Common Cryptographic Module (IC2M) version Rel5a. Refer to Table 21 for identification of the relevant CAVP certificates.

Identification and Authentication

The TOE implements three types of authentication to provide a trusted means for Security Administrators and remote servers/endpoints to securely communicate: X.509v3 certificate-based authentication for remote syslog servers, password-based authentication for Security Administrators, and pre-shared keys for MACsec endpoints.

Security Administrators have the ability to compose strong passwords which are stored using a SHA-2 hash. Additionally, the TOE detects and tracks successive unsuccessful remote authentication attempts and will prevent the offending account from making further attempts until a Security Administrator time period has elapsed or until the Administrator manually unblocks the account.

Security Management

The TOE provides secure remote administrative interface and local interface to perform security management functions. This includes ability to configure cryptographic functionality; an access banner containing an advisory notice and consent warning message; a session inactivity timer before session termination as well as an ability to update TOE software.

The TOE provides a Security Administrator role and only the Security Administrator can perform the above security management functions.

Protection of the TSF

The TOE protects critical security data including keys and passwords against tampering by untrusted subjects. The TOE provides reliable timestamps to support monitoring local and remote interactive administrative sessions for inactivity, validating X.509 certificates (to determine if a certificate has expired), and to support accurate audit records.

The TOE provides self-tests to ensure it is operating correctly, including the ability to detect software integrity failures. Additionally, the TOE provides an ability to perform software updates and to verify those software updates are from Cisco Systems, Inc.

TOE Access

The TOE monitors both local and remote admin sessions for inactivity and terminates when a threshold time period is reached. Once a session has been terminated the TOE requires the user to re-authenticate.

The TOE also displays a Security Administrator specified advisory notice and consent warning message prior to initiating identification and authentication for each administrative user.

Trusted Path/Channels

The TOE provides encryption (protection from disclosure and detection of modification) for communication paths between itself and remote endpoints.

In addition, the TOE provides two-way authentication of each endpoint in a cryptographically secure manner, meaning that even if there was a malicious attacker between the two endpoints, any attempt to represent themselves to either endpoint of the communications path as the other communicating party would be detected.

1.9. Excluded Functionality

The functionality listed below is not included in the evaluated configuration.

Table 4. Excluded Functionality and Rationale

Function Excluded	Rationale
Non-FIPS 140-2 mode of operation	The TOE includes FIPS mode of operation. The FIPS modes allows the TOE to use only approved cryptography. FIPS mode of operation must be enabled in order for the TOE to be operating in its evaluated configuration.
HTTP/HTTPS	Remote Management is performed using SSH
SNMP	Remote Management is performed using SSH

These services can be disabled by using the configuration settings as described in section 4.2.18 of the Administrative Guidance Documents (AGD).

Additionally, the TOE includes a number of functions where there are no Security Functional Requirements that apply from the collaborative Protection Profile for Network Devices v2.2e or the PP-Module for MACsec Ethernet Encryption v1.0. The excluded functionality does not affect the TOE's conformance to the claimed Protection Profiles.

2. Conformance Claims

2.1.Common Criteria Conformance Claim

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

2.2.PP Configuration Conformance Claim

The TOE and ST are conformant with the PP Configuration identified in the PP-Configuration column of Table 5.

Table 5. PP Configuration Conformance

PP-Configuration	Component	Version	Date
PP-Configuration for Network Devices and MACsec Ethernet Encryption, 2023-03-29, Version 1.0, (CFG_NDcPP-MACsec_V1.0), which includes the components in the next column	Base-PP: collaborative Protection Profile for Network Devices (CPP_ND_V2.2E)	2.2e	March 23, 2020
	PP-Module: PP-Module for MACsec Ethernet Encryption (MOD_MACsec_V1.0)	1.0	March 2, 2023

This ST applies the following NIAP Technical Decisions:

Table 6. NIAP Technical Decisions

Number	Title	PP	Applicable	Exclusion Rational
TD0800	Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	[NDcPP]	Yes	
TD0792	NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR	[NDcPP]	Yes	
TD0790	NIT Technical Decision: Clarification Required for testing IPv6	[NDcPP]	Yes	
TD0738	NIT Technical Decision for Link to Allowed-With List	[NDcPP]	Yes	
TD0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	[NDcPP]	Yes	
TD0639	NIT Technical Decision for Clarification for NTP MAC Keys	[NDcPP]	Yes	
TD0638	NIT Technical Decision for Key Pair Generation for Authentication	[NDcPP]	Yes	
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	[NDcPP]	No	The TOE does not claim FCS_SSHC_EXT.1
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	[NDcPP]	Yes	
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs	[NDcPP]	Yes	
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	[NDcPP]	Yes	
TD0592	NIT Technical Decision for Local Storage of Audit Records	[NDcPP]	Yes	
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	[NDcPP]	Yes	
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	[NDcPP]	Yes	

Number	Title	PP	Applicable	Exclusion Rational
TD0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	[NDcPP]	Yes	
TD0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	[NDcPP]	Yes	
TD0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1	[NDcPP]	Yes	
TD0570	NiT Technical Decision for Clarification about FIA_AFL.1	[NDcPP]	Yes	
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	[NDcPP]	No	FCS_TLSS_EXT.1 not claimed
TD0564	NiT Technical Decision for Vulnerability Analysis Search Criteria	[NDcPP]	Yes	
TD0563	NiT Technical Decision for Clarification of audit date information	[NDcPP]	Yes	
TD0556	NIT Technical Decision for RFC 5077 question	[NDcPP]	No	FCS_TLSS_EXT.1 not claimed
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	[NDcPP]	No	FCS_TLSS_EXT.1 not claimed
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	[NDcPP]	Yes	
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	[NDcPP]	No	FCS_DTLSC_EXT.1 not claimed
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	[NDcPP]	Yes	
TD0536	NIT Technical Decision for Update Verification Inconsistency	[NDcPP]	Yes	
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	[NDcPP]	No	FCS_NTP_EXT.1 not claimed
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	[NDcPP]	Yes	
TD0817	MACsec Data Delay Protection, Key Agreement, and Conditional Support for Group CAK	[MOD_MACSEC]	Yes	
TD0816	Clarity for MACsec Self Test Failure Response	[MOD_MACSEC]	Yes	
TD0748	Correction to FMT_SMF.1/MACSEC Test 21	[MOD_MACSEC]	Yes	
TD0746	Correction to FPT_RPL.1 Test 25	[MOD_MACSEC]	Yes	
TD0728	Corrections to MACSec PP-Module SD	[MOD_MACSEC]	Yes	
TD0826	Aligning MOD_MACSEC_V1.0 with CPP_ND_V3.0E	[MOD_MACSEC]	No	CPP_ND_V3.0E not claimed

2.3. Protection Profile Conformance Claim Rationale

2.3.1. TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profiles.

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 [NDcPP] and [MOD_MACSEC] for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in [NDcPP] and [MOD_MACSEC] for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.3.3. Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in [NDcPP] and [MOD_MACSEC] for which conformance is claimed verbatim. All concepts covered the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target are identical to the Security Assurance Requirements included in the claimed Protection Profiles.

3. Security Problem Definition

This section identifies the following:

- Assumptions about the TOE's operational 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.
- Threats addressed by the TOE and the IT Environment.
- Organizational Security Policies imposed by an organization on the TOE to address its security needs.

The security problem definition below has been drawn verbatim from [NDcPP] and [MOD_MACSEC].

3.1. Assumptions

Table 7. TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality). If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of Network Devices (e.g., firewall).

A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
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.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.
A.VS_REGULAR_UPDATES (applies to vNDs only)	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATON (applies to vNDs only)	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.

A.VS_CORRECT_CONFIGURATION (applies to vNDs only)	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

3.2. Threats

Table 8. 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.
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 layer 2 link in a way that is not detected by the recipient. Devices on a network may be exposed to attacks that attempt to corrupt or modify data in transit without authorization. If malicious devices are able to modify and replay data that is transmitted over a layer 2 link, then the data contained within the communications may be susceptible to a loss of integrity.
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. A MACsec device may sit on the periphery of a network, which means that it may have an externally-facing interface to a public network. Devices located in the public network may attempt to exercise services located on the internal network that are intended to be accessed only from within the internal network or externally accessible only from specifically authorized devices. If the MACsec device allows unauthorized external devices access to the internal network, these devices on the internal network may be subject to compromise. Similarly, if two MACsec devices are deployed to facilitate end-to-end encryption of traffic that is contained within a single network, an attacker could use an insecure MACsec device as a method to access devices on a specific segment of that network such as an individual LAN.

T.UNTRUSTED_MACSEC_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. A generic network device may be threatened by the use of insecure communications channels to transmit sensitive data. The attack surface of a MACsec device also includes the MACsec trusted channels. Inability to secure communications channels, or failure to do so correctly, would expose user data that is assumed to be secure to the threat of unauthorized disclosure.

3.3. Organizational Security Policies

Table 9. 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 following table identifies the Security Objectives for the TOE. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies. The security objectives below have been drawn verbatim from [NDcPP] and [MOD_MACSEC].

Table 10. Security Objectives for the TOE

Environment Security Objective	TOE Security Objective Definition
O.AUTHENTICATION_MACSEC	To further address the issues associated with unauthorized disclosure of information, a compliant TOE's authentication ability (MKA) will allow a MACsec peer to establish connectivity associations (CAs) with another MACsec peer. MACsec endpoints authenticate each other to ensure they are communicating with an authorized MAC Security Entity (SecY) entity. Addressed by: FCS_MACSEC_EXT.4, FCS_MKA_EXT.1, FIA_PSK_EXT.1, FCS_DEVID_EXT.1 (selection-based), FCS_EAP-TLS_EXT.1 (selection-based)
O.AUTHORIZED_ADMINISTRATION	All network devices are expected to provide services that allow the security functionality of the device to be managed. The MACsec device, as a specific type of network device, has a refined set of management functions to address its specialized behavior. In order to further mitigate the threat of a compromise of its security functionality, the MACsec device prescribes the ability to limit brute-force authentication attempts by enforcing lockout of accounts that experience excessive failures and by limiting access to security-relevant data that administrators do not need to view. Addressed by: FMT_SMF.1/MACSEC, FPT_CAK_EXT.1, FIA_AFL_EXT.1 (optional), FTP_TRP.1/MACSEC (optional), FMT_SNMP_EXT.1 (selection-based)
O.CRYPTOGRAPHIC_FUNCTIONS_MACSEC	To address the issues associated with unauthorized modification and disclosure of information, compliant TOEs will implement cryptographic capabilities. These capabilities are intended to maintain confidentiality and allow for detection and modification of data that is transmitted outside of the TOE. Addressed by: FCS_COP.1/CMAC, FCS_COP.1/MACSEC, FCS_MACSEC_EXT.2, FCS_MACSEC_EXT.3, FTP_ITC.1/MACSEC, FTP_TRP.1/MACSEC (optional), FCS_SNMP_EXT.1 (selection-based)
O.PORT_FILTERING_MACSEC	To further address the issues associated with unauthorized network access, a compliant TOE's port filtering capability will restrict the flow of network traffic through the TOE based on layer 2 frame characteristics and whether or not the traffic represents valid MACsec frames and MACsec Key Agreement Protocol Data Units (MKPDUs). Addressed by: FCS_MACSEC_EXT.1, FIA_PSK_EXT.1, FPT_DDP_EXT.1

O.REPLAY_DETECTION	A MACsec device is expected to help mitigate the threat of MACsec data integrity violations by providing a mechanism to detect and discard replayed traffic for MPDUs. Addressed by: FPT_RPL.1, FPT_RPL_EXT.1 (optional)
O.SYSTEM_MONITORING_MACSEC	To address the issues of administrators being able to monitor the operations of the MACsec device, compliant TOEs will implement the ability to log the flow of Ethernet traffic. Specifically, the TOE will provide the means for administrators to configure rules to 'log' when Ethernet traffic grants or restricts access. As a result, the 'log' will result in informative event logs whenever a match occurs. In addition, the establishment of security CAs is auditable, not only between MACsec devices, but also with MAC Security Key Agreement Entities (KaYs). Addressed by: FAU_GEN.1/MACSEC
O.TSF_INTEGRITY	To mitigate the security risk that the MACsec device may fail during startup, it is required to fail-secure if any self-test failures occur during startup. This ensures that the device will only operate when it is in a known state. Addressed by: FPT_FLS.1

4.2. Security Objectives for the Environment

The following table identifies the Security Objectives for the Environment. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies. The security objectives below have been drawn verbatim from [NDcPP] and [MOD_MACSEC].

Table 11. Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance in a trusted manner. For vNDs, this includes the VS Administrator responsible for configuring the VMs that implement ND functionality. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.

OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING (applies to distributed TOEs only)	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
OE.VM_CONFIG`URATION (applies to vNDs only)	For vNDs, the Security Administrator ensures that the VS and VMs are configured to ▪ reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and ▪ correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualisation features such as cloning, save/restore, suspend/resume, and live migration. If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.

5. Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements in this section are drawn from [CC_PART2], [NDcPP], [MOD_MACSEC], and NIAP Technical Decisions.

5.1. Conventions

[CC_PART1] defines operations on Security Functional Requirements. This document uses the following conventions to identify the operations permitted by [NDcPP], [MOD_MACSEC] and NIAP Technical Decisions.

Table 12. Security Requirement Conventions

Convention	Indication
Assignment	Indicated with *italicized* text
Refinement	Indicated with **bold** text and ~~strikethroughs~~
Selection	Indicated with underlined text
Assignment within a Selection	Indicated with *italicized and underlined* text
Iteration	indicated by adding a string starting with '/' (e.g. 'FCS_COP.1/Hash')

Where operations were completed in the [NDcPP] itself, the formatting used in the [NDcPP] has been retained. Formatting used in [NDcPP] and [MOD_MACSEC] that is inconsistent with the listed conventions has not been retained in the ST.

The TOE Security Functional Requirements are identified in the following table and are described in more detail in the following subsections.

Table 13. Security Functional Requirements

Class Name	Component Identification	Component Name	Drawn From
FAU: Security Audit	FAU_GEN.1	Audit data generation	[NDcPP]
	FAU_GEN.1/MACSEC	Audit Data Generation (MACsec)	[MOD_MACSEC]
	FAU_GEN.2	User Identity Association	[NDcPP]
	FAU_STG_EXT.1	Protected Audit Event Storage	[NDcPP]
FCS: Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation (Refinement)	[NDcPP]
	FCS_CKM.2	Cryptographic Key Establishment	[NDcPP]
	FCS_CKM.4	Cryptographic Key Destruction	[NDcPP]
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)	[NDcPP]
	FCS_COP.1/MACSEC	Cryptographic Operation (MACsec AES Data Encryption/Decryption)	[MOD_MACSEC]
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)	[NDcPP]
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	[NDcPP]
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)	[NDcPP]
	FCS_COP.1/CMAC	Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)	[MOD_MACSEC]
	FCS_IPSEC_EXT.1	IPsec Protocol	[NDcPP]

	FCS_RBG_EXT.1	Random Bit Generation	[NDcPP]
	FCS_MACSEC_EXT.1	MACsec	[MOD_MACSEC]
	FCS_MACSEC_EXT.2	MACsec Integrity and Confidentiality	[MOD_MACSEC]
	FCS_MACSEC_EXT.3	MACsec Randomness	[MOD_MACSEC]
	FCS_MACSEC_EXT.4	MACsec Key Usage	[MOD_MACSEC]
	FCS_MKA_EXT.1	MACsec Key Agreement	[MOD_MACSEC]
	FCS_SSHS_EXT.1	SSH Server Protocol	[NDcPP]
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management	[NDcPP]
	FIA_PMG_EXT.1	Password Management	[NDcPP]
	FIA_PSK_EXT.1	Extended: Pre-Shared Key Composition	[MOD_MACSEC]
	FIA_UIA_EXT.1	User Identification and Authentication	[NDcPP]
	FIA_UAU_EXT.2	Password-based Authentication Mechanism	[NDcPP]
	FIA_UAU.7	Protected Authentication Feedback	[NDcPP]
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation	[NDcPP]
	FIA_X509_EXT.2	X.509 Certificate Authentication	[NDcPP]
	FIA_X509_EXT.3	X.509 Certificate Requests	[NDcPP]
FMT: Security Management	FMT_MOF.1/ManualUpdate	Management of security functions behaviour	[NDcPP]
	FMT_MTD.1/CoreData	Management of TSF Data	[NDcPP]
	FMT_MTD.1/CryptoKeys	Management of TSF Data	[NDcPP]
	FMT_SMF.1	Specification of Management Functions	[NDcPP]
	FMT_SMF.1/MACSEC	Specification of Management Functions (MACsec)	[MOD_MACSEC]
	FMT_SMR.2	Restrictions on Security Roles	[NDcPP]
FPT: Protection of the TSF	FPT_CAK_EXT.1	Protection of CAK Data	[MOD_MACSEC]
	FPT_FLS.1	Failure with Preservation of Secure State	[MOD_MACSEC]

	FPT_RPL.1	Replay Detection	[MOD_MACSEC]
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords	[NDcPP]
	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)	[NDcPP]
	FPT_STM_EXT.1	Reliable Time Stamps	[NDcPP]
	FPT_TST_EXT.1	TSF Testing (Extended)	[NDcPP]
	FPT_TUD_EXT.1	Trusted update	[NDcPP]
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking	[NDcPP]
	FTA_SSL.3	TSF-initiated Termination	[NDcPP]
	FTA_SSL.4	User-initiated Termination	[NDcPP]
	FTA_TAB.1	Default TOE Access Banners	[NDcPP]
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel	[NDcPP]
	FTP_ITC.1/MACSEC	Inter-TSF Trusted Channel (MACsec Communications)	[MOD_MACSEC]
	FTP_TRP.1/Admin	Trusted Path	[NDcPP]

5.2. Class: Security Audit (FAU)

5.2.1. 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 shutdown of the audit functions;

b) All auditable events for the <u>not specified</u> 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).*
- *[<u>Starting and stopping services</u>];*

d) Specifically defined auditable events listed in Table 14.

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 cPP/ST, [*information specified in column three of Table 14*].

Table 14. 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.
FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None.

5.2.2. FAU_GEN.1/MACSEC – Audit Data Generation (MACsec)

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [*not specified*] level of audit;

c) All administrative actions;

d) [Specifically defined auditable events listed in the Auditable Events table (Table 15)]

Table 15. MACsec Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)
FCS_MACSEC_EXT.3	Creation and update of SAK	Creation and update times
FCS_MACSEC_EXT.4	Creation of CA	Connectivity Association Key Names (CKNs)
FPT_RPL.1	Detected replay attempt	None.

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

a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP-Module/ST, [information specified in column three of the Auditable Events table (Table 15)].

5.2.3. FAU_GEN.2 – User Identity Association

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

5.2.4. FAU_STG_EXT.1 – Protected Audit Event Storage

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

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

- <u>The TOE shall consist of a single standalone component that stores audit data locally</u>].

FAU_STG_EXT.1.3 The TSF shall [<u>*overwrite previous audit records according to the following rule:* [*oldest audit records are overwritten*]</u>] when the local storage space for audit data is full.

5.3. Class: Cryptographic Support (FCS)

5.3.1. FCS_CKM.1 – Cryptographic Key Generation (Refinement)

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

- <u>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</u>;

- <u>ECC schemes using ‘NIST curves’ [P-256, P-384] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4.</u>

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

5.3.2. FCS_CKM.2 – Cryptographic Key Establishment (Refinement)

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

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

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

5.3.3. 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, a new value of the key]]*;*
- *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, a new value of the key]]*;*

  that meets the following: *No Standard.*

5.3.4. 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].

5.3.5. FCS_COP.1/MACSEC – Cryptographic Operation (MACsec AES Data Encryption/Decryption)

FCS_COP.1.1/MACSEC The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES used in AES Key Wrap, GCM*] and cryptographic key sizes [128] bits that meets 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*].

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

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

[

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [*2048 bits, 3072 bits*],

]

that meet the following:

[

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

].

5.3.7. FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)

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

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

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

5.3.9. FCS_COP.1/CMAC – Cryptographic Operation (AES-CMAC Keyed Hash Algorithm)

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

5.3.10. 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 [tunnel mode, transport mode].

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP[1] as defined by RFC 4303 using the cryptographic algorithms [AES-CBC-128 (RFC3602), AES-CBC-256 (RFC3602), AES-GCM-128 (RFC 4106), AES-GCM-256 (RFC 4106)] together with a Secure Hash Algorithm (SHA)-based HMAC [HMAC-SHA-256, no HMAC algorithm].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

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

].

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

FCS_IPSEC_EXT.1.7 The TSF shall ensure that [

- IKEv2 SA lifetimes can be configured by a Security Administrator based on
[
  - length of time, where the time values can be configured within [*2 minutes to 24*] hours

  ]

].

FCS_IPSEC_EXT.1.8 The TSF shall ensure that [

- IKEv2 Child SA lifetimes can be configured by a Security Administrator based on
[
  - number of bytes
  - length of time, where the time values can be configured within [*2 minutes to 8*] hours;

  ]

[1] ESP – Encapsulating Security Protocol

].

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 [*128 (for DH Group 19), 192 (for DH Group 20)*] bits.

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

- at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash

].

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [[19 (256-bit Random ECP), 20 (384-bit Random ECP)] according to RFC 5114.

].

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

FCS_IPSEC_EXT.1.13 The TSF shall ensure that all IKE protocols perform peer authentication using [RSA] that use X.509v3 certificates that conform to RFC 4945 and [no other method].

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

5.3.11. FCS_RBG_EXT.1 – Random Bit Generation

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

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

5.3.12. FCS_MACSEC_EXT.1 – MACsec

FCS_MACSEC_EXT.1.1 The TSF shall implement MACsec in accordance with IEEE Standard 802.1AE-2018.

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 an 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 (Port Access Entity (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC control frames (EtherType is 88-08) and shall discard others.

5.3.13. 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 SAK.

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

5.3.14. 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 nonces for the derivation of SAKs using the TOE's random bit generator as specified by FCS_RBG_EXT.1.

5.3.15. FCS_MACSEC_EXT.4 – MACsec Key Usage

FCS_MACSEC_EXT.4.1 The TSF shall support peer authentication using pre-shared keys (PSKs) [no other method].

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

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 SAKs that are defined by the KDF using the CAK as input data (per IEEE 802.1X-2010, Section 9.8.1).

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

5.3.16. 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 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.1.3 The TSF shall provide the ability to derive an Integrity Check Value Key (ICK) from a CAK using a KDF.

FCS_MKA_EXT.1.4 The TSF shall enforce an MKA Lifetime Timeout limit of 6.0 seconds and [MKA Bounded Hello Timeout limit of 0.5 seconds].

FCS_MKA_EXT.1.5 The key server shall refresh a SAK when it expires. The key server shall distribute a SAK by [

- pairwise CAKS that are PSKs

].

FCS_MKA_EXT.1.6 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.1.7 The TSF shall validate MKPDUs according to IEEE 802.1X-2010 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 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
d. 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-2010 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 IEEE 802.1X-2010 Section 9.4.1 shall be decoded as specified in IEEE 802.1X-2010 Section 11.11.4.

5.3.17. 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, [5656, 6668, 8308 section 3.1, 8332].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following user 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 [*33,038*] 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, aes128-gcm@openssh.com, aes256-gcm@openssh.com].

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

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

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

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

5.4. Class: Identification and Authentication (FIA)

5.4.1. FIA_AFL.1 – Authentication Failure Management

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

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until [*unblocking action*] is taken by an Administrator; prevent the offending Administrator from successfully establishing remote session using any authentication method that involves a password until an Administrator defined time period has elapsed].

5.4.2. FIA_PMG_EXT.1 – Password Management

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

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” [*Additional Special Characters listed in Table 16*]];

Table 16. Additional Password Special Characters

Special Character	Name
	Space
;	Semicolon
:	Colon
"	Double Quote
‘	Single Quote
|	Vertical Bar
+	Plus
-	Minus
=	Equal Sign
.	Period
,	Comma
/	Slash
\	Backslash
<	Less Than
>	Greater Than
_	Underscore
`	Grave accent (backtick)
~	Tilde
{	Left Brace
}	Right Brace

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

5.4.3. FIA_PSK_EXT.1 – Pre-Shared Key Composition

FIA_PSK_EXT.1.1 The TSF shall use PSKs for MKA as defined by IEEE 802.1X-2010, [no other protocols].

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

5.4.4. 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;
- [no other actions]

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

5.4.5. FIA_UAU_EXT.2 – Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local [password-based, SSH public key-based] authentication mechanism to perform local administrative user authentication.

5.4.6. FIA_UAU.7 – Protected Authentication Feedback

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

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

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

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates.**
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
    - Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - 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.

5.4.8. 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 [not accept the certificate].

5.4.9. FIA_X509_EXT.3 – X.509 Certificate Requests

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

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

5.5.Class: Security Management (FMT)

5.5.1. FMT_MOF.1/ManualUpdate – Management of Security Functions Behavior

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

5.5.2. FMT_MTD.1/CoreData – Management of TSF Data

FMT_MTD.1.1/CoreData The TSF shall restrict the ability to *manage* the *TSF data* to *Security Administrators*.

5.5.3. 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*.

5.5.4. 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 [digital signature] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*

  [

  - *Ability to modify the behaviour of the transmission of audit data to an external IT entity;*
  - *Ability to manage the cryptographic keys;*
  - *Ability to configure the cryptographic functionality;*
  - *Ability to configure thresholds for SSH rekeying;*
  - *Ability to configure the lifetime for IPsec SAs;*
  - *Ability to re-enable an Administrator account;*
  - *Ability to set the time which is used for time-stamps;*
  - *Ability to configure the reference identifier for the peer;*
  - *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;*
  - *Ability to import X.509v3 certificates to the TOE's trust store;*
  - *Ability to manage the trusted public keys database*

]

5.5.5. FMT_SMF.1/MACSEC – Specification of Management Functions (MACsec)

FMT_SMF.1.1/MACSEC The TSF shall be capable of performing the following management functions **related to MACsec functionality:** [*Ability of a Security Administrator to:*

- *Manage a PSK-based CAK and install it in the device*
- *Manage the key server to create, delete, and activate MKA participants [as specified in IEEE 802.1X-2020, Sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipant Entry) and section 12.2 (cf. function createMKA()]*
- *Specify the lifetime of a CAK*
- *Enable, disable, or delete a PSK-based CAK using [CLI management commands]*

[

- *Manage generation of a PSK-based CAK*

]].

5.5.6. FMT_SMR.2 – Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator*.

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

are satisfied.

5.6.Class: Protection of the TSF (FPT)

5.6.1. FPT_CAK_EXT.1 Protection of CAK Data

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

5.6.2. FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall **fail-secure** 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].

5.6.3. 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.

5.6.4. FPT_APW_EXT.1 – Protection of Administrator Passwords

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

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

5.6.5. 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.

5.6.6. FPT_STM_EXT.1 – Reliable Time Stamps

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

FPT_STM_EXT.1.2 The TSF shall [allow the Security Administrator to set the time].

5.6.7. FPT_TST_EXT.1 – TSF Testing

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

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

].

5.6.8. 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 means to authenticate firmware/software updates to the TOE using a [digital signature] prior to installing those updates.

5.7. Class: TOE Access (FTA)

5.7.1. 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.

5.7.2. 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*.

5.7.3. FTA_SSL.4 – User-initiated Termination

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

5.7.4. FTA_TAB.1 – Default TOE Access Banners

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

5.8.Class: Trusted Path/Channels (FTP)

5.8.1. FTP_ITC.1 – Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall **be capable of using** [IPsec] **to** provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server,** [***no other capabilities***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from **disclosure and detection of modification of the channel data**.

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [

- *Syslog server over IPsec*

]

5.8.2. FTP_ITC.1/MACSEC – Inter-TSF Trusted Channel (MACsec Communications)

FTP_ITC.1.1/MACSEC The TSF shall provide a communication channel between itself and a MACsec peer that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/MACSEC The TSF shall permit [the TSF, another trusted IT product] to initiate communication via the trusted channel.

FTP_ITC.1.3/MACSEC The TSF shall initiate communication via the trusted channel for [*communications with MACsec peers that require the use of MACsec*].

5.8.3. FTP_TRP.1/Admin – Trusted Path

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

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

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

5.9. TOE SFR Dependencies Rationale

The Security Functional Requirements included in the ST represent all mandatory, optional, and selection-based SFRs specified in [NDcPP] and [MOD_MACSEC] against which exact compliance is claimed.

All dependency rationale in the ST are considered to be identical to those that are defined in the claimed PP.

5.10. TOE SFR Dependencies Rationale

The TOE assurance requirements for this ST are taken directly from the NDcPP which are derived from [CC_PART3]. The assurance requirements are summarized in the table below.

Table 17. Assurance Requirements

Assurance Class	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 procedures
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 survey

5.11. TOE SFR Dependencies Rationale

[NDcPP] and [MOD_MACSEC] contain all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PPs themselves have been approved.

5.12. Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the [NDcPP] and [MOD_MACSEC]. As such, the [NDcPP] and [MOD_MACSEC] SAR rationale is deemed acceptable since the PPs themselves have been approved.

5.13. Assurance Measures

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

Table 18. Assurance Measures

Assurance Component	Rationale

ASE_INT.1 ASE_CCL.1 ASE_OBJ.1 ASE_ECD.1 ASE_REQ.1 ASE_SPD.1 ASE_TSS.1	Cisco provided this Security Target document.
ADV_FSP.1	No additional "functional specification" documentation was provided by Cisco to satisfy the Evaluation Activities.
AGD_OPE.1 AGD_PRE.1	Cisco will provide the guidance documents with the ST.
ALC_CMC.1 ALC_CMS.1	Cisco will identify the TOE such that it can be distinguished from other products or versions from the Cisco and can be easily specified when being procured by an end user.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for Vulnerability Analysis.

6. TOE Summary Specification

The table below identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 19. TSS Rationale

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FAU_GEN.1
FAU_GEN.1/MACSEC</td><td>The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include start-up and shut-down of the audit mechanism cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in Error! Reference source not found. and 15 Error! Reference source not found..

Each of the events is specified in the audit record is in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred such as generating keys, including the key identifier. Additionally, the start-up and shut-down of the audit functionality is audited.

The audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes at least all the required information. Additional information can be configured.</td></tr>
<tr><td>FAU_GEN.2</td><td>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.</td></tr>
<tr><td>FAU_STG_EXT.1</td><td>The TOE is a standalone device configured to export syslog records to a specified, external syslog server in real-time. The TOE protects communications with an external syslog server using 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 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 2,147,483,647 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 can clear the local logs, and local audit records are stored in a directory that does not allow Administrators to modify the contents.</td></tr>
<tr><td>FCS_CKM.1</td><td rowspan="2">The following table describes the key generation algorithms the TOE implements to generate asymmetric keys used for device authentication:

<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/
NIST Curve</th><th>SFR</th><th>Service</th></tr>
<tr><td rowspan="2">RSA</td><td rowspan="2">FIPS PUB 186-4</td><td rowspan="2">2048
3072</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
<tr><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
</table></td></tr>
<tr><td>FCS_CKM.2</td></tr>
</table>

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
With the exception to SSH, the keys are used to generate certificate signing requests (CSRs) in which the public key is associated with an X.509 certificate.
The following table shows the key generation algorithms the TOE implements to generate asymmetric keys used for key establishment:
<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/ NIST Curve</th><th>SFR</th><th>Service</th></tr>
<tr><td rowspan="2">ECC</td><td rowspan="2">FIPS PUB 186-4</td><td>DH Group 19 (P-256)

DH Group 20 (P-384)</td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
<tr><td>P-256
P-384</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
</table>
The following table shows the methods the TOE implements for key establishment:
<table>
<tr><th>Scheme</th><th>Standard</th><th>SFR</th><th>Service</th></tr>
<tr><td rowspan="2">EC-DH</td><td rowspan="2">NIST SP 800-56A Revision 3</td><td>FCS_IPSEC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
<tr><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
</table>
</td></tr>
<tr><td>FCS_CKM.4</td><td>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 section 6.1 Error! Reference source not found. for additional details on key zeroization.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode and GCM mode (128 and 256 bits) as described in ISO/IEC 18033-3, ISO/IEC 10116, and ISO/IEC 19772. AES is implemented in the SSH and IPsec protocols. Refer to Error! Reference source not found.21 for the FIPS validated algorithm certificate numbers.</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE provides cryptographic signature services using a RSA Digital Signature Algorithm with key size of 2048 or 3072 as specified in FIPS PUB 186-4. Refer to Error! Reference source not found.21 for the FIPS validated algorithm certificate numbers.</td></tr>
<tr><td>FCS_COP.1/Hash
FCS_COP.1/KeyedHash</td><td>
The TOE provides cryptographic hashing services using SHA-256 and SHA-512 as specified in ISO/IEC 10118-3:2004 (with key sizes and message digest sizes of 256 and 512 bits respectively).
The TOE provides keyed-hashing message authentication services using HMAC-SHA-256 that operates on 512-bit blocks with key sizes and message digest sizes of 256 bits as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.
SHA-512 hashing is used for verification of software image integrity.
</td></tr>
</table>

TOE SFRs	How the SFR is Met
	Refer to **Error! Reference source not found.**21 for the FIPS validated algorithm certificate numbers.
FCS_COP.1/CMAC FCS_COP.1/MACSEC	The TSF implements keyed-hash message authentication in accordance with AES-CMAC and cryptographic key size of 128 bits with message digest size of 128 bits, block size of 128 bits, and MAC length of 128 bits which meets NIST SP 800-38B. The TSF implements symmetric encryption and decryption capabilities using AES in AES Key Wrap and GCM mode (128 bits) as described in AES as specified in ISO/IEC 18033-3, AES Key Wrap as specified in NIST SP800-38F, GCM as specified in ISO/IEC 19772. AES is implemented in the MACsec protocol. Refer to **Error! Reference source not found.** for the FIPS validated algorithm certificate numbers.
FCS_IPSEC_EXT.1	The TSF implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of syslog authentication data as it travels over the external network. The TSF's implementation of the IPsec standard (in accordance with the RFCs noted in the SFR) uses the Internet Key Exchange version 2 (IKEv2) protocol and the Encapsulating Security Payload (ESP) protocol to provide authentication and encryption supporting the following algorithms: ▪ AES-CBC-128 and AES-CBC-256 with HMAC-SHA-256 ▪ AES-GCM-128 and AES-GCM-256. The TOE supports both transport and tunnel mode for IPsec communications between the TOE and an external audit server. The administrator defines the traffic that needs to be protected between two IPsec peers by configuring access lists and applying these access lists to interfaces using crypto map sets. A crypto map set can contain multiple entries, each with a different access list. The crypto map entries are searched in a sequence--the router attempts to match the packet to the access list specified in that entry. When a packet matches a permit entry in a particular access list, and the corresponding crypto map entry is tagged connections are established, if necessary. If the crypto map entry is tagged as ipsec-isakmp, IPsec is triggered. If there is no SA that the IPsec can use to protect this traffic to the peer, IPsec uses IKE to negotiate with the re-mote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry. Once established, the set of SAs (outbound to the peer) is then applied to the triggering packet and to subsequent applicable packets as those packets exit the Switch. "Applicable" packets are packets that match the same access list criteria that the original packet matched. For example, all applicable packets could be encrypted be-fore being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer. Access lists associated with IPsec crypto map entries also represent the traffic that the Switch needs protected by IPsec. Inbound traffic is processed against crypto map entries. if an unprotected packet matches a permit entry in a particular access list associated with an IPsec crypto

TOE SFRs	How the SFR is Met
	map entry, that packet is dropped because it was not sent as an IPsec-protected packet. The traffic matching the permit ACLs would then flow through the IPsec tunnel and be classified as "PROTECTED". Traffic that does not match a permit ACL in the crypto map, but that is not disallowed by other ACLs on the interface is allowed to BYPASS the tunnel. Traffic that does not match a permit ACL and is also blocked by other non-crypto ACLs on the interface would be DISCARDED. Rules applied to an access control list can be applied to either inbound or outbound traffic. IPsec Internet Key Exchange, also called ISAKMP, is the negotiation protocol that lets two peers agree on how to build an IPsec Security Association (SA). The strength of the symmetric algorithm negotiated to protect the IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv2 CHILD_SA connection. The IKE protocols implement Peer Authentication using RSA X.509v3 certificates or pre-shared keys. IKE separates negotiation into two phases: IKEv2 SA and IKEv2 Child SA. The IKEv2 SA creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated during the IKEv2 SA enables IKE peers to negotiate IKE v2 Child SA and establishes the IPsec SA to communicate securely. 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. The resulting potential strength of the symmetric key will be 128 or 256 bits of security depending on the algorithms negotiated between the two IPsec peers. As part of this negotiation, the TOE verifies that the negotiated IKE Child SA symmetric algorithm key strength is at most as large as the negotiated IKE SA key strength as configured on the TOE and peer via an explicit check. Each IKE negotiation begins by agreement of both peers on a common (shared) IKE policy. This policy states which security parameters will be used to protect subsequent IKE negotiations and mandates how the peers are authenticated. The Security Administrator can configure multiple, prioritized policies on each peer, each with a different combination of parameter values. However, at least one of these policies must contain exactly the same encryption, hash, authentication, and Diffie-Hellman parameter values as one of the policies on the remote peer. For each policy created, the Security Administrator assign's a unique priority (1 through 10,000, with 1 being the highest priority). When the IKE negotiation begins, IKE searches for an IKE policy that is the same on both peers. The peer that initiates the negotiation will send all its policies to the remote peer, and the remote peer will try to find a match. The remote peer looks for a match by comparing its own highest priority policy against the policies received from the other peer. The remote peer checks each of its policies in order of its priority (highest priority first) until a match is found. 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. When a packet is processed by the TOE and it determines it requires IPsec, it uses active SA settings or creates new SAs for initial connections with the IPsec peer.

TOE SFRs	How the SFR is Met
	The TOE supports IKEv2 session establishment. The TOE supports configuration of session lifetimes for both IKEv2 SAs and IKEv2 Child SAs using the following the command "lifetime." The time values for IKEv2 SAs can be limited up to 24 hours and for IKEv2 Child SAs up to 8 hours. The IKEv2 Child SA lifetimes can also be configured by an Administrator based on number of bytes. The TOE supports Diffie-Hellman Group 19 and 20. The TSF generates the secret value 'x' used in the IKEv2 Diffie-Hellman key exchange ('x' in g^x mod p) using the NIST approved DRBG specified in FCS_RBG_EXT.1 and having possible lengths of 256 or 384 bits. The TOE generates nonces used in IKEv2 exchanges, of at least 128 bits in size and at least half the output size of the negotiated pseudorandom function (PRF) hash. 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. The TOE supports authentication of IPsec peers using pre-shared keys and RSA X.509 certificates. The TOE validates the presented identifier provided supporting the following fields and types: SAN: IP address, SAN: Fully Qualified Domain Name (FQDN). Certificate maps provide the ability for a certificate to be matched with a given set of criteria. The Administrator is instructed in the CC Configuration Guide to specify one or more certificate fields together with their matching criteria and the value to match. In the evaluated configuration, the field name must specify the SAN (alt-subject-name) field. Match criteria should be "eq" for equal. SAN example: alt-subject-name eq <peer.cisco.com> The TOE will reject the IKE connection in any of these situations: 1) If the data ID Payload for any of those ID Types does not match the peer's certificate exactly; 2) If an ID Payload is not provided by the peer; 3) If multiple ID Types are provided in the ID Payload.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR DRBG, as specified in ISO/IEC 18031:2011 seeded by an entropy source that accumulates entropy from a TSF-platform- based noise source. The DRBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.
FCS_MACSEC_EXT.1	The TOE implements MACsec in compliance with Institute of Electrical and Electronics Engineers (IEEE) Standard 802.1AE-2018. The MACsec connections maintain confidentiality of transmitted data and takes measures against frames transmitted or modified by unauthorized devices. The Secure Channel Identifier (SCI) is composed of a globally unique 48-bit Message Authentication Code (MAC) Address and the Secure System Address (port). The SCI is part of the SecTAG if the Secure Channel (SC) bit is set and will be at the end of the tag. Any MAC Protocol Data Units (MPDUs) during a given session that contain an SCI other than the one used to establish that session is rejected. Only Extensible Authentication Protocol over LAN (EAPOL) (Physical Address Extension (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC control frames (EtherType 88-08) are permitted. All others are rejected.

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td>FCS_MACSEC_EXT.2</td><td>The TOE implements the MACsec requirement for integrity protection with the confidentiality offsets of 0, 30 and 50 using the ‘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) of 16-bytes derived with the SAK is used to provide assurance of the integrity of MPDUs.

The TOE derives the ICK from a CAK using KDF, using the SCI as the most significant bits of the Initialization Vector (IV) and the 32 least significant bits of the PN as the IV.</td></tr>
<tr><td>FCS_MACSEC_EXT.3</td><td>Each SAK is generated using the KDF specified in IEEE 802.1X-2010 section 6.2.1 using the following transform - KS-nonce = a nonce of the same size as the required SAK, obtained from a Random Number Generator (RNG) each time an SAK is generated.

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 are tied to the identity of the CAK, and thus restricted to use with that 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 key size is 32-bit hexadecimal in length for AES 128-bit CMAC mode encryption.</td></tr>
<tr><td>FCS_MACSEC_EXT.4</td><td>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 in accordance with AES as specified in ISO/IEC 18033-3, AES in CMAC mode as specified in NIST SP800-38B, and GCM as specified in ISO/IEC 19772.</td></tr>
<tr><td>FCS_MKA_EXT.1</td><td>The TOE implements the MKA Protocol 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 MPDUs. The “Delay Protection” does not operate if MKA operation is suspended. An MKA Lifetime Timeout limit of 6.0 seconds and Hello Timeout limit of 2.0 seconds is enforced by the TOE.

The TOE discards MACsec Key Agreement Protocol Data Units (MKPDUs) that do not satisfy the requirements listed under FCS_MKA_EXT.1.7. All valid MKPDUs that meet the requirements as defined under FCS_MKA_EXT.1.7 are decoded in a manner conformant to IEEE 802.1x-2010 Section 11.11.4.

On successful peer authentication, a unique 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. The TOE does not support group CAKs.

For the Data Integrity Check, MACsec uses MKA to generate an 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;</td></tr>
</table>

TOE SFRs	How the SFR is Met
	otherwise, it is dropped. The key string is the CAK that is used for ICV validation by the MKA protocol.
FCS_SSHS_EXT.1	The TSF implements SSHv2 conformant to RFCs 4251, 4252, 4253, 4254, 5656, 6668, 8308 section 3, and 8332 to provide a secure command line interface for remote administration. The TOE uses rsa-sha2-512 and rsa-sha2-256 for host key authentication and uses ssh-rsa for client or user password-based authentication. SSHv2 connections will be dropped if the TOE receives a packet larger than 33,038 bytes. Large packets are detected by the SSHv2 implementation and dropped internal to the SSH process. The TSF's SSH transport implementation supports the following encryption algorithms when aes128-cbc or aes-256-cbc is used: ■ aes128-cbc ■ aes256-cbc ■ aes128-gcm@openssh.com ■ aes256-gcm@openssh.com When aes128-gcm@openssh.com or aes256-gcm@openssh.com is used as the encryption algorithm the MAC algorithm is implicit. All connection attempts from remote SSH clients requesting any other encryption algorithm is denied. The TSF's SSH transport implementation supports the following MAC algorithms: ■ hmac-sha2-256 All connection attempts from remote SSH clients requesting any other MAC algorithm is denied. The TSF's SSH transport implementation supports the following public-key algorithms for Hostkey authentication: ■ rsa-sha2-256 ■ rsa-sha2-512 The TSF's SSH transport implementation supports the following public-key algorithms for Client Authentication: ■ ssh-rsa The public-key algorithm is consistent with the RSA digital signature algorithm in FCS_COP.1/SigGen. When the SSH client presents a public key, the TSF verifies it matches the one configured for the Administrator account. If the presented public key does not match the one configured for the Administrator account, access is denied. The TSF's SSH key exchange implementation supports the following key exchange algorithm: ■ ecdh-sha2-nistp256 ■ ecdh-sha2-nistp384

TOE SFRs	How the SFR is Met
	The TSF's SSH implementation will perform a rekey after no longer than one hour or more than one gigabyte of data has been transmitted with the same session key. Both thresholds are checked. Rekeying is performed upon reaching whichever threshold is met first. The Administrator can configure lower rekey values if desired. The minimum time value is 10 minutes. The minimum volume value is 100 kilobytes.
FIA_AFL.1	To block password-based brute force attacks, the TOE uses an internal AAA function to detect and track failed login attempts. When an account attempting to log into an administrative interface reaches the set maximum number of failed authentication attempts, the account will not be granted access until the time period has elapsed or until the Administrator manually unblocks the account. The TOE provides the Administrator the ability to specify the maximum number of unsuccessful authentication attempts before an offending account will be blocked. The TOE also provides the ability to specify the time period to block offending accounts. To avoid a potential situation where password failures made by Administrators leads to no Administrator access until the defined blocking time period has elapsed, the CC Configuration Guide instructs the Administrator to configure the TOE for SSH public key authentication which is not subjected to password-based brute force attacks. During the block out period, the TOE provides the ability for the Administrator account to login remotely using SSH public key authentication.
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 other special characters listed in table 16. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 1 and maximum of 127 characters. A minimum password length of 8 is recommended.
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, but 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 TOE accepts pre-shared keys that are 32 characters in length.
FIA_UIA_EXT.1 FIA_UAU_EXT.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed. Prior to being granted access, a login warning banner is displayed. Administrative access to the TOE is facilitated through a local password-based authentication and SSH public key authentication mechanisms on the TOE through which all Administrator actions are mediated. Once a potential (unauthenticated) administrative user attempts to access the TOE through an interactive administrative interface, the TOE prompts the user for a user name and password or SSH public key authentication. No access is allowed to the administrative functionality of the TOE until the administrator is successfully identified and authenticated 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 grants administrative access (if the combination of username and password is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE does not echo any characters as the password is entered. For remote session authentication, the TOE does not echo any characters as they are entered.
FIA_X509_EXT.1/Rev	The TOE uses X.509v3 certificates to support authentication for IPsec connections. The TSF determines the validity of certificates by ensuring that the certificate and the certificate path are valid in accordance with RFC 5280. The certificate path is validated by ensuring that all the CA

TOE SFRs	How the SFR is Met
	certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate. CRL revocation checking is supported by the TOE. Revocation checking is performed on the leaf and intermediate certificate(s) when authenticating a certificate chain provided by the remote peer. There are no functional differences if a full certificate chain or only a leaf certificate is presented.
FIA_X509_EXT.2	The TOE determines which certificate to use based upon the trustpoint configured. The instructions for configuring trustpoints is provided in CC Configuration Guide. In the event that a network connection cannot be established to verify the revocation status of certificate for an external peer, the certificate will be rejected and the connection will not be established.
FIA_X509_EXT.3	A Certificate Request Message can be generated as specified by RFC 2986 and provide the following information in the request – Common Name(CN), Organization(O), Organizational Unit(OU), and Country(C). The TOE can validate the chain of certificates from the Root CA when the CA Certificate Response is received.
FMT_MOF.1/ManualUpdate FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys	The TOE provides the ability for Security Administrators to access TOE data, such as audit data, configuration data, security attributes, routing tables, and session thresholds and to perform manual updates to the TOE. Only Security Administrators can access the TOE's trust store. Each of the predefined and administratively configured roles has create (set), query, modify, or delete access to the TOE data, though with some privilege levels, the access is limited. 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 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 customizable. The term "Authorized Administrator" is used in this ST to refer to any user that 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 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 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 levels has a set of permissions that will grant 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 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, the Authorized Administrators can obtain, verify the integrity of, and install those updates. The Authorized Administrator generates RSA key pairs to be used in the IPsec and SSH protocols. Zeroization of these keys is provided in **Error! Reference source not found.**20 **Error! Reference source not found.**. Prior to authentication the TOE may be configured by the Administrator to display a customized login banner, which describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. No administrative functionality is available prior to administrative login. TOE Administrators can control (generate/delete) the following keys, RSA Key Pairs and SSH RSA Key Pairs by following the instruction in the AGD.

TOE SFRs	How the SFR is Met
FMT_SMF.1 FMT_SMF.1/MACSEC	The TOE provides all capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The Authorized Administrator can perform all management functions by accessing the TOE directly via connected console cable or remote administration via SSHv2 secure connection. 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 • 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 set and modify the time limits of session inactivity • The ability to configure the number of failed Administrator logon attempts that will cause the account to be locked until a specified time period has elapsed. • The ability to update the IOS-XE software. The validity of the image is provided using a digital signature prior to installing the update • The ability to modify the behavior of the transmission of audit data to an external IT entity. • The ability to manage cryptographic keys • 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 • Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchor • Ability to configure thresholds for SSH rekeying • Ability to configure the lifetime for IPsec SAs • Ability to re-enable an Administrator account • The ability to manage the trusted public keys database • The ability to manage the Key Server and associated MKA participants • The ability to generate a PSK and install in the CAK cache • The ability to initiate the generation of a new CAK from the Key Server • 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 • Ability to import X.509v3 certificates to the TOE's trust store
FMT_SMR.2	The TOE maintains privileged and semi-privileged Administrator roles. The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to TOE functions. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for IOS-XE privilege level (PL) 15. Semi-privileged roles are assigned a PL of 0 – 14. PL 0 and 1 are defined by default and are customizable, while PL 2-14 are undefined by default and are also customizable. Note: Levels 0 – 14 are a subset of PL 15 and the levels are not 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.

TOE SFRs	How the SFR is Met
	The TOE can and shall be configured to authenticate all access to the command line interface using a username and password. The TOE supports both local administration via a directly connected console cable and remote administration via SSHv2 secure connection.
FPT_CAK_EXT.1	A CAK value is specified in the configuration file by the Administrator using a bit-based (hex) format. The interface specifically implemented in the TSF for viewing the configuration file is the "show running-config" or "show startup-config "CLI commands. When the TOE is operating in the evaluated configuration, and the Administrator executes the "show running-config" or "show startup-config" CLI commands, the CAK data will not be displayed. This protects the CAK data from unauthorized disclosure.
FPT_FLS.1.	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 will attain a secure/safe state by disabling its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads. If 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 Authorized Administrator must contact Cisco Technical Assistance Center (TAC).
FPT_RPL.1	Replayed data is discarded by the TOE and the attempt to replay data is logged. MPDUs are replay protected in the TOE. The MKA frames are guarded against replay, such that if a MPDU contains a duplicate Member Number (MN) and not the most current MN, then this MPDU will be dropped and not processed further. In addition, the attempt to replay data is logged.
FPT_APW_EXT.1	The TOE is designed specifically to not disclose any passwords stored in the TOE. All passwords are stored using a SHA-2 hash. 'Show' commands display only the hashed password. The CC Configuration Guide instructs the Administrator to use the algorithm-type scrypt sub-command when passwords are created or updated. The scrypt is password type 9 and uses a SHA-2 hash.
FPT_SKP_EXT.1	The TOE is designed specifically to not disclose any keys stored in the TOE. The TOE stores all private keys in a secure directory that cannot be viewed or accessed, even by the Administrator. The TOE stores symmetric keys only in volatile memory. Pre-shared keys may be specified in the configuration file by the Administrator using a bit-based (hex) format. Only the Administrator may view the configuration file.
FPT_STM_EXT.1	The TSF implements a clock function to provide a source of date and time. The clock function is reliant on the system clock provided by the underlying hardware. All Switch models have a real-time clock (RTC) with battery to maintain time across reboots and power loss. The TOE relies upon date and time information for the following security functions: ■ To monitor local and remote interactive administrative sessions for inactivity (FTA_SSL_EXT.1, FTA_SSL.3); ■ Validating X.509 certificates to determine if a certificate has expired (FIA_X509_EXT.1/Rev); ■ To determine when IKEv2 SA lifetimes have expired and to initiate a rekey (FCS_IPSEC_EXT.1); ■ To determine when IPsec Child SA lifetimes have expired and to initiate a rekey (FCS_IPSEC_EXT.1);

TOE SFRs	How the SFR is Met
	■ To determine when SSH session keys have expired and to initiate a rekey (FCS_SSHS_EXT.1); ■ To provide accurate timestamps in audit records (FAU_GEN.1.2).
FPT_TUD_EXT.1	An Authorized Administrator can query the software version running on the TOE and can initiate updates to (replacements of) software images. The current active version can be verified by executing the "show version" command from the TOE's CLI. When software updates are made available by Cisco, an Administrator can obtain, verify the integrity of, and install the updates. The updates can be downloaded from https://software.cisco.com/ The TOE will authenticate the image using a digital signature verification check to ensure it has not been modified since distribution using the following process: Prior to being made publicly available, the software image is hashed using a SHA512 algorithm and then digitally signed. The digital signature is embedded to the image (hence the image is signed). The TOE uses a Cisco public key to validate the digital signature to obtain the SHA512 hash. The TOE then computes its own hash of the image using the same SHA512 algorithm and verifies the computed hash against the embedded hash. If they match the image has not been modified or tampered since distributed from Cisco meaning the software is authenticated. If they do not match the image will not install.
FPT_TST_EXT.1	The TOE runs a suite of self-tests during initial start-up to verify correct operation of the cryptographic module. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. If any of the tests fail, the system halts and a message is displayed to the local console. These tests include: ***AES Known Answer Test***: For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value. If the encrypted texts match, the test passes; otherwise, the test fails. 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. If the decrypted texts match, the test passes; otherwise, the test fails. ***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. If the encrypted values, the test passes; otherwise, the test fails. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value. If the decrypted values match, the test passes; otherwise, the test fails. ***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. If the random bits match, the test passes; otherwise, the test fails. ***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. If the MAC values match, the test passes; otherwise, the test fails. ***Software Integrity Test:*** The Software Integrity Test is run automatically whenever the module is loaded and confirms the module has maintained its integrity. ***SHA-256/512 Known Answer Test:***

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>For each of the values listed, the SHA implementation is fed known data and a key. These values are used to generate a hash. This hash is compared to a known value. If the hash values match, the test passes; otherwise, the test fails.

If any component reports failure for the POST, the system crashes. Appropriate information is displayed on the screen and saved in the crashinfo file.

All ports are blocked during the POST. If all components pass the POST, the system is placed in FIPS PASS state and ports can forward data traffic.

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

Example Error Message:
%CRYPTO-0-SELF_TEST_FAILURE: Crypto algorithms self-test failed (SHA hashing)

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.</td></tr>
<tr><td>FTA_SSL_EXT.1
FTA_SSL.3</td><td>An Authorized Administrator can configure maximum inactivity times individually for both local and remote administrative sessions using the “exec-timeout” command applied to the console and virtual terminal (vty) lines. The allowable inactivity timeout range is from is <0-35791> minutes.

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. The local interactive session terminates and does not lock. If a local user session is inactive for a configured period, the session will be terminated and will require re-identification and authentication to login. If a remote user session is inactive for a configured period, the session will be terminated and will require re-identification and authentication to establish a new session.</td></tr>
<tr><td>FTA_SSL.4</td><td>An Authorized Administrator can exit out of both local and remote administrative sessions by issuing the ‘exit’ or ’logout’ command.</td></tr>
<tr><td>FTA_TAB.1</td><td>The Administrator can configure an access banner that describes restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE. The banner will display on the local console port and SSH interfaces prior to allowing any administrative access.</td></tr>
<tr><td>FTP_ITC.1
FTP_ITC.1/MACSEC</td><td>The TOE uses secure protocols to provide trusted communications between itself and authorized IT entities as specified in the table below:

<table>
<tr><th>IT Entity</th><th>TOE Acting as Client or Server</th><th>Secure Communication Mechanism/ Protocol</th><th>Non-TSF Endpoint Identification</th></tr>
<tr><td>Syslog Server</td><td>Client</td><td>IPsec</td><td>X.509 Certificate</td></tr>
<tr><td>MACsec Peer</td><td>Client or Server</td><td>MACsec</td><td>Pre-Shared Key</td></tr>
</table></td></tr>
<tr><td>FTP_TRP.1/Admin</td><td>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) can initiate SSHv2 communications with the TOE.</td></tr>
</table>

6.1. Key Zeroization

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

Table 20. Key Zeroization

Key	Description	Storage Location	Zeroization Method
MACsec SAK	The SAK is used to secure the control plane traffic.	internal ASIC register	Automatically when MACsec session terminated. The value is zeroized by overwriting with another key or freed when the session expires.
MACsec CAK	The CAK secures the control plane traffic.	internal ASIC register	Automatically when MACsec session terminated. The value is zeroized by overwriting with another key or freed when the session expires.
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 (SCA).	internal ASIC register	Automatically when MACsec session terminated. The value is zeroized by overwriting with another key or freed when the session expires.
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.	internal ASIC register	Automatically when MACsec session terminated. The value is zeroized by overwriting with another key or freed when the session expires.
SSH Session Key	Used to encrypt SSH traffic	SDRAM	Overwritten automatically with 0x00 when the SSH trusted channel is no longer in use.
SSH Private Key	Used in establishing a secure SSH session	NVRAM	Overwritten with 0x00 by using the following command: `#crypto key zeroize <label>`
Diffie-Hellman Shared Secret	The shared secret used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman Exchange.	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
Diffie Hellman private key	The private key used in Diffie-Hellman (DH) Exchange	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
Skey_id	IKE SA key from which Phase2/Child IPsec keys are derived.	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.

Key	Description	Storage Location	Zeroization Method
IKE session encrypt key	Used for IKE payload protection	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
IKE session authentication key	Used for IKE payload integrity verification	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
IPsec encryption key	Used to secure IPsec traffic	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.
IPsec authentication key	Used to authenticate the IPsec peer	SDRAM	Overwritten automatically with 0x00 when the IPsec trusted channel is no longer in use.

6.2. CAVP Certificates

The table below lists the CAVP certificates for the TOE

Table 21. CAVP Certificates

SFR	Selection	Algorithm	Implementation	Certificate Number
FCS_CKM.1 – Cryptographic Key Generation	2048 3072	RSA	IC2M	A1462
FCS_CKM.1 – Cryptographic Key Generation	P-256 P-384	ECDSA	IC2M	A1462
FCS_CKM.2 – Cryptographic Key Establishment	P-256 P-384	KAS-ECC	IC2M	A1462
FCS_COP.1/DataEncryption – AES Data Encryption/Decryption	AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256	AES	IC2M	A1462
FCS_COP.1/MACSEC	AES-GCM-128	AES	UADP MSC	AES 4769 [2]
	AES-KW 128 bits	AES	IC2M	A1462
FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)	2048 3072	RSA	IC2M	A1462

[2] The Tested Environment is Synopsys VCS v2011.12mx-SP1-3

SFR	Selection	Algorithm	Implementation	Certificate Number
FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)	SHA-256 SHA-512	SHS	IC2M	A1462
FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	HMAC-SHA-256	HMAC	IC2M	A1462
FCS_COP.1/CMAC	AES-CMAC 128 bits	AES-CMAC	IC2M	A1462
FCS_RBG_EXT.1– Random Bit Generation	CTR_DRBG (AES) 256 bits	DRBG	IC2M	A1462

7. References

The documentation listed below was used to prepare this ST.

Table 22. References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-004
[NDcPP]	collaborative Protection Profile for Network Devices, version 2.2e, March 23, 2020
[SD]	Supporting Document – Evaluation Activities for Network Device cPP, version 2.2, December-2019
[MOD_MACSEC]	PP-Module for MACsec Ethernet Encryption Version 1.0, 2023-03-02
IEEE 802.1X-2010	IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control
IEEE Standard 802.1AE-2018	IEEE Standard for Local and metropolitan area networks-Media Access Control (MAC) Security
ISO 18033-3	Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
ISO 10116	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
ISO 19772	Information technology -- Security techniques -- Authenticated encryption

Identifier	Description
ISO/IEC 10118-3:2004	Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
ISO/IEC 9797-2:2011	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 18031:2011	Information technology -- Security techniques -- Random bit generation
NIST SP800-38B	Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication
NIST SP800-38F	Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping

7.1.Acronyms and Terms

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

Table 23. Acronyms and Terms

Acronym/Term	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
AES-CMAC	Advanced Encryption Standard - Cipher-based Message Authentication Code
CAK	Connectivity Association Key
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CMAC	Cipher-based Message Authentication Code
DHCP	Dynamic Host Configuration Protocol
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
GE	Gigabit Ethernet port
ICMP	Internet Control Message Protocol
IT	Information Technology
KCK	Key Confirmation Key
KEK	Key Encryption Key
MACsec	Media Access Control Security
MKA	MACsec Key Agreement

MKPDU	MACsec Key Agreement Protocol Data Unit
MU-MIMO	Multi-User Multiple-Input Multiple-Output
NDcPP	collaborative Network Device Protection Profile
OFDMA	Orthogonal Frequency-Division Multiple Access
OS	Operating System
PoE	Power over Ethernet
POST	Power On Self Test
PRF	Pseudo-random function
PP	Protection Profile
RFC	Request for Comment
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SSHv2	Secure Shell (version 2)
ST	Security Target
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
TSS	TOE Summary Specification
UDP	User datagram protocol
WAN	Wide Area Network

7.2.Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

7.3.Contacting Cisco

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.