



Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15

Security Target

Version: 1.0

Date: October 1, 2025

Table of Contents

| | | |
|----------|--|-----------|
| 1 | SECURITY TARGET INTRODUCTION | 6 |
| 1.1 | ST AND TOE REFERENCE..... | 6 |
| 1.2 | TOE OVERVIEW | 6 |
| 1.2.1 | <i>TOE Product Type</i> | <i>6</i> |
| 1.3 | SUPPORTED NON-TOE HARDWARE/ SOFTWARE/ FIRMWARE | 7 |
| 1.4 | TOE DESCRIPTION | 7 |
| 1.5 | TOE EVALUATED CONFIGURATION | 8 |
| 1.6 | PHYSICAL SCOPE OF THE TOE..... | 11 |
| 1.7 | LOGICAL SCOPE OF THE TOE | 15 |
| 1.7.1 | <i>Security Audit.....</i> | <i>15</i> |
| 1.7.2 | <i>Cryptographic Support.....</i> | <i>16</i> |
| 1.7.3 | <i>Identification and Authentication</i> | <i>18</i> |
| 1.7.4 | <i>Security Management</i> | <i>19</i> |
| 1.7.5 | <i>Protection of the TSF.....</i> | <i>19</i> |
| 1.7.6 | <i>TOE Access.....</i> | <i>19</i> |
| 1.7.7 | <i>Trusted path/Channels.....</i> | <i>20</i> |
| 1.8 | EXCLUDED FUNCTIONALITY | 21 |
| 2 | CONFORMANCE CLAIMS..... | 22 |
| 2.1 | COMMON CRITERIA CONFORMANCE CLAIM | 22 |
| 2.2 | PROTECTION PROFILE CONFORMANCE | 22 |
| 2.2.1 | <i>TOE Appropriateness.....</i> | <i>24</i> |
| 2.2.2 | <i>TOE Security Problem Definition Consistency.....</i> | <i>24</i> |
| 2.2.3 | <i>Statement of Security Requirements Consistency.....</i> | <i>24</i> |
| 3 | SECURITY PROBLEM DEFINITION | 25 |
| 3.1 | ASSUMPTIONS | 25 |
| 3.2 | THREATS..... | 26 |
| 3.3 | ORGANIZATIONAL SECURITY POLICIES | 27 |
| 4 | SECURITY OBJECTIVES | 28 |
| 4.1 | SECURITY OBJECTIVES FOR THE TOE..... | 28 |
| 4.2 | SECURITY OBJECTIVES FOR THE ENVIRONMENT | 29 |
| 5 | SECURITY REQUIREMENTS..... | 30 |
| 5.1 | CONVENTIONS..... | 30 |
| 5.2 | TOE SECURITY FUNCTIONAL REQUIREMENTS | 30 |
| 5.2.1 | <i>Security audit (FAU)</i> | <i>32</i> |
| 5.2.2 | <i>Cryptographic Support (FCS)</i> | <i>34</i> |
| 5.2.3 | <i>Identification and authentication (FIA)</i> | <i>41</i> |
| 5.2.4 | <i>Security Management (FMT).....</i> | <i>43</i> |
| 5.2.5 | <i>Protection of the TSF (FPT).....</i> | <i>45</i> |
| 5.2.6 | <i>TOE Access (FTA)</i> | <i>46</i> |
| 5.2.7 | <i>Trusted Path/Channels (FTP)</i> | <i>47</i> |
| 5.3 | TOE SFR DEPENDENCIES RATIONALE FOR SFRs FOUND IN NDCPP v3.0e | 47 |
| 5.4 | SECURITY ASSURANCE REQUIREMENTS | 48 |
| 5.4.1 | <i>SAR Requirements.....</i> | <i>48</i> |
| 5.4.2 | <i>Security Assurance Requirements Rationale.....</i> | <i>48</i> |
| 5.5 | ASSURANCE MEASURES | 48 |
| 6 | TOE SUMMARY SPECIFICATION | 50 |

| | | |
|-----|---|-----------|
| 6.1 | TOE SECURITY FUNCTIONAL REQUIREMENT MEASURES..... | 50 |
| 7 | ANNEX A: KEY ZEROIZATION | 64 |
| 8 | ANNEX B: ACRONYMS | 66 |
| 9 | ANNEX C: TERMINOLOGY | 69 |
| 10 | ANNEX D: REFERENCES | 70 |

List of Tables

| | |
|--|----|
| TABLE 1 ST AND TOE IDENTIFICATION..... | 6 |
| TABLE 2 IT ENVIRONMENT COMPONENTS..... | 7 |
| TABLE 3 HARDWARE MODELS AND SPECIFICATIONS | 12 |
| TABLE 4 FIPS ALGORITHM REFERENCES | 16 |
| TABLE 5 TOE PROVIDED CRYPTOGRAPHY | 17 |
| TABLE 6 EXCLUDED FUNCTIONALITY | 21 |
| TABLE 7 CFG_NDcPP-MACSEC_V2.0 COMPONENTS | 22 |
| TABLE 8 FUNCTIONAL PACKAGES | 22 |
| TABLE 9 - NIAP TECHNICAL DECISIONS (TD)..... | 22 |
| TABLE 10 TOE ASSUMPTIONS | 25 |
| TABLE 11 THREATS..... | 26 |
| TABLE 12 ORGANIZATIONAL SECURITY POLICIES..... | 27 |
| TABLE 13 SECURITY OBJECTIVES FOR THE TOE | 28 |
| TABLE 14 SECURITY OBJECTIVES FOR THE ENVIRONMENT..... | 29 |
| TABLE 15 SECURITY FUNCTIONAL REQUIREMENTS | 30 |
| TABLE 16 AUDITABLE EVENTS..... | 32 |
| TABLE 17 AUDITABLE EVENTS (MACSEC) | 34 |
| TABLE 18. ADDITIONAL PASSWORD SPECIAL CHARACTERS | 41 |
| TABLE 19 ASSURANCE MEASURES..... | 48 |
| TABLE 20 ASSURANCE MEASURES..... | 48 |
| TABLE 21 HOW TOE SFRS MEASURES | 50 |
| TABLE 22 TOE KEY ZEROIZATION | 64 |
| TABLE 23 ACRONYMS..... | 66 |
| TABLE 24 TERMINOLOGY | 69 |
| TABLE 25 REFERENCES..... | 70 |

List of Figures

| | |
|---|----|
| FIGURE 1 - TOE EXAMPLE DEPLOYMENT | 10 |
|---|----|

DOCUMENT INTRODUCTION

Prepared By:

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 9513

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15. 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. In this document, Administrators of the TOE will be referred to as Administrators, Authorized Administrators, TOE Administrators, semi-privileged, privileged Administrators, and security Administrators.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2025 Cisco Systems, Inc. All rights reserved.

1 Security Target Introduction

The Security Target (ST) contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- Security Requirements [Section 5]
- Target of Evaluation (TOE) Summary Specification [Section 6]
- Annex A: Key Zeroization (Section 7)
- Annex B: Acronyms (Section 8)
- Annex C: Terminology (Section 9)
- Annex D: References (Section 10)

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

1.1 ST and TOE Reference

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

Table 1 ST and TOE Identification

| Name | Description |
|----------------------|---|
| ST Title | Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 Security Target |
| ST Version | 1.0 |
| Publication Date | 10/2/25 |
| Vendor and ST Author | Cisco Systems, Inc. |
| TOE Reference | Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 |
| TOE Hardware Models | IE-9310-26S2C IE-9320-26S2C IE-9320-22S2C4X IE-9320-24T4X IE-9320-24P4X IE-9320-24P4S IE-9320-16P8U4X |
| TOE Software Version | IOS-XE 17.15 |
| Keywords | Audit, Authentication, Encryption, MACsec, Network Device, Secure Administration |

1.2 TOE Overview

The TOE is the Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 all running Internetworking Operating System (IOS)-XE 17.15. The TOE is a purpose-built, switching and routing platform with Open System Interconnection (OSI) Layer2 and Layer3 traffic filtering capabilities. The TOE also supports Media Access Control Security (MACsec) encryption for switch-to-switch (inter-network device) security. The TOE includes the hardware models as defined in [Table 3](#) below.

1.2.1 TOE Product Type

The Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 are switching and routing platforms that provide connectivity and security services, including MACsec encryption, on a single, secure device. These switches offer broadband speeds and simplified management to small businesses, enterprise small branch, and teleworkers.

The TOE is a network device that includes MACsec encryption as defined in NDcPP v3.0e¹ and MOD_MACsec v1.0². The TOE is comprised of both hardware and software. The hardware is the IE9300 switch as described in section 1.6 below. The software is the Cisco IOS-XE 17.15.

The TOE and ST are also conformant with the Functional Package for Secure Shell (SSH), Version 1.0, May 13, 2021 [PKG_SSH_v1.0].

The Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches are single-device security and switching solutions for protecting the network.

1.3 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware components in its operational environment. Each component is identified as being required or not based on the claims made in this ST. All environment components listed in Table 2 below are supported by all TOE evaluated configurations.

Table 2 IT Environment Components

| Component | Required | Usage/Purpose Description for TOE performance |
|--|-------------|--|
| Audit (syslog) Server | Yes | This includes any syslog server to which the TOE transmits syslog messages over a secure Internet Protocol security (IPsec) trusted channel either directly or connected to a TOE Peer that also supports a secure IPsec trusted channel |
| Local Console | Yes | This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE Administrator to support TOE administration |
| Management Workstation with Secure Shell v2 (SSHv2) client | Yes | This includes any IT Environment Management workstation that is used by the TOE Administrator to support TOE administration using SSHv2 protected channels. Any SSH client that supports SSHv2 may be used |
| MACsec Peer | Yes | This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications |
| Certification Authority (CA) | Yes | This includes any IT Environment CA on the TOE network. The CA can be used to provide the TOE with a valid certificate during certificate enrolment as well as validating a certificate |
| TOE Peer | Conditional | The TOE Peer is required if the remote syslog server is attached to the TOE Peer and used by the TOE. If the remote syslog server is directly connected to the TOE for the TOE's use, then the TOE Peer is not required |

1.4 TOE Description

This section provides an overview of the Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following hardware models as described in 1.6 Physical Scope of the TOE. The software is comprised of the Universal Cisco Internet Operating System (IOS) XE software image Release IOS-XE 17.15. The Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches that comprises the TOE has common hardware characteristics as described in Table 3 Hardware Models and Specifications. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware. The Cisco Catalyst Industrial Ethernet IE9300 Rugged Series Switches primary features include the following:

- Central processor that supports all system operations.

¹ collaborative Protection Profile for Network Devices Version 3.0e

² PP-Module for MACsec Ethernet Encryption Version 1.0

- Full Gigabit Ethernet switch:
 - Total of 28 Gigabit Ethernet ports provide multiple resilient design options
 - Provides secure access for new high-speed applications in the industrial space
- Memory:
 - 4-GB DRAM
 - 8-GB onboard flash memory
- Available Interfaces:
 - USB 2.0 (all models)
 - RS-232 (via RJ-45) and 1 Micro USB Console Interfaces (all models)
 - Note: an RJ-45-to-DB-9 adapter cable is supplied to be used to connect the console port of the switch to a console PC.
 - **IE-9310-26S2C, IE-9320-26S2C**
 - 22 100/1000M SFP fiber ports
 - 2 Combo (100/1000M SFP, 10/100/1000M RJ-45) ports
 - 4 1G SFP fiber ports
 - **IE-9320-22S2C4X**
 - 22 100/1000M SFP fiber ports
 - 2 Combo (100/1000M SFP, 10/100/1000M RJ-45) ports
 - 4 1/10G SFP+ fiber ports
 - **IE-9320-24P4S**
 - - 24 10/100/1000M RJ-45 PoE+
 - 4 1G SFP fiber ports
 - **IE-9320-24T4X**
 - 24 10/100/1000M RJ-45
 - 4 1/10G SFP+ fiber ports
 - **IE-9320-24P4X**
 - 24 10/100/1000M RJ-45 PoE+
 - 4 1/10G SFP+ fiber ports
 - **IE-9320-16P8U4X**
 - 16 10/100/1000M PoE+
 - 8 Combo (100/1000/2500M 4PPoE)
 - 4 1/10G SFP+ fiber ports

Cisco IOS-XE is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although IOS-XE performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 Logical Scope of the TOE below.

1.5 TOE Evaluated Configuration

The TOE evaluated configuration consists of one or more physical devices as specified in section 1.6 below and includes Cisco IOS-XE software. When deployed in its evaluated configuration, the Cisco IOS-XE software determines how packets are handled to and from the TOE's network interfaces. Typically, packet flows are passed through internetworking devices and forwarded to their configured destination.

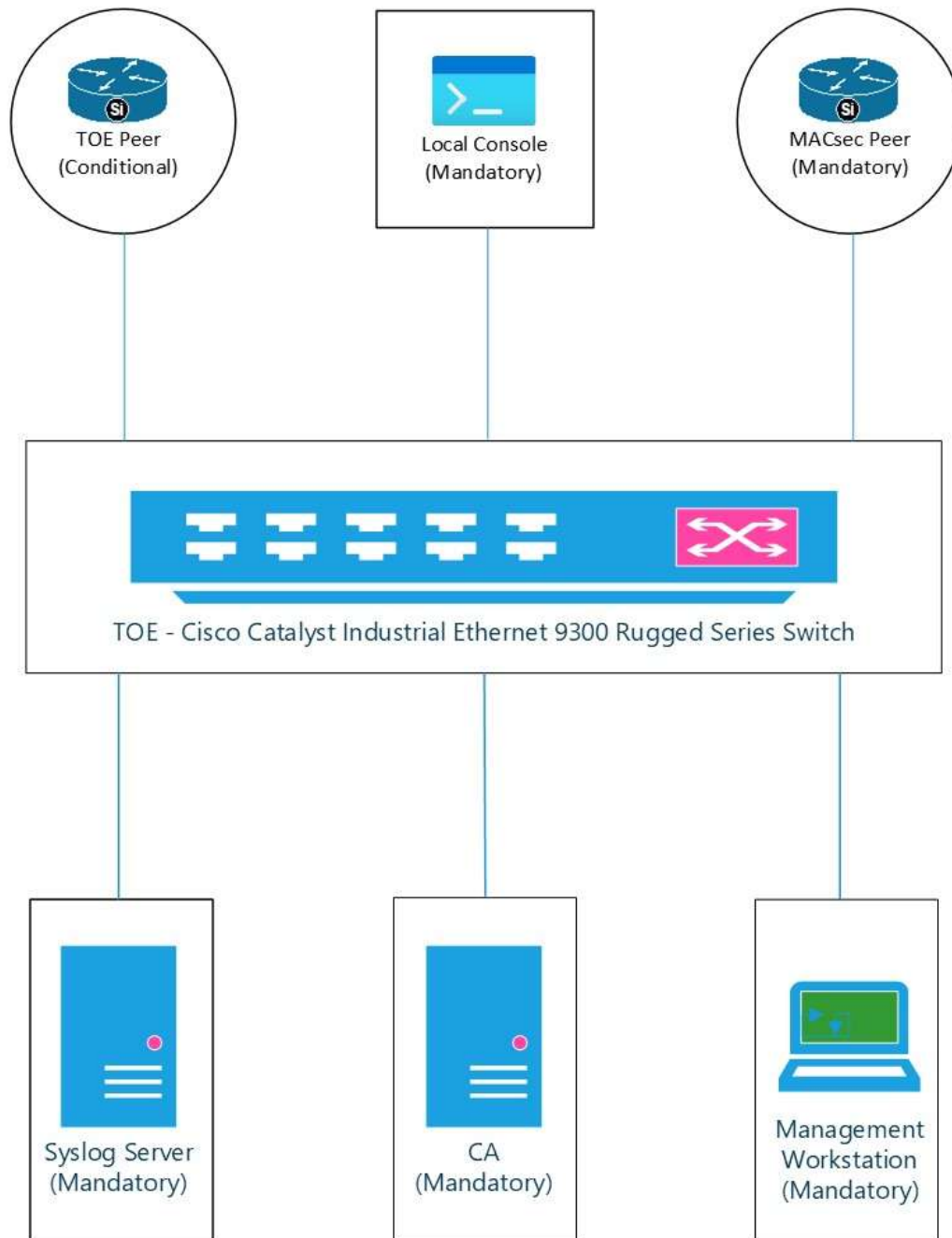
The TOE evaluated configuration requires the following components in the operational environment:

- A syslog server to which the TOE transmits syslog messages over a secure Internet Protocol security (IPsec) trusted channel either directly or connected to a TOE Peer that also supports a secure IPsec trusted channel.
- A Management workstation that is used by the TOE Administrator to support TOE administration using SSHv2 protected channels.
- A local console that is directly connected to the TOE via the Serial Console Port and is used by the TOE Administrator to support TOE administration.

- A MACsec peer device with which the TOE participates in MACsec communications.
- A Certification Authority (CA) used to provide the TOE with a valid certificate during certificate enrolment as well as validating a certificate.

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

Figure 1 - TOE Example Deployment



The previous figure includes the following:

- Examples of TOE Models
- The following are considered to be in the IT Environment:
 - MACsec Peer
 - TOE Peer
 - Management Workstation
 - Audit (Syslog) Server
 - Local Console
 - Certification Authority (CA)

NOTE: While the previous figure includes several non-TOE IT environment devices, the TOE is only the IE9300 device. Only one TOE device is required for deployment in an evaluated configuration.




1.6 Physical Scope of the TOE


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



- IE-9310-26S2C
- IE-9320-26S2C
- IE-9320-22S2C4X
- IE-9320-24T4X
- IE-9320-24P4X
- IE-9320-24P4S
- IE-9320-16P8U4X

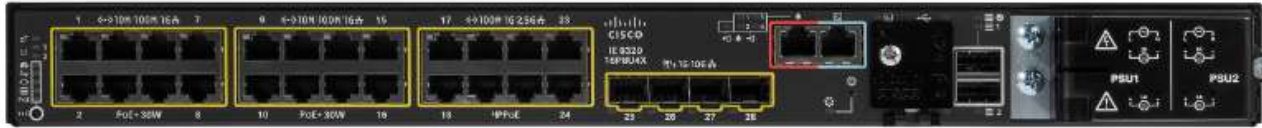
The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XE software image Release 17.15. In addition, the software image is also downloadable from the Cisco web site. A login id and password are required to download the software image. The TOE is comprised of the following physical specifications as described in Table 3 below:

Table 3 Hardware Models and Specifications

| Hardware | Processor | Features |
|---|--|--|
| <p>IE-9310-26S2C:</p>  <p>IE-9320-26S2C:</p>  | | |
| <p>Cisco Industrial Ethernet 9300 Series</p> <p>IE-9310-26S2C IE-9320-26S2C</p> | <p>Cisco Cray64 CPU integrated in DopplerGS ASIC (ARMv8 Cortex A53)</p> <p>MACSec: MSC MACsec embedded in ASICs v1.1</p> | <p>Physical dimensions (W x D)</p> <ul style="list-style-type: none"> IE-9310-26S2C: 1.72 x 17.5 x 14.0 in. IE-9320-26S2C: 1.72 x 17.5 x 14.0 in. <p>Main Board Interfaces</p> <ul style="list-style-type: none"> 22 100/1000M fiber ports 2 combo (100/1000M SFP, 10/100/1000M RJ-45) ports 4 1G SFP fiber port RS-232 Console Interface Micro USB Console Interface 2 Stacking ports (all listed models except IE-9310-26S2C) <p>Memory</p> <ul style="list-style-type: none"> 4 GB DDR4 DRAM 8 GB onboard flash memory <p>Power</p> <ul style="list-style-type: none"> Dual AC/DC power inputs |
| <p>IE-9320-22S2C4X:</p>  | | |

| Hardware | Processor | Features |
|--|---|--|
| Cisco Industrial Ethernet 9300 Series IE-9320-22S2C4X | Cisco Cray64 CPU integrated in DopplerGS ASIC (ARMv8 Cortex A53) MACSec: MSC MACsec embedded in ASICs v1.1 | Physical dimensions (W x D) <ul style="list-style-type: none"> IE-9320-22S2C4X: 1.72 x 17.5 x 14.0 in. Main Board Interfaces <ul style="list-style-type: none"> 22 100/1000M fiber ports 2 combo (100/1000M SFP, 10/100/1000M RJ-45) ports 4 1/10G SFP+ fiber ports RS-232 Console Interface Micro USB Console Interface 2 Stacking ports (all listed models except IE-9310-26S2C) Memory <ul style="list-style-type: none"> 4 GB DDR4 DRAM 8 GB onboard flash memory Power <ul style="list-style-type: none"> Dual AC/DC power inputs |
| IE-9320-24P4S:  | | |
| Cisco Industrial Ethernet 9300 Series IE-9320-24P4S | Cisco Cray64 CPU integrated in DopplerGS ASIC (ARMv8 Cortex A53) MACSec: MSC MACsec embedded in ASICs v1.1 | Physical dimensions (W x D) <ul style="list-style-type: none"> IE-9320-24P4S: <ul style="list-style-type: none"> 1.72 x 17.5 x 14.0 in. 1.72 x 17.5 x 15.18 in. 1.72 x 17.5 x 15.57 in. Main Board Interfaces <ul style="list-style-type: none"> 24 10/100/1000M RJ-45 PoE+ ports 4 1G SFP fiber ports RS-232 Console Interface Micro USB Console Interface 2 Stacking ports (all listed models except IE-9310-26S2C) Memory <ul style="list-style-type: none"> 4 GB DDR4 DRAM 8 GB onboard flash memory Power <ul style="list-style-type: none"> Dual AC/DC power inputs |

| Hardware | Processor | Features |
|--|---|--|
| IE-9320-24T4X:  | | |
| Cisco Industrial Ethernet 9300 Series IE-9320-24T4X | Cisco Cray64 CPU integrated in DopplerGS ASIC (ARMv8 Cortex A53) MACSec: MSC MACsec embedded in ASICs v1.1 | Physical dimensions (W x D) <ul style="list-style-type: none"> IE-9320-24T4X: 1.72 x 17.5 x 14.0 in. Main Board Interfaces <ul style="list-style-type: none"> 24 10/100/1000M RJ-45 ports 4 1/10G SFP+ fiber ports RS-232 Console Interface Micro USB Console Interface 2 Stacking ports (all listed models except IE-9310-26S2C) Memory <ul style="list-style-type: none"> 4 GB DDR4 DRAM 8 GB onboard flash memory Power <ul style="list-style-type: none"> Dual AC/DC power inputs |
| IE-9320-24P4X  | | |
| Cisco Industrial Ethernet 9300 Series IE-9320-24P4X | Cisco Cray64 CPU integrated in DopplerGS ASIC (ARMv8 Cortex A53) MACSec: MSC MACsec embedded in ASICs v1.1 | Physical dimensions (W x D) <ul style="list-style-type: none"> IE-9320-24P4X: <ul style="list-style-type: none"> 1.72 x 17.5 x 14.0 in. 1.72 x 17.5 x 15.18 in. 1.72 x 17.5 x 15.57 in. Main Board Interfaces <ul style="list-style-type: none"> 24 10/100/1000M RJ-45 PoE+ ports 4 1/10G SFP+ fiber ports RS-232 Console Interface Micro USB Console Interface 2 Stacking ports (all listed models except IE-9310-26S2C) Memory <ul style="list-style-type: none"> 4 GB DDR4 DRAM 8 GB onboard flash memory Power <ul style="list-style-type: none"> Dual AC/DC power inputs |

| Hardware | Processor | Features |
|--|---|--|
| IE-9320-16P8U4X:  | | |
| Cisco Industrial Ethernet 9300 Series IE-9320-16P8U4X | Cisco Cray64 CPU integrated in DopplerGS ASIC (ARMv8 Cortex A53) MACSec: MSC MACsec embedded in ASICs v1.1 | Physical dimensions (W x D) <ul style="list-style-type: none"> IE-9320-16P8U4X: <ul style="list-style-type: none"> 1.72 x 17.5 x 14.0 in. 1.72 x 17.5 x 15.18 in. 1.72 x 17.5 x 15.57 in. Main Board Interfaces <ul style="list-style-type: none"> 16 10/100/1000M PoE+ ports 8 100/1000/2500M 4PPoE ports 4 1/10G SFP+ fiber ports RS-232 Console Interface Micro USB Console Interface 2 Stacking ports (all listed models except IE-9310-26S2C) Memory <ul style="list-style-type: none"> 4 GB DDR4 DRAM 8 GB onboard flash memory Power <ul style="list-style-type: none"> Dual AC/DC power inputs |

1.7 Logical Scope of the TOE

The TOE is comprised of the following security features:

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

These features are described in more detail in the subsections below. In addition, the TOE implements all Request for Comments (RFCs) of the NDcPP v3.0e and MOD_MACsec v1.0 as necessary to satisfy testing/assurance measures prescribed therein.

1.7.1 Security Audit

The Cisco Catalyst IE9300 Rugged Series Switches provide extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event.

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

The TOE also internally stores audit records in a circular log file where the oldest audit records are overwritten when the audit trail becomes full. The audit logs can be viewed on the TOE using the appropriate IOS-XE 17.15 commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the Authorized Administrator to clear audit data stored locally on the TOE.

1.7.2 Cryptographic Support

The TOE provides the cryptography to support all security functions. All algorithms claimed have Cryptographic Algorithm Validation Program (CAVP certificates running on the processors specified in [Table 3](#) above).

The TOE leverages the IOS Common Cryptographic Module (IC2M), firmware version Rel5a (CAVP cert. #A1462).

The TOE supports MACsec using the proprietary UAPD MSC MACsec embedded in ASICs v1.1 (CAVP Cert. #4848).

Refer to Table 4 below for algorithm certificate references.

Table 4 FIPS Algorithm References

| SFR | Selection | Algorithm | Implementation | Certificate Number |
|---|------------------------|-----------|----------------|---|
| FCS_CKM.1 – Cryptographic Key Generation | 2048 3072 | RSA | IC2M Rel5a | A1462 |
| RSA schemes comply with: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 ECC schemes comply with: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4; FFC schemes comply with: NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and RFC 3526 | Dh-14 | FFC | IC2M Rel5a | Tested with a known good implementation |
| | ECC p-256 ECC p-384 | ECC | IC2M Rel5a | A1462 |
| FCS_CKM.2 – Cryptographic Key Establishment | Dh-14 | FFC | IC2M Rel5a | Tested with a known good implementation |
| | ECC p-256 ECC p-384 | ECC | IC2M Rel5a | A1462 |
| FCC complies with: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and groups listed in RFC 3526 | | | | |
| ECC complies with: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4; | | | | |

| | | | | |
|---|--|----------|------------|-------|
| FCS_COP.1/DataEncryption – AES Data Encryption/Decryption AES complies with ISO 18033-3 CBC complies with ISO 10116 GCM complies with ISO 19772 | AES-CBC-128 AES-CBC-256 AES-GCM-128 AES-GCM-256 | AES | IC2M Rel5a | A1462 |
| FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification) Complies with: 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 | 2048 3072 | RSA | IC2M Rel5a | A1462 |
| FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm) Complies with: ISO/IEC 10118-3:2004 | SHA-1 SHA-256 SHA-512 | SHA | IC2M Rel5a | A1462 |
| FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm) Complies with: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2” | HMAC-SHA-256 | HMAC | IC2M Rel5a | A1462 |
| FCS_COP.1/CMAC Cryptographic Operation (AES-CMAC Keyed Hash Algorithm) Complies with: NIST SP800-38B | AES-CMAC 128 bits AES-CMAC 256bits | AES-CMAC | IC2M Rel5a | A1462 |
| FCS_COP.1/MACSEC Cryptographic Operation (MACsec AES Data Encryption/Decryption) AES complies with ISO 18033-3 GCM complies with ISO 19772 | AES-GCM-128 bits AES-GCM-256 bits | AES | MACsec | 4848 |
| FCS_COP.1/MACSEC Cryptographic Operation (MACsec AES Data Encryption/Decryption) AES Key Wrap complies with NIST SP800-38F | AES-KW 128 bits AES-KW 256 bits | AES | IC2M Rel5a | A1462 |
| FCS_RBG_EXT.1– Random Bit Generation Complies with: ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions” | CTR_DRBG (AES-256 bits) | DRBG | IC2M Rel5a | A1462 |

The TOE provides cryptographic support for IPsec, which is used to secure the session between the TOE and the audit server.

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

The cryptographic services provided by the TOE are described in Table 5 below.

Table 5 TOE Provided Cryptography

| Cryptographic Method | Use within the TOE |
|----------------------------|--|
| AES | Used to encrypt IPsec session traffic Used to encrypt SSH session traffic Used to encrypt MACsec traffic |
| HMAC | Used for keyed hash, integrity services in IPsec and SSH session establishment |
| DH | Used as the Key exchange method for IPsec and SSH |
| Internet Key Exchange | Used to establish initial IPsec session |
| RSA Signature Services | Used in IPsec session establishment Used in SSH session establishment X.509 certificate signing |
| RSA | Used in IKE protocols peer authentication Used to provide cryptographic signature services Used in Cryptographic Key Generation |
| Secure Shell Establishment | Used to establish initial SSH session |
| SHA | Used to provide IPsec traffic integrity verification Used to provide SSH traffic integrity verification Used for keyed-hash message authentication |
| NIST SP800-90A DRBG | Used for random number generation, key generation and seeds to asymmetric key generation Used in IPsec session establishment Used in SSH session establishment Used in MACsec session establishment |

The Catalyst IE9300 Rugged Series Switches contain the processors listed in [Table 3](#) above.

1.7.3 Identification and Authentication

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

The TOE provides authentication services for administrative users to connect to the TOE's secure Command Line Interface (CLI) Administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE provides Administrator authentication against a local user database. Password-based authentication can be performed on the local serial console or SSHv2 interfaces. The SSHv2 interface also supports authentication using SSH keys.

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

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

1.7.4 Security Management

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

- Administration of the TOE locally and remotely
- Configuration of warning and consent access banners
- Configuration of session inactivity thresholds
- Updates of the TOE software
- Configuration of authentication failures
- Configuration of the audit functions of the TOE
- Configuration of the TOE provided services
- Configuration of the cryptographic functionality of the TOE
- Generate, install, and manage Pre-Shared Key (PSK)
- Manage the Key Server, Connectivity Association Key (CAK) and MKA participants
- Configure lockout time interval for excessive authentication failures

The TOE supports two separate Administrator roles: non-privileged Administrator and privileged Administrator. Only the privileged Administrator can perform the above security relevant management functions. The privileged Administrator is the Authorized Administrator of the TOE who can enable, disable, determine, and modify the behaviour of the security functions of the TOE as described in this document.

1.7.5 Protection of the TSF

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

The TOE can verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

The TOE detects replay of information received via secure channels (MACsec). The detection is applied to network packets that terminate at the TOE, such as trusted communications between the TOE and an IT entity (e.g., MACsec peer). If replay is detected, the packets are discarded.

The TOE internally maintains the date and time. This date and time information is used as the timestamp that is applied to audit records generated by the TOE. The TOE provides the Authorized Administrators the capability to update the TOE's clock manually to maintain a reliable timestamp.

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

1.7.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated, the TOE requires the user to re-authenticate to establish a new session.

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

1.7.7 Trusted path/Channels

The TOE allows a trusted path to be established to itself from remote Administrators over SSHv2 and initiates outbound IPsec trusted channels to transmit audit messages to remote syslog servers.

The TOE supports MACsec secured trusted channels between itself and MACsec peers.

1.8 Excluded Functionality

Functionality in Table 6 below is excluded from the evaluation.

Table 6 Excluded Functionality

| Excluded Functionality | Exclusion Rationale |
|--|---|
| Non-FIPS 140-2 mode of operation | This mode of operation includes non-FIPS allowed operations |
| Telnet | Telnet sends authentication data in plain text. This feature must remain disabled in the evaluated configuration. SSHv2 must be used to secure the trusted path for remote administration for all SSHv2 sessions. |
| Transport Layer Security (TLS) | TLS is not associated with Security Functional Requirements claimed in [NDcPP] IPsec is used instead. |
| Hypertext Transfer Protocol (HTTP) | Remote Management is performed using SSH |
| Hypertext Transfer Protocol Secure (HTTPS) | Remote Management is performed using SSH |
| TOE Peer (Conditional) | If the remote syslog server is directly connected to the TOE for the TOE's use, then the TOE Peer is not required. |

These services can be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect the compliance to the NDcPP v3.0e or the MOD_MACsec v1.0.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

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

2.2 Protection Profile Conformance

The TOE and ST are conformant with the PP-Configuration for Network Devices and MACsec Ethernet Encryption, 2024-04-25 (CFG_NDcPP-MACsec_V2.0). Table 7 below lists the components of CFG_NDcPP-MACsec_V1.0. This ST applies the NIAP Technical Decisions described in Table 9 below.

The TOE and ST are also conformant with the Functional Package for Secure Shell (SSH), Version 1.0, May 13, 2021 [PKG_SSH_v1.0].

Table 7 CFG_NDcPP-MACsec_V2.0 Components

| Protection Profile | Date |
|--|----------------|
| Base-PP: collaborative Protection Profile for Network Devices, Version 3.0e (CPP_ND_V3.0E) | June 04, 2023 |
| PP-Module: PP-Module for MACsec Ethernet Encryption, Version 1.0 (MOD_MACsec_V1.0) | March 02, 2023 |

Table 8 Functional Packages

| Functional Package | Date |
|---|--------------|
| Functional Package for SSH (PKG_SSH_V1.0) | May 13, 2021 |

This ST applies the following NIAP Technical Decisions:

Table 9 - NIAP Technical Decisions (TD)

| TD Identifier | TD Name | Protection Profiles | References | Publication Date | Applicable? |
|---------------|--|---------------------|--|------------------|-------------|
| TD0923 | NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2 | [CPP_ND_V3.0E] | FAU_GEN.1.2 | 2025.06.25 | Yes |
| TD0921 | NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment | [CPP_ND_V3.0E] | FCS_CKM.1, FCS_COP.1/SigGen, CPP_ND_V3.0e-SD | 2025.06.25 | Yes |
| TD0900 | NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3 | [CPP_ND_V3.0E] | FIA_UIA_EXT.1.3 | 2025.02.27 | Yes |
| TD0899 | NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2 | [CPP_ND_V3.0E] | FCS_TLSC_EXT.1.9, FCS_TLSS_EXT.1.8, CPP_ND_3.0E-SD | 2025.03.06 | No |
| TD0891 | Correlation of Implicitly Satisfied Requirements when CPP_ND_V3.0E is the Base-PP | MOD_MACSEC_V1.0 | Appendix D | 2024.11.20 | Yes |
| TD0889 | Correction For Tests Incorrectly Requiring Group MACsec | MOD_MACSEC_V1.0 | FCS_MKA_EXT.1.7, FMT_SMF.1/MACSEC, FPT_DDP_EXT.1, MOD_MACSEC_V1.0-SD | 2024.10.31 | Yes |

| TD Identifier | TD Name | Protection Profiles | References | Publication Date | Applicable? |
|---------------|---|---------------------|---|------------------|-------------|
| TD0886 | Clarification to FAU_STG_EXT.1 Test 6 | [CPP_ND_V3.0E] | FAU_STG_EXT.1, CPP_ND_V3.0E-SD | 2024.10.16 | Yes |
| TD0884 | Expansion of Permitted EtherTypes in FCS_MACSEC_EXT.1.4 | MOD_MACSEC_V1.0 | FCS_MACSEC_EXT.1.4, MOD_MACSEC_V1.0-SD | 2024.10.16 | Yes |
| TD0882 | MACsec Data Delay Protection, Key Agreement, and Conditional Support for Group CAK | MOD_MACSEC_V1.0 | FCS_MKA_EXT.1.4, FCS_MKA.1.7, FPT_DDP_EXT.1, MOD_MACSEC_V1.0-SD | 2024.10.28 | Yes |
| TD0881 | Correction to MN Usage for FPT_RPL.1 Test | MOD_MACSEC_V1.0 | FPT_RPL.1, MOD_MACSEC_V1.0-SD | 2024.09.20 | Yes |
| TD0880 | NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1 | [CPP_ND_V3.0E] | FMT_SMF.1.1 | 2024.09.17 | Yes |
| TD0879 | NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E | [CPP_ND_V3.0E] | Appendix B.6.3, Appendix B.7 | 2024.09.17 | Yes |
| TD0868 | NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8 | [CPP_ND_V3.0E] | FCS_IPSEC_EXT.1.7, FCS_IPSEC_EXT.1.8 | 2024.09.17 | Yes |
| TD0836 | NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1 | [CPP_ND_V3.0E] | FPT_TST_EXT.1, CPP_ND_V3.0E-SD, Section 4.1.5 | 2024.04.25 | Yes |
| TD0870 | Security Objectives Rationale for MOD_MACSEC_V1.0 | MOD_MACSEC_V1.0 | Section 4.3 | 2024.08.08 | Yes |
| TD0840 | Alignment of Test 22.1 to FMT_SMF.1/MACSEC | MOD_MACSEC_V1.0 | FMT_SMF.1/MACSEC, MOD_MACSEC_V1.0-SD | 2024.08.14 | Yes |
| TD0826 | Aligning MOD_MACSEC_V1.0 with CPP_ND_V3.0E | MOD_MACSEC_V1.0 | Section 1.1, MOD_MACSEC_V1.0-SD | 2024.04.25 | Yes |
| TD0816 | Clarity for MACsec Self Test Failure Response | MOD_MACSEC_V1.0 | FPT_FLS.1, MOD_MACSEC_V1.0-SD | 2024.03.22 | Yes |
| TD0746 | Correction to FPT_RPL.1 Test 25 | MOD_MACSEC_V1.0 | FPT_RPL.1, MOD_MACSEC_V1.0-SD | 2023.05.29 | Yes |
| TD0728 | Corrections to MACSec PP-Module SD | MOD_MACSEC_V1.0 | FCS_COP.1/MACSEC, FPT_RPL_EXT.1 | 2023.04.03 | Yes |
| TD0777 | Clarification to Selections for Auditable Events for FCS_SSH_EXT.1 | [PKG_SSH_v1.0] | Section 3.1, Table 1 | 2023.08.23 | Yes |

| TD Identifier | TD Name | Protection Profiles | References | Publication Date | Applicable? |
|---------------|---|---------------------|------------------------|------------------|-------------|
| TD0732 | FCS_SSHS_EXT.1.3 Test 2 Update | [PKG_SSH_v1.0] | FCS_SSH_EXT.1.3 | 2023.05.19 | Yes |
| TD0695 | Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package. | [PKG_SSH_v1.0] | Section 1.3, FCS_COP.1 | 2022.12.14 | Yes |
| TD0682 | Addressing Ambiguity in FCS_SSHS_EXT.1 Tests | [PKG_SSH_v1.0] | FCS_SSHS_EXT.1 | 2022.12.13 | Yes |

2.2.1 TOE Appropriateness

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

- collaborative Protection Profile for Network Devices Version 3.0e (NDcPP v3.0e)
- PP-Module for MACsec Ethernet Encryption Version 1.0 (MOD_MACsec v1.0)
- Functional Package for SSH Version 1.0 (PKG_SSH_V1.0)

2.2.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the NDcPP v3.0e and the MOD_MACsec v1.0 for which conformance is claimed verbatim. All concepts covered in the Protection Profiles Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the NDcPP v3.0e and the MOD_MACsec v1.0, for which conformance is claimed verbatim. All concepts covered in the Protection Profiles Statement of Security Objectives are included in the Security Target.

2.2.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the NDcPP v3.0e and the MOD_MACsec v1.0, for which conformance is claimed verbatim. All concepts covered in the Protection Profiles Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in the NDcPP v3.0e and the MOD_MACsec v1.0.

3 Security Problem Definition

This section identifies the following:

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

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

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE. Note, the assumption, A.NO_THRU_TRAFFIC_PROTECTION is strike-through since the TOE does provide protection against the traffic that does traverse the TOE, which is countered by the TOE objectives defined in 4.1 Security Objectives for the TOE.

Table 10 TOE Assumptions

| Assumption | Assumption Definition |
|----------------------------|--|
| A.PHYSICAL_PROTECTION | The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP 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. |
| A.LIMITED_FUNCTIONALITY | The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). |
| 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.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. |

| Assumption | Assumption Definition |
|------------------------------|---|
| A.NO_THRU_TRAFFIC_PROTECTION | A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall). |

3.2 Threats

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

Table 11 Threats

| Threat | Threat Definition |
|-------------------------------------|---|
| T.UNAUTHORIZED_ADMINISTRATOR_ACCESS | Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides. |
| T.WEAK_CRYPTOGRAPHY | Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort. |
| T.UNTRUSTED_COMMUNICATION_CHANNELS | Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself. |
| T.WEAK_AUTHENTICATION_ENDPOINTS | Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised. |
| T.UPDATE_COMPROMISE | Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. 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. |

| Threat | Threat Definition |
|---|---|
| T.SECURITY_FUNCTIONALITY_COMPROMISE | Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. |
| T.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 | <p>An attacker may modify data transmitted over the layer 2 link in a way that is not detected by the recipient.</p> <p>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.</p> |
| T.NETWORK_ACCESS | <p>An attacker may send traffic through the TOE that enables them to access devices in the TOE's operational environment without authorization.</p> <p>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.</p> |
| T.UNTRUSTED_MACSEC_COMMUNICATION_CHANNELS | <p>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.</p> <p>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.</p> |

3.3 Organizational Security Policies

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

Table 12 Organizational Security Policies

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

4 Security Objectives

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

4.1 Security Objectives for the TOE

The NDcPP v3.0e does not define any security objectives for the TOE, however the MOD_MACsec v1.0 includes security objectives listed in Table 13 below specific to MACsec devices.

Table 13 Security Objectives for the TOE

| Security Objective and SFR mapping | 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 |
| 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 |
| 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. |

4.2 Security Objectives for the Environment

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

Table 14 Security Objectives for the Environment

| Environment Security Objective | IT Environment Security Objective Definition |
|--------------------------------|--|
| OE.PHYSICAL | Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment. |
| OE.NO_GENERAL_PURPOSE | There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE. |
| OE.TRUSTED_ADMIN | Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted. |
| OE.UPDATES | The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities. |
| OE.ADMIN_CREDENTIALS_SECURE | The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside. |
| OE.RESIDUAL_INFORMATION | The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. |

5 Security Requirements

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

5.1 Conventions

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

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

Extended SFRs are identified by having a label “EXT” at the end of the SFR name.

Formatting conventions outside of operations and iterations matches the formatting specified within the NDcPP v3.0e and MOD_MACsec v1.0.

The following conventions were used to resolve conflicting SFRs between NDcPP v3.0e and MOD_MACsec v1.0:

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

5.2 TOE Security Functional Requirements

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

Table 15 Security Functional Requirements

| Class Name | Component Identification | Component Name |
|----------------------------|--------------------------|---|
| FAU: Security audit | FAU_GEN.1 | Audit data generation |
| | FAU_GEN.2 | User Identity Association |
| | FAU_STG_EXT.1 | Protected Audit Event Storage |
| | FAU_GEN.1/MACSEC | Audit Data Generation (MACsec) |
| FCS: Cryptographic support | FCS_CKM.1 | Cryptographic Key Generation (Refinement) |
| | FCS_CKM.2 | Cryptographic Key Establishment |
| | FCS_CKM.4 | Cryptographic Key Destruction |

| Class Name | Component Identification | Component Name |
|--|--------------------------|--|
| | FCS_COP.1/DataEncryption | Cryptographic Operation (AES Data Encryption/Decryption) |
| | FCS_COP.1/SigGen | Cryptographic Operation (Signature Generation and Verification) |
| | FCS_COP.1/Hash | Cryptographic Operation (Hash Algorithm) |
| | FCS_COP.1/KeyedHash | Cryptographic Operation (Keyed Hash Algorithm) |
| | FCS_COP.1/CMAC | Cryptographic Operation (AES-CMAC Keyed Hash Algorithm) |
| | FCS_COP.1/MACSEC | Cryptographic Operation (MACsec AES Data Encryption and Decryption) |
| | FCS_RBG_EXT.1 | Random Bit Generation |
| | FCS_IPSEC_EXT.1 | IPsec Protocol |
| | FCS_SSH_EXT.1 | SSH Protocol |
| | FCS_SSHS_EXT.1 | SSH Server Protocol |
| | FCS_MACSEC_EXT.1 | MACsec |
| | FCS_MACSEC_EXT.2 | MACsec Integrity and Confidentiality |
| | FCS_MACSEC_EXT.3 | MACsec Randomness |
| | FCS_MACSEC_EXT.4 | MACsec Key Usage |
| | FCS_MKA_EXT.1 | MACsec Key Agreement |
| FIA: Identification and authentication | FIA_AFL.1 | Authentication Failure Handling |
| | FIA_PMG_EXT.1 | Password Management |
| | FIA_UIA_EXT.1 | User Identification and Authentication |
| | FIA_UAU.7 | Protected Authentication Feedback |
| | FIA_X509_EXT.1/Rev | X.509 Certificate Validation |
| | FIA_X509_EXT.2 | X.509 Certificate Authentication |
| | FIA_X509_EXT.3 | X.509 Certificate Requests |
| | FIA_PSK_EXT.1 | Extended: Pre-Shared Key Composition |
| FMT: Security management | FMT_MOF.1/ManualUpdate | Management of security functions behaviour |
| | FMT_MTD.1/CoreData | Management of TSF Data |
| | FMT_MTD.1/CryptoKeys | Management of TSF Data |
| | FMT_SMF.1 | Specification of Management Functions |
| | FMT_SMF.1/MACSEC | Specification of Management Functions (MACsec) |
| | FMT_SMR.2 | Restrictions on Security Roles |
| FPT: Protection of the TSF | FPT_SKP_EXT.1 | Extended: Protection of TSF Data (for reading of all pre-shared, symmetric and private keys) |
| | FPT_PPW_EXT.1 | Extended: Protection of Administrator Passwords |
| | FPT_TST_EXT.1 | TSF Testing (Extended) |
| | FPT_TUD_EXT.1 | Trusted Update |
| | FPT_STM_EXT.1 | Reliable Time Stamps |
| | FPT_CAK_EXT.1 | Protection of CAK Data |
| | FPT_FLS.1 | Failure with Preservation of Secure State |
| | FPT_RPL.1 | Replay Detection |
| | FPT_RPL_EXT.1 | Replay Protection for XPN |
| FTA: TOE Access | FTA_SSL_EXT.1 | TSF-initiated Session Locking |
| | FTA_SSL.3 | TSF-initiated Termination |
| | FTA_SSL.4 | User-initiated Termination |
| | FTA_TAB.1 | Default TOE Access Banners |
| FTP: Trusted path/channels | FTP_ITC.1 | Inter-TSF trusted channel |
| | FTP_ITC.1/MACSEC | Inter-TSF Trusted Channel (MACsec Communications) |
| | FTP_TRP.1/Admin | Trusted Path |

5.2.1 Security audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

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

- a) Start-up and shut-down of the audit functions;
- b) All auditable events for the not specified level of audit; and
- c) *All administrative actions comprising:*
 - *Administrative login and logout (name of Administrator account shall be logged if individual 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 Administrator account shall be logged)];*
- d) *Specifically defined auditable events listed in Table 16.*

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

- a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
- b) For each audit event type, based on the auditable event definitions of the functional components included in the CPP/ST, *information specified in column three of Table 16.*

Table 16 Auditable Events

| SFR | Auditable Event | Additional Audit Record Contents |
|--------------------------|---|--|
| FAU_GEN.1 | None. | None. |
| FAU_GEN.2 | None. | None. |
| FAU_STG_EXT.1 | Configuration of local audit settings. | Identity of account making changes to the audit configuration. |
| 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_SSH_EXT.1 | [Failure to establish SSH connection] | [Reason for failure and Non-TOE endpoint of connection (IP Address)] |
| FCS_SSH_EXT.1 | [Establishment of SSH connection] | [Non-TOE endpoint of connection (IP Address)] |
| FCS_SSH_EXT.1 | [Termination of SSH connection session] | [Non-TOE endpoint of connection (IP Address)] |
| FCS_SSH_EXT.1 | [None] | [None] |
| FCS_SSHS_EXT.1 | No events specified | N/A |
| FCS_RBG_EXT.1 | None. | None. |
| FIA_AFL.1 | Unsuccessful login attempts limit is met or exceeded. | Origin of the attempt (e.g., IP address). |
| FIA_PMG_EXT.1 | None. | None. |
| FIA_UIA_EXT.1 | All use of the identification and authentication mechanism. | Origin of the attempt (e.g., IP address). |
| FIA_UAU.7 | None. | None. |

| SFR | Auditable Event | Additional Audit Record Contents |
|-------------------------|--|--|
| 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 |
| FMT_MTD.1/CryptoKeys | None | None |
| FMT_SMF.1 | All management activities of TSF data. | None. |
| FMT_SMR.2 | None. | None. |
| FPT_SKP_EXT.1 | None. | None. |
| FPT_APW_EXT.1 | None. | None. |
| FPT_TST_EXT.1 | None. | None. |
| FPT_TUD_EXT.1 | Initiation of update; result of the update attempt (success and failure) | 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). |
| 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. |
| FPT_ITC.1 | Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions. | None None Reason for failure |
| FTP_TRP.1/Admin | Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions. | None None Reason for failure |

5.2.1.2 FAU_GEN.2 User Identity Association

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

5.2.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

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

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

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

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

FAU_STG_EXT.1.4 The TSF shall be able to store [nonpersistent] audit records locally with a minimum storage size of [150000000 bytes].

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

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

5.2.1.4 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:

- Start-up and shutdown of the audit functions;
- All auditable events for the *[not specified]* level of audit;
- All administrative actions;**
- [Specifically defined auditable events listed in the Auditable Events table (Table 17)]***

Table 17 Auditable Events (MACSEC)

| 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:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- 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 17)]*.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation

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

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

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

5.2.2.2 FCS_CKM.2 Cryptographic Key Establishment

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

- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526]

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

5.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

- *For plaintext keys in volatile storage, the destruction shall be executed by a [single overwrite consisting of [zeroes, 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.*

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

FCS_COP.1.1/DataEncryption The TSF shall perform *encryption/decryption* in accordance with a specified cryptographic algorithm *AES used in [CBC, GCM] mode* and cryptographic key sizes [128 bits, 256 bits] that meet the following: *AES as specified in ISO 18033-3, [CBC as specified in ISO 10116, GCM as specified in ISO 19772].*

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

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

[

- RSA Digital Signature Algorithm,

]

and cryptographic key sizes [

- For RSA: modulus 2048 bits or greater,

]

that meet the following:

[

- For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

].

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

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

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

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

5.2.2.8 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, 256] bits and message digest size of 128 bits that meets the following: [NIST SP800-38B].

5.2.2.9 FCS_COP.1/MACSEC Cryptographic Operation (MACsec AES Data Encryption and 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, 256] bits that meet the following: [AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP800-38F, GCM as specified in ISO 19772].

5.2.2.10 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] software-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.

5.2.2.11 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 ESP³ 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].

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol: [

- IKEv2 as defined in RFC 7296 [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 between [2 minutes] and [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] and [720 hours];
]
].

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange (“x” in $g^x \text{ mod } p$) using the random bit generator specified in FCS_RBG_EXT.1 and having a length of at least [224 (for DH Group 14)] 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) [[14 (2048-bit MODP)] according to RFC 3526.
].

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

³ ESP – Encapsulating Security Protocol

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].

5.2.2.1 FCS_SSH_EXT.1 SSH Protocol

FCS_SSH_EXT.1.1 The TSF shall implement SSH acting as a [server] in accordance with that complies with RFCs 4251, 4252, 4253, 4254, [5647, 5656, 6668, 8332] and [no other standard].

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

- password" (RFC 4252),
- "publickey" (RFC 4252): [
 - rsa-sha2-256 (RFC 8332),
 - rsa-sha2-512 (RFC 8332),

] and no other methods.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [65806] in an SSH transport connection are dropped.

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

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

] and no other mechanisms.

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

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

] and no other mechanisms.

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

- ecdh-sha2-nistp256 (RFC 5656),
- ecdh-sha2-nistp384 (RFC 5656),

] and no other mechanisms.

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

- RFC 5656 (Section 4)

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

FCS_SSH_EXT.1.8 The TSF shall ensure that [

- a rekey of the session keys,

] occurs when any of the following thresholds are met:

- one hour connection time

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

5.2.2.2 FCS_SSHS_EXT.1 SSH Server Protocol

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

- ssh-rsa (RFC 4253),
- rsa-sha2-256 (RFC 8332),
- rsa-sha2-512 (RFC 8332),

].

5.2.2.3 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 TSF shall permit only EAPOL (Port Access Entity (PAE) EtherType 88-8E), MACsec frames (EtherType 88-E5), and [no other frame types] and shall discard others.

5.2.2.4 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.

5.2.2.5 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.

5.2.2.6 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).

5.2.2.7 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.

5.2.3 Identification and authentication (FIA)

5.2.3.1 FIA_AFL.1 Authentication Failure Handling (Refinement)

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 a remote session using any authentication method that involves a password until [unblocking action] is taken by a local 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].

5.2.3.2 FIA_PMG_EXT.1 Password Management

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

- a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["!", "@", "#", "\$", "%", "^", "&", "*", "(", ")"][Additional Special Characters listed in Table 18];

Table 18. 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 |

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

5.2.3.3 FIA_UIA_EXT.1 User Identification and Authentication

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

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

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

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

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

5.2.3.4 FIA_UAU.7 Protected Authentication Feedback

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

5.2.3.5 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [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.

5.2.3.6 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].

5.2.3.7 FIA_X509_EXT.3 X.509 Certificate Requests

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

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

5.2.3.8 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 PSKs.

5.2.4 Security Management (FMT)

5.2.4.1 FMT_MOF.1/ManualUpdate Management of Security Functions Behaviour

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

5.2.4.2 FMT_MTD.1/CoreData Management of TSF Data

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

5.2.4.3 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.

5.2.4.4 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 remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the remote session inactivity time before session termination;*
- *Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates;*
- [
 - *Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full, changes to local audit storage size);*
 - *Ability to 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 generate Certificate Signing Request (CSR) and process CA certificate response;*
 - *Ability to administer the TOE locally;*
 - *Ability to configure the authentication failure parameters for FIA AFL.1;*
 - *Ability to manage the trusted public keys database;*
 - *Ability to configure the local session inactivity time before session termination or locking*
]

5.2.4.5 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 ieee8021XKeyMkaParticipant 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]*

[

- *No other MACsec management functions*

].

5.2.4.6 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator.*

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

5.2.5 Protection of the TSF (FPT)

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

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

5.2.5.2 FPT_APW_EXT.1: Protection of Administrator Passwords

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

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

5.2.5.3 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) to verify the integrity of the TOE firmware and software;*
 - *Prior to providing any cryptographic services and [on-demand] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;*
 - *[no other]*
- to demonstrate the correct operation of the TSF.

FPT_TST_EXT.1.2 The TSF shall respond to all failures by [rebooting].

5.2.5.4 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 [the most recently installed version of the TOE firmware/software].

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.

5.2.5.5 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].

5.2.5.6 FPT_CAK_EXT.1 Protection of CAK Data

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

5.2.5.7 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]*.

5.2.5.8 FPT_RPL.1 Replay Detection

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

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

5.2.6 TOE Access (FTA)

5.2.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [
 • terminate the session]
 after a Security Administrator-specified time period of inactivity.

5.2.6.2 FTA_SSL.3 TSF-initiated Termination

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

5.2.6.3 FTA_SSL.4 User-initiated Termination

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

5.2.6.4 FTA_TAB.1 Default TOE Access Banners

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

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 FTP_ITC.1

Inter-TSF trusted channel

FTP_ITC.1.1 Refinement: The TSF shall **be capable of using [IPsec]** to provide a trusted communication channel between itself and ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, [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 ~~modification~~ disclosure and detection of modification of the channel data.

FTP_ITC.1.2 The TSF shall permit **the TSF** 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*

].

5.2.7.2 FTP_ITC.1/MACSEC Communications)

Inter-TSF trusted channel (MACsec

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*].

5.2.7.3 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** ~~users~~ that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data **from disclosure and provides detection of modification of the channel data.**

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

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

5.3 TOE SFR Dependencies Rationale for SFRs Found in NDcPP v3.0e

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPP v3.0e and MOD_MACsec v1.0. As such, the NDcPP v3.0e and MOD_MACsec v1.0 SFR dependency rationale is deemed acceptable since the PP itself has been validated.

5.4 Security Assurance Requirements

5.4.1 SAR⁴ Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPP v3.0e and MOD_MACsec v1.0, which are derived from Common Criteria Version 3.1, Revision 5, dated April 2017. The assurance requirements are summarized in Table 19 below.

Table 19 Assurance Measures

| Assurance Class | Components | Components Description |
|--------------------------------|------------|---|
| Security Target (ASE) | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_OBJ.1 | Security objectives for the operational environment |
| | ASE_REQ.1 | Stated security requirements |
| | ASE_SPD.1 | Security Problem Definition |
| | ASE_TSS.1 | TOE summary specification |
| Development (ADV) | ADV_FSP.1 | Basic Functional Specification |
| Guidance Documents (AGD) | AGD_OPE.1 | Operational user guidance |
| | AGD_PRE.1 | Preparative procedures |
| Life Cycle Support (ALC) | ALC_CMC.1 | Labeling of the TOE |
| | ALC_CMS.1 | TOE CM coverage |
| | ALC_FLR.2 | Flaw Reporting Procedures |
| Tests (ATE) | ATE_IND.1 | Independent testing - conformance |
| Vulnerability Assessment (AVA) | AVA_VAN.1 | Vulnerability survey |

5.4.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPP v3.0e and MOD_MACsec v1.0. As such, the NDcPP v3.0e and MOD_MACsec v1.0 SAR rationale is deemed acceptable since the PP itself has been validated.

5.5 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Cisco to satisfy the assurance requirements. Assurance measures are provided in Table 20 below.

Table 20 Assurance Measures

| Component | How requirement will be met |
|--|--|
| Security Target (ASE) ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.1 ASE_REQ.1 ASE_SPD.1 ASE_TSS.1 | Section 2 of this ST includes the TOE and ST conformance claim to CC Version 3.1, Revision 5, dated: April 2017, CC Part 2 extended and CC Part 3 conformant, NDcPP v3.0e and MOD_MACsec v1.0 and the rationale of how TOE provides all of the functionality at a level of security commensurate with that identified in NDcPP v3.0e and MOD_MACsec v1.0. Section 2 also includes the consistency rationale for the TOE Security Problem Definition and the Security Requirements to include the extended components definition. |

⁴ SAR – Security Assurance Requirements

| Component | How requirement will be met |
|-----------|--|
| ADV_FSP.1 | <p>The functional specification describes the external interfaces of the TOE, such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements.</p> <p>The interfaces are described in terms of their:</p> <ul style="list-style-type: none"> • purpose (general goal of the interface) • method of use (how the interface is to be used) • parameters (explicit inputs to and outputs from an interface that control the behaviour of that interface) • parameter descriptions (tells what the parameter is in some meaningful way) • error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes) <p>The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.</p> |
| AGD_OPE.1 | The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the ST. |
| AGD_PRE.1 | The Installation Guide describes the installation, generation and start-up procedures so that the users of the TOE can setup the components of the TOE into the evaluated configuration. |
| ALC_CMC.1 | The CM ⁵ document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE. |
| ALC_CMS.1 | |
| ALC_FLR.2 | Cisco will provide the flaw remediation and reporting procedures to document how TOE users can submit security flaw reports to the developer and how the security flaw reports will be appropriately acted upon. |
| ATE_IND.1 | Cisco will provide the TOE for testing. |
| AVA_VAN.1 | Cisco will provide the TOE for testing. |

⁵ CM – Configuration Management

6 TOE Summary Specification

6.1 TOE Security Functional Requirement Measures

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

Table 21 How TOE SFRs Measures

| TOE SFRs | How the SFR is Met |
|-------------------------------|---|
| FAU_GEN.1 FAU_GEN.1/MACSEC | <p>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 Table 16 and Table 17 above.</p> <p>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 type of key, and the key label. Additionally, the start-up and shut-down of the audit functionality is audited.</p> <p>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. Following is the audit record format:</p> <pre>seq no:timestamp: %facility-severity-MNEMONIC:description (hostname-n)</pre> <p>Following is an example of an audit record:</p> <pre>*Mar 1 18:46:11: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) 18:47:02: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36) *Mar 1 18:48:50.483 UTC: %SYS-5-CONFIG_I: Configured from console by vty2 (10.34.195.36)</pre> <p>The logging buffer size can be configured from a range of 4096 (default) to 2147483647 bytes. It is noted, do not make the buffer size too large because the TOE could run out of memory for other tasks. Use the show memory privileged EXEC command to view the free processor memory on the TOE. However, this value is the maximum available, and the buffer size should not be set to this amount.</p> <p>The Administrator can also configure a 'configuration logger' to keep track of configuration changes made with the command-line interface (CLI). The Administrator can configure the size of the configuration log from 1 to 1000 entries (the default is 100).</p> <p>The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging privileged EXEC command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc.</p> <p>The logs can be saved to flash memory, so records are not lost in case of failures or restarts. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.</p> <p>The Administrator can set the level of the audit records to be displayed on the console or sent to the syslog server. For instance, all emergency, alerts, critical, errors, and warning messages can be sent to the console alerting the Administrator that some action needs to be taken as these types of messages mean that the functionality of the TOE is affected. All notifications and information type message can be sent to the syslog server.</p> <p>To configure the TOE to send audit records to a syslog server, the 'set logging server' command is used. A maximum of three syslog servers can be configured. The audit records are transmitted using an IPsec tunnel to the syslog server. If communications to the syslog server are lost, the TOE will store all audit records locally and when the connection to the remote syslog server is restored, all stored audit records will be transmitted to the remote syslog server.</p> <p>Once the box is up and operational and the crypto self-test command is entered, then the result messages are displayed on the console and an audit record is generated. If the TOE encounters a failure to invoke any cryptographic function, a log record is generated.</p> |

| TOE SFRs | How the SFR is Met | | | | | | | | | | | | | | | | | | |
|---------------|--|---|-----|---------|-----|---------------------------------|--|-----|-----------------|---|--------|-----|---------|-----------|---------------------------------|--|-----------|--|--|
| | When the incoming traffic to the TOE exceeds what the interface can handle, the packets are dropped at the input queue itself and there are no error messages generated. | | | | | | | | | | | | | | | | | | |
| FAU_GEN.2 | The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. | | | | | | | | | | | | | | | | | | |
| FAU_STG_EXT.1 | <p>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 via IPsec. If the IPsec connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents to the syslog server.</p> <p>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.</p> <p>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.</p> | | | | | | | | | | | | | | | | | | |
| FCS_CKM.1 | The TOE implements and uses primes as specified in RFC 3526 Section 3 when generating parameters for the key exchange. | | | | | | | | | | | | | | | | | | |
| FCS_CKM.2 | <p>Asymmetric cryptographic keys used for IKE peer authentication are generated according to FIPS PUB 186-4, Appendix B.3 for RSA schemes.</p> <p>The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation and key establishment in the NIST SP800-56Arev3 and with section 6.</p> <p>The TOE can create an RSA public-private key pair using key sizes of 2048-bit or 3072-bit that can be used to generate a Certificate Signing Request (CSR). Through use of Simple Certificate Enrolment Protocol (SCEP), the TOE can send the CSR to a CA for the CA to generate a certificate and receive its X509v3 certificate from the CA.</p> <p>Integrity of the CSR and certificate during transit are assured through use of digital signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate).</p> <p>The key pair generation portions of "The RSA Validation System" for FIPS PUB 186-4 were used as a guide in testing the FCS_CKM.1 during the FIPS validation.</p> <p>The TOE implements EC-DH key establishment schemes in SSH remote administration. The ECC key generation meets FIPS PUB 186-4.</p> <p>The TOE implements DH group 14 (2048) bit key establishment schemes in IPsec. The DH key generation meets RFC 3526, Section 3.</p> <p>The following table shows the key generation algorithms the TOE implements for authentication:</p> <table><tr><th>Scheme</th><th>SFR</th><th>Service</th></tr><tr><td>RSA</td><td>FCS_SSH_EXT.1 FCS_SSHS_EXT.1</td><td>Authentication for Remote Administration</td></tr><tr><td>RSA</td><td>FCS_IPSEC_EXT.1</td><td>Peer Authentication for IPsec Protocol used in Remote syslog server</td></tr></table> <p>The following table shows the key establishment algorithms the TOE implements for ECC p-256 and p-384:</p> <table><tr><th>Scheme</th><th>SFR</th><th>Service</th></tr><tr><td>ECC p-256</td><td>FCS_SSH_EXT.1 FCS_SSHS_EXT.1</td><td>Key Exchange for Remote Administration</td></tr><tr><td>ECC p-384</td><td></td><td></td></tr></table> | Scheme | SFR | Service | RSA | FCS_SSH_EXT.1 FCS_SSHS_EXT.1 | Authentication for Remote Administration | RSA | FCS_IPSEC_EXT.1 | Peer Authentication for IPsec Protocol used in Remote syslog server | Scheme | SFR | Service | ECC p-256 | FCS_SSH_EXT.1 FCS_SSHS_EXT.1 | Key Exchange for Remote Administration | ECC p-384 | | |
| Scheme | SFR | Service | | | | | | | | | | | | | | | | | |
| RSA | FCS_SSH_EXT.1 FCS_SSHS_EXT.1 | Authentication for Remote Administration | | | | | | | | | | | | | | | | | |
| RSA | FCS_IPSEC_EXT.1 | Peer Authentication for IPsec Protocol used in Remote syslog server | | | | | | | | | | | | | | | | | |
| Scheme | SFR | Service | | | | | | | | | | | | | | | | | |
| ECC p-256 | FCS_SSH_EXT.1 FCS_SSHS_EXT.1 | Key Exchange for Remote Administration | | | | | | | | | | | | | | | | | |
| ECC p-384 | | | | | | | | | | | | | | | | | | | |

| TOE SFRs | How the SFR is Met | | | | | | |
|--------------------------|---|--|-----|---------|--------|-----------------|--|
| | <p>The following table shows the key establishment algorithms the TOE implements for DH-14:</p> <table><tr><th>Scheme</th><th>SFR</th><th>Service</th></tr><tr><td>FFC/DH</td><td>FCS_IPSEC_EXT.1</td><td>Key Exchange for IPsec Protocol used in Remote syslog server</td></tr></table> <p>For details on each protocol, see the related SFR.</p> | Scheme | SFR | Service | FFC/DH | FCS_IPSEC_EXT.1 | Key Exchange for IPsec Protocol used in Remote syslog server |
| Scheme | SFR | Service | | | | | |
| FFC/DH | FCS_IPSEC_EXT.1 | Key Exchange for IPsec Protocol used in Remote syslog server | | | | | |
| FCS_CKM.4 | The TOE meets all requirements specified in FIPS 140-2 for destruction of keys and Critical Security Parameters (CSPs) when no longer required for use. See section 7 below for additional details on key zeroization. | | | | | | |
| FCS_COP.1/DataEncryption | The TOE provides symmetric encryption and decryption capabilities using AES in CBC and GCM mode (128 and 256 bits) as described in ISO/IEC 18033-3 and ISO/IEC 10116. AES is implemented in the SSH and IPsec protocols. Refer to Table 4 above for the FIPS validated algorithm certificate numbers. | | | | | | |
| FCS_COP.1/SigGen | 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 Table 4 above for the FIPS validated algorithm certificate numbers. | | | | | | |
| FCS_COP.1/Hash | <p>The TOE provides cryptographic hashing services using SHA-1, SHA-256 and SHA-512 as specified in ISO/IEC 10118-3:2004 (with key sizes and message digest sizes of 160, 256, and 512 bits respectively).</p> <p>The TOE provides keyed-hashing message authentication services using HMAC-SHA-256 that operates on 512-bit blocks, with key size and message digest size of 256 as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.</p> <p>For IKE Internet Security Association and Key Management Protocol (ISAKMP) hashing, Administrators configure the SHA and message digest to be used with remote IPsec endpoints.</p> <p>SHA-256 hashing is used for verification of software image integrity.</p> <p>For IPsec Security Association (SA) authentication integrity options Administrators can select esp-sha256-hmac (HMAC-SHA-256) with message digest size of 256 to be part of the IPsec SA transform-set to be used with remote IPsec endpoints.</p> <p>For SSH remote administration, Administrators configure HMAC-SHA2-256 for MAC integrity.</p> <p>Refer to Table 4 above for the FIPS validated algorithm certificate numbers.</p> | | | | | | |
| FCS_COP.1/KeyedHash | | | | | | | |
| FCS_COP.1/CMAC | <p>The TOE implements AES-CMAC keyed hash function for message authentication as described in NIST SP800-38B.</p> <p>The key length, hash function used, block size, message digest and output MAC length used are as follows:</p> <p>AES-128 (hash function and key length) Block Sizes: Full (block size) Message Length: 0-256 bits (output MAC length)</p> <p>AES-256 (hash function and key length) Block Sizes: Full (block size) Message Length: 0-256 bits (output MAC length)</p> <p>The TOE provides symmetric encryption and decryption capabilities using AES in AES Key Wrap and GCM mode (128 bits, 256 bits) as described in AES as specified in ISO/IEC 18033-3, AES Key Wrap in CMAC mode as specified in NIST SP800-38F, GCM as specified in ISO/IEC 19772.</p> <p>AES is implemented in the MACsec protocol.</p> <p>Refer to Table 4 above for the FIPS validated algorithm certificate numbers.</p> | | | | | | |
| FCS_COP.1/MACSEC | | | | | | | |
| FCS_RBG_EXT.1 | The TOE implements a NIST-approved CTR DRBG, as specified in ISO/IEC 18031:2011 seeded by an entropy source that accumulates entropy from a software-based noise source. | | | | | | |

| TOE SFRs | How the SFR is Met |
|-----------------|--|
| | <p>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.</p> |
| FCS_IPSEC_EXT.1 | <p>The TSF implements IPsec to provide authentication and encryption services to prevent unauthorized viewing or modification of syslog 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 Encapsulating Security Payload (ESP) protocol to provide authentication, encryption and anti-replay services supporting the following algorithms:</p> <ul style="list-style-type: none"> ■ AES (AES-CBC-128 (RFC 3602), AES-CBC-256 (RFC 3602), AES-GCM-128 (RFC 5282) and AES-GCM-256 (RFC 5282) with a SHA-based HMAC (HMAC-SHA-256) to implement the IPsec protocol ESP as defined in RFC 4303. <p>The algorithms above are both for IKE and ESP.</p> <p>The TOE provides IPsec protection supporting one of two modes: 1) With a syslog server operating as an IPsec peer of the TOE (transport mode); or 2) With a syslog is not directly co-located with the TOE but is adjacent to an IPsec peer within a trusted facility, and the syslog records are tunneled over the public network (tunnel mode).</p> <p>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.</p> <p>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 remote peer to set up the necessary IPsec SAs on behalf of the data flow. The negotiation uses information specified in the crypto map entry as well as the data flow information from the specific access list entry.</p> <p>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 before being forwarded to the remote peer. The corresponding inbound SAs are used when processing the incoming traffic from that peer.</p> <p>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 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.</p> <p>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. IKE separates negotiation into two phases: phase 1 and phase 2. Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. The key negotiated in phase 1 enables IKE peers to communicate securely in phase 2. During Phase 2 IKE establishes the IPsec SA. IKE maintains a trusted channel, referred to as a Security Association (SA), between IPsec peers that is also used to manage IPsec connections, including:</p> <ul style="list-style-type: none"> ■ The negotiation of mutually acceptable IPsec options between peers (including peer authentication parameters), ■ 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. <p>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 phase 2 symmetric algorithm key strength is at most as large as the negotiated phase 1 key strength as configured on the TOE and peer via an explicit check.</p> |

| TOE SFRs | How the SFR is Met |
|----------------|---|
| | <p>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.</p> <p>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 assigns a unique priority (1 through 10,000, with 1 being the highest priority).</p> <p>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.</p> <p>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.</p> <p>The TOE supports IKEv2 session establishment. The TOE supports configuration of session lifetimes for both Phase 1 SAs and Phase 2 SAs using the following the command "lifetime." The time values for Phase 1 SAs can be limited from 2 minutes to 24 hours and for Phase 2 SAs up to 8 hours. The Phase 2 SA lifetimes can also be configured by an Administrator based on number of bytes. The TOE supports Diffie-Hellman Group 14.</p> <p>The TSF generates the secret value 'x' used in the IKEv2 Diffie-Hellman key exchange ('x' in $g^x \text{ mod } p$) 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 of a specific IPsec SA is less than $1 \text{ in } 2^{128}$. The nonce is likewise generated using the CTR DRBG.</p> <p>The TOE supports authentication of IPsec peers using RSA X.509 certificates. For peer authentication using RSA certificates, the TOE validates the presented identifier provided supporting the following fields and types: SAN: IP address, SAN: Fully Qualified Domain Name (FQDN).</p> <p>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></p> <p>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.</p> |
| FCS_SSHS_EXT.1 | <p>The TOE implementation of SSHv2 supports the following:</p> <p>The TSF implements SSHv2 conformant to RFCs 4251, 4252, 4253, 4254 5647, 5656, 6668, and 8332 to provide a secure command line interface for remote administration. The TOE supports public-key authentication with ssh-rsa public key algorithm and password-based authentication methods.</p> <p>SSHv2 connections will be dropped if the TOE receives a packet larger than 65806 bytes. Large packets are detected by the SSHv2 implementation and dropped internal to the SSH process.</p> <p>The TSF's SSH transport implementation supports the following encryption algorithms:</p> <ul style="list-style-type: none"> ■ aes128-cbc ■ aes256-cbc ■ aes128-gcm@openssh.com ■ aes256-gcm@openssh.com |

| TOE SFRs | How the SFR is Met |
|------------------|--|
| | <p>All connection attempts from remote SSH clients requesting any other encryption algorithm is denied.</p> <p>The TSF's SSH transport implementation supports the following MAC algorithms with aes-cbc encryption algorithms:</p> <ul style="list-style-type: none"> ■ hmac-sha2-256 <p>When aes128-gcm@openssh.com or aes256-gcm@openssh.com is used as the encryption algorithm the MAC algorithm is implicit.</p> <p>All connection attempts from remote SSH clients requesting any other MAC algorithm is denied.</p> <p>The TSF's SSH transport implementation supports the following Hostkey authentication algorithms:</p> <ul style="list-style-type: none"> ■ ssh-rsa ■ rsa-sha2-256 ■ rsa-sha2-512 <p>The TSF's SSH transport implementation supports the following public-key algorithms for Client Authentication:</p> <ul style="list-style-type: none"> ■ rsa-sha2-256 ■ rsa-sha2-512 <p>The public-key algorithm is consistent with the RSA digital signature algorithm in FCS_COP.1/SigGen.</p> <p>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.</p> <p>The TSF's SSH key exchange implementation supports the following key exchange algorithm:</p> <ul style="list-style-type: none"> ■ ecdh-sha2-nistp256 ■ ecdh-sha2-nistp384 <p>The TOE derives cryptographic session keys via shared secret using SSH KDF as defined in RFC 5656 (Section 4).</p> <p>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.</p> <p>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.</p> |
| FCS_MACSEC_EXT.1 | <p>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.</p> <p>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.</p> <p>Only Extensible Authentication Protocol over LAN (EAPOL) (Physical Address Extension (PAE) EtherType 88-8E) and MACsec frames (EtherType 88-E5), are permitted. All others are rejected.</p> |

| TOE SFRs | How the SFR is Met |
|------------------|---|
| FCS_MACSEC_EXT.2 | <p>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.</p> <p>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.</p> <p>An Integrity Check Value (ICV) of 16-bytes derived with the SAK is used to provide assurance of the integrity of MPDUs.</p> <p>The TOE derives the ICV 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.</p> |
| FCS_MACSEC_EXT.3 | <p>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.</p> <p>Each of the keys used by MKA is derived from the CAK.</p> <p>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.</p> <p>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.</p> <p>The size of the key is based on the configured AES key sized used. If using AES 128-bit CMAC mode encryption, the key string will be 32-bit hexadecimal in length. If using 256-bit encryption, the key string will be 64-bit hexadecimal in length.</p> |
| FCS_MACSEC_EXT.4 | <p>MACsec peer authentication is achieved by only using pre-shared keys.</p> <p>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.</p> <p>The 'Key-chain macsec lifetime' configuration command is used to specify the lifetime for CAKs.</p> <p>The 'MACSEC Key-chain key' command is used to specify the length of the CKN. The CKN can be set between 1 and 32 octets.</p> |
| FCS_MKA_EXT.1 | <p>The TOE implements the MKA Protocol in accordance with IEEE 802.1X-2010 and 802.1Xbx-2014.</p> <p>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.</p> <p>The TOE discards MACsec Key Agreement Protocol Data Units (MKPDUs) that do not satisfy the requirements listed under FCS_MKA_EXT.1.8 in Section 5.2.2.7. All valid MKPDUs that meet the requirements as defined under FCS_MKA_EXT.1.8 are decoded in a manner conformant to IEEE 802.1x-2010 Section 11.11.4.</p> <p>On successful peer authentication, a connectivity association is formed between the peers and a secure Connectivity Association Key Name (CKN) is exchanged. After the exchange, the MKA ICV is validated with a Connectivity Association Key (CAK), which is effectively a secret key.</p> <p>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; otherwise, it is dropped. The key string is the CAK that is used for ICV validation by the MKA protocol.</p> <p>The Key Server generates a new group CAK when CLI management commands are executed. The Key Server distributes a SAK by pairwise CAKs.</p> |

| TOE SFRs | How the SFR is Met | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|-------------------|--|-------------------|------|--|-------|---|-----------|---|-------|---|--------------|---|--------------|--|--------------|---|------|---|-------|---|------------|---|--------|---|-------|---|-------|---|-----------|---|-----------|---|--------------|---|------------|
| FIA_AFL.1 | <p>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.</p> <p>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.</p> <p>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.</p> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| FIA_PMG_EXT.1 | <p>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 the table below. Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths of 1 character and maximum of 127 characters. A minimum password length of 8 is recommended.</p> <table border="1"> <thead> <tr> <th>Special Character</th><th>Name</th></tr> </thead> <tbody> <tr> <td></td><td>Space</td></tr> <tr> <td>;</td><td>Semicolon</td></tr> <tr> <td>:</td><td>Colon</td></tr> <tr> <td>"</td><td>Double Quote</td></tr> <tr> <td>'</td><td>Single Quote</td></tr> <tr> <td> </td><td>Vertical Bar</td></tr> <tr> <td>+</td><td>Plus</td></tr> <tr> <td>-</td><td>Minus</td></tr> <tr> <td>=</td><td>Equal Sign</td></tr> <tr> <td>.</td><td>Period</td></tr> <tr> <td>,</td><td>Comma</td></tr> <tr> <td>/</td><td>Slash</td></tr> <tr> <td>¥</td><td>Backslash</td></tr> <tr> <td><</td><td>Less Than</td></tr> <tr> <td>></td><td>Greater Than</td></tr> <tr> <td>_</td><td>Underscore</td></tr> </tbody> </table> | 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 |
| 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 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| TOE SFRs | How the SFR is Met | | | | | | | | |
|--|---|---|-------------------------|---|-------|---|------------|---|-------------|
| | <table> <tr> <td data-bbox="542 226 984 296">`</td><td data-bbox="984 226 1425 296">Grave accent (backtick)</td></tr> <tr> <td data-bbox="542 296 984 359">~</td><td data-bbox="984 296 1425 359">Tilde</td></tr> <tr> <td data-bbox="542 359 984 422">{</td><td data-bbox="984 359 1425 422">Left Brace</td></tr> <tr> <td data-bbox="542 422 984 491">}</td><td data-bbox="984 422 1425 491">Right Brace</td></tr> </table> | ` | Grave accent (backtick) | ~ | Tilde | { | Left Brace | } | Right Brace |
| ` | Grave accent (backtick) | | | | | | | | |
| ~ | Tilde | | | | | | | | |
| { | Left Brace | | | | | | | | |
| } | Right Brace | | | | | | | | |
| FIA_UIA_EXT.1 | <p>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. Network packets, as configured by the Authorized Administrator, may flow through the switch without a user being logged in to the device.</p> <p>Administrative access to the TOE is facilitated through the TOE's CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 secured connection, the TOE prompts the user for a username and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is granted to the administrative functionality of the TOE until an Administrator is successfully identified and authenticated.</p> <p>The TOE provides a local password-based authentication mechanism.</p> <p>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.</p> <p>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.</p> | | | | | | | | |
| FIA_UAU.7 | <p>When a user enters their password at the local console, the TOE does not echo any characters as the password is entered.</p> <p>For remote session authentication, the TOE does not echo any characters as they are entered.</p> | | | | | | | | |
| FIA_X509_EXT.1/Rev | <p>The TOE uses X.509v3 certificates to support authentication for IPsec connections. The TSF determines the validity of certificates at the time of peer authentication 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 certificates have the basicConstraints extension and the CA flag is set to TRUE and the certificate path must terminate with a trusted CA certificate.</p> <p>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.</p> <p>As OCSP revocation checking is not supported, the OCSP signing purpose is not checked in the extendedKeyUsage field and thus is trivially satisfied by the TOE.</p> | | | | | | | | |
| FIA_X509_EXT.2 | <p>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 connection will be rejected.</p> | | | | | | | | |
| FIA_X509_EXT.3 | <p>A Certificate Request Message can be generated as specified by RFC 2986 and provide the following information in the request – CN, O, OU, and Country. The TOE can validate the chain of certificates from the Root CA when the CA Certificate Response is received.</p> | | | | | | | | |
| FIA_PSK_EXT.1 | <p>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 or 64 characters in length.</p> | | | | | | | | |
| FMT_MOF.1/ManualUpdate FMT_MOF.1/Services FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys | <p>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</p> | | | | | | | | |

| TOE SFRs | How the SFR is Met |
|-----------|---|
| | <p>roles has create (set), query, modify, or delete access to the TOE data, though with some privilege levels, the access is limited.</p> <p>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.</p> <p>See FMT_SMF.1 for services only the Security Administrator can start and stop. Management functionality of the TOE is provided through the TOE CLI. Refer to the <i>Cisco Catalyst Industrial Ethernet 9300 Rugged Series Switches running IOS-XE 17.15 Common Criteria Configuration Guide</i> for information on how the Security Administrator can stop, start, and configure services.</p> <p>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.</p> <p>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.</p> <p>The TOE does not provide automatic updates to the software version running on the TOE.</p> <p>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.</p> <p>The Authorized Administrator generates RSA key pairs to be used in the IKE and SSH protocols. Zeroization of these keys is provided in Table 22 below.</p> <p>In addition, network packets are permitted to flow, as configured by the Authorized Administrator, through the TOE prior to the identification and authentication of an Authorized Administrator. The warning and access banner may also be displayed prior to the identification and authentication of an Authorized Administrator. However, no administrative functionality is available prior to administrative login. TOE Administrators can control (generate/delete) the following keys, IKE RSA Key Pairs and SSH RSA Key Pairs by following the instruction in the AGD.</p> |
| FMT_SMF.1 | <p>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.</p> <p>The specific management capabilities available from the TOE include:</p> <ul style="list-style-type: none"> • Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above • The ability to manage the warning banner message and content which allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session • The ability to set and modify the time limits of session inactivity • The ability to update the IOS-XE software. The validity of the image is provided using SHA-256 and/or digital signature prior to installing the update: • The ability to configure the number of failed Administrator logon attempts that will cause the account to be locked until it is reset • The ability to manage audit behaviour and the audit logs which allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs • The ability to manage 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 |

| TOE SFRs | How the SFR is Met |
|------------------|---|
| | <ul style="list-style-type: none"> • The ability to configure the IPsec functionality which supports the secure connections to the audit server • The ability to manually unlock a locked account • 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 • The ability to start and stop the audit service through the CLI • The ability to import the X.509v3 certificates and validate for use in authentication and secure connections • The ability to configure the local session inactivity time before session termination or locking |
| FMT_SMF.1/MACSEC | <p>The TOE provides all necessary capabilities related to MACsec functionality to securely manage the TOE and the services provided by the TOE. The management functionality related to MACsec of the TOE is provided through the TOE CLI. The Authorized Administrator can perform all management functions related to MACsec functionality by accessing the TOE directly via connected console cable or remote administration via SSHv2 secure connection.</p> <p>The specific management capabilities related to MACsec functionality available from the TOE include:</p> <ul style="list-style-type: none"> • The ability to generate a PSK and install in the CAK cache • The ability to manage the Key Server and associated MKA participants • 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 initiate the generation of a new CAK from the Key Server |
| FMT_SMR.2 | <p>The TOE maintains privileged and semi-privileged Administrator roles.</p> <p>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.</p> <p>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.</p> <p>The privilege level determines the functions the user can perform, hence the Authorized Administrator with the appropriate privileges.</p> <p>The TOE can and shall be configured to authenticate all access to the command line interface using a username and password.</p> <p>The TOE supports both local administration via a directly connected console cable and remote administration via SSHv2 secure connection.</p> |
| FPT_SKP_EXT.1 | <p>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.</p> |
| FPT_APW_EXT.1 | <p>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.</p> <p>The CC Configuration Guide instructs the Administrator to use the algorithm-type sha256 or scrypt sub-command when passwords are created or updated. The SHA256 sub-command is password type 8 while scrypt is password type 9. Both password types use SHA-2.</p> |
| FPT_TST_EXT.1 | <p>The TOE runs a suite of self-tests during initial start-up to verify its correct operation. For testing of the TSF, the TOE automatically runs checks and tests at start-up, during resets and periodically during normal operation to ensure the TOE is operating correctly, including checks of image integrity and all cryptographic functions.</p> <p>During the system bootup process (power on or reboot), all the Power on Self Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software).</p> <p>The TOE performs the following tests:</p> <p>AES Known Answer Test:</p> |

| TOE SFRs | How the SFR is Met |
|---------------|---|
| | <p>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.</p> <p><i>RSA Signature Known Answer Test (both signature/verification):</i> 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.</p> <p><i>RNG/DRBG Known Answer Test:</i> 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.</p> <p><i>HMAC Known Answer Test:</i> 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.</p> <p><i>Software Integrity Test:</i> The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that is about to be loaded has maintained its integrity. The software contains a SHA-512 hash. This hash is compared to a pre-loaded hash. If the hash values match, the test passes; otherwise, the test fails.</p> <p><i>SHA-1/256/512 Known Answer Test:</i> 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.</p> <p>If any component reports failure for the POST, the system crashes. Appropriate information is displayed on the screen and saved in the crashinfo file.</p> <p>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.</p> <p>If an error occurs during the self-test, a SELF_TEST_FAILURE system log is generated.</p> <p>Example Error Message: _FIPS-2-SELF_TEST_IOS_FAILURE: "IOS crypto FIPS self-test failed at %s." Explanation FIPS self-test on IOS crypto routine failed.</p> <p>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.</p> |
| FPT_TUD_EXT.1 | <p>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 software.cisco.com.</p> <p>A digital signature is used to verify software files (to ensure they have not been modified from the originals distributed by Cisco) before loading. If the integrity check fails, the software is not loaded and the system reboots to attempt the test again. If the test continues to fail, the Authorized Administrator must contact Cisco. If the integrity check is successful, the software is loaded and the device continues with the bootup process.</p> <p>To verify the digital signature prior to installation, the "show software authenticity file" command displays software authentication related information that includes image credential information, key type used for verification, signing information, and other attributes in the signature envelope, for a specific image file. If the output from the "show software authenticity file" command does not provide the expected output, contact Cisco TAC.</p> |

| TOE SFRs | How the SFR is Met |
|----------------------------|---|
| | <p>The software image can be installed in one step or in multiple stages, loading the image first and then installing. The loaded but not yet installed image can be queried using the “show active install” command.</p> <p>Once the integrity check is complete, the power-on self-tests are executed. If the power-on self-tests are successful, the TOE continues to load into an operational state. If a power-on self-test fails, the TOE automatically reboots to attempt to clear the error state. The TOE will continue to reboot until the error is cleared and the device is operational. If the error persists, the Authorized Administrator must contact Cisco.</p> |
| FPT_STM_EXT.1 | <p>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.</p> <p>The TOE relies upon date and time information for the following security functions:</p> <ul style="list-style-type: none"> ■ 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, FIA_X509_EXT.1/ITT); ■ To determine when SSH session keys have expired and to initiate a rekey (FCS_SSHS_EXT.1); ■ 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); ■ To provide accurate timestamps in audit records (FAU_GEN.1.2). |
| FPT_CAK_EXT.1 | <p>During the setup and configuration of the TOE and the MACsec functionality, the Authorized Administrator issues the command – “service password – encryption”. This prevents the CAK value from being shown in clear text to the Administrators on the CLI when the “show run” output is displayed.</p> <p>In addition, CAK data is stored in a secure directory that is not readily accessible to an Administrator.</p> |
| FPT_FLS.1 | <p>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 attains a secure/safe state by securely disabling its interfaces to prevent the unintentional flow of any information to or from the TOE and reloads.</p> <p>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 should contact Cisco Technical Assistance Center (TAC).</p> |
| FPT_RPL.1 | <p>Replayed data is discarded by the TOE and the attempt to replay data is logged.</p> <p>MKPDUs are replay protected in the TOE. The MKA frames are guarded against replay, such that if a MKPDU contains a duplicate Member Number (MN) and not the most current MN, then this MKPDU will be dropped and not processed further. In addition, the attempt to replay data is logged.</p> |
| FTA_SSL_EXT.1 FTA_SSL.3 | <p>An Authorized Administrator can configure maximum inactivity times individually for both local and remote administrative sessions using the “session-timeout” setting applied to the console and virtual terminal (vty) lines.</p> <p>The configuration of the vty lines sets the configuration for the remote console access.</p> <p>The line console settings are not immediately activated for the current session. The current line console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session. If a local user session is inactive for a configured period, 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.</p> <p>Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the “exec-timeout” setting.</p> |

| TOE SFRs | How the SFR is Met | | | |
|-------------------------------|--|--------------------------------|--|---------------------------------|
| | The allowable inactivity timeout range is from 1 to 35791 minutes. | | | |
| FTA_SSL.4 | An Authorized Administrator can exit out of both local and remote administrative sessions by issuing the ‘exit’ command. | | | |
| FTA_TAB.1 | 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. | | | |
| FTP_ITC.1 FTP_ITC.1/MACSEC | The TOE uses secure protocols to provide trusted communications between itself and authorized IT entities as specified in the table below: | | | |
| | IT Entity | TOE Acting as Client or Server | Secure Communication Mechanism/ Protocol | Non-TSF Endpoint Identification |
| | Syslog Server | Client | IPsec | X.509 Certificate |
| | MACsec Peer | Client or Server | MACsec | Pre-Shared Key |
| FTP_TRP.1/Admin | All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption. The remote users (Authorized Administrators) can initiate SSHv2 communications with the TOE. | | | |

7 Annex A: Key Zeroization

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

Table 22 TOE Key Zeroization

| Name | Description | Zeroization |
|--------------------------------|---|--|
| DH Shared Secret | The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0's. This key is stored in Dynamic Random-Access Memory (DRAM). | Automatically after completion of DH exchange. Overwritten with: 0x00 |
| DH private exponent | This is the private exponent used as part of the Diffie-Hellman key exchange. This key is stored in DRAM. | Zeroized upon completion of DH exchange. Overwritten with: 0x00 |
| skeyid | This is an IKE intermittent value used to create skeyid_d. This information is stored in DRAM. | Automatically after IKE session terminated. Overwritten with: 0x00 |
| skeyid_d | This is an IKE intermittent value used to derive keying data for IPsec. This information is stored in DRAM. | Automatically after IKE session terminated. Overwritten with: 0x00 |
| IKE session encrypt key | This the key IPsec key used for encrypting the traffic in an IPsec connection. This key is stored in DRAM. | Automatically after IKE session terminated. Overwritten with: 0x00 |
| IKE session authentication key | This the key IPsec key used for authenticating the traffic in an IPsec connection. This key is stored in DRAM. | Automatically after IKE session terminated. Overwritten with: 0x00 |
| ISAKMP preshared | This is the configured pre-shared key for ISAKMP negotiation. This key is stored in NVRAM. | Zeroized using the following command: # no crypto isakmp key ⁶ Overwritten with: 0x00 |
| IKE RSA Private Key | The RSA private-public key pair is created by the device itself using the key generation CLI described below. The device's public key must be added into the device certificate. The device's certificate is created by creating a trustpoint on the device. This trustpoint authenticates with the CA server to get the CA certificate and to enrol with the CA server to generate the device certificate. In the IKE authentication step, the device's certificate is first sent to another device so that it can be authenticated. The other device verifies the certificate is signed by CA's signing key, and then the device sends a random secret encrypted by the device's public key in the valid device certificate. Thus, establishing the | Zeroized using the following command: # crypto key zeroize rsa ⁷ Overwritten with: 0x00 |

⁶ Using this command will zeroize all isakmp keys.

⁷ Using this command will zeroize all RSA keys.

| Name | Description | Zeroization |
|----------------------------------|--|---|
| | trusted connection since only the device with the matching device private key can decrypt the message and obtain the random secret. This key is stored in NVRAM. | |
| IPsec encryption key | This is the key used to encrypt IPsec sessions. This key is stored in DRAM. | Automatically when IPsec session terminated. Overwritten with: 0x00 |
| IPsec authentication key | This is the key used to authenticate IPsec sessions. This key is stored in DRAM. | Automatically when IPsec session terminated. Overwritten with: 0x00 |
| MACsec SAK | The SAK is used to secure the control plane traffic. This key is stored in 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. This key is stored in 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). This key is stored in 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. This key is stored in internal ASIC register. | Automatically when MACsec session terminated. The value is zeroized by overwriting with another key or freed when the session expires. |
| SSH Private Key | Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents). This key is stored in NVRAM. | Zeroized using the following command: # crypto key zeroize rsa ⁸ Overwritten with: 0x00 |
| SSH Session Key | Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents). This key is stored in DRAM. | Automatically when the SSH session is terminated. Overwritten with: 0x00 |

⁸ Using this command will zeroize all RSA keys

8 Annex B: Acronyms

Table 23 below provides a list of acronyms and abbreviations that are common and may be used in this Security Target.

Table 23 Acronyms

| Acronyms / Abbreviations | Definition |
|--------------------------|---|
| AAA | Administration, Authorization, and Accounting |
| AC | Alternating Current |
| ACL (acl) | Access Control Lists |
| AES | Advanced Encryption Standard |
| AGD | Guidance Document |
| APT | Adaptive Proportion Test |
| ASCII | American Standard Code for Information Interchange |
| ASIC | Application Specific Integrated Circuit |
| CA | Connectivity Association |
| CAK | (Secure) Connectivity Association Key |
| CAVP | Cryptographic Algorithm Validation Program |
| CBC | Cipher Block Chaining |
| CC | Common Criteria for Information Technology Security Evaluation |
| CDP | CRL Distribution Point |
| CEM | Common Evaluation Methodology for Information Technology Security |
| CKN | Secure Connectivity Association Key Name |
| CLI | Command Line Interface |
| CM | Configuration Management |
| CMAC | Cipher Based Message Authentication Code |
| CPU | Central Processing Unit |
| CRL | Certificate Revocation List |
| CS | Certificate Server |
| CSP | Critical Security Parameter |
| CSR | Certificate Signing Request |
| CTR | Counter |
| CVL | Component Validation List |
| DH | Diffie-Hellman |
| DHCP | Dynamic Host Configuration Protocol |
| DM | Division Multiplexing |
| DN | Distinguished Name |
| DRAM | Dynamic Random-Access Memory |
| DRBG | Deterministic Random Bit Generator |
| DW | Dense Wavelength |
| EAP | Extensible Authentication Protocol |
| EAP-TLS | EAP Transport Layer Security |
| EAPOL | EAP over LANs |
| EEPROM | Electrically Erasable Programmable Read-Only Memory |
| EHWIC | Ethernet High-Speed WIC |
| ESP | Encapsulating Security Payload |
| FFC | Finite Field Cryptography |
| FQDN | Fully Qualified Domain Name |
| FRU | Field Replaceable Unit |
| GB | Giga Byte |
| GCM | Galois Counter Mode |
| GE | Gigabit Ethernet port |
| GUI | Graphical User Interface |
| HMAC | Hash-based Message Authentication Code |
| HTTP | Hypertext Transfer Protocol |
| HTTPS | HTTP Secure |
| IC2M | IOS Common Cryptographic Module |
| ICK | Integrity Check Key |
| ICMP | Internet Control Message Protocol |

| Acronyms / Abbreviations | Definition |
|-----------------------------|---|
| ICV | Integrity Check Value |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IFS | IOS-XE File System |
| IGMP | Internet Group Management Protocol |
| IKE | Internet Key Exchange |
| IOS | Internetworking Operating System |
| IP | Internet Protocol |
| IPsec | IP Security |
| ISAKMP | Internet Security Association and Key Management Protocol |
| ISDN | Integrated Services Digital Network |
| ISO | International Organization of Standardization |
| IT | Information Technology |
| KDF | Key Derivation Function |
| KEK | Key Encryption Key |
| KAS | Key Agreement Scheme |
| KAS-SSC | KAS-Shared Secret Computation |
| KW | Key Wrap |
| LC | Lucent Connector |
| MAC | Media Access Control |
| MACsec | MAC Security |
| MKA | MACsec Key Agreement protocol |
| MKPDU | MACsec Key Agreement Protocol Data Unit |
| MN | Member Number |
| MPDU | MAC Protocol Data Unit |
| MSAP | MAC Service Access Point |
| MSC | MACsec Controller |
| MSDU | MAC Service Data Unit |
| MSK | Master Session Key |
| NDcPP | collaborative Network Device Protection Profile |
| NIST | National Institute of Standards and Technology |
| NVRAM | Non-Volatile Random-Access Memory |
| OCS | Online Certificate Status Protocol |
| OS | Operating System |
| OSI | Open System Interconnection |
| OSP | Organizational Security Policies |
| PAE | Physical Address Extension |
| PC | Personal Computer |
| PKCS | Public Key Cryptography Standard |
| PoE | Power over Ethernet |
| POST | Power-on Self-Test |
| PP | Protection Profile |
| PRNG | Pseudo Random Number Generator |
| PSK | Pre-Shared Key |
| PUB | Publication |
| RA | Registration Authority |
| RADIUS | Remote Authentication Dial-In User Service |
| RCT | Repetition Count Test |
| RFC | Request for Comment |
| RJ | Registered Jack |
| RNG | Random Number Generator |
| ROM | Read-Only Memory |
| RSA | Rivest, Shamir and Adleman |
| SA | Security Association |
| SAK | Secure Association Key |
| SAR | Security Assurance Requirement |
| SATA | Serial Advanced Technology Attachment |
| SC | Secure Channel |
| SCI | Secure Channel Identifier |

| Acronyms / Abbreviations | Definition |
|-----------------------------|---|
| SCEP | Simple Certificate Enrollment Protocol |
| SCI | Secure Channel Identifier |
| SecTAG | MAC Security TAG |
| SecY | MAC Security Entity |
| SFP | Small-Form-Factor Pluggable Port |
| SFR | Security Functional Requirement |
| SHA | Secure Hash Algorithm |
| SM | Service Module |
| SNMP | Simple Network Management Protocol |
| SP | Special Publication |
| SPD | Security Policy Definition |
| SSD | Solid State Drive |
| SSHv2 | Secure Shell (version 2) |
| ST | Security Target |
| TAC | Technical Assistance Center |
| TCP | Transport Control Protocol |
| TCP/IP | Transmission Control Protocol/Internet Protocol |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |
| TSC | TSF Scope of Control |
| TSF | TOE Security Function |
| TSP | TOE Security Policy |
| UADP | Unified Access Data Plane |
| UDP | User Datagram Protocol |
| U.S. | United States |
| USB | Universal Serial Bus |
| UTP | Universal Twisted Pair |
| VPN | Virtual Private Network |

9 Annex C: Terminology

Table 24 below provides a list of terms that are common and may be used in this Security Target.

Table 24 Terminology

| Term | Definition |
|--|--|
| Authorized Administrator | Any user that has been assigned to a privilege level that is permitted to perform all TSF-related functions. |
| IOS-XE | Proprietary operating system developed by Cisco Systems. |
| Peer | Another switch on the network that the TOE interfaces. |
| MACsec Peer | This includes any MACsec peer with which the TOE participates in MACsec communications. MACsec Peer may be any device that supports MACsec communications |
| Packet | A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message. |
| Remote VPN Gateway/Peer | A remote VPN Gateway/Peer is another network device that the TOE sets up a VPN connection with. This could be a VPN client or another switch. |
| Security Administrator | Synonymous with Authorized Administrator for the purposes of this evaluation. |
| User | Any entity (human user or external IT entity) outside the TOE that interacts with the TOE. |
| vty | vty is a term used by Cisco to describe a single terminal (whereas Terminal is more of a verb or general action term). |
| Firmware (per NIST for FIPS validated cryptographic modules) | The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution. |

10 Annex D: References

Documentation listed in Table 25 below was used to prepare this ST.

Table 25 References

| Identifier | Description |
|------------------|---|
| [CC_PART1] | Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 5, dated: April 2017 |
| [CC_PART2] | Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 5, dated: April 2017 |
| [CC_PART3] | Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 5, dated: April 2017 |
| [CEM] | Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Version 3.1, Revision 5, dated: April 2017 |
| [NDcPP] | collaborative Protection Profile for Network Devices, Version NDcPP v3.0e, 23 March 2020 |
| [MOD_MACsec] | PP-Modulefor MACsec Ethernet Encryption, Version 1.0, 02 March 2023 |
| [800-38B] | NIST Special Publication 800-38B, May 2005 |
| [800-56Arev3] | NIST Special Publication 800-56Arev3, April 2018 |
| [FIPS 140-2] | FIPS PUB 140-2 Federal Information Processing Standards Publication |
| [FIPS PUB 186-4] | FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS) October 2015 |
| [800-90Brev1] | NIST Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation January 2018 |