



Cisco Expressway X12.5 System Common Criteria Security Target

Version 1.5

19 February 2020



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

© 2020 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

Table of Contents

1	SECURITY TARGET INTRODUCTION.....	8
1.1	ST and TOE Reference	8
1.2	TOE Overview	8
1.2.1	TOE Product Type	8
1.2.2	Supported non-TOE Hardware/ Software/ Firmware	9
1.3	TOE DESCRIPTION.....	9
1.4	TOE Evaluated Configuration	14
1.5	Physical Scope of the TOE.....	14
1.6	Logical Scope of the TOE.....	18
1.6.1	Security Audit	19
1.6.2	Communications	19
1.6.3	Cryptographic Support.....	19
1.6.4	Identification and authentication	21
1.6.5	Security Management	21
1.6.6	Protection of the TSF	21
1.6.7	TOE Access	22
1.6.8	Trusted path/Channels.....	22
1.7	Excluded Functionality	22
2	Conformance Claims.....	24
2.1	Common Criteria Conformance Claim	24
2.2	Protection Profile Conformance	24
2.2.1	Protection Profile Additions	30
2.3	Protection Profile Conformance Claim Rationale	30
2.3.1	TOE Appropriateness.....	30
2.3.2	TOE Security Problem Definition Consistency.....	30
2.3.3	Statement of Security Requirements Consistency	30
3	SECURITY PROBLEM DEFINITION.....	32
3.1	Assumptions	32
3.2	Threats.....	33
3.3	Organizational Security Policies.....	35
4	SECURITY OBJECTIVES	36
4.1	Security Objectives for the TOE.....	36
4.2	Security Objectives for the Environment	36
5	SECURITY REQUIREMENTS	37
5.1	Conventions.....	37
5.2	TOE Security Functional Requirements	37
5.2.1	Security audit (FAU).....	39
5.2.2	Communications (FCO).....	41
5.2.3	Cryptographic Support (FCS).....	41
5.2.4	Identification and authentication (FIA).....	46
5.2.5	Security management (FMT)	48
5.2.6	Protection of the TSF (FPT).....	49
5.2.7	TOE Access (FTA)	50

5.2.8 Trusted Path/Channels (FTP)51

5.3 TOE SFR Dependencies Rationale for SFRs Found in NDcPPv2.0e52

5.4 Security Assurance Requirements52

5.4.1 SAR Requirements.....52

5.4.2 Security Assurance Requirements Rationale53

5.5 Assurance Measures53

6 TOE Summary Specification56

6.1 TOE Security Functional Requirement Measures56

7 Annex A: Key Zeroization70

7.1 Key Zeroization70

8 Annex B: References.....71

List of Tables

TABLE 1 ACRONYMS.....	5
TABLE 2 TERMINOLOGY.....	6
TABLE 3 ST AND TOE IDENTIFICATION.....	8
TABLE 4 IT ENVIRONMENT COMPONENTS	9
TABLE 5 HARDWARE MODELS AND SPECIFICATIONS.....	15
TABLE 6 FIPS REFERENCES.....	19
TABLE 7 EXCLUDED FUNCTIONALITY	23
TABLE 8 TECHNICAL DECISIONS (TD).....	24
TABLE 9 PROTECTION PROFILES	30
TABLE 10 TOE ASSUMPTIONS.....	32
TABLE 11 THREATS	33
TABLE 12 ORGANIZATIONAL SECURITY POLICIES.....	35
TABLE 13 SECURITY OBJECTIVES FOR THE ENVIRONMENT.....	36
TABLE 14 SECURITY FUNCTIONAL REQUIREMENTS.....	37
TABLE 15 AUDITABLE EVENTS	39
TABLE 16: ASSURANCE MEASURES	53
TABLE 17 ASSURANCE MEASURES	54
TABLE 18 HOW TOE SFRS MEASURES	56
TABLE 19: TOE KEY ZEROIZATION	70
TABLE 20: REFERENCES.....	71

List of Figures

FIGURE 1 CISCO UCS C220 M4 SERVER.....	10
FIGURE 2 CISCO UCS C240 M4 SERVER.....	10
FIGURE 3 CISCO UCS C220 M5 SERVER.....	11
FIGURE 4 CISCO UCS C240 M5 SERVER.....	11
FIGURE 5 TOE EXAMPLE DEPLOYMENT	13

Acronyms

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

Table 1 Acronyms

Acronyms / Abbreviations	Definition
AAA	Administration, Authorization, and Accounting
AES	Advanced Encryption Standard
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
GCM	Galois Counter Mode
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IT	Information Technology
NDcPP	collaborative Network Device Protection Profile
OS	Operating System
Packet	A block of data sent over the network transmitting the identities of the sending and receiving stations, error-control information, and message.
PP	Protection Profile
PRNG	Pseudo Random Number Generator
RADIUS	Remote Authentication Dial In User Service
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman (algorithm for public-key cryptography)
SHS	Secure Hash Standard
SSHv2	Secure Shell (version 2)
ST	Security Target
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
XMPP	Extensible Messaging and Presence Protocol

Terminology

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

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user that has been assigned administrative privileges is permitted to perform TSF-related functions.
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.
Firmware (per NIST for FIPS validated cryptographic modules)	The programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

DOCUMENT INTRODUCTION

Prepared By:

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco Expressway X12.5 system. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE, which meet the set of requirements. Administrators of the TOE may be referred to as administrators, Authorized Administrators, TOE administrators and security administrators in this document.

1 SECURITY TARGET INTRODUCTION

The Security Target contains the following sections:

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

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

1.1 ST and TOE Reference

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

Table 3 ST and TOE Identification

Name	Description
ST Title	Cisco Expressway X12.5 System Common Criteria Security Target
ST Version	1.5
Publication Date	19 February 2020
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Expressway X12.5
TOE Hardware Models	UCS C220 M4, UCS C240 M4, UCS C220 M5 and UCS C240 M5
TOE Software Version	X12.5
Keywords	Audit, Authentication, Encryption and Secure Administration

1.2 TOE Overview

The Cisco Expressway X12.5 is designed specifically to provide a gateway solution that extends the services and access to users inside and outside of the organization's firewall. The TOE includes the hardware models as defined in Table 3 in Section 1.1.

Cisco Expressway X12.5 software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective services that extend secure services to users inside and outside the organizations firewall. Although Cisco Expressway X12.5 software performs many networking functions, this Security Target only addresses the functions that provide for the security of the TOE itself as described in Section 1.7 TOE logical scope below.

1.2.1 TOE Product Type

The Cisco Expressway X12.5 TOE is a network device as defined in the NDcPPv2.0e and as described below.

The Cisco Expressway, a distributed TOE, is deployed as a pair of components. Both components, Expressway C and Expressway E run the same software, Cisco Expressway X12.5. The differences in the two components are based on the deployed location as described below.

The Expressway-C component is located within the organization's network with a trunk and line-side connection to Unified Call Manager (CUCM).

The Expressway-E component is located at the perimeter of the organization's network for devices which are located outside the internal network. For example, the organization's employees that work from home, employees that are on business travel and mobile workers. The Expressway-E is configured with a traversal server zone to the Expressway-C.

1.2.2 Supported non-TOE Hardware/ Software/ Firmware

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

Table 4 IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
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 installation.
Management Workstation using web browser for HTTPS	Yes	This includes any IT Environment Management workstation with a web browser installed that is used by the TOE administrator to support TOE administration through HTTPS protected channels. Any web browser that supports TLSv1.1 and/or TLSv1.2 included the supported ciphersuites may be used.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages using TLSv1.1 and/or TLSv1.2 to secure the connection. The audit records are automatically sent to the remote syslog once the configuration and settings are complete.
Cisco Unified Communications Manager (CUCM))	Yes	CUCM serves as the component of the Cisco Unified Communications family of products which provides network-based presence to endpoints.
DNS Server	Yes	The TOE supports communications with the DNS Server that is required for communications with other components.
Certification Authority (CA)	Yes	This includes any IT Environment Certification Authority (CA) on the TOE network. The CA can be used to provide the TOE with a valid certificate during certificate enrollment as well as validating a certificate.
Firewalls	Yes	This includes any commercially available firewall capable of separating a company's internal network from the public network. They should be installed on both the public and private side of the Cisco Expressway E device.

1.3 TOE DESCRIPTION

This section provides an overview of the Cisco Expressway Target of Evaluation (TOE). Cisco Expressway is an advanced gateway that extend services to users inside and outside the organization firewall, such as desktop share, instant messaging, and presence.

The TOE is comprised of both software and hardware. The TOE deployment is the Cisco Expressway instance running X12.5 software installed on one of four different models of the Cisco Unified Computing System™ (Cisco UCS), all of which are described below. The Cisco UCS boxes are administered through a single management entity called the Cisco UCS Manager (Cisco Unified Computing System (UCS) Manager 2.2(3a)). It is assumed the Cisco UCS is setup, configured in their evaluated configurations and ready for use.

The Cisco Unified Computing System™ (Cisco UCS) C220 M4 Rack Server (one rack unit [1RU]) offers up to two Intel® Xeon® E5 Series processors, 24 DIMM slots, eight small form-factor (SFF) disk drives or four large form-factor (LFF) drives, and two 1 Gigabit Ethernet LAN-on-motherboard (LOM) ports. Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C220 M4.



Figure 1 Cisco UCS C220 M4 Server

The Cisco Unified Computing System™ (Cisco UCS) C240 M4 Rack Server (two rack unit [2RU]) offers up to two Intel® Xeon® E5 Series processors, 24 DIMM slots, 24 small form-factor (SFF) disk drives or 12 large form-factor (LFF) drives, and two 1 Gigabit Ethernet LAN-on-motherboard (LOM) ports. Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C240 M4.



Figure 2 Cisco UCS C240 M4 Server

The Cisco UCS C220 M5 Rack Server is a two-socket 1 Rack Unit (1RU) rack-mount server offers up to two Intel® Xeon® Scalable Series processors. The UCS C220 M5 supports:

- up to 24 DDR4 DIMMs
- up to 10 Small-Form-Factor (SFF) 2.5-inch drives or 4 Large-Form-Factor (LFF) 3.5-inch drives (77 TB storage capacity with all NVMe PCIe SSDs)
- support for 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards
- Modular LAN-On-Motherboard (mLOM) slot that can be used to install a Cisco UCS Virtual Interface Card (VIC) without consuming a PCIe slot
- dual embedded Intel x550 10GBASE-T LAN-On-Motherboard (LOM) ports

Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C220 M5.



Figure 3 Cisco UCS C220 M5 Server

The Cisco Unified Computing System™ (Cisco UCS) C240 M5 2 Rack Unit (2RU) offers up to two Intel® Xeon® Scalable series processors. The C240 M5 supports:

- up to 24 DDR4 DIMM slots
- up to 26 hot-swappable Small-Form-Factor (SFF) 2.5-inch drives, including 2 rear hot-swappable SFF drives
- support for 12-Gbps SAS modular RAID controller in a dedicated slot Modular LAN-On-Motherboard (mLOM) slot that can be used to install a Cisco UCS Virtual Interface Card (VIC) without consuming a PCIe slot.

Also supporting dual 10- or 40-Gbps network connectivity, Dual embedded Intel x550 10GBASE-T LAN-On-Motherboard (LOM) ports and modular M.2 or Secure Digital (SD) cards that can be used for boot.

Refer to Table 5 Hardware Models and Specifications for the primary features of the Cisco UCS C240 M5.



Figure 4 Cisco UCS C240 M5 Server

The TOE includes a web-browsable interface for the system configuration for administrators. Cisco Expressway supports the following operating system browsers:

- Internet Explorer 8, 9, 10, and 11
- Firefox 3 or later
- Chrome

HTTPS is used to secure the connection between Cisco Expressway and the browser.

The TOE will be configured to only to use x.509v3-ssh-rsa public key algorithm for secure connection between Expressway-C and Expressway-E in MRA mode. This is a dedicated SSHv2

connection between the two components. The Expressway-C component is configured as the SSH Client and the Expressway-E is configured as the SSH Server. For the outbound port from Expressway-C (private) it is an ephemeral port to Expressway-E (DMZ) port 2222, a listening port. The Expressway-E listens on port 222 for SSH tunnel traffic and the only legitimate sender of SSH traffic is the Expressway-C. Refer to the Cisco Expressway X12.5 System Common Criteria Configuration Guide for details and configuration settings for the evaluated configuration.

TLS is used to secure the connection between Cisco Expressway and the syslog server. This includes any syslog server to which the TOE would transmit syslog messages using TLSv1.1 or TLSv1.2 to secure the connection.

Cisco Expressway X12.5 software is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective services to users inside and outside the organization. Although X12.5 software performs many functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.6 Logical Scope of the TOE.

The following figure provides a visual depiction of a TOE deployment. The TOE boundary are the blue boxes.

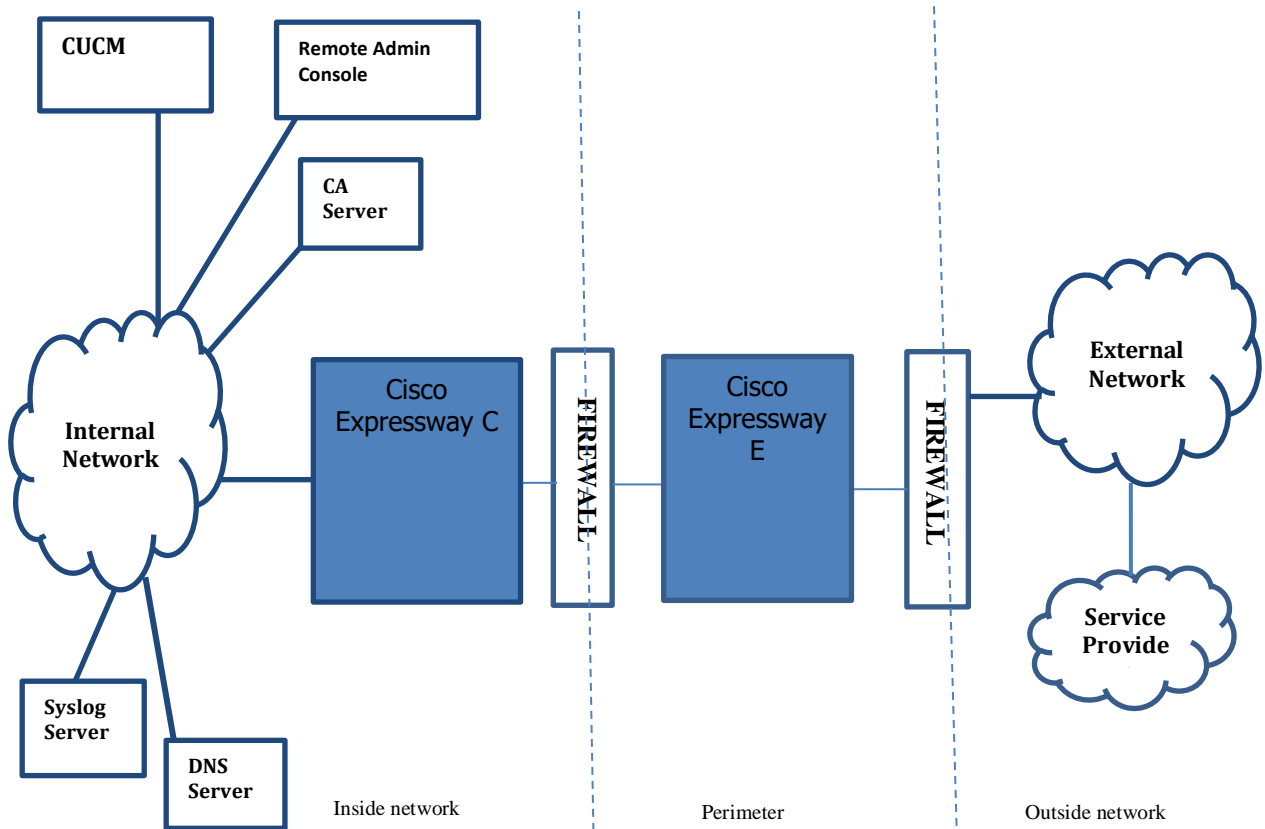


Figure 5 TOE Example Deployment

The previous figure includes the following:

- The TOE
 - Cisco Expressway X12.5 running on UCS M4 or UCS M5
- The following IT entities that are considered to be in the IT Environment:
 - CA (Certificate Authority) Server
 - DNS Server
 - Management Workstation to support Administration (secure connection is HTTPS)
 - Firewalls
 - Cisco CUCM
 - Syslog Server (secure connection is TLS)
 - Service Provider

1.4 TOE Evaluated Configuration

The TOE consists of Cisco Expressway software installed on one or more UCS appliances as described in section 1.5 below.

The TOE consists of two components, Expressway-C and Expressway-E that work together to form a highly secure traversal link to provide a gateway solution that extends the services and access to users inside and outside of the organization's firewall.


The TOE is administered using the Cisco Expressway Administration program from an administrative workstation. No browser software exists on the Cisco Expressway server. When connecting to Cisco Expressway the administrative workstation must be connected to an internal network and HTTPS must be used to secure the connection to the TOE. An external audit server is also used to store Cisco Expressway audit records. The external audit server must be attached to the internal (trusted) network and TLS is used to secure the connection and to secure the transmission of data. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic and one that is in a controlled environment where implementation of security policies can be enforced.

The USB ports located on each TOE hardware must not be used for installation. The serial port found on each TOE hardware is only used during installation.


1.5 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the Cisco Expressway. The TOE hardware platform is at least one of the following Cisco UCS platforms, UCS C220 M4, UCS C240 M4, UCS C220 M5 or the UCS C240 M5. The TOE software is the Cisco Expressway X12.5 software. The network, on which the TOE resides is considered part of the environment. The TOE guidance documentation, the Cisco Expressway Common Criteria Configuration Guide that is also considered to be part of the TOE can be found listed and are downloadable from the <http://cisco.com> web site. The TOE hardware is comprised of the following physical specifications as described in Table 5 below:


Table 5 Hardware Models and Specifications

Hardware/Processor/Software	Picture	Size	Power	Interfaces
<p>UCS C220 M4</p> <p>While tested on the specific processor model listed¹, any Intel® Xeon® E526xx v4, processor may be used as part of the evaluated configuration with VMware ESXi 6.0</p> <p>Expressway X12.5 software</p>		<p>1RU: 1.7 x 16.9 x 29.8 in. (4.32 x 43 x 75.6 cm)</p>	<p>Up to two 770 W (AC) hot swappable power supplies or two 1050 W (DC) power supplies. One is mandatory; one more can be added for 1 + 1 redundancy.</p>	<ul style="list-style-type: none"> • Up to 4 LFF or 8 SFF front-accessible, hot-swappable, internal SAS, SATA, or SSD drives, providing redundancy options and ease of serviceability • Various PCIe card ports (dependent on which cards are installed), • Virtual Interface Card (VIC) ports, Converged Network Adapter (CNA) ports, Network Interface Card (NIC) ports, Host Bus Adapter (HBA) ports • I/O performance and flexibility with one x8 half-height and half-length slot, and one x16 full-height and half-length slot • Up to two internal 32GB or two 64GB Cisco FlexFlash drives (SD cards) • One internal USB flash drive <p>Front panel - One KVM console connector (supplies two USB 2.0 connectors, one GA DB15 connector, and one serial port (RS232) RJ45 connector)</p> <p>Rear panel - One DB15 VGA connector, One RJ45 serial port connector, Two USB 3.0 port connectors, One RJ-45 10/100/1000 Ethernet management port, using Cisco Integrated Management Controller (CIMC) firmware, two Intel i350 embedded (on the motherboard) GbE LOM ports, One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards</p>


¹ Intel® Xeon® E5 2660 v4 Series processor

Hardware/Processor/ Software	Picture	Size	Power	Interfaces
<p>UCS C240 M4</p> <p>While tested on the specific processor model listed², any Intel® Xeon® E526xx v4, processor may be used as part of the evaluated configuration with VMWare ESXi 6.0</p> <p>Expressway X12.5 software</p>		<p>2RU: 3.43 x 17.65 x 29.0 in. (8.7 x 44.8 x 73.8 cm)</p>	<p>The server is available with four types of power supplies:</p> <ul style="list-style-type: none"> • 650 W (AC) • 930 W (DC) • 1200 W (AC) • 1400 W (AC)) 	<ul style="list-style-type: none"> • Up to 12 LFF or 24 SFF front-accessible, hot-swappable, SAS, SATA, or SSD drives for local storage, providing redundancy options and ease of serviceability <p>Rear panel</p> <ul style="list-style-type: none"> • One DB15 VGA connector • One RJ45 serial port connector • Two USB 3.0 port connectors • One RJ-45 10/100/1000 Ethernet management port, using Cisco Integrated • Management Controller (CIMC) firmware • Two Intel i350 embedded (on the motherboard) GbE LOM ports • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards, Various PCIe card ports (dependent on which cards are installed) • Virtual Interface Card (VIC) ports • Converged Network Adapter (CNA) ports • Network Interface Card (NIC) ports • Host Bus Adapter (HBA) ports <p>Front panel</p> <ul style="list-style-type: none"> • One KVM console connector (supplies two USB 2.0 connectors, one VGA, DB15 video connector, and one serial port (RS232) RJ45 connector) support the InfiniBand architecture. <p>A front panel controller provides status indications and control buttons</p>

² Intel® Xeon® E5 2660 v4 Series processor

Hardware/Processor/ Software	Picture	Size	Power	Interfaces
<p>UCS C220 M5</p> <p>While tested on the specific processor model listed³, any Intel® Xeon® Scalable processor with the Skylake-SP microarchitecture may be used as part of the evaluated configuration with VMware ESXi 6.0</p> <p>Expressway X12.5 software</p>		<p>Height 1.7 in. (4.32 cm)</p> <p>Width 16.89 in. (43.0 cm) including handles: 18.98 in. (48.2 cm)</p> <p>Depth 29.8 in. (75.6 cm) including handles: 30.98 in. (78.7 cm)</p>	<p>Up to two of the following hot-swappable power supplies:</p> <ul style="list-style-type: none"> • 770 W (AC) • 1050 W (AC) • 1050 W V2 (DC) 	<p>Rear panel</p> <ul style="list-style-type: none"> • One 1-Gbps RJ-45 management port (Marvell 88E6176) • Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard) • One RS-232 serial port (RJ45 connector) • One DB15 VGA connector • Two USB 3.0 port connectors • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards <p>Front panel</p> <ul style="list-style-type: none"> • One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232) RJ45 connector) <p>Modular LAN on Motherboard (mLOM) slot</p> <p>The dedicated mLOM slot on the motherboard can flexibly accommodate the following cards:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Cisco Virtual Interface Cards <input type="checkbox"/> Quad Port Intel i350 1GbE RJ45 Network Interface Card (NIC)

³ Intel® Xeon® Scalable Platinum 8160M Series processors

Hardware/Processor/Software	Picture	Size	Power	Interfaces
<p>UCS C240 M5</p> <p>While tested on the specific processor model listed⁴, any Intel® Xeon® Scalable processor with the Skylake-SP microarchitecture may be used as part of the evaluated configuration with VMware ESXi 6.0</p> <p>Expressway X12.5 software</p>		<p>Height 3.43 in. (8.70 cm)</p> <p>Width (including slam latches) 17.65 in. (44.8 cm)</p> <p>Including handles: 18.96 in. (48.2 cm)</p> <p>Depth 29.0 in. (73.8 cm)</p> <p>Including handles: 30.18 in. (76.6 cm)</p>	<p>Up to two of the following hot-swappable power supplies:</p> <ul style="list-style-type: none"> • 1050 W (AC) power supply • 1050 W V2 (DC) power supply • 1600 W (AC) power supply 	<p>Rear panel</p> <ul style="list-style-type: none"> • One 1-Gbps RJ-45 management port (Marvell 88E6176) • Two 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard) • One RS-232 serial port (RJ45 connector) • One DB15 VGA connector • Two USB 3.0 port connectors • One flexible modular LAN on motherboard (mLOM) slot that can accommodate various interface cards <p>Front panel</p> <ul style="list-style-type: none"> • One KVM console connector (supplies two USB 2.0 connectors, one VGA DB15 video connector, and one serial port (RS232)) <p>Modular LAN on Motherboard (mLOM) slot</p> <p>The dedicated mLOM slot on the motherboard can flexibly accommodate the following cards:</p> <ul style="list-style-type: none"> • Cisco Virtual Interface Cards • Quad Port Intel i350 1GbE RJ45 mLOM Network Interface Card (NIC)

1.6 Logical Scope of the TOE

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

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

⁴Intel® Xeon® Scalable Platinum 8160M Series processors

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v2.0e as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco Expressway provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The Cisco Expressway generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE audit event logging is centralized and enabled by default. Audit logs can be sent to an external audit server over a secure TLS channel.

1.6.2 Communications

The TOE provides the configuration options for the Authorized Administrator to enable the persistent, dedicated secure connections using SSHv2.0 between the two components, Expressway-C and Expressway-E. This connection forms a highly secure traversal link to provide a gateway solution that extends the services and access to users inside and outside of the organization's firewall.

1.6.3 Cryptographic Support

The TOE provides cryptography in support of other Cisco Expressway security functionality. The Expressway software calls the CiscoSSL FIPS Object Module (FOM) v6.2 that has been validated in accordance with the specified standards to meet the requirements listed below and all the algorithms claimed have CAVP certificates.

Refer to Table 6 for algorithm certificate references.

Table 6 FIPS References

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation, PKCS#1 v.1.5, 2048 bit key	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/SigGen
ECDSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_CKM.1 FCS_COP.1/SigGen
AES	Used for symmetric encryption/decryption	AES Key Wrap in CBC, CTR and	C905 (UCS M5)	CiscoSSL FIPS Object	FCS_COP.1/DataEncryption

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
		GCM (128 and 256 bits)	C924 (UCS M4)	Module (FOM) v6.2	
SHS (SHA-1, 256, 384, 512)	Cryptographic hashing services	Byte Oriented	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_COP.1//Hash
HMAC SHA-1, SHA-256, SHA-384, SHA-512	Keyed hashing services and software integrity test	Byte Oriented	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_RBG_EXT.1
CVL SSH/TLS	Key Agreement	NIST Special Publication 800-56A	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_CKM.2
CVL – KAS-ECC	Key Agreement	NIST Special Publication 800-56A	C905 (UCS M5) C924 (UCS M4)	CiscoSSL FIPS Object Module (FOM) v6.2	FCS_CKM.2

The algorithm certificates are applicable to the TOE based on Expressway and Intel® Xeon® processors as noted in Section 1.5 Physical Scope of the TOE.

The TOE provides cryptography in support of remote administrative management via HTTPS/TLS, the secure connection to an external audit server using TLS and a dedicated SSHv2 secure connection between the Expressway C and E components. The TOE uses the X.509v3 certificate for securing the SSH and TLS connections.

The TOE also authenticates software updates to the TOE using a published SHA512 hash.

1.6.4 Identification and authentication

The TOE provides authentication services for administrative users to connect to the TOEs GUI administrator interface. The TOE requires Authorized Administrators to be successfully identified and authenticated prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters. The TOE provides administrator authentication against a local user database using the GUI interface accessed via secure HTTPS connection.

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

The TOE uses SSHv2 to secure the connection and the associated X509v3 certificates to authenticate the Expressway C and Expressway E TOE components.

1.6.5 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 HTTPS session or via a local console connection. The TOE provides the ability to securely manage:

- Ability to administer the TOE locally and remotely;
- Ability to configure the access banner;
- Ability to update the TOE, and to verify the updates using published hash capability prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- Ability to configure audit behaviour;
- Ability to configure the cryptographic functionality;
- Ability to configure the interaction between TOE components;
- Ability to re-enable an Administrator account;
- Change a user's password;
- Require a user's password to be changed upon next login and
- Configure NTP

The TOE supports the security administrator role. Only the Authorized Administrator can perform the above security relevant management functions.

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

1.6.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification and authentication to Authorized Administrators. The TOE prevents reading of

cryptographic keys and passwords. The TOE also protects data from disclosure and detects modification when transmitted between the Expressway C and Expressway E components using SSHv2. Additionally, Cisco Expressway is not a general-purpose operating system and access to Cisco Expressway memory space is restricted to only Cisco Expressway functions.

The TOE initially synchronizes time with an NTP server and then internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE.

The TOE performs testing to verify correct operation of the system itself and that of the cryptographic module.

Finally, the TOE is able to verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software via a published hash.

1.6.7 TOE Access

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

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

1.6.8 Trusted path/Channels

The TOE allows trusted channels to be established to itself from remote Authorized Administrators using HTTPS, initiates outbound TLS secure connection to transmit audit messages to remote syslog servers and uses NTPv4 to secure the connection to the NTP server.

The TOE can also establish trusted paths between the Expressway C and Expressway E components using SSHv2 when configured in Mobile and Remote Access (MRA) mode. In MRA mode the TOE provides secure a highly secure traversal link to provide a gateway solution that extends the services and access to users inside and outside of the organization's firewall.

In MRA mode, SSHv2 is used to secure the persistent, dedicated connection where Expressway C acts as the SSH server and the Expressway E acts as the SSH client, therefore creating a distributed TOE.

If any of the established trusted channels/paths are unintentionally broken, the connection will need to be re-established as described in this document and the referenced Cisco Expressway X12.5 System Common Criteria Configuration Guide.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 7 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS mode of operation	This mode of operation includes non-FIPS allowed operations.
USB Ports	The USB ports on the TOE hardware must not be used

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 NDcPPv2.0e.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 4, dated: September 2012. For a listing of Assurance Requirements claimed see section 5.4.

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

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 9 Protection Profiles below. The following NIAP Technical Decisions (TD) have also been applied to the claims in this document. Each posted TD was reviewed and considered based on the TOE product type, the PP claims and the security functional requirements claimed in this document.

Table 8 Technical Decisions (TD)

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0453	NIT Technical Decision for Clarify authentication methods SSH clients can use to authenticate SSH	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_SSHC_EXT.1.9	2019.09.16	Yes - TD has been applied
TD0451	NIT Technical Decision for ITT Comm UUID Reference Identifier	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_TLSS_EXT.1.2 and FCS_TLSS_EXT.2.2	2019.09.16	Yes - TD has been applied
TD0450	NIT Technical Decision for RSA-based ciphers and the Server Key Exchange message	CPP_ND_V2.0E, CPP_ND_V2.1	FCS_TLSS_EXT.*.3, FCS_DTLSS_EXT.*.4, ND SD v2.1, ND SD v2.0E	2019.09.16	Yes - TD has been applied
TD0448	NIT Technical Decision for Documenting Diffie-Hellman 14 groups	CPP_ND_V2.0E, CPP_ND_V2.1	FCS_CKM.2	2019.09.16	Yes - TD has been applied
TD0447	NIT Technical Decision for Using 'diffie-hellman-group-exchange-sha256' in	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_SSHC_EXT.1.7, FCS_SSHS_EXT.1.7	2019.09.16	No - Referenced SFR is not being claimed

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
	FCS_SSHC/S_EXT.1.7				
TD0425	NIT Technical Decision for Cut-and-paste Error for Guidance AA	CPP_ND_V2.0E, CPP_ND_V2.1	ND SD V2.0e, ND SD V2.1, FTA_SSL.3	2019.05.31	Yes - TD has been applied
TD0423	NIT Technical Decision for Clarification about application of RfI#201726rev 2	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	ND SD V2.0E, FW SD V2.0E, ND SD V2.1	2019.05.31	Yes - TD has been applied
TD0412	NIT Technical Decision for FCS_SSHS_EXT.1.5 SFR and AA discrepancy	CPP_FW_V2.0E, CPP_ND_V2.0, CPP_ND_V2.1	FCS_SSHS_EXT.1.5, ND SD V2.0e, ND SD V2.1	2019.03.22	Yes - TD has been applied
TD0411	NIT Technical Decision for FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_SSHC_EXT.1.5, ND SD V2.0E, ND SD V2.1	2019.03.22	Yes - TD has been applied
TD0410	NIT technical decision for Redundant assurance activities associated with FAU_GEN.1	CPP_ND_V1.0, CPP_ND_V2.0E, CPP_ND_V2.1	FAU_GEN.1, ND SD V1.0, ND SD V2.0e, ND SD V2.1	2019.03.22	Yes - TD has been applied
TD0409	NIT decision for Applicability of FIA_AFL.1 to key-based SSH authentication	CPP_ND_V2.0E, CPP_ND_V2.1	FIA_AFL.1, ND SD v2.0e, ND SD v2.1	2019.03.22	No, referenced features is not being claimed
TD0408	NIT Technical Decision for local vs. remote administrator accounts	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FIA_AFL.1, FIA_UAU_EXT.2, FMT_SMF.1	2019.03.22	Yes - TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0407	NIT Technical Decision for handling Certification of Cloud Deployments	CPP_ND_V2.0E, CPP_ND_V2.1		2019.03.22	No, referenced features is not being claimed
TD0402	NIT Technical Decision for RSA-based FCS_CKM.2 Selection	CPP_FW_V2.0E, CPP_ND_V2.0E	FCS_CKM.2, ND SD V2.0E	2019.02.24	Yes - TD has been applied
TD0401	NIT Technical Decision for Reliance on external servers to meet SFRs	CPP_ND_V2.0E	FTP_ITC.1	2019.02.24	Yes - TD has been applied
TD0400	NIT Technical Decision for FCS_CKM.2 and elliptic curve-based key establishment	CPP_FW_V2.0E, CPP_ND_V2.0E	FCS_CKM.1, FCS_CKM.2	2019.02.24	Yes - TD has been applied
TD0399	NIT Technical Decision for Manual installation of CRL (FIA_X509_EXT.2)	CPP_ND_V2.0E, CPP_ND_V2.1	FIA_X509_EXT.2, ND SD V2.0E, ND SD V2.1	2019.02.24	Yes - TD has been applied
TD0398	NIT Technical Decision for FCS_SSH*EXT.1.1 RFCs for AES-CTR	CPP_FW_V2.0E, CPP_ND_V2.0E	FCS_SSHC_EXT.1.1, FCS_SSHS_EXT.1.1,	2019.02.24	Yes - TD has been applied
TD0397	NIT Technical Decision for Fixing AES-CTR Mode Tests	CPP_ND_V2.0E	FCS_COP.1/DataEncryption, ND SD V2.0E	2019.02.24	Yes - TD has been applied
TD0396	NIT Technical Decision for FCS_TLSC_EXT.1.1, Test 2	CPP_ND_V2.0E	FCS_DTLSC_EXT.1.1, FCS_DTLSC_EXT.2.1, FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1, ND SD V2.0E	2019.02.24	Yes - TD has been applied
TD0395	NIT Technical Decision for Different Handling of	CPP_ND_V2.0E	FCS_TLSS_EXT.2.4, FCS_TLSS_EXT.2.5, ND SD V2.0E	2019.02.24	Yes - TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
	TLS1.1 and TLS1.2				
TD0394	NIT Technical Decision for Audit of Management Activities related to Cryptographic Keys	CPP_FW_V2.0E, CPP_ND_V2.0E	FAU_GEN.1, ND SD v2.0E	2019.02.24	Yes - TD has been applied
TD0343	NIT Technical Decision for Updating FCS_IPSEC_EXT.1.14 Tests	CPP_FW_V2.0E, CPP_ND_V2.0E	ND SD V2.0, FCS_IPSEC_EXT.1.14	2018.08.02	No, Referenced SFR is not being claimed.
TD0342	NIT Technical Decision for TLS and DTLS Server Tests	CPP_ND_V2.0E	ND SD V2.0, FCS_DTLSS_EXT.1, FCS_DTLSS_EXT.2, FCS_TLSS_EXT.1, FCS_TLSS_EXT.2	08/02/18	Yes - TD has been applied
TD0341	NIT Technical Decision for TLS wildcard checking	CPP_ND_V2.0E	ND SD V2.0, FCS_TLSC_EXT.1.2, FCS_TLSC_EXT.2.2, FCS_DTLSC_EXT.1.2, FCS_DTLSC_EXT.2.2,	08/02/18	Yes - TD has been applied
TD0340	NIT Technical Decision for Handling of the basicConstraints extension in CA and leaf certificates	CPP_FW_V2.0E, CPP_ND_V2.0E	FIA_X509_EXT.1.1	2018.08.02	Yes - TD has been applied
TD0339	NIT Technical Decision for Making password-based authentication optional in FCS_SSHS_EXT.1.2	CPP_FW_V2.0E, CPP_ND_V2.0E	ND SD V2.0, FCS_SSHS_EXT.1.2	2018.08.02	Yes - TD has been applied
TD0338	NIT Technical Decision for Access Banner Verification	CPP_ND_V2.0E	ND SD V2.0, FTA_TAB.1	08/02/18	Yes - TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0337	NIT Technical Decision for Selections in FCS_SSH*_EXT.1.6	CPP_FW_V2.0E, CPP_ND_V2.0E	ND SD V2.0, FCS_SSHC_EXT.1, FCS_SSHS_EXT.1	2018.08.02	Yes - TD has been applied
TD0336	NIT Technical Decision for Audit requirements for FCS_SSH*_EXT.1.8	CPP_ND_V2.0E	ND SD V2.0, FCS_SSHC_EXT.1.8, FCS_SSHS_EXT.1.8	08/01/18	Yes - TD has been applied
TD0335	NIT Technical Decision for FCS_DTLS Mandatory Cipher Suites	CPP_FW_V2.0E, CPP_ND_V2.0E	FCS_DTLS_EXT.1.1, FCS_DTLS_EXT.2.1, FCS_DTLSS_EXT.1.1, FCS_DTLSS_EXT.2.1, FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1, FCS_TLSS_EXT.1.1, FCS_TLSS_EXT.2.1	2018.08.01	Yes - TD has been applied
TD0334	NIT Technical Decision for Testing SSH when password-based authentication is not supported	CPP_ND_V2.0E	ND SD V2.0, FCS_SSHC_EXT.1.9	08/01/18	Yes - TD has been applied
TD0333	NIT Technical Decision for Applicability of FIA_X509_EXT.3	CPP_FW_V2.0E, CPP_ND_V2.0E	ND SD V2.0, FIA_X509_EXT	2018.08.01	Yes - TD has been applied
TD0324	NIT Technical Decision for Correction of section numbers in SD Table 1	CPP_ND_V2.0E	Table 1	05/18/18	Yes - TD has been applied
TD0323	NIT Technical Decision for DTLS server testing - Empty Certificate Authorities list	CPP_ND_V2.0E	ND SD V2.0, FCS_DTLSS_EXT.2.7, FCS_DTLSS_EXT.2.8	05/18/18	No, Referenced SFR is not being claimed.
TD0322	NIT Technical Decision for TLS server testing - Empty Certificate Authorities list	CPP_ND_V2.0E	ND SD V.1.0, ND SD V2.0, FCS_TLSS_EXT.2.4, FCS_TLSS_EXT.2.5	05/18/18	Yes - TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0321	Protection of NTP communications	CPP_FW_V2.0E, CPP_ND_V2.0E	FTP_ITC.1, FPT_STM_EXT.1	05/21/18	Yes - TD has been applied
TD0291	NIT technical decision for DH14 and FCS_CKM.1	CPP_FW_V1.0, CPP_FW_v2.0, CPP_FW_V2.0E, CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	FCS_CKM.1.1, ND SD V1.0, ND SD V2.0	02/03/18	Yes - TD has been applied
TD0290	NIT technical decision for physical interruption of trusted path/channel.	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	FTP_ITC.1, FTP_TRP.1, FPT_ITT.1, ND SD V1.0, ND SD V2.0	02/03/18	Yes - TD has been applied
TD0289	NIT technical decision for FCS_TLSC_EXT.x.1 Test 5e	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1, FCS_DTLSC_EXT.1.1 (only ND SD V2.0), FCS_DTLSC_EXT.2.1 (only ND SD V2.0)	02/03/18	Yes - TD has been applied
TD0281	NIT Technical Decision for Testing both thresholds for SSH rekey	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	FCS_SSHC_EXT.1.8, FCS_SSHS_EXT.1.8, ND SD V1.0, ND SD V2.0	01/05/18	Yes - TD has been applied
TD0259	NIT Technical Decision for Support for X509 ssh rsa authentication IAW RFC 6187	CPP_FW_v2.0, CPP_FW_V2.0E, CPP_ND_V2.0, CPP_ND_V2.0E	FCS_SSHC_EXT.1.5/FC S_SSHS_EXT.1.5	11/13/17	Yes - TD has been applied
TD0257	NIT Technical Decision for Updating FCS_DTLSC_EXT.x.2/FCS_TLSC_EXT.x.2 Tests 1-4	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	ND SD V1.0, ND SD V2.0, FCS_DTLSC_EXT.1.2/FCS_DTLSC_EXT.2.2 Tests 1-4 (ND SD V2.0), FCS_TLSC_EXT.1.2/FC S_TLSC_EXT.2.2, Tests 1-4 (ND SD V1.0, ND SD V2.0)	11/13/17	Yes - TD has been applied
TD0256	NIT Technical Decision for Handling of TLS connections with and without mutual authentication	CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	ND SD V1.0, ND SD V2.0, FCS_DTLSC_EXT.2.5 (ND SD V2.0), FCS_TLSC_EXT.2 (ND SD V1.0, ND SD V2.0)	11/13/17	Yes - TD has been applied

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0228	NIT Technical Decision for CA certificates - basicConstraints validation	CPP_FW_V1.0, CPP_ND_V1.0, CPP_ND_V2.0, CPP_ND_V2.0E	ND SD V1.0, ND SD V2.0, FIA_X509_EXT.1.2	06/15/18	Yes - TD has been applied

Table 9 Protection Profiles

Protection Profile	Version	Date
collaborative Protection Profile for Network Devices (NDcPP) + Errata	2.0e	14 March 2018

2.2.1 Protection Profile Additions

The ST claims exact conformance to the collaborative Protection Profile for Network Devices (NDcPP) +Errata 20180314, Version 2.0e. The ST does not include any additions to the functionality described in the NDcPPv2.0e.

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

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

- collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, version 2.0e

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the collaborative Protection Profile for Network Devices (NDcPP) + Errata 20180314, NDcPPv2.0e for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition is included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in the NDcPPv2.0e, for which conformance is claimed verbatim. All concepts covered in the Protection Profile Statement of Security Objectives is included in the Security Target.

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the NDcPP+ Errata 20180314, Version 2.0e, for which

conformance is claimed verbatim. All concepts covered in the Protection Profile Statement of Security Requirements is included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in the NDcPP + Errata 20180314, Version 2.0e.

3 SECURITY PROBLEM DEFINITION

This section identifies the following:

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

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

3.1 Assumptions

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

Table 10 TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device’s physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
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.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.

Assumption	Assumption Definition
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.COMPONENTS_RUNNING	For distributed TOEs it is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. It is also assumed that in addition to the availability of all components it is also checked as appropriate that the audit functionality is running properly on all TOE components.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

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.

Threat	Threat Definition
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

3.3 Organizational Security Policies

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

Table 12 Organizational Security Policies

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

4 SECURITY OBJECTIVES

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

4.1 Security Objectives for the TOE

The collaborative Protection Profile for Network Devices + Errata 20180314 v2.0e does not define any security objectives for the TOE.

4.2 Security Objectives for the Environment

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

Table 13 Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.COMPONENTS_RUNNING	For distributed TOEs the Security Administrator ensures that the availability of every TOE component is checked as appropriate to reduce the risk of an undetected attack on (or failure of) one or more TOE components. The Security Administrator also ensures that it is checked as appropriate for every TOE component that the audit functionality is running properly.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5 SECURITY REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012 and all international interpretations.

5.1 Conventions

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

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

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

Formatting conventions outside of operations and iterations matches the formatting specified within the NDcPPv2.0e.

5.2 TOE Security Functional Requirements

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

Table 14 Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation

Class Name	Component Identification	Component Name
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	Protected Audit Event Storage
FCO: Communications	FCO_CPC_EXT.1	Component Registration Channel Definition
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (Refinement)
	FCS_CKM.2	Cryptographic Key Establishment (Refinement)
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_HTTPS_EXT.1	HTTPS Protocol
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_SSHC_EXT.1	SSH Client Protocol
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.2	TLS Client Protocol with authentication
	FCS_TLSS_EXT.2	TLS Server Protocol with mutual authentication
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management
	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Extended: Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/ITT	X.509 Certificate Validation
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
FMT: Security management	FMT_MOF.1(1)/ManualUpdate	Management of security functions behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all symmetric keys)
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing (Extended)
	FPT_TUD_EXT.1	Trusted Update
	FPT_STM_EXT.1	Reliable Time Stamps
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(2)	Inter-TSF trusted channel
	FTP_ITC.1(3)	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path

5.2.1 Security audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

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

- a) Start-up and shut-down of the audit functions;
- b) All auditable events for the not specified level of audit; and
- c) *All administrator actions comprising:*
 - *Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).*
 - *Security related configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
 - *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
 - *Resetting passwords (name of related user account shall be logged).*
 - [Starting and stopping services (if applicable)];
- d) *Specifically defined auditable events listed in Table 15 Auditable Events.*

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

For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of Table 15*].

Table 15 Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
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.
FCO_CPC_EXT.1	Enabling communications between a pair of components. Disabling communications between a pair of components.	Identities of the endpoints pairs enabled or disabled.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS session.	Reason for failure.
FCS_SSHC_EXT.1	Failure to establish an SSH session	Reason for failure.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
FCS_RBG_EXT.1	None.	None.
FCS_TLSC_EXT.2	Failure to establish an TLS session	Reason for failure.
FCS_TLSS_EXT.2	Failure to establish an TLS session	Reason for failure.
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/ITT	Unsuccessful attempt to validate a certificate.	Reason for failure.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	All management activities of TSF data.	None.
FMT_MTD.1_CryptoKeys	Management of cryptographic keys.	None.
FMT_SMF.1	None.	None.
FMT_SMR.2	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_ITT.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FPT_SKP_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. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	Any attempts at unlocking of an interactive session.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None

5.2.1.2 FAU_GEN.2 User Identity Association

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

5.2.1.3 FAU_STG_EXT.1 Protected Audit Event Storage

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

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

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

5.2.2 Communications (FCO)

5.2.2.1 FCO_CPC_EXT.1 Component Registration Channel Definition

FCO_CPC_EXT.1.1 The TSF shall require a Security Administrator to enable communications between any pair of TOE components before such communication can take place.

FCO_CPC_EXT.1.2 The TSF shall implement a registration process in which components establish and use a communications channel that uses [

- A channel that meets the secure channel requirements in [FTP_ITC.1],

].
for at least TSF data.

FCO_CPC_EXT.1.3 The TSF shall enable a Security Administrator to disable communications between any pair of TOE components.

5.2.3 Cryptographic Support (FCS)

5.2.3.1 FCS_CKM.1 Cryptographic Key Generation (Refinement)

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

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using “NIST curves” [P-256, P-384] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;

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

5.2.3.2 FCS_CKM.2 Cryptographic Key Establishment (Refinement)

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

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1;
- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;

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

5.2.3.3 FCS_CKM.4 Cryptographic Key Destruction

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

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

that meets the following: *No Standard.*

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

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

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

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

[

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

]

that meet the following: [

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

].

5.2.3.6 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-384, SHA-512] and ~~cryptographic key sizes [assignment: cryptographic key sizes]~~ and **message digest sizes [160, 256, 384, 512]** bits that meet the following: [ISO/IEC 10118-3:2004].

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

FCS_COP.1.1/KeyedHash The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm [HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [160, 256-bit, 384-bit, 512-bit] and **message digest sizes [160, 256, 384, 512]** bits that meet the following: [ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”].

5.2.3.8 FCS_HTTPS.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [**not establish the connection**] if the peer certificate is deemed invalid.

5.2.3.9 FCS_RBG_EXT.1 Random Bit Generation

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

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

5.2.3.10 FCS_SSHC_EXT.1 SSH Client Protocol

FCS_SSHC_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs [4251, 4252, 4253, 4254, 4344, 6187, 6668].

FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based [**no other methods**].

FCS_SSHC_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [32768 bytes] bytes in an SSH transport connection are dropped.

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

FCS_SSHC_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [x509v3-ssh-rsa] as its public key algorithm(s) and rejects all other public key algorithms.

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

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

FCS_SSHC_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

FCS_SSHC_EXT.1.9 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key and [no other methods] as described in RFC 4251 section 4.1.

5.2.3.11 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs [4251, 4252, 4253, 4254, 4344, 6187, 6668].

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based [no other methods].

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [32768 bytes] bytes in an SSH transport connection are dropped.

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

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [x509v3-ssh-rsa] as its public key algorithm(s) and rejects all other public key algorithms.

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

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

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

5.2.3.12 FCS_TLSC_EXT.2 TLS Client Protocol with authentication

FCS_TLSC_EXT.2.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] supporting the following ciphersuites: [

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
 - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
 - TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
 - TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
 - TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
-].

FCS_TLSC_EXT.2.2 The TSF shall verify that the presented identifier matches the reference identifier per RFC 6125 section 6.

FCS_TLSC_EXT.2.3 The TSF shall only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [not establish the connection].

FCS_TLSC_EXT.2.4 The TSF shall [*not present the Supported Elliptic Curves Extension: [and no other curves]*] in the Client Hello.

FCS_TLSC_EXT.2.5 The TSF shall support mutual authentication using X.509v3 certificates.

5.2.3.13 FCS_TLSS_EXT.21 TLS Server Protocol with mutual authentication

FCS_TLSS_EXT.2.1 The TSF shall implement [TLS 1.2 (RFC 5246), TLS 1.1 (RFC 4346)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5289

].

FCS_TLSS_EXT.2.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [none].

FCS_TLSS_EXT.2.3 The TSF shall [perform RSA key establishment with key size [2048 bits]; [generate EC Diffie-Hellman parameters over NIST curves [secp256r1, secp384r1] and no other curves].

FCS_TLSS_EXT.2.4 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.2.5 The TSF shall not establish a trusted channel if the client certificate is invalid. If the client certificate is deemed invalid, then the TSF shall [not establish the connection].

FCS_TLSS_EXT.2.6 The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

5.2.4 Identification and authentication (FIA)

5.2.4.1 Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [1-3] unsuccessful authentication attempts occur related to Administrators attempting to authenticate remotely using a password.

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

5.2.4.2 FIA_PMG_EXT.1 Password Management

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

- a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(,”)], [*no other characters*];
- b) Minimum password length shall be configurable to [15] and [15].

5.2.4.3 FIA_UIA_EXT.1 User Identification and Authentication

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

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

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

5.2.4.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

5.2.4.5 FIA_UAU.7 Protected Authentication Feedback

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

5.2.4.6 FIA_X509_EXT.1/ITT X509 Certificate Validation

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

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of two certificates**.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [no revocation method].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
 - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field*
 - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
 - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

FIA_X509_EXT.1.2/ITT 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.

5.2.4.7 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates**.
- The certificate path must terminate with a trusted CA certificate.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- The TSF shall validate the extendedKeyUsage field according to the following rules:

- *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
- *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
- *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
- *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.

5.2.4.1 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 [TLS, SSH], 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 [accept the certificate].

5.2.4.2 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.

5.2.5 Security management (FMT)

5.2.5.1 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 update to Security Administrators*.

5.2.5.2 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*.

5.2.5.3 FMT_MTD.1/CryptoKeys Management of TSF data

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

5.2.5.4 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [hash comparison] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
-
- [
 - Ability to configure audit behaviour;
 - Ability to configure thresholds for SSH rekeying;
 - Ability to configure the cryptographic functionality;
 - Ability to configure the interaction between TOE components; and
 - Ability to re-enable an Administrator account
-].

5.2.5.5 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator.*

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FPT_APW_EXT.1: Protection of Administrator Passwords

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

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

5.2.6.2 FPT_ITT.1 Basic internal TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from disclosure and detect its modification when it is transmitted between separate parts of the TOE **through the use of [SSH]**.

5.2.6.3 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.

5.2.6.4 FPT_STM_EXT.1 Reliable Time Stamps

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

FPT_STM_EXT.1.2 The TSF shall [*synchronise time with external time sources*].

5.2.6.5 FPT_TST_EXT.1: TSF Testing

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

- *Power-on Self-Tests*
- *Software and firmware Integrity Test*

].

5.2.6.6 FPT_TUD_EXT.1 Trusted Update

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

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

FPT_TUD_EXT.1.3 The TSF shall provide a means to authenticate firmware/software updates to the TOE using a [*published hash*] prior to installing those updates.

5.2.7 TOE Access (FTA)

5.2.7.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- lock the session - disable any activity of the user's data access/display devices other than unlocking the session, and requiring that the administrator re-authenticate to the TSF prior to unlocking the session]

after a Security Administrator-specified time period of inactivity.

5.2.7.2 FTA_SSL.3 TSF-initiated Termination

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

5.2.7.3 FTA_SSL.4 User-initiated Termination

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

5.2.7.4 FTA_TAB.1 Default TOE Access Banners

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

5.2.8 Trusted Path/Channels (FTP)

5.2.8.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1(1) Refinement: The TSF shall be capable of using TLS, and [NTPv4(RFC5905), SSH] to provide a trusted communication channel between itself and **authorized IT entities supporting the following capabilities: audit server, NTP server, [Expressway C and Expressway E in MRA mode]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data.

FTP_ITC.1.2(1) The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for [communications with the following:

- *external audit server using TLS*
- *external NTP server using NTPv4*
- *Expressway C and Expressway E in MRA mode using SSH*

].

5.2.8.2 FTP_TRP.1 Trusted Path

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

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

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

5.3 TOE SFR Dependencies Rationale for SFRs Found in NDcPPv2.0e

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDcPPv2.0e. As such, the NDcPPv2.0e dependency rationale is deemed acceptable since the PP itself has been validated.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPPv2.0e, which is derived from Common Criteria Version 3.1, Revision 4, dated September 2012. The assurance requirements are summarized in the table below.

Table 16: Assurance Measures

Assurance Class	Assurance Components
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives for the operational environment (ASE_OBJ.1)
	Stated security requirements (ASE_REQ.1)
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Labelling of the TOE (ALC_CMC.1)
	TOE CM coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – sample (ATE_IND.1)
Vulnerability assessment (AVA)	Vulnerability survey (AVA_VAN.1)

5.4.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDcPPv2.0e. As such, the NDcPPv2.0e SAR rationale is deemed acceptable since the PP itself has been validated.

5.5 Assurance Measures

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

Table 17 Assurance Measures

Assurance Class / 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	<p>Section 2 of this ST includes the TOE and ST conformance claim to CC Version 3.1, Revision 4, dated: September 2012, CC Part 2 extended and CC Part 3 conformant and NDcPPv2.0e and the rationale of how TOE provides all of the functionality at a level of security commensurate with that identified in NDcPPv2.0e. Section 2 also includes the consistency rationale for the TOE Security Problem Definition and the Security Requirements to include the extended components definition.</p> <p>Section 1 in this ST provides the introduction of the ST, the TOE and its references, an overview of the TOE, the TOE product type and the description of the TOE to include the evaluated configuration and the physical and logical cope of the TOE.</p> <p>Section 5 of this ST identifies the security functional requirements, the assurance requirements and how the assurance requirements are met. Section 6 provides the rationale of how the Security Functional Requirements are met by the TOE</p>
Development (ADV) / 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. The interfaces are described in terms of</p> <ul style="list-style-type: none"> • their purpose (general goal of the interface), • method of use (how the interface is to be used), • parameters (explicit inputs to and outputs from an interface that control the behaviour of that interface), • parameter descriptions (tells what the parameter is in some meaningful way), and • error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes) <p>The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.</p>
Guidance documents (AGD) / AGD_OPE.1	<p>The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.</p>
Guidance documents (AGD) / AGD_PRE.1	<p>The Installation Guide describes the installation, generation and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.</p>
Life cycle support (ALC) / ALC_CMC.1	<p>The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s) identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.</p>
Life cycle support (ALC) / ALC_CMS.1	
Tests (ATE) / ATE_IND.1	<p>Cisco will provide the TOE for testing.</p>

Assurance Class / Component	How requirement will be met
Vulnerability assessment (AVA) / AVA VAN.1	Cisco will provide the TOE for testing.

6 TOE SUMMARY SPECIFICATION

6.1 TOE Security Functional Requirement Measures

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

Table 18 How TOE SFRs Measures

TOE SFRs	How the SFR is Met
FAU_GEN.1	<p>By default, the TOE generates logs for the required events that are stored internally in a log file within the TOE whenever an audited event occurs. The log file is a rotating local log file that overwrites logs as the allocated space fills, and it is not accessible for administrators to edit or tamper with. The log files can be securely sent to one or more configured remote syslog servers using TLS.</p> <p>The types of events that cause audit records to be generated include administrative events, security configuration changes, cryptography related events, identification and authentication related events. The specific events and the contents of each audit record are listed in Table 15 Auditable Events. Each of the events are specified in the syslog internal to the TOE 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. For cryptographic key related events, the details of the certificate associated with the private key are included within the audit record to identify the key operated on. Additionally, the startup and shutdown of the audit functionality is audited. The start and stop of auditing is equated with turning on/booting and shut-down of the TOE.</p> <p>Following are a few examples of audit records. Refer to the Cisco Expressway X12.5 System Common Criteria Configuration Guide for examples of each required auditable event.</p> <p>admin login/logout: ----- 2016-06-16T14:57:42.915+00:00 dchokshi-exp-c taa-chkpasswd: Event="pam" Module="pam_unix(taa-chkpasswd-webadmin:session)" Level="INFO" Detail="session opened for user admin by (uid=2)" UTCTime="2016-06-16 14:57:42" 2016-06-16T14:57:42.917+00:00 dchokshi-exp-c httpd[12201]: web: User="admin" Event="Admin Session Start" Src-ip="10.122.81.100" Src-port="55924" UTCTime="2016-06-16 14:57:42"</p> <p>2016-06-16T14:58:31.731+00:00 dchokshi-exp-c httpd[23604]: web: User="admin" Event="Admin Session Finish" Src-ip="10.122.81.100" Src-port="56108" UTCTime="2016-06-16 14:58:31"</p> <p>admin timeout: ----- 2016-06-16T14:59:23.912+00:00 dchokshi-exp-c taa-chkpasswd: Event="pam" Module="pam_unix(taa-chkpasswd-webadmin:session)" Level="INFO" Detail="session opened for user admin by (uid=2)" UTCTime="2016-06-16 14:59:23" 2016-06-16T14:59:23.914+00:00 dchokshi-exp-c httpd[13502]: web: User="admin" Event="Admin Session Start" Src-ip="10.122.81.100" Src-port="56334" UTCTime="2016-06-16 14:59:23"</p> <p>2016-06-16T15:29:24.810+00:00 dchokshi-exp-c httpd[15188]: web: User="" Event="Admin Session Finish" Src-ip="10.122.81.100" Src-port="35362" Detail="expired" UTCTime="2016-06-16 15:29:24"</p>

TOE SFRs	How the SFR is Met
FAU_GEN.2	<p>The log entry includes the user credentials that triggered the event, the event and the outcome of the event. For example, for 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, host name, or other configured identification is presented. For cryptographic keys, when the Authorized administrator generates keys or deletes keys, the event is audited with the relevant information as listed below, to include the type of key (e.g. rsa).</p> <p>Following is the audit record format:</p> <p style="padding-left: 40px;">Date/time of event, the user (human or device), the event, where the event occurred, and the outcome of the event</p>
FAU_STG_EXT.1	<p>Audit records from both Expressway C and Expressway E components are written to the local storage and can also be sent to one or more configured remote syslog servers. For a secure connection to the remote syslog server(s), TLS is used. Once the configuration settings to the remote syslog server(s) and the level of auditing is configured, as the audit records are generated they are automatically sent to the remote syslog server(s) in real time.</p> <p>The TOE event log is a 2GB rotating local log file. When the space is nearing exhaustion, the oldest entries will be overwritten.</p> <p>The types of events that cause audit records to be generated include administrative events, security configuration changes, cryptography related events, identification and authentication related events. The specific events and the contents of each audit record are listed in Table 15 Auditable Events.</p> <p>Each of the events is specified in the syslog internal to the TOE 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.</p> <p>The Authorized Administrator can specify the local event log verbosity of the event information that is recorded locally. The verbosity level controls the granularity of the event logging with 1 as the least verbose and 4 the most. It is recommended to set the level at 2.</p> <p>As noted above, the event log is a rotating log file where older records may be over-written. However, there is no interface in which the Authorized Administrator can access the records.</p> <p>Refer to the Cisco Expressway X12.5 System Common Criteria Configuration Guide for full details and configuration settings.</p>
FCO_CPC_EXT.1	<p>The Authorized Administrator can configure MRA mode between Cisco Expressway C and Expressway E using SSH to secure the connections. This is a persistent, dedicated SSHv2 connection between the two components. This connection protects the TSF data from disclosure and allows for detection of modification.</p> <p>The MRA mode provides to provide a gateway solution that extends the services and access to users inside and outside of the organization's firewall.</p> <p>Refer to the Cisco Expressway X12.5 System Common Criteria Configuration Guide for full details and configuration settings.</p>

TOE SFRs	How the SFR is Met									
<p>FCS_CKM.1 FCS_CKM.2</p>	<p>The TOE utilizes a cryptographic module, Cisco FIPS Object Module to provide the cryptographic functions. Refer to Table 6 FIPS References for the listing of the CAVP certificate for each of the related SFRs.</p> <p>For key generation for asymmetric keys the TOE implements RSA with key size 2048 bits according to FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3 and ECC with NIST curves P-256 and P-384 that meets FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4.</p> <p>The TOE supports key establishment including RSA-based schemes that meets RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 and Elliptic curve-based schemes that meets NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”.</p> <table border="1" data-bbox="565 688 1383 997"> <thead> <tr> <th data-bbox="571 697 834 728">Scheme</th> <th data-bbox="834 697 1097 728">SFR</th> <th data-bbox="1097 697 1377 728">Service</th> </tr> </thead> <tbody> <tr> <td data-bbox="571 728 834 873">RSA (2048) ECC (P-256 / P-384)</td> <td data-bbox="834 728 1097 873">FCS_TLSC/S_EXT.2</td> <td data-bbox="1097 728 1377 873">Remote Administration Transmit audit log records to remote syslog server</td> </tr> <tr> <td data-bbox="571 873 834 997"></td> <td data-bbox="834 873 1097 997">FCS_SSHC/S_EXT.1</td> <td data-bbox="1097 873 1377 997">Authentication of Expressway C and Expressway E for MRA mode</td> </tr> </tbody> </table> <p>Using the GUI, the Authorized Administrator can generate a RSA public-private key pair, with a minimum RSA key size of 2048-bit and ECDSA key pairs using NIST curves P-256 and P-384. Both the RSA and ECC schemes can be used to generate a Certificate Signing Request (CSR) for X509 certificates that are used for securing SSH and TLS sessions.</p> <p>The TOE complies with section 5.6 and all subsections regarding asymmetric key pair generation in the NIST SP 800-56A and with section 6 and all subsections regarding RSA key pair generation. The TOE employs RSA-based key establishment, RSAES-PKCS1-v1_5 used in cryptographic operations as specified in Section 7.2 of RFC 8017.</p> <p>The TOE operates as both a SSH Server and a SSH Client for the secure connection between the Expressway C and Expressway E in support of MRA mode. As such, the TOE functions as both a sender and recipient for X509v3-ssh-rsa based key establishment schemes. ECDH is used for key exchange for the SSHv2 sessions</p> <p>The TOE also operates as both a TLS Server and a TLS Client. As such, the TOE functions as both a sender and recipient for RSA-based key establishment schemes.</p> <p>For details on each protocol, see the related SFRs.</p>	Scheme	SFR	Service	RSA (2048) ECC (P-256 / P-384)	FCS_TLSC/S_EXT.2	Remote Administration Transmit audit log records to remote syslog server		FCS_SSHC/S_EXT.1	Authentication of Expressway C and Expressway E for MRA mode
Scheme	SFR	Service								
RSA (2048) ECC (P-256 / P-384)	FCS_TLSC/S_EXT.2	Remote Administration Transmit audit log records to remote syslog server								
	FCS_SSHC/S_EXT.1	Authentication of Expressway C and Expressway E for MRA mode								
<p>FCS_CKM.4</p>	<p>The TOE meets all requirements as specified by the cryptographic key destruction method of the keys and the Critical Security Parameters (CSPs) when no longer required for use.</p> <p>The keys are destroyed by overwriting with a new key and can be verified by accessing the Trusted CA certificate page (Maintenance > Security certificates > Trusted CA certificate) and verified through clicking Show all (PEM file).</p>									

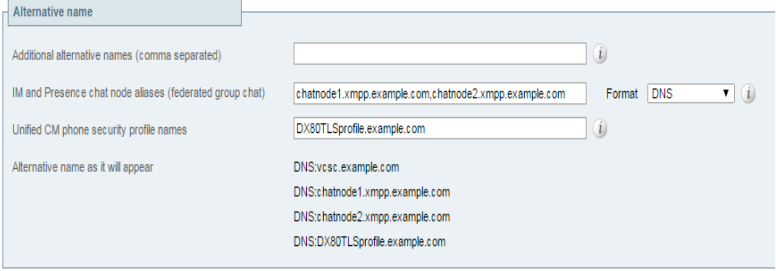
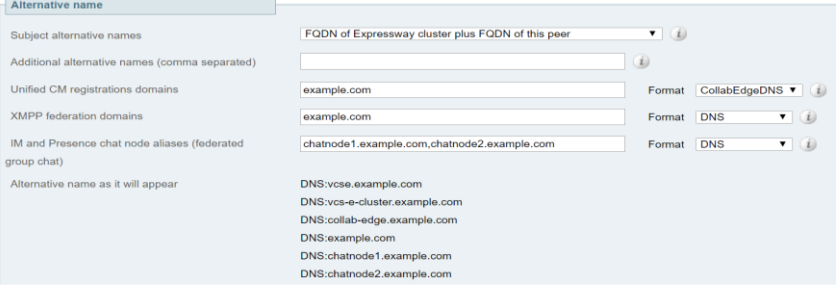
TOE SFRs	How the SFR is Met
	<p>The keys can also be destroyed by clicking on Delete and then selecting the applicable PEM file.</p> <p>Additionally, none of the credentials, CRLs, symmetric keys, pre-shared keys, or private keys are stored in plaintext form.</p> <p>See Table 19: TOE Key Zeroization in Section 7.1 Key Zeroization. The information provided in the table includes all the secrets, keys and associated values, the description, and the method used to zeroization when no longer required for use. This information is provided in the reference section for ease and readability of the all secrets, keys and associated values, their description and zeroization methods.</p>
FCS_COP.1/DataEncryption	<p>The TOE provides symmetric encryption and decryption capabilities using AES in CBC, CTR and GCM mode (128, 256 bits) as described in AES and specified in ISO 18033-3, CBC as specified in ISO 10116, CTR as specified in ISO 10116 and GCM as specified in ISO 19772.</p> <p>Through the implementation of the cryptographic module, the TOE provides AES encryption and decryption in support of SSH, HTTPS and TLS for secure communications.</p> <p>The configuration and management of the cryptographic algorithms is provided through the TOE GUI, to include the auditing of configuring the options by the Authorized Administrator.</p> <p>The relevant FIPS certificate numbers are listed in Table 6 Algorithm Certificate References</p>
FCS_COP.1/SigGen	<p>The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 as specified in FIPS PUB 186-4, “Digital Signature Standard (DSS)” Section 5.5.</p> <p>Through the implementation of the cryptographic module, the TOE provides cryptographic signatures in support of SSH, HTTPS and TLS for secure communications.</p> <p>The configuration and management of the cryptographic algorithms is provided through the TOE GUI, to include the auditing of configuring the options by the Authorized Administrator.</p> <p>The relevant FIPS certificate numbers are listed in Table 6 Algorithm Certificate References</p>
FCS_COP.1Hash	<p>The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384 and SHA-512 as specified in FIPS Pub 180-3 “Secure Hash Standard.”</p>
FCS_COP.1KeyedHash	<p>Through the implementation of the cryptographic module, the TOE provides SHS hashing and HMAC message authentication in support of HTTPS, TLS and SSH for secure communications and verification of software updates.</p> <p>The configuration and management of the cryptographic algorithms is provided through the TOE GUI, to include the auditing of configuring the options by the Authorized Administrator.</p> <p>The TOE supports SHS hashing and HMAC message authentication (SHA-1, SHA-256, SHA-384, SHA-512 and HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) that the Authorized Administrator can configure to be used with endpoints in the establishment of HTTPS and TLS sessions. The TOE provides keyed-hashing message authentication services using HMAC-SHA-1 and HMAC-SHA-256 operates on 512-bit blocks, HMAC-SHA-384 and HMAC-SHA-512 operate on 1024-bit blocks of data, with key</p>

TOE SFRs	How the SFR is Met
	<p>sizes and message digest sizes of 160-bits, 256 bits, 384 bits and 512 bits respectively) as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.</p> <p>The TOE also uses the hashing services for verification of the TOE software image integrity.</p> <p>The relevant FIPS certificate numbers are listed in Table 6 Algorithm Certificate References</p>
FCS_RBG_EXT.1	<p>The TOE is hardware and software comprised of the Cisco Expressway OS software image Release X12.5 and the hardware as described Table 5 Hardware Models and Specifications.</p> <p>The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90 seeded by an entropy source that accumulates entropy from a TSF-hardware based noise source.</p> <p>The deterministic RBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.</p>
FCS_SSHC/S_EXT.1	<p>For secure communications between Expressway C and Expressway E SSHv2 is configured. This is a persistent dedicated connection where Expressway-C acting as the SSH client and Expressway-E acting as the SSH Server. For the outbound port from Expressway-C (private) it is an ephemeral port to Expressway-E (DMZ) port 2222, a listening port. The Expressway-E listens on port 222 for SSH tunnel traffic and the only legitimate sender of SSH traffic is the Expressway-C. This connection forms a highly secure traversal link to provide a gateway solution that extends the services and access to users inside and outside of the organization’s firewall.</p> <p>Refer to the TOE guidance documentation, the Cisco Expressway Common Criteria Configuration Guide for configuration settings.</p> <p>The TOE implementation of SSHv2 protocol supports the following options as required in the evaluated configuration, with no additional optional characteristics beyond what is claimed in the 5.2.3.10 FCS_SSHC_EXT.1 SSH Client Protocol, 5.2.3.11 FCS_SSHS_EXT.1 SSH Server Protocol and as described below:</p> <ul style="list-style-type: none"> • Compliance to the following RFCs - 4251, 4252, 4253, 4254, 4344, 6187 and 6668 • Supports public-key authentication between Expressway C and Expressway E • Drops packets that are greater than 32768 bytes since that size is in violations with the IP packet size limitations. This is accomplished by buffering all data for a particular SSH packet transmission until the buffer limit is reached and then dropping the packet if this limit is exceeded • Once configured, only aes256-cbc and aes256-ctr encryption algorithms are allowed for use that ensures confidentiality of the session • Once configured, only x509v3-ssh-rsa public key algorithm is allowed for use for authentication • Once configured, only hmac-sha2-512 hashing algorithms are allowed for use to ensure the integrity of the session • Once configured, only ECDH (ecdh-sha2-nistp256 and ecdh-sha2-nistp384) key exchange method is allowed for use <p>The TOE can also be configured to ensure that SSH re-keying occurs prior to one hour of time or prior to more than one gigabyte of transmitted data for that session key.</p> <p>If the connection between Expressway C and Expressway E using SSHv2 is unintentionally broken, the connection will need to be re-established. The keys will be overwritten, new</p>

TOE SFRs	How the SFR is Met
	<p>keys will need to be generated and the connection reestablished as described in the TOE guidance documentation, the Cisco Expressway Common Criteria Configuration Guide.</p> <p>For details on key generation and destruction, see the related SFRs. Note, the x509v3-ssh-rsa key pairs are associated with the X509 certificate, not stored in plaintext and automatically stored in a specified filesystem directory. No optional SSH characters are supported by the TOE.</p>
<p>FCS_HTTPS_EXT.1, FCS_TLSC_EXT.2 and FCS_TLSS_EXT.2</p>	<p>The TOE supports HTTPS to secure the sessions for remote administration.</p> <p>The TOE supports TLS v1.1 and TLS v1.2 to protect the sessions to the remote audit server. Though it is recommended that TLSv1.2 be used to protect the sessions.</p> <p>The TOE also uses TLS for SIP trunking.</p> <p>The supported ciphersuites include the following:</p> <ul style="list-style-type: none"> • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC5289 <p>Once configured, the TOE will not establish TLS v1.0 and related SSL versions connections if offered by the client. In addition, the TOE will only establish a connection if the peer presents a valid certificate during the handshake.</p> <p>Following is the TLS with mutual authentication handshake and exchange of parameters between the client and the TOE. Note, elliptic curve extensions are not supported in the Client Hello.</p>

TOE SFRs	How the SFR is Met
	<div style="text-align: center;"> <pre> sequenceDiagram participant Client participant Server Note over Client: Client Hello Client sends the server the version of TLS it would like to use along with supported cipher. The client also sends a random string to be used later in the negotiation Client->>Server: Note over Server: Server Hello The server sends the TLS version and cipher that will be used. The server also sends a random string that will be used by the client later in the session. The server sends its certificate; proof of identification; and send a client certificate request 'done' Server-->>Client: Note over Client: Client sends secret that was generated using the random strings that is encrypted with the public key from the server's certificate and its certificate. The client lets the server know that all messages will now be encrypted and 'finished' Client->>Server: Note over Server: The server verifies the clients certificate and sends a message to the client that all messages will now be encrypted using the keys that were negotiated and 'finished'. Server-->>Client: Note over Client, Server: data Client <--> Server: data </pre> </div> <p>When acting as an HTTPS server, this exchange is conformant to RFC 2818.</p> <p>Where the TOE is the client, such as connecting to the remote syslog server, the handshake above is the same process except the server (remote syslog server) would not request the client certificate in the Server Hello, see the following:</p>

TOE SFRs	How the SFR is Met
	<div data-bbox="505 233 1240 1087" data-label="Diagram"> <pre> sequenceDiagram participant Client participant Server Note over Client: Client Hello Client sends the version of TLS it would like to use along with supported cipher. The client also sends a random string to be used later in the negotiation. Client->>Server: Note over Server: Server Hello The server sends the TLS version and cipher that will be used. The server also sends a random string that will be used by the client later in the session. The server sends its certificate; proof of identification and 'done'. Server-->>Client: Note over Client: Client sends secret that was generated using the random strings that is encrypted with the public key from the server's certificate. The client lets the server know that all messages will now be encrypted and 'finished'. Client->>Server: Note over Server: The server sends a message to the client that all messages will now be encrypted using the keys that were negotiated and 'finished'. Server-->>Client: Note over Client: data Note over Server: data Client<-><->Server: data </pre> </div> <p data-bbox="505 1157 1508 1276">Using wildcards is not supported in identity certificates, such as when you import the certificate and private key into Expressway. However, wild card certificates can be used as a trust certificate where it is the leftmost identifier, for example CN=*.webexconnect.com. IP addresses are not supported as reference identifiers.</p> <p data-bbox="505 1310 889 1339">Certificate pinning is not supported.</p> <p data-bbox="505 1373 1508 1520">Since RSA is being used for key exchange and authentication there are no specific parameters associated with the server key exchange. Using the above listed TLS_RSA ciphers the RSA public key (with a minimum RSA key size 2048) is used for authentication and key exchange. If using ECDHE or DHE ciphers, the standard diffie hellman parameters P, Q, and G are used for key exchange.</p> <p data-bbox="505 1554 1508 1644">The Expressway certificate signing request (CSR) tool prompts for and incorporates the relevant subject alternative name (SAN) entries as appropriate for the Unified Communications features that are supported on that Expressway.</p> <p data-bbox="505 1677 1508 1734">For example, Entering subject alternative names for security profiles and chat node aliases on the Expressway-C's CSR generator:</p>

TOE SFRs	How the SFR is Met
	 <p>and Entering subject alternative names for Unified CM registration domains, XMPP federation domains, and chat node aliases, on the Expressway-E's CSR generator</p> 
FIA_AFL.1	<p>The TOE provides the administrator the ability to specify the maximum number of unsuccessful authentication attempts before administrator is locked out. The number can be set between 1-3 attempts, with one (1) being the lowest setting allowed and three (3) being the maximum number of attempts allowed. If the account is locked by exceeding the number of attempts to login, local access will still be available, and the local Administrator must unlock the user account before the remote Administrator can attempt to login.</p> <p>To ensure the Administrator account does not get locked out by the number of failed attempts, the Emergency account must be enabled. This requires the use of an enabled local administrator account that has read-write access and web access. The purpose of this account is a work around to ensure administrator access to the TOE is available when remote authentication is not available. Access to this account should be limited and only used in when no other option is available to gain access to the TOE, such as another Authorized Administrator.</p> <p>Refer to the Cisco Expressway X12.5 System Common Criteria Configuration Guide for full details and configuration settings.</p>
FIA_PMG_EXT.1	<p>The TOE supports the local definition of users with corresponding passwords.</p> <p>In the evaluated configuration, the Enforce strict passwords must be set to <i>On</i>. When set to <i>On</i>, the following rules apply:</p> <ul style="list-style-type: none"> • Password can never be blank • No multiple instances of the same characters • No dictionary words • No palindromes, such as "risetovotesir" • Length must be at least 6 ASCII characters, but can be up to 255. The default is set to 15 characters. Minimum length will be enforced. This can range between 6 ASCII characters and 255. The default is set to 15 characters. The number that is

TOE SFRs	How the SFR is Met
	<p>set, is the minimum number of characters that will be required and values beyond that setting will be allowed</p> <ul style="list-style-type: none"> • Number of numeric digits [0-9] may be between 0 and 255 (default 2) • Number of uppercase letters [A-Z] may be between 0 and 255 (default 2) • Number of lowercase letters [a-z] may be between 0 and 255 (default 2) • Number of special characters [printable characters from 7-bit ASCII, eg. (space), @, \$ etc.] may be between 0 and 255 (default 2) • Number of consecutive repeated characters allowed may be between 1 and 255 (the default 0 disables the check, so consecutive repeated characters are allowed by default; set it to 1 to prevent a password from containing any consecutive repeats) • The minimum number of character classes may be between 0 and 4 (the default 0 disables the check). Character classes are digits, lowercase letters, uppercase letters, and special characters.
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 except for the login warning banner that is displayed prior to user authentication and any network packets as configured by the authorized administrator may flow through the TOE. This is required for both the local and remote GUI interfaces.</p>
FIA_UAU_EXT.2	<p>Administrative access to the TOE is facilitated through the TOE's GUI. The TOE mediates all administrative actions through the GUI. Once a potential administrative user attempts to access the GUI of the TOE through a HTTPS secured connection, the TOE prompts the user for a user name and password credentials. Only after the administrative user presents the correct authentication credentials (user name and password) will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an Authorized Administrator is successfully identified and authenticated, which constitutes a successful login.</p>
FIA_UAU.7	<p>All passwords on the Expressway are encrypted, so you only see placeholder characters. The TOE does not echo any characters as they are entered.</p>
FIA_X509_EXT.1/ITT	<p>The TOE uses X.509v3 certificates as defined by RFC 5280 to support mutual authentication for TLS connections. The certificate request message includes the public key and common name per RFC 2986. The CN naming attributes in the certificate is compared with the expected CN naming attributes and deemed valid if the attribute types are the same and the values are the same and as expected.</p> <p>X.509v3 certificates are also used to support authentication for the SSH connections between Expressway C and Expressway E components. This is a persistent, dedicated SSHv2 connection between the two components with no revocation method.</p> <p>The TOE supports the following methods to obtain a certificate from a CA:</p> <ul style="list-style-type: none"> • Third-party-signed certificates – the certificates are uploaded, to include the certificate authority root certificate of the certificate authority that signed an application certificate. You can also upload the PKCS#7 format certificate chain of all certificate authority certificates • Self-signed certificate enrollment for a trust point <p>The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. The administrator may configure the level to which a certificate chain is processed on all certificates including subordinate CA certificates. If a</p>
FIA_X509_EXT.1/Rev	
FIA_X509_EXT.2	
FIA_X509_EXT.3	

TOE SFRs	How the SFR is Met
	<p>connection cannot be established with the trust point to verify the certificate validity, the TOE will continue to accept the certificate.</p> <p>There is a configuration knob labels ‘Client certificate-based security’. If you set it to Certificate Validation, you will enter this mode. To enter this mode, you must upload a CA certificate to use for client certificate verification and the latest CRL for that CA since all CRLs in the trusted certificate chain of the CA that issued the client’s certificate are checked. Certificate chains are uploaded to the TOE via the TOE GUI. Once a certificate is uploaded to the TOE, endpoints connecting to the TOE which are signed by the configured certificate chains may be used for secure connections with the TOE. In the case where multiple certificate chains are configured on the TOE, the TOE compares peer presented endpoint certificates to each of the configured certificate chains to verify the validity of the certificate. If the presented certificate is not signed by any of the configured chains, the TOE will deny the configuration.</p> <p>Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The certificate(s) that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensures that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted. Additional checking of the extendedKeyUsage field includes the server and client authentication.</p> <p>Additionally, the certificates themselves provide protection in that they are digitally signed. If a certificate is modified in any way, it would be invalidated. The digital signature verifications process would show that the certificate had been tampered with when the hash value would be invalid.</p> <p>The physical security of the TOE (A.PHYSICAL_PROTECTION) protects the TOE and the certificates from being tampered with and/or deleted. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE.</p> <p>Furthermore, the certificates are stored in a hidden and protected directory on the TOE that has no external interfaces to gain access.</p>
FMT_MOF.1(1)/ManualUpdate	<p>The TOE does not provide automatic updates to the software version running on the TOE.</p> <p>The Authorized Administrators can query the software version running on the TOE and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates.</p>
FMT_MTD.1/CoreData	<p>The TOE provides the ability for Authorized Administrators to access TOE data, such as audit data, configuration data, security attributes and login banners via the GUI.</p> <p>The term “Authorized Administrator” is used in this ST to refer to any user which is permitted to perform the relevant action.</p>
FMT_MTD.1/CryptoKeys	<p>The TOE provides the ability for Authorized Administrators to generate and manage the cryptographic keys that used to secure connections on the TOE. The Authorized Administrators accesses the GUI for manage of the cryptographic functions.</p> <p>The term “Authorized Administrator” is used in this ST to refer to any user that is permitted to perform the relevant action.</p>
FMT_MTD.1/SystemTime	<p>The TOE provides the ability for the Authorized Administrators to synchronize the date and timestamp with an NTP server. The connection to the NTP server is NTPv4.</p>

TOE SFRs	How the SFR is Met
	<p>The NTP Server is required in the IT environment in support of synchronize time stamps for the TOE. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond, thus ensuring the TOE provides a reliable timestamp.</p>
FMT_SMF.1	<p>The TOE provides all the functionality for the Authorized Administrator that is required to configure and manage the TOE in a secure manner. The Authorized Administrator can securely connect to the TOE using the GUI via HTTPS over TLS to perform these functions or at the local console.</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 GUI as described above; • The ability to configure a notice and consent warning banner that is displayed prior to logging on the TOE; • The ability to configure inactivity session time periods; • The ability to update the TOE software (using hash comparisons) • The ability to configure the authentication failure parameters • The ability to configure the auditing capabilities and the secure transmission of the logs to a remote syslog server • The ability to configure the cryptographic functionality • The ability to configure the communications and interactions between TOE components, • The ability to manage and change user passwords and • The ability to configure NTP server for a reliable timestamp
FMT_SMR.2	<p>The term “Authorized Administrator” is used in this ST to refer to any user that has been assigned administrative privileges that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions.</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 authentication via HTTPS over TLS secure connection.</p>
FPT_APW_EXT.1	<p>The TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. Additionally, all pre-shared keys, symmetric keys and CRLs are stored in encrypted form to prevent access.</p> <p>The TOE also ensures that passwords will not be stored in plaintext. The Administrator passwords are stored in a database where the password is encrypted before being stored.</p>
FPT_SKP_EXT.1	
FPT_ITT.1	<p>The TOE configured in MRA mode to provide a gateway solution that extends the services and access to users inside and outside of the organization’s firewall. As such, the TOE will be configured to only to use x.509v3-ssh-rsa public key algorithm for secure connection between Expressway-C and Expressway-E in MRA mode. This is a persistent, dedicated SSHv2 connection between the two components. This connection protects the TSF data from disclosure and allows for detection of modification.</p>
FPT_STM_EXT.1	<p>The TOE provides a source of date and time information that is used as the time stamp applied to the generated audit records and used to track inactivity of administrative sessions. This source is also used for cryptographic functions. A reliable timestamp is also required to display the correct data and time for the users and tags the correct date and time for SIP calls and media traffic.</p> <p>The TOE synchronizes with an NTP server for its reliable and accurate timestamp. The TOE can be configured to support up to five (5) NTP servers. The TOE supports NTPv4 and</p>

TOE SFRs	How the SFR is Met
	<p>validates the integrity of the time-source using SHA1 symmetric key authentication. In addition, the TOE does not allow the timestamp to be updated from broadcast addresses.</p> <p>Expressway maintains its system time in UTC (Coordinated Universal Time) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond⁵.</p> <p>If no NTP servers are available, then Expressway uses its own operating system time to determine the time and date. As mentioned above Expressway maintains its own system time in UTC format. By specifying the local time zone, allows Expressway to determine the local date/time based on where the system is located. It does this by offsetting UTC time by the number of hours (or factions of hours) associated with the selected time zone. There is no other interface to adjust the 'timestamp' beyond setting the time zone. This design facilitates an accurate date/timestamp without relying on outside intervention.</p> <p>Also note, the UTC timestamps are included at the end of each entry in the Event Log. The local time zone is used to set the timestamp that appears at the start of each line in the Event Log.</p>
FPT_TUD_EXT.1	<p>The Authorized Administrator can query the software version running on the TOE by accessing the Administration web page that displays the system version and can initiate updates to (replacements of) software images.</p> <p>When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from Cisco.com website.</p> <p>The image verification, a SHA-512 hash is used to verify software/firmware update file to make sure it has not been modified from the original distributed by Cisco before it is used to update the TOE.</p> <p>Once the Authorized Administrator has verified the TOE image, the Authorized Administrator can install the file on the TOE after they have logged in and have been successfully identified and authenticated.</p> <p>If the verification of the image files fails, the Authorized Administrator is instructed to contact Cisco Technical Assistance Center (TAC).</p> <p>For full details on downloading and installing the TOE software, refer to the Cisco Expressway X12.5 System Common Criteria Operational User Guidance And Preparative Procedures.</p>
FPT_TST_EXT.1	<p>The TOE runs a suite of self-test during initial start-up to verify its correct operation. 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.</p> <p>The TOE also runs a periodic continuous random number generator health test, which will also be run any time a request for entropy is made by the application.</p> <p>If any of the tests fail, the TOE will not boot, and the Authorized Administrator is instructed to contact Cisco Technical Assistance Center (TAC).</p>

⁵ <http://searchnetworking.techtarget.com/definition/Network-Time-Protocol>

TOE SFRs	How the SFR is Met
	<p>During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include:</p> <ul style="list-style-type: none"> • Power-on Self-Tests Self-tests are performed automatically at power-up and does not require operator intervention to run. Once the module is turned on or reloaded, the power-up self-tests are initiated automatically. 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. If the file image that includes the cryptographic module (FOM), checksums or certificate signatures were tampered with or modified in anyway, the installation would halt or if an error in the cryptographic module (FOM) a log message to indicate FIPS POST failure will be logged and the TOE will reboot at which time the Administrator will need to call Cisco TAC to obtaining technical assistance. If all the checks of the image software passes, to include the cryptographic module (FOM), there will be no log message other than to indicate that the POST started and POST finished and the Administrator will be presented with the logon prompt. <p>Prior to installing the image, the Authorized Administrator can verify the public hash to ensure the files has not been tampered with prior to installing. In addition, the Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity.</p> <p>The tests are run on all components of the TOE to ensure correct operation of the TOE.</p>
FTA_SSL_EXT.1	The Authorized Administrator can configure maximum inactivity times individually for both local and remote administrative sessions using the GUI System administration web page.
FTA_SSL.3	<p>The default setting is 30 minutes, though this can be changed for up to 65535 minutes in which the session can be inactive before the session is timed-out.</p> <p>The session has been ended due to inactivity, the Authorized Administrator will have to log back in with the correct user name and password credentials.</p>
FTA_SSL.4	An Authorized Administrator is able to exit out of both local and remote administrative sessions by clicking on the 'Log Out' icon that appears on the top right corner of every page. By clicking on the icon, the session will end.
FTA_TAB.1	The Authorized administrator can define a custom login banner that will be displayed on the GUI management interface and the local console interface prior to allowing any administrative access to the TOE. This is applicable for both local and remote TOE administration.
FTP_ITC.1	The TOE protects communications between the TOE and the remote audit server using TLS that provides a secure channel to transmit the log events, supports NTPv4 for the connection to the NTP server and SSHv2 between Expressway C and Expressway E.
FTP_TRP.1	All remote administrative communications take place over a secure encrypted HTTPS session. The HTTPS session is over TLS. The remote users (Authorized Administrators) can initiate HTTPS communications with the TOE.

7 ANNEX A: KEY ZEROIZATION

7.1 Key Zeroization

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

Table 19: TOE Key Zeroization

Name	Description	Storage	Zeroization
NTP Keys	This is the key that is used for encryption and decryption of authentication of NTP packets. NVRAM	NVRAM	Zeroized by overwriting with new key
User Password	This is a variable 15+ character password that is used to authenticate local users.	NVRAM	Zeroized by overwriting with new password
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents) using memset. This overwrites the key with all 0's.	SDRAM	Zeroized by overwriting with new key
SSH Session Key	The results zeroized using the positioning in free to overwrite the values with 0x00. This is called by the ssh_close function when a session is ended.	SDRAM	Automatically when the SSH session is terminated. Overwritten with: 0x00
TLS server private key	This key is used for authentication, so the server can prove who it is. The private key used for TLS secure connections.	NVRAM	Zeroized by overwriting with new key
TLS server public key	This key is used to encrypt the data that is used to compute the secret key. The public key used for TLS secure connection.	NVRAM	Zeroized by overwriting with new key
TLS pre-master secret	The pre-master secret is the client and server exchange of random numbers and a special number, the pre-master secret, This, pre-master secret is using asymmetric cryptography from which new TLS session keys can be created.	SDRAM	Automatically after TLS session terminated. Overwritten with: 0x00
TLS session encryption key	The session encryption key is unique for each session and is based on the shared secrets that were negotiated at the start of the session. The Key is used to encrypt TLS session data.	SDRAM	Automatically after TLS session terminated. Overwritten with: 0x00
TLS session integrity key	This key is used to provide the privacy and TLS data integrity protection.	SDRAM	Automatically after TLS session terminated. The entire object is overwritten with zeros

8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 20: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 4, dated September 2012
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 4, dated September 2012
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, April 2017, version 3.1, Revision 4, dated September 2012
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, April 2017, version 3.1, Revision 4, dated September 2012
[NDcPP]	collaborative Protection Profile for Network Devices+ Errata 20180314, Version 2.0e, 14 March 2018
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008
[FIPS PUB 186-4]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2013
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[800-90]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2012
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008