
Cisco Email Security Appliance Security Target

Version: 1.0

Date: 12 September 2024



Americas Headquarters:

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

Table of Contents

Table of Contents	2
List of Tables	4
List of Figures	4
1 SECURITY TARGET INTRODUCTION.....	8
1.1 ST and TOE Reference	8
1.2 TOE Overview	8
1.2.1 TOE Product Type.....	9
1.2.2 Supported non-TOE Hardware/ Software/ Firmware	9
1.3 TOE DESCRIPTION	10
1.4 TOE Evaluated Configuration	12
1.5 Physical Scope of the TOE	12
1.6 Logical Scope of the TOE.....	20
1.6.1 Security Audit.....	20
1.6.2 Cryptographic Support.....	21
1.6.3 Identification and authentication	24
1.6.4 Security Management.....	24
1.6.5 Protection of the TSF	25
1.6.6 TOE Access	25
1.6.7 Trusted path/Channels	25
1.7 Excluded Functionality	25
2 Conformance Claims	27
2.1 Common Criteria Conformance Claim	27
2.2 Protection Profile Conformance	27
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	31
3	SECURITY PROBLEM DEFINITION	32
3.1	Assumptions.....	32
3.2	Threats	34
3.3	Organizational Security Policies.....	36
4	SECURITY OBJECTIVES.....	37
4.1	Security Objectives for the TOE	37
4.2	Security Objectives for the Environment.....	37
5	SECURITY REQUIREMENTS.....	39
5.1	Conventions	39
5.2	TOE Security Functional Requirements	39
5.2.1	Security audit (FAU)	41
5.2.2	Cryptographic Support (FCS).....	45
5.2.3	Identification and authentication (FIA).....	50
5.2.4	Security management (FMT)	52
5.2.5	Protection of the TSF (FPT)	53
5.2.6	TOE Access (FTA).....	54
5.2.7	Trusted Path/Channels (FTP)	55
5.3	TOE SFR Dependencies Rationale for SFRs Found in NDcPPv2.2e	56
5.4	Security Assurance Requirements	56
5.4.1	SAR Requirements	56
5.4.2	Security Assurance Requirements Rationale.....	57
5.5	Assurance Measures	57
6	TOE Summary Specification	59
6.1	TOE Security Functional Requirement Measures	59
7	Annex A: Key Zeroization	83
7.1	Key Zeroization	83
8	Annex B: References	85

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	13
TABLE 6 PROCESSORS AND FOM	22
TABLE 7 FIPS REFERENCES	22
TABLE 8 EXCLUDED FUNCTIONALITY	25
TABLE 9: PROTECTION PROFILES.....	27
TABLE 10:NIAP TECHNICAL DECISIONS (TD)	27
TABLE 11: TOE ASSUMPTIONS	32
TABLE 12: THREATS.....	34
TABLE 13: ORGANIZATIONAL SECURITY POLICIES	36
TABLE 14: SECURITY OBJECTIVES FOR THE ENVIRONMENT	37
TABLE 15: SECURITY FUNCTIONAL REQUIREMENTS	40
TABLE 16: AUDITABLE EVENTS	42
TABLE 17: ASSURANCE MEASURES.....	56
TABLE 18: ASSURANCE MEASURES.....	57
TABLE 19: HOW TOE SFRS ARE MET	59
TABLE 20: TOE KEY ZEROIZATION.....	83
TABLE 21: REFERENCES	85

List of Figures

FIGURE 1: TOE EXAMPLE DEPLOYMENT.....	11
---------------------------------------	----

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
ESA	Email Security Appliance
GCM	Galois Counter Mode
HTTPS	Hyper-Text Transport Protocol Secure
IP	Internet Protocol
IT	Information Technology
NDcPP	collaborative Network Device Protection Profile
PP	Protection Profile
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 Functionality TSF = TOE for pND TSF = TOE + VS for vND
TSP	TOE Security Policy

Terminology

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

Table 2 Terminology

Term	Definition
Authorized Administrator	Any user that has been assigned to a privilege level that is permitted to perform all TSF-related functions.
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 Email Security Appliance (ESA) running ESA AsyncOS 15.5. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE, which meet the set of requirements. Administrators of the TOE will be referred to as Administrators, Authorized Administrators, 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 Email Security Appliance Common Criteria Security Target
ST Version	1.0
Publication Date	12 September 2024
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Email Security Appliance
TOE Hardware Models	C195, C395, C695, C695F and the virtual appliances running on UCS platforms, C100v, C300v and C600v on UCS-C220-M5, UCS-240-M5, UCS-480-M5, UCS-C220-M6, and UCS-240-M6.
TOE Software Version	ESA AsyncOS 15.5
Keywords	Email, Data Protection, Authentication, Network Device

1.2 TOE Overview

The TOE, which consists of the Cisco Email Security Appliance, is a network device. ESA is an appliance that provides comprehensive email protection services for a company's email system. It is an email protection product that monitors Simple Mail Transfer Protocol (SMTP) network traffic, analyzes the monitored network traffic using various techniques, and reacts to identified

threats associated with email messages (such as spam and inappropriate or malicious content). The TOE includes the hardware models as defined in Table 3 in section 1.1.

1.2.1 TOE Product Type

Cisco ESA is a network device that provides connectivity and security services, including the capability to secure and control traffic in one device. ESA serves as a secure SMTP gateway, providing the Message Transfer Agent (MTA) role in the customer's network infrastructure. Even though the email protection services are contained within the TOE, this functionality was not evaluated.

Cisco ESA provides two management interfaces: a Command Line Interface (CLI) and a web-based Graphical User Interface (GUI). The GUI contains most of the functionality to configure and monitor the TOE. However, not all CLI commands are available in the GUI; some features are only available through the CLI.

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
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration using the CLI interface through SSH protected channels. Any SSH client that supports SSHv2 may be used.
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 using the web GUI interface through HTTPS/TLS protected channels. Any web browser that supports TLSv1.1 and TLSv1.2 with the supported ciphersuites may be used.
Local Console	Yes	This includes any IT Environment console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
SMTP Server	Yes	This includes any SMTP servers that the TOE receives and sends email traffic. This functionality was not evaluated.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit audit log messages using SCP over a secure SSHv2 trusted channel.

Component	Required	Usage/Purpose Description for TOE performance
CA Server	Yes	This includes any IT Environment CA Server to validate X509 certificates
Update Server	Yes	This includes updates for the potentially malicious files of various types to filter traffic for restricted content. This functionality was not evaluated.

1.3 TOE DESCRIPTION

This section provides an overview of ESA Target of Evaluation (TOE). ESA is a security appliance that is installed between an external network and the customer's internal network. Traffic flowing to and from the external network to the internal network is first routed through the ESA.

The Cisco ESA AsyncOS 15.5 is a Cisco-developed highly configurable proprietary operating system (based on FreeBSD 13) that can detect potentially malicious files of various types, filter traffic for restricted content, and detect email containing spam messages or phishing attempts. This TOE only addresses the functions that provide for the security of the TOE itself as described in Section 1.6 Logical Scope of the TOE below.

The TOE comprises both software and hardware. The TOE deployment is ESA running ESA AsyncOS 15.5 software installed on one of the platforms, all of which are described below.

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

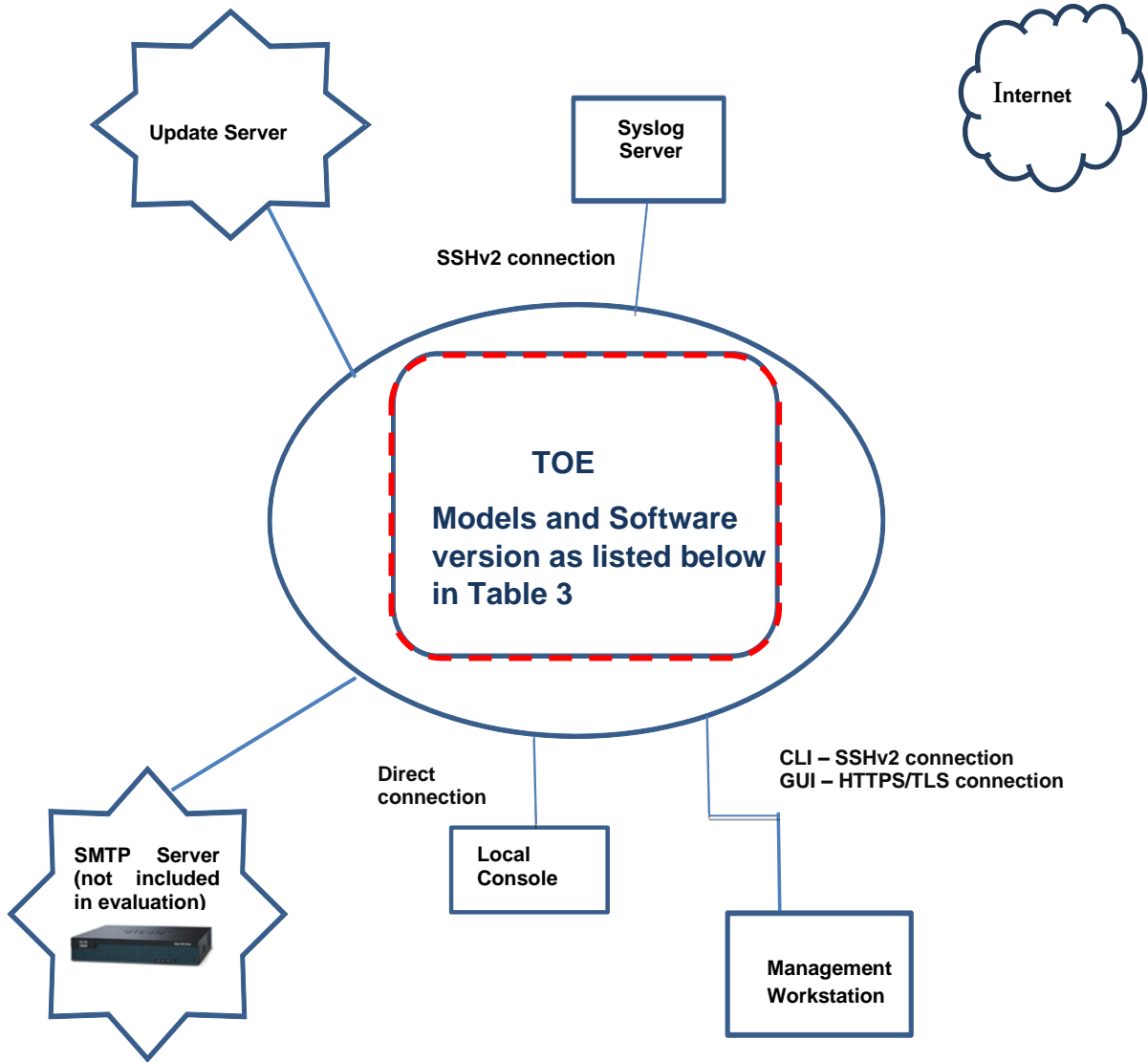


Figure 1: TOE Example Deployment

The previous figure includes the following devices:

- The TOE ESA appliances include:
 - C195, C395, C695, C695F and the virtual appliances - C100v, C300v and C600v, running on UCS platforms - UCS-C220-M5, UCS-C240-M5, UCS-C480-M5, UCS-C220-M6, and UCS-C240-M6 - all running Cisco ESA AsyncOS software version 15.5
- The following are considered to be in the IT Environment:
 - Local Console to support local Administration (direct connection)
 - Management Workstation to support remote Administration (secure connection is SSHv2 for the CLI and HTTPS/TLS for the GUI)
 - Syslog Server (secure connection is SCP over SSHv2)
 - Update Server
 - Certificate Authority (CA)
- The following are part of the IT Environment but are not evaluated
 - SMTP Server

1.4 TOE Evaluated Configuration

The TOE consists of one or more appliances as specified in section 1.5 Physical Scope of the TOE below, and includes the ESA AsyncOS software version 15.5.

In addition, if the TOE is to be remotely administered, then the management workstation must be connected to an internal network, SSHv2 must be used to remotely connect to the appliance for the CLI interface and HTTPS/TLS for the GUI interface.

A syslog server is used to store audit records, and the connection is secured using SCP over SSHv2. It is recommended that these servers be installed on the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic, in a controlled environment where implementation of security policies can be enforced.



1.5 Physical Scope of the TOE



The TOE is a hardware and software solution that makes up the Cisco ESA. The TOE hardware includes the following: C195, C395, C695, C695F and the C100v, C300v, C600v running on Cisco UCS servers. The TOE software is the ESA AsyncOS software version 15.5.



The network, on which they reside, is considered part of the environment.


The TOE comprises the following physical specifications as described in Table 5 Hardware Models and Specifications below.

Table 5 Hardware Models and Specifications



Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
<p>C195</p> <p>Intel Xeon Silver 4110 (Skylake) processor</p> <p>ESA AsyncOS software version 15.5</p>		<p>1RU: 1.7 x 16.89 x 29.8 in. (4.32x 43.0 x 75.6 cm)</p>	<p>One 770W</p> <p>Redundant power supply</p>	<p>Two 1-GB Base-T Ethernet LAN ports, can be used as management ports</p> <p>RAID mirroring</p> <p>10/100/1000 Mbps</p> <p>Two 600-GB hard disk drives (2.5" 10K SAS) hot swappable access for SAS drives</p> <p>One- 16GB DDR4-2133 DIMM1</p>
<p>C395</p> <p>Intel Xeon Silver 4116 (Skylake) processor</p> <p>ESA AsyncOS software version 15.5</p>		<p>1RU: 1.7 x 16.89 x 29.8 in. (4.32x 43.0 x 75.6 cm)</p>	<p>Two 770W</p> <p>Redundant power supply</p>	<p>Six 1-Gb Base-T Ethernet LAN ports</p> <p>One management interface (RJ-45), restricted to management use only</p> <p>RAID mirroring</p> <p>10/100/1000</p> <p>Two 600 GB hard disk drives (2.5" 10K SAS) hot swappable access for SAS drives</p> <p>One- 16GB DDR4-2133 DIMM1</p>

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
<p>C695</p> <p>Intel Xeon Gold 6126 (Skylake) processor</p> <p>ESA AsyncOS software version 15.5</p>		<p>1RU: 1.7 x 16.89 x 29.8 in. (4.32x 43.0 x 75.6 cm)</p>	<p>Two 770W</p> <p>Redundant power supply</p>	<p>Six 1-GB Base-T Ethernet LAN ports, can be used as management ports</p> <p>RAID mirroring</p> <p>10/100/1000 Mbps</p> <p>Eight 600-GB hard disk drives (2.5" 10K SAS) hot swappable access for SAS drives</p> <p>Two- 16GB DDR4-2666 DIMM1</p>
<p>C695F</p> <p>Intel Xeon Gold 6126 processor (Skylake)</p> <p>ESA AsyncOS software version 15.5</p>		<p>1RU: 1.7 x 16.89 x 29.8 in. (4.32x 43.0 x 75.6 cm)</p>	<p>Two 770W</p> <p>Redundant power supply</p>	<p>Six 1-GB Base-T Ethernet LAN ports, can be used as management ports</p> <p>RAID mirroring</p> <p>10/100/1000 Mbps</p> <p>Eight 600-GB hard disk drives (2.5" 10K SAS) hot swappable access for SAS drives</p> <p>Two- 16GB DDR4-2666 DIMM1</p>
<p>C100v, C300v and C600v—installed on UCS-C220-M5</p>		<p>Height</p> <p>1.7 in. (4.32 cm)</p>	<p>Up to two of the following hot-swappable power supplies:</p>	<p>Rear panel</p>

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
<p>Intel® Xeon® Gold 6248R Series processors (Skylake),</p> <p>with VMware ESXi 7.0 Hypervisor, with a single Guest Virtual Machine</p> <p>ESA AsyncOS software version 15.5</p>		<p>1RU:</p> <p>Width</p> <p>16.89 in. (43.0 cm)</p> <p>including handles:</p> <p>18.98 in. (48.2 cm)</p> <p>Depth</p> <p>29.8 in. (75.6 cm)</p> <p>including handles:</p> <p>30.98 in. (78.7 cm)</p>	<p>770 W (AC)</p> <p>1050 W (AC)</p> <p>1050 W (DC)</p> <p>1600 W (AC)</p> <p>1050ELV (AC)</p>	<ul style="list-style-type: none"> • One 1-GbaseT 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> <p>Cisco Virtual Interface Cards</p> <p>Quad Port Intel i350 1GbE RJ45 Network Interface Card (NIC)</p>
<p>C100v, C300v and C600v–installed on UCS-C240-M5</p>		<p>Height</p> <p>3.43 in. (8.70 cm)</p>	<p>Up to two of the following hot-swappable power supplies:</p>	<p>Rear panel</p> <ul style="list-style-type: none"> • One 1-Gbps RJ-45 management port (Marvell 88E6176)

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
<p>Intel® Xeon® Gold 6248R Series processors (Skylake), with VMware ESXi 7.0 Hypervisor, with a single Guest Virtual Machine</p> <p>ESA AsyncOS software version 15.5</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>1050 W (AC) power supply 1050 W V2 (DC) power supply 1600 W (AC) power supply</p>	<ul style="list-style-type: none"> • 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> <p>Cisco Virtual Interface Cards</p> <p>Quad Port Intel i350 1GbE RJ45 mLOM Network Interface Card (NIC)</p>
<p>C100v, C300v and C600v—installed on UCS-C480-M5</p> <p>Intel® Xeon® Gold 6248R Series processors (Skylake), with VMware ESXi 7.0 Hypervisor,</p>		<p>Height 6.9 in. (176 mm)</p> <p>Width 19.0 in. (483 mm)</p> <p>Length (including front handles and power supplies)</p>	<p>Power supplies are hot-swappable and rear-accessible. They default to redundant as 2+2 (or 1+1 for servers with only two power supplies)</p>	<p>Front Panel</p> <p>Drive bay module 1 (drive bays 1 – 8)</p> <ul style="list-style-type: none"> • Bays 3, 4, 5, 6 support SAS/SATA drives only • Bays 1, 2, 7, 8 support SAS/SATA or NVMe drives <p>Drive bay module 2 (drive bays 9 – 16)</p> <ul style="list-style-type: none"> • Bays 11, 12, 13, 14 support SAS/SATA drives only

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
<p>with a single Guest Virtual Machine</p> <p>ESA AsyncOS software version 15.5</p>		<p>32.7 in. (830 mm)</p>		<ul style="list-style-type: none"> • Bays 9, 10, 15, 16 support SAS/SATA or NVMe drives <p>Drive bay module 3 supports either</p> <ul style="list-style-type: none"> • Optional DVD drive module, or • Bays 19, 20, 21, 22 support SAS/SATA drives only • Bays 18, 18, 23, 24 support SAS/SATA or NVMe drives <p>KVM console connector (used with a KVM cable that provides two USBs, one VGA, and one serial connector)1</p> <p>CPU module bay 1, the system must have at least one CPU module in bay 1 to boot. It must also have either a CPU module or a blank filler module in bay 2.</p> <p>CPU module bay 2, If no CPU module is present in bay 2, there must be a blank filler module in bay 2 for the system to boot</p> <p>Rear Panel</p> <p>Serial Port (DB-9 connector)</p> <p>VGA Video Port (DB-15 connector)</p> <p>10 Gb Ethernet ports</p> <p>10/100/1000 Ethernet dedicated management port</p> <p>USB 3.0 ports (three)</p> <p>Power supplies 1-4</p> <p>PCIe slots 1-12</p>

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
<p>C100v, C300v and C600v—installed on UCS-220-M6</p> <p>Intel® Xeon Gold 6342 Series processors (Ice Lake), with VMware ESXi 7.0 Hypervisor, with a single Guest Virtual Machine</p> <p>ESA AsyncOS software version 15.5</p>		<p>2RU:</p> <p>Height 3.42 in. (8.7 cm)</p> <p>Width 16.9 in. (42.9 cm) including slam latches: 18.9 in. (48.0 cm)</p> <p>Depth 30 in. (76.2 cm)</p>	<p>Up to two of the following hot-swappable power supplies:</p> <p>1050 W (AC) 1050 W (DC) 1600 W (AC) 2300 W (AC)</p>	<p>Rear panel</p> <ul style="list-style-type: none"> • One 1-GbaseT RJ-45 management port • 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 DB-15 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 card:</p> <p>☑Cisco Virtual Interface Cards</p>
<p>C100v, C300v and C600v—installed on UCS-C240-M6</p> <p>Intel® Xeon Platinum 8360Y Series</p>		<p>2RU:</p> <p>Height 3.42 in. (8.7 cm)</p> <p>Width 16.9 in. (42.9 cm)</p>	<p>Up to two of the following hot-swappable power supplies:</p> <p>1050 W (AC) 1050 W (DC) 1600 W (AC)</p>	<p>Rear panel</p> <ul style="list-style-type: none"> • One 1-GB management port • One 1-GB and one 10-GB auto-negotiating Ethernet ports • One RS-232 serial port (RJ45 connector)

Hardware/ Processor/ Software	Picture	Size	Power	Interfaces
<p>processors (Ice Lake), with VMware ESXi 7.0 Hypervisor, with a single Guest Virtual Machine</p> <p>ESA AsyncOS software version 15.5</p>		<p>including slam latches: 18.9 in. (48.0 cm)</p> <p>Depth 30 in. (76.2 cm)</p>	2300 W (AC)	<ul style="list-style-type: none"> • 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 DB-15 video connector, and one serial port (DB-9) RJ45 connector) <p>Modular LAN on Motherboard (mLOM) slot</p> <p>The dedicated mLOM slot on the motherboard can flexibly accommodate the following card:</p> <p>☐ Cisco Virtual Interface Cards</p>

To order the TOE hardware and delivery via commercial carriers, visit Cisco.com Support for the specific model. For an example of the ordering details, see <https://www.cisco.com/c/en/us/support/security/email-security-appliance/series.html>.

The software is the ESA AsyncOS software version 15.5. For ordering and downloading the TOE software, contact Cisco support.

The primary TOE guidance documentation that is also considered to be part of the TOE is the Cisco Email Security Appliance (ESA) Common Criteria Configuration Guide document. This document (Cisco Email Security Appliance running AsyncOS 15.5 Common Criteria Operational User Guidance And Preparative Procedures v1.0) is downloadable from the <http://cisco.com> web site at: <https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html>

In Table 1 Common Criteria Certified Product Guidance, enter the certified product name or simply click on the certification date for the product. A PDF version of the document will be displayed, which can be downloaded and saved.

Additional guidance documentation includes the following:

[User Guide for AsyncOS 15.5.2 for Cisco Secure Email Gateway - MD \(Maintenance Deployment\), first published August 19, 2024](#)

[CLI Reference Guide for AsyncOS 15.5.2 for Cisco Secure Email Gateway - MD \(Maintenance Deployment\), first published August 19, 2024](#)

[Cisco Secure Email Virtual Gateway and Secure Email and Web Manager Virtual Appliance Installation Guide, published April 30, 2024](#)

[Cisco Email Security Appliance C195, C395, C695, and C695F Hardware Installation Guide, last modified January 23, 2023](#)

[Best Practice Guide for Anti-Spam, Anti-Virus, Graymail and Outbreak Filters, updated January 9, 2020](#)

1.6 Logical Scope of the TOE

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

1. Security Audit
2. Cryptographic Support
3. Identification and Authentication
4. Security Management
5. Protection of the TSF
6. TOE Access
7. Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the NDcPP v2.2e as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The Cisco Email Security Appliance provides extensive auditing capabilities. The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE

records the date and time of each event, the type of event, the subject identity, and the outcome of the event.

Auditable events include:

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

The TOE is configured to transmit its audit messages to an SCP server on a remote syslog server. Communication with the syslog server is protected using SCP over SSHv2, and the TOE can determine when communication with the syslog server fails. If the connection fails, the session will need to be reestablished following the configuration settings described in the Cisco Email Security Appliance (ESA) Common Criteria Configuration Guide document.

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

1.6.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates, based on ESA on the platforms and processors as noted above in Table 5 Hardware Models and Specifications.

The TOE provides cryptography in support of other Cisco ESA security functionality. The ESA software calls the Cisco FIPS Object Module (FOM) v7.3a 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 and Table 7 for algorithm certificate references.

Table 6 Processors and FOM

CPU Family	CPU Model (Microarchitecture)	FOM Version	Physical Appliances/Platform	CAVP Certificate
Intel Xeon Scalable	Intel Xeon Silver 4110 (Skylake)	CiscoSSL FOM 7.3a	C195	A4446
Intel Xeon Scalable	Intel Xeon Silver 4116 (Skylake)	CiscoSSL FOM 7.3a	C395	A4446
Intel Xeon Scalable	Intel Xeon Gold 6126 (Skylake)	CiscoSSL FOM 7.3a	C695, C695F	A4446
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Skylake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C220-M5	A4595
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Skylake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C240-M5	A4595
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Skylake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C480-M5	A4595
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Icelake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C220-M6	A4595
ESXi 7.0 on Intel®	VMware ESXi 7.0 on Intel® Xeon® Scalable (Icelake)	CiscoSSL FOM 7.3a	C100v, C300v and C600v– installed on UCS-C240-M6	A4595

Table 7 FIPS References

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
AES	Used for symmetric encryption/decryption	CBC (128, 256) CTR (128, 256) GCM (128, 256)	A4446 A4595	CiscoSSL FOM 7.3a	FCS_COP.1/DataEncryption

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
SHS (SHA-1, SHA-256, SHA-384 and SHA-512)	Cryptographic hashing services	Byte Oriented	A4446 A4595	CiscoSSL FOM 7.3a	FCS_COP.1//Hash
HMAC SHA-1 HMAC SHA-256	Keyed hashing services and software integrity test	Byte Oriented	A4446 A4595	CiscoSSL FOM 7.3a	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with NIST SP 800-90A	CTR_DRBG (AES 256)	A4446 A4595	CiscoSSL FOM 7.3a	FCS_RBG_EXT.1
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation, PKCS#1 v.1.5, 2048 bit key,	A4446 A4595	CiscoSSL FOM 7.3a	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/SigGen
ECDSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	A4446 A4595	CiscoSSL FOM 7.3a	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/SigGen
DSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	A4446 A4595	CiscoSSL FOM 7.3a	FCS_CKM.1
CVL – KAS-ECC	Key Agreement	NIST Special Publication 800-56A	A4446 A4595	CiscoSSL FOM 7.3a	FCS_CKM.2
CVL KAS-FFC	Key Agreement	NIST Special Publication 800-56A	A4446 A4595	CiscoSSL FOM 7.3a	FCS_CKM.2

The TOE provides cryptography in support of remote administrative management via SSHv2 for the CLI and HTTPS/TLS for the GUI. SCP over SSHv2 is used to secure the transmission of audit

records to the SCP server on the remote syslog server. In addition, the TOE uses the X.509v3 certificate for securing the TLS connections.

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

1.6.3 Identification and authentication

The TOE provides authentication services for administrative users connecting to the TOE's secure CLI and GUI administrative interfaces, using SSHv2 and HTTPS/TLS, respectively, to secure the connections. Prior to an administrator logging in, a login banner is presented at both the CLI and GUI interfaces. The TOE requires Authorized Administrators to be successfully identified and authenticated prior to being granted access to the TOE and any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as character complexity rules.

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

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

1.6.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure HTTPS/TLS (GUI interface), SSHv2 (CLI interface) session or via a direct 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 configure the session inactivity time before session termination or locking
- ability to update the TOE, and to verify the updates using published hash prior to installing those updates
- ability to configure the authentication failure parameters
- ability to configure the cryptographic functionality
- ability to re-enable an administrator account
- ability to configure the audit behavior
- ability to set the time

The CLI is the main interface used to administer the TOE, since all functionality to configure, securely manage and to monitor the TOE is available via the CLI. The GUI can also be used, but not all functionality to configure the TOE is available in the GUI. Therefore, in the evaluated configuration it is recommended to use the CLI to perform all configuration and setting of the security functions and to securely manage the TOE.

The TOE supports the security administrator role and is referred to as the Authorized Administrator. 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.

1.6.5 Protection of the TSF

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

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

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

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

1.6.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time period. Once a session has been terminated, the TOE requires the user to be successfully re-identified and re-authenticated to establish a new session. Sessions can also be terminated if an Authorized Administrator enters the "exit" command.

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

1.6.7 Trusted path/Channels

The TOE allows trusted path to be established to itself from remote administrators over SSHv2 for the CLI and HTTPS/TLS for the GUI. The TOE also uses SCP over SSHv2 to push the audit logs to a SCP server on a remote syslog server.

1.7 Excluded Functionality

The following functionality is excluded from the evaluation.

Table 8 Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS mode of operation	This mode of operation includes non-FIPS allowed operations.
AsyncOS API	Does not include any claimed or in-scope functionality
SMTP Server	Not included in the evaluation

The TOE is evaluated in FIPS mode. FIPS mode is enabled using configuration settings as described in the Cisco Email Security Appliance (ESA) Common Criteria Configuration Guide document. The exclusion of non-FIPS mode does not affect the compliance to the collaborative Protection Profile for Network Devices Version 2.2e. In addition, any general product functionality that is discussed in the product overview but not discussed as part of the logical boundary is not covered by the evaluation.

2 CONFORMANCE CLAIMS

2.1 Common Criteria Conformance Claim

The TOE and ST are compliant with the Common Criteria (CC) Version 3.1, Revision 5, dated: April 2017. For a listing of Assurance Requirements claimed, see section 5.4.

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

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 9 Protection Profiles below. The following NIAP Technical Decisions (TD) (as listed in Table 10 NIAP Technical Decisions (TD)) have 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 9: Protection Profiles

Protection Profile	Version	Date
Network Device Collaborative Protection Profile (NDcPP)	2.2e	23 March 2020

Table 10: NIAP Technical Decisions (TD)

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD800	Updated NIT Technical Decision for IPsec IKE/SA Lifetimes Tolerance	CPP_ND_V2.2E	FCS_IPSEC_EXT.1.7, FCS_IPSEC_EXT.1.8, CPP_ND_V2.2-SD	2023.11.13	No – referenced SFRs not being claimed
TD792	NIT Technical Decision: FIA_PMG_EXT.1 - TSS EA not in line with SFR	CPP_ND_V2.2E	FIA_PMG_EXT.1, CPP_ND_V2.2-SD	2023.09.27	Yes – TD has been applied
TD790	NIT Technical Decision: Clarification Required for testing IPv6	CPP_ND_V2.2E	FCS_DTLSC_EXT.1.2, FCS_TLSC_EXT1.2, CPP_ND_V2.2-SD	2023.09.27	No – referenced SFRs not being claimed
TD0738	NIT Technical Decision for Link to Allowed-With List	CPP_ND_V2.2E	Chapter 2	2023.05.19	Yes – TD has been applied

TD0670	NIT Technical Decision for Mutual and Non-Mutual Auth TLSC Testing	CPP_ND_V2.2E	ND SD2.2, FCS_TLSC_EXT.2.1	2022.09.16	No - Referenced SFR is not being claimed
TD0639	NIT Technical Decision for Clarification for NTP MAC Keys	CPP_ND_V2.2E	FCS_NTP_EXT.1.2FA U_GEN.1, FCS_CKM.4, FPT_SKP_EXT.1	2022.08.26	No – FCS_NTP_EXT.1 is not being claimed
TD0638	NIT Technical Decision for Key Pair Generation for Authentication	CPP_ND_V2.2E	FCS_CKM.1	2022.08.05	Yes – TD has been applied.
TD0636	NIT Technical Decision for Clarification of Public Key User Authentication for SSH	CPP_ND_V2.2E	ND SD2.2, FCS_SSHC_EXT.1	2022.03.21	Yes – TD has been applied.
TD0635	NIT Technical Decision for TLS Server and Key Agreement Parameters	CPP_ND_V2.2E	FCS_TLSS_EXT.1.3, NDSD v2.2	2022.03.21	Yes – TD has been applied.
TD0632	NIT Technical Decision for Consistency with Time Data for vNDs	CPP_ND_V2.2E	ND SD2.2, FPT_STM_EXT.1.2	2022.03.21	Yes – TD has been applied.
TD0631	NIT Technical Decision for Clarification of public key authentication for SSH Server	CPP_ND_V2.2E	ND SDv2.2, FCS_SSHS_EXT.1, FMT_SMF.1	2022.03.21	Yes – TD has been applied.
TD0592	NIT Technical Decision for Local Storage of Audit Records	CPP_ND_V2.2E	FAU_STG	2021.05.21	Yes - TD has been applied
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	CPP_ND_V2.2E	A.LIMITED_FUNCTIONALITY, ACRONYMS	2021.05.21	No – virtual TOE meets the criteria for Case 1 (described in 2.2e section 1.2) and thus the TD doesn't apply
TD0581	NIT Technical Decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3	CPP_ND_V2.2E	FCS_CKM.2	2021.04.09	Yes - TD has been applied

TD0580	NIT Technical Decision for clarification about use of DH14 in NDcPPv2.2e	CPP_ND_V2.2E	FCS_CKM.1.1, FCS_CKM.2.1	2021.04.09	Yes - TD has been applied
TD0572	NiT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	CPP_ND_V2.1, CPP_ND_V2.2E	FTP_ITC.1	2021.01.29	Yes – TD has been applied.
TD0571	NiT Technical Decision for Guidance on how to handle FIA_AFL.1	CPP_ND_V2.1, CPP_ND_V2.2E	FIA_UAU.1, FIA_PMG_EXT.1	2021.01.29	Yes – TD has been applied.
TD0570	NiT Technical Decision for Clarification about FIA_AFL.1	CPP_ND_V2.1, CPP_ND_V2.2E	FIA_AFL.1	2021.01.29	Yes – TD has been applied.
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	CPP_ND_V2.2E	ND SD v2.2, FCS_DTLSS_EXT.1.7, FCS_TLSS_EXT.1.4	2021.01.28	Yes – TD has been applied
TD0564	NiT Technical Decision for Vulnerability Analysis Search Criteria	CPP_ND_V2.2E	NDSDv2.2, AVA_VAN.1	2021.01.28	Yes - TD has been applied
TD0563	NiT Technical Decision for Clarification of audit date information	CPP_ND_V2.2E	NDcPPv2.2e, FAU_GEN.1.2	2021.01.28	Yes - TD has been applied
TD0556	NIT Technical Decision for RFC 5077 question	CPP_ND_V2.2E	NDSDv2.2, FCS_TLSS_EXT.1.4, Test 3	2020.11.06	Yes - TD has been applied
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	CPP_ND_V2.2E	NDSDv2.2, FCS_TLSS_EXT.1.4, Test 3	2020.11.06	Yes - TD has been applied
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	CPP_ND_V2.1, CPP_ND_V2.2E	ND SDv2.1, ND SDv2.2, AVA_VAN.1	2020.10.15	Yes – TD has been applied.
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	CPP_ND_V2.2E	FCS_DTLSC_EXT.1.1	2020.10.15	No - Referenced SFR is not being claimed

TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	CPP_ND_V2.2E	FIA_X509_EXT.2.2	2020.07.13	Yes - TD has been applied
TD0536	NIT Technical Decision for Update Verification Inconsistency	CPP_ND_V2.1, CPP_ND_V2.2E	AGD_OPE.1, ND SDv2.1, ND SDv2.2	2020.07.13	Yes - TD has been applied
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	CPP_ND_V2.1, CPP_ND_V2.2E	FCS_NTP_EXT.1.4, ND SD v2.1, ND SD v2.2	2020.07.13	No, referenced SFR (FCS_NTP_EXT.1) is not being claimed
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	CPP_ND_V2.2E	FIA_X509_EXT.1/REV, FIA_X509_EXT.1/ITT	2020-07-01 2020-12-01	Yes – TD has been applied

2.2.1 Protection Profile Additions

The ST claims exact conformance to the collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e. The ST does not include any additions to the functionality described in the NDcPPv2.2e.

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

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

- collaborative Protection Profile for Network Devices, Version 2.2e

2.3.2 TOE Security Problem Definition Consistency

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

The Security Objectives included in the Security Target represent the Security Objectives specified in the NDcPP v2.2e, 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 v2.2e, 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 v2.2e.

3 SECURITY PROBLEM DEFINITION

This section identifies the following:

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

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

3.1 Assumptions

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

Table 11: TOE Assumptions

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

Assumption	Assumption Definition
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).
A.TRUSTED_ADMINISTRATOR	<p>The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).</p>
A.REGULAR_UPDATES	The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.VS_TRUSTED_ADMINISTRATOR	The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.

Assumption	Assumption Definition
A.VS_REGULAR_UPDATES	The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.VS_ISOLATION	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

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 12: 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.

Threat	Threat Definition
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target Network Devices that do not use standardized secure 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.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the Network Device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

Threat	Threat Definition
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.3 Organizational Security Policies

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

Table 13: Organizational Security Policies

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

4 SECURITY OBJECTIVES

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

4.1 Security Objectives for the TOE

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

4.2 Security Objectives for the Environment

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

Table 14: Security Objectives for the Environment

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

Environment Security Objective	IT Environment Security Objective Definition
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.
O.E.VM_CONFIGURATION (applies to vNDs only)	<p>For vNDs, the Security Administrator ensures that the VS and VMs are configured to</p> <ul style="list-style-type: none"> • reduce the attack surface of VMs as much as possible while supporting ND functionality (e.g., remove unnecessary virtual hardware, turn off unused inter-VM communications mechanisms), and • correctly implement ND functionality (e.g., ensure virtual networking is properly configured to support network traffic, management channels, and audit reporting). <p>The VS should be operated in a manner that reduces the likelihood that vND operations are adversely affected by virtualization features such as cloning, save/restore, suspend/resume, and live migration.</p> <p>If possible, the VS should be configured to make use of features that leverage the VS's privileged position to provide additional security functionality. Such features could include malware detection through VM introspection, measured VM boot, or VM snapshot for forensic analysis.</p>

5 SECURITY REQUIREMENTS

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

5.1 Conventions

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

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

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

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

5.2 TOE Security Functional Requirements

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

Table 15: Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	Protected Audit Event Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_HTTPS_EXT.1	HTTPS
	FCS_RBG_EXT.1	Cryptographic Operation (Random Bit Generation)
	FCS_SSHC_EXT.1	SSH Client Protocol
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSS_EXT.1	TLS Server Protocol
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	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation

Class Name	Component Identification	Component Name
	FIA_X509_EXT.2	X.509 Certificate Authentication
	FIA_X509_EXT.3	X.509 Certificate Requests
FMT: Security management	FMT_MOF.1/Functions	Management of security functions behaviour
	FMT_MOF.1/ManualUpdate	Management of security functions behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_APW_EXT.1	Protection of Administrator Passwords
	FPT_SKP_EXT.1	Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TST_EXT.1	TSF Testing
	FPT_TUD_EXT.1	Trusted Update
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1/Admin	Trusted Path

5.2.1 Security audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

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

- a) Start-up and shut-down of the audit functions;
- b) All auditable events for the not specified level of audit; and
- c) *All administrative actions comprising:*
 - *Administrative login and logout (name of user account shall be logged if individual user accounts are required for administrators).*
 - *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*
 - *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*
 - *Resetting passwords (name of related user account shall be logged).*
 - *[no other actions]*
- d) *Specifically defined auditable events listed in Table 16.*

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

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

Table 16: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	As indicated in FAU_GEN.1.1
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.

Requirement	Auditable Events	Additional Audit Record Contents
FCS_HTTPS_EXT.1	Failure to establish an HTTPS session.	Reason for failure.
FCS_RBG_EXT.1	None.	None.
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_TLSS_EXT.1	Failure to establish a 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.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	<ul style="list-style-type: none"> • Unsuccessful attempt to validate a certificate • Any addition, replacement or removal of trust anchors in the TOE's trust store 	<ul style="list-style-type: none"> • Reason for failure of certificate validation • Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/Functions	None.	None.
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None	None.
FMT_MTD.1/CryptoKeys	None	None
FMT_SMF.1	All management activities of TSF data.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_STM_EXT.1	Discontinuous changes to time – either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success and failure)	None.
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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. In addition

[

- The TOE shall consist of a single standalone component that stores audit data locally,

]

FAU_STG_EXT.1.3 The TSF shall [overwrite previous audit records according to the following rule: [the newest record will overwrite the oldest record]] when the local storage space for audit data is full.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation

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

[

- RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;
- ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4;
- FFC Schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B1

]

5.2.2.2 FCS_CKM.2 Cryptographic Key Establishment

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

[

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1;
- Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";
- Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.";

]

5.2.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

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

]

that meets the following: *No Standard.*

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

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

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

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

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

- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 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
 - For ECDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [P-256,]; ISO/IEC 14888-3, Section 6.4
-].

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

FCS_COP.1.1/Hash The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm [SHA-1, SHA-256, SHA-384, SHA-512] and **message digest sizes** [160, 256, 384, 512] bits that meet the following: *ISO/IEC 10118-3:2004*.

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

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

5.2.2.8 FCS_HTTPS_EXT.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.

5.2.2.9 FCS_RBG_EXT.1 Random Bit Generation

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

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [1 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.

5.2.2.10 FCS_SSHC_EXT.1 SSH Client Protocol

FCS_SSHC_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254 [4256, 4344, 5647, 5656, 6187, 6668, 8268, 8308 Section 3.1, and 8332].

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

FCS_SSHC_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [256K] 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: [aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr, aes128-gcm@openssh.com].

FCS_SSHC_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [rsa-sha2-256] 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-sha1, hmac-sha256] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHC_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1, ecdh-sha2-nistp256] and [ecdh-sha2-nistp384, ecdh-sha2-nistp521] 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 each encryption key is used to protect no more than one gigabyte of data. After any of the thresholds are reached, a rekey needs to be performed.

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.

5.2.2.11 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol in accordance with: RFCs 4251, 4252, 4253, 4254 [4256, 4344, 5647, 5656, 6187, 6668, 8268, 8308 Section 3.1, and 8332].

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

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [256K] bytes in an SSH transport connection are dropped.

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

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses [rsa-sha2-256, ecdsa-sha2-nistp256] as its public key algorithm(s) and rejects all other public key algorithms.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1, ecdh-sha2-nistp256] and [ecdh-sha2-nistp384, ecdh-sha2-nistp521] are the only allowed key exchange methods used for the SSH protocol.

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

5.2.2.12 FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1 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 256 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 128 CBC SHA as defined in RFC 4492
- TLS ECDHE RSA WITH AES 128 CBC SHA256 as defined in RFC 4492
- TLS ECDHE RSA WITH AES 256 CBC SHA384 as defined in RFC 4492
- TLS ECDHE RSA WITH AES 128 GCM SHA256 as defined in RFC 5289
- TLS ECDHE RSA WITH AES 256 GCM SHA384 as defined in RFC 5289
- TLS DHE RSA WITH AES 128 CBC SHA as defined in RFC 3268
- TLS DHE RSA WITH AES 256 CBC SHA as defined in RFC 3268
- TLS DHE RSA WITH AES 128 CBC SHA256 as defined in RFC 5246
- TLS DHE RSA WITH AES 256 CBC SHA256 as defined in RFC 5246
- TLS DHE RSA WITH AES 128 GCM SHA256 as defined in RFC 5288
- TLS DHE RSA WITH AES 256 GCM SHA384 as defined in RFC 5288

].

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and [none].

FCS_TLSS_EXT.1.3 The TSF shall perform key establishment for TLS using [RSA with key size [2048 bits], Diffie-Hellman parameters with size [2048 bits], ECDHE curves [secp256r1, secp384r1, secp521r1];

FCS_TLSS_EXT.1.4 The TSF shall support [session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2)].

5.2.3 Identification and authentication (FIA)

5.2.3.1 FIA_AFL.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 Administrator from successfully establishing a remote session using any authentication method that involves a password until [an Authorized Administrator unlocks the locked user account] is taken by a local Administrator].

5.2.3.2 FIA_PMG_EXT.1 Password Management

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

- a) Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [“!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, “)”, [no other characters]];
- b) Minimum password length shall be configurable to [15] and [128].

5.2.3.3 FIA_UIA_EXT.1 User Identification and Authentication

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

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

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

5.2.3.4 FIA_UAU_EXT.2 Password-based Authentication Mechanism

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

5.2.3.5 FIA_UAU.7 Protected Authentication Feedback

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

5.2.3.6 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certification path validation **supporting a minimum path length of three certificates**.
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
 - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
 - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
 - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
 - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

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

5.2.3.7 FIA_X509_EXT.2 X.509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [TLS, HTTPS], 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].

5.2.3.8 FIA_X509_EXT.3 X.509 Certificate Requests

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

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

5.2.4 Security management (FMT)

5.2.4.1 FMT_MOF.1/Functions

Management of Security Functions Behaviour

FMT_MOF.1.1/Functions The TSF shall restrict the ability to [determine the behaviour of] the functions [transmission of audit data to an external IT entity] to *Security Administrators*.

5.2.4.2 FMT_MOF.1/ManualUpdate

Management of Security Functions Behaviour

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

5.2.4.3 FMT_MTD.1/CoreData

Management of TSF Data

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

5.2.4.4 FMT_MTD.1/CryptoKeys

Management of TSF Data

FMT_MTD.1/CryptoKeys The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.

5.2.4.5 FMT_SMF.1 Specification of Management Functions

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

- *Ability to administer the TOE locally and remotely;*

- Ability to configure the access banner;
- Ability to configure the session inactivity time before session termination or locking;
- Ability to update the TOE, and to verify the updates using [hash comparison] prior to installing those updates;
- Ability to configure the authentication failure parameters for FIA_AFL.1;
- [
 - Ability to configure audit behaviour (e.g., changes to storage locations for audit; changes to behaviour when local audit storage space is full);
 - Ability to manage the cryptographic keys;
 - Ability to configure the cryptographic functionality;
 - Ability to re-enable an Administrator account;
 - Ability to set the time which is used for time-stamps;
 - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors;
 - Ability to import X.509v3 certificates to the TOE's trust store;
-].

5.2.4.6 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator.*

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

5.2.5 Protection of the TSF (FPT)

5.2.5.1 FPT_APW_EXT.1: Protection of Administrator Passwords

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

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

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

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

5.2.5.3 FPT_STM_EXT.1 Reliable time stamps

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

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

5.2.5.4 FPT_TST_EXT.1: TSF Testing

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

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

].

5.2.5.5 FPT_TUD_EXT.1 Trusted Update

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

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

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

5.2.6 TOE Access (FTA)

5.2.6.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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

- terminate the session]

after a Security Administrator-specified time period of inactivity.

5.2.6.2 FTA_SSL.3 TSF-initiated Termination

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

5.2.6.3 FTA_SSL.4 User-initiated Termination

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

5.2.6.4 FTA_TAB.1 Default TOE Access Banners

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

5.2.7 Trusted Path/Channels (FTP)

5.2.7.1 FTP_ITC.1 Inter-TSF Trusted Channel

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

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

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

- *external audit server using SSH*

].

5.2.7.2 FTP_TRP.1/Admin Trusted Path

FTP_TRP.1.1/Admin: The TSF shall **be capable of using [SSH, TLS, 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 NDcPPv2.2e

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

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDcPPv2.2e which are derived from Common Criteria Version 3.1, Revision 5, dated April 2017. The assurance requirements are summarized in the table below.

Table 17: Assurance Requirements

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

5.4.2 Security Assurance Requirements Rationale

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

5.5 Assurance Measures

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

Table 18: Assurance Measures

Component	How requirement will be met
Security Target (ASE) /	Section 2 of this ST includes the TOE and ST conformance claim to CC Version 3.1, Revision 5, dated: April 2017, CC Part 2 extended and CC Part 3 conformant and NDcPPv2.2e and the rationale of how TOE provides all of the functionality at a level of security commensurate with that identified in NDcPPv2.2e. Section 2 also includes the consistency rationale for the TOE Security Problem Definition and the Security Requirements to include the extended components definition.
ASE_CCL.1 /	
ASE_ECD.1 /	
ASE_INT.1 /	
ASE_OBJ.1 /	
ASE_REQ.1 /	
ASE_SPD.1 /	
ASE_TSS.1	

Component	How requirement will be met
ADV_FSP.1	<p>The functional specification describes the external interfaces of the TOE, such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements.</p> <p>The interfaces are described in terms of their:</p> <ul style="list-style-type: none"> • purpose (general goal of the interface); • method of use (how the interface is to be used); • parameters (explicit inputs to and outputs from an interface that control the behaviour of that interface); • parameter descriptions (tells what the parameter is in some meaningful way); 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>
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 ST.</p>
AGD_PRE.1	<p>The Installation Guide describes the installation, generation and startup procedures so that the users of the TOE can setup the components of the TOE in the evaluated configuration.</p>
ALC_CMC.1 ALC_CMS.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).</p> <p>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>
ATE_IND.1	<p>Cisco will provide the TOE for testing.</p>
AVA_VAN.1	<p>Cisco will provide the TOE for testing.</p>

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 19: How TOE SFRs Are Met

TOE SFRs	How the SFR is Met
FAU_GEN.1	<p>The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. Audit records are stored in files within the file system provided by the TOE. The TOE stores auditable events in separate log files containing related types of audited data. The following log files together comprise the TSF audit trail by covering all events listed in Table 16.</p> <p>The TOE ensures that each auditable event is associated with the user that triggered the event and thus is traceable to a specific user. For example, a human user, user identity, or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. Each audit record includes date and time of the audited event, type of event, subject identity, and the outcome (success or failure) of the event. The auditable events include:</p> <ul style="list-style-type: none"> • Start-up and shutdown of the audit function - recorded in System Logs. • Access to the TOE and System data - recorded in CLI Audit Logs (for console interfaces) and GUI logs; and Updater logs (TOE updates). • Reading of information from the audit records - recorded in CLI Audit Logs and HTTP logs for GUI. • Unsuccessful attempts to read information from the audit records - recorded in CLI Audit Logs and HTTP logs for GUI. • All modifications to the audit configuration that occur while the audit collection functions are operating - recorded in CLI Audit Logs and HTTP logs for GUI. • All modifications in the behavior of the functions of the TSF, that include all administrative actions, such as login/logout, generating/import of, changing, or deleting of cryptographic keys (including a reference of any associated keys), resetting of passwords- recorded in CLI Audit Logs and HTTP logs for GUI • All modifications to the values of TSF data, that include all administrative actions, such as login/logout, generating/import of, changing, or deleting of cryptographic keys (including a reference of any associated keys), resetting of passwords - recorded in CLI Audit Logs and HTTP logs for GUI.

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"> • Modifications to the group of users that are part of an Administrator role - recorded in CLI Audit Logs and HTTP logs for GUI. <p>Authorized Administrators can access all audit information. The Authorized Administrators can manually download the log files by clicking a link to the log directory on the Log Subscriptions page, then clicking the log file to access. Depending on the browser, an Authorized Administrator can view the file in a browser window, or open or save it as a text file. This method uses the HTTP(S) protocol and is the default retrieval method.</p>
FAU_GEN.2	<p>The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example, a human user, user identity, or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented.</p>
FAU_STG_EXT.1	<p>The TOE is configured to send the audit log records within each of the log files listed below to a specified, SCP server on a remote syslog server. The TOE protects communications with the remote syslog server via SCP over SSHv2. This must be configured by an Authorized Administrator. Once configured, the TOE can automatically send the audit records to the configured SCP server on a remote syslog server. The log files that must be configured to be sent to the external syslog server are:</p> <ul style="list-style-type: none"> • Audit Logs • Authentication Logs • CLI Audit Logs • GUI Logs • System Logs <p>Note that the TOE can also export various other log file's audit records to an external syslog server, but these other log files do not contain logs that satisfy the TOE's auditing requirements.</p> <p>The TOE provides the following mechanisms for sending the log files to a remote syslog server:</p> <ul style="list-style-type: none"> • SCP on Remote [syslog] Server - a remote syslog server that supports an SCP command can copy log files from the TOE to the remote syslog server. The user of the SCP command on the remote syslog server must be the

TOE SFRs	How the SFR is Met
	<p>Authorized Administrator on the TOE, as the TOE will prompt for the Authorized Administrator password before processing the SCP request.</p> <ul style="list-style-type: none"> • SCP Push - additionally, the TOE can be configured to periodically push log files to an SCP server on a remote syslog server. <p>The Authorized Administrator can configure the time interval for sending the log files to the remote syslog with a minimum time lapse of 60 seconds and maximum time of 12 days. The time setting is customized based on day, hour, minutes and seconds. There is also a configurable maximum log file size limit (100KB – 104MB configuration range) for sending logs. If the log file size crosses the limit before the configured time duration has expired, the logs will still get pushed.</p> <p>Both of the above SCP methods are secured by SCP over SSHv2. The SCP is the method that periodically pushes log files to an SCP server on a remote syslog server. This method requires an SSH SCP server on the remote syslog server using SSHv2 protocol. The subscription requires a username, SSH key, and destination directory on the remote syslog server. Log files are transferred based on a rollover schedule set by the Authorized Administrator. The TOE generates an email alert to the Authorized Administrator and begins overwriting the oldest stored audit records when the audit trail becomes full. (Note that the TOE does not stop collecting or producing System data.) The alert is generated to an Authorized Administrator who has been configured via the Command Line Interface (<i>alertconfig</i> command) to receive email alerts for this event. The TOE does not provide interfaces to modify individual records. When the audit trail becomes full, the TOE ensures that the most recent audit records will be maintained, limited only by the available storage space.</p> <p>The SCP push method periodically pushes log files to an SCP server on a remote syslog server. This method also requires an SSH SCP server on a remote syslog server using SCP over SSHv2 protocol to secure the connection. The subscription requires a username (recommend that it is Authorized Administrator on the TOE), SSH key and destination directory on the remote syslog server. Log files are transferred based on a rollover schedule set by the Authorized Administrator.</p> <p>The TOE is capable of detecting when the SSH connection fails. If the connection fails, the session will need to be reestablished following the configuration settings described in the Cisco Email Security Appliance (ESA) Common Criteria Configuration Guide document. The TOE also stores a local set of audit records on the TOE and continues to do so if the communication with the syslog server goes down. Once the connection is restored, the audit records will be sent to the remote syslog server as configured. For example, on the next SCP push based on either the maximum log file size being exceeded or on the time interval, the current log file and the log files previously unsuccessfully transferred will be transferred.</p>

TOE SFRs	How the SFR is Met
	<p>The TOE stores the audit logs locally as configured with the <i>logconfig</i> command in the CLI and the Log Subscriptions page in the GUI. The size of the local log files is set by an Authorized Administrator using the 'Rollover by File Size' configuration setting. Once the file reaches the specified size, they are sent to the remote syslog server using SCP over SSHv2. These transfers can also be configured based on configured time intervals.</p> <p>Only Authorized Administrators are able to clear the local logs, and there is no TOE interface that allows for administrators to modify the contents of the local audit records.</p> <p>The TOE's default installation configures the audit log files to maintain 10 files of no more than 10MB for each log subscription. The Authorized Administrator does not need to configure this setting however, this value is customizable. The Authorized Administrators can configure each log subscription to allow 1-1000 maximum log files, and each log file can be configurable to a maximum of between 100KB and 100MB. There is no limit to the number of log subscriptions that the Authorized Administrator can create.</p> <p>With a typical configuration, the log space should not grow beyond a reasonable limit. If through customization of the log limits, the log files grow too much, alerts will be sent to the Authorized Administrators when the log partition grows beyond 90% usage. If the space available for storing audit records is exhausted, the TOE will start to overwrite the oldest records in the audit trail and generate an email alert to this effect and send it to an Authorized Administrators.</p> <p>Refer to the Cisco Email Security Appliance Common Criteria Configuration Guide for full details and configuration settings.</p>
FCS_CKM.1	<p>The TOE implements Diffie-Hellman based key establishment schemes with cryptographic key sizes of 2048-bit or greater that meets FIPS 186-4, "Digital Signature Standard", Appendix B1. The TOE implements and uses the prime and generator specified in RFC 3526 Section 3 when generating parameters for the key exchange. In addition, ECC schemes are used with P-256, P-384 and P-521.</p>
FCS_CKM.2	<p>The TOE complies with FIPS 186-4 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 3447.</p> <p>The TOE can create an RSA public-private key pair of 2048 bit or greater that can be used to generate a Certificate Signing Request (CSR). Via offline CSR the TOE can send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its certificate (including X.509v3) from the CA.</p>

TOE SFRs	How the SFR is Met																			
	<p>The Integrity of the CSR and certificate during transit are assured through use of digital signatures (encrypting the hash of the TOE’s public key contained in the CSR and certificate).</p> <p>The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The TOE can also use X.509v3 certificates for authentication of TLS sessions. The TOE acts as both a sender and receiver for RSA-based key establishment schemes 800-56A and 800-56B.</p> <p>The key pair generation portions of "The RSA Validation System" for FIPS 186-4 were used as a guide in testing the FCS_CKM.1.</p> <p>TOE acts as both a sender and receiver for Diffie-Helman and RSA based key establishment schemes.</p> <table border="1" data-bbox="545 898 1336 1612"> <thead> <tr> <th>Scheme</th> <th>SFR</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>RSA</td> <td>FCS_TLSS_EXT.1 FCS_SSHC/S_EXT.1</td> <td rowspan="4">Remote Administration</td> </tr> <tr> <td>FFC</td> <td>FCS_TLSS_EXT.1 FCS_SSHC/S_EXT.1</td> </tr> <tr> <td>RSAES-PKCS1</td> <td>FCS_TLSS_EXT.1</td> </tr> <tr> <td>ECC</td> <td>FCS_SSHC/S_EXT.1</td> </tr> <tr> <td>RSA</td> <td>FCS_SSHC/S_EXT.1</td> <td rowspan="3">Remote Syslog Server</td> </tr> <tr> <td>FFC</td> <td>FCS_SSHC/S_EXT.1</td> </tr> <tr> <td>ECC</td> <td>FCS_SSHC/S_EXT.1</td> </tr> </tbody> </table> <p>For details on each protocol see the related SFR.</p>	Scheme	SFR	Service	RSA	FCS_TLSS_EXT.1 FCS_SSHC/S_EXT.1	Remote Administration	FFC	FCS_TLSS_EXT.1 FCS_SSHC/S_EXT.1	RSAES-PKCS1	FCS_TLSS_EXT.1	ECC	FCS_SSHC/S_EXT.1	RSA	FCS_SSHC/S_EXT.1	Remote Syslog Server	FFC	FCS_SSHC/S_EXT.1	ECC	FCS_SSHC/S_EXT.1
Scheme	SFR	Service																		
RSA	FCS_TLSS_EXT.1 FCS_SSHC/S_EXT.1	Remote Administration																		
FFC	FCS_TLSS_EXT.1 FCS_SSHC/S_EXT.1																			
RSAES-PKCS1	FCS_TLSS_EXT.1																			
ECC	FCS_SSHC/S_EXT.1																			
RSA	FCS_SSHC/S_EXT.1	Remote Syslog Server																		
FFC	FCS_SSHC/S_EXT.1																			
ECC	FCS_SSHC/S_EXT.1																			
FCS_CKM.4	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																			

TOE SFRs	How the SFR is Met
	<p>required for use. The TOE is configured in FIPS mode with the option chosen to encrypt all passwords and keys.</p> <p>The TOE zeroizes all the cryptographic keys used within the TOE after the key is no longer of use to the TOE. The cryptographic module performs the overwrite of the cryptographic keys and other critical security parameters that are handled by the CiscoSSL library (FOM) are zeroized using a function that will overwrite the memory once they are no longer in use.</p> <p>Swap space is encrypted using AES to avoid accidental leakage of CSPs. As part of the reload command, an option to wipe the data is provided. The wipe option along with the 'wipedata' command will overwrite the hard drive with zeros so that the keys are zeroized within the old core dump files.</p> <p>The information provided in Table 20 TOE Key Zeroization 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 all 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 and 256 bits) as described in ISO 18033-3, ISO 19772, and ISO 10116.</p> <p>Table 7 FIPS References for validation details.</p> <p>AES is implemented in the following protocols: TLSv1.1, TLSv1.2 and SSHv2.</p> <p>The TOE also provides AES encryption and decryption in support of SSHv2 and TLSv1.1/2 for secure communications.</p> <p>The configuration and management of the cryptographic algorithms is provided through the CLI, to include the auditing of configuring the options by the Authorized Administrator.</p> <p>The relevant FIPS certificate numbers are listed in Table 7 FIPS References.</p>
FCS_COP.1/SigGen	<p>The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 and greater and ECDSA with key size 256 bits as specified in FIPS PUB 186-4, "Digital Signature Standard". The relevant FIPS certificate numbers are listed in Table 7 FIPS References.</p>

TOE SFRs	How the SFR is Met
	<p>The TOE provides cryptographic signatures in support of SSHv2 and TLSv1.1/2 for secure communications. The TOE provides the RSA option in support of SSHv2 and TLSv1.1/2 key establishment. RSA 2048-bit is used in the establishment of both TLSv1.1/2 and SSHv2 key establishment. For SSHv2, RSA and ECDSA host keys are supported.</p> <p>Management of the cryptographic algorithms is provided through the CLI with auditing of those commands.</p> <p>The relevant FIPS certificate numbers are listed in Table 6 Algorithm Certificate References</p>
FCS_COP.1/Hash	<p>The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004. The TOE provides hashing as part of the TLS session integrity. In addition, SHA-384 hashing is used for verification of software image integrity.</p>
FCS_COP.1/KeyedHash	<p>The TOE uses server-side X.509v3 certificates for authentication. The digital signature consists of an encrypted hash function. Verification of the digital signature includes the process of decrypting the encrypted hash and verifying the hash is valid. SHA1 is also used in the keyed hash function of HMAC.</p> <p>The TOE provides Secure Hash Standard (SHS) hashing in support of TLS, for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands.</p> <p>The TOE provides keyed-hashing message authentication services using HMAC-SHA-1 (key size and message digest size 160 bits) and HMAC-SHA-256 (key size and message digest size 256 bits) as specified in ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". The block size for HMAC-SHA1 and HMA-SHA-256 is 512 bits.</p> <p>The TOE provides SHS hashing and HMAC message authentication in support of SSHv2, and TLSv1.1/2 for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands.</p> <p>SHS hashing and HMAC message authentication (SHA-1) is used in the establishment of HTTPS, TLS and SSHv2 sessions.</p> <p>Refer to the Cisco Email Security Appliance Common Criteria Configuration Guide for full details and configuration settings.</p>
FCS_HTTPS_EXT.1	<p>The TOE implements HTTPS over TLS as specified in RFC 2818 and FCS_TLSS_EXT.1.</p>

TOE SFRs	How the SFR is Met
	<p>The TSF HTTPS implementation authenticates the TOE to the remote client with an X.509 certificate. Authorized Administrators manage the TOE identity certificates using the Destination Controls page in the GUI or <i>Interfaceconfig</i> command in the TOE CLI. HTTPS then uses the Authorized Administrators selected identity certificate.</p> <p>The TSF HTTPS implementation performs server-based authentication using a server X.509v3 certificate to establish the TLS session. The TSF HTTPS implementation does not require client authentication at the TLS level but presents the Web interface logon page for Authorized Administrators to authenticate using their name and password.</p>
FCS_RBG_EXT.1	<p>The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in SP 800-90A, seeded by an entropy source that accumulates entropy from a TSF-software based noise source as described in FCS_RBG_EXT.1. This output is used directly to seed the DRBG.</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_EXT.1	<p>The TOE implements SSHv2 to secure the remote session between the TOE and syslog server. SSHv2 is implemented according to the following RFCs: 4251, 4252, 4253, 4254, 4256, <u>4344, 5647, 5656, 6187, 6668, 8268, 8308</u> Section 3.1, and 8332.</p> <p>The TOE supports public key-based authentication.</p> <p>The TOE uses an SCP push to securely send the audit logs to a remote syslog server over a secured SSHv2 session. The SSH client (the TOE) authenticates the identity of the SSH server (remote syslog server) using a local database associating each host name with its corresponding public key as described in RFC 4251 section 4.1.</p> <p>SSH connections will be dropped if the TOE receives a packet larger than 256KB (262,144 bytes). Large packets are detected by the SSH implementation and dropped internal to the SSH process. A rekey occurs after a threshold of no longer than one hour and no more than one gigabyte of transmitted data.</p> <p>The key exchange methods allowed by the TOE in the evaluated configuration are, diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp521. Any session where the SSH server offers only non-compliant algorithms or key sizes will be rejected by the SSH client. SSH sessions can only be established when compliant algorithms and key sizes can be negotiated. Noting the SSH client only negotiates ssh-rsa during hostkey negotiation.</p>

TOE SFRs	How the SFR is Met
	<p>The TOE implementation of SSHv2 supports the following:</p> <ul style="list-style-type: none"> • public key algorithms for authentication: rsa-sha2-256 • encryption algorithms, aes128-cbc, aes256-cbc, aes128-ctr,aes256-ctr, and aes128-gcm@openssh.com to ensure confidentiality of the session. • hashing algorithms HMAC-SHA1 and HMAC-SHA256 to ensure the integrity of the session.
FCS_SSHS_EXT.1	<p>The TOE implements SSHv2 for remote CLI sessions. SSHv2 is implemented according to the following RFCs: 4251, 4252, 4253, 4254, 4256, <u>4344, 5647, 5656, 6187, 6668, 8268, 8308 Section 3.1, and 8332.</u></p> <p>The TOE supports both public key-based and password-based authentication.</p> <p>When establishing a connection to the SSH server using a public key, the public key is compared to the public key stored in the authorized_keys file. If the keys match, the connection is established.</p> <p>The remote CLI SSHv2 sessions are limited to an Authorized Administrators configurable session timeout period and will be rekeyed after a threshold of no longer than one hour, and no more than one gigabyte of transmitted data.</p> <p>SSH connections will be dropped if the TOE receives a packet larger than 256KB (262,144 bytes). Large packets are detected by the SSH implementation and dropped internal to the SSH process.</p> <p>Any session where the SSH client offers only non-compliant algorithms or key sizes will be rejected by the SSH server. SSH sessions can only be established when compliant algorithms and key sizes can be negotiated.</p> <p>The TOE implementation of SSHv2 supports the following:</p> <ul style="list-style-type: none"> • public key algorithms for authentication: rsa-sha2-256 andecdsa-sha2-nistp256. • public key exchange: diffie-hellman-group14-sha1, ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp521 • public key-based and password-based authentication for administrative users accessing the TOE's CLI through SSHv2. • encryption algorithms, aes128-cbc, aes256-cbc, aes128-ctr,aes256-ctr, and aes128-gcm@openssh.com to ensure confidentiality of the session.

TOE SFRs	How the SFR is Met
	<ul style="list-style-type: none"><li data-bbox="591 266 1422 321">• hashing algorithms HMAC-SHA1 and HMAC-SHA2-256 are used to ensure the integrity of the session.
FCS_TLSS_EXT.1	<p data-bbox="542 363 1422 422">An Authorized Administrator can initiate inbound TLSv1.1 and TLSv1.2 connections using the web-based GUI for remote administration of the TOE.</p> <p data-bbox="542 443 1422 501">Following is the TLS handshake and exchange of parameters between the client and the TOE.</p>

TOE SFRs	How the SFR is Met	
	<pre> sequenceDiagram participant Client participant Server Note over Client: Client Hello Client->>Server: Note over Server: Server Hello 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>	
	<p>Using wildcards is not supported in identity certificates, such as when you import the certificate and private key into ESA. Certificate pinning is also not supported in the evaluated configuration.</p> <p>Since RSA is being used for key exchange and authentication there are no specific parameters associated with the server key exchange. Using the below TLS_RSA ciphers the RSA public key (with a minimum RSA key size 2048) is used for authentication and key exchange. Using the below TLS_DHE ciphers the standard</p>	

TOE SFRs	How the SFR is Met
	<p>diffie hellman parameters P, Q, and G are used for key exchange. Using the below TLS_ECDHE ciphers the ECDSA curves secp256r1, secp384r1, secp521r1 are used for key exchange.</p> <p>The supported ciphersuites include the following:</p> <ul style="list-style-type: none"> • <u>TLS_RSA_WITH_AES_128_CBC_SHA</u> as defined in RFC 3268 • <u>TLS_RSA_WITH_AES_256_CBC_SHA</u> as defined in RFC 3268 • <u>TLS_RSA_WITH_AES_128_CBC_SHA256</u> as defined in RFC 5246 • <u>TLS_RSA_WITH_AES_256_CBC_SHA256</u> as defined in RFC 5246 • <u>TLS_RSA_WITH_AES_128_GCM_SHA256</u> as defined in RFC 5288 • <u>TLS_RSA_WITH_AES_256_GCM_SHA384</u> as defined in RFC 5288 • <u>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA</u> as defined in RFC 4492 • <u>TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256</u> as defined in RFC 4492 • <u>TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384</u> as defined in RFC 4492 • <u>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</u> as defined in RFC 5289 • <u>TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384</u> as defined in RFC 5289 • <u>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</u> as defined in RFC 3268 • <u>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</u> as defined in RFC 3268 • <u>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256</u> as defined in RFC 5246 • <u>TLS_DHE_RSA_WITH_AES_256_CBC_SHA256</u> as defined in RFC 5246 • <u>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256</u> as defined in RFC 5288 • <u>TLS_DHE_RSA_WITH_AES_256_GCM_SHA384</u> as defined in RFC 5288 <p>Once configured, the TOE will not establish TLS v1.0, SSL2.0 or SSL3.0 connections if offered by the client and only the supported/configured TLS ciphersuites will be used to establish the session. In addition, the TOE will only establish a connection if the peer presents a valid X509 certificate during the handshake.</p> <p>The TOE supports TLS session resumption based on session IDs according to RFC 4346 (TLS1.1) or RFC 5246 (TLS1.2). TLS session resumption is enabled by default. The TOE supports session resumption as a single context. The session is resumed using the session ID. If the client hello has a valid session ID, then the session resumes using that session ID.</p>
FIA_AFL.1	The TOE provides the Authorized Administrators the ability to specify the maximum number of unsuccessful authentication attempts before Authorized

TOE SFRs	How the SFR is Met
	<p>Administrator is locked out through the administrative CLI and GUI interfaces. While the TOE supports a range from 1- 25 with a default of 5 attempts, in the evaluated configuration, the maximum number of failed attempts is required to be set to 3.</p> <p>When the Authorized Administrator attempting to log into the administrative CLI or GUI interface reaches the administratively set maximum number of failed authentication attempts, the user will not be granted access to the administrative functionality of the TOE until an Authorized Administrator resets the user's number of failed login attempts through the administrative CLI using the <i>userconfig</i> command or GUI Edit User webpage.</p> <p>The TOE includes the following administrative roles and access:</p> <ul style="list-style-type: none"> • “Administrators” have full access to all system configuration settings. This Authorized Administrator account does meet the lockout criteria at the local console and when remotely connected to the TOE via the GUI (secured with HTTPS/TLS) and therefore should be used for the daily management of the TOE. There is also a default admin account that is not subject to the lock out at the local console (this is to ensure administrators do not get totally locked out of the TOE). • “Operators” are restricted from creating new user accounts. • “Read-Only Operators” may only view settings and status information. • “Guests” may only view status information. • “Technicians” can only manage upgrades and feature keys. • “Help Desk Users” only have access to ISQ and Message Tracking. <p>Each individual account is required to have a unique name, and roles are applied to individual accounts. This ensures that the user name of the account responsible for taking an action is logged in the audit records and thus each such action can be tied to an individual user.</p>
FIA_PMG_EXT.1	<p>The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower-case letters, numbers, and special characters (that include: “!”, “@”, “#”, “\$”, “%”, “^”, “&”, “*”, “(”, and “”).</p> <p>By default, the password can be set from 0 to 128 characters, however in the evaluated configuration the password length must be configured to enforce a minimum of 15 characters. The number that is set, is the minimum number of characters that will be required, and the upper limit value can be a range of 15 characters or greater. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.</p>

TOE SFRs	How the SFR is Met
FIA_UIA_EXT.1 FIA_UAU_EXT.2	<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 banner that is displayed prior to user authentication.</p> <p>Administrative access to the TOE is facilitated through the TOE's CLI and GUI. The TOE mediates all administrative actions through the CLI and GUI. Once the administrative user attempts to access the CLI via either a directly connected console or remotely through SSHv2, the TOE prompts the user for a username and password. Likewise, when the administrative user attempts to access the web-based GUI of the TOE through HTTPS over TLSv1.1/2, the TOE prompts the user for a username and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until the Authorized Administrators is successfully identified and authenticated.</p> <p>The TOE provides a local password-based authentication mechanism for the CLI when accessed both locally and remotely as well as the GUI. When the CLI is accessed remotely, the session is secured via SSHv2 and authenticated using SSH public key. The password mechanism can be configured to require passwords to be a minimum of 15 characters from the printable character set. The TOE prevents administrative user actions from being performed prior to successful identification and authentication of the Authorized Administrators.</p> <p>Note, however, that users accessing the CLI via SSHv2 can be authenticated using public key cryptography. This requires the user's public key to be entered into the TOE (using the <i>sshconfig</i> command) and associated with the user's account. If there is no public key configured for the user, the user will instead be prompted to enter a password to authenticate.</p>
FIA_UAU.7	<p>When a user enters their password at the directly connected local console, the TOE will not echo any characters so that the user password is obscured.</p> <p>For remote session authentication via SSHv2 or TLSv1.1/2 secured connection, the TOE does not echo any characters as they are entered.</p>

FIA_X509_EXT.1/Rev	<p>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. The certificate validation checking takes place when the certificate is imported.</p> <p>The TOE supports the following methods to obtain a certificate from a CA:</p> <ul style="list-style-type: none"> • Manual cut-and-paste - ESA generates the Certificate Request Message as described in RFC 2986 which contains the public key and is displayed via the GUI or CLI interface. This allows the administrator to copy the certificate request and in a secure offline manner send the request to a Certification Authority to be transformed into an X.509v3 public-key certificate. • Both the certificate request message and 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. • 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. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate is reached. • The Authorized Administrator can also configure one or more certificate fields as listed below that will be used to compare the imported certificate to specific criteria such as: <ul style="list-style-type: none"> • alt-subject-name (If subject name doesn't match request, then the alternative subject name filed is used) • expires-on (If certificate is expired, rejects certificate) • issuer-name (Is there a trusted root certificate installed for the CA that signed the certificate). • name (Does the name in the request match the name in the certificate) • serial-number (Has the certificate been revoked. Serial number will be in the CRL) • subject-name (Does the name in the request match the name in the certificate) <p>The administrative user manually installs and selects the certificate used by the TOE for each certificate.</p>	
FIA_X509_EXT.2		
FIA_X509_EXT.3		

	<p>The physical security of the TOE (A.PHYSICAL_PROTECTION) protects ESA and the certificates from being tampered with or deleted. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE.</p> <p>The use of CRL is configurable and may be used for certificate revocation. CRL -- Certificate checking is performed by a CRL. This is the default option. the TOE performs revocation checking of the entire cert chain (CRL is configured for the certificate authority) at the time of import of the leaf and checks all CA certs (except the trust anchor) every time a leaf is imported.</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 local certificate that was imported must contain the basic constraints extension with the CA flag set to TRUE, the check also ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted.</p> <p>All the certificates include at least the following information: public key, Common Name, Organization, Organizational Unit and Country.</p> <p>If the connection to determine the certificate validity cannot be established, ESA will accept the certificate based on the last known state.</p>
<p>FMT_MOF.1/Functions FMT_MOF.1/ManualUpdate FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys</p>	<p>The TOE provides administrative users with a CLI and web-based GUI to interact with and manage the security functions of the TOE. The CLI is the main interface used to administer the TOE since all functionality to configure, securely manage and to monitor the TOE is available via the CLI. The GUI interface can also be used however not all functionality to configure the TOE is available in the GUI. In the evaluated configuration it is recommended to use the CLI to perform all configuration and setting of the security functions and to securely manage the TOE.</p> <p>No administrative functionality is available prior to the Authorized Administrators logging in and being identified and authenticated.</p> <p>Through the CLI, the TOE provides the ability for Authorized Administrators to manage TOE data, such as audit data, configuration settings, cryptographic keys, security attributes, uploading and enabling X509 certificates and login banners via the CLI and GUI.</p> <p>A subset of functionality is available in the GUI. For example, the TOE can initially be installed and set up using the GUI via the System Setup Wizard and saving the config file, selecting the SCP Push method for sending the log files to the remote syslog server and setting inactive timeout.</p>

	<p>The term “Authorized Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges can also modify TOE data if granted the privilege. See FMT_SMR.2 for more details on the TOE roles and related privileges.</p> <p>Manual software updates can only be done by the Authorized Administrator through either the CLI or GUI. These updates include software upgrades.</p> <p>The TOE also provides the ability for Authorized Administrators to manage the cryptographic keys that used to secure connections on the TOE. The Authorized Administrators access the CLI for management of the cryptographic functions. Following are the functions that can be performed for certain keys:</p> <ul style="list-style-type: none"> • X.509v3 certificates: import, modify, delete • SSH host keys: generate, modify, delete • SSH user keys: generate, delete
FMT_SMF.1	<p>The TOE provides all the capabilities necessary to securely manage the TOE. The Security Administrators (aka Authorized Administrators) user can connect to the TOE using the CLI to perform these functions via SSHv2 secured connection, via the GUI over HTTPS/TLS or at the local console. The CLI is the main interface used to administer the TOE since all functionality to configure, securely manage and to monitor the TOE is available via the CLI. The GUI interface can also be used however not all functionality to configure the TOE is available in the GUI. Therefore, in the evaluated configuration it is recommended to use the CLI to perform all configuration and setting of the security functions and to securely manage the TOE.</p> <p>The specific management capabilities available from the TOE include:</p> <ul style="list-style-type: none"> • Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI and GUI interfaces, as described above; • The ability to manage the warning banner message and content which allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g., administrative users); • The ability to manage the time limits of session inactivity which allows the Authorized Administrator the ability to set and modify the inactivity time threshold; • The ability to configure the number of failed administrator logon attempts that will cause the account to be locked until it is reset; • The ability to re-enable an administrator’s account that has been locked;

	<ul style="list-style-type: none"> • The ability to update the AsyncOS software. The validity of the image is provided using SHA-384 hash prior to installing the update; • The ability to manage audit behavior and the audit logs which allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs; • The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2 and TLSv1.1/2; • The ability to configure the SSHv2 functionality which supports the secure connections to the audit server; • The ability to import the X.509v3 certificates and validate for use in authentication and secure connections; • The ability to configure and set the time clock. <p>A subset of functionality is available in the GUI. For example, the TOE can initially be installed and set up using the GUI via the System Setup Wizard and saving the config file, selecting the SCP Push method for sending the log files to the remote syslog server and setting inactive timeout.</p>
FMT_SMR.2	<p>The TOE maintains Authorized Administrators that include privileged and semi-privileged administrator roles to administer the TOE locally and remotely.</p> <p>The terms “Authorized Administrator” and "Security Administrator" may be used interchangeably in this ST to refer to any user that has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. The assigned role determines the functions the user can perform; hence the Authorized Administrator with the appropriate privileges.</p> <p>The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the semi-privileged and privileged roles. The default user account for ESA is ‘admin’ and has all administrative privileges. The admin user account cannot be deleted, but an Authorized Administrator can change the password and lock the account, which is recommended. When an Authorized Administrator creates a new user account, they can assign the user to a predefined or a custom user role. Each role contains differing levels of permissions within the system. Although there is no limit to the number of user accounts that an Authorized Administrator can create on the appliance, Authorized Administrator cannot create user accounts with names that are reserved by the system such as “operator” or “root.”</p>

	<p>The following roles are predefined by the system and can be assigned to user accounts:</p> <ul style="list-style-type: none"> • Admin - default user account that has full access to all system configuration settings. • Administrator - has full access to all system configuration settings. • Technician - can perform system upgrades, reboot the appliance, and manage key features. • Operators - are restricted from creating, editing, or removing user accounts and cannot use the following commands: resetconfig, upgradecheck, upgradeinstall, systemsetup or running the System Setup Wizard. • Read-Only Operator - can view administrative interfaces, but do not have the ability to commit configuration changes or to access the file system or SCP, thus preventing them from accessing log files. • Guest - can only view system status information. <p>The term “Authorized Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions.</p> <p>The privilege level determines the functions the user can perform; hence the Authorized Administrator with the appropriate privileges.</p> <p>The TOE can and shall be configured to authenticate all access to the CLI and GUI using a username and password.</p> <p>The TOE supports both local administration via a directly connected console cable and remote administration via CLI using SSHv2 and via the GUI using HTTPS/TLS secure connection.</p>
<p>FPT_SKP_EXT.1 and FPT_APW_EXT.1</p>	<p>In the evaluated configuration, the TOE must run in FIPS mode. To be in FIPS mode, the Authorized Administrator enters the 'fipsconfig' command at the CLI.</p> <p>During the FIPS mode setup, an Authorized Administrator is able to select the option to have all passwords and keys encrypted using AES256-CBC. In addition, there is a sub-option using the 'saveconfig' command and the save config dialog in the GUI to encrypt the passwords and keys. In the evaluated configuration, these options must be selected and configured as described in the Cisco Email Server Appliance (ESA) Common Criteria Operational User Guidance And Preparative Procedures.</p>

	<p>The encrypted passwords and keys are stored in their respective configuration files and there are no administrative interfaces available to access the data.</p> <p>Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.</p>
FPT_STM_EXT.1	<p>The TOE provides a source of date and time information used in audit event timestamps.</p> <p>The clock function is reliant on the system clock provided by the underlying hardware in the physical TOE devices. The system clock on virtual TOE devices is independent of ESXi.</p> <p>This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. The time information is also used in setting the system time and administrative session timeout.</p> <p>The time can be configured using the CLI commands: <code>settime</code> and <code>settz</code>. In the GUI, the time can be configured under the Time Zone or Time Settings page from the System Administration menu.</p>
FPT_TUD_EXT.1	<p>An Authorized Administrator can query the currently executing software version via the CLI and GUI.</p> <p>An Authorized Administrator can either manually download the updates or ESA can automatically download the updates when "automated updates" has been configured. Note, in the evaluated configuration, automated updates will not be allowed.</p> <p>Updates can be downloaded directly from the Cisco Update Servers as well as from an offline update server. Both an Authorized Administrator and the TOE can check to see if an update is available from Cisco.</p> <p>Once the file is downloaded to a server, the TOE verifies that it was not tampered with prior to moving it to the TOE by using a SHA-384 utility to compute an SHA-384 hash for the downloaded file and comparing this with the SHA-384 hash for the image listed on the download page on Cisco.com.</p> <p>Once the Authorized Administrator has verified the TOE image, the file can be installed.</p>

	<p>Attempts to perform an illegitimate update onto the system will be logged into updater logs at INFO level. The sample log line will look as follows:</p> <p>Wed Dec 14 05:50:07 2022 Info: repeng SHA384 Mismatch</p> <p>If there is an issue with the verification of the SHA384 checksum, the software should not be installed, and the Authorized Administrator should contact Cisco TAC for assistance.</p> <p>For full details, refer to the Cisco Email Server Appliance (ESA) Common Criteria Operational User Guidance And Preparative Procedures for assistance.</p>
FPT_TST_EXT.1	<p>During the system bootup process (power on or reboot), all the Power on Startup Tests (POST) are performed for all the cryptographic modules. Also, during the initialization and self-tests, the module inhibits all access to the cryptographic algorithms.</p> <p>Additionally, the power-on self-tests are performed after the cryptographic systems are initialized but prior to the underlying OS initialization of external interfaces; this prevents the security appliances from passing any data before completing self-tests and entering FIPS mode. In the event of a power-on self-test failure of any component, the system crashes and appropriate information is displayed on the screen, and an alert is sent to an administrative email each time a self-test fails for any reason and a failed part of the functionality is disabled until a problem resolution has been accomplished. This operation ensures no cryptographic algorithms can be accessed unless all power on self-tests are successful.</p> <p>The tests include:</p> <ul style="list-style-type: none"> • AES Known Answer Test – • For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. • RSA Signature Known Answer Test (both signature/verification) – • This test takes a known plaintext value and Private/Public key pair and uses the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is

compared to the original plaintext value to ensure the decrypt operation is working properly.

- RNG/DRBG Known Answer Test –
- For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly.
- HMAC Known Answer Test –
- For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly.
- SHA-1/256/512 Known Answer Test –
- For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match, and the hash operations are operating correctly.

Prior to installing the image, the Authorized Administrator can verify the public hash to ensure the files have not been tampered with prior to installing. Using a SHA-384 utility, the Authorized Administrator can compute a SHA-384 hash for the downloaded file and compare the results with the SHA-384 hash on the Cisco.com download page.

The Software Integrity Test is run automatically whenever the AsyncOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity with the signature verification of the file image. The Software Integrity Test is also run automatically whenever the AsyncOS system is rebooted. It uses RSA-2048 and SHA2-256.

The FOM cryptographic module that is part of the TOE image, performs both power-up self-tests at Module initialization and continuous conditional tests during operation. Input, output, and cryptographic functions cannot be performed while the Module is in a self-test or error state as the Module is single threaded and will not return to the calling application until the power-up self-tests are complete. If the power-up self-tests fail subsequent calls to the Module will fail and thus no further cryptographic operations are possible.

Additionally, within the system, `/etc/rc.d/init.d/verify_fsic` calls `verify_file_integ.sh` which extracts, validates, and merges hash databases generated and signed at build time. For each file in the database a current hash is calculated and compared to the hash recorded in the database. If any of the cryptographic tests or comparison of the hash values fail, the TOE will enter an

	<p>error state or reboot in an attempt to correct the problem. If the issue is not resolved, the Authorized Administrator contacts Cisco TAC for assistance.</p> <p>If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen, and an alert is sent to an administrative email each time a self-test fails for any reason and a failed part of the functionality is disabled until a problem resolution has been accomplished.</p> <p>All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic.</p> <p>These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected because any deviation in the TSF behaviour will be identified by the failure of a self-test.</p>
FTA_SSL_EXT.1 and FTA_SSL.3	<p>The Authorized Administrators can configure maximum inactivity times individually for both the CLI and GUI. The Authorized Administrator can specify how long a user can be logged into the GUI before the user is logged out due to inactivity by default it is set to 30 minutes. Once AsyncOS logs a user out, the appliance redirects the user's web browser to the login page.</p> <p>Likewise, the Authorized Administrator can specify how long a user can be logged into the Email Security appliance's CLI before AsyncOS logs the user out due to inactivity.</p> <p>If a local user session is inactive for a configured period of time, the session will be terminated and will require be re-identification and re-authentication to re-establish a new session.</p> <p>If a remote user session is inactive for a configured period of time, the session will be terminated and will require re-identification and re-authentication to establish a new session.</p>
FTA_SSL.4	<p>An administrator is able to exit out of both the CLI and GUI administrative sessions. The Authorized Administrator can log out of the CLI with the 'exit' command. The Web UI also has a logout option via the drop-down menu.</p>
FTA_TAB.1	<p>The Authorized Administrator defines a custom login banner that will be displayed at the GUI and the CLI for both local and remote access configurations prior to allowing Authorized Administrator access through those interfaces.</p>

	<p>A local console includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the Authorized Administrator to support TOE administration. Whereas a remote console is one that includes any IT Environment Management workstation with one of the supported Web Browsers or any SSH client that supports SSHv2 may be used by the Authorized Administrator to support TOE administration through HTTPS/TLS or SSH protected channels.</p>
FTP_ITC.1	<p>The TOE protects communications with the syslog server using SCP over SSHv2. SSHv2 uses a keyed hash as defined in FCS_SSHC_EXT.1.6. This protects the data from modification by hashing the data and verifying the hash on receipt of the data. This ensures that the data has not been modified in transit. In addition, encryption of the data as defined in FCS_SSHC_EXT.1.4 is provided to ensure the data is not disclosed in transit.</p> <p>SCP Push is used for sending audit logs securely over SSHv2 to a syslog server. This method periodically pushes log files to a remote Syslog server. It requires an SSH server on the Syslog Server using the SSHv2 protocol. The subscription requires a username, SSH key, and destination directory on the remote computer. Log files are transferred based on a rollover schedule set by an Authorized Administrator.</p>
FTP_TRP.1/Admin	<p>All remote administrative communications take place over a secure encrypted SSHv2 for the CLI or TLS/HTTPS for the GUI sessions. The SSHv2 session is encrypted using AES encryption. The remote users are able to initiate SSHv2 communications with the TOE for secure CLI access. TLS/HTTPS is used to secure the communications with the TOE and remote web browser for secure GUI access.</p>

7 ANNEX A: KEY ZEROIZATION

7.1 Key Zeroization

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

Table 20: TOE Key Zeroization

Name	Description	Stored	Zeroization
Diffie-Hellman Shared Secret	The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0s.	This key is stored in DRAM.	Automatically after completion of DH exchange. Overwritten with: 0x00.
Diffie Hellman private exponent	This is the private exponent used as part of the Diffie-Hellman key exchange.	This key is stored in DRAM.	Zeroized upon completion of DH exchange. Overwritten with: 0x00.
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents).	This key is stored in NVRAM	Zeroized upon deletion of the SSH public/private key pair when no longer needed. Overwritten with: 0x00.
SSH Session Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents).	This key is stored in DRAM.	Automatically when the SSH session is terminated. Overwritten with: 0x00.
TLS server private key	This key is used for authentication, so the server can prove who it is. The private key is used for TLS secure connections.	This key is stored in NVRAM.	Zeroized by overwriting with 0x00.
TLS server public key	This key is used to encrypt the data that is used to compute the secret key. The public key is used for TLS secure connection.	This key is stored in NVRAM.	Zeroized by overwriting with new key.

Name	Description	Stored	Zeroization
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.	This key is stored in SDRAM.	Automatically after TLS session terminated. The value is 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.	This key is stored in SDRAM.	Automatically after TLS session terminated. The value is overwritten with 0x00.
TLS session integrity key	This key is used to provide the privacy and TLS data integrity protection.	This key is stored in SDRAM.	Automatically after TLS session terminated. The entire object is overwritten with zeros.
User Password	This is a variable 15+ character password that is used to authenticate local users.	The password is stored in NVRAM.	Zeroized by overwriting with new password.
AES Encryption Key	This is an AES-XTS 128-bit key used to encrypt passwords, authentication information, certificates, and shared keys.	This key is stored in SDRAM.	Zeroized by overwriting with 0x00.

8 ANNEX B: REFERENCES

The following documentation was used to prepare this ST:

Table 21: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1, Revision 5, dated: April 2017
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, Version 3.1, Revision 5, dated: April 2017
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, Version 3.1, Revision 5, dated: April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, Version 3.1, Revision 5, dated: April 2017
[NDcPP]	collaborative Protection Profile for Network Devices, Version 2.2e, 21 March 2020
[800-56Arev3]	NIST Special Publication 800-56Arev3, April 2018
[800-56Brev2]	NIST Special Publication 800-56Brev2 Recommendation for Pair-Wise, March 2019
[FIPS PUB 186-4]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) July 2013
[800-90Arev1]	NIST Special Publication 800-90Arev1 Recommendation for Random Number Generation Using Deterministic Random Bit Generators June 2015
[FIPS PUB 180-4]	FIPS PUB 180-4 Federal Information Processing Standards Publication Secure Hash Standard (SHS) August 2015

