Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11

Security Target

Version: 2.5

Date: March 10, 2026

Table of Contents

List of Tables

List of Figures

Acronyms and Abbreviations

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

Table 1: Acronyms and Abbreviations

Acronym / Abbreviation	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
DHCP	Dynamic Host Configuration Protocol
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
HTTPS	Hyper-Text Transport Protocol Secure
IT	Information Technology
NDcPP	collaborative Protection Profile for Network Devices
OS	Operating System
PoE	Power over Ethernet
PP	Protection Profile
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SSH	Secure Shell protocol

ST	Security Target
TCP	Transmission Control Protocol
TSC	TSF Scope of Control
TLS	Transport Layer Security
TSF	TOE Security Function
TSP	TOE Security Policy
WAN	Wide Area Network

Document Introduction

Prepared By:

Cisco Systems, Inc.

170 West Tasman Dr.

San Jose, CA 95134

This document, a Security Target (ST) developed in reference to the Common Criteria (ISO/IEC 15408) standards, provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11.

This 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.

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 D; Part 2; Part 3; and Part 5.

1.1 ST and TOE Reference

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

Table 2: ST and TOE Identification

Name	Description
ST Title	Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11 Security Target
ST Version	2.5
Publication Date	March 10, 2026
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco ASR 9000 Series Aggregation Services Routers running IOS-XR 7.11
TOE Hardware Models	ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912, ASR-9922

TOE Software Version	IOS-XR 7.11 asr9k-iosxr-infra-64-1.0.0.3-r7111.CSCwm88377.tar asr9k-iosxr-os-64-1.0.0.3-r7111.CSCwm88377.tar asr9k-sysadmin-7.11.1.CSCwm03455.tar asr9k-x64-7.11.1.CSCwm03455.tar
Keywords	Router, Network Appliance, Data Protection, Authentication, Cryptography, Secure Administration, Network Device.

1.2 TOE Overview

The Cisco Aggregation Services Router 9000 (herein after referred to as the ASR9K) is a purpose-built, routing platform. The TOE includes the hardware models as defined in Table 4.

1.3 TOE Product Type

The ASR9K is a scalable carrier-class router, which is designed for redundancy, high security and availability, packaging, power, and other requirements needed by service providers. The ASR9K is designed to provide continuous system operation, scalability, security, and high performance.

The ASR9K runs IOS-XR that is a microkernel-based network operating system. IOS-XR is able to process data as it comes into the router without buffering delays. The microkernel is responsible for specific functions such as memory management, interrupt handling, scheduling, task switching, synchronization, and inter-process communication. The microkernel's functions do not include other system services such as device drivers, file system, and network stacks; those services are implemented as independent processes outside the kernel, and they can be restarted like any other application.

1.4 Supported non-TOE Hardware/ Software/ Firmware

The TOE supports the following hardware, software, and firmware in its environment when the TOE is configured in its evaluated configuration:

Table 3 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 remote TOE administration through SSH protected channels. Any SSH client that supports SSHv2 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.
Audit (syslog) Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages. Also referred to as audit server in the ST.
Certificate Authority	Yes	This includes any Operational Environment Certificate Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrolment.

1.5 TOE Description

This section provides an overview of the ASR9K Target of Evaluation (TOE). This section also defines the TOE components included in the evaluated configuration of the TOE. The TOE is comprised of both software and hardware. The hardware is comprised of the following: ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR-9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912 and ASR-9922. The software is comprised of the Cisco IOS-XR 7.11.

The TOE consists of a number of components including:

- Chassis: The TOE chassis includes 2-RU, 6-RU, 10-RU, 14-RU, 21-RU, 30-RU and 44-RU form factors. The chassis is the component of the TOE in which all other TOE components are housed.

- Route Switch Processor (RSP): A route processor in each chassis provides the advanced routing capabilities of the TOE. They also monitor and manage the other components in the ASR9K.

1.6 TOE Evaluated Configuration

The TOE consists of one or more physical devices as specified in section 1.7 below and includes the Cisco IOS-XR software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco IOS-XR configuration determines how packets are handled to and from the TOE's network interfaces. The router configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

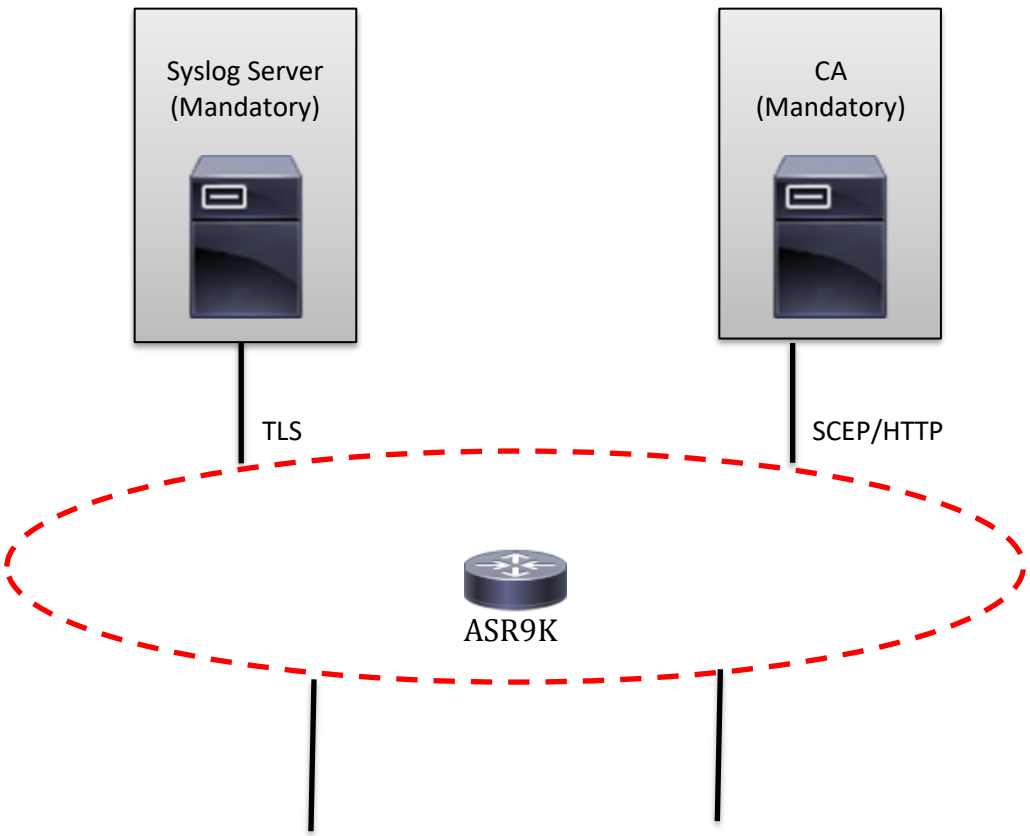
If the TOE is to be remotely administered, then the management workstation must be connected to an internal network and SSHv2 must be used to securely connect to the TOE. Servers must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.

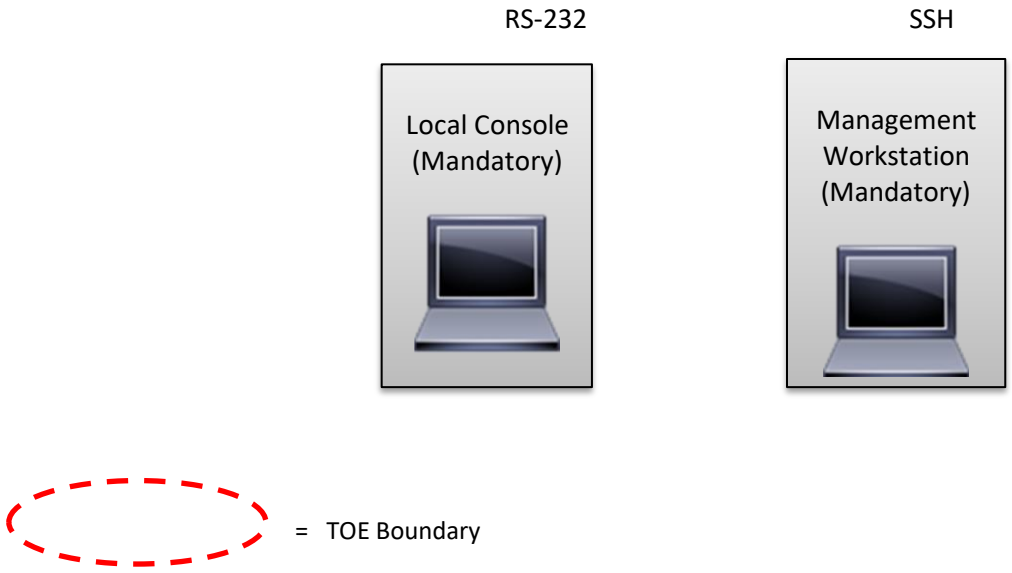
An external syslog server is required for the TOE to transmit audit records. The TOE authenticates syslog server with X.509v3 certificates and protects communication channels to the external syslog server using the TLS protocol. A CA server must be used to validate certificates. The TOE communicates to the CA server using the HTTP protocol for CRL fetching and the SCEP protocol for x509 certificate enrolment.

Secure remote administration is protected with SSH which is implemented with authentication failure handling.

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

Figure 1: Example TOE Deployment





The figure above includes the following:

- Example of TOE Models
- The following are considered to be in the IT Environment:
  - Management Workstation (over SSH)
  - Audit (Syslog) Server (over TLS)
  - Local Console
  - Certificate Authority (over HTTP/SCEP)

NOTE: *While the figure above includes several non-TOE IT environment devices, the TOE is only the ASR9K device. Only one TOE device is required for deployment in an evaluated configuration.*

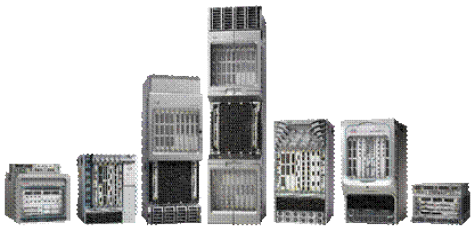
1.7 Physical Scope of the TOE

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

- Chassis: ASR-9006-SYS, ASR-9010-SYS, ASR-9902, ASR-9903, ASR-9904, ASR-9906, ASR-9910, ASR-9912, ASR-9922
- Route Processors: A99-RP3, A9K-RSP5, A99-RP3-X, A9K-RSP5-X, A99-RP-F
- Line Cards: A99-4HG-FLEX, A9K-4HG-FLEX, A9K-8HG-FLEX, A9K-20HG-FLEX, A99-10X400GE-X, A99-4T, A9903-8HG-PEC, A9903-20HG-PEC, A99-32X100GE-X, A99-32HG

The network, on which they reside, is considered part of the environment. The software is pre-installed and is comprised of the Cisco IOS-XR software image Release 7.11. In addition, the software image is also downloadable from the Cisco web site. A login id and password is required to download the software image. The TOE guidance documentation, *Cisco Aggregation Services Router 9000 (ASR9K) running IOS-XR 7.11 Common Criteria Operational User Guidance*, that is considered to be part of the TOE, is also available for download in PDF format. The TOE is comprised of the following physical specifications as described in Table 4 below:

Table 4: Hardware Models and Specifications

Hardware	Picture	Specifications
Modular Chassis		Physical dimensions (H x W x D in.) 9006: 17.50 x 17.38 x 29.05 - 10 RU 9010: 36.75 x 17.38 x 28.24 - 21 RU 9904: 10.38 x 17.57 x 25.02 - 6RU 9906: 24.39 x 17.60 x 31.45 - 14RU 9910: 36.69 x 17.60 x 30.41 - 21RU 9912: 52.5 x 17.60 x 29.25 - 30RU 9922: 77 x 17.60 x 30.1 - 44RU
Route Processors	A9K-RSP5  A99-RP3 	RSP5 CPU - Intel Xeon Silver 4109T (Skylake) 16, 24 or 40 GB DRAM 1 RS-232 console 2 GE management ports 1 auxiliary port 1 USB 2.0 port

	A9K-RSP5-X  A99-RP3-X 	RP3 CPU - Intel Xeon Silver 4109T (Skylake) 16, 24 or 40 GB DRAM 1 RS-232 console 2 GE management ports 1 auxiliary port 1 USB 2.0 port RSP5-X CPU - Intel Xeon D-1573N (Broadwell) 24 or 48 GB DRAM 1 RS-232 console 2 GE management ports 1 auxiliary port 1 USB 2.0 port RP3-X CPU - Intel Xeon D-1573N (Broadwell) 24 or 48 GB DRAM 1 RS-232 console 2 GE management ports 1 auxiliary port 1 USB 2.0 port
Line Cards	A9K-4HG-FLEX, A99-4HG-FLEX  A9K-8HG-FLEX 	A9K-4HG-FLEX, A99-4HG-FLEX MPU - Microchip META-DX1 PM6110 4x40/100GE QSFP ports 16x10/15GE SFP ports 24x10GE SFP+ ports A9K-8HG-FLEX Microchip META-DX1 PM6110

	A9K-20HG-FLEX  A99-10X400GE-X , A99-4T  A99-32X100GE-X, A99-32HG 	6x10/40/100GE QSFP ports 2x10/40/100/200/400GB QSFP ports A9K-20HG-FLEX Microchip META-DX1 PM6110 2x10/40/100GE QSFP ports 5x10/40/100/200/400GE QSFP ports A99-10X400GE-X , A99-4T Microchip META-DX1 PM6110 10x10/25/40/100/400GE QSFP ports A99-32X100GE-X, A99-32HG 32x100GE QSFP ports
Standalone Chassis	A99-RP-F  ASR-9902  ASR-9903 	A99-RP-F - 9902 / 9903 Route Processor CPU - Intel Xeon D-1533N (Broadwell) 32GB SDRAM 1 RS-232 console 2 GE management ports 1 auxiliary port 1 USB 2.0 port Dimensions (in.) 9902: 3.46 x 17.32 x 19 – 2RU 9903: 5.18 x 17.475 x 30 – 3RU 9902 Integrated Interfaces Microchip META-DX1 PM6108 2x10/40/100GE QSFP ports 6x10/40/100GE QSFP ports 16x25/10GE SFP, 24x10GE SFP+ ports 9903 Integrated Interfaces

	A9903-8HG-PEC  A9903-20HG-PEC 	Microchip META-DX1 PM6110 16x10/40/100GE QSFP ports 20x10GE SFP+ ports A9903-8HG-PEC Line card Microchip META-DX1 PM6110 32x25GE/10GE SFP+ ports 16x10GE SFP+ ports A9903-20HG-PEC Line card Microchip META-DX1 PM6108 5x20 400GE/200GE/100GE QSFP ports 15x100GE QSFP ports

Note: All Cisco HW devices are shipped via courier.

1.8 Logical Scope of the TOE

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

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

These features are described in more detail in the subsections below.

1.8.1 Security Audit

The TOE provides extensive auditing capabilities. The TOE can audit events related to cryptographic functionality, identification and authentication, and administrative actions. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations and manages audit data storage. The TOE provides the administrator with a circular audit trail.

The TOE is configured to transmit its audit messages to an external syslog as defined in RFC 5424 server over an encrypted channel using TLS as defined in RFC 5246.

1.8.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality.

The IOS-XR software calls the CiscoSSL FIPS Object Module (FOM) cryptographic implementation version 7.3a.

All the algorithms claimed in this ST have Cryptographic Algorithm Validation Program (CAVP) certificates (Operational Environment – Intel Xeon D-1533N (Broadwell), Intel Xeon D-1573N (Broadwell), Intel Xeon Silver 4109T (Skylake)). In addition, the TOE specifies hardware using the microchip META-DX1 PM6110, that is used to support MACsec. Conformance for this microchip is detailed in CAVP certificate #A1104.

See Table 5: CAVP References for a summary of the CAVP certificates and their applicability to the SFRs in this ST.

Notes:

- *The cryptographic module has been certified as conformant with FIPS 140-3 by the Cryptographic Module Validation Program (CMVP) with certificate number #4747. The Cryptographic Algorithm Validation Program (CAVP) Certificates supporting the CMVP certificate are listed at [CMVP #4747] See CAVP certificate #A4446.*

- *The Intel Xeon D-1533N is claimed as equivalent to the Intel Xeon D-1573N.*

Table 5: CAVP References

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

Algorithm	Description	Supported Mode	Module	CAVP Cert. #	SFR
		GCM (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/DataEncryption
		CMAC (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/CMAC
		AES Key Wrap (128 and 256)	FOM 7.3a	A4446	FCS_COP.1/MACSEC
		GCM (128 and 256)	MACsec	A1104	FCS_COP.1/MACSEC
SHS (SHA1, SHA-256, SHA-384, SHA-512)	Cryptographic hashing services	Byte Oriented	FOM 7.3a	A4446	FCS_COP.1/Hash
HMAC (SHA1, SHA-256, SHA-384, SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	FOM 7.3a	A4446	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	HMAC_DRBG	FOM 7.3a	A4446	FCS_RBG_EXT.1
RSA	Signature Verification and Key Transport	PKCS#1 v.1.5, 2048 and 3072 bit key	FOM 7.3a	A4446	FCS_COP.1/SigGen
	Key Generation	FIPS 186-4 Key Gen	FOM 7.3a	A4446	FCS_CKM.1
ECDSA	Key Generation	FIPS 186-4 Key Gen	FOM 7.3a	A4446	FCS_CKM.1
KAS-ECC	Key Agreement	NIST Special Publication 800-56A	FOM 7.3a	A4446	FCS_CKM.2

The TOE provides cryptography in support of remote administrative management via SSHv2 and secures the session between the ASR9K and remote syslog server using TLS.

The cryptographic services provided by the TOE are described in Table 6 below:

Table 6: TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in SSH session establishment. Used in TLS session establishment. X.509 certificate signing.
SHS	Used to provide SSH traffic integrity verification Used for keyed-hash message authentication
AES	Used to encrypt SSH session traffic. Used to encrypt TLS session traffic
HMAC	Used for keyed hash, integrity services in SSH session establishment.
TLS	Used to secure traffic to the syslog server.
ISO/IEC 18031:2011 HMAC_DRBG	Used for random number generation, key generation and seeds to asymmetric key generation Used in TLS session establishment Used in SSH session establishment

1.8.3 Identification and authentication

The TOE provides authentication services for administrative users wishing to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules.

After a configurable number of incorrect login attempts, ASR9K will lockout the account until a configured amount of time for lockout expires.

The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the serial console or SSH interfaces. The SSHv2 interface also supports authentication using SSH keys.

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

The TOE communicates to the CA server in regard to certificate enrolment using the SCEP protocol as defined in RFC 8894 and revocation (CRL fetching) using the HTTP protocol as defined in RFC 2616.

1.8.4 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure SSHv2 session or via a local console connection. The TOE provides the ability to securely manage all TOE administrative users, all identification and authentication, all audit functionality of the TOE, all TOE cryptographic functionality, the timestamps maintained by the TOE, and updates to the TOE. The TOE supports a privileged administrator role. Only the privileged administrator can perform the above security relevant management functions.

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

1.8.5 Protection of the TSF

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

The TOE internally maintains the date and time. This date and time is used as the timestamp that is applied to audit records generated by the TOE. Administrators can update the TOE's clock manually. Finally, the TOE performs testing to verify correct operation of the router itself and that of the cryptographic module.

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

1.8.6 TOE Access

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

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

1.8.7 Trusted path/Channels

The TOE establishes a trusted path between a remote administration workstation and the CLI of the TOE using SSHv2, and between the TOE and a remote syslog server using TLS.

1.9 Excluded Functionality

The following functionality is excluded from the evaluation:

Table 7: Excluded Functionality

Excluded Functionality	Exclusion Rationale
Non-FIPS 140-3 mode of operation	This mode of operation includes non-FIPS allowed operations. FIPS mode is enabled by the AGD.
MACsec	MACsec is not included in the evaluation. It must be used as specified in the AGD.
RADIUS	RADIUS is not included in the evaluation. It must be used as specified in the AGD.
TACACS+	TACACS+ is not included in the evaluation. It must remain disabled in the evaluated configuration will be disabled in the evaluated configuration.
LDAP	LDAP is not included in the evaluated configuration. LDAP (Not secure) must remain disabled in the evaluated configuration. Note that LDAP (secure) is allowed over TLS.
IPsec	IPsec was not included in the evaluated configuration. It must remain disabled in the evaluated configuration.

NTP	NTP was not included in the evaluation. It must be disabled in the evaluated configuration as specified in the AGD.

These services will be disabled by configuration settings. The exclusion of this functionality does not affect conformance with the NDcPPv3.0e or PKG_SSH_v1.0.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

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

CC Part #	Description
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance requirements, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.

2.2 Protection Profile Conformance

The TOE and ST are conformant with the Protection Profiles as listed in Table 10 below. The conformance type is Exact conformance.

Table 8 Protection Profiles

Protection Profile	Version	Date
collaborative Protection Profile for Network Devices	3.0e	6 December 2023

2.3 Package Conformance

The TOE and ST make the following claim for package conformance:
Functional Package for Secure Shell (SSH) V1.0 (PKG_SSH_V1.0) dated 13 May, 2021 Conformant.

Table 9 Functional Packages

Protection Profile	Version	Date
Functional Package for Secure Shell (SSH)	1.0	13 May 2021

2.4 Protection Profile Conformance Claim Rationale

2.4.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in CPP_ND_V3.0E and PKG_SSH_v1.0.

2.4.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organizational Security Policies included in the Security Target represent the Assumptions, Threats, and Organizational Security Policies specified in CPP_ND_V3.0E for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency.

The Security Objectives included in the Security Target represent the Security Objectives specified in CPP_ND_V3.0E for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.4.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in CPP_ND_V3.0E for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in CPP_ND_V3.0E.

3 Security Problem Definition

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational Security Policies imposed by an organization on the TOE to address the TOE's security needs.

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

3.1 Assumptions

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

Table 10: TOE Assumptions

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

A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data.
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. 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 KeyStore', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

3.2 Threats

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

Table 11: Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure 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.

Threat	Threat Definition
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
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 that must be imposed by an organization to address the security needs for the TOE.

Table 12: Organizational Security Policies

Policy Name	Policy Definition

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which Administrators 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.

This document identifies objectives of the TOE as O.OBJECTIVE with "OBJECTIVE" specifying a unique name. Objectives that apply to the IT environment are designated as OE.OBJECTIVE with "OBJECTIVE" specifying a unique name.

4.1 Security Objectives for the TOE

CPP_ND_V3.0E 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 non-IT security objectives stated in CPP_ND_V3.0E, which, in addition to the assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 13: Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_THRU_TRAFFIC_PROTECTION	The TOE does not provide any protection of traffic that traverses it. It is assumed that protection of this traffic will be covered by other security and assurance measures in the operational environment.
OE.TRUSTED_ADMIN	Security Administrators are trusted to follow and apply all guidance documentation in a trusted manner. The Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5 Security Requirements

This section identifies the Security Requirements for the TOE. The Security Requirements included in this section are derived from [CC2] and [CC3] and are as presented in CPP_ND_V3.0E and PKG_SSH_V1.0.

5.1 Conventions

The CC defines operations on Security Functional Requirements. This document uses the same conventions.

Convention	Indication
Assignment	Indicated with italicized text
Refinement	Indicated with bold text and strikethroughs
Selection	Indicated with underlined text
Assignment within a Selection	Indicated with italicized and underlined text
Iteration	Indicated by adding a string starting with "/" (e.g. 'FCS_COP.1/Hash')
Extended components	Extended components are indicated with "_EXT" and the end of the SFR component short name. E.g. "FIA_PMG_EXT.1"

5.2 Summary of TOE Security Functional Requirements

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

Table 14: Security Functional Requirements

Class	Requirement	Type
Security audit (FAU)	FAU_GEN.1 Audit Data Generation	Mandatory
	FAU_GEN.2 User identity association	Mandatory
	FAU_STG_EXT.1 Protected Audit Event Storage	Mandatory
	FCS_CKM.1 Cryptographic Key Generation	Mandatory

Class	Requirement	Type
Cryptographic Support (FCS)	FCS_CKM.2 Cryptographic Key Establishment	Mandatory
	FCS_CKM.4 Cryptographic Key Destruction	Mandatory
	FCS_COP.1/ DataEncryption Cryptographic Operation (AES Data Encryption/Decryption)	Mandatory
	FCS_COP.1/SigGen Cryptographic Operation (Signature Generation and Verification)	Mandatory
	FCS_COP.1/Hash Cryptographic Operation (Hash Algorithm)	Mandatory
	FCS_COP.1/KeyedHash Cryptographic Operation (Keyed Hash Algorithm)	Mandatory
	FCS_RBG_EXT.1 Random Bit Generation	Mandatory
	FCS_SSH_EXT.1 SSH Protocol	Selection
	FCS_SSHS_EXT.1 SSH Server Protocol	Selection
	FCS_TLSC_EXT.1 TLS Client Protocol	Selection
Identification and authentication (FIA)	FIA_AFL.1 Authentication Failure Handling	Selection
	FIA_PMG_EXT.1 Password management	Selection
	FIA_UIA_EXT.1 User Identification and Authentication	Mandatory
	FIA_UAU.7 Protected Authentication Feedback	Selection
	FIA_X509_EXT.1/Rev X.509 Certificate Validation	Selection
	FIA_X509_EXT.2 – X.509 Certificate Authentication	Selection
Security Management (FMT)	FMT_MOF.1/ManualUpdate Management of Security Functions Behaviour	Mandatory
	FMT_MTD.1/CoreData Management of TSF Data	Mandatory
	FMT_MTD.1/CryptoKeys Management of TSF Data	Selection
	FMT_SMF.1 Specification of Management Functions	Mandatory
	FMT_SMR.2 Restrictions on security roles	Mandatory

Class	Requirement	Type
Protection of the TSF (FPT)	FPT_APW_EXT.1 Protection of Administrator Passwords	Selection
	FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)	Mandatory
	FPT_STM_EXT.1 Reliable Time Stamps	Mandatory
	FPT_TST_EXT.1: TSF Testing	Mandatory
	FPT_TUD_EXT.1 Trusted Update	Mandatory
TOE Access (FTA)	FTA_SSL_EXT.1 TSF-initiated session locking	Selection
	FTA_SSL.3 TSF-initiated termination	Mandatory
	FTA_SSL.4 User-initiated termination	Mandatory
	FTA_TAB.1 Default TOE access banners	Mandatory
Trusted Path/Channels (FTP)	FTP_ITC.1 Inter-TSF trusted channel	Mandatory
	FTP_TRP.1/Admin Trusted Path	Mandatory

5.3 TOE Security Functional Requirements

5.3.1 Security audit (FAU)

5.3.1.1 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 shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrator actions comprising:

- Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).
- Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).

- Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).
- [Resetting passwords (name of related user account shall be logged)].

d) Specifically defined auditable events listed in Table 15.

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

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

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 15.

Table 15: Auditable Events

SFR	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	Configuration of local audit settings.	Identity of account making changes to the audit configuration.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_CKM_EXT.7	Success and failure of the activity	The object attribute(s), and object value(s) excluding any sensitive information.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.

FCS_COP.1/KeyedHash	None.	None.
FCS_RBG_EXT.1	None.	None.
FCS_SSH_EXT.1	Failure to establish SSH connection Establishment of SSH connection Termination of SSH connection Dropping of packets outside defined size limits	None.
FCS_SSHS_EXT.1	None.	None.
FCS_TLSC_EXT.1	Failure to establish an TLS session.	Reason for failure
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded	Origin of the attempt (e.g., IP address).
FIA_UIA_EXT.1	All use of identification and authentication mechanisms.	Origin of the attempt (e.g., IP address).
FIA_PMG_EXT.1	None.	None.
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate	Reason for failure
	Unsuccessful attempt to validate a certificate Any addition, replacement, or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates needed, replaced, or removed as trust anchor in the TOE's trust store
FIA_X509_EXT.2	None.	None.
FMT_MOF.1/ ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None.	None.
FMT_MTD.1/CryptoKeys	None.	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.

FPT_APW_EXT.1	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1 (if "terminate the session" is selected)	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the trusted path functions.	None.

5.3.1.2 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.

5.3.1.3 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 data locally].

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

FAU_STG_EXT.1.4 The TSF shall be able to store [non-persistent] audit records locally with a minimum storage size of [*1200 records*].

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

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

5.3.2 Cryptographic Support (FCS)

5.3.2.1 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.

]

5.3.2.2 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 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2";

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

5.3.2.3 FCS_CKM.4 Cryptographic Key Destruction

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

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

that meets the following: No Standard.

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

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

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

FCS_COP.1.1/SigGen The TSF shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [RSA Digital Signature Algorithm] and cryptographic key sizes [For RSA: modulus 2048 bits or greater],that meet the following: [For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3.]

5.3.2.6 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 [SHA1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits that meet the following: *ISO/IEC 10118-3:2004*.

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

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

5.3.2.8 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 [HMAC_DRBG [SHA-256]].

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

5.3.2.9 FCS_SSH_EXT.1 SSH Protocol

FCS_SSH_EXT.1.1 The TOE shall implement SSH acting as a [server] that complies with RFCs 4251, 4252, 4253, 4254,[4344, 5656, 6668, 8308 **section 3.1**, 8332,] and no other standard.

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

- "password" (RFC 4252),
- "publickey" (RFC 4252): [
    - rsa-sha2-512 (RFC 8332)
    - ecdsa-sha2-nistp384 (RFC 5656)
    - ecdsa-sha2-nistp521 (RFC 5656)

  ]

] and no other methods.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*1,262,144 bytes*] in an SSH transport connection are dropped.

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

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

] and no other mechanisms.

FCS_SSH_EXT.1.5 The TSF shall protect data in transit from modification, deletion, and insertion using [hmac-sha2-256, hmac-sha2-512, implicit,] and no other mechanisms.

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

- ecdh-sha2-nistp384 (RFC 5656)
- ecdh-sha2-nistp521 (RFC 5656)

] and no other mechanisms.

FCS_SSH_EXT.1.7 The TSF shall use an SSH KDF as defined in [RFC 5656, Section 4] to derive the following cryptographic keys from a shared secret: session keys.

FCS_SSH_EXT.1.8 The TSF shall ensure that [a rekey of the session keys] occurs when any of the following thresholds are met:

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

5.3.2.10 FCS_SSHS_EXT.1 SSH Protocol - Server

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

- *rsa-sha2-512 (RFC 8332)*
- *ecdsa-sha2-nistp384 (RFC 5656)*

- *ecdsa-sha2-nistp521 (RFC 5656)*

].

5.3.2.11 FCS_TLSC_EXT TLS Client Protocol

FCS_TLSC_EXT.1.1 The TSF shall implement [TLS 1.2 (RFC 5246)] supporting 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,*

] and no other ciphersuites.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches [the reference identifier per RFC 6125 section 6, and no other attribute types].

FCS_TLSC_EXT.1.3 The TSF shall not establish a trusted channel if the server certificate is invalid [without any administrator override mechanism].

FCS_TLSC_EXT.1.4 The TSF shall [not present the Supported Groups Extension] in the Client Hello.

FCS_TLSC_EXT.1.5 The TSF shall [present the signature_algorithms extension with support for the following algorithms*: [*

- rsa_pkcs1 with sha256(0x0401),
- rsa_pkcs1with sha384(0x0501),
- rsa_pkcs1 with sha512(0x0601),
- rsa_pss_rsae with sha256(0x0804),
- rsa_pss_rsae with sha384(0x0805),
- rsa_pss_rsae with sha512(0x0806),

] and no other algorithms;

].

FCS_TLSC_EXT.1.6 The TSF [does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.

FCS_TLSC_EXT.1.7 The TSF shall prohibit the use of the following extensions:

a) Early data extension

b) Post-handshake client authentication according to RFC 8446, Section 4.2.6.

FCS_TLSC_EXT.1.8 The TSF shall [not use PSKs].

FCS_TLSC_EXT.1.9 The TSF shall [support TLS 1.2 secure renegotiation through use of the "renegotiation_info" TLS extension in accordance with RFC 5746, reject [TLS 1.3] renegotiation attempts].

5.3.3 Identification and authentication (FIA)

5.3.3.1 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when an [Administrator configurable positive integer within [*1 to 24*]] 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 Administrator defined time period has elapsed].

5.3.3.2 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*:* ["!", "@", "#", "$", "%", "^", "&", "*", "(" , ")"];

b) Minimum password length shall be configurable to between [*8*] and [*253*] characters.

5.3.3.3 FIA_UIA_EXT.1 User Identification and Authentication

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

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

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

FIA_UIA_EXT.1.3 The TSF shall provide the following remote authentication mechanisms [SSH password, SSH public key] and local authentication mechanisms [password-based].

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

5.3.3.4 FIA_UAU.7 Protected Authentication Feedback

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

5.3.3.5 FIA_X509_EXT.1/Rev X.509 Certificate Validation

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

- RFC 5280 certificate validation and certificate path validation supporting a minimum path length of three certificates.
- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.
- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.
- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3].

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.

5.3.3.6 FIA_X509_EXT.2 – X.509 Certificate Authentication

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

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [not accept the certificate].

5.3.4 Security management (FMT)

5.3.4.1 FMT_MOF.1/ManualUpdate Management of Security Functions Behaviour

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

5.3.4.2 FMT_MTD.1/CoreData Management of TSF Data

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

5.3.4.3 FMT_MTD.1/CryptoKeys Management of TSF Data

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

5.3.4.4 FMT_SMF.1 Specification of Management Functions

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

- Ability to administer the TOE remotely;
- Ability to configure the access banner;
- Ability to configure the remote session inactivity time before session termination;
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates;

- *[*
    - Ability to configure 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 configure the cryptographic functionality*;*
    - Ability to configure thresholds for SSH rekeying*;*
    - Ability to set the time which is used for time-stamps;
    - Ability to configure the reference identifier for the peer;
    - Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors
    - Ability to manage the trusted public keys database.
    - Ability to administer the TOE locally;
    - Ability to configure the local session inactivity time before session termination or locking;

].

5.3.4.5 FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles: Security Administrator.

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

FMT_SMR.2.3 The TSF shall ensure that the conditions: The Security Administrator role shall be able to administer the TOE remotely are satisfied.

5.3.5 Protection of the TSF (FPT)

5.3.5.1 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.

5.3.5.2 FPT_SKP_EXT.1: Protection of TSF Data (for reading of all symmetric keys)

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

5.3.5.3 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].

5.3.5.4 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 verify the integrity of the TOE firmware and software; [at the conditions periodically during normal operation]] to demonstrate the correct operation of the TSF: [

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

].

And if failure detected [*the module transitions into an error state and outputs the error message via the module's status output interface. The module has one error state, called Hard error state. When a self-test fails, the module outputs "POST Failed" error. While the module is in the error state, all data through the data output interface and all cryptographic operations are disabled. The error state can only be cleared by reloading the module*.]

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

5.3.5.5 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 [digital signature] prior to installing those updates.

5.3.6 TOE Access (FTA)

5.3.6.1 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.

5.3.6.2 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.

5.3.6.3 FTA_SSL.4 User-initiated termination

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

5.3.6.4 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.

5.3.7 Trusted Path/Channels (FTP)

5.3.7.1 FTP_ITC.1 Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall be capable of using [TLS] 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**,** the authorized IT entities**]** to initiate communication via the trusted channel.

FTP_ ITC.1.3 The TSF shall initiate communication via the trusted channel for *[syslog over TLS*].

5.3.7.2 FTP_TRP.1/Admin Trusted Path

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

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

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

5.4 TOE SFR Dependencies Rationale for SFRs Found in PP

CPP_ND_V3.0E and PKG_SSH_V1.0 contain all the requirements claimed in this Security Target and demonstrate that the dependencies are satisfied.

6 Security Assurance Requirements

6.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the CPP_ND_V3.0E which is derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below:

Table 16: 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	Basic Functional Specification
Guidance documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative User guidance
Life cycle support (ALC)	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
	ALC_FLR.2	Flaw Remediation (Optional)
Tests (ATE)	ATE_IND.1	Independent testing - conformance
Vulnerability assessment (AVA)	AVA_VAN.1	Vulnerability analysis

6.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the CPP_ND_V3.0E and PKG_SSH_V1.0. As such, the SAR rationale is deemed acceptable since the cPP has been validated.

6.3 Assurance Measures

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

Table 17: Assurance Measures

Component	How requirement will be met
ASE_CCL.1 ASE_ECD.1 ASE_INT.1 ASE_OBJ.1 ASE_REQ.1 ASE_SPD.1 ASE_TSS.1	Section 2 of this ST includes the TOE and ST conformance claim to CC 2022, Revision 1, dated: November 2022, CC Part 2 extended ,CC Part 3 conformant and CC Part 5 conformant. Section 2 also includes the consistency rationale for the TOE Security Problem Definition and the Security Requirements to include the extended components definition. Section 1 of this ST provides the introduction of the ST, the TOE and its references, an overview of the TOE, the TOE product type, and the description of the TOE to include the evaluated configuration and the physical and logical cope of the TOE. Section 5 of this ST identifies the security functional requirements, the assurance requirements and how the assurance requirements are met. Section 6 provides the rat onale of how the Security Functional Requirements are met by the TOE.
ADV_FSP.1	There are no specific assurance activities associated with ADV_FSP.1. The requirements on the content of the functional specification information are implicitly assessed by virtue of the other assurance activities being performed. The functional specification is comprised of the information contained in the AGD_OPE and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation, and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.

Component	How requirement will be met
ALC_CMC.1	The AGD and ST implicitly meet this assurance requirement through the evaluation activities. During the evaluation, the evaluator checks the ST to ensure that it contains an identifier that specifically identifies the version that meets the requirements of the ST. Further, the evaluator checks the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST.
ALC_CMS.1	
ALC_FLR.2	Cisco provided the evaluators with the procedures for flaw remediation procedures addressed to TOE developers, accepting and acting upon all reports of security flaws and requests for corrections to those flaws, and flaw remediation guidance addressed to TOE users.
ATE_IND.1	Cisco provided the TOE for testing.
AVA_VAN.1	Cisco provided the TOE for testing.

7 TOE Summary Specification

7.1 TOE Security Functional Requirement Measures

This section identifies and describes how the Security Functional Requirements identified in section 5 are met by the TOE.

Table 18: How TOE SFRs are Met

TOE SFRs	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include: startup and shutdown of the audit mechanism, cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred such as generating keys, including the type of key and a key reference. Additionally, the startup and shutdown of the audit functionality is audited. The audit trail consists of the individual audit records; one audit record for each event that occurred. The audit record can contain up to 80 characters and a percent sign (%), which follows the time-stamp information. As noted above, the information includes at least all of the required information. Example audit events are included below: `RP/0/RP0/CPU0:Nov 14 2024 15:44:16.365 EST: exec[67642]: %SECURITY-LOGIN-6-AUTHEN_SUCCESS : Successfully authenticated user 'admin' from 'console' on 'con0_RP0_CPU0'` In the above log events a date and timestamp is displayed as well as an event description. The log buffer is circular, so newer messages overwrite older messages after the buffer is full. Administrators are instructed to monitor the log buffer using the show logging command to view the audit records. The first message displayed is the oldest message in the buffer. There are other associated commands to clear the buffer, to set the logging level, etc. The administrator can set the level of the audit records to be displayed on the console or sent to the syslog server. For instance, all emergency alerts, critical errors, and warning messages can be sent to the console alerting the administrator that some action needs to be taken as these types of messages mean that the

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>functionality of the TOE is affected. All notifications and information type message can be sent to the syslog server.</td></tr>
<tr><td>FAU_GEN.2</td><td>The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result, they are traceable to a specific user. For example, a human user, user identity or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. A sample audit record is below:

RP/0/RP0/CPU0:Dec 4 2024 14:32:34.459 EST: config[67725]:
%MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user
'admin'. Use 'show configuration commit changes
1000000104' to view the changes.
RP/0/RP0/CPU0:SPITFIRE(config)#show configuration commit
changes 1000000104
Building configuration...
!! IOS XR Configuration
logging buffered debugging
RP/0/RP0/CPU0:Nov 14 2024 15:49:25.467 EST: config[65679]:
%MGBL-SYS-5-CONFIG_I : Configured from console by admin</td></tr>
<tr><td>FAU_STG_EXT.1</td><td>The TOE is a standalone TOE configured to export syslog (as defined in RFC 5424) records to a specified, external syslog server in real-time. The TOE protects communications with an external syslog server via TLS (as defined in RFC 5246). If the connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents when connected to the syslog server.

For audit records stored internally to the TOE the audit records are stored in a circular log file where the TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator with the minimum value being 2097152 to 125000000 bytes of available disk space.

Only Authorized Administrators are able to clear the local logs, and local audit records are stored in a directory that does not allow administrators to modify the contents.</td></tr>
<tr><td>FCS_CKM.1

FCS_CKM.2</td><td>The following table describes the key generation algorithms the TOE implements to generate asymmetric keys:

<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/
NIST Curve</th><th>SFR</th><th>Service</th></tr>
</table>
</td></tr>
</table>

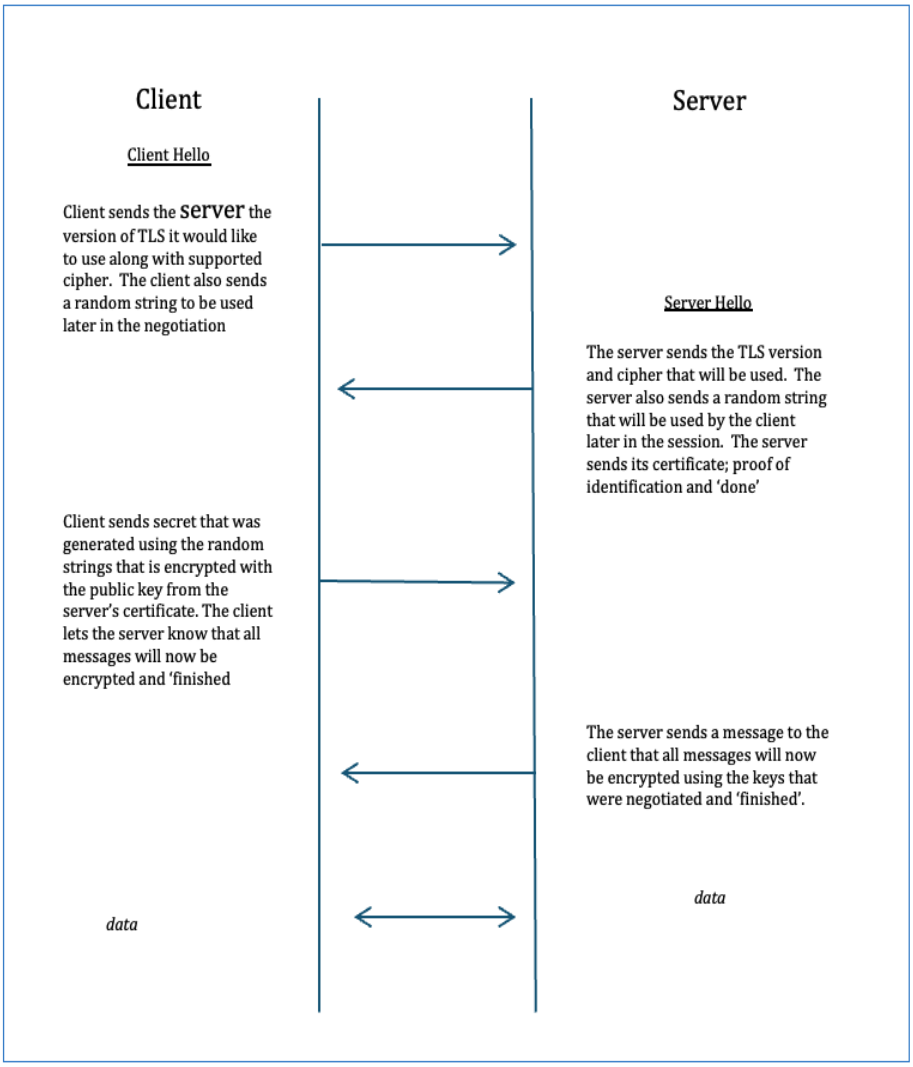
<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<table>
<tr><td>RSA</td><td>FIPS PUB 186-4</td><td>2048
3072</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
</table>
The following table shows the generation algorithms key the TOE implements to generate asymmetric keys used for key establishment:
<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/
NIST Curve</th><th>SFR</th><th>Service</th></tr>
<tr><td>ECC</td><td>FIPS PUB 186-4</td><td>P-256
P-384
P-521</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
</table>
The following table shows the methods the TOE implements for key establishment:
<table>
<tr><th>Scheme</th><th>Standard</th><th>SFR</th><th>Service</th></tr>
<tr><td>EC-DH</td><td>NIST SP 800-56A Revision 3</td><td>FCS_SSHS_EXT.1</td><td>SSH Remote Administration</td></tr>
<tr><td>RSA</td><td>RFC 3447</td><td>FCS_TLSC_EXT.1</td><td>Transmit generated audit data to an external IT entity</td></tr>
</table>
</td></tr>
<tr><td>FCS_CKM.4</td><td>The TOE meets all requirements specified in FIPS 140-3 for destruction of keys and Critical Security Parameters (CSPs) when no longer required for use.

See Table 19: TOE Key Zeroization in Section 7 Key Zeroization. The information provided in the table includes all of the all secrets, keys and associated values, the description, and the method used to zeroization when no longer required for use.

The information is provided in the reference section for ease and readability of all of the all secrets, keys and associated values, their description and zeroization methods.</td></tr>
<tr><td>FCS_COP.1/DataEncryption</td><td>The TOE provides symmetric encryption and decryption capabilities using AES in CBC mode and GCM mode (128 and 256 bits) as described in ISO/IEC 18033-3, ISO/IEC 10116, and ISO/IEC 19772. AES is implemented in the SSH and TLS protocols. Refer to Table 5 for the FIPS validated algorithm certificate numbers.</td></tr>
<tr><td>FCS_COP.1/SigGen</td><td>The TOE provides cryptographic signature services using RSA Digital Signature Algorithm with key size of 2048 or 3072 as specified in FIPS PUB 186-4.</td></tr>
</table>

TOE SFRs	How the SFR is Met
	The TOE provides cryptographic signatures in support of SSH, TLS and for trusted updates. Refer to Table 5 for the FIPS validated algorithm certificate numbers.
FCS_COP.1/Hash FCS_COP.1/KeyedHash	The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004 (with key sizes and message digest sizes of 160, 256, 384, and 512 bits respectively). The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256 that operates on 512-bit blocks and HMAC-SHA-512 operating on 1024-bit blocks of data, with key sizes and message digest sizes of 160 bits, 256 bits, and 512 bits respectively as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. SHA-512 hashing is used as part of digital signature verification of software image integrity. The TOE provides SHS hashing and HMAC message authentication in support of SSHv2 and TLSv1.2 for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands. SHS hashing and HMAC message authentication (SHA2) is used in the establishment of TLS and SSHv2 sessions. Refer to Table 5 for the FIPS validated algorithm certificate numbers.
FCS_RBG_EXT.1	The TOE implements an HMAC Deterministic Random Bit Generator (DRBG) as defined in section 10.1.2 of NIST SP 800-90A, using HMAC w/SHA-256 seeded by an entropy source that accumulates entropy from a TSF-platform based noise source. The deterministic RBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.
FCS_SSH_EXT.1 FCS_SSHS_EXT.1	The TSF implements SSHv2 conformant to RFCs 4251, 4252, 4253, 4254, 4256, 5647, 5656, 6668, 8308 section 3, and 8332 to provide a secure command line interface for remote administration. The TOE implementation of SSHv2 supports the following: TSF’s SSH transport implementation supports the following public-key algorithms for Hostkey authentication: rsa-sha2-512, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521. These ciphersuites are configured by default. Local password-based authentication for administrative users accessing the TOE through SSHv2. When the SSH client presents a public key, the TSF verifies it matches the one configured for the Administrator account. If the presented public key does not match the one configured for the Administrator account, access is denied.

TOE SFRs	How the SFR is Met
	The TSF's SSH transport implementation supports the following public-key algorithms for both Client Authentication and Hostkey authentication: rsa-sha2-256 and rsa-sha2-512. Remote CLI SSHv2 sessions are limited to an administrator configurable session timeout period. Encryption algorithms, aes128-cbc, aes256-cbc, aes128-gcm@openssh.com, and aes256-gcm@openssh.com to ensure confidentiality of the session. *Note: When aes*-gcm@openssh.com is negotiated as the encryption algorithm, the MAC algorithm field is ignored and GCM is implicitly used as the MAC.* The TOE's implementation of SSHv2 supports hashing algorithm hmac-sha2-256 and hmac-sha2-512 to ensure the integrity of the session. The TOE's implementation of SSHv2 can be configured to only allow ecdh-sha2-nistp384, and ecdh-sha2-nistp521 key exchange methods. Packets greater than 1,262,144 bytes in an SSH transport connection are dropped. Large packets are detected by the SSH implementation, and dropped internal to the SSH process. The Key Derivation Function (KDF) used in support of SSH, as defined in RFC 5656 Section 4, is used in order to derive session keys. The TOE can also be configured to ensure that SSH re-key of no longer than one hour and no more than one gigabyte of transmitted data for the session key. Rekeying is performed upon reaching the threshold that is hit first. Please refer to Table 5 for all the CAVP references.
FCS_TLSC_EXT.1	The TOE supports TLS v1.2 to protect the sessions to the remote audit server, and uses the following ciphersuites when configured in FIPS mode: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 The TOE does not support NIST Curves in the TLS Client Hello and does not support PSKs for authentication. The TOE will only establish a connection if the peer presents a valid certificate during the handshake. Where the TOE is the client, such as connecting to the remote syslog server, the handshake above is the same process except the server (remote syslog server) would not request the client certificate in the Server Hello, see the following:

TOE SFRs	How the SFR is Met
	 Any session where the server offers the following in the server hello: SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 will be rejected by the TOE (client). Certificate pinning is not supported. The TOE supports Subject Alternative Name (SAN) and Common Name (CN) "the reference identifiers" for a successful connection. SANs contain one or more alternate names and uses any variety of name forms for the entity that is bound by the Certificate Authority (CA) to the certified public key. Possible names include: DNS name. The signature_algorithms extension is supported by default and is not configurable, so the TOE will present the signature_algorithms extension in the Client Hello.

TOE SFRs	How the SFR is Met
FIA_AFL.1	The TOE provides the privileged administrator the ability to specify the maximum number of unsuccessful authentication attempts before privileged administrator or non-privileged administrator is locked out through the administrative CLI using a privileged CLI command. While the TOE supports a range from 1-24, in the evaluated configuration, the maximum number of failed attempts is recommended to be set to 3. Once the remote user is locked out, their account will not be accessible until the configured timer for lockout has been exceeded. Once the lockout time is over, then the administrator user can attempt to login again. At no point is administrator access completely unavailable when remote administrators are locked out due to unsuccessful password attempts. Local console access is always available. Administrator lockouts are not applicable to the local console.
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". Minimum password length is settable by the Authorized Administrator, and can be configured for minimum password lengths between 8 and 253 characters.
FIA_UIA_EXT.1 FIA_UAU_EXT.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login warning banner that is displayed prior to user authentication. Administrative access to the TOE is facilitated through the TOE's CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 secured connection, the TOE prompts the user for a username and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE provides a local password-based authentication mechanism for authentication of authorized administrators. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console or remotely via SSHv2 secured connection. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grants administrative access (if the combination of username and password is correct) or indicates that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.

TOE SFRs	How the SFR is Met
FIA_UAU.7	When a user enters their password at the local console, the TOE displays no characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered.
FIA_X509_EXT.1/Rev	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. Public key infrastructure (PKI) credentials are stored securely. The identification and authentication, and authorization security functions protect an unauthorized user from gaining access to the storage. The certificate validation checking takes place during the TLS session establishment and at time of import. The TOE conforms to standard RFC 5280 for certificate and path validation. CRLs can be checked for all certs in the chain except the trust anchor. And if any cert is revoked, then the TLS session is rejected. The TOE communicates to the CA for certificate enrolment using SCEP and for CRL fetching using HTTP. If a connection cannot be established to validate the certificate, then the TOE will not accept the certificate. The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set appropriately. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensures that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted. Only one certificate is imported since the only device is a syslog server, so the TOE chooses this certificate. basicConstraints checking is performed at the time of authentication during the connection attempt. If the connection to determine the certificate validity cannot be established, the certificate is not accepted. The administrators can configure a trust chain by importing the CA certificate(s) that signed and issued the server (syslog) certificate. This will tell the TOE which CA certificate(s) to use during the validation process. If the TOE does not find the trusted root CA, the TLS connection to the syslog server will fail. CRLs are used to determine revocation status, and are used during an authentication step. The CRL for the issuer is found in the CDP of the issued certificate. When the TOE is able to contact the CRL distribution point for certificate revocation checking, the TOE will reject the TLS session if the remote trust point's (e.g. syslog server's) certificate has been revoked. If the connection to determine the certificate validity cannot be established, the certificate is not accepted, and the connection will not be established.
FIA_X509_EXT.2	

TOE SFRs	How the SFR is Met
FMT_MOF.1/ManualUpdate	The TOE provides administrative users with a CLI to interact with and manage the security functions of the TOE. The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned. The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes, X509 certificates, login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles. Manual software updates can only be done by the authorized administrator through the CLI. The Security Administrators (Authorized Administrators) can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain and install those updates. The Security Administrator is able to manage the cryptographic keys (generating keys, importing keys, or deleting keys) that are used in TLS and SSH communications. These keys can be managed via CLI as part of following operations: TLS public keys, –certificate import/export, Trust store management, delete/zeroize SSH public/private keys – generate keypair, import/export public keys, public key-based authentication, delete/zeroize
FMT_MTD.1/CoreData	
FMT_MTD.1/CryptoKeys	
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE and the services provided by the TOE. The management functionality of the TOE is provided through the TOE CLI. The specific management capabilities available from the TOE include – Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above; The ability to manage the warning banner message and content – 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.

TOE SFRs	How the SFR is Met
	The ability to update the IOS-XR software. The validity of the image is provided using digital signature prior to installing the update; The ability to manage audit behavior and the audit logs which allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs; The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2; The ability to configure the authentication failure parameters for FIA_AFL.1. The ability to configure thresholds for SSH rekeying. The ability to set the time which is used for time-stamps. The ability to configure the reference identifier for the peer. The ability to import X.509v3 certificates to the TOE's trusted store. The ability to manage the trusted public keys database.
FMT_SMR.2	The TOE platform maintains both privileged and semi-privileged administrator roles. The terms "Authorized Administrator" and "Security Administrator" are used interchangeable 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. Semi-privileged administrators only contain a subset of privileges. They may also manage and modify TOE data based **only on the privileges assigned**. The TOE supports both local administration via a directly connected console cable and remote administration via SSH.
FPT_SKP_EXT.1 FPT_APW_EXT.1	The TOE stores all private keys in a secure directory that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in a hashed format that are non-readable, hence no interface access. All passwords are obscured via hashing in a secure directory. The passwords are non-readable. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. This is provided by default.
FPT_STM_EXT.1	The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock. 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 account lockout and resumption, and cert expiry checks.

TOE SFRs	How the SFR is Met
FPT_TUD_EXT.1	An Authorized Administrator can query the software version running on the TOE with the 'show version' command and can initiate updates to software images. When software updates are made available by Cisco, an administrator can obtain and install those updates. The updates can be downloaded from software.cisco.com. The validity of the image is verified using SHA-512 published hash and digital signature prior to installing the update. The TOE image files are digitally signed so their integrity is verified during the boot process, and an image that fails an integrity check will not be loaded. The TOE will not proceed until the running image passes an integrity check. The digital certificates used by the update verification mechanism are contained on the TOE. To verify the system software release version at the CLI the command "show version" is used, while the command "show install active" command will display the currently running system image filename and the system software release version.
FPT_TST_EXT.1	The TOE is designed to run a suite of power-on self-tests that comply with the FIPS140-3 requirements for self-test (e.g. known answer tests (KATs) and zeroization tests), during initial start-up to verify its correct operation. If any of the tests fail the security administrator will have to log into the CLI to determine which test failed and why. If the tests pass successfully the router will continue bootup and normal operation. During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for all the cryptographic modules perform the POST for the corresponding component (hardware or software). These tests include: AES Known Answer Test – For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly. RSA Signature Known Answer Test (both signature/verification) – This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly. RNG/DRBG Known Answer Test –

TOE SFRs	How the SFR is Met
	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. Software Integrity Test – The Software Integrity Test is run automatically whenever the IOS system images is loaded and confirms that the image file that's about to be loaded has maintained its integrity. Noise Source Health Tests – The Noise Source Health Tests check the functioning of the Noise Source that supplies randomness to the Entropy Source. The tests are designed to detect failure of the Noise Source. These tests are run at startup and continuously during normal operation. If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen, and saved in the crashinfo file. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. These tests are sufficient to verify that the cryptographic operations are all performing as expected.
FTA_SSL_EXT.1 FTA_SSL.3	An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the "session-timeout" setting applied to the console. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session. The allowable inactivity timeout range is from 1 to 65535 seconds.

TOE SFRs	How the SFR is Met
FTA_SSL.4	An administrator is able to exit out of both local and remote administrative sessions. Each administrator logged onto the TOE can manually terminate their session using the “exit” command.
FTA_TAB.1	The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. This interface is applicable for both local (via console) and remote (via SSH) TOE administration.
FTP_ITC.1	The TOE protects communications with the external audit server using TLS to secure the communications channel. TLS uses the keyed hash as defined in FCS_COP.1/KeyedHash and cryptographic hashing functions FCS_COP.1/Hash. This protects the data from modification of data by hashing that verify that data has not been modified in transit. In addition, encryption of the data as defined in FCS_COP.1/DataEncryption is provided to ensure the data is not disclosed in transit. To assure identification of a non-TSF endpoint, the endpoint presents its X.509 certificate. The TOE verifies this certificate to confirm the endpoint's identity, establishing a secure and trusted communication channel. The TOE protects communications between the TOE and the remote audit server using TLS. This provides a secure channel to transmit the log events.
FTP_TRP.1 /Admin	All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption. The remote users are able to initiate SSHv2 communications with the TOE.

ANNEX A: KEY ZEROIZATION

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

Table 19: TOE Key Zeroization

Name	Description of Key	Zeroization
Diffie-Hellman Shared Secret	This is the shared secret used as part of the Diffie-Hellman key exchange in SSH. This key is stored in DRAM (volatile).	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 (volatile).	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) using memset. This overwrites the key with all 0's. This key is stored in NVRAM (nonvolatile).	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x00
SSH Session Key	Once the function has completed the operations requiring the RSA key object, the module overwrites the entire object (no matter its contents). This is called by the ssh_close function when a session is ended. This key is stored in DRAM (volatile).	Automatically when the SSH session is terminated. Overwritten with: 0x00
User Password	This is a variable 15+ character password that is used to authenticate local users. The password is stored in NVRAM (nonvolatile)..	Zeroized by overwriting with new password
Enable Password (if used)	This is a variable 15+ character password that is used to authenticate local users at a higher privilege level. The password is stored in NVRAM (nonvolatile)..	Zeroized by overwriting with new password

Name	Description of Key	Zeroization
RNG Seed	This seed is for the RNG. The seed is stored in DRAM (volatile)	Zeroized upon power cycle the device
RNG Seed Key	This is the seed key for the RNG. The seed key is stored in DRAM (volatile).	Zeroized upon power cycle the device
AES Key	The results are zeroized by overwriting the values with 0x00. This is called by the ssh_close function when a session is ended. This key is stored in DRAM (volatile).	Automatically when the SSH session is terminated. Overwritten with: 0x00
AES Key	The results are zeroized using the poisoning in free to overwrite the values with 0x00. This is called by the ssh_close function when a session is ended.	Automatically when the SSH/TLS session is terminated. Overwritten with: 0x00
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. The key is stored in SDRAM (volatile).	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. The key is stored in SDRAM (volatile).	Automatically after TLS session terminated. The value is overwritten with "0x00."
TLS session integrity key	This key is used for TLS data integrity protection. The key is stored in SDRAM (volatile).	Automatically after TLS session terminated. The entire object is overwritten with zeros

ANNEX B: NIAP TECHNICAL DECISIONS (TDS)

The following table describes the interpretations (technical decisions) identified as relevant to the cited documents and where applicable have been applied to the specification of CPP_ND_V3.0E and PKG_SSH_V1.0.

Table 20: Technical Decisions

TD Identifier and Name	Document	Publication Date	Applicable?
TD0900 - NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	CPP_ND_V3.0E	02/27/2025	Y
TD0899 - NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	CPP_ND_V3.0E	03/06/2025	Y
TD0886 - Clarification to FAU_STG_EXT.1 Test 6	CPP_ND_V3.0E	10/16/2024	Y
TD0880 - NIT Decision: Removal of Duplicate Selection in FMT_SMF.1.1	CPP_ND_V3.0E	09/17/2024	Y
TD0879 - NIT Decision: Correction of Chapter Headings in CPP_ND_V3.0E	CPP_ND_V3.0E	09/17/2024	Y
TD0868 - NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	CPP_ND_V3.0E	09/17/2024	Y
TD0836 - NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	CPP_ND_V3.0E	04/25/2024	Y
TD0777 - Clarification to Selections for Auditable Events for FCS_SSH_EXT.1	PKG_SSH_V1.0	08/23/2023	Y
TD0732 - FCS_SSHS_EXT.1.3 Test 2 Update	PKG_SSH_V1.0	05/19/2023	Y
TD0695 - Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package.	PKG_SSH_V1.0	12/14/2022	Y
TD0682 - Addressing Ambiguity in FCS_SSHS_EXT.1 Tests	PKG_SSH_V1.0	12/13/2022	Y

ANNEX C: REFERENCES

The following documentation was used to prepare this ST:

Table 21: References

Identifier	Description
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model CCMB-2017-04-001, Version 3.1 Revision 5, April 2017.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements CCMB-2017-04-002, Version 3.1 Revision 5, April 2017.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance requirements, CCMB-2017-04-003, Version 3.1 Revision 5, April 2017.
[CEM]	Common Methodology for Information Technology Security Evaluation Evaluation methodology CCMB-2017-04-004, Version 3.1 Revision 5, April 2017
[ND3]	Collaborative Protection Profile for Network Devices Version 3.0e. 6th December, 2023
[SSH]	Functional Package for Secure Shell (SSH) Version 1.0 13th May, 2023
[NDcPP]	collaborative Protection Profile for Network Devices, Version 3.0e
[NIAP-TD]	NIAP Technical Decisions for NDcPP v3.0e, and functional package for SSH V1.0
[800-38A]	NIST Special Publication 800-38A Recommendation for Block 2001 Edition Recommendation for Block Cipher Modes of Operation Methods and Techniques December 2001
[800-56A]	NIST Special Publication 800-56A, March, 2007 Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009

Identifier	Description
	Key Establishment Schemes Using Integer Factorization Cryptography
[FIPS 140-3]	FIPS PUB 140-3 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules March 22, 2019
[CMVP #4747]	NIST CMVP : Cisco FIPS Object Module Certificate #4747. Available from: https://csrc.nist.gov/projects/cryptographic-module-validation-program/certificate/4747
[FIPS PUB 186-3]	FIPS PUB 186-3 Federal Information Processing Standards Publication Digital Signature Standard (DSS) June, 2009
[FIPS PUB 186-4]	FIPS PUB 186-4 Federal Information Processing Standards Publication Digital Signature Standard (DSS) July 2013
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008
[NIST SP 800-90A Rev 1]	NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators January 2015
[FIPS PUB 180-3]	FIPS PUB 180-3 Federal Information Processing Standards Publication Secure Hash Standard (SHS) October 2008
[FIPS PUB 198-1]	Federal Information Processing Standards Publication The Keyed-Hash Message Authentication Code (HMAC) July 2008

*** End of Document ***