Cisco Nexus 9000 Series Switches running NX-OS 10.4

Security Target

Version: 2.1

Date: 12/3/2025

Table of Contents

List of Tables

List of Figures

Acronyms

Table 1: Acronyms

Acronyms	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
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
DCNM	Data Center Network Manager
FOM	FIPS Object Module
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
IPsec	Internet Protocol security
IT	Information Technology
JENT	Cisco Jitter Entropy source
KAT	Known Answer Test
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PP	Protection Profile
PTP	Precision Time Protocol
RADIUS	Remote Authentication Dial-In User Service
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SSHv2	Secure Shell (version 2)
ST	Security Target

TACACS	Terminal Access Controller Access-Control System
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
VRF	Virtual Routing and Forwarding
WAN	Wide Area Network

Terminology

Table 2: Terminology

Term	Definition
Authorized Administrator	A person that has authorized access to the TOE to perform configuration and management tasks.
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

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 Nexus 9000 Series Switches (Nexus 9K Series).

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.

Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and Security Administrators in this document.

Revision History

Date	Version	Author	Comment
25-01-21	0.9	Cisco Systems Inc.	Published in support of CCEVS-VR-VID11514-2025
25-02-01	1.0	Cisco Systems Inc.	Base Template
25-02-28	1.1	Cisco Systems Inc.	Update Template: Styles etc Convert from NDcPP v2.0e to NDcPP v3 Remove references to NDcPP Convert to CC 2022 only with no NDcPP claim Sanity check
25-03-17	1.2	Cisco Systems Inc.	Addressing comments received after FTR
25-04-16	1.3	Cisco Systems Inc.	Updated formatting; Revert to NDcPPv3.0e CCv3.1R5 claims; Internal Review
25-05-08	1.4	Cisco Systems Inc.	Updates based on Action Item list v1.0.
25-05-15	1.5	Cisco Systems Inc.	Update based on addressing A.ASE.13

25-05-23	1.6	Cisco Systems Inc.	Added NIAP site location for PCL guidance
25-06-04	1.7	Cisco Systems Inc.	Updated to specify Cisco location used to access ST and AGD
25-06-06	1.8	Cisco Systems Inc.	Updated to include TD0918
25-06-12	1.9	Cisco Systems Inc.	Updated to include reference to ALC_FLR.2; Updated to reference FIPS 140-3 Level 1.
25-11-06	2.0	Cisco Systems Inc.	Addressing comments following ERM1+2
25-12-03	2.1	Cisco Systems Inc.	Addressing comments following ERM3

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]
- Security Functional Requirements [Section 5]
- Security Assurance Requirements [Section 6]
- TOE Summary Specification [Section 7]

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

1.1 ST and TOE Reference

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

Table 3: ST and TOE Identification

Name	Description
ST Title	Cisco Nexus 9000 Series Switches running NX-OS 10.4 Security Target
ST Version	2.1
ST Publication Date	12/3/2025
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Nexus 9000 Series Switches
TOE Hardware Models	Cisco Nexus 9200 Series Switches Cisco Nexus 9300 Series Switches Cisco Nexus 9400 Series Switches Cisco Nexus 9500 Series Switches Cisco Nexus 9800 Series Switches
TOE Software Version	Cisco NX-OS version 10.4(5)(M)
Keywords	Switch, Data Protection, Audit, Authentication, Encryption, Network Device, Secure Administration

TOE Guidance	Cisco Nexus 9000 Series Switches running on NX-OS 10.4 Common Criteria Operational User Guidance and Preparative Procedures
Guidance Version	1.6
Guidance Publication Date	11/06/2025

1.2 TOE Overview

The Target of Evaluation (TOE) is the Cisco Nexus 9000 Series Switches running NX-OS 10.4 (herein after referred to as Cisco Nexus 9K Series, Nexus 9K, or the TOE).

The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 9200, 9300, 9400, 9500, and 9800. The software is comprised of the NX-OS software image Release 10.4.

The TOE is a purpose-built data center-class switch for use as an aggregation switch in the data center. The TOE includes the hardware models as defined in Table 5 – Hardware Models and Descriptions.

Cisco NX-OS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although NX-OS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in 1.6 Logical Scope of the TOE below.

1.2.1 TOE Product Type

The Cisco Nexus 9K Series are data center-class switches for use as an aggregation switch in the data center. The Cisco Nexus 9K Series provides multilayer support, greater performance and enhanced operations through features including intelligent services, programmability, automation, analytics, and manageability.

The Nexus 9200 platform consists of industry-leading ultra-high-density fixed-configuration data center switches with line-rate Layer 2 and 3 features that support enterprise and commercial applications, service provider hosting, and cloud computing environments. These switches support a wide range of port speeds with flexible combinations of 1/ 10/ 25/ 40/ 50/ and 100-Gbps connectivity in compact One-Rack-Unit (1RU) and Two-Rack-Unit (2RU) form factors.

The Nexus 9300 platform consists of fixed-port switches designed for top-of-rack (ToR) and middle-of-row (MoR) deployment in data centers that support enterprise applications, service provider hosting, and cloud computing environments. They are Layer 2 and 3 nonblocking 10 and 40 Gigabit Ethernet switches with up to 2.56 terabits per second (Tbps) of internal bandwidth that come in compact One-Rack-Unit (1RU), Two-Rack-Unit (2RU), and Three-Rack-Unit (3RU) form factors.

The Nexus 9400 platform consists of modular switches that provide high density 400G solutions in a centralized modular chassis design. The Cisco Nexus 9400 series switches are designed with a height of 4 RU and depth of 24 inches including eight expansion slots to support 64 ports of 400G or 128

ports of 200 G. Furthermore, the chassis architecture supports a supervisor, and up to 8 expansion modules, fan tray redundancy with 5 fan trays, and power supply redundancy.

The Nexus 9500 platform consists of modular switches that provide high density 400G solutions in a centralized modular chassis design. They are Layer 2 and 3 nonblocking switches that support a comprehensive selection of line cards and fabric modules that provide 1-, 10-, 25-, 40-, 50-, 100-, 200-, and 400-Gigabit Ethernet interfaces.

The Nexus 9800 platform consists of modular switches that provide high density 400G solutions in a chassis designed for future transition to high-density 800G and higher speeds. They are Layer 2 and 3 nonblocking switches that support a comprehensive selection of line cards and fabric modules that provide 1-, 10-, 25-, 40-, 50-, 100-, 200-, and 400-Gigabit Ethernet interfaces.

1.2.2 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 4: IT Environment Components

Component	Required	Usage/Purpose Description for TOE performance
Local Console	Yes	This includes any IT Environment Console that is directly connected to the TOE via the Serial Console Port and is used by the TOE administrator to support TOE administration.
Management Workstation with SSH Client	Yes	This includes any IT Environment Management workstation with a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.

1.3 TOE Description

This section provides an overview of the Cisco Nexus 9K Series Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 9200, 9300, 9400, 9500, and 9800. The software is comprised of the NX-OS software image Release 10.4.

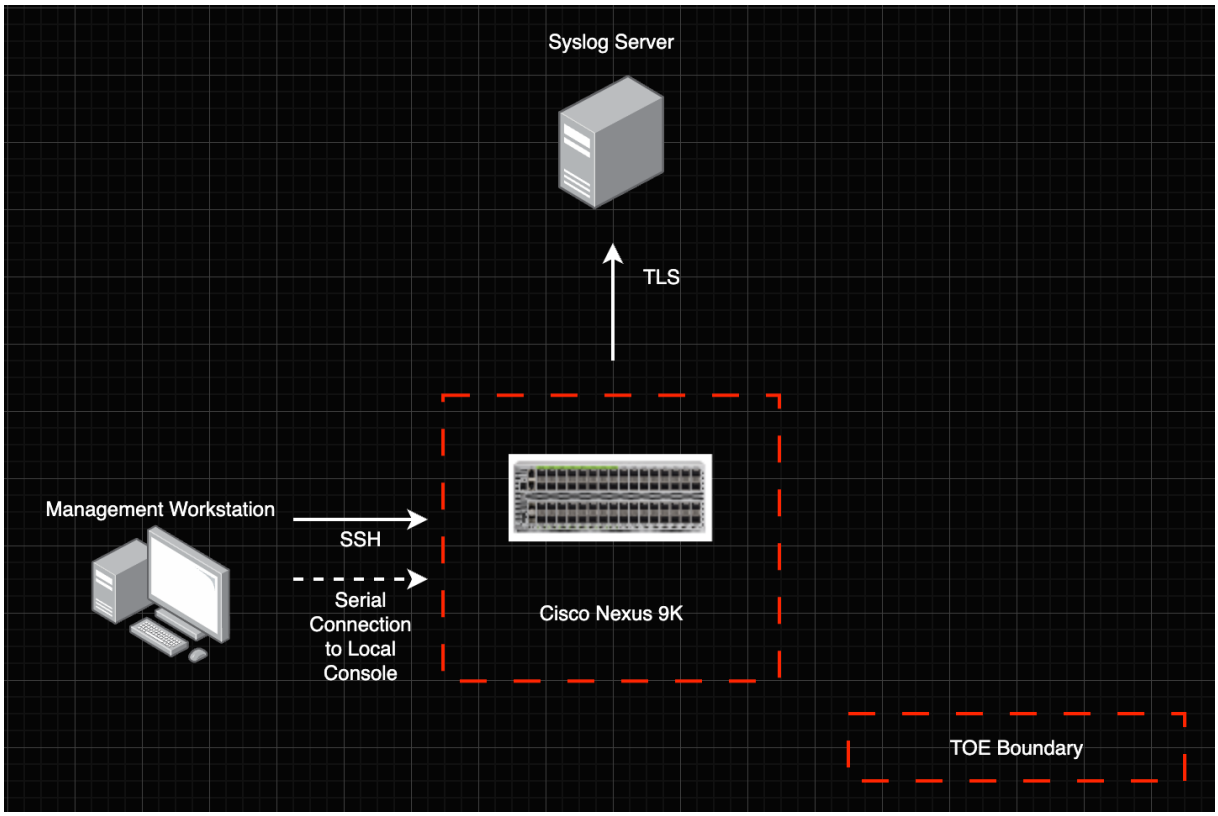
The Cisco Nexus 9000 Series Switches that comprise the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware. All security functionality is enforced on the Nexus 9000 Series switches.

NX-OS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although NX-OS performs many networking functions,

this TOE only addresses the functions that provide for the security of the TOE itself as described in 1.6 Logical Scope of the TOE below.

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

Figure 1: Nexus 9000 Series Switches TOE and the Environment



The figure above includes the following:

The TOE models:

- Cisco Nexus 9000 Series Switches

The following are considered to be in the IT Environment:

- Management Workstation
- Syslog Server

For management purposes the TOE provides command line access to administer the TOE and remote access over SSH.

1.4 TOE Evaluated Configuration

The TOE consists of one or more switches as specified in section 1.5 below and includes the NX-OS software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco NX-OS configuration determines how packets are handled to and from the TOE's network interfaces. The switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the 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. Audit records are

stored locally and are also remotely backed up to a remote syslog server. If these servers are used, they 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.

1.5 Physical Scope of the TOE

The TOE is a hardware and software solution made up of the models as follows: Nexus 9200, 9300, 9400, 9500, and 9800 series. The network, on which they reside, is considered part of the IT environment.

The TOE is comprised of the following physical specifications as described in Table 5 below. For more information on secure acceptance of the TOE hardware and software, please see Section 2 of the Cisco Nexus 9000 Series Switches running on NX-OS 10.4 Common Criteria Operational User Guidance and Preparative Procedures [AGD].

The [AGD] can be obtained at https://www.niap-ccevs.org/products by searching for the TOE, which is the Cisco Nexus 9000 Series Switches. Products currently in evaluation can be viewed on the NIAP Products in Evaluation page, and certified Cisco products can be viewed on the Product Compliance List.

[AGD]s for Cisco products can also be obtained in the Global Government Certifications section at https://www.cisco.com. Full link is below:

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html

Table 5: Hardware Models and Specifications

Model	Processor	Software	Interfaces
Cisco Nexus 9200 Series  **N9K- C92348GC-X**	**92348GC-X**: Intel Xeon D-1526 (Broadwell)	https://software.cisco.com Cisco NX-OS 10.4 **Image Name:** nxos64-cs.10.4.5.M.bin	Management ports: 1 RJ-45, 1 SFP+ Console serial port: 1 RJ-45 USB port (1)
Cisco Nexus 9300 Series	**93108TC-FX, 93216TC-FX2, 93240YC-FX2,**	https://software.cisco.com	**93108TC-EX, 93108TC-FX:**

    **N9K-C93108TC-FX,** **N9K-C9348GC-FXP,** **N9K-C93216TC-FX2,** **N9K-C93180YC-FX,** **N9K-C93240YC-FX2,** **N9K-C93360YC-FX2,** **N9K-C9364C,** **N9K-C9332C,** **N9K-C9336C-FX2,** **N9K-C9364C-GX,** **N9K-C9316D-GX,** **N9K-C93600CD-GX,** **N9K-C93400LD-H1**	**93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX**: Intel Xeon D-1526 (Broadwell) **93180YC-FX**: Intel Xeon D-1528 (Broadwell) **93400LD-H1**: Intel Xeon D-1623N (Broadwell)	Cisco NX-OS 10.4 **Image Name:** nxos64-cs.10.4.5.M.bin	Management ports: 1 RJ-45 Console serial port: 1 RJ-45 USB ports (2) **9348GC-FXP, 93216TC-FX2, 93180LC-EX**: Management ports: 1 RJ-45 and 1 SFP+ Console serial port: 1 RJ-45 USB ports (1) **93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2**: Management ports: 1 RJ-45 Console serial port: 1 RJ-45 USB ports (2) **9364C, 9332C:** Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)

			9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX, 93400LD-H1: Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)
Cisco Nexus 9400 Series  **N9K-C9400-Sup-A**	**Supervisor 9400-Sup-A:** Intel Xeon D-1633N (Broadwell)	https://software.cisco.com Cisco NX-OS 10.4 **Image Name:** nxos64-cs.10.4.5.M.bin	**N9K-C9400-Sup-A** Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1/10-Gbps SFP+) Console serial port: 2 (1 x RJ-45 and 1 x RS232) USB ports (1)
Cisco Nexus 9500 Series  **N9K-C9504,** **N9K-C9508,**	**Supervisor 9500-Sup-A+**: Intel Xeon D-1526 (Broadwell) **Supervisor 9500-Sup-B+**: Intel Xeon D-1528 (Broadwell)	https://software.cisco.com Cisco NX-OS 10.4 **Image Name:** nxos64-cs.10.4.5.M.bin	Based on Supervisor and I/O modules installed **N9K-SUP-A+, N9K-SUP-B+:** Management ports: 1 RJ-45 Console serial port: 1 RJ-45 USB ports (2)

N9K-C9516, **N9K-SUP-A+,** **N9K-SUP-B+,** **N9K-SC-A**			
Cisco Nexus 9800 Series  **N9K-C9808,** **N9K-C9804**	**Supervisor 9800-Sup-A:** Intel Xeon D-1530 (Broadwell DE)	https://software.cisco.com Cisco NX-OS 10.4 **Image Name:** nxos64-cs.10.4.5.M.bin	Based on I/O modules installed **N9K-C9808**: Cisco Nexus 9800 8-slot chassis supports eight line-card slots and three power-supply trays. **N9K-C9804**: Cisco Nexus 9800 4-slot chassis supports four line-card slots and two power-supply trays. N9K-C9804-FM-A: Cisco Nexus 9800 4-slot chassis fabric module (1st Generation) N9K-C9804-FAN-A: Cisco Nexus 9800 4-slot chassis fan tray (1st Generation)

			N9K-X9836DM-A: Nexus 9800 36-port 400G Line Card N9K-X98900CD-A: Nexus 9800 34-port 100G + 14-port 400G Line Card

1.6 Logical Scope of the TOE

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

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

These features are described in more detail in the subsections below. In addition, the TOE implements all RFCs of the None and PKG_SSH_v1.0 as necessary to satisfy testing/assurance measures prescribed therein.

1.6.1 Security Audit

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The Authorized Administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides a circular audit trail. Audit logs are transmitted to an external audit server over a trusted channel protected with TLS.

The auditable events include:

- failure on invoking cryptographic functionality such as establishment, termination and failure of cryptographic session establishments and connections;

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

The Authorized Administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE is configured to transmit the audit messages to an external syslog server. Communication with the syslog server is protected by using TLS and the TOE can determine when communication with the syslog server fails. In the presence of a TLS communication failure, the TOE will continuously and automatically re-attempt to reestablish the syslog connection in case of a network disruption. In the case of a TLS protocol failure the administrator should review the configuration of both the TOE and the syslog server.

The audit logs can be viewed on the TOE using the appropriate NX-OS commands. The records include the date/time the event occurred, the event/type of event, the user associated with the event, and additional information of the event and its success and/or failure. The TOE does not have an interface to modify audit records, though there is an interface available for the authorized administrator to clear (delete) audit data stored locally on the TOE.

1.6.2 Cryptographic Support

The TOE provides cryptography in support of remote administrative management via SSHv2 and secure the session between the TOE 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/ECDHE Signature Services	Used in SSH session establishment.
HMAC	Used for keyed hash, integrity services in SSH session establishment.
AES CBC, CTR, GCM (128, 256)	Used to encrypt SSH and TLS session traffic.

Cryptographic Method	Use within the TOE
SHA	Used to provide SSH traffic integrity verification
TLS	Used to secure traffic to the syslog server.

The NX-OS software calls the CiscoSSL FOM Cryptographic implementation version 7.3a and has been validated for conformance to the requirements of FIPS 140-3 Level 1.

1.6.3 Identification and authentication

The TOE provides cryptography in support of remote administrative management and data exports via SSHv2 and TLS to secure the transmission of audit records to the remote syslog server.

The TOE provides authentication services for administrative users wishing to connect to the TOE's secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE is configured to require a minimum password length of 8 characters as well as password-strength checking that disables the use of weak passwords. 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.

After a configurable number of incorrect login attempts, Cisco Nexus 9K Series will lockout the account until an Authorized Administrator takes action.

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

1.6.4 Security management

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

- Administration of the TOE locally and remotely;
- Configuration of warning and consent access banners;
- Configuration of session inactivity thresholds;
- Updates of the TOE software;
- Configuration of authentication failures;
- Configuration of the audit functions of the TOE;
- Configuration of the TOE provided services; and
- Configuration of the cryptographic functionality of the TOE.

The Cisco Nexus 9K Series switch supports the following predefined roles:

- network-admin – This role is a super administrative role. This role has read and write privileges for any configuration item on the Nexus 9000 Series.
- network-operator - This role has read access to the entire NX-OS device.

- server-admin - Complete read access to the entire NX-OS device and upgrade capability.

All administrators are considered to be Security Administrators in this ST. The Cisco Nexus 9K Series has a command line interface (CLI) that can be administered either remotely using SSHv2 or locally via a console that is directly connected via a serial cable.

1.6.5 Protection of the TSF

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

The TOE internally maintains the date and time. This date and time are 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 can verify any software updates prior to the software updates being installed on the TOE to avoid the installation of unauthorized software.

1.6.6 TOE Access

The TOE can terminate inactive sessions after an Authorized Administrator configurable time-period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session. The administrator can also terminate their own session by exiting out of the CLI.

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

1.6.7 Trusted path/Channels

The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 for remote CLI access. Nexus 9K also allows a trusted channel to be established with a syslog server using TLS.

1.7 Excluded Functionality

The functionality listed below will be disabled by configuration, as described in the Guidance documents (AGD). The excluded functionality does not affect conformance to the collaborative Protection Profile for Network Devices v3.0e.

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.
Bash shell	Bash shell interface was not included in the evaluation.
DCNM GUI	The DCNM GUI was not included in the evaluated configuration.
HTTP / HTTPS	HTTP web server was not included in the evaluation. It must be configured to tunnel using SSH as specified in the AGD.
IKE	IKE was not included in the evaluation. Secured connection to a remote syslog uses TLS as specified in the AGD.
IPsec	IPsec was not included in the evaluated configuration. It must remain disabled in the evaluated configuration.
LDAP	LDAP was not included in the evaluated configuration. LDAP (Not secure) must remain disabled in the evaluated configuration. Note that LDAP (secure) is allowed over TLS.
NTP	NTP was not included in the evaluation. It must be disabled in the evaluated configuration as specified in the AGD.
PTP	PTP was not included in the evaluation. It must remain disabled in the evaluated configuration as specified in the AGD.
RADIUS	RADIUS was not included in the evaluation. It must be used as specified in the AGD.
SNMP	SNMP was not included in the evaluation. It must remain disabled in the evaluated configuration.
TACACS+	TACACS+ was not included in the evaluation. It must remain disabled in the evaluated configuration and must be disabled in the evaluated configuration.
Telnet	Telnet was not included in the evaluation. It must remain disabled in the evaluated configuration

These services will be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect the compliance to the NDcPPv3.0e and 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. For a listing of Assurance Requirements claimed see section 6.

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 claim exact conformance with the Protection Profiles listed in Table 8 below which includes ALC_FLR.2 for flaw remediation.

Table 8 Protection Profiles

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

2.3 Package Conformance

In accordance with CPP_ND_V3.0E, this ST claims exact conformance with the Functional Package for Secure Shell (SSH) V1.0 (PKG_SSH_V1.0) dated 13 May, 2021.

Table 9 Functional Packages

Protection Profile	Version	Date

Functional Package for Secure Shell (SSH)	1.0	13 May 2021

The following NIAP Technical Decisions (TD) have also been applied to the claims in this document. Each posted TD was reviewed and considered based on the TOE product type, the PP claims and the security functions claimed in this document.

Table 10 Technical Decisions

TD #	TD Name	Protection Profile	Applicable	Exclusion Rationale
TD0923	NIT Technical Decision: Auditable event for FAU_STG_EXT.1 in FAU_GEN.1.2	NDcPPv3.0e	Yes	
TD0921	NIT Technical Decision: Addition of FIPS PUB 186-5 and Correction of Assignment	NDcPPv3.0e	Yes	
TD0918	NIT Technical Decision: Addition of FIPS PUB 186-5	NDcPPv3.0e	Yes	
TD0909	Updates to FCS_SSH_EXT.1.1 App Note in SSH FP 1.0	PKG_SSH_v1.0	Yes	
TD0900	NIT Technical Decision: Clarification to Local Administrator Access in FIA_UIA_EXT.1.3	NDcPPv3.0e	Yes	
TD0899	NIT Technical Decision: Correction of Renegotiation Test for TLS 1.2	NDcPPv3.0e	Yes	
TD0886	Clarification to FAU_STG_EXT.1 Test 6	NDcPPv3.0e	Yes	
TD0880	NIT Decision: Removal of Duplicate Selection in FMT_SMF.1	NDcPPv3.0e	Yes	
TD0879	NIT Decision: Correction of Chapter Headings in CPP_ND_v3.0E	NDcPPv3.0e	Yes	
TD0868	NIT Technical Decision: Clarification of time frames in FCS_IPSEC_EXT.1.7 and FCS_IPSEC_EXT.1.8	NDcPPv3.0e	No	IPsec is not claimed
TD0836	NIT Technical Decision: Redundant Requirements in FPT_TST_EXT.1	NDcPPv3.0e	Yes	

TD0828	Aligning MOD_IPS_V1.0 with CPP_ND_V3.0E	NDcPPv3.0e	No	MOD_IPS is not included
TD0827	Aligning MOD_CPP_FW_v1.4E with CPP_ND_V3.0E	NDcPPv3.0e	No	MOD_CPP_FW is not included
TD0777	Clarification to Selections for Auditable Events for FCS_SSH_EXT.1	PKG_SSH_v1.0	Yes	
TD0732	FCS_SSHS_EXT.1.3 Test 2 Update	PKG_SSH_v1.0	Yes	
TD0695	Choice of 128 or 256 bit size in AES-CTR in SSH Functional Package.	PKG_SSH_v1.0	Yes	
TD0682	Addressing Ambiguity in FCS_SSHS_EXT.1 Tests	PKG_SSH_v1.0	Yes	

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 Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the [NDcPP] and [PKG_SSH], 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 the [NDcPP] and [PKG_SSH], 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 the [NDcPP] and [PKG_SSH], 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 the [NDcPP] and [PKG_SSH].

3 SECURITY PROBLEM DEFINITION

This chapter identifies the following:

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

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

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

3.1 Assumptions

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

Table 11: TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security 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.

Assumption	Assumption Definition
	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 12: Threats

Threat	Threat Definition
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
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 of the TOE.

Table 13: Organizational Security Policies

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

The collaborative Protection Profile for Network Devices v3.0e and the Functional Package for Secure Shell (SSH) v1.0 do 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, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 14: Security Objectives for the Environment

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
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.

Environment Security Objective	IT Environment Security Objective Definition
OE.UPDATES	The TOE firmware and software is updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5 SECURITY FUNCTIONAL REQUIREMENTS

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from [NDcPP], [PKG_SSH], and NIAP Technical Decisions.

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 15: Security Functional Requirements

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

Class Name	Component Identification	Component Name
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_SSH_EXT.1	SSH Protocol
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.1	TLS Client Protocol
FIA: Identification and authentication	FIA_AFL.1	Authentication Failure Management (Refinement)
	FIA_PMG_EXT.1	Password Management
	FIA_PSK_EXT.1	Pre-Shared Key Composition
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
	FIA_X509_EXT.1/Rev	X.509 Certificate Validation
	FIA_X509_EXT.2	X.509 Certificate Authentication
FMT: Security management	FMT_MOF.1/ManualUpdate	Management of security functions behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)

Class Name	Component Identification	Component Name
	FPT_STM_EXT.1	Reliable Time Stamps
	FPT_TUD_EXT.1	Trusted update
	FPT_TST_EXT.1	TSF Testing (Extended)
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted Path

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:

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

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the **c**PP/ST, *information specified in columns two and three* of *Table 16.*

Table 16: 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_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]	Reason for failure [Non-TOE endpoint of connection (IP Address)]
	[Establishment of SSH connection]	[Non-TOE endpoint of connection (IP Address)]

	[Termination of SSH connection]	[Non-TOE endpoint of connection (IP Address)]
	[Dropping of packet(s) outside defined size limits]	[Packet size]
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_UAU_EXT.2	All use of the authentication mechanism.	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_MOF.1/Services	None.	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 [log file, buffer] of audit records in the event that an interruption of communication with the remote audit server occurs.

FAU_STG_EXT.1.4 The TSF shall be able to store [non-persistent] audit records locally with a minimum storage size of [*4096 bytes*].

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 Refinement: 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 or FIPS PUB 186-5, “Digital Signature Standard (DSS)”, A.1;

- 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, or FIPS PUB 186-5. “Digital Signature Standard (DSS)”, Appendix A.2, or ISO/IEC 14888-3, “IT Security techniques – Digital signature with appendix – Part 3: Discrete logarithm based mechanisms”, Section 6.6.;
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1

] ~~and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet~~

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

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 meets the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”;
- Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”;
- FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526].

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

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-pass] 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, CTR, GCM] *mode* and cryptographic key sizes [128 bits, 256-bits] that meet the following: *AES as specified in ISO 18033-3*, [CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772].

5.3.2.5 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
- Elliptic Curve Digital Signature Algorithm

]

and cryptographic key sizes [

- For RSA: modulus 2048 bits,
- For ECDSA: 256 bits, 384 bits, 521 bits

]

that meet the following:

[

- For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSAPKCS2v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3,

- For ECDSA schemes implementing [P-256, P-384, P-521] curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section and Appendix D, Implementing “NIST Recommended” curves; or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 6 and NIST SP 800-186 Section 3.2.1, Implementing Weierstrass curves; or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.

].

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 [SHA-256, SHA-384, SHA-512] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*]~~ and **message digest sizes** [**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-256, HMAC-SHA-512*] and cryptographic key sizes [*256-bit, 512-bit*] **and message digest sizes** [**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 [[*1*]: platform-based noise source] with minimum of [*256 bits*] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

5.3.2.9 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-sha2-256 (RFC 8332),
    - ecdsa-sha2-nistp256 (RFC 5656),
    - 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 [*262,126 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-ctr (RFC 4344),
- aes256-ctr (RFC 4344),
- aes128-gcm@openssh.com (RFC 5647),
- aes256-gcm@openssh.com (RFC 5647)

] and no other mechanisms.

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

- hmac-sha2-256 (RFC 6668),
- hmac-sha2-512 (RFC 6668),
- implicit

] and no other mechanisms.

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

- ecdh-sha2-nistp256 (RFC 5656),
- ecdh-sha2-nistp384 (RFC 5656),
- ecdh-sha2-nistp521 (RFC 5656),

] and no other mechanisms.

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

- RFC 4253 (Section 7.2),
- 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-sha2-256 (RFC 8332),
- ecdsa-sha2-nistp256 (RFC 5656),
- 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
TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492,
TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246
TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288
TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289,
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289

] 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, IPv4 address in the SAN].

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 [present the Supported Groups Extension with the following curves/groups: [secp256r1, secp384r1, secp521r1] and no other curves/groups] 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),
    - ecdsa_secp256r1 with sha256(0x0403),
    - ecdsa_secp384r1 with sha384(0x0503),
    - ecdsa_secp521r1 with sha512(0x0603),
    - rsa_pss_rsae with sha256(0x0804),
    - rsa_pss_rsae with sha384(0x0805),
    - rsa_pss_rsae with sha512(0x0806),
    - rsa_pss_pss with sha256(0x0809),
    - rsa_pss_pss with sha384(0x080a),
    - rsa_pss_pss with sha512(0x080b)
    - *]* 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:

- Early data extension
- 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 [reject [TLS 1.2] 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 [*1-65535*] unsuccessful authentication attempts occur related to *Administrators attempting to authenticate remotely using a password*.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met, the TSF shall [prevent the offending Administrator from successfully establishing a remote session using any authentication method that involves a password until [*unblocking action*] is taken by an Administrator, 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: [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”,[no other characters]];
b) Minimum password length shall be configurable to between [8] and [127] 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 [no other mechanism]. The TSF shall provide the following local authentication mechanisms [password-based].

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

5.3.3.4 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 [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- 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_MOF.1/Services Management of Security Functions Behaviour

FMT_MOF.1.1/Services The TSF shall restrict the ability to start and stop ~~the functions~~ services to Security Administrators.

5.3.4.3 FMT_MTD.1/CoreData Management of TSF Data

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

5.3.4.4 FMT_MTD.1/CryptoKeys Management of TSF Data

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

5.3.4.5 FMT_SMF.1 Specification of Management Functions

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

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

- *Ability to start and stop services;*
- *Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size);*
- *Ability to modify the behaviour of the transmission of audit data to an external IT entity;*
- *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1;*
- *Ability to manage the cryptographic keys;*
- *Ability to configure thresholds for SSH rekeying;*
- *Ability to re-enable an Administrator account;*
- *Ability to set the time which is used for time-stamps;*
- *Ability to manage the TOE's trust store and designate X509.v3 certificates as trust*

anchors;
- *Ability to administer the TOE locally;*
- *Ability to configure the local session inactivity time before session termination or locking;*
- *Ability to configure the authentication failure parameters for FIA_AFL.1;*
- *Ability to manage the trusted public keys database;*

].

5.3.4.6 FMT_SMR.2 Restrictions on security roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator*.

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

FMT_SMR.2.3 The TSF shall ensure that the conditions:

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

are satisfied.

5.3.5 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;

- Prior to providing any cryptographic service and [at no other time] to verify correct operation of cryptographic implementation necessary to fulfil the TSF;
- [start-up] self-tests [
    - *AES Known Answer Test*
    - *HMAC Known Answer Test*
    - *RNG/DRBG Known Answer Test*
    - *SHA-1/SHA-256/SHA-384/SHA-512 Known Answer Test*
    - *RSA Signature Known Answer Test (both signature/verification)*
    - *Software Integrity Test*

  ]

to demonstrate the correct operation of the TSF.

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

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

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

5.3.6 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 ~~user~~ **Administrator**-initiated termination of the ~~user's~~ **Administrator**'s own interactive session.

5.3.6.4 FTA_TAB.1 Default TOE Access Banners (Refinement)

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

5.3.7 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 ~~another trusted IT product~~ **authorized IT entities supporting the following capabilities: audit server, [*no other capabilities*]** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from ~~modification or~~ 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 *[communications with the following:*

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

FTP_TRP.1.2/Admin The TSF shall permit remote **Administrators** ~~users~~ 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

The NDcPPv3.0e and PKG_SSH_v1.0 contain all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PPs have been approved.

6 SECURITY ASSURANCE REQUIREMENTS

6.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the CPP_ND_V3.0E and PKG_SSH_v1.0, which is derived from Common Criteria Version 3.1, Revision 5. The assurance requirements are summarized in the table below:

Table 17: Assurance Measures

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

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 18: Applied 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 Version 3.1, Revision 5, dated: April 2017, CC Part 2 extended and CC Part 3 conformant and NDcPPv3.0e, and the rationale of how the TOE provides all of the functionality at a level of security commensurate with that identified in NDcPPv3.0e. 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 rationale 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.
ALC_CMC.1	The AGD and ST implicitly meet this assurance requirement. The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check 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	

Component	How requirement will be met
ALC_FLR.2	Cisco documents the flaw remediation and reporting procedures so that security flaw reports from TOE users can be appropriately acted upon, and TOE users can understand how to submit security flaw reports to the developer.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide 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 above are met by the TOE.

Table 19: How TOE SFRs are Met

TOE SFRs	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record that is stored internally within the TOE whenever an audited event occurs. The types of events that cause audit records to be generated include, cryptography related events, events related to the enforcement of information flow policies, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in Table 16. Each of the events is specified in the syslog which is stored internal to the TOE in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred. Each time an administrative user logs into or off the Nexus 9000 Series switch, an audit record is generated. The audit record contains the Day of Week, the Date, the Action, the User ID, and terminal information (where applicable) of the user logging into the Nexus 9000 Series switch. Whenever an administrative user makes a configuration change to the Nexus 9000 Series switch, an audit record is generated on a per-command basis. Likewise, the audit record contains the Day of Week, the Date, the Action, the User ID, the outcome of the event, and terminal information (where applicable) of the user making the configuration change. In addition to information such as this for the administrative task of generating/import of, changing, or deleting of cryptographic keys a unique key name is included in the audit record. Auditing cannot be disabled except by shutting down the TOE and is automatically available upon the startup of the TOE. The TOE startup and shutdown is captured in the audit trail and servers as the audit records for these events. Example audit events are included below:

TOE SFRs	How the SFR is Met

	`Sun Mar 31 02:50:39 2024:type=update:id=10.1.2.3@pts/0:user=admin:cmd= configure terminal ; username user1 password 0 ****`
	
	`**** (SUCCESS)`
	
	In the above log event a date and timestamp is displayed as well as an event description "cmd=configure terminal". The subject identity where a command is directly run by a user is displayed "user=admin." The outcome of the command is displayed: "SUCCESS"
	
	To configure the TOE to send audit records to a syslog server, the "***logging server*** *name [severity-level] [port number] [secure [trustpoint client-identity name]] [facility facility-name]*" command is used. A maximum of three syslog servers can be configured. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The audit records are transmitted using TLS to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record and all permit traffic is denied until the communications is re-established.

FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example, a human user, user identity, or related session ID would be included in the audit record. When the event is related to a remote user or entity, the IP address, MAC address, host name, or other configured identification included in the message. A sample audit record is below: `Sun Mar 31 05:49:59 2024:type=update:id=10.1.2.3@pts/0:user=admin:cmd= configure terminal ; no username user1 (SUCCESS)`
FAU_STG_EXT.1	Access to the audit records stored on the TOE is only through a TSF Mediated interface. Only users explicitly authorized to access the audit records are given access to the audit records. There is no interface which

TOE SFRs	How the SFR is Met
	may be used to perform audit record modification. In addition, logs can only be cleared by an authorized administrator. The TOE is configured to export syslog records to a specified, external syslog server. Once the configuration is complete, the audit records are automatically sent to the external syslog server at the same time as they are written to the logging buffer. The TOE protects communications with an external syslog server via TLS. If the TLS connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents to the syslog server. For the Nexus 9000 Series, logs are written to NVRAM. By default, a maximum of 100 system messages of severity 0, 1, or 2 (emergency, alert, or critical) are logged to NVRAM (#show logging nvram). Log messages are not saved across system reboots. The logging logfile global configuration command enables copying of system messages to an internal log file in flash, allows for setting the level of logging (0-7) and optionally the size of the file can be set in bytes as well as the name of the log file. The severity levels are: 0 – Emergency (System unusable) 1 – Alert (Immediate action required) 2 – Critical (Critical condition) 3 – Error (Error condition) 4 – Warning (Warning Condition) 5 – Notification (Normal but significant condition) 6 – Informational (informational messages only) 7 – Debugging (Appears during debugging only)

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>Example:

<code># logging logfile my_log 6</code>

The logging to NVRAM and flash provide persistent logging data after a system reload. By default, the logs are circular and once the log files reach capacity of the flash storage, they are overwritten. With NX-OS, there is logging of event-histories that run in the background by default. The event-history log size is configurable.</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 used for device authentication:

<table>
<tr><th>Scheme</th><th>Standard</th><th>Key Size/

NIST Curve</th><th>SFR</th><th>Service</th></tr>
<tr><td>RSA</td><td>FIPS PUB 186-4</td><td>2048</td><td>FCS_SSH_EXT.1</td><td>SSH Remote Administration</td></tr>
<tr><td>ECC</td><td>FIPS PUB 186-4</td><td>P-256

P-384

P-521</td><td>FCS_SSH_EXT.1</td><td>SSH Remote Administration</td></tr>
</table>

The following table shows the key generation algorithms implemented by the TOE 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>RSA</td><td>FIPS PUB 186-4</td><td>2048</td><td>FCS_TLSC_EXT.1</td><td>Transmit audit data to an</td></tr>
</table>
</td></tr>
</table>

TOE SFRs	How the SFR is Met

				external syslog server
ECC	FIPS PUB 186-4	P-256 P-384 P-521	FCS_SSH_EXT.1	SSH Remote Administration
			FCS_TLSC_EXT.1	Transmit audit data to an external syslog server
FFC	FIPS PUB 186-4	3072	FCS_TLSC_EXT.1	Transmit audit data to an external syslog server

The following table shows the methods that the TOE implements for key establishment:

Scheme	**Standard**	**Key Size/** **NIST Curve**	**SFR**	**Service**
RSA	FIPS PUB 186-4	2048	FCS_TLSC_EXT.1	Transmit audit data to an external syslog server
ECC	FIPS PUB 186-4	P-256 P-384 P-521	FCS_SSH_EXT.1	SSH Remote Administration
			FCS_TLSC_EXT.1	Transmit audit data to an external syslog server

<table>
<tr><th>TOE SFRs</th><th>How the SFR is Met</th></tr>
<tr><td></td><td>
<table>
<tr><td>FFC</td><td>FIPS PUB 186-4</td><td>3072</td><td>FCS_TLSC_EXT.1</td><td>Transmit audit data to an external syslog server</td></tr>
</table>

The TOE implements RSA key establishment schemes that are conformant to NIST SP 800-56B. The TOE complies with section 6 and all subsections regarding RSA key pair generation and key establishment in the NIST SP 800-56B. The TOE implements Elliptic Curve Diffie-Hellman (ECDH) (ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521) key establishment schemes in SSH. The ECDH key generation meets the NIST FIPS PUB 186-4 Appendix B.1. ECC schemes are used with P-256, P-384, and P-521.

The TOE also supports FCC schemes for key establishment with a minimum size of 3072 bits.

The key pair generation portions of "The RSA Validation System" for FIPS 186-4 were used as a guide in testing the FCS_CKM.1 during the FIPS validation.

The TOE employs RSA-based key establishment used in cryptographic operations with support for 2048-bit keys.

For details on each protocol, see the related SFR.</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) in that none of the symmetric keys, pre-shared keys, or private keys are stored in plaintext.

Through the implementation of cryptographic module, the TOE zeroizes all of the cryptographic keys used within the TOE after the key is no longer of use to the TOE. The key and CSP zeroization capabilities of the TOE have</td></tr>
</table>

TOE SFRs	How the SFR is Met
	been verified as part of the TOE's FIPS 140-3 validation. See Table 20 for more information. The cryptographic key destruction is used as follows: • After TOE administration via SSH/SFTP is completed, the tunnel is torn down and the session key is overwritten.
FCS_COP.1/DataEncryption	The TOE provides symmetric encryption and decryption capabilities using AES in CBC, CTR and GCM mode (128, 256 bits) as described in ISO 18033-3, ISO 10116, and ISO 19772. AES is used in the following protocols: SSHv2 and TLS. Through the implementation of the FIPS validated cryptographic module, the TOE provides AES encryption and decryption in support of SSHv2, and TLS for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands.
FCS_COP.1/Hash	The TOE provides cryptographic hashing services using SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004. Through the implementation of the FIPS validated cryptographic module, the TOE provides Secure Hash Standard (SHS) hashing in support of TLS and SSH for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands.
FCS_COP.1/KeyedHash	The TOE provides keyed-hashing message authentication services using HMAC-SHA-256 that operates on 512-bit blocks and HMAC-SHA-512 that operates on 1024-bit blocks of data with key sizes and message digest sizes of 256, 512 bits, respectively as specified in ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". Through the implementation of the FIPS validated cryptographic module, the TOE provides SHS hashing and HMAC message authentication in support of SSHv2, and TLSv1.2 for secure communications. Management

TOE SFRs	How the SFR is Met
	of the cryptographic algorithms is provided through the CLI with auditing of those commands. SHS hashing and HMAC message authentication (SHA) is used in the establishment of TLS/HTTPS, and SSHv2 sessions.
FCS_COP.1/SigGen	The TOE provides cryptographic signature services using the following: • RSA Digital Signature Algorithm with key size of 2048 and greater as specified in FIPS PUB 186-4, "Digital Signature Standard". • Elliptic Curve Digital Signature Algorithm and cryptographic key sizes 256 bits, 384 bits, 521 bits. Through the implementation of the FIPS validated cryptographic module, the TOE provides cryptographic signatures in support of SSHv2 for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands. For SSHv2, RSA and ECDSA host keys are supported.
FCS_RBG_EXT.1	The TOE implements an HMAC_DRBG (as defined in section 10.1.2 of NIST SP 800-90A (6), using HMAC w/SHA-256) from CiscoSSL's FIPS Object Module (FOM) to generate its cryptographic keys. The TOE uses CPU Jitter Entropy (JENT), a platform-based entropy source, to provide entropy to seed its DRBGs. JENT is based on the assumption that a small set of instructions (written in C), when executed repeatedly, will take a slightly different amount of time to execute each time. The time variance is due to a multitude of factors, including: • *CPU instruction pipelines* • *The fact that the CPU clock cycle is different than the memory bus clock speed* • *CPU frequency scaling (which alters the instructions' processing speed)*

TOE SFRs	How the SFR is Met
	• *CPU power management, which may disable certain CPU features* • *Instruction and data caches with their varying information* • *CPU topology and caches used jointly by multiple CPUs* • *Branch prediction units* • *TLB caches* • *Processes being moved from one CPU to another by the scheduler* • *HW interrupts* • *Memory segments whose access times vary due to their physical distance from the CPU* The boundary of the entropy source is the entire TOE platform. An adversary on the outside is not able to affect the entropy rate in any determinable way, because of the number of sources, and the fact that the only one of the sources (allocated packet buffer) is populated with data that came from outside of the system.
FCS_SSH_EXT.1	The TOE implements SSHv2 (telnet is disabled in the evaluated configuration). SSHv2 is implemented according to the following RFCs: 4251, 4252, 4253, 4254, 4344, 5656, 6668, 8308, and 8332. The TOE supports both public key-based and password-based authentication. The TOE derives cryptographic session keys via shared secret using SSH KDF as defined in RFC 4253 (Section 7.2) and RFC 5656 (Section 4). Public keys are mapped to user accounts using the "*username* **sshkey** *ssh-key*" command. This associates the public key with a specific user, allowing the TOE to verify that the user's presented public key matches the stored key data. If the username or key is incorrect, the TOE will deny the session. Remote CLI SSHv2 sessions are limited to an administrator configurable session timeout period and used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data. After either of the thresholds are reached a rekey needs to be performed.

TOE SFRs	How the SFR is Met
	SSHv2 connections will be dropped if the TOE receives a packet larger than 262,126 bytes. Large packets are detected by the SSH implementation and dropped internal to the SSH process. The key exchange methods used by the TOE is a configurable option but rsa-sha2-256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, and ecdh-sha2-nistp521 are the only allowed methods within the evaluated configuration. Any session where the SSH client offers only non-compliant algorithms or key sizes per the [PKG_SSH] will be rejected by the SSH server. SSH sessions can only be established when compliant algorithms and key sizes can be negotiated. The TOE implementation of SSHv2 supports the following: • public key algorithms for authentication as described in RFC 4252 • password-based authentication for administrative users accessing the TOE's CLI through SSHv2. • encryption algorithms aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, and aes256-gcm@openssh.com to ensure confidentiality of the session. • hashing algorithms hmac-sha2-256 and hmac-sha2-512 to ensure the integrity of the session. • SSH transport implementation public key algorithms: rsa-sha2-256, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521.
FCS_SSHS_EXT.1	The TOE's implementation of an SSH server supports the following to authenticate itself to its peer (SSH client): • SSH transport implementation public key algorithms: rsa-sha2-256, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, and ecdsa-sha2-nistp521.

TOE SFRs	How the SFR is Met
FCS_TLSC_EXT.1	The supported ciphersuites including the following: • TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492, • TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 • TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289 • TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

TOE SFRs	How the SFR is Met
	• TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289 The ciphersuites above are configured by default on the TOE. The TOE does not allow for TLS ciphersuites or algorithms to be configured manually. The following NIST curves are supported by default on the TOE: secp256r1, secp384r1, and secp521r1. No administrator configuration is required in order to use these curves. The signature_algorithms extension is supported by default on the TOE. It is presented with the following algorithms: • rsa_pkcs1 with sha256(0x0401), • rsa_pkcs1with sha384(0x0501), • rsa_pkcs1 with sha512(0x0601), • ecdsa_secp256r1 with sha256(0x0403), • ecdsa_secp384r1 with sha384(0x0503), • ecdsa_secp521r1 with sha512(0x0603), • rsa_pss_rsae with sha256(0x0804), • rsa_pss_rsae with sha384(0x0805), • rsa_pss_rsae with sha512(0x0806), • rsa_pss_pss with sha256(0x0809), • rsa_pss_pss with sha384(0x080a), • rsa_pss_pss with sha512(0x080b) No administrator configuration is required. When establishing a TLS connection, the TOE supports reference identifiers of type DNS-ID and IP address and will seek a match to the DNS domain name or IP address respectively in the subjectAltName extension. If the TOE determines there is a mismatch in the presented identifier, it

TOE SFRs	How the SFR is Met
	will not establish the TLS trusted channel connection. The TOE supports the use of wildcards within certificates. The TOE does not support certificate pinning. Trusted CA certificates that are uploaded to the TOE must include the basicConstraints extension with the CA flag set to True to be validated by the TOE. Server certificates must include the 'Server Auth' purpose to be validated by the TOE. The OCSP Responder must include the 'OCSP Signing' purpose. The TOE performs the following steps when verifying peer certificates: • Verifies that the peer certificate is issued by one of the locally trusted CAs. • Verifies that the peer certificate is valid (not expired) with respect to current time. • Verifies that the peer certificate is not yet revoked by the issuing CA. OCSP is used for certificate revocation checking by the TOE to confirm validity on the entire certificate chain. This occurs both during the initial upload of trusted CA certificates and during the Server Hello for new connections. The TOE uses TLS for outbound syslog connections. Any session where the server offers the following in the server hello: SSL 2.0, SSL 3.0, TLS 1.0 and TLS 1.1 will be rejected by the TOE.
FIA_AFL.1	The TOE enforces a timed lockout after an Administrator defined number of unsuccessful password attempts is exceeded. TOE supports setting the limit to any number in the range from 1-65535 failed login attempts within an admin-defined time period of 1-65535 seconds, and to lock the account for an admin-defined number of period of 1-65535 seconds.

TOE SFRs	How the SFR is Met
	For example, an authorized Administrator can be blocked from a range of 1 to 65535 seconds when 3 login attempts fail within a period of 60 seconds. Additionally, a locked account can be unlocked by another authorized Administrator using the command: `clear aaa local user blocked {username username | all}`
FIA_PMG_EXT.1	The TOE supports the configuration of passwords to be composed of any combination of upper- and lower-case letters, numbers, and special characters that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, and no other characters . Minimum password length is settable by the Authorized Administrator and can be configured for minimum password lengths of 8 characters. The password length can be configured between 8 and 127 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. 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 connection, the TOE prompts the user for a username and password. SSHv2 connections also allow for public key authentication. 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. Authentication may be provided by: Authentication against a local database.

TOE SFRs	How the SFR is Met
FIA_UAU.7	When a user enters their password at the local console or via SSH, the TOE does not echo any of the characters of the password or any representation of the characters.
FIA_X509_EXT.1 FIA_X509_EXT.2	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. The certificate validation checking takes place during the TLS session setup. The TOE uses trustpoints to map an identity certificate to a CA or CA chain for authentication purposes to an external syslog server. The TOE supports the following methods to obtain a certificate from a CA: • Manual cut-and-paste - ESA displays the Certificate Request Message via the GUI or CLI interface. This allows the administrator to copy the certificate request and in a secure offline manner send the request to a Certification Authority to be transformed into an X.509v3 public-key certificate. • Both the certificate request message and the certificates themselves provide protection in that they are digitally signed. If a certificate is modified in any way, it would be invalidated. The digital signature verifications process would show that the certificate had been tampered with when the hash value would be invalid. • The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate is reached. • The authorized administrator can also configure one or more certificate fields together with their matching criteria to match.

TOE SFRs	How the SFR is Met
	Such as: • alt-subject-name • issuer-name • name • serial-number • subject-name The physical security of the TOE (A.PHYSICAL_PROTECTION) protects the switch and the certificates from being tampered with or deleted. In addition, the TOE identification and authentication security functions protect an unauthorized user from gaining access to the TOE. OCSP is used for certificate revocation. The TOE will act accordingly based on the Authority Info Access extension in the CA or Peer certificate. Revocation checking is performed on the leaf and intermediate certificate(s) when authenticating a certificate chain provided by the remote peer. There are no functional differences if a full certificate chain or only a leaf certificate is presented. Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The imported CA must contain the keyCertSign key usage to be considered a valid CA. The local certificate that was imported must contain the basic constraints extension with the CA flag set to false. The check also ensure that the key usage extension is present, and the keyEncipherment bit (signifies that the public key is used for encrypting private or secret keys), the digitalSignature bit (indicates that the public key is used for verifying digital signatures) or the keyAgreement bit (indicates that the public key is used in a key agreement protocol such as Diffie-Hellman) or all are set. If they are not, the certificate is not accepted. If the connection to determine the certificate validity cannot be established, the certificate is not accepted.

TOE SFRs	How the SFR is Met
FMT_MOF.1/ManualUpdate FMT_MOF.1/Services FMT_MTD.1/CoreData FMT_MTD.1/CryptoKeys	Manual software updates can only be performed by the Authorized Administrator through the CLI. These updates include software upgrades. Cisco NX-OS devices use role-based access control (RBAC). The Nexus 9000 Series switch supports the following predefined roles: network-admin – This role is a super administrative role. This role has read and write privileges for any configuration item on the TOE. network-operator - This role has read access to the entire TOE. The TOE provides the ability for Authorized Administrators to access TOE data, such as audit data, configuration data, security attributes, session thresholds, cryptographic keys and updates. Each of the predefined and administratively configured privilege roles has either read or write access to the TOE data. This access takes the form of management activity that will create keys, import keys, configuring the use of keys and destroy (zeroize) keys. The keys that can be managed are associated with a CSR (see FIA_X509_EXT.1/Rev in this table), x509v3 certificates, and SSH public keys. The Authorized Administrators can query the software version running on the TOE and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates. In addition, the warning and access banner may also be displayed prior to the identification and authentication of an Authorized Administrator. No administrative functionality is available prior to administrative login.
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The Authorized Administrators user can connect to the TOE using

TOE SFRs	How the SFR is Met
	the CLI to perform these functions via SSHv2 secured connection, a terminal server, or at the local console. The specific management capabilities available from the TOE include: • Ability to administer the TOE locally and remotely; • Ability to configure the access banner; • Ability to configure the remote session inactivity time before session termination or locking; • Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates; • Ability to start and stop services; • Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size); • Ability to modify the behaviour of the transmission of audit data to an external IT entity; • Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1; • Ability to manage the cryptographic keys; • Ability to configure thresholds for SSH rekeying; • Ability to re-enable an Administrator account; • Ability to set the time which is used for time-stamps; • Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors; • Ability to administer the TOE locally; • Ability to configure the local session inactivity time before session termination or locking; • Ability to configure the authentication failure parameters for FIA_AFL.1; • Ability to manage the trusted public keys database;

TOE SFRs	How the SFR is Met
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. The TOE supports both local administration via a directly connected console and remote authentication via SSH.
FPT_APW_EXT.1	The TOE prevents reading of cryptographic passwords. AES password encryption can be configured by an Authorized Administrator to encrypt stored passwords using the "feature password encryption aes" command. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators.
FPT_SKP_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 encrypted form using AES encryption to additionally obscure access. This functionality is configured on the TOE using the `‘feature password encryption aes’` command. The TOE is configured to not display configured keys as part of configuration files using the `‘hidekeys’` command.
FPT_STM_EXT.1	The Nexus 9000 Series switch can provide hardware-based timestamp that are used to provide that timestamp in audit records. The TOE provides the use the of internally generated time stamps. The date and time are used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the TOE.

TOE SFRs	How the SFR is Met
	The clock function is reliant on the system clock provided by the underlying hardware.
FPT_TST_EXT.1	The TOE runs a suite of self-tests during initial start-up to verify its correct operation. Refer to the FIPS Security Policy for available options and management of the cryptographic self-test. For testing of the TSF, the TOE automatically runs checks and tests at startup and during resets to ensure the TOE is operating correctly. Refer to the Guidance documentation for installation configuration settings and information and troubling shooting if issues are identified. When the system is booted up in FIPS mode, the FIPS power-up self-tests run on the supervisor and line card modules. If any of these FIPS self-tests fail, the whole system is moved to the FIPS error state. In this state, as per the FIPS requirement, all cryptographic keys are deleted, and all line cards are shut down. This mode is exclusively meant for debugging purposes. Once the switch is in the FIPS error state, any reload of a line card moves it to the failure state. To move the switch back to FIPS mode, it has to be rebooted. However, once the switch is in FIPS mode, any power-up self-test failure on a subsequent line card reload or insertion affects only that line card, and only the corresponding line card is moved to the failure state. If any of the self-tests fail, the TOE transitions into an error state. In the error state, all secure data transmission is halted and the TOE outputs status information indicating the failure. The following cryptographically self-tests tests are run: • AES Known Answer Test • HMAC Known Answer Test • RNG/DRBG Known Answer Test

TOE SFRs	How the SFR is Met
	• SHA-1/SHA-256/SHA-384/SHA-512 Known Answer Test • RSA Signature Known Answer Test (both signature/verification) • Software Integrity Test
FPT_TUD_EXT.1	An Authorized Administrator can query the software version running on the TOE and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from the 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 can be verified during the boot process, and an image that fails an integrity check will not be loaded. The digital certificates used by the update verification mechanism are contained on the TOE. Detailed instructions for how to do this verification are provided in the administrator guidance for this evaluation.
FTA_SSL_EXT.1 FTA_SSL.3	An Authorized 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. These settings are not immediately activated for the current session. The current line console session must be exited. When the user logs back in, the inactivity timer will be activated for the new session. If a local user session is inactive for a configured period of time, the session will be terminated. The local user will need to re-authentication to start 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 0 to 525600 minutes, although a value of 0 should not be used to ensure an inactivity timeout is enforced. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the “exec-timeout” setting.

TOE SFRs	How the SFR is Met
FTA_SSL.4	An Authorized Administrator is able to exit out of both local and remote administrative sessions by using the “exit” command.
FTA_TAB.1	The TOE displays a customizable login banner on the local and remote CLI management interface prior to allowing any administrative access to the TOE.
FTP_ITC.1	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	All remote administrative communications take place over a secure encrypted SSH session. The SSH session is encrypted using AES encryption. A remote Authorized Administrator is able to initiate SSH communications with the TOE.

7.2 Key Zeroization

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

Table 20: TOE Key Zeroization

Name	Description	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 over writes the	Zeroized using the following command:

Name	Description	Zeroization
	entire object (no matter its contents) using memset. This overwrites the key with all 0's.	# crypto key zeroize rsa Overwritten with: 0x00
SSH Session Key	The results zeroized using the free operation with the poisoning mechanism to overwrite the values with 0x00. This is called by the ssh_close function when a session is ended.	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
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 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
User Password	This is a variable 15+ character password that is used to authenticate local users. The password is stored in NVRAM.	Zeroized by overwriting with new password
TLS server private key	This key is used for authentication, so the server can prove who it is. The private key used for SSLv3.1/TLS secure connections. The key is stored in NVRAM.	CLI command zeroize RSA

Name	Description	Zeroization
		Command: crypto key zeroise verify with command: show crypto key mypubkey all
TLS server public key	This key is used to encrypt the data that is used to compute the secret key. The public key used for SSLv3.1/TLS secure connection. The key is stored in NVRAM.	CLI command zeroize RSA Command: crypto key zeroise verify with command: show crypto key mypubkey all
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 to provide the privacy and TLS data integrity protection. The key is stored in SDRAM (volatile).	Automatically after TLS session terminated. The entire object is overwritten with zeros

8 ANNEX A: REFERENCES

The following documentation was used to prepare this ST:

Table 21: References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, Version 3.1, Revision 5
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, Version 3.1, Revision 5
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, Version 3.1, Revision 5
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated April 2017, Version 3.1, Revision 5
[NDcPP]	collaborative Protection Profile for Network Devices, Version 3.0e, 06 December 2023
[PKG_SSH]	Functional Package for Secure Shell (SSH), Version 1.0, 13 May 2021
[800-56A]	NIST Special Publication 800-56A Rev 2, May 2013
[800-56B]	NIST Special Publication 800-56B Recommendation for Pair-Wise, August 2009
[FIPS 140-3]	FIPS PUB 140-3 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules March 22, 2019
[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
[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