Cisco Network Convergence System 1000 Series

Security Target

Version: 2.0
Date: August 13 2020

Table of Contents

Table of Tables

Table of Figures

Document Introduction

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

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Cisco Network Convergence System 1000 Series (NCS1000). This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, and the IT security functions provided by the TOE which meet the set of requirements. Administrators of the TOE will be referred to as administrators, Authorized Administrators, TOE administrators, semi-privileged, privileged administrators, and security administrators in this document.

1. Security Target Introduction

This Security Target contains the following sections:

- Security Target Introduction
- Conformance Claims
- Security Problem Definition
- Security Objectives
- Security Requirements
- TOE Summary Specification
- References

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

1.1 ST and TOE Reference

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

Table 1. ST and TOE Identification

Name	Description
ST Title	Cisco Network Convergence System 1000 Series (NCS1000) Security Target
ST Version	2.0
Publication Date	August 13 2020
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Network Convergence System 1000 Series
TOE Hardware Models	NCS 1001 and NCS 1004
TOE Software Version	IOS-XR 7.2
Keywords	Routers, Data Protection, Authentication

1.2 TOE Overview

The Cisco Network Convergence System 1000 Series (herein after referred to as the NCS 1000) TOE is a purpose-built, routing platform that's primarily used for interconnecting data centers for mass scale. The TOE includes the hardware models as defined in Table 3 – Hardware Models and Descriptions.

1.3 TOE Product Type

The TOE is a network device as defined in NDcPP v2.1.

The NCS 1000 optimizes Data Center Interconnect and is designed to scale with flexibility and automated operations. The NCS 1000 also scales efficiently and flexibly through its fully programmable, high-bandwidth capacity.

The NCS1000 router runs IOS-XR that is a distributed micro kernel-based network operating system. IOS-XR can process data as it comes into the router without buffering delays. The microkernel is responsible for specific functions such as memory management, interrupt handling, scheduling, task switching, synchronization, and inter-process communication. The microkernel's functions do not include other system services such as device drivers, file system, and network stacks; those services are implemented as independent processes outside the kernel, and they can be restarted like any other application.

1.3.1 Required non-TOE Hardware/Software/Firmware

The TOE requires the following hardware/software/firmware in the IT environment when the TOE is configured in its evaluated configuration

Table 2. IT Environment Component

Component	Required	Usage/Purpose Description for TOE performance
Management Workstation with SSH Client	Yes	This includes any Operational Environment Management workstation with an 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.
Certificate Authority	Yes	This includes any Operational Environment Certificate Authority on the TOE network. This can be used to provide the TOE with a valid certificate during certificate enrollment.
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.
Syslog Server	Yes	This includes any syslog server to which the TOE would transmit syslog messages.

1.4 TOE Description

The Target of Evaluation (TOE) is the Cisco Network Convergence System 1000 Series (NCS100). The TOE is comprised of both software and hardware. The hardware is comprised of the following: NCS1001 and NCS1004. The software is comprised of the Universal Cisco Internet Operating System (IOS-XR) software image Releasese IOS-XR 7.2.

NCS1001

The Cisco NCS 1001 is a dense wavelength-division multiplexing (DWDM) line system that is mechanically optimized for data center environments; is performance optimized for maximum capacity; and provides complete automation of installation and configuration with real-time and fine-grained monitoring.

The Cisco NCS 1001 is a one Rack Unit (1RU) system that can support up to three pluggable modules. The modules can be amplifiers or protection switch modules. A 96-channel unprotected point-to-point or a protected point-to- DWDM line system can be implemented with one NCS 1001.

NCS1004

The NCS1004 chassis is a 2RU chassis and is the component of the TOE in which all other TOE components are housed. The NCS 1004 chassis provides four-line card slots. Each slot can host a 1.2Tbps coherent DWDM line card with 12 Quad Small Form-Factor Pluggable (QSFP)-28 based clients and 2 DWDM trunk ports. Each line card can provide up to 12 100Gbe/OTU4 or 3 400GE client ports.

The system supports up to 4.8Tbps of client and 4.8Tbps of trunk traffic. The NCS 1004 has two redundant and field replaceable AC & DC power supply units and three redundant and field replaceable fans. It also provides a field replaceable controller card and Solid-State Drive (SSD) disks both on-board the chassis and on the controller card for resiliency.

For connections to the Syslog audit server, the TOE authenticates those devices with X.509v3 certificates and protects communication channels with the TLS protocol. Secure remote administration is protected with SSH which is implemented with authentication failure handling.

1.5 TOE Evaluated Configuration

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

An external syslog server must be used to store audit records. For remote administration, a secure session using SSHv2 must be established.

Figure 1. TOE and Environment
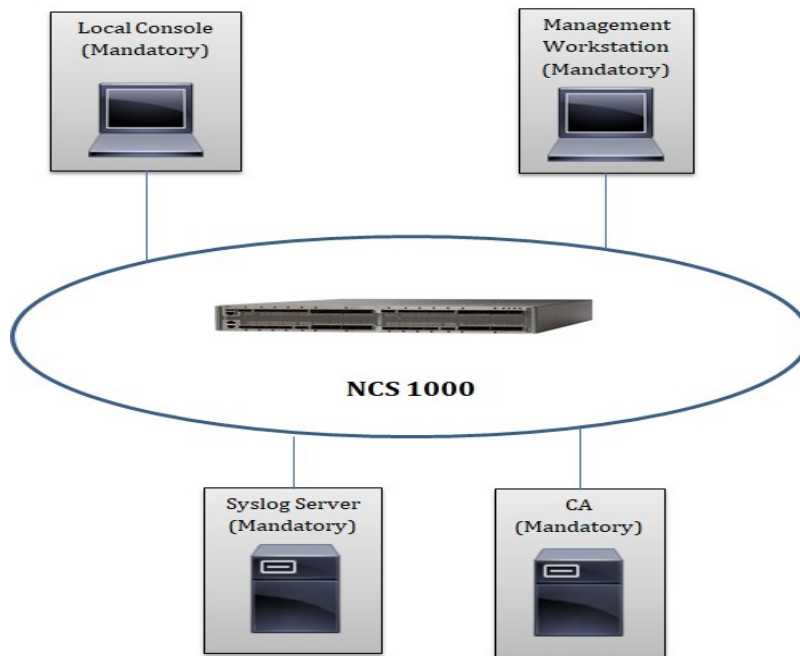
= TOE Boundary

1.6 Physical Scope of the TOE

The TOE is a hardware and software solution that makes up the router models as follows: NCS1001 and NCS1004. The network, on which they reside, is considered part of the IT environment. The TOE guidance documentation that is considered to be part of the TOE can be found listed in the Cisco NCS1000 Common Criteria Operational User Guidance and Preparative Procedures document and are downloadable from the http://cisco.com web site. The TOE is comprised of the following physical specifications as described in Table 3 – Hardware Models and Descriptions below.

Table 3. Hardware Models and Description

Hardware Platform	Processor	Software	Size	Power	Interfaces
NCS 1001	Intel Atom C2516 (Silvermont)	IOS-XR 7.2	1RU 1.73 in. x 17.5 in. x 23.6 in. (4.4 cm x 44.45 cm x 59.94 cm)	1+1 FRU AC or DC Protection Configuration: 250 W (typical), 300 W (max) Unprotected Configuration: 200 W (typical), 250 W (max)	Front • 3 UDC (user data channel) ports • 4 USB ports • 1 10/100/1000 (management) • 1 RS232 console port Rear • Control card and Solid-State Drive Disk • 2 600W AC/DC or DC/DC redundant power supply
NCS 1004	Intel Atom C3758 (Goldmont)	IOS-XR 7.2	2RU 3.5 in. x 17.5 in. x 19 in. (8.9 cm x 44.45 cm x 48.26 cm)	1+1 FRU AC or DC <30W per 100G 1300 W (typical) 1400 W (max)	two slots for 2.1kW AC redundant Power Supply Units (PSU) three redundant and field replaceable fans

1.7 Logical Scope of the TOE

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

■ Security Audit

■ Cryptographic Support

■ Identification and Authentication

■ Security Management

■ Protection of the TSF

■ TOE Access

■ Trusted Path/Channels

These features are described in more detail in the subsections below.   In addition, the TOE implements all RFCs of the NDcPP v2.1 as necessary to satisfy testing/assurance measures prescribed there.

1.7.1 Security Audit

Auditing allows Security Administrators to discover intentional and unintentional issues with the TOE's configuration and/or operation. Auditing of administrative activities provides information that may be used to hasten corrective action should the system be configured incorrectly. Security audit data can also provide an indication of failure of critical portions of the TOE (e.g. a communication channel failure or anomalous activity (e.g. establishment of an administrative session at a suspicious time, repeated failures to establish sessions or authenticate to the TOE)) of a suspicious nature.

The TOE provides extensive auditing capabilities. 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 TOE provides circular audit trail. Audit logs are transmitted to an external audit server over a trusted channel protected with TLS.

1.7.2 Cryptographic Support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operational Environment –Intel Atom). The TOE leverages the Cisco FIPS Object Module 6.0 which resides in the IOS-XR software.

The table below lists the CAVP certificates for the TOE.

Table 4. CAVP Certificates

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
AES	Used for symmetric encryption/decryption	CBC, CTR, GCM (128,192, 256)	C910	FOM 6.0	FCS_COP.1/DataEncryption
SHS (SHA-1, SHA-256 and SHA-512)	Cryptographic hashing services	Byte Oriented	C910	FOM 6.0	FCS_COP.1/Hash
HMAC (HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-512)	Keyed hashing services and software integrity test	Byte Oriented	C910	FOM 6.0	FCS_COP.1/KeyedHash
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	C910	FOM 6.0	FCS_RBG_EXT
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation PKCS #1 v1.5 2048 bit key	C910	FOM 6.0	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/SigGen

The TOE provides cryptography in support of remote administrative management via SSHv2 and secures the session between the NCS1000 and remote syslog server using TLS. The cryptographic services provided by the TOE are described in Table 5 below.

Table 5. TOE Provided Cryptography

Cryptographic Method	Use within the TOE
Secure Shell Establishment	Used to establish initial SSH session.
RSA Signature Services	Used in SSH session establishment.

HMAC	Used for keyed hash, integrity services in SSH session establishment.
AES CBC, CTR, GCM (128, 256)	Used to encrypt SSH session traffic.
SHA-1	Used to provide SSH traffic integrity verification
TLS	Used to secure traffic to the syslog server

1.7.3 Identification and Authentication

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

After a configurable number of incorrect login attempts, the NCS1000 will lockout the account until a configured amount of time for lockout expires.

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

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

1.7.4 Security Management

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

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

1.7.5 Protection of the TSF

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

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

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

1.7.6 TOE Access

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

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

1.7.7 Trusted Path/Channels

The TOE establishes a trusted path between the appliance and the CLI using SSHv2 and the syslog server using TLS.

1.8 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 v2.1.

Table 6. Excluded Functionality and Rationale

Function Excluded	Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.

2. Conformance Claims

2.1 Common Criteria Conformance Claim

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

2.2 Protection Profile Conformance Claim

The TOE and ST are conformant with the following Protection Profiles   This ST applies the NIAP Technical Decisions as described in Table 19:

Table 7. Protection Profile Conformance

Protection Profile	Version	Date
collaborative Protection Profile for Network Devices [NDcPP]	2.1	March 11, 2019

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The ST claims exact conformance to the collaborative Protection Profile for Network Devices (NDcPP), Version 2.1. The ST does not include any additions to the functionality described in the NDcPPv2.1.

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the collaborative Protection Profile for Network Devices, Version 2.1 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 collaborative Protection Profile for Network Devices, Version 2.1 for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the collaborative Protection Profile for Network Devices, Version 2.1 for which conformance is claimed verbatim. All concepts covered the Protection Profile's Statement of Security Requirements are included in the Security Target. Additionally, the Security Assurance Requirements included in the Security Target are identical to the Security Assurance Requirements included in the claimed Protection Profiles.

3. Security Problem Definition

This section identifies the following:

- Assumptions about the TOE's operational environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

- Threats addressed by the TOE and the IT Environment.

- Organizational Security Policies imposed by an organization on the TOE to address its security needs.

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

The security problem definition below has been drawn verbatim from [NDcPPv2.1].

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 8. TOE Assumptions

Assumption	Assumption Definition
A.PHYSICAL_PROTECTION	The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/ services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g, firewall).

Assumption	Assumption Definition
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

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 9. Threats

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

Threat	Threat Definition
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g., shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the network device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the administrator would have no knowledge that the device has been compromised.
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 include replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.

Threat	Threat Definition
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

3.3 Organizational Security Policies

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

Table 10. Organizational Security Policies

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

4. Security Objectives

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

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 v2.1 does not define any security objectives for the TOE.

4.2 Security Objectives for the Environment

The following table identifies the Security Objectives for the Environment. These security objectives reflect the stated intent to counter identified threats and/or comply with any security policies. The security objectives below have been drawn verbatim from [NDcPPv2.1].

Table 11. 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	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are assumed to monitor the revocation status of all certificates in the TOE's trust store and to remove any certificate from the TOE's trust store in case such certificate can no longer be trusted.
OE.UPDATES	The TOE firmware and software is updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
OE.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the TOE must be protected on any other platform on which they reside.
OE.RESIDUAL_INFORMATION	The Security Administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

5. Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements in this section are drawn from [CC_PART2], [NDcPPv2.1] and NIAP Technical Decisions.

5.1 Conventions

[CC_PART1] defines operations on Security Functional Requirements. This document uses the following conventions to identify the operations permitted by [NDcPPv2.1] and NIAP Technical Decisions.

Table 12. Security Requirement Conventions

Convention	Indication
Assignment	Indicated with *italicized* text
Refinement	Indicated with **bold** text and ~~strikethroughs~~
Selection	Indicated with <u>underlined</u> text
Assignment within a Selection	Indicated with *<u>italicized and underlined</u>* text
Iteration	indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash")

Where operations were completed in the [NDcPPv2.1] itself, the formatting used in the [NDcPPv2.1] has been retained.

5.2 TOE Security Functional Requirements

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

Table 13. 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
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM.4	Cryptographic Key Destruction
	FCS_COP.1/DataEncryption	Cryptographic Operation (AES Data Encryption/Decryption)
	FCS_COP.1/SigGen	Cryptographic Operation (Signature Generation and Verification)
	FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)

Class Name	Component Identification	Component Name
	FCS_RBG_EXT.1	Random Bit Generation
	FCS_SSHS_EXT.1	SSH Server Protocol
	FCS_TLSC_EXT.1	TLS Client Protocol
FIA: Identification and authentication	FIA_PMG_EXT.1	Password Management
	FIA_AFL.1	Authentication Failure Handling
	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
	FIA_X509_EXT.3	X.509 Certificate Requests
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: Protection of the TSF	FPT_SKP_EXT.1	Extended: Protection of TSF Data (for reading of all symmetric keys)
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_TUD_EXT.1	Trusted update
	FPT_TST_EXT.1	TSF Testing (Extended)
	FPT_STM_EXT.1	Reliable Time Stamps
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1/Admin	Trusted Path

5.3 SFRs drawn from the NDcPPv2.1

5.3.1 Class: Security Audit (FAU)

5.3.1.1 FAU_GEN.1 – Audit Data Generation

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

a) Start-up and shutdown of the audit functions;

b) All auditable events for the <u>not specified</u> level of audit; and

c) *All administrator actions comprising:*

- *Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).*

- *Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).*

- *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).*

- *Resetting passwords (name of related user account shall be logged).*

- *[<u>no other actions</u>];*

d) *Specifically defined auditable events listed in Table 14.*

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

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, *information specified in column three of Table 14*.

Table 14. Auditable Events

SFR	Auditable Event	Additional Audit Record Contents
FAU_GEN.1	None.	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM.2	None.	None.
FCS_CKM.4	None.	None.
FCS_COP.1/DataEncryption	None.	None.
FCS_COP.1/SigGen	None.	None.
FCS_COP.1/Hash	None.	None.
FCS_COP.1/KeyedHash	None.	None.

SFR	Auditable Event	Additional Audit Record Contents
FCS_RBG_EXT.1	None.	None.
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure.
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_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement or removal of trust anchors in the TOE's trust store.	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store.
FIA_X509_EXT.2	None.	None.
FIA_X509_EXT.3	None.	None.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None	None.
FMT_SMF.1	All management activities of TSF data.	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_TST_EXT.1	None.	None.
FPT_TUD_EXT.1	Initiation of update. result of the update attempt (success or failure)	None.
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process.	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
FTA_SSL_EXT.1	The termination of a local session by the session locking mechanism.	None.
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.
FTA_SSL.4	The termination of an interactive session.	None.

SFR	Auditable Event	Additional Audit Record Contents
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	None.

Application Note
NIAP TD0410 has been applied to FAU_GEN.1, though it does not change the text of this SFR.
NIAP TD0480 has been applied to FAU_GEN.1, though it impacts only the Supporting Document (SD), not the text of the SFR.

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.

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

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

5.3.2 Class: 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;

- FFC Schemes using Diffie-Hellman group 14 that meet the following: RFC 3526, Section 3

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

Application Note
NIAP TD0400 has been applied to FCS_CKM.1.

5.3.2.2 FCS_CKM.2– Cryptographic Key Establishment (Refinement)

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

- RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1

- Key establishment scheme using Diffie-Hellman group 14 that meets the following: RFC 3526, Section 3;

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

Application Note
NIAP TD0400 has been applied to FCS_CKM.2.
NIAP TD0402 has been applied to FCS_CKM.2.
NIAP TD0482 has been applied to FCS_CKM.2 though it impacts only the TSS guidance, not the text of the SFR

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*]*

Application Note
NIAP TD0397 has been applied to FCS_COP.1/DataEncrytpion, though it impacts only the tests, not the text of the SFR.

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

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

[

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

]

that meet the following:

[

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

]

5.3.2.6 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-1, SHA-256, SHA-512] ~~and cryptographic key sizes [assignment: cryptographic key sizes]~~ and **message digest sizes** [**160, 256, 512] bits** that meet the following: *ISO/IEC 10118-3:2004.*

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

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

5.3.2.9 FCS_RBG_EXT.1 – Random Bit Generation

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

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

5.3.2.10 FCS_SSHS_EXT.1 – SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs [4251, 4252, 4253, 4254, 4344, 5647, 5656, 6668].

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

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [*1262144*] bytes in an SSH transport connection are dropped.

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

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

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [hmac-sha1, hmac-sha2-256, hmac-sha2-512, implicit] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

FCS_SSHS_EXT.1.7 The TSF shall ensure that [diffie-hellman-group14-sha1] and [no other methods] are the only allowed key exchange methods used for the SSH protocol.

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

Application Note
NIAP TD0398 has been applied to FCS_SSHS_EXT.1.1.
NIAP TD0412 has been applied to FCS_SSHS_EXT.1.5, though it impacts only the tests, not the text of the SFR.
NIAP TD0424 has been applied to FCS_SSHS_EXT.1.5, though it does not impact the text of the SFR.
NIAP TD0447 has been applied to FCS_SSHS_EXT.1.7.
NIAP TD0475 has been applied to FCS_SSHS_EXT.1.8.

5.3.2.11 FCS_TLSC_EXT.1 – TLS Client Protocol

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

[

- TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
- TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
  ].

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier of the following types: [identifiers defined in RFC 6125] are matched to reference identifiers.

FCS_TLSC_EXT.1.3 When establishing a trusted channel, by default the TSF shall not establish a trusted channel if the server certificate is invalid. The TSF shall also [

- Not implement any administrator override mechanism

].

FCS_TLSC_EXT.1.4 The TSF shall [not *present the Supported Elliptic Curves Extension: and no other curves*] in the Client Hello.

Application Note
NIAP TD0396 has been applied to FCS_TLSC_EXT.1.1, though it impacts only the tests, not the text of the SFR.
NIAP TD0481 has been applied to FCS_TLSC_EXT.1.2.

5.3.3 Class: Identification and Authentication (FIA)

5.3.3.1 FIA_AFL_EXT.1 – Authentication Failure Management

FIA_AFL.1.1 The TSF shall detect when an Administrator configurable positive integer within [*2-6*] 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 remote session using any authentication method that involves a password until *an Administrator defined time period has elapsed*].

Application Note
NIAP TD0408 has been applied to FIA_AFL_EXT.1.
NIAP TD0409 has been applied to FIA_AFL_EXT.1

5.3.3.2 FIA_PMG_EXT.1 – Password Management

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

a. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")"];

b. Minimum password length shall be configurable to between [*15*] and [*15*] 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.

5.3.3.4 FIA_UAU_EXT.2 – Password-based Authentication Mechanism

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

Application Note
NIAP TD0408 has been applied to FIA_UAU_EXT.2.

5.3.3.5 FIA_UAU.7 – Protected Authentication Feedback

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

5.3.3.6 FIA_X509_EXT.1/Rev – X.509 Certificate Validation

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

- RFC 5280 certificate validation and certificate path validation **supporting a minimum path length of three certificates.**

- The certificate path must terminate with a trusted CA certificate designated as a trust anchor.

- The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE.

- The TSF shall validate the revocation status of the certificate using [a Certificate Revocation List (CRL) as specified in RFC 5759 Section 5].

- The TSF shall validate the extendedKeyUsage field according to the following rules:

   o *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.*

   o *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.*

   o *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.*

   o *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.

Application Note
NIAP TD0478 has been applied to FIA_X509_EXT.1/Rev.

5.3.3.7 FIA_X509_EXT.2 – X.509 Certificate Authentication

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

Application Note
NIAP TD0399 has been applied to FIA_X509_EXT.2.

5.3.3.8 FIA_X509_EXT.3 – X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [device-specific information].

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

Application Note
NIAP TD0423 has been applied to FIA_X509_EXT.3, , though it does not impact the text of the SFR.

5.3.4 Class: Security Management (FMT)

5.3.4.1 FMT_MOF.1/ManualUpdate – Management of Security Functions Behavior

FIA_MOF.1.1/ManualUpdate The TSF shall restrict the ability to enable the functions *to perform manual updates to Security Administrators.*

5.3.4.2 FMT_MTD.1/CoreData – Management of TSF Data

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

5.3.4.3 FMT_SMF.1 – Specification of Management Functions

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

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

- *Ability to configure the access banner;*

- *Ability to configure the session inactivity time before session termination or locking;*

- *Ability to update the TOE, and to verify the updates using [hash comparison] capability prior to installing those updates;*

- *Ability to configure the authentication failure parameters for FIA_AFL.1;*

     [

     o   *Ability to configure audit behavior;*

     o   *Ability to configure the cryptographic functionality;*

     o   *Ability to configure thresholds for SSH rekeying;*

     o   *Ability to set the time which is used for time-stamps;*

     o   *Ability to configure the reference identifier for the peer;*

     o   *Ability to import X.509v3 certificates to the TOE'S trust store*

     ]

Application Note
NIAP TD0408 has been applied to FMT_SMF.1.

5.3.4.4 FMT_SMR.2 – Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- *Security Administrator.*

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

FMT_SMR.2.3 The TSF shall ensure that the conditions

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

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

     are satisfied.

5.3.5 Class: Protection of the TSF (FPT)

5.3.5.1 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.

5.3.5.2 FPT_APW_EXT.1 – Protection of Administrator Passwords

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

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

Application Note
NIAP TD0483 has been applied to FPT_APW_EXT.1.

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 demonstrate the correct operation of the TSF: [
- *AES Known Answer Test*
- *HMAC Known Answer Test*
- *RNG/DRBG Known Answer Test*
- *SHA-1/256/512 Known Answer Test*
- *RSA Signature Known Answer Test (both signature/verification)*
- *Software Integrity Test*].

5.3.5.5 FPT_TUD_EXT.1 – Trusted Updates

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 [published hash] prior to installing those updates.

Application Note
NIAP TD0477 has been applied to FPT_TUD_EXT.1, though it impacts only the tests, not the text of the SFR

5.3.6 Class: TOE Access (FTA)

5.3.6.1 FTA_SSL_EXT.1 – TSF-initiated Session Locking

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

Application Note
NIAP TD0484 has been applied to FTA_SSL_EXT.1

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*.

Application Note
NIAP TD0425 has been applied to FTA_SSL.3, though it impacts only the AGD, not the test of the SFR.
NIAP TD0484 has been applied to FTA_SSL_EXT.3

5.3.6.3 FTA_SSL.4 – User-initiated Termination

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

5.3.6.4 FTA_TAB.1 – Default TOE Access Banners

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

5.3.7 Class: Trusted Path/Channels (FTP)

5.3.7.1 FTP_ITC.1 – Inter-TSF Trusted Channel

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

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

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

- *Syslog server over TLS.*

Application Note
NIAP TD0401 has been applied to FTP_ITC.1.

5.3.7.2 FTP_TRP.1/Admin – Trusted Path

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

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

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

5.4 TOE SFR Dependencies Rationale

[NDcPPv2.1] contain all the requirements claimed in this Security Target. As such the dependencies are not applicable since the PPs themselves have been approved.

5.5 Security Assurance Requirements

5.5.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the [NDcPPv2.1] which are derived from [CC_PART3]. The assurance requirements are summarized in the table below.

Table 15. Assurance Requirements

Assurance Class	Components Description
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)

Assurance Class	Components Description
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)	Labeling of the TOE (ALC_CMC.1)
	TOE CM coverage (ALC_CMS.1)
Tests (ATE)	Independent testing – sample (ATE_IND.1)
Vulnerability Assessment (AVA)	Vulnerability survey (AVA_VAN.1)

5.5.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the [NDcPPv2.1]. As such, the [NDcPPv2.1] SAR rationale is deemed acceptable since the PPs themselves have been approved.

5.6 Assurance Measures

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

Table 16. Assurance Measures

Assurance Component	Rationale
ADV_FSP.1	No additional "functional specification" documentation was provided by Cisco to satisfy the Evaluation Activities.
AGD_OPE.1 AGD_PRE.1	Cisco will provide the guidance documents with the ST.
ALC_CMC.1 ALC_CMS.1	Cisco will identify the TOE such that it can be distinguished from other products or versions from the Cisco and can be easily specified when being procured by an end user.
ATE_IND.1	Cisco will provide the TOE for testing.
AVA_VAN.1	Cisco will provide the TOE for Vulnerability Analysis.

TOE Summary Specification

6.1 TOE Security Functional Requirement Measures

The table below identifies and describes how the Security Functional Requirements identified above are met by the TOE.

Table 17. How TOE SFRs Measures

TOE SFR	How the SFR is Met
FAU_GEN.1	The TOE generates an audit record whenever an audited event occurs. The types of events that cause audit records to be generated include: startup and shutdown of the audit mechanism cryptography related events, identification and authentication related events, and administrative events (the specific events and the contents of each audit record are listed in the table within the FAU_GEN.1 SFR, "Auditable Events Table"). Each of the events is specified in syslog records in enough detail to identify the user for which the event is associated, when the event occurred, where the event occurred, the outcome of the event, and the type of event that occurred such as generating keys, including the type of key. Additionally, the startup and shutdown of the audit functionality is audited. `Feb 21 15:38:19.075 UTC: syslogd[309]: %OS-SYSLOG-5-LOG_NOTICE : Secure Logging: Successfully established TLS session , server :10.105.227.148` In the above log events a date and timestamp is displayed as well as an event description.

FAU_GEN.2	The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example, a human user, user identity, or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. A sample audit record is below:
	
	 `RP/0/RP0/CPU0:Feb 28 18:20:13.419 UTC: config[69603]: %MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user 'root'. Use 'show configuration commit changes 1000000011' to view the changes`
	
	 `RP/0/RSP0/CPU0:Feb 28 18:20:13.433 UTC: config[69603]: %MGBL-SYS-5-CONFIG_I : Configured from console by admin`

FAU_STG_EXT.1	The TOE is configured to export syslog records to a specified, external syslog server in real time. The TOE protects communications with an external syslog server via TLS. The TOE transmits its audit events to all configured syslog servers at the same time logs are written to the local log buffer and to the console. The TOE is capable of detecting when the TLS connection fails. The TOE also stores a limited set of audit records locally in a circular file on the TOE and continues to do so if the communication with the syslog server goes down. The default value for the size of the logging buffer on the TOE is 2097152 bytes. If the TLS connection fails, the TOE will buffer a small amount of audit records on the TOE when it discovers it can no longer communicate with its configured syslog server and will transmit the buffer contents when connectivity to the syslog server is restored. When the local audit data storage is full, the NCS1K will overwrite the oldest stored audit records when writing new audit records. The local audit records are stored in a directory that does not allow administrators to modify the contents.

TOE SFR	How the SFR is Met
FCS_CKM.1 FCS_CKM.2	The TOE generates asymmetric keys in accordance with the RSA schemes using key sizes of 2048-bit or greater that are conformant to the FIPS PUB 186-4, Appendix B.3. The TOE can create an RSA public-private key pair that can be used to generate a Certificate Signing Request (CSR). Via offline CSR or Simple Certificate Enrollment Protocol (SCEP), the TOE can: send the CSR to a Certificate Authority (CA) for the CA to generate a certificate; and receive its X.509 certificate from the CA. Integrity of the CSR and certificate during transit are assured through use of digital signatures (encrypting the hash of the TOE's public key contained in the CSR and certificate). The TOE can store and distribute the certificate to external entities including Registration Authorities (RA). The IOS-XR Software supports embedded PKI client functions that provide secure mechanisms for distributing, managing, and revoking certificates. The TOE can also use X.509v3 certificates for authentication of TLS sessions. The TOE acts as both a sender and receiver for RSA -based key establishment schemes. The RSA key establishment meets the 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. The TOE implements Diffie-Hellman (DH) group 14 (2048) bit key finite field-based key generation in conformance with RFC 3526 section 3. The TOE acts as both a sender and receiver for Diffie-Helman based key establishment schemes. The DH key generation meets the RFC 3526, Section 3.

Scheme	SFR	Service
RSA	FCS_TLSC_EXT.1 FCS_SSHS_EXT.1	Support for SSH and TLS key establishment Remote Administration for FCS_SSHS_EXT.1
FFC	FCS_SSHS_EXT.1 FCS_TLSC_EXT.1	SSH Remote Administration Syslog Server
FFC	FIA_X509_EXT.1/Rev FIA_X509_EXT.1/ITT FIA_X509_EXT.2 FIA_X509_EXT.3	Transmit generated audit data to an external IT entity

TOE SFR	How the SFR is Met
FCS_CKM.4	The TOE meets all requirements specified in FIPS 140-2 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 See Table 18 for more information on the key zeroization.
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 and ISO 10116 and 19772. AES is implemented in the following protocols: SSH and TLS. Through the implementation of the CAVP 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.

TOE SFR	How the SFR is Met
FCS_COP.1/SigGen	The TOE provides cryptographic signature services using the following: • RSA Digital Signature Algorithm with key size of 2048 as specified in FIPS PUB 186-4, "Digital Signature Standard" Through the implementation of the CAVP validated cryptographic module, the TOE provides cryptographic signatures in support of SSH and TLS for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those com-mands. The TOE provides the RSA option in support of SSH and TLS key establishment. RSA (2048-bit, 3072-bit, and 4096-bit) is used in the establishment of SSHv2 key establishment. For SSH, RSA host keys are supported.
FCS_COP.1/Hash	The TOE provides cryptographic hashing services using SHA-1, SHA-256 and SHA-512 as specified in ISO/IEC 10118-3:2004. Through the implementation of the CAVP validated cryptographic module, the TOE provides Secure Hash Standard (SHS) hashing in support of SSH and TLS 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-1, HMAC-SHA-256, HMAC-SHA-512*, key size 160, 256, 512 bits, and message digest sizes **160, 256, 512** as specified in ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2" Through the implementation of the CAVP validated cryptographic module, the TOE provides SHS hashing and HMAC message authentication in support of SSHv2, TLSv1.1 and TLSv1.2 for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands. SHS hashing and HMAC message authentication (SHA-1) is used in the establishment of TLS and SSHv2 sessions.
FCS_RBG_EXT.1	The TOE implements a NIST-approved AES-CTR Deterministic Random Bit Generator (DRBG), as specified in ISO/IEC 18031:2011 seeded by an entropy source that accumulates entropy from a TSF-hardware based noise source. The deterministic RBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.

TOE SFR	How the SFR is Met
FCS_SSHS_EXT.1	The TOE implements SSHv2 (telnet is disabled by default in the evaluated configuration). SSHv2 is implemented according to the following RFCs: 4251, 4252, 4253, 4254, 4344, 5647, 5656, and 6668. The TOE supports both public key-based and password-based authentication. Remote CLI SSHv2 sessions are limited to an administrator configurable session timeout period and will be rekeyed after no more than 1 gigabyte (binary) of data is transmitted or an hour has passed. Both thresholds are checked by the TOE and a rekeying is performed on whichever threshold is reached first.
	SSHv2 connections will be dropped if the TOE receives a packet larger than *1262144* 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 diffie-hellman-group14-sha1 is the only allowed method within the evaluated configuration. Any session where the SSH client offers only non-compliant algorithms or key sizes per the NDcPP 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: ssh-rsa. • password-based authentication for administrative users accessing the TOE's CLI through SSHv2. • encryption algorithms, *aes128-ctr, aes256-ctr, aes128-gcm@openssh.com, aes256-gcm@openssh.com* to ensure confidentiality of the session. *Note: When aes*-gcm@openssh.com is negotiated as the encryption algorithm, the MAC algorithm field is ignored and GCM is implicitly used as the MAC.* • hashing algorithms hmac-sha1, hmac-sha2-256, hmac-sha2-512 to ensure the integrity of the session. Please refer to Table 4 for all the CAVP references

FCS_TLSC_EXT.1	The TOE supports TLSv1.1 and TLS v1.2 to protect the sessions to the remote audit server.
	TLS is also used to protect the TLS sessions with the TOE, which supports the mandatory ciphersuite as well as the following optional ciphersuite:
	• *TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268* • *TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268* •
	The TOE does not support NIST Curves in the TLS Client Hello.
	The TOE will only establish a connection if the peer presents a valid certificate during the handshake.
	Where the TOE is the client, such as connecting to the remote syslog server, the handshake above is the same process except the server (remote syslog server) would not request the client certificate in the Server Hello, see the following:
	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 (client).
	Using wildcards is not supported in identity certificates.
	Certificate pinning is not supported.
	The TOE requires Subject Alternative Names (SANs) "the reference identifiers" for a successful connection. SANs contain one or more alternate names and uses any variety of name

TOE SFR	How the SFR is Met
	forms for the entity that is bound by the Certificate Authority (CA) to the certified public key. These alternate names are called "Subject Alternative Names" (SANs). Possible names include: • DNS name
FIA_AFL.1	The TOE enforces a timed lockout after an Administrator defined number of unsuccessful password attempts is exceeded. While the TOE supports a range from 2-6, in the evaluated configuration, the maximum number of failed attempts is recommended to be set to 3. Once the remote user is locked out, their account will not be accessible until the configured timer for lockout has been exceeded. Once the lockout time is over, then the administrator user can attempt to login again. At no point is administrator access completely unavailable when remote administrators are locked out due to unsuccessful password attempts. Local console access is always available. Administrator lockouts are not applicable to the local console
FIA_PMG_EXT.1	The TOE supports the local definition of users with corresponding passwords. The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: "@", "#", "$", "%", "^", "&", "*", "(", and ")"). Minimum password length is settable by the Authorized Administrator and can be configured for minimum password lengths of 15 characters.
FIA_UIA_EXT.1 FIA_UAU_EXT.2	The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login warning banner that is displayed prior to user authentication. Administrative access to the TOE is facilitated through the TOE's CLI. The TOE mediates all administrative actions through the CLI. Once a potential administrative user attempts to access the CLI of the TOE through either a directly connected console or remotely through an SSHv2 secured connection, the TOE prompts the user for a username and password. Only after the administrative user presents the correct authentication credentials will access to the TOE administrative functionality be granted. No access is allowed to the administrative functionality of the TOE until an administrator is successfully identified and authenticated. The TOE provides a local password-based authentication mechanism for authentication of authorized administrators. The TOE also provides a password based or SSH public key-based mechanism for remote authentication of authorized administrators. The process for authentication is the same for administrative access whether administration is occurring via a directly connected console or remotely via SSHv2 secured connection. At initial login, the administrative user is prompted to provide a username. After the user provides the username, the user is prompted to provide the administrative password associated with the user account. The TOE then either grant administrative access (if the combination of username and password is correct) or indicate that the login was unsuccessful. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_UAU.7	When a user enters their password at the local console, the TOE displays only '*' characters so that the user password is obscured. For remote session authentication, the TOE does not echo any characters as they are entered. The TOE does not provide a reason for failure in the cases of a login failure.
FIA_X509_EXT.1/Rev FIA_X509_EXT.2	The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. Public key infrastructure (PKI) credentials, such as private keys and certificates are stored securely. The identification and authentication, and authorization security

TOE SFR	How the SFR is Met
FIA_X509_EXT.3	functions protect an unauthorized user from gaining access to the storage . The certificate request message includes the public key and device-specific information per RFC 2986. The device specific information includes • Subject name • Router serial number • IP address The certificate validation checking takes place during the TLS session establishment and at time of import. The TOE conforms to standard RFC 5280 for certificate and path validation (i.e., peer certificate checked for expiration, peer certificate checked if signed by a trusted CA in the trust chain, peer certificate checked for unauthorized modification, peer certificate checked for revocation). The TOE supports Self-signed certificate enrollment for a trust point to obtain a certificate from a CA: The certificate chain establishes a sequence of trusted certificates, from a peer certificate to the root CA certificate. Within the PKI hierarchy, all enrolled peers can validate the certificate of one another if the peers share a trusted root CA certificate or a common subordinate CA. Each CA corresponds to a trust point. When a certificate chain is received from a peer, the default processing of a certificate chain path continues until the first trusted certificate, or trust point, is reached. 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. Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted. Only one certificate is imported since the only device is a syslog server, so the TOE chooses this certificate basicConstraints checking is performed at the time of authentication during the connection attempt. If the connection to determine the certificate validity cannot be established, the certificate is not accepted. The administrators can configure a trust chain by importing the CA certificate(s) that signed and issued the server (syslog) certificate. This will tell the TOE which CA certificate(s) to use during the validation process. If the TOE does not find the trusted root CA, the TLS connection to the syslog server will fail. When the TOE is able to contact the CRL distribution point for certificate revocation checking, the TOE will reject the TLS session if the remote trust point's (e.g. syslog server's) certificate has been revoked.

TOE SFR	How the SFR is Met
FMT_MOF.1/ManualUpdate FMT_MTD.1/CoreData	The TOE provides administrative users with a CLI to interact with and manage the security functions of the TOE. The term "Authorized Administrator" is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned. The TOE provides the ability for Authorized Administrators to access TOE data, such as user accounts and roles, audit data, audit server information, configuration data, security attributes, X509 certificates, login banners, inactivity timeout values, password complexity setting, TOE updates and session thresholds via the CLI. The TOE restricts the access to manage TSF data that can affect security functions of the TOE to the Authorized Administrator/Security Administrator roles. Manual software updates can only be done by the authorized administrator through CLI. These updates include software upgrades. The Security Administrators (a.k.a 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.

TOE SFR	How the SFR is Met
FMT_SMF.1	The TOE provides all the capabilities necessary to securely manage the TOE. The administrative user can connect to the TOE using the CLI to perform these functions via SSHv2, a terminal server, or at the local console. Refer to the Guidance documentation for configuration syntax, commands, and information related to each of these functions. The management functionality provided by the TOE includes the following administrative functions: • *Ability to administer the TOE locally and remotely* • Ability to manage the cryptographic functionality - allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2, and if used the configuration of remote authentication • Ability to manage the audit logs and functions - allows the Authorized Administrator to configure the audit logs, view the audit logs, and to clear the audit logs • Ability to manage the warning banner message and content – allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users • Ability to manage the time limits of session inactivity – allows the Authorized Administrator the ability to set and modify the inactivity time threshold and lockout after surpassing the configured number of incorrect passwords • *Ability to update the TOE, and to verify the updates using [<u>hash comparison</u>] capability prior to installing those updates;* • *Ability to configure the authentication failure parameters for FIA_AFL.1* • <u>*Ability to configure thresholds for SSH rekeying;*</u> • <u>*Ability to set the time which is used for time-stamps;*</u> • <u>*Ability to configure the reference identifier for the peer*</u>; • <u>*Ability to import X.509v3 certificates to the TOE'S trust store*</u>
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_SKP_EXT.1 and FPT_APW_EXT.1	The TOE stores all private keys in a secure directory that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in a hashed format that are non-readable, hence no interface access. All passwords are obscured via hashing in a secure directory. The passwords are non-readable. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators. This is provided by default. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.

TOE SFR	How the SFR is Met
FPT_STM_EXT.1	The TOE provides a source of date and time information used in audit event timestamps and in validating service requests. This function can only be accessed from within the configuration exec mode via the privileged mode of operation of the router. The clock function is reliant on the system clock provided by the underlying hardware. This 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.

TOE SFR	How the SFR is Met
FPT_TST_EXT.1	The TOE is designed to run the suite of power-on self-tests that comply with the FIPS140-2 requirements for self-test (e.g. know answer tests (KATs) and zeroization tests), during initial start-up to verify its correct operation. If any of the tests fail the security administrator will have to log into the CLI to determine which test failed and why. If the tests pass successfully the router will continue bootup and normal operation. During the system bootup process (power on or reboot), all the Power on Startup Test (POST) components for the cryptographic module perform the POST for the corresponding component (hardware or software). These tests include: • AES Known Answer Test - For the encrypt test, a known key is used to encrypt a known plain text value resulting in an encrypted value. This encrypted value is compared to a known encrypted value to ensure that the encrypt operation is working correctly. The decrypt test is just the opposite. In this test a known key is used to decrypt a known encrypted value. The resulting plaintext value is compared to a known plaintext value to ensure that the decrypt operation is working correctly • RSA Signature Known Answer Test (both signature/verification) - This test takes a known plaintext value and Private/Public key pair and used the public key to encrypt the data. This value is compared to a known encrypted value to verify that encrypt operation is working properly. The encrypted data is then decrypted using the private key. This value is compared to the original plaintext value to ensure the decrypt operation is working properly • RNG/DRBG Known Answer Test - For this test, known seed values are provided to the DRBG implementation. The DRBG uses these values to generate random bits. These random bits are compared to known random bits to ensure that the DRBG is operating correctly • HMAC Known Answer Test - For each of the hash values listed, the HMAC implementation is fed known plaintext data and a known key. These values are used to generate a MAC. This MAC is compared to a known MAC to verify that the HMAC and hash operations are operating correctly • SHA-1/256/512 Known Answer Test - For each of the values listed, the SHA implementation is fed known data and key. These values are used to generate a hash. This hash is compared to a known value to verify they match, and the hash operations are operating correctly. • Software Integrity Test - the software integrity test ensures the correct operation of the device and its components If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen and saved in the file called crashinfo. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected.

TOE SFR	How the SFR is Met
FPT_TUD_EXT.1	An Authorized Administrator can query the software version running on the TOE and can initiate updates to 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 cryptographic hashes (i.e., public hashes/SHA-512) are used to verify software/firmware update files (to ensure they have not been modified from the originals distributed by Cisco) before they are used to update the applicable TOE components. The hash value can be displayed by hovering over the software image name under details on the Cisco.com web site. If the hashes do not match, contact Cisco Technical Assistance Center (TAC). To verify the system software release version at the CLI the command "show version" is used, while the command "show install active" command will display the currently running system image filename and the system software release version. Detailed instructions for how to verify the hash value and verify the software version are provided in the administrator guidance for this evaluation.
FTA_SSL_EXT.1 FTA_SSL.3	An administrator can configure maximum inactivity times individually for both local and remote administrative sessions through the use of the "exec-timeout" setting applied to the console and vty for remote sessions. 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 and will require re-authentication to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session.
FTA_SSL.4	An administrator is able to exit out of both local and remote administrative sessions
FTA_TAB.1	The TOE displays a privileged Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE. This interface is applicable for both local (via console) and remote (via SSH) TOE administration
FTP_ITC.1	The TOE protects communications with the external audit server using TLS to secure the communications channel. TLS uses the keyed hash as defined in FCS_COP.1/KeyedHash and cryptographic hashing functions FCS_COP.1/Hash. This protects the data from modification of data by hashing that verify that data has not been modified in transit. In addition, encryption of the data as defined in FCS_COP.1/DataEncryption is provided to ensure the data is not disclosed in transit. .
FTP_TRP.1/Admin	All remote administrative communications take place over a secure encrypted SSHv2 session. The SSHv2 session is encrypted using AES encryption. The remote users are able to initiate SSHv2 communications with the TOE.

7. Annex A: Key Zeroization

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

Table 18. Key Zeroization

Name	Description	Zeroization
Diffie-Hellman Shared Secret	The value is zeroized after it has been given back to the consuming operation. The value is overwritten by 0's. This key is stored in DRAM	Automatically after completion of DH exchange. Overwritten with: 0x00
Diffie Hellman private exponent	The private exponent used in Diffie-Hellman (DH) exchange. Generate by the module. Zeroized after DH shared secret has been generated. . This key is stored in DRAM	Zeroized upon completion of DH exchange. Overwritten with: 0x00
SSH Private Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents) using memset. This overwrites the key with all 0's. when the command "crypto key zeroize rsa" is issued it will delete all RSA keys. This key is stored in NVRAM	Zeroized using the following command: # crypto key zeroize rsa Overwritten with: 0x00
SSH Session Key	Once the function has completed the operations requiring the RSA key object, the module over writes the entire object (no matter its contents). . This is called by the ssh_close function when a session is ended. This key is stored in DRAM.	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.	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.	Zeroized by overwriting with new password
RNG Seed	This seed is for the RNG. The seed is stored in DRAM.	Zeroized upon power cycle the device
RNG Seed Key	This is the seed key for the RNG. The seed key is stored in DRAM.	Zeroized upon power cycle the device
AES Key	The results are zeroized by overwriting the values with 0x00. This is called by the ssh_close function when a session is ended. This key is stored in DRAM	Automatically when the SSH/TLS session is terminated. Overwritten with: 0x00
TLS server private key	This key is used for authentication, so the server can prove who it is. The private key used for SSLv3.1/TLS secure connections. The key is stored in NVRAM.	Zeroized by overwriting with new key
TLS server public key	This key is used to encrypt the data that is used to compute the secret key. The public key used for SSLv3.1/TLS secure connection. The key is stored in NVRAM.	Zeroized by overwriting with new key

Name	Description	Zeroization
TLS pre-master secret	The pre-master secret is the client and server exchange of random numbers and a special number, the pre-master secret, This pre-master secret is using asymmetric cryptography from which new TLS session keys can be created. The key is stored in SDRAM.	Automatically after TLS session terminated. The value is overwritten with "0x00."
TLS session encryption key	The session encryption key is unique for each session and is based on the shared secrets that were negotiated at the start of the session. The Key is used to encrypt TLS session data. The key is stored in SDRAM.	Automatically after TLS session terminated. The value is overwritten with "0x00."
TLS session integrity key	This key is used to provide the privacy and TLS data integrity protection. The key is stored in SDRAM.	Automatically after TLS session terminated. The entire object is overwritten with zeros

8. Annex B: NIAP Technical Decisions (TDs)

NIAP TDs

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

Table 19. NIAP Technical Decisions TDs)

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0484	NIT Technical Decision for Interactive sessions in FTA_SSL_EXT.1 & FTA_SSL.3	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FTA_SSL_EXT.1, FTA_SSL.3	2019.12.18	Yes - TD has been applied
TD0483	NIT Technical Decision for Applicability of FPT_APW_EXT.1	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FPT_APW_EXT.1	2019.12.18	Yes - TD has been applied
TD0482	NIT Technical Decision for Identification of usage of cryptographic schemes	CPP_FW_v2.0, CPP_ND_V2.0E, CPP_ND_V2.1	ND SDv2.0e, FW SDv2.0e, ND SDv2.1	2019.12.18	Yes - TD has been applied
TD0481	NIT Technical Decision for FCS_(D)TLSC_EXT.X.2 IP addresses in reference identifiers	CPP_FW_v2.0, CPP_ND_V2.0E, CPP_ND_V2.1	ND SDv2.0, ND SDv2.1, FW SDv2.0e, FAU_GEN.1	2019.12.18	Yes - TD has been applied
TD0480	NIT Technical Decision for Granularity of audit events	CPP_ND_V2.0E, CPP_ND_V2.1	FIA_AFL.1 (NDcPP), section 2.3.1.3 (ND SD)	2019.12.18	Yes - TD has been applied
TD0478	NIT Technical Decision for Application Notes for FIA_X509_EXT.1 iterations	CPP_FW_v2.0, CPP_ND_V2.0E, CPP_ND_V2.1	FIA_X509_EXT.1/Rev, FIA_X509_EXT.1/ITT	2019.12.18	Yes - TD has been applied
TD0477	NIT Technical Decision for Clarifying FPT_TUD_EXT.1 Trusted Update	CPP_ND_V2.0, CPP_ND_V2.1	ND SD V2.0E, ND SD V2.1, FPT_TUD_EXT.1, Tests section	2019.12.18	Yes - TD has been applied
TD0475	NIT Technical Decision for Separate traffic consideration for SSH rekey	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_SSHC_EXT.1.1, FCS_SSHS_EXT.1.1, ND SD V2.0E, ND SD V2.1	2019.12.18	Yes - TD has been applied
TD0453	NIT Technical Decision for Clarify authentication	CPP_ND_V2.1	FCS_SSHC_EXT.1.9, ND SD v2.1	2019.09.16	No - Referenced requirement is

	methods SSH clients can use to authenticate SSH se				not being claimed
TD0451	NIT Technical Decision for ITT Comm UUID Reference Identifier	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_TLSS_EXT.1.2 and FCS_TLSS_EXT.2.2	2019.09.16	No - Referenced requirement is not being claimed.
TD0450	NIT Technical Decision for RSA-based ciphers and the Server Key Exchange message	CPP_ND_V2.1	FCS_TLSS_EXT.*.3, FCS_DTLSS_EXT.*.4, ND SD v2.1	2019.09.16	No - Referenced requirement is not being claimed.
TD0447	NIT Technical Decision for Using 'diffie-hellman-group-exchange-sha256' in FCS_SSHC/S_EXT.1.7	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_SSHC_EXT.1.7, FCS_SSHS_EXT.1.7	2019.09.16	Yes - TD has been applied
TD0425	NIT Technical Decision for Cut-and-paste Error for Guidance AA	CPP_ND_V2.0E, CPP_ND_V2.1	ND SD V2.0e, ND SD V2.1, FTA_SSL.3	31/05/19	Yes - TD has been applied
TD0424	NIT Technical Decision for NDcPP v2.1 Clarification - FCS_SSHC/S_EXT1.5	CPP_ND_V2.1	ND SD V2.1, FCS_SSHC_EXT.1.5, FCS_SSHS_EXT.1.5	31/05/19	Yes - TD has been applied
TD0423	NIT Technical Decision for Clarification about application of RfI#201726rev2	CPP_FW_V2.0E, CPP_ND_V2.0, CPP_ND_V2.1	ND SD V2.0E, FW SD V2.0E, ND SD V2.1	31/05/19	Yes - TD has been applied
TD0412	NIT Technical Decision for FCS_SSHS_EXT.1.5 SFR and AA discrepancy	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_SSHS_EXT.1.5, ND SD V2.0e, ND SD V2.1	22/03/19	Yes - TD has been applied
TD0411	NIT Technical Decision for FCS_SSHC_EXT.1.5, Test 1 - Server and client side seem to be confused	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_SSHC_EXT.1.5, ND SD V2.0E, ND SD V2.1	22/03/19	No - FCS_SSHC_EXT.1 has not been claimed in ST.
TD0410	NIT technical decision for Redundant assurance activities associated with FAU_GEN.1	CPP_ND_V1.0, CPP_ND_V2.0E, CPP_ND_V2.1	FAU_GEN.1, ND SD V1.0, ND SD V2.0e, ND SD V2.1	22/03/19	Yes - TD has been applied

TD0409	NIT decision for Applicability of FIA_AFL.1 to key-based SSH authentication	CPP_ND_V2.0E, CPP_ND_V2.1	FIA_AFL.1, ND SD v2.0e, ND SD v2.1	22/03/19	Yes - TD has been applied
TD0408	NIT Technical Decision for local vs. remote administrator accounts	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FIA_AFL.1, FIA_UAU_EXT.2, FMT_SMF.1	22/03/19	Yes - TD has been applied
TD0407	NIT Technical Decision for handling Certification of Cloud Deployments	CPP_ND_V2.0E, CPP_ND_V2.1		22/03/19	No - - ST does not include Cloud Deployment.
TD0402	NIT Technical Decision for RSA-based FCS_CKM.2 Selection	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_CKM.2, ND SD V2.0E, ND SD V2.1	24/02/19	Yes - TD has been applied
TD0401	NIT Technical Decision for Reliance on external servers to meet SFRs	CPP_ND_V2.0E, CPP_ND_V2.1	FTP_ITC.1	24/02/19	Yes - TD has been applied
TD0400	NIT Technical Decision for FCS_CKM.2 and elliptic curve-based key establishment	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_CKM.1, FCS_CKM.2	24/02/19	Yes - TD has been applied
TD0399	NIT Technical Decision for Manual installation of CRL (FIA_X509_EXT.2)	CPP_ND_V2.0E, CPP_ND_V2.1	FIA_X509_EXT.2, ND SD V2.0E, ND SD V2.1	24/02/19	Yes - TD has been applied
TD0398	NIT Technical Decision for FCS_SSH*EXT.1.1 RFCs for AES-CTR	CPP_FW_V2.0E, CPP_ND_V2.0E, CPP_ND_V2.1	FCS_SSHC_EXT.1.1, FCS_SSHS_EXT.1.1,	24/02/19	Yes - TD has been applied
TD0397	NIT Technical Decision for Fixing AES-CTR Mode Tests	CPP_ND_V2.0E, CPP_ND_V2.1	FCS_COP.1/DataEncryption, ND SD V2.0E, ND SD V2.1	24/02/19	Yes - TD has been applied
TD0396	NIT Technical Decision for FCS_TLSC_EXT.1.1, Test 2	CPP_ND_V2.0E, CPP_ND_V2.1	FCS_DTLSC_EXT.1.1FCS_DTLSC_EXT.2.1FCS_TLSC_EXT.1.1, FCS_TLSC_EXT.2.1, ND SD V2.0E, ND SD V2.1	24/02/19	Yes - TD has been applied
TD0395	NIT Technical Decision for Different Handling of TLS1.1 and TLS1.2	CPP_ND_V2.0E, CPP_ND_V2.1	FCS_TLSS_EXT.2.4, FCS_TLSS_EXT.2.5, ND SD V2.0E, ND SD V2.1	24/02/19	No - Referenced requirement is not being claimed.

9. Annex C: References

The documentation listed below was used to prepare this ST

Table 20. References

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated September 2012, version 3.1, Revision 5, CCMB-2017-04-004
[NDcPPv2.1]	collaborative Protection Profile for Network Devices, version 2.1, March 11, 2019
[SD]	Supporting Document – Evaluation Activities for Network Device cPP, version 2.1, September-2018
[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 140-2]	FIPS PUB 140-2 Federal Information Processing Standards Publication Security Requirements for Cryptographic Modules May 25, 2001
[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

10. Annex D: Acronyms and Terms

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

Table 21. Acronyms and Terms

Acronym/Term	Definition
AC	Alternating Current
ACL	Access Control Lists
AES	Advanced Encryption Standard
AES-CCM	AES Counter with CBC-MAC
AP	Access Point
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DWDM	Dense Wavelength-Division Multiplexing
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol (EAP) over LAN
ESP	Encapsulating Security Payload
GE	Gigabit Ethernet port
GMK	Group Master Key
GTK	Group Temporal Key
HTTP	Hyper-Text Transport Protocol
HTTPS	Hyper-Text Transport Protocol Secure
ICMP	Internet Control Message Protocol
IOS-XR	Universal Cisco Internet Operating System
IT	Information Technology
KCK	Key Confirmation Key
KEK	Key Encryption Key
MIC	Message Integrity Check
NCS	Network Convergence System

NDcPP	collaborative Network Device Protection Profile
OS	Operating System
PMK	Pairwise Master Key
PoE	Power over Ethernet
PRF	Pseudo-random function
PP	Protection Profile
PTK	Pairwise Transient Key
QSFP	Quad Small Form-Factor Pluggable
RSN	Robust Security Network
RU	Rack Unit
SA	Security Association
SFP	Small–form-factor pluggable port
SHS	Secure Hash Standard
SSD	Solid-State Drive
SSHv2	Secure Shell (version 2)
SSID	Service Set Identifier
ST	Security Target
Supplicant	The client software used for WLAN authentication
TCP	Transport Control Protocol
TLS	Transport Layer Security
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
WAN	Wide Area Network

11 Annex E: Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.

Contacting Cisco

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.