



# Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3

## Security Target

**Version:** 1.0  
**Date:** 22 October 2021

## Table of Contents

1.	Security Target Introduction.....	6
1.1	ST and TOE Reference .....	6
1.2	TOE Overview .....	7
1.3	TOE Product Type .....	7
1.3.1	Required non-TOE Hardware/Software/Firmware .....	8
1.4	TOE Description .....	8
1.5	TOE Evaluated Configuration.....	10
1.6	Physical Scope of the TOE.....	10
1.7	Logical Scope of the TOE .....	17
1.7.1	Security Audit .....	17
1.7.2	Cryptographic Support.....	17
1.7.3	Identification and Authentication.....	19
1.7.4	Security Management.....	19
1.7.5	Protection of the TSF .....	20
1.7.6	TOE Access .....	20
1.7.7	Trusted Path/Channels .....	20
1.8	Excluded Functionality.....	20
2.	Conformance Claims.....	21
2.1	Common Criteria Conformance Claim .....	21
2.2	Protection Profile Conformance Claim .....	21
2.3	Protection Profile Conformance Claim Rationale .....	22
2.3.1	TOE Appropriateness .....	22
2.3.2	TOE Security Problem Definition Consistency .....	22
2.3.3	Statement of Security Requirements Consistency.....	22
3.	Security Problem Definition.....	24
3.1	Assumptions .....	24
3.2	Threats.....	25
3.3	Organizational Security Policies.....	27
4.	Security Objectives .....	28
4.1	Security Objectives for the TOE.....	28
4.2	Security Objectives for the Environment.....	28
5.	Security Requirements .....	30
5.1	Conventions.....	30
5.2	TOE Security Functional Requirements .....	30
5.3	SFRs drawn from the NDcPPv2.2e .....	31
5.3.1	Class: Security Audit (FAU).....	31

5.3.1.1 FAU_GEN.1 – Audit Data Generation	31
5.3.1.2 FAU_GEN.2 – User Identity Association	34
5.3.1.3 FAU_STG_EXT.1 – Protected Audit Event Storage	34
5.3.2 Class: Cryptographic Support (FCS).....	34
5.3.2.1 FCS_CKM.1– Cryptographic Key Generation	34
5.3.2.2 FCS_CKM.2– Cryptographic Key Establishment (Refinement)	34
5.3.2.3 FCS_CKM.4 – Cryptographic Key Destruction	35
5.3.2.4 FCS_COP.1/DataEncryption – Cryptographic Operation (AES Data Encryption/Decryption)	35
5.3.2.5 FCS_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)	35
5.3.2.6 FCS_COP.1/Hash – Cryptographic Operation (Hash Algorithm)	35
5.3.2.7 FCS_COP.1/KeyedHash – Cryptographic Operation (Keyed Hash Algorithm)	35
5.3.2.8 FCS_RBG_EXT.1 – Random Bit Generation	36
5.3.2.9 FCS_SSHS_EXT.1 – SSH Server Protocol	36
5.3.2.10 FCS_TLSC_EXT.1 – TLS Client Protocol	36
5.3.3 Class: Identification and Authentication (FIA) .....	37
5.3.3.1 FIA_AFL_EXT.1 – Authentication Failure Management	37
5.3.3.2 FIA_PMG_EXT.1 – Password Management	37
5.3.3.3 FIA_UIA_EXT.1 – User Identification and Authentication	37
5.3.3.4 FIA_UAU_EXT.2 – Password-based Authentication Mechanism	37
5.3.3.5 FIA_UAU.7 – Protected Authentication Feedback	38
5.3.3.6 FIA_X509_EXT.1/Rev – X.509 Certificate Validation	38
5.3.3.7 FIA_X509_EXT.2 – X.509 Certificate Authentication	38
5.3.4 Class: Security Management (FMT) .....	38
5.3.4.1 FMT_MOF.1/ManualUpdate – Management of Security Functions Behavior	38
5.3.4.2 FMT_MTD.1/CoreData – Management of TSF Data	38
5.3.4.3 FMT_MTD.1/CryptoKeys Management of TSF data	39
5.3.4.4 FMT_SMF.1 – Specification of Management Functions	39
5.3.4.5 FMT_SMR.2 – Restrictions on Security Roles	39
5.3.5 Class: Protection of the TSF (FPT) .....	39
5.3.5.1 FPT_SKP_EXT.1 – Protection of TSF Data (for reading of all symmetric keys)	39
5.3.5.2 FPT_APW_EXT.1 – Protection of Administrator Passwords	40
5.3.5.3 FPT_STM_EXT.1 – Reliable Time Stamps	40
5.3.5.4 FPT_TST_EXT.1 – TSF Testing	40
5.3.5.5 FPT_TUD_EXT.1 – Trusted Updates	40
5.3.6 Class: TOE Access (FTA).....	40
5.3.6.1 FTA_SSL_EXT.1 – TSF-initiated Session Locking	40
5.3.6.2 FTA_SSL.3 – TSF-initiated Termination	40
5.3.6.3 FTA_SSL.4 – User-initiated Termination	40
5.3.6.4 FTA_TAB.1 – Default TOE Access Banners	41
5.3.7 Class: Trusted Path/Channels (FTP) .....	41
5.3.7.1 FTP_ITC.1 – Inter-TSF Trusted Channel	41
5.3.7.2 FTP_TRP.1/Admin – Trusted Path	41
5.4 TOE SFR Dependencies Rationale .....	41
5.5 Security Assurance Requirements .....	41
5.5.1 SAR Requirements .....	41
5.5.2 Security Assurance Requirements Rationale .....	42
5.6 Assurance Measures.....	42
6 TOE Summary Specification.....	43
6.1 TOE Security Functional Requirement Measures .....	43
7. Annex A: Key Zeroization.....	57
8. Annex B: References.....	59
9. Annex C: Acronyms and Terms.....	60

10 Annex E: Obtaining Documentation and Submitting a Service Request..... 62  
 10.1 Contacting Cisco ..... 62

## Table of Tables

Table 1. ST and TOE Identification..... 6  
 Table 2. IT Environment Component..... 8  
 Table 3. Hardware Models and Description ..... 11  
 Table 4. CAVP Certificates..... 17  
 Table 5. TOE Provided Cryptography..... 18  
 Table 6. Processors Within the TOE..... 19  
 Table 7 Excluded Functionality and Rationale ..... 20  
 Table 8. Protection Profile Conformance ..... 21  
 Table 9. NIAP Technical Decisions ..... 21  
 Table 10. TOE Assumptions ..... 24  
 Table 11. Threats ..... 26  
 Table 12. Organizational Security Policies ..... 27  
 Table 13. Security Objectives for the Environment..... 28  
 Table 14. Security Requirement Conventions ..... 30  
 Table 15. Security Functional Requirements ..... 30  
 Table 16. Auditable Events ..... 32  
 Table 17. Assurance Requirements ..... 41  
 Table 18. Assurance Measures ..... 42  
 Table 19. How TOE SFRs Measures..... 43  
 Table 20. Key Zeroization..... 57  
 Table 21. References..... 59  
 Table 22. Acronyms and Terms ..... 60

## Table of Figures

Figure 1. Cisco Nexus 3000 and Environment ..... 9  
 Figure 2. Cisco Nexus 9000 and Environment ..... 9

## 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 Nexus 3000 and 9000 Series Switches (Cisco Nexus 3K & 9K Series) running on NX-OS 9.3. 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2021 Cisco Systems, Inc. All rights reserved.

# 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 its TOE.

**Table 1. ST and TOE Identification**

Name	Description
ST Title	Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 Security Target
ST Version	1.0
Publication Date	October 22 2021
Vendor and ST Author	Cisco Systems, Inc.
TOE Reference	Cisco Nexus 3000 and 9000 Series Switches

TOE Hardware Models	<p><u>Cisco Nexus 3100 Series Switches</u></p> <ul style="list-style-type: none"> <li>3172PQ/PQ-XL, 3172TQ, 31128PQ</li> </ul> <p><u>Cisco Nexus 3100v Series Switches</u></p> <ul style="list-style-type: none"> <li>31108PC-V, 31108TC-V, Nexus 3132Q-V</li> </ul> <p><u>Cisco Nexus 3100Z Series Switches</u></p> <ul style="list-style-type: none"> <li>3132C-Z</li> </ul> <p><u>Cisco Nexus 3200 Series Switches</u></p> <ul style="list-style-type: none"> <li>3232C, 3264C-E</li> </ul> <p><u>Cisco Nexus 3400 Series Switches</u></p> <ul style="list-style-type: none"> <li>34180-YC, 3464C, 3432D-S, 3408-S</li> </ul> <p><u>Cisco Nexus 3500 Series Switches</u></p> <ul style="list-style-type: none"> <li>3524-X/XL, 3548-X/XL</li> </ul> <p><u>Cisco Nexus 3600 Series Switches</u></p> <ul style="list-style-type: none"> <li>36180YC-R, 3636C-R</li> </ul> <p><u>Cisco Nexus 9200 Series Switches</u></p> <ul style="list-style-type: none"> <li>92348GC-X, 92160YC-X, 92300YC, 9272Q</li> </ul> <p><u>Cisco Nexus 9300 Series Switches</u></p> <ul style="list-style-type: none"> <li>93108TC-EX, 93108TC-FX, 9348GC-FXP, 93216TC-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX</li> </ul> <p><u>Cisco 9500 Series Switches</u></p> <ul style="list-style-type: none"> <li>9504, 9508, 9516</li> <li>Supervisor 9500-Sup-A , Supervisor 9500-Sup-A +</li> <li>Supervisor 9500-Sup-B , Supervisor 9500-Sup-B +</li> <li>System Controller N9k-SC-A</li> </ul>
TOE Software Version	NX-OS version 9.3
Keywords	Switch, Data Protection, Audit, Authentication, Encryption, Network Device, Secure Administration

## 1.2 TOE Overview

The Cisco Nexus 3000 and 9000 Series Switches in standalone mode (herein after referred to as the Cisco Nexus 3K & 9K Series) are purpose-built data center-class switches for use as an aggregation switch in the data center. 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 v2.2e.

The TOE are data center-class switches for use as an aggregation switch in the data center. The Cisco Nexus 3K and 9K Series provides multilayer, supporting greater performance and enhanced operations through features including intelligent services. Programmability, automation, analytics and manageability. The TOE includes the hardware models as defined in Table 3 in Section 1.5.

The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 3100, 3100v, 3100z, 3200, 3400, 3500, 3600, 9200, 9300 and 9500. The software is comprised of the NX-OS software image Release 9.3

Cisco NX-OS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although NX-OS performs many networking functions, this TOE only addresses the functionality described in the Protection Profile that provide for the security of the TOE itself as described in 1.7 Logical Scope of the TOE below.

### 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 a SSH client installed that is used by the TOE administrator to support TOE administration through SSH protected channels. Any SSH client that supports SSHv2 may be used.
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 to secure the connection. The audit records are automatically sent to the remote syslog once the configuration and settings are complete.

## 1.4 TOE Description

This section provides an overview of the Cisco Nexus 3000 and 9000 Series Switches Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following model series: 3100, 3100v, 3100z, 3200, 3400, 3500, 3600, 9200, 9300 and 9500.. The software is comprised of the NX-OS software image Release 9.3.

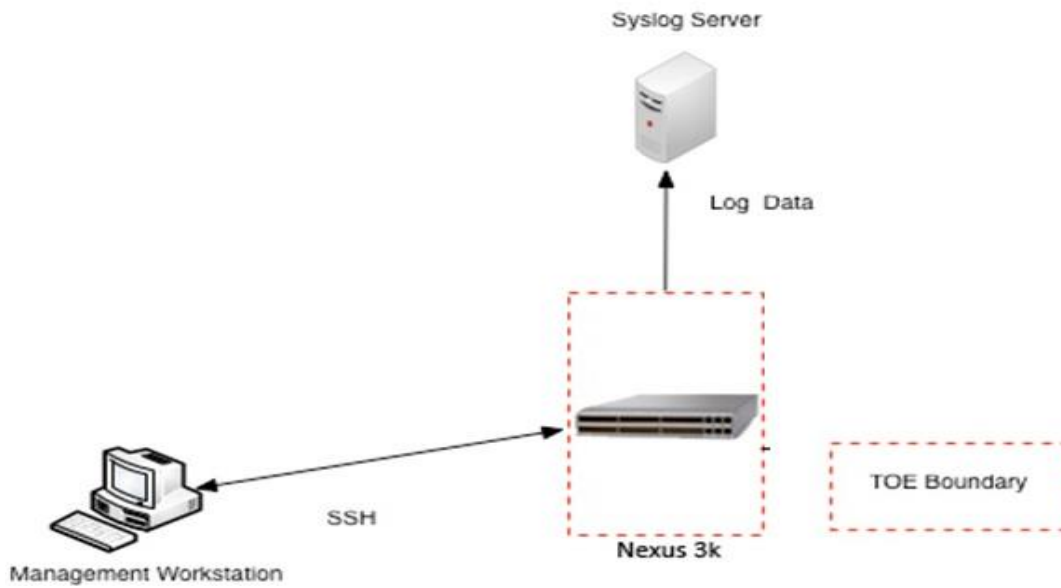
The Cisco Nexus 3000 and 9000 Series Switches that comprise the TOE have common hardware characteristics. These characteristics affect only non-TSF relevant functions of the switches (such as throughput and amount of storage) and therefore support security equivalency of the switches in terms of hardware. All security functionality is enforced on the Nexus 3000 and Nexus 9000 Series switches.

Cisco NX-OS is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching. Although NX-OS performs many networking functions, this TOE only addresses the functions that provide for the security of the TOE itself as described in 1.7 Logical Scope of the TOE below.

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



Figure 1. Cisco Nexus 3000 and Environment

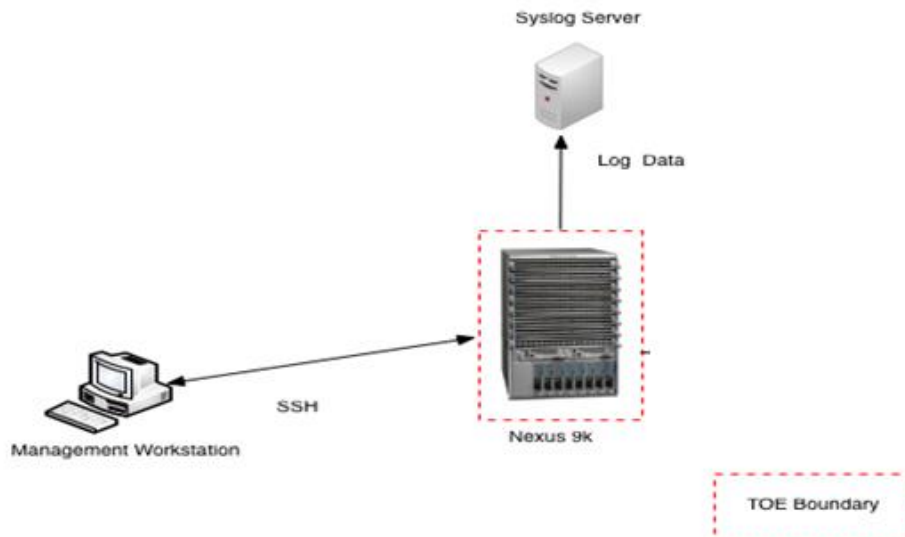


The previous figure includes the following:

- The TOE models:
  - Cisco Nexus 3000 Series
- The following are considered to be in the IT Environment:
  - Management Workstation
  - Syslog Server

For management purposes the TOE provides command line access to administer the TOE.

Figure 2. Cisco Nexus 9000 and Environment



The previous figure includes the following:

- The TOE models:
  - Cisco Nexus 9000 Series
- The following are considered to be in the IT Environment:
  - Management Workstation
  - Syslog Server

For management purposes the TOE provides command line access to administer the TOE.

## 1.5 TOE Evaluated Configuration

The TOE consists of one switch as specified in section 1.6 below and includes the Cisco NX-OS software. The TOE has two or more network interfaces and is connected to at least one internal and one external network. The Cisco NX-OS configuration determines how packets are handled to and from the TOE's network interfaces. The switch configuration will determine how traffic flows received on an interface will be handled. Typically, packet flows are passed through the internetworking device and forwarded to their configured destination.

If the TOE is to be remotely administered, then the management workstation must be connected to an internal network and SSHv2 must be used to securely connect to the TOE. Audit records are stored locally and are also remotely backed up to a remote syslog server. If these servers are used, they must be attached to the internal (trusted) network. The internal (trusted) network is meant to be separated effectively from unauthorized individuals and user traffic; one that is in a controlled environment where implementation of security policies can be enforced.



All supported models for the 3000, 3100, 3100v, 3100z, 3200, 3400, 3500, 3600, 9300 and 9500 series are considered part of the TOE evaluated configuration.

## 1.6 Physical Scope of the TOE

The TOE is a hardware and software solution made up of the models as follows: 3100, 3100v, 3100z, 3200, 3400, 3500, 3600, 9200, 9300 and 9500 series. 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 Nexus 3000 and 9000 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.



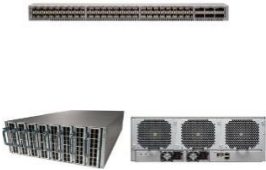
The I/O modules that are compatible with the Nexus 9500 Series are listed on the Cisco web site in the I/O data sheets for the respective module: <http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/models-comparison.html>. For conciseness the I/O modules are not listed explicitly in the below table.

Table 3. Hardware Models and Description


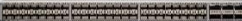

Hardware Platform	Model	External Identification	Description	Interfaces
Cisco 3100 Models				
	Nexus 3172PQL	N3K-C3172PQ-10GE	72 x 10 Gigabit Ethernet ports (48 SFP+ <sup>1</sup> and 6 QSFP+)	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45</li> <li>• Console serial port: 1 RS-232 connector</li> <li>• USB ports (1)</li> </ul>
	Nexus 3172PQ-XL	N3K-C3172PQ-XL		
	Nexus 3172TQ	N3K-C3172TQ-10GT N3K-C3172TQ-32T	72 x 10 Gigabit Ethernet ports (48 10GBASE-T and 6 QSFP+)	
	Nexus 31128PQ	N3K-C31128PQ-10GE	48 x 10 Gigabit Ethernet ports (32 10GBASE-T and 6 QSFP+)	
Cisco 3100v Models				
	Nexus 31108PC-V	N3K-C31108PC-V	48 x 10-Gbps SFP+ ports and 6 x QSFP28 <sup>2</sup> ports (all QSFP ports can operate at 40 or 100 Gbps)	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45</li> <li>• Console serial port: 1 RS-232 connector</li> <li>• USB ports (1)</li> </ul>
	Nexus 31108TC-V	N3K-C31108TC-V	48 x 10GBASE-T ports and 6 x QSFP28 ports (all QSFP ports can operate at 40 or 100 Gbps)	•
	Nexus 3132Q-V	N3K-C3132Q-V	32 x 40-Gbps QSFP+ ports (all ports are capable of 10 or 40 Gbps)	•
Cisco 3100z Models				

<sup>1</sup> SFP+ - Enhanced Small Form-Factor Pluggable


<sup>2</sup> QSFP28 - Quad Small Form-Factor Pluggable

<p>Cisco Nexus 3100Z Series</p> 	<p>Nexus 3132C-Z</p>	<p>N3K-C3132C-Z</p>	<p>32 fixed 100-Gigabit Ethernet QSFP28 ports</p>	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45</li> <li>• Console serial port: 1 RS-232 connector</li> <li>• USB ports (1)</li> <li>• 10-Gbps SFP port (2)</li> </ul>
<p>Cisco 3200 Models</p>				
<p>Cisco Nexus 3200 Series</p> 	<p>Nexus 3232C</p>	<p>N3K-C3232C</p>	<p>32 fixed 100 Gigabit Ethernet QSFP28 ports</p>	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45</li> <li>• Console serial port: 1 RS-232 connector</li> <li>• USB ports (2)</li> </ul>
	<p>Nexus 3264C-E</p>	<p>N3K-C3264C-E</p>	<p>64 fixed 100-Gigabit Ethernet QSFP28 ports</p>	
<p>Cisco 3400 Models</p>				
<p>Cisco Nexus 3400 Series</p> 	<p>Nexus 34180-YC</p>	<p>N3K-C34180YC</p>	<p>48 x SFP+/SFP28 and 6 x QSFP+/QSFP28 ports</p>	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45, 1 SFP</li> <li>• Console serial port: 1 RS-232 connector</li> <li>• USB ports (1)</li> </ul>
	<p>Nexus 3464C</p>	<p>N3K-C3464C</p>	<p>64 x QSFP+/QSFP28 ports and 2 x SFP+</p>	
	<p>Nexus 3432D-S</p>	<p>N3K-C3432D-S</p>	<p>32 fixed 400-Gigabit Ethernet QSFP-DD<sup>3</sup> ports</p>	
	<p>Nexus 3408-S</p>	<p>N3K-C3408-S</p>	<p>4RU, 8-slot chassis. 128 ports of 100G or 32 ports of 400G.</p>	
<p>Cisco 3500 Models</p>				
<p>Cisco Nexus 3500 Series</p>	<p>Nexus 3524-X</p>	<p>N3K-C3524P-10GX</p>	<p>48 fixed SFP+ ports (1 or 10 Gbps); the Cisco Nexus 3524-X enables only 24 ports</p>	<ul style="list-style-type: none"> <li>• Management ports: 2 RJ-45</li> </ul>

<sup>3</sup> QSFP-DD – Quad Small Form-factor pluggable Double Density

	Nexus 3524-XL	N3K-C3524P-XL	48 fixed SFP+ ports (1 or 10 Gbps); the Cisco Nexus 3524-XL enables only 24 ports	<ul style="list-style-type: none"> <li>• Console serial port: 1 RS-232 connector</li> <li>• USB ports (1)</li> </ul>
	Nexus 3548-X	N3K-C3548P-10GX	48 fixed SFP+ ports (1 or 10 Gbps); the Cisco Nexus 3524-XL enables only 24 ports	
	Nexus 3548-XL	N3K-C3548P-XL	48 fixed SFP+ ports (1 or 10 Gbps); the Cisco Nexus 3524-XL enables only 24 ports	
Cisco 3600 Models				
	Nexus 36180YC-R	N3K-C36180YC-R	48 ports 1, 10, or 25 Gigabit Ethernet SFP. 6 ports 100 Gigabit Ethernet QSFP28.	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45</li> <li>• Console serial port: 1 RS-232 connector</li> <li>• USB ports (1)</li> </ul>
	Nexus 3636C-R	N3K-C3636C-R	36 QSFP28 ports operating at 40 or 100 Gigabit Ethernet.	
Cisco 9200 Models				
	Nexus 92348GC-X	N9K- C92348GC-X	48p 100M/1G Base-T ports + 4p 1/10/25G SPF28,+2p 40/100G QSFP28	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45, 1 SFP+</li> <li>• Console serial port: 1 RJ-45</li> <li>• USB ports (1)</li> </ul>
	Nexus 92160YC-X	N9K-C92160YC-X	8 x 1/10/25-Gbps SFP+ ports and 6 x QSFP28 ports (4 of the QSFP+ ports are 100 Gbps capable ports)	
	Nexus 92300YC	N9K-C92300YC	48 x 1/10/25-Gbps SFP+ ports and 18 x 40/100-Gbps QSFP28 ports	
	Nexus 9272Q	N9K-C9272Q	72 x 40-Gbps QSFP+ ports	
	Nexus 9272Q	N9K-C9272Q		
Cisco 9300 Models				

<p>Cisco Nexus 9300 Series</p> 	93108TC-EX	N9K-C93108TC-EX	Four 48 x 10GBASE-T ports and 6 x 40/100-Gbps QSFP28 ports	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45</li> <li>• Console serial port: 1 RJ-45</li> <li>• USB ports (2)</li> </ul>
	Nexus 93108TC-FX	N9K-C93108TC-FX	48 x 100M/1/10GBASE-T ports and 6 x 40/100-Gbps QSFP28 ports	
	Nexus 9348GC-FXP	N9K-C9348GC-FXP	48 x 100M/1G BASE-T ports, 4 x 1/10/25-Gbps SFP28 ports and 2 x 40/100-Gbps QSFP28 ports	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45 and 1 SFP+</li> <li>• Console serial port: 1 RJ-45</li> <li>• USB ports (1)</li> </ul>
	Nexus 93216TC-FX2	N9K-C93216TC-FX2	96 x 100M/1/10GBASE-T ports and 12 x 40/100-Gigabit QSFP28 ports	
	Nexus 93180LC-EX	N9K-C93180LC-EX	Up to 32 x 40/50-Gbps QSFP+ ports OR 18 x 100-Gbps QSFP28 ports	
	Nexus 93180YC-EX	N9K-C93180YC-EX	Four 48 x 10/25-Gbps fiber ports and 6 x 40/100-Gbps Quad Small Form-Factor Pluggable 28 (QSFP28) ports	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45</li> <li>• Console serial port: 1 RJ-45</li> <li>• USB ports (2)</li> </ul>
	Nexus 93180YC-FX	N9K-C93180YC-FX	48 x 1/10/25-Gbps fiber ports and 6 x 40/100-Gbps QSFP28 ports	
	Nexus 93240YC-FX2	N9K-C93240YC-FX2	48 x 1/10/25-Gbps fiber ports and 12 x 40/100-Gbps QSFP28 ports	
	Nexus 93360YC-FX2	N9K-C93360YC-FX2	96 x 1/10/25-Gbps fiber ports and 12 x 40/100-Gbps QSFP28 ports	
	Nexus 9364C	N9K-C9364C	64-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports	<ul style="list-style-type: none"> <li>• Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+)</li> <li>• Console serial port: 1 RJ-45</li> <li>• USB ports (1)</li> </ul>
	Nexus 9332C	N9K-C9332C	32-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports	
	Nexus 9336C-FX2	N9K-C9336C-FX2	36 x 40/100-Gbps QSFP28 ports	

	Nexus 9364C-GX	N9K-C9364C-GX	64 x 100/40-Gbps Quad Small Form-Factor Pluggable (QSFP28)	<ul style="list-style-type: none"> <li>• Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+)</li> <li>• Console serial port: 1 RJ-45</li> <li>• USB ports (1)</li> </ul>
	Nexus 9316D-GX	N9K-C9316D-GX	16 x 400/100-Gbps QSFP-DD ports	
	Nexus 93600CD-GX	N9K-C93600CD-GX	28 x 100/40-Gbps Quad Small Form-Factor Pluggable (QSFP28) and 8 x 400/100-Gbps QSFP-DD ports	
Cisco 9500 Models				
	Nexus 9504	N9K-C9504	Chassis: up to 2 supervisor modules of the same type, 4 I/O modules, and up to 6 fabric modules, 2 system controllers	<ul style="list-style-type: none"> <li>• Based on Supervisor and I/O modules installed)</li> </ul>
	Nexus 9508	N9K-C9508	Chassis: up to 2 supervisor modules of the same type, 8-I/O modules, up to two system controller modules, up to six fabric modules	
	Nexus 9516	N9K-C9516	Chassis: up to 2 supervisor modules and 16 I/O modules, up to two system controller modules, up to six fabric modules	
	Supervisor 9500-Sup-A	N9K-SUP-A	Four cores, 1.8 GHz, 16 GB of memory, and 64 GB of SSD (N9K-SUP-A)	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45</li> <li>• Console serial port: 1 RJ-45</li> <li>• USB ports (2)</li> </ul>
	Supervisor 9500-Sup-A+	N9K-SUP-A+	Four cores/8-Thread, 1.8 GHz, 16 GB of memory, and 64 GB of SSD (N9K-SUP-A+)	
	Supervisor 9500-Sup-B	N9K-SUP-B	Six cores, 2.1 GHz, 24 GB of memory, and 256 GB of SSD (N9K-SUP-B)	<ul style="list-style-type: none"> <li>• Management ports: 1 RJ-45</li> <li>• Console serial port: 1 RJ-45</li> </ul>

	Supervisor 9500-Sup-B+	N9K-SUP-B+	Six cores/12-Thread, 1.9 GHz, 24 GB of memory, and 256 GB of SSD <sup>4</sup> (N9K-SUP-B+)	<ul style="list-style-type: none"> <li>• USB ports (2)</li> </ul>
	System Controller N9k-SC-A	N9K-SC-A	A pair of redundant system controllers offloads chassis management functions from the supervisor modules. The controllers are responsible for managing power supplies and fan trays and are a central point for the Gigabit Ethernet out-of-band channel (EOBC) between the supervisors, fabric modules, and line cards.	<ul style="list-style-type: none"> <li>• Not applicable</li> </ul>

---

<sup>4</sup> SSD – Solid-state Drive



## 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 v2.2e as necessary to satisfy testing/assurance measures prescribed therein.

### 1.7.1 Security Audit

The TOE provides extensive capabilities to generate audit data targeted at detecting such activity. The TOE generates an audit record for each auditable event. Each security relevant audit event has the date, timestamp, event description, and subject identity. The administrator configures auditable events, performs back-up operations and manages audit data storage. 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. The TOE leverages the Cisco FIPS Object Module (FOM) 6.2 certificate A397 and has been validated for conformance to the requirements of FIPS140-2 140-2 Level 1.

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, 256)	A397	FOM 6.2	FCS_COP.1/DataEncryption
SHS (SHA-1, SHA-256, SHA-384 and SHA-512)	Cryptographic hashing services	Byte Oriented	A397	FOM 6.2	FCS_COP.1/Hash
HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and	Keyed hashing services and software integrity test	Byte Oriented	A397	FOM 6.2	FCS_COP.1/KeyedHash

Algorithm	Description	Supported Mode	CAVP Cert. #	Module	SFR
HMAC-SHA-512)					
DRBG	Deterministic random bit generation services in accordance with ISO/IEC 18031:2011	CTR_DRBG (AES 256)	A397	FOM 6.2	FCS_RBG_EXT
RSA	Signature Verification and key transport	FIPS PUB 186-4 Key Generation  PKCS #1 v2.1 2048 bit key	A397	FOM 6.2	FCS_CKM.1  FCS_CKM.2  FCS_COP.1/SigGen
ECDSA	Cryptographic Signature services	FIPS 186-4, Digital Signature Standard (DSS)	A397	FOM 6.2	FCS_CKM.1  FCS_CKM.2  FCS_COP.1/SigGen
CVL KAS ECC	Key Agreement	NIST Special Publication 800-56AR3	A397	FOM 6.2	FCS_CKM.1  FCS_CKM.2
CVL KAS FFC	Key generation and establishment	NIST Special Publication 800-56AR3	A397	FOM 6.2	FCS_CKM.1  FCS_CKM.2
FFC	Key generation and establishment	FIPS 186-4, Digital Signature Standard (DSS)	A397	FOM 6.2	FCS_CKM.1  FCS_CKM.2

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

The Nexus 3000 and 9000 Series Switches platforms contain the processors as listed in Table 6 below.

Table 6. Processors Within the TOE

Processor	Use on TOE Platform
Intel Pentium B925C 2.0 GHz (Ivy Bridge)	3172PQ, 3172TQ, 3524-X, 3548-X
Intel Core i3-3115C 2.5GHz (Ivy Bridge)	31128PQ, 3172PQ-XL, 31108PC-V, 31108TC-V, 3132Q-V, 3524-XL, 3548-XL, 92160YC-X
Intel Xeon (Broadwell) D-1526 1.8GHz <sup>5</sup>	3132C-Z, 3264C-E, 34180-YC, 3464C, 3432D-S, 92348GC-X, 92300YC, 93108TC-FX, 93180LC-EX, 9348GC-FXP, 93216TC-FX2, 93240YC-FX2, 93360YC-FX2, 9364C, 9332C, 9336C-FX2, 9364C-GX, 9316D-GX, 93600CD-GX, Supervisor 9500-Sup-A+
Intel Xeon D-1528 1.9GHz (Broadwell)	3408-S, 36180YC-R, 93180YC-FX, Supervisor 9500-Sup-B +
Intel Xeon D-1548 2.0GHz (Broadwell)	3636C-R
Intel Xeon E5-2403 v2 (Ivy Bridge) 1.8GHz <sup>6</sup>	3232C, Supervisor 9500-Sup-A
Intel Xeon E5-2420 v2 (Ivy Bridge) @ 2.20 GHz	Supervisor 9500-Sup-B
Intel Xeon (Ivy Bridge) E3-1105C V2 @ 1.80GHz	9272Q, 93108TC-EX, 93180YC-EX

### 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 TOE 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.

<sup>5</sup> While tested on the Intel Xeon (Broadwell) D-1526, any Intel® Xeon® D-15xx (Broadwell) processor may be used as part of the evaluated configuration.

<sup>6</sup> While tested on the Intel Xeon E5-2402 v2 (Ivy Bridge), any Intel Xeon E5-24xx (Ivy Bridge) processor may be used as part of the evaluated configuration.

### 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 NX-OS is not a general-purpose operating system and access to Cisco NX-OS memory space is restricted to only Cisco NX-OS functions.

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

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

### 1.7.6 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 administrator can also terminate their own session by exiting out of the CLI.

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

### 1.7.7 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 v2.2e.

**Table 7 Excluded Functionality and Rationale**

Function Excluded	Rationale
Non-FIPS 140-2 mode of operation	This mode of operation includes non-FIPS allowed operations.
Telnet	Telnet will be disabled in the evaluated configuration.
SNMP	SNMP will be disabled in the evaluated configuration.
NTP	NTP will be disabled in the evaluated configuration.
DCNM GUI	The DCNM GUI was not included in the evaluated configuration.
Bash shell	Bash shell interface was not included in the evaluation.
PTP	PTP is not included in the evaluation.

This service can be disabled by configuration settings as described in the Guidance documents (AGD). The exclusion of this functionality does not affect the compliance to the collaborative Protection Profile for Network Devices Version 2.2e.

## 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 as listed in Table 8. This ST applies the NIAP Technical Decisions as described in Table 9:

**Table 8. Protection Profile Conformance**

Protection Profile	Version	Date
collaborative Protection Profile for Network Devices [NDcPP]	2.2e	March 23, 2020

**Table 9. NIAP Technical Decisions**

TD Identifier	TD Name	Protection Profiles	References	Publication Date	Applicable?
TD0592	NIT Technical Decision for Local Storage of Audit Records	CPP_ND_V2.2E	FAU_STG	2021.05.21	Yes- TD has been applied
TD0591	NIT Technical Decision for Virtual TOEs and hypervisors	CPP_ND_V2.2E	A.LIMITED_FUNCTIONALITY, ACRONYMS	2021.05.21	Yes- TD has been applied
TD0581	The NIT has issued a technical decision for Elliptic curve-based key establishment and NIST SP 800-56Arev3.	CPP_ND_V2.2E	FCS_CKM.2	2021.04.09	Yes- TD has been applied
TD0580	The NIT has issued a technical decision for clarification about use of DH14 in NDcPPv2.2e.	CPP_ND_V2.2E	FCS_CKM.1.1, FCS_CKM.2.1	2021.04.09	Yes- TD has been applied
TD0572	NIT Technical Decision for Restricting FTP_ITC.1 to only IP address identifiers	CPP_ND_V2.1, CPP_ND_V2.2E	FTP_ITC.1	2021.01.29	Yes- TD has been applied
TD0571	NIT Technical Decision for Guidance on how to handle FIA_AFL.1	CPP_ND_V2.1, CPP_ND_V2.2E	FIA_UAU.1, FIA_PMG_EXT.1	2021.01.29	Yes- TD has been applied
TD0570	NIT Technical Decision for Clarification about FIA_AFL.1	CPP_ND_V2.1, CPP_ND_V2.2E	FIA_AFL.1	2021.01.29	Yes- TD has been applied
TD0569	NIT Technical Decision for Session ID Usage Conflict in FCS_DTLSS_EXT.1.7	CPP_ND_V2.2E	ND_SD v2.2, FCS_DTLSS_EXT.1.7, FCS_TLSS_EXT.1.4	2021.01.28	No, SFR not claimed
TD0564	NIT Technical Decision for Vulnerability Analysis Search Criteria	CPP_ND_V2.2E	NDSDv2.2, AVA_VAN.1	2021.01.28	Yes- TD has been applied
TD0563	NIT Technical Decision for Clarification of audit date information	CPP_ND_V2.2E	NDcPPv2.2e, FAU_GEN.1.2	2021.01.28	Yes- TD has been applied

TD0556	NIT Technical Decision for RFC 5077 question	CPP_ND_V2.2E	NDSDv2.2, FCS_TLSS_EXT.1.4, Test 3	2020.11.06	No, SFR not claimed
TD0555	NIT Technical Decision for RFC Reference incorrect in TLSS Test	CPP_ND_V2.2E	NDSDv2.2, FCS_TLSS_EXT.1.4, Test 3	2020.11.06	No, SFR not claimed
TD0547	NIT Technical Decision for Clarification on developer disclosure of AVA_VAN	CPP_ND_V2.1, CPP_ND_V2.2E	ND SDv2.1, ND SDv2.2, AVA_VAN.1	2020.10.15	Yes
TD0546	NIT Technical Decision for DTLS - clarification of Application Note 63	CPP_ND_V2.2E	FCS_DTLS_EXT.1.1	2020.10.15	No, SFR not claimed
TD0538	NIT Technical Decision for Outdated link to allowed-with list	CPP_ND_V2.1, CPP_ND_V2.2E	Section 2	2020.07.13	Yes
TD0537	NIT Technical Decision for Incorrect reference to FCS_TLSC_EXT.2.3	CPP_ND_V2.2E	FIA_X509_EXT.2.2	2020.07.13	Yes
TD0536	NIT Technical Decision for Update Verification Inconsistency	CPP_ND_V2.1, CPP_ND_V2.2E	AGD_OPE.1, ND SDv2.1, ND SDv2.2	2020.07.13	Yes
TD0528	NIT Technical Decision for Missing EAs for FCS_NTP_EXT.1.4	CPP_ND_V2.1, CPP_ND_V2.2E	FCS_NTP_EXT.1.4, ND SD v2.1, ND SD v2.2	2020.07.13	No, SFR not claimed
TD0527	Updates to Certificate Revocation Testing (FIA_X509_EXT.1)	CPP_ND_V2.2E	FIA_X509_EXT.1/REV, FIA_X509_EXT.1/ITT	2020.07.01	Yes

## 2.3 Protection Profile Conformance Claim Rationale

### 2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profile and extended package:

- collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e

### 2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the collaborative Protection Profile for Network Devices, Version 2.2e for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition 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 2.2e 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 2.2e 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 [NDcPPv2.2e].

#### 3.1 Assumptions

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

Table 10. TOE Assumptions

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



Assumption	Assumption Definition
A.TRUSTED_ADMINISTRATOR	<p>The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes 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.</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).</p>
A.REGULAR_UPDATES	<p>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.</p>
A.ADMIN_CREDENTIALS_SECURE	<p>The administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.</p>
A.RESIDUAL_INFORMATION	<p>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.</p>

### 3.2 Threats

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

Table 11. Threats

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

Threat	Threat Definition
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

### 3.3 Organizational Security Policies

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

**Table 12. Organizational Security Policies**

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

## 4. Security Objectives

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

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 v2.2e 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 [NDcPPv2.2e].

**Table 13. Security Objectives for the Environment**

Environment Security Objective	IT Environment Security Objective Definition
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE. . Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. . Note: For vNDs the TOE includes only the contents of the its own VM, and does not include other VMs or the VS.  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.

Environment Security Objective	IT Environment Security Objective Definition
OE.RESIDUAL_INFORMATION	<p>The TOE administrator ensures that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment. For vNDs, this applies when the physical platform on which the VM runs is removed from its operational environment.</p>

## 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], [NDcPPv2.2e] 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 [NDcPPv2.2e] and NIAP Technical Decisions.

**Table 14. Security Requirement Conventions**

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

Where operations were completed in the [NDcPPv2.2e] itself, the formatting used in the [NDcPPv2.2e] 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 15. Security Functional Requirements**

Class Name	Component Identification	Component Name
FAU: Security Audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	Protected Audit Event Storage
FCS: Cryptographic Support	FCS_CKM.1	Cryptographic Key Generation
	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)

Class Name	Component Identification	Component Name
	FCS_COP.1/KeyedHash	Cryptographic Operation (Keyed Hash Algorithm)
	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
FMT: Security management	FMT_MOF.1/ManualUpdate	Management of security functions behaviour
	FMT_MTD.1/CoreData	Management of TSF Data
	FMT_MTD.1/CryptoKeys	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_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 NDcPPv2.2e

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

**FAU\_GEN.1.2** The TSF shall record within each audit record at least the following information:

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

**Table 16. Auditable Events**

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.
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.



SFR	Auditable Event	Additional Audit Record Contents
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FIA_X509_EXT.1/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.
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.
FMT_MTD.1/CoreData	None	None.
FMT_MTD.1/Cryptokey	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.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel.  Termination of the trusted channel.  Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.
FTP_TRP.1/Admin	Initiation of the trusted path.  Termination of the trusted path.  Failures of the trusted path functions.	None.

### 5.3.1.2 FAU\_GEN.2 – User Identity Association

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

### 5.3.1.3 FAU\_STG\_EXT.1 – Protected Audit Event Storage

**FAU\_STG\_EXT.1.1** The TSF shall be able to transmit the generated audit data to an external IT entity using a trusted channel according to FTP\_ITC.1.

**FAU\_STG\_EXT.1.2** The TSF shall be able to store generated audit data on the TOE itself. In addition

[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;
- ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4
- FFC schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.1
- FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526];

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

### 5.3.2.2 FCS\_CKM.2– Cryptographic Key Establishment (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 meets the following: RSAES-PKCS1-v1\_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”;
- ECC schemes using “NIST curves” [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.4
- Finite field-based key establishment schemes that meets the following: NIST Special Publication 800-56A Revision 2, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography”
- FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800-56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526];

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

### 5.3.2.3 FCS\_CKM.4 – Cryptographic Key Destruction

**FCS\_CKM.4.1** The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [

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

*that meets the following: No Standard.*

### 5.3.2.4 FCS\_COP.1/DataEncryption – Cryptographic Operation (AES Data Encryption/Decryption)

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

### 5.3.2.5 FCS\_COP.1/SigGen – Cryptographic Operation (Signature Generation and Verification)

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

[

- RSA Digital Signature Algorithm and cryptographic key sizes (modulus) [2048 bits].
- Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [256 bits or greater]

]

that meet the following:

[

- For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1\_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3.
- For ECDSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section and Appendix D, Implementing “NIST curves” P-256, P-384, and [P-521, no other curves]; ISO/IEC 14888-3, Section 6.4

]

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

### 5.3.2.7 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-384, HMAC-SHA-512, implicit] and cryptographic key sizes [160, 256, 384, 512] and **message digest sizes [160, 256, 384, 512] bits** that meet the following: *ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.*

### 5.3.2.8 FCS\_RBG\_EXT.1 – Random Bit Generation

**FCS\_RBG\_EXT.1.1** The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [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] *platform-based noise source* with minimum of [256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 “Security Strength Table for Hash Functions”, of the keys and hashes that it will generate.

### 5.3.2.9 FCS\_SSHS\_EXT.1 – SSH Server Protocol

**FCS\_SSHS\_EXT.1.1** The TSF shall implement the SSH protocol in accordance with RFCs [4251, 4252, 4253, 4254, 4344, 5647, 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 [262126] 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, AEAD\_AES\_128\_GCM, AEAD\_AES\_256\_GCM].

**FCS\_SSHS\_EXT.1.5** The TSF shall ensure that the SSH public-key based authentication implementation uses [rsa-sha2-256, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521] 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, AEAD\_AES\_128\_GCM, AEAD\_AES\_256\_GCM] as its MAC algorithm(s) and rejects all other MAC algorithm(s).

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

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

### 5.3.2.10 FCS\_TLSC\_EXT.1 – TLS Client Protocol

**FCS\_TLSC\_EXT.1.1** The TSF shall implement [TLS 1.2 (RFC 5246)] and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 3268
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 3268
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 4492
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 4492
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA as defined in RFC 4492
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA as defined in RFC 4492
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 as defined in RFC 5246
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256 as defined in RFC 5246
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288
- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 as defined in RFC 5288
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 as defined in RFC 5288



### 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 [the Online Certificate Status Protocol (OCSP) as specified in RFC 6960].
- The TSF shall validate the extendedKeyUsage field according to the following rules:
  - *Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.*
  - *Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.*
  - *Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.*
  - *OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.*

**FIA\_X509\_EXT.1.2/Rev** The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

#### **Application Note**

NIAP TD0527 has been applied to FIA\_X509\_EXT.1/Rev, though it impacts only the tests, not the text of the SFR

### 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 TD0537 has been applied to FIA\_X509\_EXT.2.

## 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\_MTD.1/CryptoKeys Management of TSF data

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

#### 5.3.4.4 FMT\_SMF.1 – Specification of Management Functions

**FMT\_SMF.1.1** The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to configure the access banner;*
- *Ability to configure the session inactivity time before session termination or locking;*
- *Ability to update the TOE, and to verify the updates using [hash comparison] capability prior to installing those updates;*
- *Ability to configure the authentication failure parameters for FIA\_AFL.1;*
  - [
  - *Ability to configure audit behavior (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);*
  - *Ability to configure the cryptographic functionality;*
  - *Ability to configure thresholds for SSH rekeying;*
  - *Ability to set the time which is used for time-stamps;*
  - *Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA\_UJA\_EXT.1;*
  - *Ability to configure the reference identifier for the peer;*
  - *Ability to import X.509v3 certificates to the TOE'S trust store*
  - ]

#### 5.3.4.5 FMT\_SMR.2 – Restrictions on Security Roles

**FMT\_SMR.2.1** The TSF shall maintain the roles:

- *Security Administrator.*

**FMT\_SMR.2.2** The TSF shall be able to associate users with roles.

**FMT\_SMR.2.3** The TSF shall ensure that the conditions

- *The Security Administrator role shall be able to administer the TOE 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 prevent the reading of plaintext administrative passwords.

### 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: [

- *Power-on Self tests*
  - *Firmware Integrity Test*
  - *Known Answer tests*
    - *AES Known Answer Test*
    - *HMAC Known Answer Test*
    - *DRBG Known Answer Test*
    - *KAS ECC Known Answer Test*
    - *KAS FFC Known Answer Test*
    - *RSA Signature Known Answer Test (both signature/verification)*
    - *SP800-56B RSA key wrap/unwrap Known Answer Test*
- *Conditional Self-Tests (run periodically during normal operation):*
  - *Continuous Random Number Generator test for DRBG*
  - *Continuous Random Number Generator test for Entropy Source*
  - *RSA Pairwise Consistency Test*
  - *Bypass 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.

## 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.

### 5.3.6.2 FTA\_SSL.3 – TSF-initiated Termination

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

### 5.3.6.3 FTA\_SSL.4 – User-initiated Termination

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



### 5.3.6.4 FTA\_TAB.1 – Default TOE Access Banners

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

## 5.3.7 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.*

### 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

[NDcPPv2.2e] 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 [NDcPPv2.2e] which are derived from [CC\_PART3]. The assurance requirements are summarized in the table below.

**Table 17. 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)

Assurance Class	Components Description
	Security Problem Definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance Documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life Cycle Support (ALC)	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 [NDcPPv2.2e]. As such, the [NDcPPv2.2e] 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 18. 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.

## 6 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 19. How TOE SFRs Measures**

TOE SFR	How the SFR is Met
FAU_GEN.1	<p>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. The key is identified by name for example rsa key. Additionally, the startup and shutdown of the audit functionality is audited.</p> <p>Each time an administrative user logs into or off of the TOE, an audit record is generated. The audit record contains the Day of Week, the Date, the Action, the User ID, and terminal information (where applicable) of the user logging into the TOE. Whenever an administrative user makes a configuration change to the TOE, an audit record is generated on a per-command basis. Likewise, the audit record contains the Day of Week, the Date, the Action, the User ID, the outcome of the event, and terminal information (where applicable) of the user making the configuration change.</p> <p>Auditing cannot be disabled except by shutting down the TOE and is automatically available upon the startup of the TOE. The TOE startup and shutdown is captured in the audit trail and servers as the audit records for these events.</p> <p>Example audit events are included below:</p> <pre>Fri May 30 13:21:22 2014:type=update:id=64.103.212.160@pts/0:user=admin :cmd=configure terminal ; username test123 password ***** role network-operator (SUCCESS)</pre> <p>In the above log event, a date and timestamp are displayed as well as an event description "cmd=configure terminal". The subject identity where a command is directly run by a user is displayed "user=admin." The outcome of the command is displayed: "SUCCESS"</p> <p>To configure the TOE to send audit records to a syslog server, the 'logging server' command is used. A maximum of eight syslog servers can be configured. Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information. The audit records are transmitted using TLS to the syslog server. If the communications to the syslog server is lost, the TOE generates an audit record and all permit traffic is denied until the communications are re-established.</p>

TOE SFR	How the SFR is Met
FAU_GEN.2	<p>The TOE shall ensure that each auditable event is associated with the user that triggered the event and as a result they are traceable to a specific user. For example a human user, user identity, or related session ID would be included in the audit record. For an IT entity or device, the IP address, MAC address, host name, or other configured identification is presented. A sample audit record is below:</p> <p>Fri May 30 13:21:22 2014:type=update:id=64.103.212.160@pts/0:user=admin:cmd=deleted user test123</p>
FAU_STG_EXT.1	<p>The TOE is configured to export syslog records to a specified, external syslog server in real-time. Once the configuration is complete, the audit records are automatically sent to the external syslog server at the same time as they are written to the logging buffer. The TOE protects communications with an external syslog server via TLS. If the TLS connection fails, the TOE will store audit records on the TOE when it discovers it can no longer communicate with its configured syslog server. When the connection is restored, the TOE will transmit the buffer contents to the syslog server.</p> <p>Access to the audit records stored on the TOE is only through a TSF Mediated interface. Only Authorized Administrators are explicitly authorized to access the audit records are given access to the audit records. There is no interface that allows Authorized Administrators to perform audit record modification. However, logs can only be cleared to free up space by an authorized administrator.</p> <p>The TOE overwrites the oldest audit records when the audit trail becomes full. The size of the logging files on the TOE is configurable by the administrator. The default value for the size of the logging buffer on the TOE is 4194304 bytes. Please refer to the Guidance documentation for configuration information.</p>

TOE SFR	How the SFR is Met															
<p>FCS_CKM.1 FCS_CKM.2</p>	<p>The TOE implements Diffie-Hellman based key establishment schemes that meets RFC 3526 and NIST Special Publication 800-56A Revision 3. The TOE implements and uses the prime and generator specified in RFC 3526 when generating parameters for the key exchange.</p> <p>The TOE also implements RSA key establishment schemes that is conformant to Section 7.2 of RFC 3447.</p> <p>The key pair generation portions of "The RSA Validation System" for FIPS 186-4 were used as a guide in testing the FCS_CKM.1 during the FIPS validation.</p> <p>The TOE employs RSA-based key establishment used in cryptographic operations.</p> <p>The TOE implements Elliptic Curve Diffie-Hellman (ECDH) (ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp52) key establishment schemes in SSH. The ECDH key generation meets the NIST FIPS PUB 186-4 Appendix B.4.</p> <p>The TOE also operates as a TLS Client. As such, the TOE functions as a receiver for RSA-based key establishment schemes. The TOE acts as a receiver for SSH communications.</p> <p>For details on each protocol, see the related SFR.</p> <table border="1" data-bbox="531 913 1235 1447"> <thead> <tr> <th>Scheme</th> <th>SFR</th> <th>Service</th> </tr> </thead> <tbody> <tr> <td>RSA</td> <td>FCS_TLSC_EXT.1 FCS_SSHS_EXT.1</td> <td>Support for SSH and TLS key establishment  Remote Administration for FCS_SSHS_EXT.1</td> </tr> <tr> <td>ECC/FFC</td> <td>FCS_TLSC_EXT.1</td> <td>Syslog Server</td> </tr> <tr> <td>ECC</td> <td>FIA_X509_EXT.1/Rev FIA_X509_EXT.2</td> <td>Transmit generated audit data to an external IT entity</td> </tr> <tr> <td>FFC</td> <td>FIA_X509_EXT.1/Rev FIA_X509_EXT.2</td> <td>Transmit generated audit data to an external IT entity</td> </tr> </tbody> </table>	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	ECC/FFC	FCS_TLSC_EXT.1	Syslog Server	ECC	FIA_X509_EXT.1/Rev FIA_X509_EXT.2	Transmit generated audit data to an external IT entity	FFC	FIA_X509_EXT.1/Rev FIA_X509_EXT.2	Transmit generated audit data to an external IT entity
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														
ECC/FFC	FCS_TLSC_EXT.1	Syslog Server														
ECC	FIA_X509_EXT.1/Rev FIA_X509_EXT.2	Transmit generated audit data to an external IT entity														
FFC	FIA_X509_EXT.1/Rev FIA_X509_EXT.2	Transmit generated audit data to an external IT entity														
<p>FCS_CKM.4</p>	<p>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.</p> <p>See Table 20 for more information on the key zeroization. The information provided in the table includes all of the all secrets, keys and associated values, the description, and the method used to zeroization when no longer required for use.</p> <p>The information is provided in the reference section for ease and readability of all of the all secrets, keys and associated values, their description and zeroization methods.</p>															

TOE SFR	How the SFR is Met
FCS_COP.1/DataEncryption	<p>The TOE provides symmetric encryption and decryption capabilities using AES in CBC, CTR and GCM mode (128, 256 bits) as described in ISO 18033-3 and ISO 10116. AES is implemented in the following protocols: SSHv2 and TLS.</p> <p>Through the implementation of the FIPS validated cryptographic module, the TOE provides AES encryption and decryption in support of SSHv2, and TLS for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands.</p>
FCS_COP.1/SigGen	<p>The TOE provides cryptographic signature services using the following:</p> <ul style="list-style-type: none"> <li>• RSA Digital Signature Algorithm with key size of 2048 as specified in FIPS PUB 186-4, “Digital Signature Standard”</li> <li>• ECDSA with key size of 256 or greater as specified in FIPS PUB 186-4, “Digital Signature Standard”.</li> </ul> <p>Through the implementation of the FIPS validated cryptographic module, the TOE provides cryptographic signatures in support of TLS for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands. The TOE provides the RSA option in support of SSHv2 and TLS key establishment. RSA (2048-bit) is used in the establishment of SSHv2 key establishment. For SSHv2, RSA and ECDSA host keys are supported.</p> <p>The TOE provides cryptographic signature services using ECDSA that meets ISO/IEC 14888-3, Section 6.4 with NIST curves P-256, P-384 and P-521.</p>
FCS_COP.1/Hash	<p>The TOE provides cryptographic hashing services using SHA-1, SHA-256, SHA-384, and SHA-512 as specified in ISO/IEC 10118-3:2004.</p> <p>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.</p>
FCS_COP.1/KeyedHash	<p>The TOE provides keyed-hashing message authentication services using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512, key size 160, 256, 384, 512 bits, and message digest sizes 160, 256, 384, 512 as specified in ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.</p> <p>Through the implementation of the CAVP validated cryptographic module, the TOE provides SHS hashing and HMAC message authentication in support of SSHv2 and TLSv1.2 for secure communications. Management of the cryptographic algorithms is provided through the CLI with auditing of those commands. SHS hashing and HMAC message authentication (SHA-1) is used in the establishment of TLS and SSHv2 sessions.</p>
FCS_RBG_EXT.1	<p>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-platform based noise source.</p> <p>The deterministic RBG is seeded with a minimum of 256 bits of entropy, which is at least equal to the greatest security strength of the keys and hashes that it will generate.</p>

TOE SFR	How the SFR is Met
FCS_SSHS_EXT.1	<p>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 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 of data is transmitted or an hour has passed. Both of these thresholds are checked by the TOE and a rekeying is performed on whichever threshold is reached first.</p> <p>SSHv2 connections will be dropped if the TOE receives a packet larger than 262126 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, ecdh-sha2-nistp256, ecdh-sha2-nistp384 and ecdh-sha2-nistp521 are the only allowed methods within the evaluated configuration. Any session where the SSH client offers only non-compliant algorithms or key sizes per the NDcPP will be rejected by the SSH server. SSH sessions can only be established when compliant algorithms and key sizes can be negotiated.</p> <p>The TOE implementation of SSHv2 supports the following:</p> <ul style="list-style-type: none"> <li>• public key algorithms for authentication: <i>rsa-sha2-256, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521.</i></li> <li>• password-based authentication for administrative users accessing the TOE's CLI through SSHv2.</li> <li>• encryption algorithms, <i>aes128-ctr, aes256-ctr, AEAD_AES_128_GCM, AEAD_AES_256_GCM</i> to ensure confidentiality of the session.</li> <li>• hashing algorithms <i>hmac-sha1, hmac-sha2-256, hmac-sha2-512, AEAD_AES_128_GCM and AEAD_AES_256_GCM</i> to ensure the integrity of the session.</li> <li>• SSH transport implementation public key algorithms: <i>rsa-sha2-256, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp52.</i></li> </ul> <p>Please refer to Table 4 for all the CAVP references.</p>

FCS_TLSC_EXT.1	<p>The TOE supports TLS v1.2 to protect the sessions to the remote audit server.</p> <p>TLS is also used to protect the TLS sessions with the TOE, which supports the mandatory ciphersuite as well as the following optional ciphersuite:</p> <ul style="list-style-type: none"><li>• TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268</li><li>• TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268</li><li>• TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268</li><li>• TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268</li><li>• TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492</li><li>• TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492</li><li>• TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492</li><li>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492</li><li>• TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246</li><li>• TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246</li><li>• TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246</li><li>• TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246</li><li>• TLS_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288</li><li>• TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288</li><li>• TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288</li><li>• TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288</li><li>• TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289</li><li>• TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289</li><li>• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289</li><li>• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289</li><li>• TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289</li><li>• TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289</li></ul> <p>The following NIST curves are supported by default on the TOE: secp256r1, secp384r1. No administrator configuration is required in order to use these curves.</p> <p>The TOE will only establish a connection if the peer presents a valid certificate during the handshake.</p> <p>Where the TOE is the client, such as connecting to the remote syslog server, the handshake above is the same process except the server (remote syslog server) would not request the client certificate in the Server Hello, see the following:</p>
----------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------





TOE SFR	How the SFR is Met
<p>FIA_UIA_EXT.1 FIA_UAU_EXT.2</p>	<p>The TOE requires all users to be successfully identified and authenticated before allowing any TSF mediated actions to be performed except for the login warning banner that is displayed prior to user authentication.</p> <p>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 user name 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.</p> <p>The TOE provides a local password based authentication mechanism for authentication of authorized administrators.</p> <p>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.</p> <p>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.</p>
<p>FIA_UAU.7</p>	<p>When a user enters their password at the local console or via SSHv2, the TOE displays no characters so that the user password is obscured.</p>
<p>FIA_X509_EXT.1/Rev FIA_X509_EXT.2</p>	<p>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections.</p> <p>The TOE uses X.509v3 certificates as defined by RFC 5280 to support authentication for TLS connections. The certificate validation checking takes place during the TLS session setup.</p> <p>The certificates for trustchain, RootCA’s and SubCA’s are imported onto the TOE via copy and paste.</p> <p>For certificate revocation, OSCP is used.</p> <p>Checking is also done for the basicConstraints extension and the CA flag to determine whether they are present and set to TRUE. The local certificate that was imported must contain the basic constraints extension with the CA flag set to true, the check also ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set. If they are not, the certificate is not accepted. Only one certificate is imported since the only device is a syslog server, so the TOE chooses this certificate.</p> <p>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.</p>

TOE SFR	How the SFR is Met
<p>FMT_MOF.1/ManualUpdate</p> <p>FMT_MTD.1/CoreData</p> <p>FMT_MTD.1/CryptoKeys</p>	<p>The TOE provides administrative users with a CLI to interact with and manage the security functions of the TOE.</p> <p>The term “Authorized Administrator” is used in this ST to refer to any user which has been assigned to a privilege level that is permitted to perform the relevant action; therefore, has the appropriate privileges to perform the requested functions. Therefore, semi-privileged administrators with only a subset of privileges may also manage and modify TOE data based on the privileges assigned.</p> <p>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 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.</p> <p>Manual software updates can only be done by the authorized administrator through CLI. These updates include software upgrades.</p> <p>The Authorized Administrators can query the software version running on the TOE and can initiate updates to (replacements of) software images. When software updates are made available by Cisco, the Authorized Administrators can obtain, verify the integrity of, and install those updates.</p> <p>The TOE provides the ability for Authorized Administrators to manage the cryptographic keys.</p>

TOE SFR	How the SFR is Met
FMT_SMF.1	<p>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.</p> <p>The management functionality provided by the TOE includes the following administrative functions:</p> <ul style="list-style-type: none"> <li>• Local and remote administration of the TOE and the services provided by the TOE via the TOE CLI, as described above;</li> <li>• The ability to manage the warning banner message and content which allows the Authorized Administrator the ability to define warning banner that is displayed prior to establishing a session (note this applies to the interactive (human) users; e.g. administrative users;</li> <li>• The ability to manage the time limits of session inactivity which allows the Authorized Administrator the ability to set and modify the inactivity time threshold;</li> <li>• The ability to update the NX-OS software. The validity of the image is provided using hash comparison prior to installing the update;</li> <li>• The ability to configure the authentication failure parameters for FIA_AFL.1.</li> <li>• The ability to manage termination of a local session due to exceeding the threshold of authentication failure attempts. The account is locked until an Authorized Administrator defined time period has elapsed;</li> <li>• The ability to manage audit behavior and the audit logs which allows the Authorized Administrator to view the audit logs and to clear the audit logs;</li> <li>• The ability to manage the cryptographic functionality which allows the Authorized Administrator the ability to identify and configure the algorithms used to provide protection of the data, such as generating the RSA keys to enable SSHv2 and to configure thresholds for SSH rekeying;</li> <li>• The ability to configure and set the time clock;</li> <li>• The ability to configure the reference identifier for the peer;</li> <li>• The ability to import X.509v3 certificates to the TOE'S trust store.</li> </ul> <p>In addition, the warning and access banner may also be displayed prior to the identification and authentication of an Authorized Administrator. No administrative functionality is available prior to administrative login;</p>
FMT_SMR.2	<p>The TOE platform maintains both privileged and semi-privileged administrator roles.</p> <p>The TOE performs role-based authorization, using TOE platform authorization mechanisms, to grant access to the privileged and semi-privileged roles. For the purposes of this evaluation, the privileged role is equivalent to full administrative access to the CLI, which is the default access for NX-OS privilege level 15; and the semi-privileged role equates to any privilege level that has a subset of the privileges assigned to level 15. Privilege levels 0 and 1 are defined by default and are customizable, while levels 2-14 are undefined by default and also customizable. Note: the levels are not theoretically hierarchical.</p> <p>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.</p> <p>The TOE supports both local administration via a directly connected console and remote authentication via SSH.</p>

TOE SFR	How the SFR is Met
<p>FPT_SKP_EXT.1 and FPT_APW_EXT.1</p>	<p>The TOE stores all private keys in a secure directory that is not readily accessible to administrators. All pre-shared and symmetric keys are stored in encrypted form using AES encryption to additionally obscure access. This functionality is configured on the TOE using the 'feature password encryption aes' command.</p> <p>Passwords must be configured to be in encrypted format. The TOE encrypts clear text passwords before saving them to the running configuration. Encrypted format passwords are saved to the running configuration without further encryption. SHA256 is the hashing algorithm used for password encryption. The command is 'username <i>user-id</i> [password [5] <i>password</i>] [expire <i>date</i>] [role <i>role-name</i>]'. </p> <p>All passwords are stored in encrypted form in /etc/shadow to prevent access. In this manner, the TOE ensures that plaintext user passwords will not be disclosed even to administrators.</p> <p>Refer to the Common Criteria Operational User Guidance and Preparative Procedures for command description and usage information.</p>
<p>FPT_STM_EXT.1</p>	<p>The TOE provides a hardware based system clock which tracks inactivity of administrative sessions and generates the time stamp that is applied to TOE audit records. Administrators can manually configure the time from within configuration exec mode via the privileged mode operation of the TOE.</p> <p>The hardware based system clock (time source) is also used for the SSH rekey time threshold.</p>

FPT_TST_EXT.1	<p>The TOE is designed to runs the suite of power-on self-tests that comply with the FIPS140-2 requirements for self-test (eg 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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• 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.</li> <li>• <i>KAS ECC KAT</i> - Also known as the 'ECC Primitive "Z" KAT', the KAT shall be performed on the point multiplication for the ECC-based protocol.</li> <li>• <i>KAS FFC KAT</i> - Also known as the 'FFC Primitive "Z" KAT', the KAT shall be performed on the underlying mathematical function(s) which use modular exponentiation for an FFC-based key establishment protocol.</li> <li>• <i>SP 800-56B RSA key wrap/unwrap KAT</i> - The module has an RSA encryption pre-computed and then, while performing a power-up self-test, the module performs the RSA encryption again and compares the newly-generated result to the pre-computed value. The module also has a separate known answer for the RSA decryption by starting with a given value representing an RSA encryption and decrypting this value using the RSA algorithm. The result of said decryption operation is compared to a pre-computed result.</li> <li>• Firmware Integrity Test - the software integrity test ensures the correct operation of the device and its components.</li> </ul> <p>Conditional Self-Tests (run periodically during normal operation):</p> <ul style="list-style-type: none"> <li>• <i>Continuous Random Number Generator test for DRBG</i> - - The first n-bit block generated after power-up, initialization, or reset shall not be used, but shall be saved for comparison with the next n-bit block to be generated. Each subsequent generation of an n-bit block shall be compared with the previously generated block. The test shall fail if any two compared n-bit blocks are equal.</li> <li>• <i>Continuous Random Number Generator test for Entropy Source</i> -- This test functions precisely the same as the CRNGT for the DRBG (described above) except that input to the test is taken from the Entropy Source output as opposed to the DRBG output.</li> <li>• <i>RSA Pairwise Consistency Test</i> - Each time a new RSA public/private keypair is generated, the public key is used to encrypt a plaintext value. The resulting ciphertext value is then compared to the original plaintext value. If the two values are equal, then the test is considered to have failed. If the two values differ, then the private key is used to decrypt the ciphertext and the resulting value is then compared to the</li> </ul>
---------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

TOE SFR	How the SFR is Met
	<p>original plaintext value. If the two values are not equal, the test is considered to have failed.</p> <p>If any component reports failure for the POST, the system crashes and appropriate information is displayed on the screen and saved in the crashinfo file.</p> <p>All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic.</p> <p>These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected.</p>
FPT_TUD_EXT.1	<p>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 actually update the applicable TOE components. Once the file is downloaded from the Cisco.com web site, and upon installation of a TOE update, a digital signature verification check will automatically be performed to ensure it has not been modified since distribution. The authorized source for the digitally signed updates is "Cisco Systems, Inc."</p> <p>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).</p> <p>Detailed instructions for how to verify the hash value are provided in the administrator guidance for this evaluation.</p>

FTA_SSL_EXT.1	<p>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. When a session is inactive (i.e., no session input from the administrator) for the configured period of time the TOE will terminate the session, and no further activity is allowed requiring the administrator to log in (be successfully identified and authenticated) again to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require authentication to establish a new session.</p> <p>The allowable inactivity timeout range is from 1 to 65535 seconds. Administratively configurable timeouts are also available for the EXEC level access (access above level 1) through use of the “exec-timeout” setting.</p>
FTA_SSL.3	
FTA_SSL.4	<p>An administrator can manually logout from the evaluated configuration either from the local console or remotely with the following command: “exit”.</p>
FTA_TAB.1	<p>The TOE displays a privileged Administrator customizable 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.</p>
FTP_ITC.1	<p>The TOE protects communications with the external audit server using TLS to secure the communications channel. This protects the data from disclosure by encryption and by checksums that verify that data has not been modified.</p> <p>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.</p>
FTP_TRP.1/Admin	<p>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.</p>



## 7. Annex A: Key Zeroization

The table below describes the key zeroization referenced by FCS\_CKM.4 provided by the TOE.

**Table 20. 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.	CLI command zeroize RSA  Command: crypto key zeroize  verify with command: show crypto key mypubkey all  Zeroized by overwriting with new key

Name	Description	Zeroization
TLS server public key	This key is used to encrypt the data that is used to compute the secret key. The public key used for SSLv3.1/TLS secure connection. The key is stored in NVRAM.	CLI command zeroize RSA  Command: crypto key zeroize  verify with command: show crypto key mypubkey all  Zeroized by overwriting with new key
TLS pre-master secret	The pre-master secret is the client and server exchange of random numbers and a special number, the pre-master secret, this pre-master secret is using asymmetric cryptography from which new TLS session keys can be created. 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: References

The documentation listed below was used to prepare this ST.

**Table 21. References**

Identifier	Description
[CC_PART1]	Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-001
[CC_PART2]	Common Criteria for Information Technology Security Evaluation – Part 2: Security functional components, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-002
[CC_PART3]	Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-003
[CEM]	Common Methodology for Information Technology Security Evaluation – Evaluation Methodology, dated April 2017, version 3.1, Revision 5, CCMB-2017-04-004
[NDcPPv2.2e]	collaborative Protection Profile for Network Devices, version 2.2e, March 23, 2020
[SD]	Supporting Document – Evaluation Activities for Network Device cPP, version 2.2, December 2019
[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

## 9. Annex C: Acronyms and Terms

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

**Table 22. Acronyms and Terms**

Acronym/Term	Definition
AAA	Administration, Authorization, and Accounting
ACL	Access Control Lists
AES	Advanced Encryption Standard
AES-CCM	AES Counter with CBC-MAC
AP	Access Point
Authorized Administrator	Any user which has been assigned to a privilege level that is permitted to perform all TSF-related functions.
BRI	Basic Rate Interface
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria for Information Technology Security Evaluation
CEM	Common Evaluation Methodology for Information Technology Security
CM	Configuration Management
DHCP	Dynamic Host Configuration Protocol
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
ISDN	Integrated Services Digital Network
IT	Information Technology
KCK	Key Confirmation Key
KEK	Key Encryption Key
MIC	Message Integrity Check
ND	Network Device

NDcPP	collaborative Network Device Protection Profile
OS	Operating System
Peer switch	Another switch on the network that the TOE interfaces with.
PMK	Pairwise Master Key
PoE	Power over Ethernet
PRF	Pseudo-random function
PP	Protection Profile
PTK	Pairwise Transient Key
RSN	Robust Security Network
SA	Security Association
Security Administrator	Synonymous with Authorized Administrator for the purposes of this evaluation.
SFP	Small-form-factor pluggable port
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SSHv2	Secure Shell (version 2)
SSID	Service Set Identifier
ST	Security Target
Supplicant	The client software used for WLAN authentication
TCP	Transport Control Protocol
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
UDP	User datagram protocol
VM	Virtual Machine
vND	Virtual Network Device
VPN	Virtual Private Network
VS	Virtualisation System
WAN	Wide Area Network
WIC	WAN Interface Card

## 10 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.

### 10.1 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](http://www.cisco.com/go/offices).

---

<sup>i</sup> While tested on the Intel Xeon (Broadwell) D-1526, any Intel® Xeon® D-15xx (Broadwell) processor may be used as part of the evaluated configuration.