

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

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

Report Number: CCEVS-VR-VID11173-2021
Dated: November 12, 2021
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort. Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

Patrick Mallett, Ph.D.
Jerome Myers, Ph.D.
The Aerospace Corporation

Common Criteria Testing Laboratory

Cody Cummins
Shahid Islam
Katie Sykes
Gossamer Security Solutions
Columbia, MD

Table of Contents

1	Executive Summary	1
2	Identification	2
3	Architectural Information	3
3.1	TOE Evaluated Configuration	3
3.2	TOE Architecture	3
3.3	Physical Boundaries	5
4	Security Policy	10
4.1	Security audit	10
4.2	Cryptographic support	10
4.3	Identification and authentication	10
4.4	Security management	11
4.5	Protection of the TSF	11
4.6	TOE access	11
4.7	Trusted path/channels	11
5	Assumptions	11
5.1	Clarification of Scope	12
6	Documentation	12
7	Product Testing	13
7.1	Developer Testing	13
7.2	Evaluation Team Independent Testing	13
8	Evaluated Configuration	13
9	Results of the Evaluation	13
9.1	Evaluation of the Security Target (ASE)	13
9.2	Evaluation of the Development (ADV)	14
9.3	Evaluation of the Guidance Documents (AGD)	14
9.4	Evaluation of the Life Cycle Support Activities (ALC)	14
9.5	Evaluation of the Test Documentation and the Test Activity (ATE)	14
9.6	Vulnerability Assessment Activity (VAN)	14
9.7	Summary of Evaluation Results	15
10	Validator Comments/Recommendations	16
11	Annexes	16
12	Security Target	16
13	Glossary	16
14	Bibliography	17

1 Executive Summary

The evaluation of Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 was performed by Gossamer Security Solutions, in the United States and was completed in November 2021. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Gossamer Security Solutions determined that the product satisfies evaluation assurance level “EAL 1” as defined within the Common Criteria (CC). The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the *Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 Security Target, Version 1.0, October 22, 2021*.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and versions of the ETR. Also, at some discrete points during the evaluation, validators formed a Validation Oversight Review panel in order to review the Security Target and other evaluation evidence materials along with the corresponding evaluation findings in detail. The validation team found that the evaluation showed that the product satisfies all of the security functional and assurance requirements stated in the Security Target (ST). Therefore, the validation team concludes that the testing laboratory’s findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 Security Target, Version 1.0, October 22, 2021* produced by Cisco.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020
ST	Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 Security Target, Version 1.0, October 22, 2021
Evaluation Technical Report	Evaluation Technical Report for Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 version 1.1, 11/09/2021
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	Cisco Systems, Inc
Developer	Cisco Systems, Inc
Common Criteria Testing Lab (CCTL)	Gossamer Security Solutions, Inc. Columbia, MD
CCEVS Validators	Patrick Mallett, Jerome Myers

3 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

The Target of Evaluation (TOE) is the Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3. The Cisco Nexus 3000 and 9000 Series Switches in standalone mode are purpose-built data center-class switches for use as an aggregation switch in the data center.

3.1 TOE Evaluated Configuration

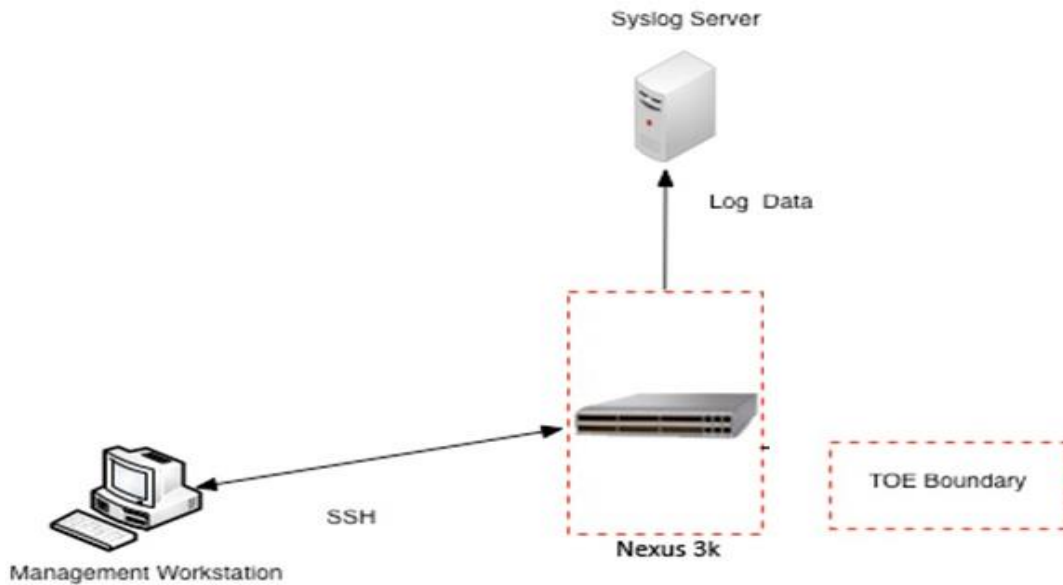
Detail regarding the evaluated configuration is provided in Section 8 below.

3.2 TOE Architecture

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 software is comprised of the NX-OS software image Release 9.3. 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.

Figure 1. Cisco Nexus 3000 and Environment

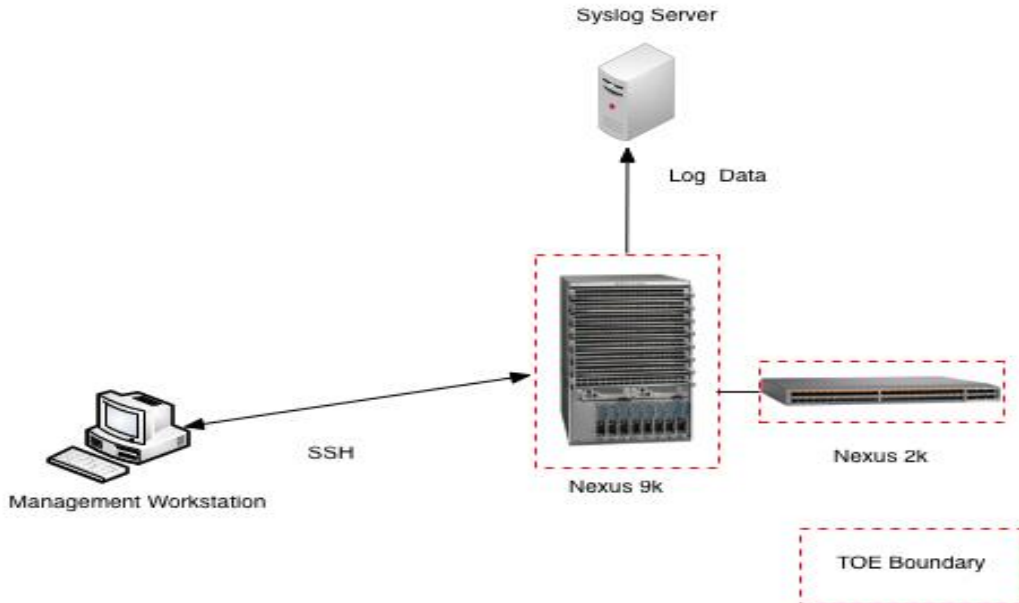


The previous figure includes the following:

- 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


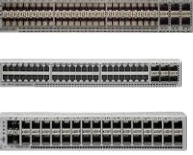


For management purposes the TOE provides command line access to administer the TOE.

3.3 Physical Boundaries

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 1 below.





Table 1 Hardware Models and Specifications

Hardware Platform	Model	External Identification	Description	Interfaces
Cisco 3100 Models				
Cisco Nexus 3100 Series	Nexus 3172PQL	N3K-C3172PQ-10GE		<ul style="list-style-type: none"> • Management ports: 1 RJ-45


	Nexus 3172PQ-XL	N3K-C3172PQ-XL	72 x 10 Gigabit Ethernet ports (48 SFP+ ¹ and 6 QSFP+)	<ul style="list-style-type: none"> • Console serial port: 1 RS-232 connector • USB ports (1)
	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				
Cisco Nexus 3100V Series 	Nexus 31108PC-V	N3K-C31108PC-V	48 x 10-Gbps SFP+ ports and 6 x QSFP28 ² ports (all QSFP ports can operate at 40 or 100 Gbps)	<ul style="list-style-type: none"> • Management ports: 1 RJ-45 • Console serial port: 1 RS-232 connector • USB ports (1)
	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				
Cisco Nexus 3100Z Series 	Nexus 3132C-Z	N3K-C3132C-Z	32 fixed 100-Gigabit Ethernet QSFP28 ports	<ul style="list-style-type: none"> • Management ports: 1 RJ-45 • Console serial port: 1 RS-232 connector • USB ports (1) • 10-Gbps SFP port (2)
Cisco 3200 Models				
Cisco Nexus 3200 Series 	Nexus 3232C	N3K-C3232C	32 fixed 100 Gigabit Ethernet QSFP28 ports	<ul style="list-style-type: none"> • Management ports: 1 RJ-45 • Console serial port: 1 RS-232 connector • USB ports (2)
	Nexus 3264C-E	N3K-C3264C-E	64 fixed 100-Gigabit Ethernet QSFP28 ports	
Cisco 3400 Models				
Cisco Nexus 3400 Series	Nexus 34180-YC	N3K-C34180YC	48 x SFP+/SFP28 and 6 x QSFP+/QSFP28 ports	<ul style="list-style-type: none"> • Management ports: 1 RJ-45, 1 SFP


¹ SFP+ - Enhanced Small Form-Factor Pluggable

² QSFP28 - Quad Small Form-Factor Pluggable

	Nexus 3464C	N3K-C3464C	64 x QSFP+/QSFP28 ports and 2 x SFP+	<ul style="list-style-type: none"> • Console serial port: 1 RS-232 connector • USB ports (1)
	Nexus 3432D-S	N3K-C3432D-S	32 fixed 400-Gigabit Ethernet QSFP-DD ³ ports	
	Nexus 3408-S	N3K-C3408-S	4RU, 8-slot chassis. 128 ports of 100G or 32 ports of 400G.	
Cisco 3500 Models				
	Nexus 3524-X	N3K-C3524P-10GX	48 fixed SFP+ ports (1 or 10 Gbps); the Cisco Nexus 3524-X enables only 24 ports	<ul style="list-style-type: none"> • Management ports: 2 RJ-45 • Console serial port: 1 RS-232 connector • USB ports (1)
	Nexus 3524-XL	N3K-C3524P-XL	48 fixed SFP+ ports (1 or 10 Gbps); the Cisco Nexus 3524-XL enables only 24 ports	
	Nexus 3548-X	N3K-C3548P-10GX	48 fixed SFP+ ports (1 or 10 Gbps); the Cisco Nexus 3524-X 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"> • Management ports: 1 RJ-45 • Console serial port: 1 RS-232 connector • USB ports (1)
	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"> • Management ports: 1 RJ-45, 1 SFP+ • Console serial port: 1 RJ-45 • USB ports (1)
	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	

³ QSFP-DD – Quad Small Form-factor pluggable Double Density

	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"> Management ports: 1 RJ-45 Console serial port: 1 RJ-45 USB ports (2)
	Nexus 93108TC-FX	N9K-C93108TC-FX	48 x 100M/1/10GBASE-T ports and 6 x 40/100-Gbps QSFP28 ports	<ul style="list-style-type: none"> Management ports: 1 RJ-45 and 1 SFP+ Console serial port: 1 RJ-45 USB ports (1)
	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"> Management ports: 1 RJ-45 Console serial port: 1 RJ-45 USB ports (1)
	Nexus 93216TC-FX2	N9K-C93216TC-FX2	96 x 100M/1/10GBASE-T ports and 12 x 40/100-Gigabit QSFP28 ports	<ul style="list-style-type: none"> Management ports: 1 RJ-45 Console serial port: 1 RJ-45 USB ports (2)
	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"> Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)
	Nexus 93180YC-FX	N9K-C93180YC-FX	48 x 1/10/25-Gbps fiber ports and 6 x 40/100-Gbps QSFP28 ports	<ul style="list-style-type: none"> Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)
	Nexus 93240YC-FX2	N9K-C93240YC-FX2	48 x 1/10/25-Gbps fiber ports and 12 x 40/100-Gbps QSFP28 ports	<ul style="list-style-type: none"> Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)
	Nexus 93360YC-FX2	N9K-C93360YC-FX2	96 x 1/10/25-Gbps fiber ports and 12 x 40/100-Gbps QSFP28 ports	<ul style="list-style-type: none"> Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)
	Nexus 9364C	N9K-C9364C	64-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports	<ul style="list-style-type: none"> Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)
	Nexus 9332C	N9K-C9332C	32-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports	<ul style="list-style-type: none"> Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)
	Nexus 9336C-FX2	N9K-C9336C-FX2	36 x 40/100-Gbps QSFP28 ports	<ul style="list-style-type: none"> Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)
	Nexus 9364C-GX	N9K-C9364C-GX	64 x 100/40-Gbps Quad Small Form-Factor Pluggable (QSFP28)	<ul style="list-style-type: none"> Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)
	Nexus 9316D-GX	N9K-C9316D-GX	16 x 400/100-Gbps QSFP-DD ports	<ul style="list-style-type: none"> Management ports: 2 (1 x 10/100/1000BASE-T and 1 x 1-Gbps SFP+) Console serial port: 1 RJ-45 USB ports (1)

	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				
<p>Cisco Nexus 9500 Series</p> 	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"> Based on Supervisor and I/O modules installed)
	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"> Management ports: 1 RJ-45 Console serial port: 1 RJ-45 USB ports (2)
	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"> Management ports: 1 RJ-45 Console serial port: 1 RJ-45 USB ports (2)
	Supervisor 9500-Sup-B +	N9K-SUP-B+	Six cores/12-Thread, 1.9 GHz, 24 GB of memory, and 256 GB of SSD ⁴ (N9K-SUP-B+)	
	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	<ul style="list-style-type: none"> Not applicable

⁴ SSD – Solid-state Drive

			supervisors, fabric modules, and line cards.	
--	--	--	--	--

4 Security Policy

The TOE enforces the following security policies as described in the ST:

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

4.1 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.

4.2 Cryptographic support

The TOE provides cryptography in support of other TOE security functionality. All the algorithms claimed have CAVP certificates (Operational Environment –Intel Xeon processor). The TOE leverages the Cisco FIPS Object Module (FOM) 6.2 certificate and has been validated for conformance to the requirements of FIPS140-2 140-2 Level 1.

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.

4.3 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.

4.4 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.

4.5 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.

4.6 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.

4.7 Trusted path/channels

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

5 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 (NDcPP22e)

That information has not been reproduced here and the NDcPP22e should be consulted if there is interest in that material.

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP22e as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

5.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made with a certain level of assurance (the assurance activities specified in Protection Profile for Network Devices and performed by the evaluation team).
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process.
- This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The functionality evaluated is scoped exclusively to the security functional requirements specified in the NDcPP22e and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

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.

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

6 Documentation

The guidance documentation examined during the course of the evaluation and therefore delivered with the TOE is as follows:

- Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 Common Criteria Operational User Guidance and Preparative Procedures, Version 1.0, September 7, 2021

Only the Administrator Guide listed above the specific sections of any other documents referenced by that guide should be trusted for the installation, administration, and use of this product in its evaluated configuration.

7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the Assurance Activity Report (NDcPP22e) for Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 Version 1.1, 11/09/2021 (AAR).

7.1 Developer Testing

No evidence of developer testing is required in the assurance activities for this product.

7.2 Evaluation Team Independent Testing

The evaluation team verified the product according a Common Criteria Certification document and ran the tests specified in the NDcPP22e including the tests associated with optional requirements. The specific test configurations and test tools utilized may be found in Section 3.4 of the AAR.

8 Evaluated Configuration

The TOE is comprised of both software and hardware when configured in accordance with the documentation specified in section 6. 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.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary ETR. The reader of this document can assume that all assurance activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 5 and CEM version 3.1 rev 5. The evaluation determined the Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 TOE to be Part 2 extended, and to meet the SARs contained in the NDcPP22e.

9.1 Evaluation of the Security Target (ASE)

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 products that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team applied each ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security target and Guidance documents. Additionally, the evaluator performed the assurance activities specified in the NDcPP22e related to the examination of the information contained in the TSS.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team applied each AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. All of the guides were assessed during the design and testing phases of the evaluation to ensure they were complete.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team applied each ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team applied each ATE CEM work unit. The evaluation team ran the set of tests specified by the assurance activities in the NDcPP22e and recorded the results in a Test Report, summarized in the AAR.

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (VAN)

The evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the Detailed Test Report (DTR) prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities and fuzz testing. Neither the public search for vulnerabilities nor the fuzz testing uncovered any residual vulnerability.

The evaluation team performed a public search for vulnerabilities in order to ensure there are no publicly known and exploitable vulnerabilities in the TOE from the following sources:

- National Vulnerability Database (<https://web.nvd.nist.gov/vuln/search>)
- Vulnerability Notes Database (<http://www.kb.cert.org/vuls/>)
- Rapid7 Vulnerability Database (<https://www.rapid7.com/db/vulnerabilities>)
- Tipping Point Zero Day Initiative (<http://www.zerodayinitiative.com/advisories>)
- Exploit / Vulnerability Search Engin (<http://www.exploitsearch.net>)
- SecurITeam Exploit Search (<http://www.securiteam.com>)
- Tenable Network Security (<http://nessus.org/plugins/index.php?view=search>)
- Offensive Security Exploit Database (<https://www.exploit-db.com/>)

The search was performed on 10/20/2021 with the following search terms:

- "NX-OS 9.3"
- "Cisco Nexus"
- "Nexus 3000"
- "Nexus 9000"
- "3000"
- "3100"
- "3100v"
- "3100z"
- "3200"
- "3400"
- "3500"
- "3600"
- "9300"
- "9500"
- "Intel Pentium B925C"
- "Intel i3-3115C"
- "Intel Xeon D-1500"
- "Intel Xeon E5-2400"
- "Intel Xeon E3-1105C"
- "Cisco FOM "

The validator reviewed the work of the evaluation team, and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's testing also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 Common Criteria Operational User Guidance And Preparative Procedures, Version 1.0, September 7, 2021 document. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. Other functionality provided by devices in the operational environment, such as the syslog server, need to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Annexes

Not applicable.

12 Security Target

The Security Target is identified as: Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 Security Target, Version 1.0, October 22, 2021.

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.

- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

- [1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 5, April 2017.
- [2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 5, April 2017.
- [3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 5, April 2017.
- [4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.
- [5] collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 (NDcPP22e)
- [6] Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3 Security Target, Version 1.0, October 22, 2021.
- [7] Assurance Activity Report for Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3, Version 1.1, 11/09/2021 (AAR).
- [8] Detailed Test Report for Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3, Version 1.1, 11/09/2021 (DTR).
- [9] Evaluation Technical Report for Cisco Nexus 3000 and 9000 Series Switches running on NX-OS 9.3, Version 1.1, 11/09/2021 (ETR).