Certification Report

Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders, v7.0(3)I5(1)

Sponsor and developer: ***Cisco Systems Inc.***
170 West Tasman Dr.
San Jose, CA 95134
USA

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Reportnumber: **NSCIB-CC-93012-CR**

Report version: **1**

Projectnumber: **93012**

Authors(s): **Denise Cater**

Date: 13 June 2017

Number of pages: **20**

Number of appendices: **1**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**CC-17-93012**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Cisco Systems Inc.** **170 West Tasman Dr., San Jose, CA 95134 USA**
Product and assurance level	**Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders, v7.0(3)I5(1),** Assurance Package: ▪ EAL2
Project number	**NSCIB-CC-93012**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of issue	: **15-06-2017**
	Certificate expiry	: **15-06-2022**

Registration number

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands.

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

TÜVRheinland®
Precisely Right.

CONTENTS:

TÜVRheinland®
Precisely Right.

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

A part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or sitecomplies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements stated in the (site) security target.

TÜVRheinland®
Precisely Right.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate would indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 8 September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders, v7.0(3)I5(1). The developer of the Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders is Cisco Systems Inc. located in San Jose, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders offer both modular (9500 switches) and fixed (9300 switches) 1,10, 40, and 100 Gigabit Ethernet (GE) configurations designed to operate in one of two modes providing Data Center Ethernet (DCE):

- Cisco NX-OS mode for traditional architectures and consistency across the Cisco Nexus portfolio
- ACI mode to take full advantage of the policy-focused services and infrastructure automation features of the Cisco Application Centric Infrastructure (ACI)

In addition to the Nexus 9000 Series Switches, the solution provided by the TOE includes the Cisco Nexus 2000 Series Fabric Extenders, and the NX-OS software. The TOE can be deployed with the Nexus 9k or together with the Nexus 2000 Fabric Extender. In this Common Criteria Evaluation the TOE will be in standalone mode using NX-OS with Nexus 2000 Fabric Connector (FEX). The Nexus 2000 FEX is an optional component.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on June 09 2017 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the EAL2 (EAL2) assurance requirements for the evaluated security functionality.

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders, v7.0(3)I5(1) evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders, v7.0(3)I5(1) from Cisco Systems Inc. located in San Jose, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Nexus 9300 switches (9332PQ, 9372PX, 9372PX-E, 9372TX, 9372TX-E, 9396PX, 9396TX, 93120TX, 93128TX, 93180YC-EX, 93108TC-EX) and Nexus 9500 switches (9504, 9508, 9516) with Supervisor A or Supervisor B, and optionally Nexus 2000 Fabric Extenders (2348TQ, 2348UPQ, 2248TP, 2248TP-E, 2232PP, 2248PQ, 2232TM, 2232TM-E). For details of the supported I/O modules see Appendix 1.	n/a
Software	NX-OS	v7.0(3)I5(1)

To ensure secure usage a set of guidance documents is provided together with the Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders. Details can be found in section 2.5 of this report.

2.2 Security Policy

The major security features provided by the TOE are:

- The TOE can audit events related to cryptographic functionality, identification and authentication, enforcement of information flow control policies and administrative actions. Each security relevant audit event has the date, timestamp, event description, and subject identity. The authorized administrator configures auditable events, performs back-up operations, and manages audit data storage. The TOE provides the administrator with a circular audit trail. Logs are written to DRAM, NVRAM, and flash.
- The TOE provides cryptography in support of other Cisco 9K security functionality and to support remote management via SSHv2. The cryptographic services provided by the TOE are:

Cryptographic Method	Use within the TOE
Secure Shell Establishment	Used to establish initial SSH session
RSA/DSA Signature Services	Used in SSH session establishment.
SHA-1	Used to provide SSH traffic integrity verification
AES CTR, ECB, GMAC (128, 192, 256)	Used to encrypt SSH session traffic.
HMAC	Used for keyed hash, integrity services in SSH session establishment. Cryptographic algorithm used to authenticate the RADIUS message. Cryptographic algorithm used to authenticate the PAC authentication

- The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Packets are padded with zeros. Residual data is never transmitted from the TOE.
- The TOE performs user authentication for the Authorized Administrator of the TOE. The TOE provides authentication services for administrative users to connect to the TOE's secure administrator interfaces. 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 as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password-based authentication can be performed on the local serial port referred to as the management port on the Nexus switches. In addition, password-based authentication can be performed when connecting to the TOE CLIs remotely using SSHv2. The SSHv2 interface also supports authentication using SSH keys. The TOE supports use of a RADIUS or TACACS+ AAA server (part of the IT Environment) to facilitate authentication (including single-use authentication, or password-based authentication) and authorization (roles) for administrative users attempting to connect to the TOE's CLI. When the role is defined via the CLI on the TOE it is sent to the RADIUS server using Vendor Specific Attributes (VSA).
- The TOE provides the ability to control traffic flow into or out of the Nexus 9000 switch. The following types of traffic flow are controlled for both IPv4 and IPv6 traffic:
  - Layer 3 Traffic – RACLs
  - Layer 2 Traffic – PACLs
  - VLAN Traffic – VACLs
  - Virtual Routing and Forwarding - VRFs
- 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. Cisco NX-OS devices use role-based access control (RBAC). To enable both types of devices to be administered by the same TACACS+ servers, an authorized administrator can map the privilege. levels configured on TACACS+ servers to user roles configured on Cisco NX-OS devices. The Nexus 9000 Series switch supports the following predefined roles:
  - network-admin – This role is a super administrative role. This role has read and write privileges for any configuration item on the Nexus 9000 Series.
  - network-operator - This role has read access to the entire Cisco NX-OS device.
- The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration and access to Authorized Administrators. The TOE prevents reading of cryptographic passwords. Use of separate VLANs is used to ensure routing protocol communications between the TOE and neighbour switches including routing table updates and neighbour switch authentication will be logically isolated from traffic on other VLANs.
- The administrator can terminate their own session by exiting out of the CLI. The TOE can also be configured to display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.
- The TOE allows trusted paths to be established to itself from remote administrators over SSHv2 for remote CLI access.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

Detailed information on the assumption and threats can be found in the *[ST]* sections 3.1 and 3.2 respectively. Detailed information on the security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

2.4 Architectural Information

The general architecture consists of three subsystems:

- The Hardware subsystem providing:
  - hardware clock, CPU, memory, network ports, and interrupts to switch.
  - local storage (NVRAM, DRAM, and FLASH memory) of audit data and other data
  - physical ports
  - self-tests on boot up
- The Cryptographic subsystem providing cryptographic support for:
  - Encrypting of communication with users and other systems (SSH)
  - Hashing of stored passwords
  - Generation and zeroizing cryptographic keys
- The NX-OS subsystem providing all other SFR-related functionality, such as:
  - Security Audit
  - Full Residual Information Protection
  - Information Flow Control
    - Control traffic flow (Packet Filtering)
    - ACL enforcement
  - Identification and Authentication (I&A)
  - Protection of the TSF
  - TOE Access
  - Security Management
  - Trusted Path/ Channels (the SSH functionality)

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Cisco Nexus 9K Switch Common Criteria Configuration Guide	1.0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer tests consist of eleven (11) tests, some of which were quite extensive. The developer performed these 11 tests on one model of the 9300 series (N9K-9396PX with N2K-C2248TP) and one model of the 9500 series (N9K-C9504 with N2K-C2248TP-E with supervisor A and fabric module N9K-C9504-FM). These tests cover all TSFI and all SFRs and include both positive and negative tests. Brightsight repeated four (4) of the eleven (11) developer tests.

In addition to the developer tests, the evaluator derived and executed nine (9) additional functional tests. Of the 9 tests, all of them were performed on N9K-C9516 and 6 of them were repeated on the N9K-C9372PX to ensure the consistent behaviour between the devices. A hardware rationale was produced to demonstrate equivalency between the various models within each of the hardware series (9500, 9300, 2300 and 2200).

2.6.2 Independent Penetration Testing

The evaluators produced twenty-one (21) penetration tests in total. These were derived from a vulnerability analysis comprised of 3 parts:

1. Public domain vulnerability analysis of TOE specific vulnerabilities (vulnerabilities specific for Cisco 9500/9300/2200/2300 series hardware and NX-OS 7.0(3)I5(1) software);
2. Public domain vulnerability analysis of TOE-type vulnerabilities (vulnerabilities that are generic for routers/switches) and a vulnerability scanning tool was used to identify generic potential vulnerabilities;
3. Analysis of TOE deliverables (AGD, FSP, TDS etc.).

The evaluators considered the potential vulnerabilities in the context of the management plane and the data plane. Of the thirteen (13) penetration tests identified for the Data Plane, ten (10) of them were performed on the N9K-C9516 (with N2K-C2348TQ is applicable), nine (9) of them were performed on the N9K-C9372PX (with N2K-C2232PP-10GE if applicable), and six (6) of them were performed on both devices to ensure the equivalence between the devices.

Of the eight (8) penetration tests identified for the Management Plane, seven (7) tests were performed on the N9K-C9516, five (5) tests were performed on the N9K-C9372PX, and four (4) tests were performed on both devices to ensure the equivalence between the devices.

2.6.3 Test Configuration

The network diagram in Figure 1 describes the overall setup of the lab used for evaluator testing (some tests required additional network components e.g. virtual devices, sniffers, etc).

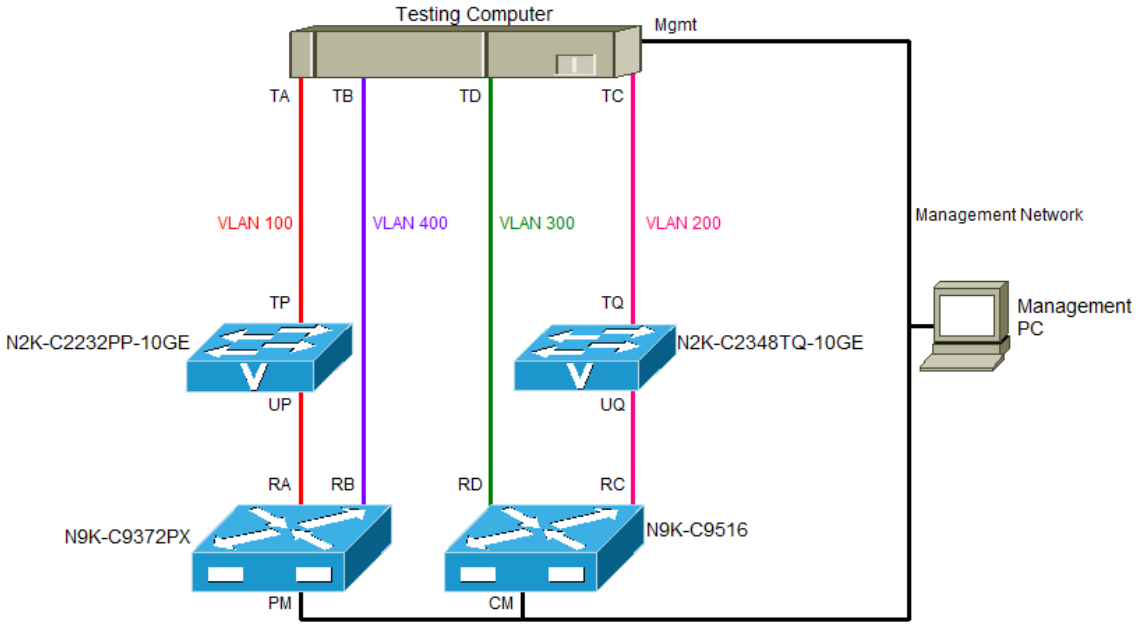

Figure 1 Baseline evaluator test setup

The ports are labelled as follows:

Port	Type	Description
Management PC (Mgmt-PC)		
EH	Ethernet	Management port
N9K-C9516		
CM	Ethernet	SUP-1 Management port
RD	SFP	Ethernet port 1/5 to TD

Port	Type	Description
RC	SFP	Ethernet port 1/1 – 1/4 configured as FEX ports
N2K-C2348TQ-10GE		
UQ	QSFP	Uplink port 1/1 Extends the I/O module managed by N9K-C9516
TQ	Ethernet	Port 122/1/1 and connects to TC
N9K-C9372PX		
PM	Ethernet	Management port
RB	SFP	Ethernet port 1/1 to TB
RA	SFP	Ethernet port 1/2 configured as FEX ports
N2K-C2232PP-10GE		
UP	SFP	Uplink port 1/1 Extends the I/O module managed by N9K-C9372PX
TP	SFP	Port 111/1/1 and connects to TA
Testing Computer		
TA	SFP	TA testing computer
TB	SFP	TB testing computer
TD	SFP	TD testing computer
TC	Ethernet	TC testing computer
Mgmt	Ethernet	Management port

The TOE devices sampled in the evlauator testing were:

Identifier	Product name	Firmware
N9K-C9372PX	Cisco Nexus 9372PX Switch	NX-OS 7.0(3)I5(1)
N9K-C9516	Cisco Nexus 9516 Switch Line card – N9K-X9564PX Fabric module – N9K-C9516-FM System Controller – N9K-SC-A Supervisor module – N9K-SUP-A	NX-OS 7.0(3)I5(1)
N2K-C2232PP -10GE	Cisco Nexus 2232PP Fabric Extender	NX-OS 7.0(3)I5(1)
N2K-C2348TQ-10GE	Cisco Nexus 2348TQ Fabric Extender	NX-OS 7.0(3)I5(1)

The following tools were used for testing:

Description	Package Name	Platform	Version
Management PC			
Operating system	Windows 7 professional SP1	X86_64	6.1.7601
Terminal	Putty	X86_64	2011-1’2-1’9:r9371
Packet capture	Wireshark	X64	2.0.2
Virtualization	VM VirtualBox	X64	5.0.0

VM	Debian 8 (Jessie) VM	X64	Linux kernel 3.16
Testing Computer			
Operating system	Debian 8 (Jessie)	X64	Linux kernel 3.16
Packet capture	Tcpdump	X64	4.6.2
Complier	Gcc	X64	5.4.0 20160609
Network enumeration	Nmap	X64	6.49BETAA4
IP stack integrity checker	Isic	X64	0.07
VLAN hopping	Python-scapy	X64	2.2.0-1'kali1
Vulnerability scan tool	Nessus	X64	6.5.2
Port bridging	Bridge-utils	X64	1.6
Mac flooding	Macoff	X64	1.07
Test-Pi			
Operating system	Raspberry pi	X32	Raspbain debian 8 Linux kernel 4.4.50 version 7
System logs	Syslog-ng	X32	3.5.6
DHCP attacks	Yersina	X32	0.7.3
Attacker-2			
Operating system	Raspberry pi	X32	Raspbian debian 8 Linux kernel 4.4.50 version 7
DHCP Server	Isc-dhcp-server	X32	Isc-dhcpd-4.3.1
DHCP attacks	Yersina	X32	0.7.3

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders, v7.0(3)I5(1). The details of the models of the Nexus 9000 series switches and Nexus 2000 Fabric Extenders included in the TOE are provided in Section 2.1.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references the ASE Intermediate Report and other NSP#6-compliant evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders, v7.0(3)I5(1), to be CC Part 2 extended, CC Part 3 conformant, and to meet the requirements of **EAL 2**.This implies that the product satisfies the security technical requirements specified in Security Target Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders v7.0(3) Security Target, version 1.0, May 31 2017.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. Please note that the documents contain relevant details with respect to the resistance against certain attacks. The TOE user should take particular note of the following items:

- The TOE user is responsible for configuring secure connections between the TOE and any time, authentication and syslog servers. See the guidance documentation for details.
- The TOE supports additional protocols to those that are enabled in the evaluated configuration; enabling these additional protocols may lead to the TOE no longer meeting the SFRs.
- The TOE provides only logical separation between the Management plane and the Data plane and this must be configured by the administrator. By default it is possible for the users at the Data plane to access the Management plane. To prevent this, the administrator must follow the instructions provided in the guidance documentation to properly configure the logical separation.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

3 Security Target

The Security Target, Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders v7.0(3) Security Target, version 1.0, May 31 2017 *[ST],* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

ACL	Access Control List
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Netherlands scheme for certification in the area of IT security
PP	Protection Profile
TOE	Target of Evaluation

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1,revision 4, September 2012.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4, September 2012.
[ETR]	Evaluation Technical Report Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders v7.0(3)I5(1), 17-RPT-240, version 3.0, 8 June 2017.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.
[ST]	Cisco Nexus 9000 Switches in standalone mode with Nexus 2000 Fabric Extenders v7.0(3) Security Target, version 1.0, May 31 2017.

Appendix 1

The following sections list the Nexus 9000 series models included in the TOE, and their associated I/O modules:

Cisco Nexus 9300 Series

Model	Description	Interfaces	Supported Modules
9332PQ	QSFP+ 40-Gigabit downlink interface ports. Ports 1 to 12 and 15 to 26 also support 40-Gigabit-to-4x10-Gigabit breakout cables with the Dynamic Breakout feature. QSFP+ 40-Gigabit uplink interface ports (6)	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	QSFP-40G-ER4
9372PX	1- and 10-Gigabit SFP+ interface ports (48) QSFP+ 40-Gigabit interface ports (6)	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	Uplinks: QSFP-40G-ER4
9372PX-E	1- and 10-Gigabit BASE-T interface ports (48) QSFP+ 40-Gigabit interface ports (6)	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	Uplinks: QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-CSR4 QSFP-40GE-LR4 QSFP-40G-LR4 WSP-Q40GLR4L QSFP-40G-LR4-S QSFP-40G-ER4
9372TX	48 1- and 10-Gigabit Ethernet Small Form-Factor 10 Pluggable (SFP+) optical ports (supporting 1-Gigabit and 10-Gigabit speeds) QSFP+ 40-Gigabit interface ports (6)	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	Uplinks: QSFP-40G-ER4
9372TX-E	48 1- and 10-Gigabit BASE-T QSFP+ 40-Gigabit interface ports (6)	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	Uplinks: QSFP-40G-SR4 QSFP-40G-SR4-S QSFP-40G-CSR4 QSFP-40GE-LR4 QSFP-40G-LR4 WSP-Q40GLR4L QSFP-40G-LR4-S QSFP-40G-ER4
9396PX	4-port 100-Gigabit Ethernet CFP2 optical ports, or 6- or 12-port 40-Gigabit Ethernet Quad Small Form-Factor Pluggable (QSFP+) optical ports for connections to other devices 48 1- and 10-Gigabit Ethernet Small Form-	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1	Uplink Module – M4PC – M6PQ – M12PQ

Model	Description	Interfaces	Supported Modules
	Factor 10 Pluggable (SFP+) optical ports (supporting 1-Gigabit and 10-Gigabit speeds) to switches or Fabric Extenders (FEXs)	RJ45 connector USB ports (2)	
9396TX	4-port 100-Gigabit Ethernet CFP2 optical ports, or 6- or 12-port 40-Gigabit Ethernet Quad Small Form-Factor Pluggable (QSFP+) optical ports for connections to other devices 48 10GBASE-T copper ports (supporting 10 100-Megabit, 1-Gigabit, and 10-Gigabit speeds) for connections to other devices	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	Uplink Module – M4PC – M6PQ – M12PQ
93120TX	96 10GBASE-T copper ports (supporting speeds 6 of 100 Megabits, 1 Gigabit, and 10 Gigabits) to other devices 6 40-Gigabit Ethernet Quad Small Form-Factor 7 Pluggable (QSFP+) optical ports for uplink connections to aggregation switches	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	Uplinks: QSFP-40G-SR4 QSFP-40G-CSR4 QSFP-40GE-LR4 QSFP-40G-SR4-S QSFP-40G-LR4 WSP-Q40GLR4L QSFP-40G-LR4-S QSFP-40G-ER4
93128TX	Four, six, or 12 40-Gigabit Ethernet Quad Small Form-Factor Pluggable (QSFP+) optical ports for uplink connections to aggregation switches 96 10GBASE-T copper ports (supporting speeds 10 of 100 Megabits, 1 Gigabit, and 10 Gigabits) to other devices	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	Uplink Module – M4PC – M6PQ – M12PQ
93180YC-EX	Intel Core i3 processor Four 48 x 10/25-Gbps fibre ports and 6 x 40/100-Gbps Quad Small Form-Factor Pluggable 28 (QSFP28) ports	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (1)	Uplinks: QSFP-40G-SR4 QSFP-40G-CSR4 QSFP-40GE-LR4 QSFP-40G-SR4-S QSFP-40G-LR4 QSFP-40G-LR4-S QSFP-40G-ER4 WSP-Q40GLR4L QSFP-100G-SM-SR
93108TC-EX	Intel Core i3 processor Four 48 x 10GBASE-T ports and 6 x 40/100-Gbps QSFP28 ports	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (1)	Uplinks: QSFP-40G-SR4 QSFP-40G-CSR4 QSFP-40GE-LR4 QSFP-40G-SR4-S QSFP-40G-LR4 QSFP-40G-LR4-S

Model	Description	Interfaces	Supported Modules
			QSFP-40G-ER4 WSP-Q40GLR4L QSFP-100G-SM-SR

Cisco Nexus 9500 Series

Model	Description	Interfaces	Supported Modules
9504	Chassis: up to 2 supervisor modules of the same type, 4 I/O modules, and up to 6 fabric modules, 2 system controllers	Based on Supervisor and I/O modules installed	I/O modules: – 48-port 1-/10-Gigabit SFP+ plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9464PX) – 48-port 1-/10-GBASE-T plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9464TX) – 48-port 1-/10-GBASE-T plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9564TX) – 48-port 1-/10-Gigabit SFP+ plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9564PX) – 36-port 40-Gigabit QSFP+ aggregation I/O module (N9K-X9636PQ) – 36-port 40-Gigabit QSFP+ I/O module (N9K-X9536PQ) – 32-port 40-Gigabit QSFP+ I/O module (N9K-X9432PQ) Fabric modules: N9K-C9504-FM N9K-C9504-FM-S N9K-C9504-FM-E
9508	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	Based on Supervisor and I/O modules installed	I/O modules: – 48-port 1-/10-Gigabit SFP+ plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9464PX) – 48-port 1-/10-GBASE-T plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9464TX) – 48-port 1-/10-GBASE-T plus 4-port QSFP+ I/O module (N9K-X9564TX) – 48-port 1-/10-Gigabit SFP+ plus 4-port QSFP+ I/O module (N9K-X9564PX) – 36-port 40-Gigabit QSFP+ aggregation (non-blocking) I/O module (N9K-X9636PQ) – 36-port 40-Gigabit QSFP+ I/O module (N9K-X9536PQ) – 32-port 40-Gigabit QSFP+ I/O module (N9K-X9432PQ) – 8-port 100-Gigabit CFP2 I/O module (N9K-X9408PC-CFP2) Fabric modules: N9K-C9508-FM

Model	Description	Interfaces	Supported Modules
			N9K-C9508-FM-S N9K-C9508-FM-E
9516	Chassis: up to 2 supervisor modules and 16 I/O modules, up to two system controller modules, up to six fabric modules	Based on Supervisor and I/O modules installed	I/O modules: – 48-port 1-/10-Gigabit SFP+ plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9464PX) – 48-port 1-/10-GBASE-T plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9464TX) – 48-port 1-/10-GBASE-T plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9564TX) – 48-port 1-/10-Gigabit SFP+ plus 4-port 40-Gigabit QSFP+ I/O module (N9K-X9564PX) – 36-port 40-Gigabit QSFP+ aggregation I/O module (N9K-X9636PQ) – 36-port 40-Gigabit QSFP+ I/O module (N9K-X9536PQ) – 32-port 40-Gigabit QSFP+ I/O module (N9K-X9432PQ) – 8-port 100-Gigabit QSFP+ I/O module (N9K-X9408PC-CFP2) Fabric modules: N9K-C9516-FM N9K-C9516-FM-S N9K-C9516-FM-E
Supervisor A	four cores, 1.8 GHz, 16 GB of memory, and 64 GB of SSD (N9K-SUP-A)	Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	Not Applicable
Supervisor B	six cores, 2.1 GHz, 24 GB of memory, and 256 GB of SSD (N9K-SUP-B)	Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)	Not Applicable
System Controller	A pair of redundant system controllers offloads chassis management functions from the supervisor modules. The controllers are responsible for managing power supplies	Not Applicable	Not Applicable

Model	Description	Interfaces	Supported Modules
	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.		

(This is the end of this report).