TÜVRheinland®
Precisely Right.

Certification Report

Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders

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

Evaluation facility: ***Brightsight***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0163806-CR**

Report version: **1**

Project number: **0163806**

Author(s): **Brian Smithson**

Date: **2 February 2021**

Number of pages: **16**

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 7 879

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

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

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.

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 site complies 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 (site) 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 or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates 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 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 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders. The developer of the Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders is Cisco Systems, Inc. located in San Jose, California, 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 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders is a software defined network solution intended to be deployed with a physically secure data centre. These components comprise the Cisco ACI (Application Centric Infrastructure) fabric. The minimum number of TOE components needed to deploy the Cisco ACI fabric is as follows:

- Two (2) spine switches (running NX-OS System Software-ACI)
- Two (2) leaf switches (running NX-OS System Software-ACI)
- One (1) APIC (running APIC software)

The 9300 switches that act as leaf switches, or in the case of 9332C and 9364C act as spine switches, are fixed form factor.

The 9500 switches that act as spine switches are modular and are available in 8, 32, 36 and 48 slot chassis sizes. The 9500 modular chassis can be outfitted with the following types of modules; noting that at least one supervisor module and one-line card is required, and the fabric modules are optional.

- Supervisor modules: Supervisor modules provide scalable control plane and management functions for the switch.
- Fabric modules: Fabric modules provide the central switching element for fully distributed forwarding on the I/O modules.
- Line Card I/O modules: The Line Card Modules are full-featured, high-performance modules with support for high-density 10, 40, and 100 Gigabit Ethernet interfaces.

The APIC (Cisco Application Policy Infrastructure Controller) is the security management controller used to manage the ACI fabric. The use of the Nexus 2000 Fabric Extender is optional.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 19 January 2021 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 Switch Series with ACI mode, APIC and 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 Switch Series with ACI mode, APIC and 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 provides sufficient evidence that the TOE meets the 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 5 and *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the 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 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders from Cisco Systems, Inc. located in San Jose, California, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	9300- and 9500-series switches, 2000-series fabric extenders, and line cards (detailed in Appendix A)	See Appendix A
Software	Cisco NX-OS System Software-ACI	14.2(4o)
	Cisco APIC	4.2(4o)

To ensure secure usage a set of guidance documents is provided together with the Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders. Details can be found in section 2.5 of this report.

2.2 Security Policy

Security Audit

The TOE generates audit records to assist the Authorized Administrator in monitoring the security state of the TOE as well as trouble shooting various problems that arise throughout the operation of the system. Audit records are stored locally and may be 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.

Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic.

Identification and authentication

The TOE ensures that all Authorized Administrator are successfully identified and authenticated prior to gaining access to the TOE. The TOE also performs device level authentication. The TOE can optionally be configured to support IT environment RADIUS or TACACS+ AAA server that provides single-use authentication mechanisms. 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.

Information Flow Control

The TOE provides the ability to control traffic flow into or out of the Nexus 9000 switch.

Secure Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE.

Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication and limits configuration and access to Authorized Administrators.

TOE Access

The TOE displays a warning banner prior to allowing any administrative access to the TOE. The TOE also provides the mechanism for the Authorized Administrators to terminate their own sessions.

Trusted Path

The TOE ensures trusted paths are established to itself from remote administrators over secure SSHv2 connection for remote CLI access and secure HTTPS/TLSv1.2 connection for the web-based GUI.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

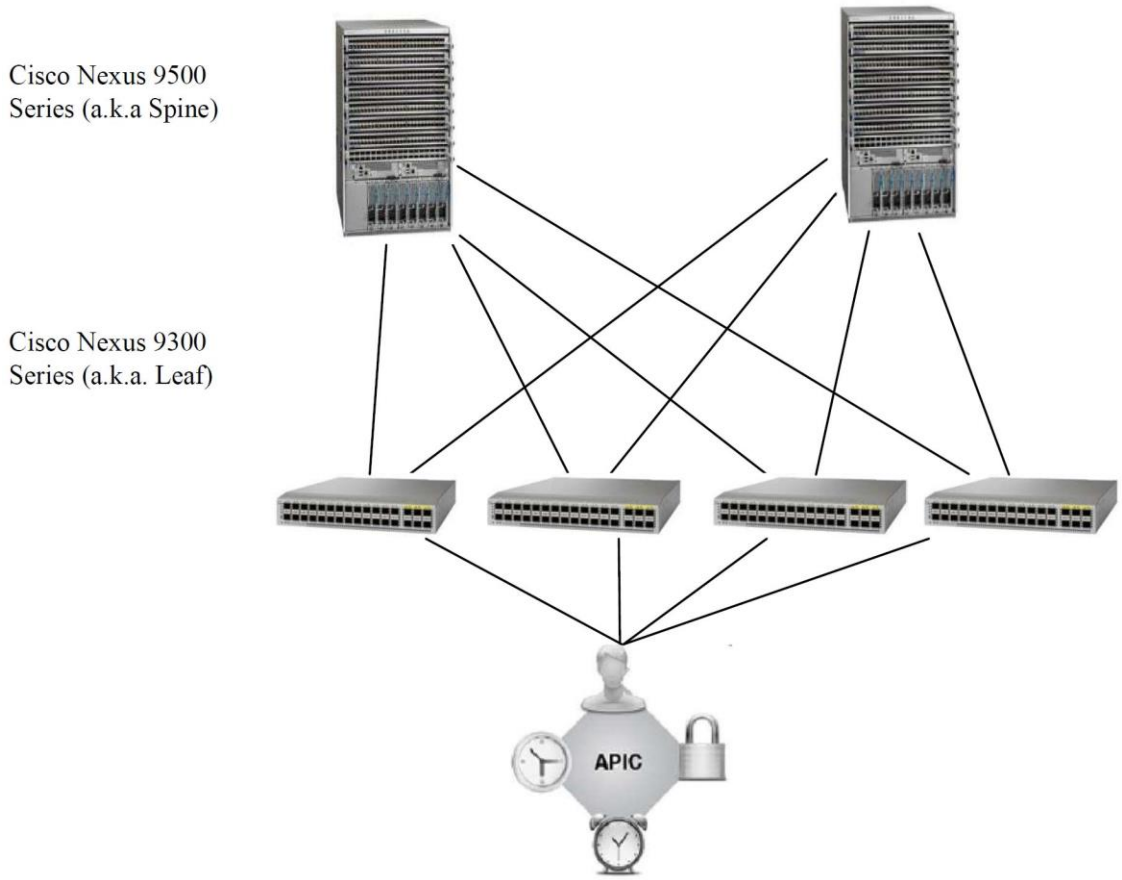
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 3.1 of the *[ST]*.

2.3.2 Clarification of scope

The TOE requires a properly configured firewall to be installed between the ACI fabric and untrusted networks in the Organization's operational environment, as described in section 3.1 of the *[ST]* and section 1.5 of the *[AGD]*.

2.4 Architectural Information

The TOE is composed of three subsystems, depicted in the figure below:



APIC subsystem

The subsystem is comprised by hardware clock, CPU, memory, local storage (NVRAM, DRAM, and FLASH memory), network ports and the APIC OS as the management software of the ACI fabric (the network).

The APIC subsystem provides centralized access to the fabric's information and configuration, sends switch configuration to the leaf and spine switches, and enforces security functions in these areas:

- Security Audit
- Identification and authentication
- Secure Management
- Protection of the TSF
- TOE Access
- Trusted Path

Leaf subsystem

The subsystem is composed of a hardware clock, CPU, memory, local storage (NVRAM, DRAM, and FLASH memory), network ports, and the NX OS in ACI mode as the operating system The NX OS is built on a Linux kernel, providing control over the hardware and a hardware abstraction of the physical ports.

The Leaf subsystem receives switch configuration from APIC, sends generated audit logs to APIC, and enforces security functions in these areas:

- Security Audit
- Full Residual Information Protection
- Information Flow Control
- Protection of the TSF

Spine subsystem

The subsystem is composed of a hardware clock, CPU, memory, local storage (NVRAM, DRAM, and FLASH memory), network ports and the NX OS in ACI mode as the operating system The NX OS is built on a Linux kernel, providing control over the hardware and a hardware abstraction of the physical ports.

The Spine subsystem receives switch configuration from APIC, sends generated audit logs to APIC, and enforces security functions in these areas:

- Security Audit
- Full Residual Information Protection
- Protection of the TSF

2.5 Documentation

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

Identifier	Version
Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders Common Criteria Operational User Guidance and Preparative Procedures	Version 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

Developer tests

The developer focused on functional testing and manually tested all of the defined test cases. The developer executed nine (9) test cases covering the following logical security functions:

- Auditing
- Identification and authentication
- Information flow control
- Secure management
- TOE access
- Trusted path

Each defined test case runs independently. There is no sequence dependency between test cases. The developer tested all the TSFIs.

The developer provided a test plan *[ATE]* for test coverage. The developer executed the test plan on the following:

APIC device:

- APIC-SERVER-M3 running 4.2(4o)

Leaf switch:

- N9K-C93180LC-EX running 14.2(4o)
- N9K-C93180LC-EX running 14.2(4o)

Spine switch:

- N9K-C9332C running 14.2(4o)

Evaluator tests

The sampling strategy for defining the repeated evaluator tests was to verify the user identification and authentication, access banners and obscured feedback and the configuration of the Information Flow Control SFP.

The evaluator chose to repeat three (3) of the developer's test cases.

The evaluator defined eight (8) independent-defined tests. The general strategy for defining the independent evaluator tests are to:

- Verify the AGD_PRE.1.2E activity;
- Verify the discovery and authentication of the switches (leaf or spine) into the ACI fabric;
- Verify time management;
- Verify TOE core management functionalities (such as authentication and logging);
- Scan and fingerprint for libraries/services searching for public known vulnerabilities to include in the vulnerability assessment;
- Verify TOE specific claims/security mechanisms.

2.6.2 Independent Penetration Testing

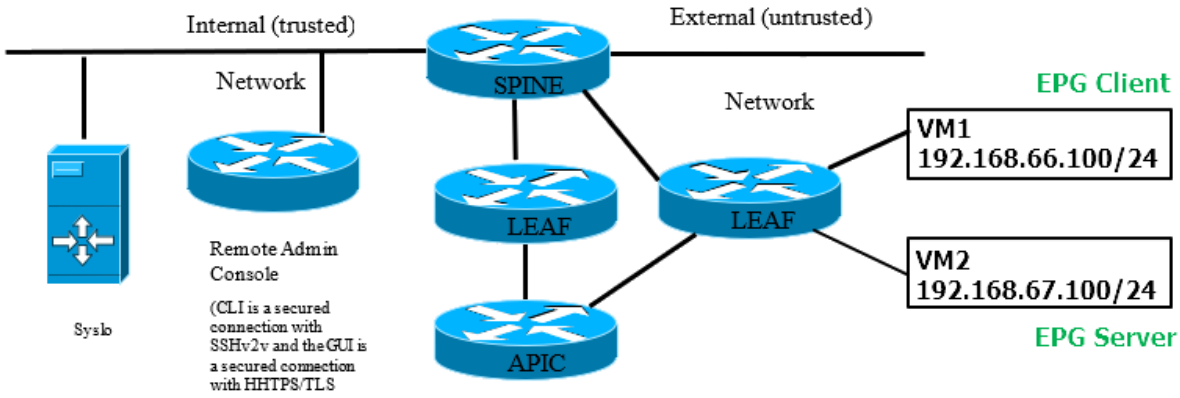
To identify potential vulnerabilities the evaluator performed the following activities:

- SFR analysis: The evaluator applied their knowledge of attacks applicable to the TOE type.
- Public domain analysis: The evaluator performed a public domain vulnerability search for TOE specific items (TOE name, TOE-type, secure libraries, etc.), and used the websites provided by NSCIB as biases to perform the search.
- Network scanning tools: The evaluator ran vulnerability-scanning tools to identify potential vulnerabilities.

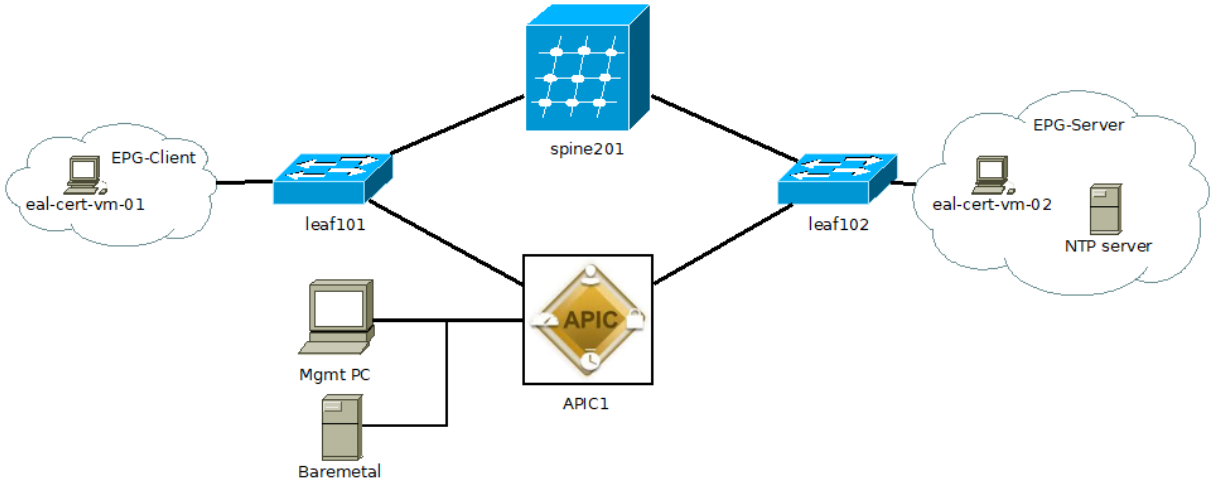
Penetration tests were created based on the vulnerabilities that are applicable to an attacker possessing Basic attack potential. The evaluator devised ten (10) penetration tests were created to verify that the TOE, in its operational environment, is resistant to an attacker possessing a Basic attack potential.

2.6.3 Test Configuration

The developer's test configuration is depicted below:



The evaluator's test configuration used was different from the developer's test configuration, due to the additional test cases defined by the evaluator for ATE_IND.2 and AVA_VAN.2:



The TOE components sampled for evaluator tests were:

Identifier	Product name	Serial number	Firmware
spine201	N9K-C9332C	FD022220V62	14.2(4o)
leaf101	N9K-C93180LC-EX	FD0204917E5	14.2(4o)
leaf102	N9K-C93180LC-EX	FD020481E22	14.2(4o)
APIC1	APIC-SERVER-L3	WZP234607UJ	4.2(4o) with VNIC 1455

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 Re-used evaluation results

There is no re-use of evaluation results in this certification.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders (as detailed in Appendix A). The chassis of each hardware component is labelled with its identifier. The version of software executing on each component can be verified through the CLI/GUI to be APIC v4.2(4o) for the APIC Controller, and NX-OS System Software-ACI 14.2(4o) for the Cisco Nexus 9000 Switch Series with ACI mode switches and Nexus 2000 Fabric Extenders. Hash values are provided in section 2, step 9, of the *[AGD]*.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an ASE Intermediate Report and other 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 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders, to be **CC Part 2 conformant**, **CC Part 3 conformant**, and to meet the requirements of **EAL 2.** This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 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. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to the resistance against certain attacks.

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.

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>.

3 Security Target

The Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders Common Criteria Security Target, Version 1.0, 14 January 2021 *[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:

ACI	Application-Centric Infrastructure
APIC	Application Policy Infrastructure Controller
IT	Information Technology
ITSEF	IT Security Evaluation Facility
JIL	Joint Interpretation Library
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:

[AGD] Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders Common Criteria Operational User Guidance and Preparative Procedures, Version 1.0, 14 January 2021

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR] Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders - Evaluation Technical Report EAL2 (20-RPT-585), Version 1.0, 18 January 2021

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

[ST] Cisco Nexus 9000 Switch Series with ACI mode, APIC and Nexus 2000 Fabric Extenders Common Criteria Security Target, Version 1.0, 14 January 2021.

Appendix A

The following table details the applicable hardware models of the TOE:

Component	Model	Description
Leaf	93180LC-EX	32 x 40/50-Gbps QSFP+ ports OR 18 x 100-Gbps QSFP28 ports, 4 cores CPU, 24 GB system memory, 64 GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC
	93108TC-EX	48 x 10GBASE-T and 6 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 64GB SSD, Power supplies (up to 2) 500W AC, 650W AC, 930W DC, or 1200W HVAC/HVDC
	93108TC-FX	48 x 100M/1/10GBASE-T ports and 6 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC
	9348GC-FXP	48 x 100M/1G BASE-T ports, 4 x 1/10/25-Gbps SFP28 ports and 2 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1200W AC or 1200W HVAC/HVDC
	93216TC-FX2	96 x 100M/1/10GBASE-T ports and 12 x 40/100-Gigabit QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC
	93180YC-EX	48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports, 6 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC
	93180YC-FX	48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports, 6 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC
	93240YC-FX2	48 x 1/10/25-Gbps fiber ports and 12 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC
	93360YC-FX2	96 x 1/10/25-Gbps and 12 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1200W AC, or 1200W HVAC/HVDC
	9336C-FX2	36 x 40/100-Gbps QSFP28 ports, 4 core CPU, 24GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC
	9364C-GX	64 x 100/40-Gbps QSFP28 ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC
	9316D-GX	16 x 400/100/40-Gbps QSFP-DD ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC
	93600CD-GX	28 x 100/40-Gbps QSFP28 ports and 8 x 400/100-Gbps QSFP-DD ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1100W AC, 1100W DC, or 1100W HVAC/HVDC

Component	Model	Description
Spine	9332C	32-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports, 4 core CPU, 16GB system memory, 128GB SSD, Power supplies 1100W AC, 1100W DC, or 2000W HVAC/HVDC
	9364C	64-port 40/100G QSFP28 ports and 2-port 1/10G SFP+ ports, 4 core CPU, 32GB system memory, 128GB SSD, Power supplies 1200W AC, 93000W DC, or 1100W HVAC/HVDC
	9504	Chassis: 4-slot, up to 4 line cards, up to 4 power supplies, up to 6 fabric modules of same type, up to 2 system controllers, up to 2 supervisors of the same type, and up to 3 fan trays
	9508	Chassis: 8-slot, up to 8 line cards, up to 8 power supplies, up to 6 fabric modules of same type, up to 2 system controllers, up to 2 supervisors of the same type, and up to 3 fan trays
	9516	Chassis: 16-slot, up to 16 line cards, up to 10 power supplies, up to 6 fabric modules of same type, up to 2 system controllers, up to 2 supervisors of the same type, and up to 3 fan trays
9500 models supervisor	N9K-SUP-A N9K-SUP-A+	Supervisor A/A+ 4 core cpu, 16 GB of memory and 64 GB of SSD
	N9K-SUP-B N9K-SUP-B+	Supervisor B/B+ 6 core cpu, 24 GB of memory and 256 GB of SSD
9500 line card I/O modules	N9K-X9432C-S	100 Gigabit Ethernet Line Card
	N9K-X9736PQ	40 Gigabit Ethernet Line Card
	N9K-X9636PQ	40 Gigabit Ethernet Line Card
	N9K-X9536PQ	40 Gigabit Ethernet Line Card
	N9K-X9432PQ	40 Gigabit Ethernet Line Card
	N9K-X9564PX	1 and 10 Gigabit Ethernet and 10 and 40 Gigabit Ethernet Line Card
	N9K-X9464PX	1- and 10-Gigabit Ethernet and 10- and 40-Gigabit Ethernet Line Card
	N9K-X9564TX	1 and 10 Gigabit Ethernet Copper and 10 and 40 Gigabit Ethernet Line Card
	N9K-X9464TX2	1 and 10 Gigabit Ethernet Copper and 10 and 40 Gigabit Ethernet Line Card
Fabric Extenders	2248TP-E	48 x 100/1000BASE-T host interfaces and 4 x 10 Gigabit Ethernet fabric interfaces (SFP+)
	2232PP-10GE	32 x 1/10 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE) host interfaces (SFP+) and 8 x 10 Gigabit Ethernet and FCoE fabric interfaces (SFP+)
	2232TM-E	32 x 100M, 1/10GBASE-T host interfaces and uplink modules (8 x 10 Gigabit Ethernet fabric interfaces [SFP+]); FCoE support up to 30m with Category 6a and 7 cables
	2348TQ-E	48 x 100MBASE-T and 1/10GBASE-T port host interfaces (RJ-45) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30m with Category 6a and 7 cables
	2332TQ	32 x 100MBASE-T and 1/10GBASE-T port host interfaces (RJ-45) and up to 4 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30m with Category 6a and 7 cables

Component	Model	Description
	2348TQ	48 x 100MBASE-T and 1/10GBASE-T port host interfaces (RJ-45) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces; FCoE support up to 30m with Category 6a and 7 cables
	2348UPQ	48 x 1/10 Gigabit Ethernet and unified port host interfaces (SFP+) and up to 6 QSFP+ 10/40 Gigabit Ethernet fabric interfaces
APIC	APIC-SERVER-L3	A server based on UCS C220 M5 (large-size CPU, hard drive, and memory). The server contains 1x 1-Gbps RJ-45 management port (Marvell 88E6176), 2x 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard), 1x RS-232 serial port (RJ45 connector), 1x DB15 VGA connector, 2x USB 3.0 port connectors, One flexible modular LAN on motherboard (mLOM) slot that accommodates a virtual interface card.
	APIC-SERVER-M3	A server based on UCS C240 M5 (medium-size CPU, hard drive, and memory). The server contains 1x 1-Gbps RJ-45 management port (Marvell 88E6176), 2x 10GBase-T LOM ports (Intel X550 controller embedded on the motherboard), 1x RS-232 serial port (RJ45 connector), 1x DB15 VGA connector, 2x USB 3.0 port connectors, One flexible modular LAN on motherboard (mLOM) slot that accommodates a virtual interface card.
Virtual interface card installed on the APIC	VIC 1225T	The module supports copper connectors, copper cables, and switches with copper downlink ports (such as: Cisco Nexus 93108TC-EX, 93108TC-FX, 93120TX, 93128TX, 9372TX, 9372TX-E, and 9396TX switches).
	VIC 1225	The module supports optical transceivers, optical cables, and switches with optical downlink ports (such as: Cisco Nexus 93180LC-EX, 93180YC-EX, 93180YC-FX, 9332PQ, 9336C-FX2, 9348GC-FXP, 9372PX, 9372PX-E, 9396PX, and 93600CD-GC switches).
	VIC 1455	The module supports optical transceivers, optical cables, and switches with optical downlink ports (such as: Cisco Nexus 9336C-FX2, 93180LC-EX, 93180YC-EX, 93180YC-FX, 93240YC=FX2, and 93600CD-GC switches).

(This is the end of this report).