Certification Report

Cisco Nexus 9000 Switch Series with ACI mode, APIC 6.1(2g) and NX-OS software-ACI 16.1(2g)

Sponsor and developer:	***Cisco Systems, Inc.*** **170 West Tasman Drive** **95134 San Jose, CA** **USA**
Evaluation facility:	***SGS Brightsight B.V.*** **Brassersplein 2** **2612 CT Delft** **The Netherlands**
Report number:	**NSCIB-CC-2400067-01-CR**
Report version:	**1**
Project number:	**NSCIB-2400067-01**
Author(s):	**Brian Smithson**
Date:	**16 May 2025**
Number of pages:	**17**
Number of appendices:	**1**

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, TrustCB 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 TrustCB 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 TrustCB B.V. to perform Common Criteria evaluations; a significant requirement for such a licence 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, TrustCB 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, 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 (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since 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.

For details of the current list of signatory nations and approved certification schemes, see http://www.commoncriteriaportal.org.

European recognition

The SOG-IS MRA Version 3, effective since April 2010, provides mutual recognition in Europe of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (respectively E3-basic) is provided for products related to specific technical domains. This agreement was signed initially by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOG-IS MRA in December 2010.

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.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 6.1(2g) and NX-OS software-ACI 16.1(2g). The developer of the Cisco Nexus 9000 Switch Series with ACI mode, APIC 6.1(2g) and NX-OS software-ACI 16.1(2g) 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 TOE is composed of the Nexus 9000 Series Switches that include the 9300, 9400 and 9500 models with ACI mode and the APIC. The APIC is the security management controller used to manage the ACI fabric. The 9K switches with ACI and APIC, are collectively referred to as TOE or individually as TOE Components. The 9300 switches are fixed form factor, the 9400 and 9500 switches are modular and are available in 8, 32 (9500 series only), 36 (9500 series only) and 48 (9500 series only) slot chassis. The 9400 and 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. 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 Cisco Application Policy Infrastructure Controller (Cisco APIC) is a hardware appliance with a software-only image that includes an underlying Linux OS. The APIC appliance is a centralized, clustered controller that optimizes performance and unifies operation of physical and virtual environments. Furthermore, the APIC provides the capabilities for information flow control.

The Cisco ACI fabric is composed of the APIC and the Cisco Nexus 9000 Series with ACI mode leaf and spine switches. The Cisco APIC provides centralized access to all fabric information and supports flexible application provisioning across physical and virtual resources. Cisco ACI consists of:

- APIC
- Nexus 9000 Series Switches in ACI spine and leaf configuration

Typically, the APIC will be deployed in a cluster with a minimum of three controllers for scalability and redundancy purposes, though it's not required.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 2025-05-14 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 6.1(2g) and NX-OS software-ACI 16.1(2g), 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 6.1(2g) and NX-OS software-ACI 16.1(2g) 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 the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

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

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TrustCB 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. Note that the certification results apply only to the specific version of the product as evaluated.

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 6.1(2g) and NX-OS software-ACI 16.1(2g) 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 ACI Leaf Models 9300, 9400 and 9500 ACI Spine Models Cisco 9500 Model Supervisor and Line Card Models (See Appendix A)	See Appendix A
Software	NX-OS APIC	16.1(2g) 6.1(2g)

To ensure secure usage a set of guidance documents is provided, together with the Cisco Nexus 9000 Switch Series with ACI mode, APIC 6.1(2g) and NX-OS software-ACI 16.1(2g). For details, see section 2.5 “Documentation” 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 Administrators 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 ACACS+ 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.

Security Management - The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All CLI TOE administration occurs either through SSHv2 secure connection or a direct local console connection. In addition, the web-based GUI can be used for TOE administration using HTTPS (TLSv1.2 or TLSv1.3) secure connection. The TOE provides the ability to securely perform the following:

- Review audit record logs;
- Manage information flow policies and rules;
- Maintain the timestamp;
- Manage Authorized Administrators security attributes
- Administer the TOE remotely

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 or TLSv1.3) connection for the web-based GUI.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

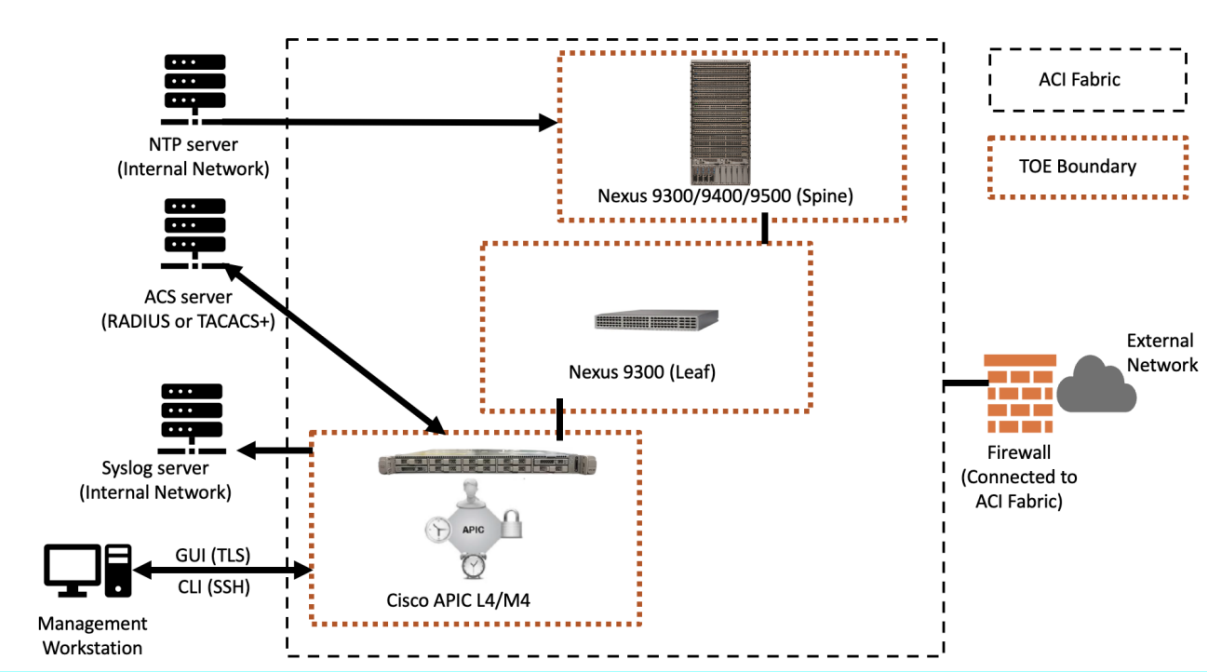
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 3.1 of the *[ST]*.

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 logical architecture of the TOE can be depicted as follows:



The TOE is composed of three subsystems:

1. Cisco NX-OS software-ACI

This subsystem that provides or supports the following security functionalities:

- Security Audit: Generates and stores audit logs that are traceable to a specific user.
- User data protection: Allows and maintains communication with APIC to receive flow control policies.

- Identification and authentication: Maintains user ID and user password as user security attributes.
- Security Management: Allows local CLI or SSH CLI connection for the admin to perform management functions.
- Protection of the TSF: During the initial start-up runs a suite of self-tests to verify its correct operation
- TOE Access: Displays a customizable login banner and allows admin to terminate local or remote sessions.
- Trusted Path: Requires trusted paths (SSH) to be established for the purpose of troubleshooting & configuration.

This subsystem receives switch configuration from APIC and sends generated audit logs to APIC.

2. Cisco APIC Software

This subsystem provides or supports the following security functionalities:

- Security Audit: Generates and stores audit logs that are traceable to a specific user. Additionally, it provides the CLI and GUI interfaces for the Authorized Administrators to read all of the TOE audit records.
- User data protection: Allows an administrator to configure ingress and egress traffic flow policies to N9k interfaces via NX-OS.
- Identification and authentication: Maintains user ID and user password as user security attributes.
- Security Management: Provides all the capabilities necessary to securely manage the TOE either via CLI or Web GUI. It also allows the administrator to manage the information flow control security attributes.
- Protection of the TSF: During the initial start-up runs a suite of self-tests to verify its correct operation.
- TOE Access: Displays a customizable login banner and allows admin to terminate local or remote sessions.
- Trusted Path: Requires trusted paths over SSHv2 for CLI access and HTTPS/TLSv1.3 to be established to itself from remote administrators.

This subsystem sends switch configuration to the leaf and spine switches.

3. Cisco Nexus 9K Appliance Hardware

This subsystem provides the physical underlying platform for the NX-OS subsystem to operate and connect to networks (WAN and/or LAN). This subsystem provides or supports the following security functionalities:

- User data protection: Enforces every ingress and egress traffic flow. The contracts are applied to each type of received and sent traffic.

This subsystem enforces every ingress and egress traffic flow from Cisco NX-OS software-ACI.

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 NX-OS software-ACI Common Criteria Administrator Guidance	v1.0

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 provided test plans to address the TOE test setup and test execution. The developer performed 9 tests, each of which tests an important security feature, and mapped to the relevant SFRs.

After considering the developer tests' coverage of security functions, the following 4 developer tests were sampled and repeated:

- Trusted path and user-initiated termination
- Audit generation and reliable time stamps
- TSF self-test during power up
- User attribution definition and security roles

2.6.2 Independent penetration testing

Security mechanisms that aren't covered by the developer tests were covered through independent testing:

- Verify TOE core management functionalities (such as authentication and auditing capabilities);
- Verify TOE specific claims/security mechanisms (no access during TOE initialization, trusted path, password complexity, etc.);
- Verify the information flow policies enforced by the TOE;
- Verify that there are no undocumented ports/services running and no undocumented commands available to the user;
- Verify that the REST API interface is available only to authenticated users;
- Scanning and fingerprinting for libraries/services searching for public known vulnerabilities to include in the vulnerability assessment.

In total, 9 Evaluator-defined test cases were devised.

To identify potential vulnerabilities the evaluator performed the following activities:

- SFR design analysis: SFR implementation details were examined in the SFR design analysis. During this examination several potential vulnerabilities were identified.
- CWE vulnerability focus: Using the CWE weaknesses collection, the evaluator collected a list of security questions and related answers. This approach ensured that the evaluator was forced to think in terms of vulnerabilities from all different angles and improved completeness in the vulnerability analysis. Also, during this examination several potential vulnerabilities were identified.
- Use of Scanning tools: The evaluator runs vulnerability scanning tools to identify potential vulnerabilities.
- Public vulnerability search: Several additional potential vulnerabilities were identified during a search in the public domain.

The total test effort expended by the evaluators was 2.125 person-weeks.

2.6.3 Test configuration

The TOE consists of a number of different models of hardware:

- Cisco 9300 ACI Leaf Models
- Cisco 9300, 9400 and 9500 ACI Spine Models

- Supervisor modules and Line Cards for the Cisco 9500 switch series
- APIC M4 and APIC L4 servers

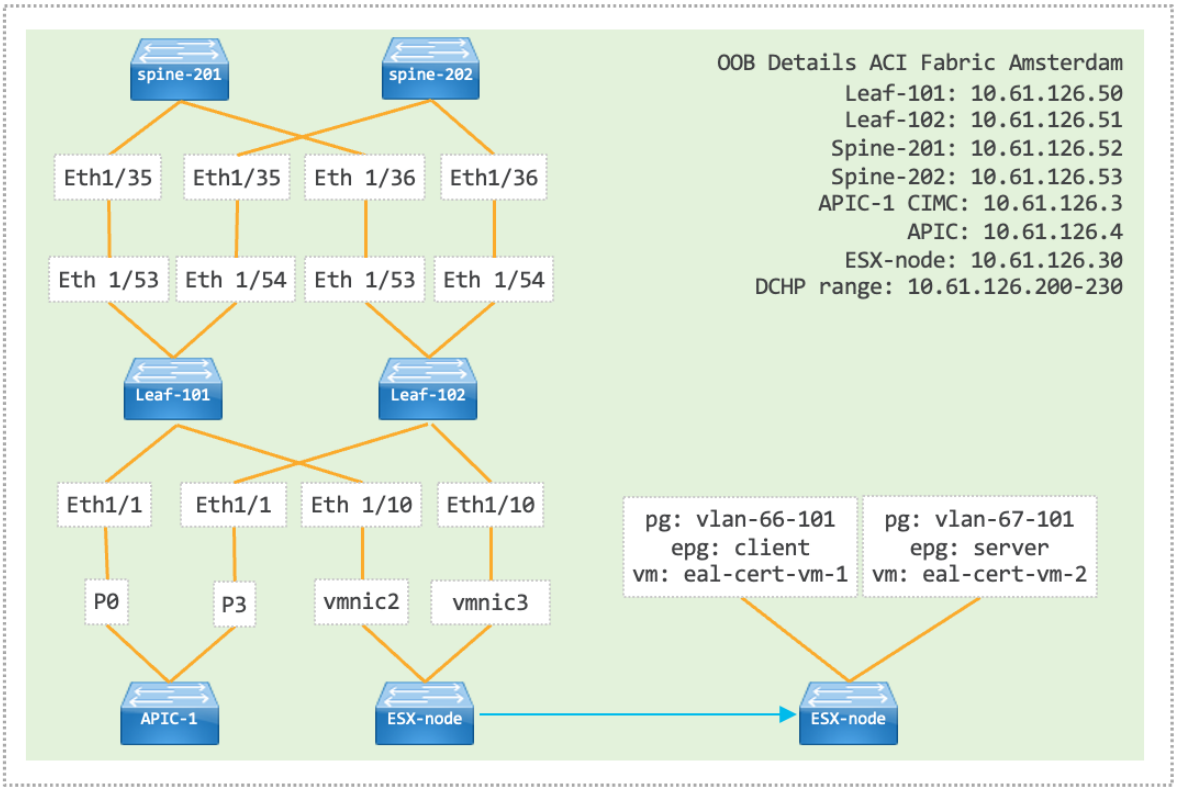
All the Cisco leaf and spine switch series run the same version of NX-OS software (16.1(2g)) and both APIC server models run the same version of the APIC software (6.1(2g)). All of the TOE security functions are enforced by the TOE software. The hardware can be easily hot-swapped into the fabric, and the fabric functions identically regardless of the hardware being inserted into it.

Therefore, it is concluded that all the hardware models are equivalent from the claimed security point of view.

The TOE was tested using the following hardware models and software versions:

- TOE Hardware
  - APIC-SERVER-M4
  - N9K-C93600CD-GX Spine Switch
  - N9K-C93180YC-FX3 Leaf Switch
- TOE Software Version
  - Cisco NX-OS System Software-ACI 16.1(2g)
  - APIC 6.1(2g)

The TOE was tested in the following configuration:



2.6.4 Test 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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e., from the current best cryptanalytic attacks published, has been taken into account.

2.7 Reused Evaluation Results

There is no reuse 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 6.1(2g) and NX-OS software-ACI 16.1(2g). The version of software executing on each component can be verified through the CLI/GUI and compared to the hash values provided in section 2, step 9, of the *[AGD]*.

2.9 Evaluation Results

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 6.1(2g) and NX-OS software-ACI 16.1(2g), to be **CC Part 2 conformant, CC Part 3 conformant**, and to meet the requirements of **EAL 2 augmented with ALC_FLR.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 "Documentation" 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 concerning 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 must 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. For the evolution of attack methods and techniques to be covered, the customer 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>, which are out of scope as there are no security claims relating to these.

3 Security Target

The Cisco Nexus 9000 Switch Series with ACI mode, APIC and NX-OS software-ACI Common Criteria Security Target, v1.0, 15 April 2025 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions 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.

[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] Evaluation Technical Report “Cisco Nexus 9000 Switch Series with ACI mode, APIC and NX-OS software-ACI” – EAL2+", 24-RPT-1574, v1.0, 16 April 2025

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.6, 02 August 2022

[ST] Cisco Nexus 9000 Switch Series with ACI mode, APIC and NX-OS software-ACI Common Criteria Security Target, v1.0, 15 April 2025

Appendix A

Model	Description	Management Interfaces
Cisco 9300 ACI Leaf Models		
93108TC-FX3H	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	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93108TC-FX3P	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	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
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	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
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	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93180YC-FX3H	48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports, 4 core CPU, 16GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 port - (L1 and L2 ports are unused) 1 USB port 1 RS-232 serial port
93180YC-FX3	48 x 1/10/25-Gbps and 6 x 40/100-Gbps QSFP28 ports, 4 core CPU, 16GB system memory, 128GB SSD, Power supplies (up to 2) 500W AC, 930W DC, or 1200W HVAC/HVDC	1 RJ-45 port - (L1 and L2 ports are unused) 1 USB port 1 RS-232 serial port
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	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
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	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
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	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9336C-FX2-E	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	1 RJ-45 1SFP+ 1 USB port 1 RS-232 serial port
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	1 RJ-45 1 SFP+ 1 USB port

		1 RS-232 serial port
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	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
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	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9364D-GX2A	64 x 400/100-Gbps QSFP-DD ports and 2 x 1/10-Gbps SFP+ ports, 6 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 3200W AC/HVDC, 3200W DC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9348D-GX2A	48-port 400G QSFP-DD ports and 2-port 1/10G SFP+ ports, 6 core CPU, 32GB system memory, 128GB SSD, Power supply 1500W AC, 1100W DC, 1100 HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9332D-GX2B	32 x 400/100-Gbps QSFP-DD ports and 2 x 1/10-Gbps SFP+ ports, 6 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1500W AC/HVDC, 1500W DC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
Cisco 9300, 9400 and 9500 ACI Spine Models		
9316D-GX	16 x 400/100-Gbps QSFP-DD ports, 4 core CPU, 32 GB system memory, 128 GB SSD, Power supplies 1100W AC, 1100DC, 1100WHVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9332D-GX2B	32 x 400/100-Gbps QSFP-DD ports and 2 x 1/10-Gbps SFP+ ports, 6 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 1500W AC/HVDC, 1500W DC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
9348D-GX2A	48-port 400G QSFP-DD ports and 2-port 1/10G SFP+ ports, 6 core CPU, 32GB system memory, 128GB SSD, Power supply 1500W AC, 1100W DC, 1100 HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB port 1 RS-232 serial port
93600CD-GX	28 x 100/40-Gbps QSFP28 ports and 8 x 400/100-Gbps QSFP-DD port, 4 core CPU, 32GB system memory, 128GB SSD, Power supply 1100W AC, 1100W DC, 1100 HVAC/HVDC	1 RJ-45 1 SFP+ 1 USB 1 RS-232 serial ports
9364C-GX	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	1 x 10/100/1000BASE-T 1 x 1-Gbps SFP) 1 USB port 1 RS-232 serial port
9364D-GX2A	64 x 400/100-Gbps QSFP-DD ports and 2 x 1/10-Gbps SFP+ ports, 6 core CPU, 32GB system memory, 128GB SSD, Power supplies (up to 2) 3200W AC/HVDC, 3200W DC/HVDC	1 RJ-45 1 SFP+ 1 USB 1 RS-232 serial ports
C9408	Chassis: 1 supervisor slot, 8 LEM slots, up to 4 power supplies	Based on Supervisor and ACI compatible I/O modules installed. Each line

		card should be ACI compatible
C9504	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	Based on Supervisor and ACI compatible I/O modules installed. Each line card should be ACI compatible
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	Based on Supervisor and ACI compatible I/O modules I/O modules installed
C9508-FM-E2	8-slot 800-Gbps Cloud Scale fabric module for the Cisco Nexus 9508 Switch chassis	N/A
C9516	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, up to 3 fan trays, 4 core cpu, 230	Based on Supervisor and ACI compatible I/O modules I/O modules installed
Cisco 9500 Model Components		
Supervisor A/A+	4 core cpu, 16 GB of memory and 64 GB of SSD (N9K-SUP-A/A+)	Two USB ports, a serial port, and a 10/100/1000-Mbps Ethernet port
Supervisor B /B+	6 core cpu, 24 GB of memory and 256 GB of SSD (N9K-SUP-B/B+)	Two USB ports, a serial port, and a 10/100/1000-Mbps Ethernet port
Supervisor A	Nexus 9400 CPU card with PTP, SyncE (N9K-C9400-SUP-A)	1 x 10/100/1000BASE-T 1 x 1-Gbps SFP) 1 USB port 1 RS-232 serial port
N9K-SC-A	Cisco Nexus 9500 System Controller	N/A
Line Card I/O Modules	N9K-X9400-16W Nexus 9400 16p 200G LEM	N/A
	N9K-X9400-8D Nexus 9400 8p 400G QSFP DD LEM	N/A
	N9K-X9716D-GX 16-port 400-Gigabit Ethernet Quad Small Form-Factor Pluggable Double Density (QSFP-DD) line card	N/A
	N9K-X9736C-FX 36-port 100-Gigabit Ethernet Quad Small Form-Factor Pluggable 28 (QSFP28) line card	N/A
	N9K-X9736Q-FX 36-port 40-Gigabit Ethernet Quad Small Form-Factor Pluggable 28 (QSFP28) line card	N/A

(This is the end of this report.)