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 Dr.
San Jose, CA 95134
USA

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

Report number:	**NSCIB-CC-142306-CR**
Report version:	**1**
Project number:	**142306**
Author(s):	**Denise Cater**
Date:	**30 April 2018**
Number of pages:	**19**
Number of appendices:	**1**

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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

Certificate

Standard
Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)

Certificate number
CC-18-142306

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

Assurance Package:
- EAL2

Project number
142306

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.

SOGIS Mutual Recognition Agreement for components up to EAL4

Validity
Date of 1st issue : **04-05-2018**
Certificate expiry : **04-05-2023**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

C.C.M. van Houten, LSM Systems
TÜV Rheinland Nederland B.V.
Westervoortsedijk 73, 6827 AV Arnhem
P.O. Box 2220, NL-6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

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.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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, 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 (Application-Centric Infrastructure) mode, APIC (Application Policy Infrastructure Controller), and Nexus 2000 Fabric Extenders offer both modular (9500 switches) and fixed (9300 switches) 1, 10, 40, and 100 Gigabit Ethernet configurations. The TOE operates in ACI mode to take full advantage of the policy-focused services and infrastructure automation features of the ACI.

The TOE is comprised of the Nexus 9000 Series Switches that include the 9300, 9500 models with ACI mode and the APIC including the optional Nexus 2000 Fabric Extenders. The APIC is the security management controller used to manage the ACI fabric and is installed on Cisco UCS C-series servers. The Nexus 2000 Fabric Extender functions essentially as a remote line card and is optional to the deployment of the Nexus 9000 Switch Series with APIC/ACI to add additional ports. The Nexus 9000 Switch Series with ACI, APIC, and optional Fabric Extender are collectively referred to as TOE or individually as TOE Components.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 30 April 2018 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 provide sufficient evidence that it 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 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 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, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	9300 models, 9500 models, Fabric Extenders and ACI Line Cards (for detailed models please refer to Appendix A)	n/a
Software	NX-OS System Software-ACI	12.3(1f)
	APIC	2.3(1f)

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

- The TOE can audit events related to cryptographic functionality, identification and authentication, enforcement of information flow control policies and administrative actions. The Cisco Nexus 9000 Switch in ACI mode and APIC generate an audit record for each auditable event. 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 an internal database.
- 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
Transport Layer Security (TLS)	Used in TLS session establishment
RSA/DSA Signature Services	Used in SSH session establishment Used in TLS session establishment
SHA-1, SHA-256, SHA-512	Used to provide SSH traffic integrity verification Used to provide TLS traffic integrity verification Password hashing
AES CBC, GCM, and CTR (128, 192, 256)	Used to encrypt SSH session traffic Used to encrypt TLS session traffic
HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	Used for keyed hash, integrity services in SSH and TLS session establishment

- 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 and device level authentication. 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 GUI and CLI. When the role is defined through the management interface on the TOE, it is sent to the RADIUS server using Vendor Specific Attributes (VSA). Password based authentication is used for authenticating to the APIC using a browser to access the web based GUI secured by TLS.

- 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 (Contracts)
    - Layer 2 Traffic – PACLs (Contracts)
    - VLAN Traffic – VACLs (Contracts)
    - Virtual Routing and Forwarding – VRFs (tenant)
- 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 a secure SSHv2 session or via a local console connection. In addition, the web based GUI can be used for TOE administration using TLS. For the 9k with ACI, the APIC controls the management of the devices within the ACI fabric. Cisco NX-OS in ACI mode and APIC devices use role-based access control (RBAC). Preconfigured roles can be used and customized roles can be created.
- 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 TOE internally maintains the date and time and the TOE performs power-up self-tests and conditional self-tests to verify correct operation of the switch itself and that of the cryptographic module.
- The administrator can terminate their own session by exiting out of the CLI and GUI. The TOE can also be configured to display an Authorized Administrator specified banner on the CLI and GUI management interfaces 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 and TLS using a browser for connection to the web based GUI on the APIC.

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 is mainly designed to regulate traffic of Layer 3 and above. To mitigate against hostile and malicious traffic, especially against Layer 2 attacks such as ARP spoofing, the TOE requires a properly configured firewall to be installed between the trusted and untrusted networks in the Organization's operational environment.

2.4 Architectural Information

The general architecture consists of four 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)
- The APIC Subsystem providing
  - Security Audit
  - Identification and Authentication (I&A)
  - Protection of the TSF
  - TOE Access
  - Security Management
  - Trusted Path/Channels (the SSH and SSL functionalities)

2.5 Documentation

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

Identifier	Version
Cisco Nexus 9k Switch with APIC/ACI Common Criteria Configuration Guide	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 tests consist of the twenty two (22) tests. These tests cover all TSFI and all SFRs and include both positive and negative tests. The developer performed these twenty-two (22) tests on 2 setups.

The 1st setup includes:

- N9K-C9396PQ (SPINE) running NX-OS System Software ACI Mode 12.3(1e)
- N9K-C93180YC (LEAF) running NX-OX System Software ACI Mode 12.3(1e)
- N9K-C9372PX-E (LEAF) running NX-OS System Software ACI Mode 12.3(1e)
- UCS-C220-M4 APIC v2.3(1e) – three in a cluster

The 2nd setup includes:

- N9K-C9396PX running NX-OS System Software ACI Mode 12.3(1e)
- N9K-C9508 running NX-OS System Software ACI Mode 12.3(1e) with supervisor module A and N9K-X9736PQ line card.
- N9K-C93180YC-EX running NX-OS System Software ACI Mode 12.3(1e)
- UCS-C220-M4 APIC v2.3(1e) – three in a cluster

The evaluator repeated six (6) of the twenty-two (22) developer tests, using the hardware setup:

- 2 of N9K-C9372PX running NX-OS System Software ACI Mode 12.3(1e)
- N9K-C9336PQ running NX-OS System Software ACI Mode 12.3(1e)
- UCS-C220-M3 APIC v2.3(1e) – 1 for testing purpose (not in cluster)
- N2K-C2232PP and N2K-C2348TQ running same NX-OS as their parents

The TOE software was updated from NX-OS System Software ACI Mode 12.3(1e) and APIC v2.3(1e) to NX-OS System Software ACI Mode 12.3(1f) and APIC v2.3(1f). The evaluator performed an analysis of the changes and repeated the agreed subset of developer test cases using the updated software versions.

In addition to the developer tests, the evaluator derived and executed eleven (11) additional functional tests. On the basis of the evaluator analysis of the software changes, 6 tests were performed using APIC v2.3(1e) / NX-OS ACI Mode 12.3(1e), and 6 tests were performed on the updated TOE software APIC v2.3(1f) / NX-OS ACI Mode 12.3(1f), with 1 test performed on both versions.

2.6.2 Independent Penetration Testing

The evaluators produced twenty-nine (29) penetration tests in total. These were derived from a vulnerability analysis comprised of 3 parts:

1. Public domain vulnerability analysis of TOE specific vulnerabilities (both hardware and 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, the data plane and the APIC Controller. All penetration tests were performed using the hardware setup:

- 2 of N9K-C9372PX running NX-OS System Software ACI Mode
- N9K-C9336PQ running NX-OS System Software ACI Mode
- UCS-C220-M3 APIC– 1 for testing purpose (not in cluster)
- N2K-C2232PP and N2K-C2348TQ running same NX-OS as their parents

On the basis of the evaluator analysis of the software changes, 12 tests were performed on the version APIC 2.3(1e) / NX-OS 12.3(1e), and 18 tests were performed on the version APIC 2.3(1f) /

NX-OS 12.3(1f), with 1 test performed on both versions, in accordance with the change analysis presented

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).

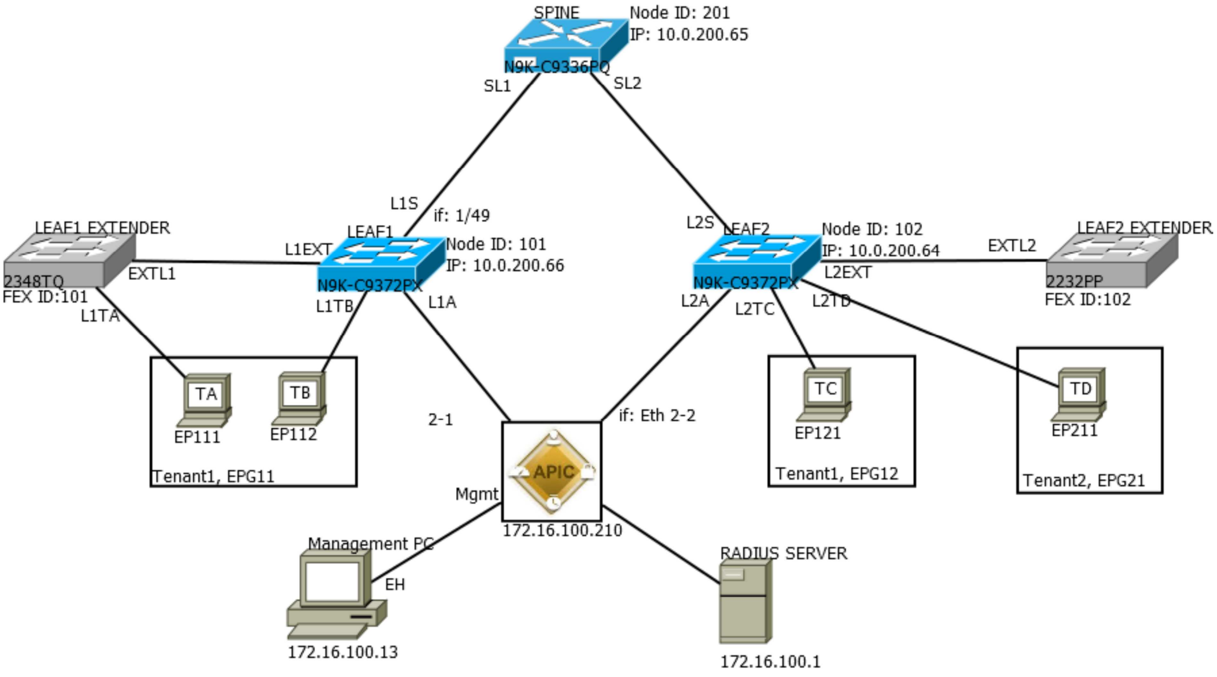

Figure 1 Baseline evaluator test setup

The ports are labelled as follows:

Port	Type	Description
Management PC (Mgmt-PC)		
EH	Ethernet	Management port
N9K-C9336PQ		
SL1	SFP	Ethernet port 1/1
SL2	SFP	Ethernet port 1/2
API-SERVER-M1		
AL1	SFP	Port Eth 2-1 which connects the APIC to the LEAF1 switch
AL2	SFP	Port Eth 2-2 which connects the APIC to the LEAF2 switch
Mgmt	Ethernet	Management Ethernet port which connects the APIC to the Management PC
N9K-C9372PX (LEAF1)		
L1A	SFP	Port Eth 1/1 connects the LEAF1 Switch to the APIC
L1S	QSFP	Port Eth 1/49 connects the LEAF1 Switch to the Spine
L1TB	SFP	Ethernet port connects leaf1 WITH Tester TB
L1EXT	4*SFP	Ethernet ports 1/3 – 1/6 which connects the Leaf1 switch to the Extender
N2K-C2348TQ-10GE (LEAF1 EXTENDER)		
EXTL1	QSFP	Uplink port 1/1 Extends the I/O module managed by LEAF1

Port	Type	Description
L1TA	SFP	Ethernet port connects the LEAF1 Extender to tester TA
N9K-C9372PX (LEAF2)		
L2A	SFP	Port Eth 1/1 connects the LEAF2 Switch to the APIC
L2S	QSFP	Port Eth 1/49 connects the LEAF1 Switch to the Spine
L2TC	SFP	Ethernet port connects leaf1 WITH Tester TC
L2TD	SFP	Ethernet port connects leaf1 WITH Tester TD
EXTL2	QSFP	Uplink port 1/1 Extends the I/O module managed by LEAF2
Testing Computer (Debian workstation)		
TA	SFP	TA testing computer
TB	SFP	TB testing computer
TC	SFP	TD testing computer
TD	Ethernet	TC testing computer
Management PC	Ethernet	Management port

The TOE devices sampled in the evaluator testing were[2]:

Identifier	Product name	Firmware
N9K-C9372PX	Cisco Nexus 9372PX Switch	NX-OS ACI mode: 12.3 (1f)
N9K-C9336PQ	Cisco Nexus 9336PQ Switch	NX-OS ACI mode: 12.3 (1f)
N2K-C2232PP-10GE	Cisco Nexus 2232PP Fabric Extender	NX-OS ACI mode: 12.3 (1f)
N2K-C2348TQ-10GE	Cisco Nexus 2348TQ Fabric Extender	NX-OS ACI mode: 12.3 (1f)
APIC-SERVER-M1	Cisco UCS C220-M3 server	APIC v2.3 (1f)

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
Terminal	putty	X86_64	2011-1’2-1’9:r9371
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

[2] Note that originally the TOE software version was APIC v2.3(1e) / NX-OS ACI mode 12.3(1e). However, during the evaluation the developer advanced the TOE version to APIC v2.3(1f) / NX-OS ACI mode 12.3(1f). Consequently, as a result of evaluator analysis, some tests were performed on APIC v2.3(1e) / NX-OS ACI Mode 12.3(1e), some tests were performed on APIC v2.3(1f) / NX-OS ACI Mode 12.3(1f), and some of the tests were performed on both versions.

Description	Package Name	Platform	Version
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
Teardrop attack	Targa2.c	X64	2.1
CVE-2016-8858	kexkill	X64	1.0
CVE-2016-10010	ExploitDB script#40962	X64	1.0
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.

As the result of the test execution the evaluator determined that the TOE needs to rely on the evaluated configuration to defend against some of these attacks. The developer consequently updated the relevant documents, clarifying the evaluated configuration to ensure these attacks are not applicable to the TOE in its evaluated configuration.

As a result, the independent penetration tests found no exploitable vulnerabilities in the TOE when operated in its evaluated configuration.

2.7 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 v2.3(1f) for the APIC Controller and NX-OS ACI Mode 12.3(1f) for the Cisco Nexus 9000 Switch Series with ACI mode switches and Nexus 2000 Fabric Extenders.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[3] which references a 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 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders, 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 requirements specified in Security Target *[ST]*.

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.

When an administrative user is deleted, it is required to reload all the APIC to ensure any existing sessions associated with that user are terminated as instructed in the guidance [AGD].

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 implemented cryptographic algorithms and protocols was not rated in the course of this evaluation.

[3] 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 Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders Security Target, Version 1.0, April 12, 2018 *[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
UCS	Unified Computing System

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 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 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders, 18-RPT-152, Version 3.0, 30 April 2018.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.4, 27 September 2017.

[ST] Cisco Nexus 9000 Switch Series with ACI mode, APIC, and Nexus 2000 Fabric Extenders Security Target, Version 1.0, April 12, 2018.

Appendix A

The following table provides the detailed hardware models of the TOE:

Model	Description	Interfaces
Cisco 9300 models with ACI support		
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)
9336PQ	36 line-rate QSFP+ ports. 10 and 40 Gigabit Ethernet ports.	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 RJ45 connector USB ports (2)
N9K-C9372PX-E	Intel Core i3 processor Four 48 x 10/25-Gbps fiber 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)
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)
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)
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-Factor 10 Pluggable (SFP+) optical ports (supporting 1-Gigabit and 10-Gigabit speeds) to switches or Fabric Extenders (FEXs)	I/O ports as described Management ports: 1 RJ45 connector Console serial port: 1 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 10100-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)

Model	Description	Interfaces
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)
C93180LC-EX	Intel Core i3 processor Four 48 x 10/25-Gbps fiber 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)
93180YC-EX	Intel Core i3 processor Four 48 x 10/25-Gbps fiber 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)
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)
Cisco 9500 models		
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 ACI compatible I/O modules installed. Each line card should be ACI compatible
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 ACI compatible I/O modules I/O modules installed
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 ACI compatible I/O modules I/O modules installed
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)
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)
System Controller	A pair of redundant system controllers offloads chassis management functions from the supervisor modules. The controllers are responsible for managing power supplies and fan trays and are a	Not Applicable

Model	Description	Interfaces
	central point for the Gigabit Ethernet out-of-band channel (EOBC) between the supervisors, fabric modules, and line cards.	
APIC (Medium - Large) and clustered	An APIC appliance comprises either a cluster of Cisco UCS C-Series 220 M4 (second generation appliance) or Cisco UCS C-Series 220 M3 (first generation appliance) servers manufactured with an image secured with Trusted Platform Module (TPM), certificates, and an APIC product ID (PID). The interfaces are the same between the med, large, and clustered APIC it is just the processor, hard drive, memory will be larger with more I/O ports for scalability.	Management ports: 2 RJ45 connector Console serial port: 1 RJ45 connector Cisco Integrated Management Controller (CIMC) alternative console port for 1 Gig Ethernet USB ports (2) Virtual Interface Card for optical or 10BaseT
2000 Series Fabric Extenders		
Cisco Nexus C2248PQ-10GE	48 100/1000BASE-T host interfaces and 4 10 Gigabit Ethernet fabric interfaces (SFP+)	I/O ports as described
Cisco Nexus 2248TP-E	48 100/1000BASE-T host interfaces and 4 10 Gigabit Ethernet fabric interfaces (SFP+)	I/O ports as described
Cisco Nexus 2248TP-1GE	48 100/1000BASE-T host interfaces and 4 10 Gigabit Ethernet fabric interfaces (SFP+) [32MB Shared Buffer]	I/O ports as described
Cisco Nexus 2232PP-10GE	32 1/10 Gigabit Ethernet and FCoE host interfaces (SFP+) and 8 10 Gigabit Ethernet and FCoE fabric interfaces (SFP+)	I/O ports as described
Cisco Nexus 2232TM-E	32 1/10 G BASE-T host interfaces and 8 10 Gigabit Ethernet (SFP+) Uplink Module (Lower power consumption and improved BER)	I/O ports as described
Cisco Nexus 2348UPQ	48 100Mĩ/1/10 Gigabit Ethernet and Unified Port host interfaces (SFP+) and up to 6ĩ QSFP+ 10/40 Gigabit Ethernet fabric interfaces.	I/O ports as described
ACI Line Cards		
N9K-X9732C-EX	ACI Ready Spine Line Card: 32p QSFP28 40/100G (32p line rate)	I/O ports as described
N9K-X9736PQ	ACI Ready Spine Line Card: 36p QSFP 40G (36p line rate)	I/O ports as described

(This is the end of this report).