TÜV Rheinland Nederland B.V.

Version 20101101

Certification Report

Cisco Nexus 7000 Series Switches, running NX-OS 6.2.12

Sponsor and developer:	***Cisco Systems Inc.*** **170 West Tasman Dr.** **San Jose, CA 95134** **USA**
Evaluation facility:	***Brightsight*** **Delftechpark 1** **2628 XJ Delft** **The Netherlands**
Reportnumber:	**NSCIB-CC-14-49712-CR**
Report version:	**1**
Projectnumber:	**NSCIB-CC-14-49712**
Authors(s):	**Denise Cater**
Date:	**11 August 2015**
Number of pages:	**13**
Number of appendices:	**0**

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Apeldoorn:
Vissenstraat 6
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Enschede:
JosinkEsweg10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a
registered company with the
Amsterdam Chamber of Commerce
under number 27288788
info@nl.tuv.com
www.tuv.com/nl

Certificate

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

Certificate number: **CC-14-49712**

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 7000 Series Switches, running NX-OS 6.2.12,**

Assurance Package:

- EAL2

Project number: **NSCIB-CC-14-49712-CR**

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

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

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

Validity

Date of issue : **11-08-2015**

Certificate expiry : **11-08-2020**

Registration number
PRODUCTS
RvA C078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

CONTENTS:

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 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 intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements stated in the (site) security target.

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

Recognition of the certificate

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

International recognition

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

European recognition

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the **Cisco Nexus 7000 Series Switches running NX-OS 6.2.12**. The developer of the **Cisco Nexus 7000 Series Switches running NX-OS 6.2.12** 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 TOE is a data center-class switch for 10 Gigabit Ethernet networks with a fabric architecture that scales to 17 terabits per second (Tbps). The TOE is both IPv4 and IPv6 capable and provides network virtualization running Cisco NX-OS, which is a Cisco-developed highly configurable proprietary operating system that provides for efficient and effective routing and switching as well as network virtualization.

The NX-OS supports Virtual Device Contexts (VDC), which enables the partitioning of a single physical Nexus 7000 device into multiple logical devices. Each VDC appears as a unique device and enables separate Roles-Based Access Control Management (RBAC) per VDC. This enables VDCs to be administered by different administrators while still maintaining a rich, granular RBAC capability. With this functionality, each administrator can define VRF names and VLAN IDs independent of those used in other VDCs safely with the knowledge that VDCs maintain their own unique software processes, configuration, and data plane forwarding tables.

NX-OS provides virtual routing and forwarding capabilities that logically segment the network by virtualizing both the routing control plane and data plane functions into autonomous instances. Routing protocols and interfaces, both physical and logical, become members of a specific VRF instance via configuration. For each VRF, IPv4 and IPv6 tables are created automatically and independent routing and forwarding decisions are made. NX-OS supports up to 1000 unique VRF instances, whether defined in a single Virtual Device Context (VDC) or spread across multiple VDCs.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on July 2015 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 7000 Series Switches**, 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 7000 Series Switches** 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 **Cisco Nexus 7000 Series Switches running NX-OS 6.2.12** 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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the **Cisco Nexus 7000 Series Switches running NX-OS 6.2.12** from **Cisco Systems Inc.** located in San Jose, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	Cisco Nexus 7004, 7009, 7010, 7018 Series switches with network modules Cisco Nexus 7000 Series Switches Fabric-2 Modules and either Cisco Nexus 7000 Supervisor2 or Supervisor 2E Module Cisco Nexus 7706, 7710, 7718 Series switches with applicable network modules (Cisco Nexus 7700 6-Slot Fabric Module, 10-Slot Fabric Module or 18-Slot Fabric Module) and Cisco Nexus 7700 Supervisor2E	n/a
Software	Cisco NX-OS	6.2.12

To ensure secure usage a set of guidance documents is provided together with the **Cisco Nexus 7000 Series Switches running NX-OS 6.2.12**. Details can be found in section 2.5 of this report.

2.2 Security Policy

The major security features provided by the TOE are:

- The TOE can audit events related to cryptographic functionality, identification and authentication, enforcement of information flow control policies and administrative actions
- The TOE provides cryptography in support of remote administrative management via SSHv2.
- The TOE performs user authentication for the Authorized Administrator of the TOE.
- The following types of traffic flow may be able to be controlled for both IPv4 and IPv6 traffic:
  - Layer 3 Traffic – RACLs (A RACL is an administratively configured access control list that is applied to Layer 3 traffic that is routed into or out Nexus 7000 Series switch)
  - Layer 2 Traffic – PACLs (A PACL is an administratively configured access control list that is applied to Layer 2 traffic that is routed into Nexus 7000 Series switch)
  - VLAN Traffic – VACLs (A VACL is an administratively configured access control list that is applied to packets that are routed into or out of a VLAN or are bridged within a VLAN. VACLs are strictly for security packet filtering and for redirecting traffic to specific physical interfaces)
  - VRFs (Virtual Routing and Forwarding allows multiple instances of routing tables to exist within the Nexus 7000 Series switch TOE component simultaneously)
- The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE;
- The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication and access controls to limit configuration to authorized administrators;
- The TOE can terminate inactive sessions after an authorized administrator configurable time-period and can also display a Security Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

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

- Administrators are assumed to be non-malicious with appropriate training.
- The TOE will be physically protected within controlled access facilities;
- There are no general-purpose computing capabilities available on the TOE, only those services necessary for the operation, administration and support of the TOE.

2.4 Architectural Information

The general architecture consists of the following subsystems, as depicted in Figure 1 below:

- 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
  - Entropy for random numbers
  - Self-tests on boot up
- The Cryptographic subsystem providing cryptographic support for:
  - Encrypting of communication with users and other systems
  - Encryption of stored passwords
- The NX-OS subsystem providing all other SFR-related functionality, such as:
  - Generating audit records
  - Packet filtering
  - Routing
  - Management
  - Communicating with users and other systems

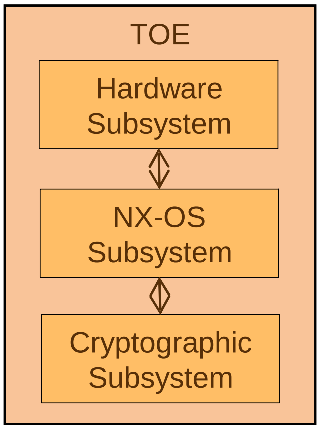

Figure 1 TOE Architecture

2.5 Documentation

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

Identifier	Version
Cisco Nexus 7000 Series Switch Common Criteria Configuration Guide	1.0

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

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 11 tests, some of which were quite extensive. These tests cover all TSFI and all SFRs and include both positive and negative tests. Brightsight repeated three of the 11 developer tests.

In addition to the developer tests, the evaluator derived and executed 4 additional functional tests.

2.6.2 Independent Penetration Testing

The evaluators performed 28 penetration tests. These were derived from a vulnerability analysis comprised of 3 parts:

1. Public domain vulnerability analysis of TOE specific vulnerabilities (vulnerabilities specific for 7000/7700 series hardware and NX-OS 6.2.12 software);
2. Public domain vulnerability analysis of TOE-type vulnerabilities (vulnerabilities that are generic for routers/switches);
3. Analysis of TOE deliverables (FSP/TDS etc.).

2.6.3 Test Configuration

The network diagram in Figure 2 describes the overall setup of the lab and the IP addresses used for developer and evaluator testing. Ports are labelled as follows:

- Ports on the router (TOE) are labelled with R (RA, RB, RC for regular interfaces, RL for loopback interface, RM for management interface);
- Ports on the Testing computer are labelled T (TA, TB, TC for regular interfaces, TL for loopback interface);
- SER is the serial port on the testing computer and CO is the console port of the TOE.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

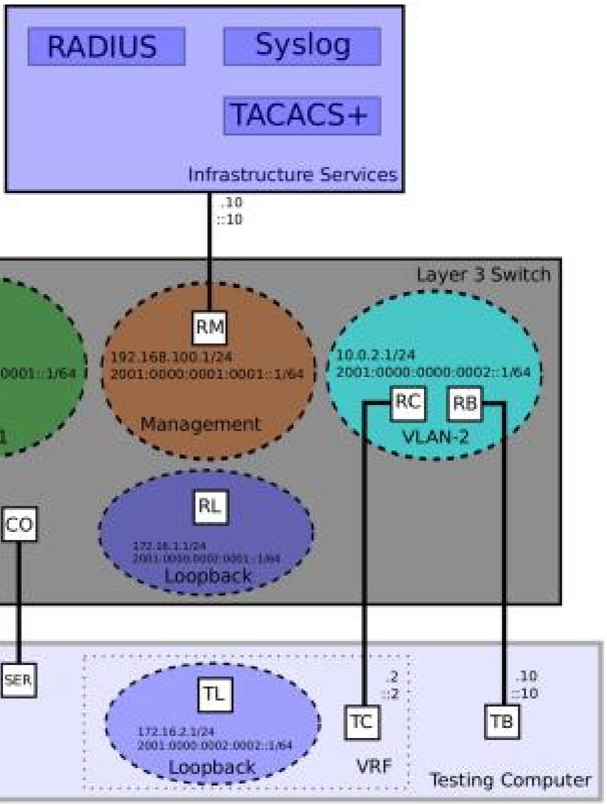

Figure 2 Test Configuration

Test cases load a baseline configuration (verified to match the security guidance provided in [AGD]) on the TOE before configuring the TOE into the state necessary for the test case to proceed. The baseline configuration has been created by the Evaluator and saved in flash memory on the TOE.

The following tools were used for testing:

Description	Package Name	Platform	Version
Linux Kernel	linux-image-3.2.0-4-486	i386	3.2.57-3
GNU/Linux Debian	Wheezy	Debian	7.0
SSH Client Software	openssh-client	i386	1:6.0p1-4+deb7ul
SSH Client Software	Bitvise SSH client	i386	
Serial console client	Minicom	I386	2.6.1
Test Automation	python-pexpect	i386	2.4-1
Test Automation	python-scapy	i386	2.2.0-1
VLAN hopping	Frogger	i386	Github 13d2f78
VLAN hopping	Python-scapy	I386	2.2.0-1
VLAN hopping	Yersinia framework	i386	0.7.1
Dsniff framework	Layer2 attacks	i386	2.4
Packet capture	Tcpdump	I386	4.3.0
Packet capture	Wireshark	i386	1.8.2
IP fragmentation	Rose attack tool	I386	Rev. 20061112
Network enumeration	nmap	i386	6.0
Packet crafting	Hping	I386	3.0.a2
Password attacks	Hydra	I386	8.1

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.

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number **Cisco Nexus 7000 Series Switches running NX-OS 6.2.12**.

2.8 Results of the Evaluation

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

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

Based on the above evaluation results the evaluation lab concluded the **Cisco Nexus 7000 Series Switches running NX-OS 6.2.12**, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL** 2.This implies that the product satisfies the security technical requirements specified in Security Target Cisco Nexus 7000 Series Switch Security Target, version 1.0, dated 23 July 2015.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. In particular, the customer must verify the version of the Supervisor module using the guidance provided in *[AGD]* section 3.2.1.

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

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

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

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

3 Security Target

The Security Target Cisco Nexus 7000 Series Switch Security Target, version 1.0, dated 23 July 2015 *[ST]* is included here by reference

4 Definitions

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

ACL	Access Control List
IT	Information Technology
ITSEF	IT Security Evaluation Facility
LAN	Local Address Network
NSCIB	Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging
PACL	Port ACL
PP	Protection Profile
RACL	Router ACL
RBAC	Roles-Based Access Control (management)
SSH	Secure Shell
TOE	Target of Evaluation
VACL	VLAN ACL
VDC	Virtual Device Context
VLAN	Virtual LAN
VRF	Virtual Routing and Forwarding

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.

5 Bibliography

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

[AGD] Cisco Nexus 7000 Series Switch Common Criteria Configuration Guide, version 1.0

[CC] Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1,revision 4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4, September 2012.

[ETR] Brightsight, Evaluation Technical Report Cisco Nexus 7000 Series Switches running NX-OS 6.2.12-EAL2, 15-RPT-220, Version 1.0, 28 July 2015.

[NSCIB] Nederlands Schema for Certification in the Area of IT Security, Version 2.1, August1st, 2011.

[ST] Cisco Nexus 7000 Series Switch Security Target, version 1.0, dated 23 July 2015.

(This is the end of this report).

® TÜV, TUEV and TUV are registered trademarks. Any use or application requires prior approval.