Certification Report

HUAWEI CE16800 series Switches and CE6800 series Switches V200R005C20SPC800

Sponsor and developer: ***Huawei Technologies Co., Ltd.***
Administration Building, Huawei Base,
Bantian, Longgang District, Shenzhen 518129
China

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

Report number:	**NSCIB-CC-0059187-CR**
Report version:	**1**
Project number:	**0059187**
Author(s):	**Andy Brown**
Date:	**15 April 2020**
Number of pages:	**12**
Number of appendices:	**0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

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

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

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

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

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

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

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

CONTENTS:

Foreword

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

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

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

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

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

Recognition of the certificate

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

International recognition

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

European recognition

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

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the HUAWEI CE16800 series Switches and CE6800 series Switches V200R005C20SPC800. The developer of the HUAWEI CE16800 series Switches and CE6800 series Switches V200R005C20SPC800 is Huawei Technologies Co., Ltd. located in Shenzhen, China 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 Huawei CloudEngine 16800 (CE16800 for short) series switches has an embedded AI chip and uses the unique iLossless algorithm to learn and train network-wide traffic in real time. Using the Huawei Versatile Routing Platform (VRP) software platform, CE16800 switches deliver Layer 2 and Layer 3 switching services, providing an open data center cloud network platform.

Huawei CloudEngine 6800 (CE6800 for short) series switches are next-generation 10G/25G Ethernet switches designed for data centers and high-end campus networks. Using the Huawei Versatile Routing Platform (VRP) software platform, CE6800 switches can function as 10GE/25GE access switches with high-density ports on data center networks. They can also be used as aggregation or access switches on enterprise campus networks.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 15 April 2020 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 HUAWEI CE16800 series Switches and CE6800 series Switches V200R005C20SPC800, 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 HUAWEI CE16800 series Switches and CE6800 series Switches V200R005C20SPC800 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provides sufficient evidence that the TOE meets the EAL2 augmented (EAL2+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.2 (Flaw reporting procedures).

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]*.

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 HUAWEI CE16800 series Switches and CE6800 series Switches V200R005C20SPC800 from Huawei Technologies Co., Ltd. located in Shenzhen, China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	CE16804 CE16808 CE16816	See *[ST]* section 1.4.2 table 2 and table 3 for lists of hardware model, board, and their versions
	CE6863-48S6CQ CE6881-48S6CQ	
Software	CE16800 series Switches V200R005C20SPC800	V200R005C20SPC800
	CE6800 series Switches V200R005C20SPC800	V200R005C20SPC800

To ensure secure usage a set of guidance documents is provided together with the HUAWEI CE16800 series Switches and CE6800 series Switches V200R005C20SPC800. Details can be found in section 2.5 of this report.

2.2 Security Policy

The major security features provided by the TE are summarised as follows:

1. Authentication: The TOE authenticates administrative users based on the user name and password. The TOE supports local authentication and remote authentication via RADIUS or TACACS+ server.
2. Access Control: The TOE supports multiple user access levels. By default there are 4 different user levels. The user levels can be refined and extended to 16 levels.
3. Traffic Forwarding: The TOE forwards network packets based on static routing tables or dynamic routing tables.
4. Auditing: The TOE logs all security management events and provides functionality to the administrators to review the audit logs.
5. Communication Security: The TOE provides SSHv2 for the administrators to connect to the TOE and manage the TOE.
6. IP-based ACL: The TOE offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow to and from interfaces on Interface boards. The administrator can create, delete, and modify rules for ACL configuration to filter, prioritize, rate-limit the information flow destined to TOE through interfaces on Interface boards by matching information contained in the headers of IP packets against ACL rules specified.
7. Security functionality management: Security functionality management includes not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters.
8. Cryptographic functions: The TOE provides the following cryptographic functions: AES encryption for SSHv2, RSA used for SSH authentication, HMAC-SHA256/HMAC-SHA512 for SSH verification algorithm, and HMAC-SHA256 as verification algorithm for the OSPF, BGP, and ISIS protocols.

9. SNMP Trap: The TOE provides SNMP trap to notify a fault occurs or the system does not operate properly.

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 4.2 of the *[ST]*.

2.3.2 Clarification of scope

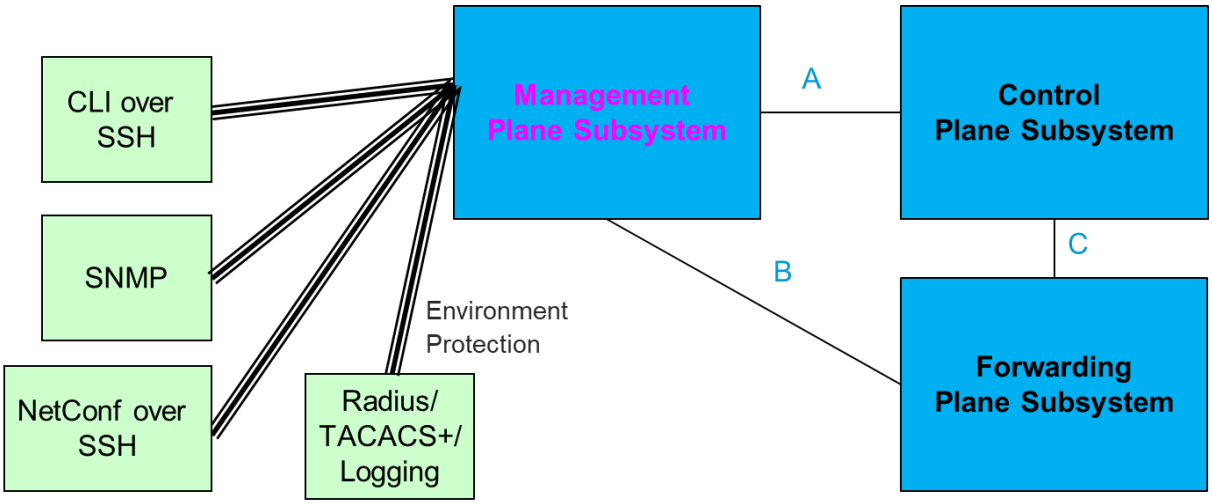
The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

The TOE is advertised that it has VXLAN and SDN capability in its general advertisement. However the user should be aware that in the certified configuration, both VXLAN and the SDN are excluded from the certified configuration and should not be used in the certified configuration. See [AGD] section 10 for more details and all other non-evaluated options.

2.4 Architectural Information

The subsystems of the TOE are represented in the three functional groups, each group corresponding with one major security functionality:

- Management Plane Subsystem: Management plane subsystem provides maintenance and management functions, and is responsible for handling commands from the Device Manager, such as command, Net-manager, schema, etc.
- Control Plane Subsystem: Control plane subsystem is responsible for controlling protocol interaction between devices, and issues hardware forwarding table according to Control plane calculation results.
- Forwarding Subsystem: Forwarding plane subsystem is responsible for querying forwarding table, processing and forwarding the packet. Considering forwarding performance, it is mostly for hardware forwarding (forwarding engine) and a few may use software forwarding (soft forwarding).



2.5 Documentation

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

Identifier	Version
HUAWEI CloudEngine 16800 series Switches & CloudEngine 6800 series Switches V200R005C20 Common Criteria Security Evaluation - Certified Configuration	V2.0 2020-03-12
CloudEngine 16800 Series Switches V200R005C20 Product Documentation	V200R005C20
CloudEngine 8800, 7800, 6800, and 5800 Series Switches V200R005C20 Product Documentation	V200R005C20

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 test plan consists of 12 different categories of tests of 84 tests. The categories are based on groupings of major security functionalities, and, in combination with all SFRs and TSFIs. In addition, the developer also performed a number of penetration tests to demonstrate the TOE is resistant against common attacks of the switch/router TOE type. The evaluator repeated 9 of the developer test cases.

In addition the evaluator derived and executed 12 functional test cases focused on verifying router core functionalities, Scanning and fingerprinting for libraries/services, verifying TOE specific security mechanisms (e.g. plane separation) and extending the test coverage across TSFI.

2.6.2 Independent Penetration Testing

The evaluator performed a total of 16 penetration tests; 8 test cases related to the Management Plane and 8 related to the data plane. These were derived from a vulnerability analysis including:

- SFR design analysis: Based on the information obtained in the evaluation evidence, the SFR implementation details were examined. The aspects described in CEM annex B were considered. During this examination several potential vulnerabilities were identified.
- Additional security analysis: When the implementation of the SFR was understood, a coverage check was performed on the relevant aspects of all SFRs. This expanded the list of potential vulnerabilities.
- Scanning the TOE using the applicable vulnerability scanning tools (e.g., NMAP, NESSUS, NEXPOSE) to collect information about the TOE and identify potential vulnerabilities.
- Public vulnerability search: The evaluator performed public domain vulnerability search based on the TOE name, TOE type, and identified 3rd party security relevant libraries and/or services. Several additional potential vulnerabilities were identified during a search in the public domain.
- The potential vulnerabilities identified were analysed, and some of the potential vulnerabilities were concluded not exploit within in the Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

2.6.3 Test Configuration

The developer testing was performed using:

- CE16804 device running V200R005C20SPC800, with:
    - CE-MPUD-HALF

- CE-SFU16G-G
- 36 ports 40GE line card
- 48 ports 10GE line card

- CE6881 device running V200R005C20SPC800

The following TOE devices were used to perform the evaluator independent functional and penetration tests:

- CE16808, with
  - CE-MPUD-HALF
  - CE-SFU16G-G
  - 18 ports 100GE line card
  - 36 ports 40GE line card
  - 48 ports 10GE line card
- CE6863

These devices were used for the execution of all except two test cases, which were executed using CE16804 and CE6881.

2.6.4 Testing Results

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

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

No exploitable vulnerabilities were found with the independent penetration tests.

2.7 Re-used evaluation results

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

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number HUAWEI CE16800 series Switches and CE6800 series Switches V200R005C20SPC800.

The digital signature for the TOE software should be verified using the signature details provided in *[ST]* section 1.4.2.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]* which references an ASE Intermediate Report and other evaluator documents.

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

Based on the above evaluation results the evaluation lab concluded the HUAWEI CE16800 series Switches and CE6800 series Switches V200R005C20SPC800, 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 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE.

Please note that the documents contain relevant details with respect to the resistance against certain attacks. The product is advertised as having VXLAN and SDN capability. However, the user should be aware that in the certified configuration, both VXLAN and the SDN are excluded from the certified configuration and should not be used in the certified configuration. The user guidance has details and all other non-evaluated options.

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.

3 Security Target

The HUAWEI CE16800 series Switches & CE6800 series Switches V200R005C20 Security Target, v2.0, 2020-03-12 *[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:

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
SDN	Software Defined Networking
TOE	Target of Evaluation
VXLAN	Virtual Extensible LAN

5 Bibliography

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

[AGD]	HUAWEI CloudEngine 16800 series Switches & CloudEngine 6800 series Switches V200R005C20 Common Criteria Security Evaluation - Certified Configuration, V2.0, 2020-03-12
[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 HUAWEI CE16800 CE6800 series –EAL2, 19-RPT-898, Version 2.0, 03 April 2020.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.
[ST]	HUAWEI CE16800 series Switches & CE6800 series Switches V200R005C20 Security Target, v2.0, 2020-03-12.

(This is the end of this report).