SERTIT
Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-114 CR Certification Report

Issue 1.0 4 July 2018

Expiry date 4 July 2023

Huawei NE9000 Router V800R010C00SPC200

CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

SERTIT, Postboks 814, 1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of the CCRA July 2nd 2014.

The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Agreement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Agreement and is the Party's claim that the certificate has been issued in accordance with the terms of this Agreement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

Mutual recognition under SOGIS MRA applies to components up to EAL 4.

Contents

1 Certification Statement

Huawei Technology Co. Ltd. HUAWEI NE9000 Router V800R010C00SPC200 is a series of routers that have large capacity and high performance, and are developed to meet the requirement of carrier-class reliability.

HUAWEI NE9000 Router V800R010C00SPC200 have been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) augmented requirements of Evaluation Assurance Level EAL 2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Arne Høye Rage Quality Assurance Arne H. Rage
Approved	Jørn Arnesen Head of SERTIT
Date approved	4 July 2018

2 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SoF	Strength of Function
SPM	Security Policy Model
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Huawei NE9000 Router V800R010C00SPC200 Security Target, Huawei Technology Co. Ltd., Version 1.8, 2018-05-15.

[2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R5, April 2017.

[3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R5, April 2017.

[4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R5, April 2017.

[5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.

[6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, 3.1 R5, April 2017.

[7] Evaluation Technical Report, Version 2.0, 31 May 2018.

[8] Huawei NE9000 Common Criteria Security Evaluation - Certified Configuration, Version 1.1, April 2018

[9] NE9000 V800R010C00SPC200 Product Documentation 01

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of HUAWEI NE9000 Router version V800R010C00SPC200 to the Sponsor, Huawei Technology Co. Ltd., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was HUAWEI NE9000 Router version V800R010C00SPC200.

These products are also described in this report as the Target of Evaluation (TOE). The developer was Huawei Technologies.

The HUAWEI NE9000 Router (NE9000) is a large-capacity and high-performance router designed by HUAWEI to provide carrier-class reliability. Based on the powerful versatile routing platform (VRP), the NE9000 provides strong switching capabilities, dense ports, and high reliability. NE9000s mainly serve as super-core nodes on carriers' backbone networks, core nodes on metropolitan area networks (MANs), egresses in large-scale Internet Data Centers (IDCs), and core nodes on large-scale enterprise networks.

The NE9000 can be flexibly deployed at the edge or core of IP/MPLS networks to simplify the network structure and provide an extensive range of services and reliable service quality.

At the core of each chassis is the Versatile Routing Platform (VRP), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include assigning different privileges to administration users with different privilege levels; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the Security Target[1] chapter 1.4.2 and 1.4.3.

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL 2, augmented by ALC_FLR.2. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

There are no Organizational Security Policies or rules with which the TOE must comply.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives counter and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- T.UnwantedNetworkTraffic

  Unwanted network traffic sent to the TOE will not only consume the TOE's processing capacity for incoming network traffic thus fails to process traffic expected to be processed, but an internal traffic jam might happen when those traffic are sent to MPU from LPU within the TOE. This may cause denial of service of TOE.

  This may further cause the TOE fails to respond to system control and security management operations.

  Routing information exchanged between the TOE and peer routes may also be affected due to the traffic overload.

- T.UnwantedNetworkTraffic

  A user who is not a user of the TOE gains access to the TOE.

- T.UnauthorizedAccess

  A user of the TOE authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for. This threat also includes data leakage to non-intended person or device

- T.Eavesdrop

An eavesdropper (remote attacker) in the management network served by the TOE is able to intercept, and potentially modify or re-use information assets that are exchanged between TOE and LMT/RMT.

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

It is assumed that the TOE (including any console attached) is protected against unauthorized physical access.

The environment is supposed to provide supporting mechanism to the TOE:

- A Radius server or TACACS+ server for external authentication/authorization decisions;
- NMS, logging server and SNMP trapserver used for administration of the TOE

In addition, it is assumed the Radius server, and TACACS+ server, and the NMS are all trusted and will not be used to attack the TOE.

- Peer router(s) for the exchange of dynamic routing information;
- A remote entities (PCs) used for administration of the TOE.

It is assumed that the ETH interface on MPU in the TOE will be accessed only through sub-network where the TOE hosts. The sub-network is separate from the application (or, public) networks where the interfaces on LPU in the TOE are accessible.

The authorized users will be competent, and not careless or wilfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

4.12 IT Security Objectives

The following objectives must be met by the TOE:

- O. DeviceAvail
  The TOE shall ensure its own availability.
- O.UserAvail
  The TOE shall ensure authorized users can access network resources through the TOE.
- O. DataFilter
  The TOE shall ensure that only allowed traffic goes through the TOE.
- O.Communication

The TOE must implement logical protection measures for network communication between the TOE and LMT/RMT from the operational environment.

- O.Authorization
  The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual administrators.
- O.Authentication
  The TOE must authenticate users of its user access.
- O.Audit
  The TOE shall provide functionality to generate audit records for security-relevant administrator actions.

4.13 Non-IT Security Objectives

- OE.NetworkElements:
  The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. For example, other routers for the exchange of routing information, PCs used for TOE administration, and Radius and TACACS+ servers for obtaining authentication and authorization decisions.
- OE.Physical:
  The TOE (i.e., the complete system including attached peripherals, such as a console, and hard disk inserted in the MPU) shall be protected against unauthorized physical access.
- OE.NetworkSegregation:
  The operational environment shall provide segregation by deploying the Ethernet interface on MPU in TOE into a local sub-network, compared to the interfaces on LPU in TOE serving the application (or public) network.
- OE.Person:
  Personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE.

4.14 Security Functional Requirements

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 User identity association
- FAU_SAR.1 Audit review
- FAU_SAR.3 Selectable audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.3 Action in case of possible audit data loss
- FCS_COP.1/AES Cryptographic operation

FCS_COP.1/RSA	Cryptographic operation
FCS_COP.1/MD5	Cryptographic operation
FCS_COP.1/HMAC-SHA256	Cryptographic operation
FCS_COP.1/DHKeyExchange	Cryptographic operation
FCS_CKM.1/AES	Cryptographic key generation
FCS_CKM.1/RSA	Cryptographic key generation
FCS_CKM.1/HMAC-SHA256	Cryptographic key generation
FCS_CKM.1/DHKey	Cryptographic key generation
FCS_CKM.4/AES	Cryptographic key destruction
FCS_CKM.4/RSA	Cryptographic key destruction
FCS_CKM.4/HMAC-SHA256	Cryptographic key destruction
FCS_CKM.4/DHKey	Cryptographic key destruction
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_DAU.1	Basic Data Authentication
FDP_IFC.1(1)	Subset information flow control- CPU-defend
FDP_IFC.1(2)	Subset information flow control- Data plane traffic control
FDP_IFF.1(1)	Simple security attributes - CPU-defend
FDP_IFF.1(2)	Simple security attributes – Data plane traffic control
FIA_AFL.1	Authentication failure handling
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.1	Timing of authentication –Administrator Authentication
FIA_UAU.5	Multiple authentication mechanisms
FIA_UID.1	Timing of identification – Administrator Identification
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1	Management of security attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security roles
FPT_STM.1	Reliable time stamps

- FTA_SSL.3 TSF-initiated termination
- FTA_TSE.1 TOE session establishment
- FTP_TRP.1 Trusted path
- FTP_ITC.1 Trusted channel

4.15 Security Function Policy

At the core of each chassis is the Versatile Routing Platform (VRP), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include assigning different privileges to administration users with different privilege levels; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

The Main Processing Units (MPU) integrate the main control unit and the system maintenance unit. The MPU controls and manages the system in a centralized way and is responsible for data exchange.

The Line Processing Units (LPU) are the actual hardware providing network traffic processing capacity. Network traffic is processed and forwarded according to routing decisions downloaded from VRP.

Besides the MPUs and LPUs, there are other type of boards on TOE, such as Switch Fabric Unit (SFU). Only MPU and LPU are security relevant.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5] . The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 31-05-2018. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 2 assurance package augmented with ALC_FLR.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Functional specification with complete summary
	ADV_TDS.1	Architectural design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Production support, acceptance procedures and automation
	ALC_CMS.2	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_OBJ.2	Security objectives
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Analysis of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall “pass” verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance listed in the ST[1] chapter 1.4.2. The Common Criteria Security Evaluation – Certified Configuration [8] describes all necessary steps to configure the TOE in the certified configuration.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The evaluator while performing other evaluation activities (ASE, ADV and AGD) considered direct attacks, monitoring and misuse attacks, to identify potential vulnerabilities.

The evaluator also, conducted a public domain vulnerability search to further search for potential vulnerabilities. Both TOE specific and TOE type search terms were used. The evaluator also used a vulnerability scanning tool (Nessus) to identify potential vulnerabilities.

The evaluator assessed all possible vulnerabilities found during evaluation. Potential vulnerabilities were found however none of them turned out to be possibly exploitable.

5.6 Developer's Tests

The developer test plan consists of 12 different categories of tests of 90 tests. The categories are based on major groupings of security functionalities, and, in combination with all SFRs and TSFIs.

5.7 Evaluators' Tests

For independent testing, the evaluator has chosen to perform some additional testing although the developer's testing was extensive but some additional assurance could be gained by additional testing.

For independent testing, the evaluator has made a sample of penetration tests performed by the developer.

Part of the tests were performed remotely (from Brightsight premises) between 26th March and 20th April 2018. The remaining tests were performed during an on-site visit at the Huawei premises in Beijng between the 23rd and 25th of April 2018.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that HUAWEI NE9000 Router version V800R010C00SPC200 meet the Common Criteria Part 3 augmented requirements of Evaluation Assurance Level 2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2conformant functionality in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of HUAWEI NE9000 Router version V800R010C00SPC200 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 "TOE Scope" and Section 5 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

The above "Evaluation Findings" include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of:

Hardware:

There are two types of chassis of NE9000 as shown in the Table below.

BOM	Module	Description	NE9000-8	NE9000-20
03056766	CR9D0MPUN180	NE9000-20 Main Processing Unit N1(MPUN1)	-	●
03057531	CR9D0MPUP180	NE9000-8 Main Processing Unit P1(MPUP1)	●	-
03056798	CR9D0SFUTF80	NE9000-20 Switch Fabric Unit F for Single Chassis(SFUI-F)	-	●
03057529	CR9D0SFUT480	NE9000-20 Switch Fabric Unit for Single Chassis(SFU4T-B)	-	●
03057530	CR9D0SFUT481	NE9000-8 Switch Fabric Unit for Single Chassis(SFU4T-A)	●	-
03056788	CR9D00E8NC80	8-Port 100GBase-CFP2 Integrated Line Process Unit(LPUI-1T)	●	●
03056789	CR9D00EFMB80	24-Port 40GBase-QSFP+ Integrated Line Process Unit(LPUI-1T)	●	●

03057028	CR9D00EPXF80	60-Port 10GBase LAN/WAN-SFP+ Integrated Line Process Unit(LPUI-1T)	●	●
03057024	CR9D00EDNB80	16-Port 100GBase-QSFP28 Integrated Line Process Unit(NE9000 LPUI-2T)	●	●
03057279	CR9D00D8NC80	8-Port 100GBase DWDM CFP Integrated Line Process Unit(LPUI-1T)	●	●
03057679	CR9D00EDNB8P	16-Port 100GBase-QSFP28 Integrated Line Process Unit CM(NE9000 LPUI-2T-CM)	●	●
03057680	CR9D00E8NC8P	8-Port 100GBase-CFP2 Integrated Line Process Unit CM(LPUI-1T-CM)	●	●
03057682	CR9D00EPXF8P	60-Port 10GBase LAN/WAN-SFP+ Integrated Line Process Unit CM(LPUI-1T-CM)	●	●
03057643	CR9D00DDNC80	16-Port 100G ETH/DWDM CFP2 Integrated Line Process	●	●

		Unit(LPUI-2T)		
03057989	CR9D00DDNC8P	16-Port 100G ETH/DWDM CFP2 Integrated Line Process Unit CM(LPUI-2T-CM)	●	●
03057932	CR9D00EENB80	20-Port 100GBase-QSFP28 Integrated Line Process Unit (LPUI-2T)	●	●
03057988	CR9D00EENB8P	20-Port 100GBase-QSFP28 Integrated Line Process Unit CM(LPUI-2T-CM)	●	●
03057534	CR9D00EKNB80	40-Port 100GBase QSFP28 Integrated Line Process Unit(LPUI-4T)	●	●
03057533	CR9D00EKNB8P	40-Port 100GBase QSFP28 Integrated Line Process Unit CM(LPUI-4T-CM)	●	●
03057532	CR9DLPUFK080	480G Flexible Card Line Processing Unit(NE9000 LPUF-480,2 sub-slots)	●	●
03057702	CR9DLPUFT280	2T Flexible Card Line Processing Unit(NE9000E LPUF-2T,2 sub-	●	●

		slots)		
03032JVE	CR9D00LFXF80	24-Port 1000M/10GBase LAN/WAN-SFP+ Flexible Card	●	●
03032JVD	CR9D00NBXF80	12-Port 10G OTN/ETH-SFP+ Flexible Card	●	●
03032PCC	CR9D00N2NC80	2-Port 100G OTN/ETH-CFP2 Flexible Card	●	●
03032NAC	CR9D00D8KC80	8-Port 100G ETH/DWDM CFP2 Flexible Card	●	●

Software:

NE9000 Router V800R010C00SPC200

Format:

V800R010C00SPC200-NE9000.cc

Users can verify the software by digital signature (The digital signature is also published on HUAWEI support website and in the ST).

TOE Documentation

The supporting guidance documents evaluated were:

[a] HUAWEI NE9000 Common Criteria Security Evaluation - Certified Configuration.doc, version 1.1, 28 April 2018.

[b] NE9000 V800R010C00SPC200 Product Documentation 01, version V800R010C00SPC200.

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

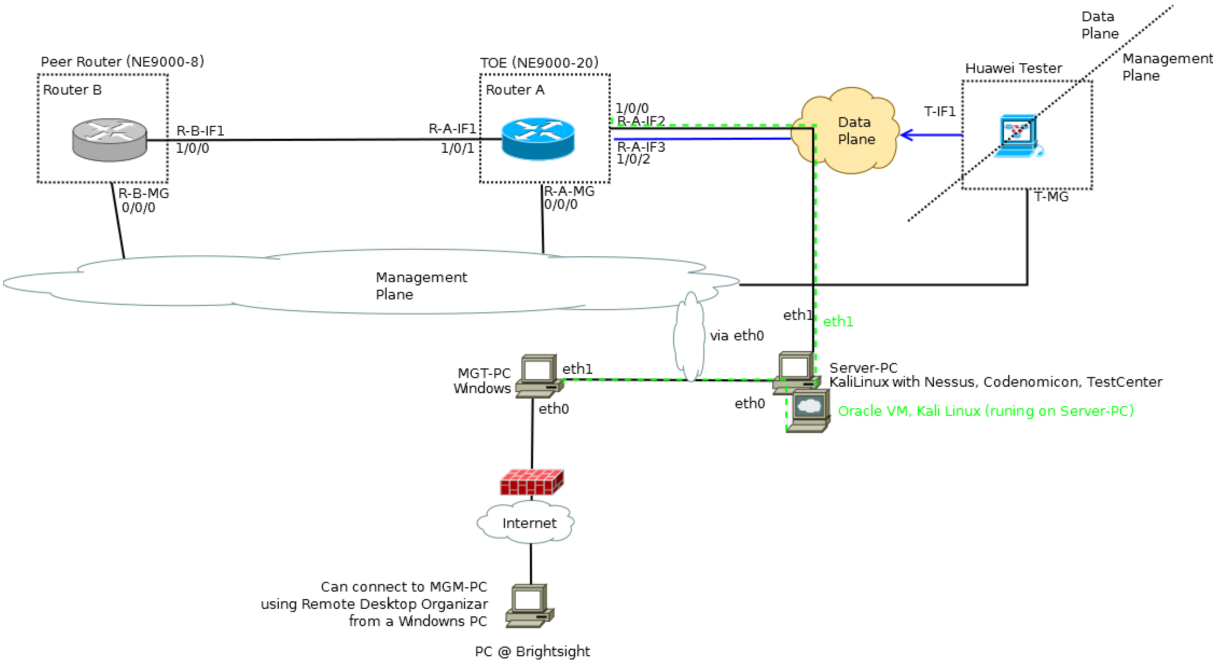
TOE Configuration

The following configuration was used for testing:

HARDWARE	One of the hardware models from each series listed in section TOE Identification
SOFTWARE	Product software version NE9000 Router V800R010C00SPC200, configured according to [8].
MANUALS	HUAWEI NE9000 Common Criteria Security Evaluation - Certified Configuration.doc, version 1.1, 28 April 2018. NE9000 V800R010C00SPC200 Product Documentation 01, version V800R010C00SPC200.

Environmental Configuration

The TOE is tested in the following test setup:



The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunctionwith the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Certificate

Certificate Identifier: SERTIT-114 C

Product Name: Huawei NE9000 Router

Version and Release Numbers: V800R010C00SPC200

Type of Product: Network Device

Product Manufacturer: HUAWEI Technologies Co., Ltd

Assurance Type: EAL 2 augmented with ALC_FLR.2

Evaluation Criteria: Common Criteria Version 3.1 Revision 5

Name of IT Security Evaluation Facility: Brightsight B.V.

Name of Validation Body and Certification Authority: SERTIT

Certification Report Identifier: SERTIT-114 CR, issue 1.0, 04 July 2018

Certificate Issued Date: 04. July 2018 Certificate Expiry Date: 04. July 2023

Kjartan Jæger Kvassnes
Certifier

Arne H. Rage
Arne Høye Rage
Quality Assurance

Jørn Arnesen
Head of SERTIT

SERTIT
Norwegian Certification Authority for IT Security

CC Recognition Arrangement for cPPs or components up to EAL 2 and ALC_FLR

SOGIS
IT SECURITY CERTIFIED

SOGIS Recognition Agreement for components up to EAL 4