Certification Report

Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100

Sponsor and developer: ***Huawei Technologies Co., Ltd.***
Administration Building, Huawei Industrial Base, Bantian, Longgang
Shenzhen 518129
People's Republic of China

Evaluation facility: ***SGS Brightsight B.V.***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number: **NSCIB-CC-0615858-CR**

Report version: **1**

Project number: **0615858**

Author(s): **Kjartan Jæger Kvassnes**

Date: **16 May 2023**

Number of pages: **12**

Number of appendices: **0**

Head Office:
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 Netherlands Chamber of Commerce (KVK), 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 licence is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, 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, 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

The presence of the Common Criteria Recognition Arrangement (CCRA) and the SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS Mutual Recognition Agreement (SOG-IS MRA) and will be recognised by the participating nations.

International recognition

The CCRA was signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the Common Criteria (CC). Since September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR.

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

European recognition

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

For details of the current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies, see https://www.sogis.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100. The developer of the Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100 is Huawei Technologies Co., Ltd. located in Shenzhen, People's Republic of 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 TOE is the software running on the Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 series firewalls. These firewalls consist of both hardware (non-TOE) and software. The software running on the firewalls is denominated Versatile Routing Platform (VRP) developed by Huawei.

The TOE has been evaluated by SGS Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on Date 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 Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100, 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 Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100 are advised to verify that their own environment is consistent with the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]* [1] for this product provide sufficient evidence that the TOE meets the EAL4 Include the following, if applicable: augmented (EAL4+) 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]* (Parts I, II and III).

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. Note that the certification results apply only 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 available for public review.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100 from Huawei Technologies Co., Ltd. located in Shenzhen, People's Republic of China.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Software	USG6000F_V600R021C10SPC100	V600R021C10SPC100
	USG12000_V600R021C10SPC100	V600R021C10SPC100
	Eudemon1000E-F_V600R021C10SPC100	V600R021C10SPC100
	Eudemon9000E-X_V600R021C10SPC100	V600R021C10SPC100
	AntiDDoS1900_V600R021C10SPC100	V600R021C10SPC100
	AntiDDoS12000_V600R021C10SPC100	V600R021C10SPC100

TOE in the certified configuration can only run on the following non-TOE Hardware:

- Eudemon9000E-X4(HTM)
- Eudemon9000E-X8(HTM)
- Eudemon1000E-F15(HTM)
- Eudemon1000E-F25(HTM)
- Eudemon1000E-F35(HTM)
- Eudemon1000E-F55(HTM)
- Eudemon1000E-F85(HTM)
- USG12004(HTM)
- USG12008(HTM)
- USG6615F(HTM)
- USG6625F(HTM)
- USG6635F(HTM)
- USG6655F(HTM)
- USG6685F(HTM)
- USG6715F(HTM)
- USG6725F(HTM)
- AntiDDoS1905(HTM)
- AntiDDoS1908(HTM)
- AntiDDoS12004(HTM)
- AntiDDoS12008(HTM)

Where HTM indicates the hardware has built-in Hardware Trust Module

To ensure secure usage a set of guidance documents is provided, together with the Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100. For details, see section 2.5 "Documentation" of this report.

2.2 Security Policy

The TOE provides the following security features:

- Security audit
- Cryptographic support
- Identification and authentication
- Secure Management
- Protection of the TSF
- TOE access through user authentication
- Trusted path and channels for device authentication
- Trusted software updates
- Firewall

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

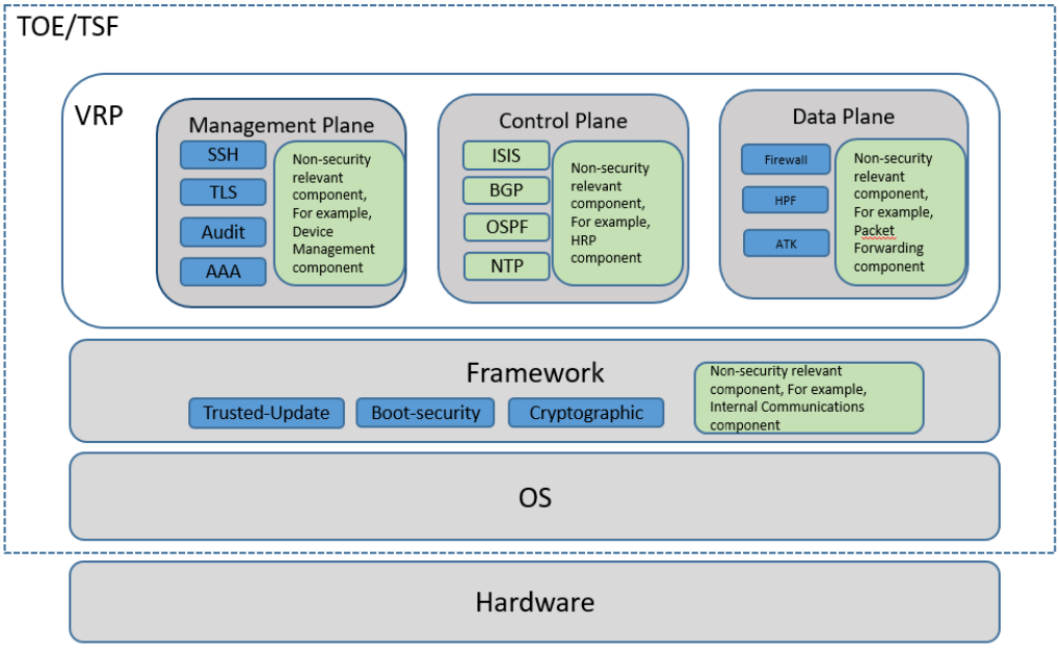
The assumptions defined in the Security Target are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. For detailed information on the security objectives that must be fulfilled by the TOE environment, see section 4.2 of the *[ST]*.

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.

2.4 Architectural Information

The logical architecture, originating from the Security Target [ST] of the TOE can be depicted as follows:



2.5 Documentation

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

Identifier	Version
AGD_PRE Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewalls running VRP software V600R021C10 Preparative Procedures, dated 2023-2-28	V04
AGD_OPE Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewalls running VRP software V600R021C10 Operational User Guidance, dated 2022-07-14	V03
HiSecEngine AntiDDoS1900 V600R021C10 Upgrade Guide, dated 2022-04-15	v01
HiSecEngine AntiDDoS12000 V600R021C10 Upgrade Guide, dated 2022-04-15	v01
HiSecEngine USG6000F V600R021C10 Upgrade Guide, dated 2022-04-15	v01
HiSecEngine USG12000 V600R021C10 Upgrade Guide, dated 2022-04-15	v01
HUAWEI Eudemon1000E-F V600R021C10 Upgrade Guide, dated 2022-04-15	v01
HUAWEI Eudemon9000E-X V600R021C10 Upgrade Guide, dated 2022-04-15	v01
HiSecEngine AntiDDoS1900+SecoManager Solution V600R021C10 Product Documentation V600R021C10, dated 2022-09-09	V04
HiSecEngine AntiDDoS12000+SecoManager Solution V600R021C10 Product Documentation V600R021C10, dated 2022-09-09	V04
HiSecEngine USG6000F V600R021C10 Product Documentation V600R021C10, dated 2022-09-06	V04
HiSecEngine USG12000 V600R021C10 Product Documentation V600R021C10, dated 2022-09-06	V04
HUAWEI Eudemon1000E-F V600R021C10 Product Documentation V600R021C10, dated 2022-09-06	V04
HUAWEI Eudemon9000E-X, Eudemon9000E-F V600R021C10 Product Documentation V600R021C10, dated 2022-09-06	V04

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 performed extensive testing on functional specification, subsystem and module level. All parameter choices were addressed at least once. All boundary cases identified were tested explicitly, and additionally the near-boundary conditions were covered probabilistically. The testing was largely automated using industry standard and proprietary test suites. Test scripts were used extensively to verify that the functions return the expected values.

For the testing performed by the evaluators, the developer provided samples and a test environment. The evaluators reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

2.6.2 Independent penetration testing

To identify potential vulnerabilities the evaluator performed the following activities:

- 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 were 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) 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 analyzed, and some of the potential vulnerabilities were concluded not exploitable within in the Enhanced-Basic attack potential, or covered by guidance. For remaining potential vulnerabilities, penetration tests were devised.

The total test effort expended by the evaluators was 5 weeks. During that test campaign, 100% of the total time was spent on logical tests.

2.6.3 Test configuration

The TOE was tested in the following configuration:

- V600R021C10SPC100 running on
  - USG6615F(HTM)
  - Eudemon1000E- F15(HTM)
  - AntiDDOS1905(HTM)

The evaluator analysed the differences between the non-TOE hardware models used for testing and the hardware models listed in section 2.1 and concluded that the hardware models are equivalent from a security perspective, thus the test results are valid for all hardware models listed in section 2.1

2.6.4 Test results

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

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

No exploitable vulnerabilities were found with the independent penetration tests.

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

2.7 Reused Evaluation Results

There has been extensive reuse of the ALC aspects for the sites involved in the development and production of the TOE, by use of 2 Site Technical Audit Reports.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100.

2.9 Evaluation Results

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

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

Based on the above evaluation results the evaluation lab concluded the Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 4 augmented with ALC_FLR.2**. This implies that the product satisfies the security requirements specified in Security Target *[ST]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 "Documentation" contains necessary information about the usage of the TOE.

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

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

The strength of the cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: <none>, which are out of scope as there are no security claims relating to these.

3 Security Target

The Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100 Security Target, Version 0.8, Dated 31 March 2023 *[ST]* is included here by reference.

4 Definitions

This list of acronyms and definitions contains elements that are not already defined by the CC or CEM:

ACL	Access Control List
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
DES	Data Encryption Standard
IT	Information Technology
ITSEF	IT Security Evaluation Facility
LAN	Local Area Network
MAC	Message Authentication Code
MITM	Man-in-the-Middle
NSCIB	Netherlands Scheme for Certification in the area of IT Security
SCP	Secure Channel Protocol
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
RADIUS	Remote Authentication Dial-In User Service
TOE	Target of Evaluation

5 Bibliography

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

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 5, April 2017
[CEM]	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017
[ETR]	Evaluation Technical Report “Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100” – EAL4+, 22-RPT-740, Version 2.0, 3 April 2023
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019
[ST]	Huawei Eudemon9000E & Eudemon1000E & USG12000 & USG6000F & AntiDDoS1000 & AntiDDoS12000 Series Firewall running VRP software V600R021C10SPC100 Security Target, Version 0.8, Dated 31 March 2023

(This is the end of this report.)