| | |
|---|---|
| REF: 2016-40-INF-2019 v3 | Created by: CERT9 |
| Target: Expediente | Revised by: CALIDAD |
| Date: 07.09.2017 | Approved by: TECNICO |

# CERTIFICATION REPORT

File: 2016-40 Huawei Eudemon 8000E-X V300R001C01SPC300B113

Applicant: 440301192W HUAWEI Technologies Co., Ltd.

References:

[EXT-3148] Certification request of Huawei Eudemon 8000E-X V300R001C01SPC300B113

[EXT-3366] Evaluation Technical Report of Huawei Eudemon 8000E-X V300R001C01SPC300B113.

The product documentation referenced in the above documents.

Certification report of the product “Huawei Eudemon8000E-X/USG9500 Series Firewall version V300R001C01SPC300B113”, as requested in [EXT-3148] dated 12-09-2016, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-3366] received on 11/05/2017.

## TABLE OF CONTENTS

# EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product "Huawei Eudemon8000E-X/USG9500 Series Firewall version V300R001C01SPC300B113".

The TOE is a firewall system composed of a hardware platform and a software running within the platform as a whole system. The evaluation has been performed on product series with multiple HW platforms. The applicable HW platforms of the TOE have been identified as shown in the table below:

| Series Id | Model Name | ESN |
|---|---|---|
| Eudemon8000E-X<br>Secospace USG9500 | Eudemon8000E-X3 | 210235G6QB10E5000001 |
| | Eudemon8000E-X8 | 210235G6QD10E5000009 |
| | Eudemon8000E-X8 | 210235G6QDZ0C5000008 |
| | Eudemon8000E-X16 | 2102351931P0B5000301 |
| | USG9520 | 210235G7F6 |

The version of the TOE software installed in the testing platform is V300R001C01SPC300B113.

**Developer/manufacturer**: Huawei Technologies Co., Ltd..

**Sponsor**: Huawei Technologies Co., Ltd..

**Certification Body**: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

**ITSEF**: Epoche & Espri S.L.U..

**Protection Profile**: None.

**Evaluation Level**: Common Criteria v3.1 R4 - EAL4+ALC_FLR.1.

**Evaluation end date**: 11 May 2017.

All the assurance components required by the evaluation level EAL4 (augmented with ALC_FLR.1) have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL4+ALC_FLR.1, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product "Huawei Eudemon8000E-X/USG9500 Series Firewall version V300R001C01SPC300B113", a positive resolution is proposed.

## TOE SUMMARY

The TOE consists of a hardware platform and software image integrated as a whole system. The TOE is designed to provide firewall, VPN, VLAN, antivirus protection, anti-spam protection and content filtering etc. to provide protection on TCP/IP networks. It can protect computer networks from abuse.

The series firewall resides between the network it is protecting and an external network such as the Internet, restricting the information flow between the networks to that permitted by a policy (set of rules) defined by the Security Administrator. They detect and eliminate the most damaging, content-based threats from email and web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real-time; without degrading network performance. In addition to providing stateful application-level protection, the TOE delivers a full range of network-level services including; firewall, Virtual Private Network (VPN), Virtual Local Area Network (VLAN), antivirus protection, anti-spam protection and content filtering etc.; using dedicated, easily managed platforms.

**TOE major security features**

The major security features implemented by the TOE and subject to evaluation (no assurance can be supposed to any other functionality) to, can be summarised as follows:

- Authentication
  - The TOE can authenticate administrative users by user name and password. Administration may either be performed locally using the Local Console CLI or remotely using the Network Web-Based GUI or Network CLI. The TOE provides a local authentication scheme for this, or can optionally enforce authentication decisions obtained from a Radius or TACACS+ server in the IT environment.
  - Authentication is always enforced for network remote sessions via SSH, SFTP (Secure FTP),and HTTPS (Web-Based GUI) sessions. Authentication for access via the console is always enabled and password protected.
- Access Control
  - The TOE has the ability to control the administrator permissions for every administrator account. This control is performed using three different control policies: administrator roles, administrator levels and users built-in.
- Communication Security
  - The TOE provides communication security by implementing SSH protocol.
  - Two versions of SSH: SSHv1 (SSH1.5) and SSHv2 (SSH2.0) are implemented.
- Flow Control

- The TOE provides a policy mechanism based on security rules and traffic engineering rules. For each policy item, aspects like packet source and destination addresses, in and out interfaces, security zones, and ports can be used as filters, and actions like allow, block or even traffic engineering processes can be assigned. Through such mechanism, we can define a policy and drop attacks for the TOE itself.
- The TOE also offers a feature Access Control List (ACL) for filtering incoming and outgoing information flow.

- Security functionality management
  - Security functionality management includes not only authentication, administrator role, but also managing security related data consisting of configuration profile and runtime parameters.
- Cryptographic functions
  - Cryptographic functions are required by security features as dependencies, where:
    - AES is used as default encryption algorithm for SSH.
    - 3DES is used as optional encryption algorithm for SSH.
    - RSA is used in user authentication when user tries to authenticate and gain access to the TOE.
    - HMAC-SHA is used as verification algorithm for packets of SSH protocols.

## SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL4 and the evidences required by the additional component ALC_FLR.1, according to Common Criteria v3.1 R4.

| | |
|---|---|
| ASE: Security Target Evaluation | ASE_INT.1. ST Introduction |
| | ASE_CCL.1. Conformance claims |
| | ASE_SPD.1. Security problem definition |
| | ASE_OBJ.2. Security objectives |
| | ASE_ECD.1. Extended component definition |
| | ASE_REQ.2. Derived security requirements |
| | ASE_TSS.1. TOE summary specification |
| ADV: Development | ADV_ARC.1. Security architecture description |

| | |
|---|---|
| | ADV_FSP.4. Complete functional specification |
| | ADV_IMP.1. Implementation representation of the TSF |
| | ADV_TDS.3. Basic modular design |
| AGC: Guidance documents | AGD_OPE.1. Operational user guidance |
| | AGD_PRE.1. Preparative procedures |
| ALC: Life cycle support | ALC_CMC.4. Production support, acceptance procedures and automation |
| | ALC_CMS.4. Problem tracking CM coverage |
| | ALC_DEL.1. Delivery procedures |
| | ALC_DVS.1. Identification of security measures |
| | ALC_FLR.1. Flaw remediation |
| | ALC_LCD.1. Developer defined life-cycle model |
| | ALC_TAT.1. Well-defined development tools |
| ATE: Tests | ATE_COV.2. Analysis of coverage |
| | ATE_DPT.1. Testing: basic design |
| | ATE_FUN.1. Functional tests |
| | ATE_IND.2. Independent testing - sample |
| AVA: Vulnerability assessment | AVA_VAN.3. Focused vulnerability analysis |

## SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

| | |
|---|---|
| FCS: Cryptographic support | FCS_COP.1. Cryptographic operation |
| | FCS_CKM.1. Cryptographic key generation |
| FDP: User data protection | FDP_ACC.1. Subset access control |

| | |
|---|---|
| | FDP_ACF.1. Security attribute based access control |
| | FDP_ICF.1. Subset information flow control |
| | FDP_IFF.1. Simple security attributes |
| FIA: Identification and authentication | FIA_ATD.1. User attribute definition |
| | FIA_UAU.2. User authentication before any action |
| | FIA_UID.2. User identification before any action |
| FMT: Security management | 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 |
| FTA: TOE access | FTA_SSL.3. TSF initiated termination |

## IDENTIFICATION

**Product**: "Huawei Eudemon8000E-X/USG9500 Series Firewall version V300R001C01SPC300B113"

**Security Target:** "Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 Security Target, version 1.3 (May 5, 2017)".

**Security Target Lite:** "Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 Security Target, version 1.4 (September 7, 2017)".

**Protection Profile**: None.

**Evaluation Level**: Common Criteria v3.1 R4 EAL4+ALC_FLR.1.

## SECURITY POLICIES

The "Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 Security Target, version 1.3 (May 5, 2017)" does not define any Organizational Security Policy.

# ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

### Assumption 01: A.PhysicalProtection

The TOE is physically protected so that only the authorized user of the TOE has physical access.

### Assumption 02: A.NetworkElements

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

- A Radius server or TACACS+ server for external authentication/authorization decisions.
- Peer router(s) for the exchange of dynamic routing information.
- Remote entities (PCs) used for administration of the TOE.

### Assumption 03: A.NetworkSegregation

It is assumed that the ETH interface in the TOE will be accessed only through an independent local network. This network is separate from the networks that use the other interfaces of the TOE.

### Assumption 04: A.NoEvil

The administration users who manage the TOE and TOE environmental components are appropriately trained, non-hostile, and follow all guidance.

## CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product “Huawei Eudemon8000E-X/USG9500 Series Firewall version V300R001C01SPC300B113”, although the agents implementing attacks have the attack potential according to the Enhanced Basic of EAL4+ALC_FLR.1 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

### Threat 01: T.UnwantedTraffic

Any network user that sends unwanted/unexpected traffic to/through the TOE will: cause the TOE and/or resources on the network to become too slow or unavailable, or reach resources on the network that it is not allowed to reach.

### Threat 02: T.UnauthenticatedAccess

A user who is not an administrator gains access to the management interface of the TOE

### Threat 03: T.UnauthorizedAccess

An administrator authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for.

### Threat 04: T.Eavesdrop

An eavesdropper is able to intercept, and potentially modify or re-use information assets that are exchanged between:

- TOE and LMT/RMT (management traffic).
- TOE and other routers/switches (routing information).

## OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

### Environment objective 01: OE.NetworkElements

The operational environment shall provide network devices that the TOE needs to cooperate with:

- A Radius server or TACACS+ server for external authentication/authorization decisions.
- Peer router(s) for the exchange of dynamic routing information.
- Remote entities (PCs) used for administration of the TOE.

### Environment objective 02: OE.Physical

The operational environment shall protect the TOE against unauthorized physical access.

### Environment objective 03: OE.NetworkSegregation

The operational environment shall ensure that hat the ETH interface in the TOE will be accessed only through an independent local network This network is separate from the networks that use the other interfaces of the TOE.

### Environment objective 04: OE.Manage

Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system and its environment are used securely.

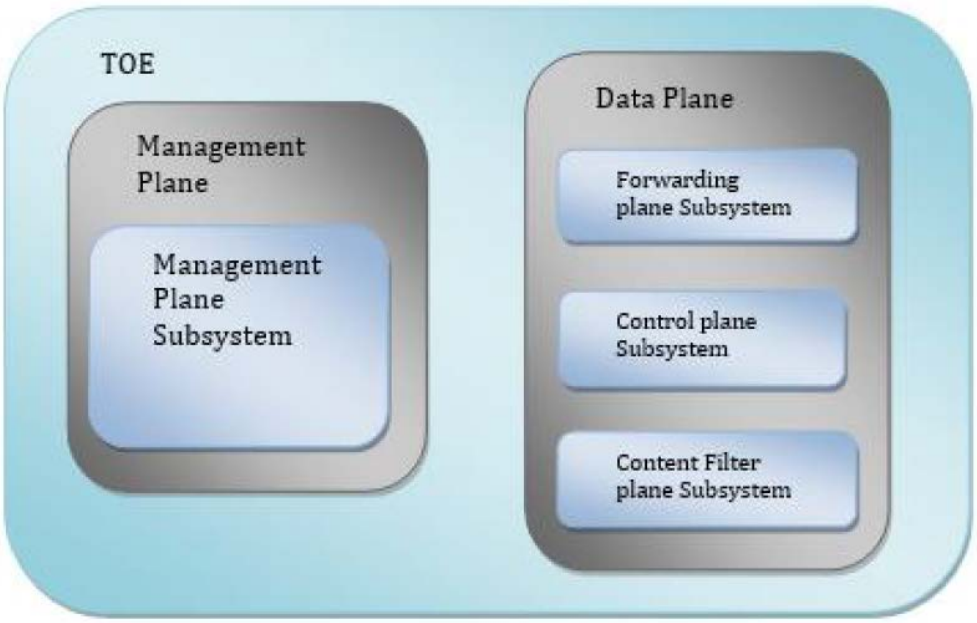
The details of the product operational environment (assumptions and threats) and the TOE security requirements are included in the associated security target.

# ARCHITECTURE

## LOGICAL ARCHITECTURE

The TOE software is divided into two different planes: Management Plane (MP) and a Data Plane (DP), as shown in the figure in the next page.

- The Management Plane is composed by only one subsystem called Management Plane Subsystem. It provides the following security functionalities: configuration management, protocol, status, routing management and device management.
- The Data Plane is composed by three subsystems called Forwarding Plane Subsystem, Control Plane Subsystem, and Content Filter Subsystem.
    - Forwarding Plane Subsystem provides firewall packet forwarding, security check and traffic control. (Flow control policy, Communication Security).
    - Control Plane Subsystem provides user authentication (local or remote using a RADIUS or TACACS server), relation analysis and remote query for specific operation. (Authentication, Communication security).
    - Content Filter Plane Subsystem provides functionality which is not SFR-related such as anti-virus, anti-spam, DPI (Deep Protocol Identification), and other non-security features.




## PHYSICAL ARCHITECTURE

The "Huawei Eudemon8000E-X/USG9500 Series Firewall version V300R001C01SPC300B113" groups a set of different products, all of them have identical security functionalities. They differ in their modularity and throughput. The evaluated platforms are included in the table below.

| Series Id | Model Name | ESN |
|---|---|---|
| Eudemon8000E-X Secospace USG9500 | Eudemon8000E-X3 | 210235G6QB10E5000001 |
| | Eudemon8000E-X8 | 210235G6QD10E5000009 |
| | Eudemon8000E-X8 | 210235G6QDZ0C5000008 |
| | Eudemon8000E-X16 | 2102351931P0B5000301 |
| | USG9520 | 210235G7F6 |

The binary files names and MD5 hashes are shown in the table below:

| Binary file | MD5 |
|---|---|
| Eudemon_8000E_V300R001C01SPC300B113_X3.cc | d6fc00f5a7e60e5bcc58e85c43251fec |
| Eudemon_8000E_V300R001C01SPC300B113_X8X16.cc | c685782f735ca0b1 |

| Binary file | MD5 |
|---|---|
| | 5bc34d63f480416f |

# DOCUMENTS

The Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- "Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 Security Target, version 1.4 (September 7, 2017)".
- Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 Operational User Guidance, version 1.0.
- Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 Preparative Procedure, version 1.1.

# PRODUCT TESTING

The developer has executed test for all the security functions. All the tests have been performed by the developer in its premises, with a satisfactory result.

During the evaluation process it has been verified each unit test checking that the security functionality that covers is been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

In addition, the lab has devised a test for each of the security function of the product verifying that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

# EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product "Huawei Eudemon8000E-X/USG9500 Series Firewall version V300R001C01SPC300B113" it is necessary the disposition of the following components:

| Series Id | Model Name | ESN |
|---|---|---|
| Eudemon8000E-X Secospace USG9500 | Eudemon8000E-X3 | 210235G6QB10E5000001 |
| | Eudemon8000E-X8 | 210235G6QD10E5000009 |
| | Eudemon8000E-X8 | 210235G6QDZ0C5000008 |
| | Eudemon8000E-X16 | 2102351931P0B5000301 |
| | USG9520 | 210235G7F6 |

The binary files names and MD5 hashes are shown in the table below:

| Binary file | MD5 |
|---|---|
| Eudemon_8000E_V300R001C01SPC300B113_X3.cc | d6fc00f5a7e60e5bcc58e85c43251fec |
| Eudemon_8000E_V300R001C01SPC300B113_X8X16.cc | c685782f735ca0b15bc34d63f480416f |

## EVALUATION RESULTS

The product "Huawei Eudemon8000E-X/USG9500 Series Firewall version V300R001C01SPC300B113" has been evaluated against the Security Target "Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 Security Target, version 1.3 (May 5, 2017)".

All the assurance components required by the evaluation level EAL4+ALC_FLR.1 have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL4+ALC_FLR.1, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

## COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product:

- The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

# CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product "Huawei Eudemon8000E-X/USG9500 Series Firewall version V300R001C01SPC300B113", a positive resolution is proposed.

# GLOSSARY

| | |
|---|---|
| CCN | Centro Criptológico Nacional |
| CNI | Centro Nacional de Inteligencia |
| EAL | Evaluation Assurance Level |
| ETR | Evaluation Technical Report |
| OC | Organismo de Certificación |
| TOE | Target Of Evaluation |

# BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4 Final, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4 Final, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4 Final, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4 Final, September 2012.

# SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is stored and protected in the Certification Body premises. This document is identified as:

- "Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 Security Target, version 1.3 (May 5, 2017)".

The public version of this document constitutes the ST Lite. The ST Lite has also been reviewed for the needs of publication according to [CCDB-2006-04-004], and it is published along with this certification report in the Certification Body and CCRA websites. The ST Lite identifier is:

- “Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300B113 Security Target, version 1.4 (September 7, 2017)”.