REF: 2014-12-INF-1600 v1	Created by: CERT9
Difusión: Expediente	Revised by: CALIDAD
Fecha: 20.04.2016	Approved by: TECNICO

CERTIFICATION REPORT

File: 2014-12 Eudemon8000E-X/USG9500 Series Firewall

Applicant: 440301192W HUAWEI Technologies Co., Ltd.

References:

[EXT-2419] Certification request of Eudemon8000E-X/USG9500 Series Firewall

[EXT-2972] Huawei Eudemon8000E-X/USG9500 Series Firewall Evaluation Technical Report, version 2.0, 23-12-2015

The product documentation referenced in the above documents.

Certification report of the product Eudemon8000E-X/USG9500 Series Firewall, as requested in [EXT-2419] dated 7/03/2014, and evaluated by the laboratory Epoche & Espri S.L.U, as detailed in the Evaluation Technical Report [EXT-2972] received on 23/12/2015.

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TABLE OF CONTENTS

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

EXECUTIVE SUMMARY

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

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 following table.

Series	Model	ESN
8000E	Eudemon8000E-X3	210235G6QB10E5000001
	Eudemon8000E-X8	210235G6QD10E5000009
	USG9520	210235G7F6
	Eudemon8000E-X8	210235G6QDZ0C5000008
	Eudemon8000E-X16	2102351931P0B5000301

The version of the TOE SW installed in the testing platforms 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: No.

Evaluation Level: Common Criteria v3.1 R4 – EAL3 + ALC_CMC.4 + ALC_CMS.4

Evaluation end date: 23/12/2015.

All the assurance components required by the evaluation level EAL3+ (augmented with ALC_CMC.4 Production support, acceptance procedures and automation + ALC_CMS.4 Problem tracking CM coverage) 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 EAL3 + ALC_CMC.4 + ALC_CMS.4, 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 (running on the above mentioned platforms), a positive resolution is proposed.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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: SSH1 (SSH1.5) and SSH2 (SSH2.0) are implemented.

- Flow Control Policy
  - The TOE provides a policy mechanism based on security rules and traffic engineering rules. For each policy item, aspects like packet source and

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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 evidences required to fulfil the evaluation level EAL3+ and the evidences required by the additional components ALC_CMC.4 Production support, acceptance procedures and automation and ALC_CMS.4 Problem tracking CM coverage, according to Common Criteria v3.1 R4.

Class	Family/Component
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.3 Functional specification with complete summary ADV_TDS.2 Architectural design
AGD: 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

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

	ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

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

Class	Family/Component
FCS	COP.1/AES COP.1/3DES COP.1/RSA COP.1/HMAC-SHA CKM.1/AES CKM.1/3DES CKM.1/RSA CKM.1/HMAC_SHA
FDP	ACC.1 ACF.1 IFC.1 IFF.1
FIA	ATD.1 UAU.2 UID.2
FMT	MOF.1 MSA.1 MSA.3 SMF.1 SMR.1
FTA	SSL.3

IDENTIFICATION

Product: Huawei Eudemon8000E-X/USG9500 Series Firewall

SW version: V300R001C01SPC300B113
HW platforms ESN:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Series	Model	ESN
8000E	Eudemon8000E-X3	210235G6QB10E5000001
	Eudemon8000E-X8	210235G6QD10E5000009
	USG9520	210235G7F6
	Eudemon8000E-X8	210235G6QDZ0C5000008
	Eudemon8000E-X16	2102351931P0B5000301

Security Target: Huawei Eudemon8000E-X/USG9500 Series Firewall V300R001C01SPC300 Security Target, version 1.20, December 2015

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 – EAL3+ALC_CMC.4+ALC_CMS.4

SECURITY POLICIES

There are no Organizational Security Policies defined for this evaluation.

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 [ST]. 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 Name	Assumption Definition
A.PhysicalProtection	The TOE is physically protected so that only the authorized user of the TOE has physical access.
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.
A.NetworkSegregation	It is assumed that the ETH management

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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

THREATS

The threats to the IT assets against which protection is required by the TOE or by the security environment are listed below.

The information assets to be protected are the information stored, processed or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information and passwords, routing configuration data, etc.) and other information that the TOE facilitates access to (such as system software, patches and network traffic routed by the TOE) are all considered part of information assets.

The threats defined are:

Threat Name	Threat Definition
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.
T.UnauthenticatedAccess	A user who is not an administrator gains access to the management interface of the TOE
T.UnauthorizedAccess	An administrator authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for.
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)

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

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.

Security Objectives that are to be satisfied by the environment:

Environment Security Objective	Definition
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.
OE.Physical	The operational environment shall protect the TOE against unauthorized physical access.
OE.NetworkSegregation	The operational environment shall ensure that the ETH management 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.
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.

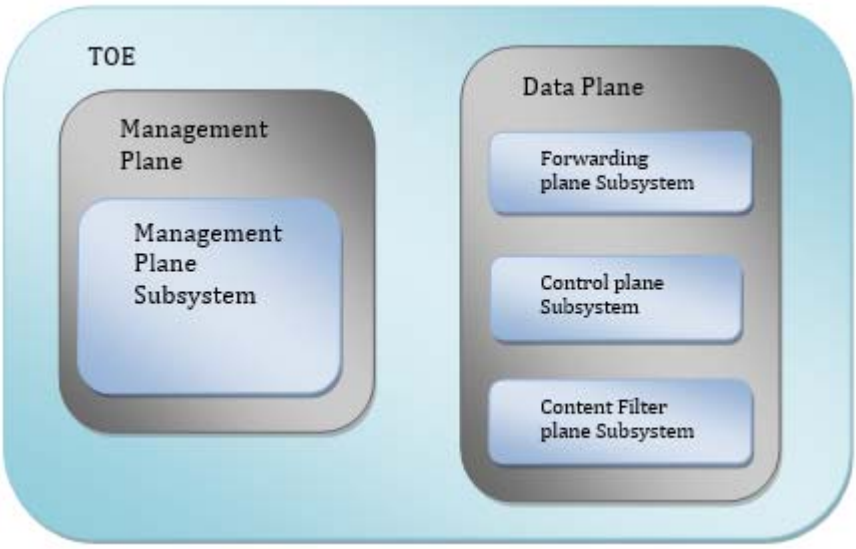
ARCHITECTURE

LOGICAL ARCHITECTURE

The logical architecture is depicted in the following figure:

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es



The TOE software is divided into two different planes: Management Plane (MP) a Data Plane (DP). MP is composed by only one subsystem called Management plane Subsystem. DP is composed by three subsystems called Forwarding plane Subsystem, Control plane Subsystem, and Content Filter Subsystem.

Management plane subsystem provides configuration management, protocol, status, routing management and device management. (Security Function Management, Cryptographic support, Access control, Authentication, Communication Security)

Forwarding plane subsystem provide 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 analyze 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. This subsystem is irrelevant with the security features, and therefore will no longer be mentioned along this security target.

PHYSICAL ARCHITECTURE

The TOE is defined by its name and version number:

- Eudemon8000E-X/USG9500 Series Firewall.

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

The following platforms

Series	Model	ESN
8000E	Eudemon8000E-X3	210235G6QB10E5000001
	Eudemon8000E-X8	210235G6QD10E5000009
	USG9520	210235G7F6
	Eudemon8000E-X8	210235G6QDZ0C5000008
	Eudemon8000E-X16	2102351931P0B5000301

running the SW version: V300R001C01SPC300B113. Two different binaries allocated to the platforms as follows:

Binary identifier
File names (for X3 and UGS 9520 platforms): - Eudemon_8000E_V300R001C01SPC200_X3.cc - Secospace_USG9520_V300R001C01SPC200_X3.cc HASH: 3d0c2d7d45db97113289a96175af4a66.
File names (for X8, X16, UGS 9560 and UGS 9580 platforms): - Eudemon_8000E_V300R001C01SPC200_X8X16.cc - Secospace_USG9580&9560_V300R001C01SPC200_X8X16.cc HASH: d26263bba05b0c35567421932ebc0aeb.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

The manual and guides of the product are published at technical support web site (http://www.huawei.com) of Huawei Technologies Co., Ltd. The user can retrieve, browse, and download all the documents online from this site.

- Huawei Eudemon8000E-X/USG9500 Firewall V300R001SPC300B113 Operational User Guidance, version 0.9, September 2015

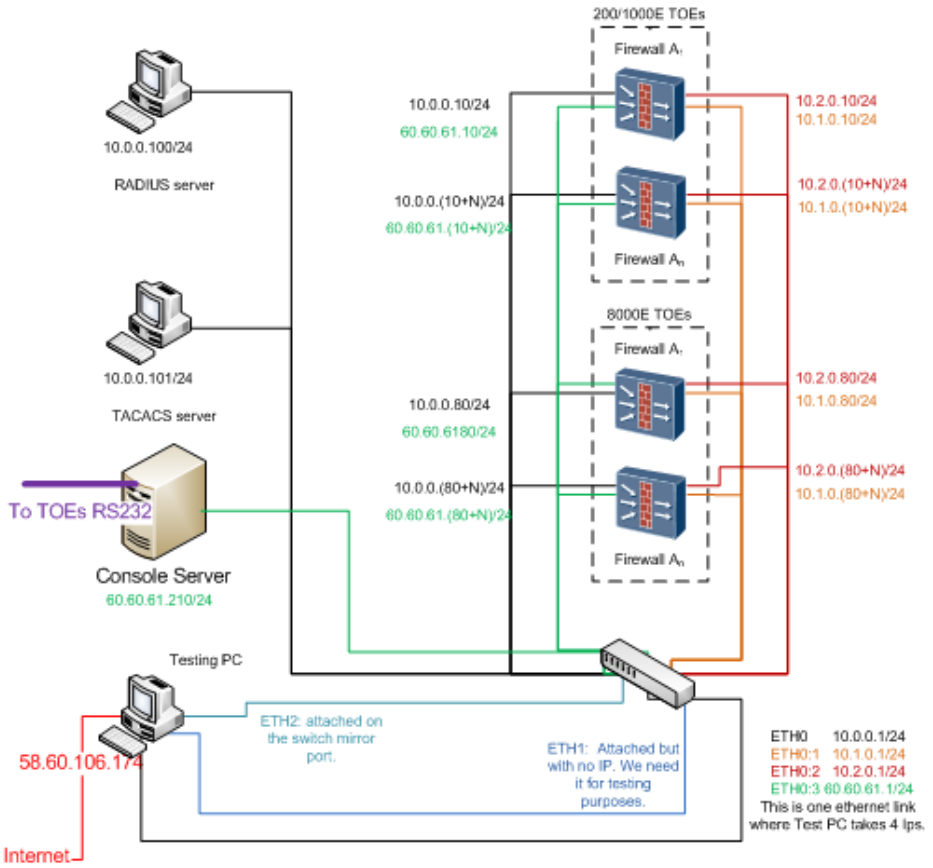
PRODUCT TESTING

The tests performed by both the evaluator and the developer are based on the TSFIs description included in the functional specification, the SFRs description included in [ST], and the subsystems and modules defined in the TOE design documentation.

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE configuration used to execute the independent tests is consistent with the evaluated configuration according to security target [ST]. The evaluator has repeated all the cases specified by the developer in the test documentation and has compared the obtained results with those obtained by the developer and documented in each associated report. The test repetition performed by the evaluator has demonstrated that the test plan and report provided by the vendor contains information enough to make a reader able to repeat all tests included. Additionally, after the repetition, the evaluator has obtained the same results as the expected ones. The independent testing has covered 100% of SFRs of the [ST] and TSFIs defined in the functional specification for the TOE, sampling has not been performed. The test cases have taken into account critical parameters values, searching that the TOE behaves in a non-expected manner. There has not been any deviation from the expected results under the environment defined in security target [ST].

The deployed testing platforms for the evaluation are presented in the following figure:

C/ Argentona nº 20
Email: organismo.certificacion@cni.es



PENETRATION TESTING

The evaluator has performed an installation and configuration of the TOE and its operational environment following the steps included in the installation and operation manuals. The TOE does NOT present exploitable vulnerabilities under the environment defined in the security target [ST]. All identified vulnerabilities can be considered closed if the TOE is installed and operated according to the security target [ST] and related documentation. The overall test result is that no deviations were found between the expected and the actual test results taking into account that environment. No attack scenario with the attack potential “Basic” has been successful in the TOE’s operational environment as defined in the security target [ST] when all measures required by the developer are applied.

EVALUATED CONFIGURATION

The evaluated platforms of the Huawei Eudemon8000E-X/USG9500 Series Firewall have been

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

Series	Model	ESN
8000E	Eudemon8000E-X3	210235G6QB10E5000001
	Eudemon8000E-X8	210235G6QD10E5000009
	USG9520	210235G7F6
	Eudemon8000E-X8	210235G6QDZ0C5000008
	Eudemon8000E-X16	2102351931P0B5000301

running the SW version: V300R001C01SPC300B113.

There have been two different binaries allocated to the platforms as follows:

Binary identifier
File names (for X3 and UGS 9520 platforms): - Eudemon_8000E_V300R001C01SPC200_X3.cc - Secospace_USG9520_V300R001C01SPC200_X3.cc HASH: 3d0c2d7d45db97113289a96175af4a66.
File names (for X8, X16, UGS 9560 and UGS 9580 platforms): - Eudemon_8000E_V300R001C01SPC200_X8X16.cc - Secospace_USG9580&9560_V300R001C01SPC200_X8X16.cc HASH: d26263bba05b0c35567421932ebc0aeb.

To set up the TOE in a way consistent to the evaluated configuration and the operational environment defined in the security target [ST], users must follow the steps included in the installation and operation manuals (see section DOCUMENTS).

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

EVALUATION RESULTS

The product "Huawei Eudemon8000E-X/USG9500 Series Firewall" has been evaluated against the "Huawei Eudemon8000E-X/USG9500 Series Firewall Security Target, Version 1.20, December 2015".

All the assurance components required by the evaluation level EAL3+ALC_CMC.4+ALC_CMS.4 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 EAL3+ALC_CMC.4+ALC_CMS.4, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

The TOE usage is recommended given that there are not exploitable vulnerabilities in the operational environment. Nonetheless, the following usage recommendations are given:

- The fulfilment of the assumptions within indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.
- It is very important the adequate fulfilling of the installation procedures; the installation procedure may be vulnerable if those procedures are not followed.

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

SFR Security Functional Requirement

ENAC CERTIFICACIÓN Nº 45/C-PR110

C/ Argentona nº 20
Email: organismo.certificacion@cni.es

TOE Target Of Evaluation

TSF TOE Security Functionality

TSFI TSF Interface

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, Sept. 2012.

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

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

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

[ST] Huawei Eudemon8000E-X/USG9500 Series Firewall Security Target, Version 1.20, December 2015

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body:

- Huawei Eudemon8000E-X/USG9500 Series Firewall Security Target, Version 1.20, December 2015

C/ Argentona nº 20
Email: organismo.certificacion@cni.es