MINISTERIO DE DEFENSA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF:	2010-16-INF-682 v2	Creado:	CERT2
Difusión:	Expediente	Revisado:	TECNICO
Fecha:	13.07.2011	Aprobado:	JEFEAREA

CERTIFICATION REPORT

Expediente:	2010-16
Datos del solicitante:	440301192W HUAWEI

References:

EXT-1099 Certification Request of Huawei NetEngine40E/CX600 Universal Service Router V600R001 21/10/2010. Huawei Technologies Co., Ltd.

EXT-1284 Evaluation Report for Huawei NetEngine40E/CX600 Universal Service Router V600R001 ETRHUAW002 M0 28/04/11. LGAI-APPLUS.

CCRA Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

SOGIS European Mutual Recognition Agreement of IT Security Evaluation Certificates v3.0, January 2010.

Certification report of Huawei NetEngine40E/CX600 Universal Service Router V600R001, as requested by Huawei Technologies in [EXT-1099] dated 21-10-2010, and evaluated by the laboratory LGAI-APPLUS, as detailed in the Evaluation Technical Report [EXT-1284] received on April 28th 2011, and in compliance with [CCRA] and for components up to EAL3. This CR also is covered by the [SOGIS] agreement but only for components until EAL2.

Table Of Contents

Executive Summary

This document constitutes the Certification Report for the product Huawei NetEngine40E/CX600 Universal Service Router V600R001 developed by Huawei Technologies Co., Ltd.

Developer/manufacturer: Huawei Technologies Co., Ltd.

Sponsor: Huawei Technologies Co., Ltd.

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

ITSEF: LGAI Technological Center. APPLUS.

Protection Profile: No conformance to a Protection Profile is claimed.

Evaluation Level: EAL3.

Evaluation end date: 28/04/2011.

All the assurance components required by the level EAL3 have been assigned a "PASS" verdict. Consequently, the laboratory (LGAI-APPLUS) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Considering the obtained evidences during the instruction of the certification request of the Huawei NetEngine40E/CX600 Universal Service Router V600R001 product, a positive resolution is proposed.

TOE Summary

Huawei NetEngine40E/CX600 Universal Service Router V600R001 provides high-end networking capacities for telecom and enterprise core networks. It consists of both hardware and software.

At the core of each router is the Versatile Routing Platform (VRP) deployed on board Main Processing Unit (MPU) or Switch Routing Unit (SRU), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include different interfaces with according access levels for administrators; 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 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.

Security Assurance Requirements

The product was evaluated with all the evidence required to fulfil EAL3, according to CC Part 3 [CC-P3].

Assurance Class	**Assurance Components**
Security Target	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1
Development	ADV_ARC.1, ADV_FSP.3, ADV_TDS.2
Guidance	AGD_OPE.1, AGD_PRE.1
Life Cycle	ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1
Tests	ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2
Vulnerability Analysis	AVA_VAN.2

Security Functional Requirements

The product security functionality satisfies several requirements as stated by its Security Target, and according to CC Part 2 [CC-P2]. They are requirements for security functions such as information flow control, identification and authentication.

These functional requirements satisfied by the product are:

Security Audit (FAU)	FAU_GEN.1 Audit data generation	FAU_GEN.1
	FAU_GEN.2 User identity association	FAU_GEN.2
	FAU_SAR.1 Audit Review	FAU_SAR.1
	FAU_SAR.3 Selectable audit review	FAU_SAR.3
	FAU_SGT.1 Protected trail storage	FAU_SGT.1
	FAU_SGT.3 Action in case of possible audit data loss	FAU_SGT.3
	FPT_STM.1 Reliable time stamps	FPT_STM.1
Cryptographic Support (FCS)	FCS_COP.1/AES Cryptographic operation	FCS_COP.1/AES
	FCS_COP.1/3DES Cryptographic operation	FCS_COP.1/3DES
	FCS_COP.1/RSA Cryptographic operation	FCS_COP.1/RSA
	FCS_COP.1/MD5 Cryptographic operation	FCS_COP.1/MD5
	FCS_COP.1/HMAC-MD5 Cryptographic operation	FCS_COP.1/HMAC-MD5
	FCS_CKM.1/AES Cryptographic key generation	FCS_CKM.1/AES
	FCS_CKM.1/3DES Cryptographic key generation	FCS_ CKM.1/3DES
	FCS_CKM.1/RSA Cryptographic key generation	FCS_ CKM.1/RSA
	FCS_CKM.1/RSA Cryptographic key destruction	FCS_ CKM.1/RSA
User Data Protection (FDP)	FDP_ACC.1 Subset access control	FDP_CKM.1
	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
Identification and Authentication (FIA)	FIA_AFL.1 Authentication failure handling	FIA_AFL.1

	FIA_ATD.1 User attribute definition	FIA_ATD.1
	FIA_SOS.1 Verification of secrets	FIA_SOS.1
	FIA_SOS.2 TSF Generation of secrets	FIA_SOS.2
	FIA_UAU.2 User authentication before any action	FIA_UAU.2
	FIA_UID.2 User identification before any action	FIA_UID.2
Security Management (FMT)	FMT_MOF.1 Management of security functions behaviour	FMT.MOF.1
	FMT_MSA.1 Management of security attributes	FMT_MSA.1
	FMT_MSA.3 Static attribute initialization	FMT_MSA.3
	FMT_SMF.1 Specification of Management Functions	FMT_SMF.1
	FMT_SMR.1 Security roles	FMT_SMR.1
Protection of the TSF (FTP)	FPT_ITT.1 Basic internal TSF data transfer protection	FPT_ITT.1
Resource utilization (FRU)	FRU_PRS.1 Limited priority of service	FRU_PRS.1
	FRU_RSA.1 Maximum quotas	FRU_RSA.1
TOE Access (FTA)	FTA_SSL.3 TSF-initiated termination	FTA_SSL.3
	FTA_TAB.1 Default TOE access banners	FTA_TAB.1
	FTA_TSE.1 TOE session establishment	FTA_TSE.1
Trusted Path/Channels (FTP)	FTP_TRP.1 Trusted path	FTP_TRP.1

Identification

Product: Huawei NetEngine40E/CX600 Universal Service Router V600R001.

Security Target: Huawei NetEngine40E/CX600 Universal Service Router V600R001 Security Target**.** V0.68, 2011/02/24.

Protection Profile: No conformance to a Protection Profile is claimed.

Evaluation Level: CC v3.1 r3 EAL3.

Security Policies

There are no security policies declared in the ST.

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, and briefly described below. These same 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.

In this ST there are only these assumptions to be considered:

- **A.PhysicalProtection** It is assumed that the TOE (including any console attached, access of CF card) is protected against unauthorized 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;
  - A remote entities (PCs) used for administration of the TOE.

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

Threats

This section describes the security threats to the TOE:

- **T.UnwantedNetworkTraffic** Unwanted network traffic sent to the TOE will not only cause the TOE's processing capacity for incoming network traffic is consumed thus fails to process traffic expected to be processed, but an internal traffic jam might happen when those traffics are sent to MPU from LPU within the 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 the traffic overload.

- **T.UnauthenticatedAccess** 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.

- **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.

Any other threats not included in this list are not necessarily resisted by the TOE.

Operational environment objectives

The product requires the cooperation from its operational environment to fulfil the requirements listed in its Security Target. This section identifies the IT security objectives that are to be satisfied by the imposing of technical or procedural requirements on the TOE operational environment. These security objectives are assumed by the Security Target to be permanently in place in the TOE environment.

With this purpose, the security objectives declared for the TOE operational environment are the following:

- **OE.NetworkElements** The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. 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 CF card 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/SRU in TOE into a local sub-network, compared to

TOE Architecture

Physical Architecture

The physical architecture includes the following systems:

- Power distribution system
- Functional host system
- Heat dissipation system
- Network management system

The functional host system is the target of this evaluation and following introductions will focus on the functional host system only. The Network management system, power distribution system and heat dissipation system are not within the scope of this evaluation.

The functional host system processes data. In addition, it monitors and manages the entire system, including the power distribution system, heat dissipation system, and NMS through NMS interfaces which are not within the scope of this evaluation.

The physical boundary of the TOE is the actual router system itself – in particular, the functional host system. The Network management system is not within the scope of this evaluation. The power distribution system and heat dissipation system are part of the TOE but not to be evaluated because they are security irrelevant.

The TOE provides several models. These models differ in their modularity and throughput by supplying more slots in hosting chassis, but they offer exchangeable forwarding unit modules, switch fabrics, and use the same version of software.

The following models will be covered during this evaluation:

- NE40E-X16 CX600-X16
- NE40E-X8 CX600-X8
- NE40E-X3 CX600-X3
- NE40E-8 CX600-8
- NE40E-4 CX600-4

Software Architecture

In terms of the software, the TOE's software architecture consists of three logical planes to support centralized routing and control and distributed forwarding mechanism.

- Data plane - is responsible for high speed processing and non-blocking switching of data packets.
- Control and management plane - is the core of the entire system. It controls and manages the system.

- Monitoring plane - is to monitor the system environment by detecting the voltage, controlling power-on and power-off of the system. The monitoring plane is not considered security-related thus will not be further covered.

The VRP is the control and management platform that runs on the SRU / MPU. The VRP supports IPv4 / IPv6, and routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), calculates routes, generates forwarding tables, and delivers routing information to the LPU(s). The VRP includes Service Control Plane (SCP), System Manage Plane (SMP), General Control Plane (GCP) and other TSF, non-TSF subsystems.

The LPU implements the functions of the link layer and IP protocol stacks on interfaces and performs hardware-based IPv4 / IPv6 forwarding, multicast forwarding and statistics.

The logical boundary of the TOE, namely the Versatile Routing Platform (VRP), is a software platform from view of software architecture, and the forwarding engine that processes the incoming and outgoing network traffic.

The TOE controls the flow of IP traffic (datagrams) between network interfaces by matching information contained in the headers of connection-oriented or connectionless IP packets against routing table in forwarding engine.

The routing table in forwarding engine is delivered from VRP's routing unit whereas the routing table in VRP's routing module can be statically configured or imported through dynamic routing protocol such as BGP, Open Shortest Path Find (OSPF). Note that BGP/OSPF functionality configuration must be performed via s secure channel enforcing SSH prior to routing table importing.

System control and security managements are performed either through interfaces on MPU/SRU or interfaces on LPU via a secure channel enforcing SSH.

Documents

The basic documentation distributed with the TOE to be used with the security assurance provided by the certificate issued is:

- Huawei NetEngine40E/CX600 Universal Service Router V600R001 Security Target, v0.68.

- Huawei NetEngine40E/CX600 Service Router Version 6 Release 1 Operational User Guidance , v0.5.

- Huawei NetEngine80E/40E Router V600R001C01_Configuration Guide - Routine Maintenance, v01.

- Huawei NetEngine80E and 40E Universal Service Router Command Reference V600R001C01_05, v0.5.

- Huawei NetEngine80E/40E Router V600R001C00_Configuration Guide - IP Routing, v04.

- Huawei NetEngine40E/CX600 Service Router Version 6 Release 1 Preparative Procedure , v0.51.

TOE Testing

The process has 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.

The TOE configuration is described in each test. Evaluator devised test results are consistent with the expected results.

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.

The evaluator examined the design specification and test documentation, concluding that all the modules functionality are tested. Therefore, all TSFIs are fully tested. The evaluator verified that TSFI were tested in test plan. The test procedures mapped all TSFI to SFR-enforcing modules.

The evaluator has repeated all the tests defined in the TOE test specification according to the different configurations defined by the developer. All tests have been successfully performed.

The evaluator executed the tests and updated the test documentation with new devised tests. The evaluator verified that the obtained results were consistent to the expected results.

The result of independent tests was successfully performed and there were neither inconsistencies nor deviations between the actual and the expected results.

Penetration Testing

The approach of the penetration testing focused on testing the weakest points of the TOE by design or by technologies that are commonly known to be easy to exploit.

The independent penetration testing devised attack vector and performed test cases covering the main types of attacks for this TOE including command retrieval, packet reinjection, MAC supplantation, denial of service, signature forgery, or seed discovery attacks.

The evaluator did not find either exploitable vulnerabilities or residual vulnerabilities in the operational environment as a result of independent penetration testing.

Evaluated Configuration

The TOE is defined by its name and version number:

- **Huawei NetEngine40E/CX600 Universal Service Router V600R001**

Evaluation Results

The product Huawei NetEngine40E/CX600 Universal Service Router V600R001 has been evaluated in front of the "Huawei NetEngine40E/CX600 Universal Service Router V600R001 Security Target**.** V0.68", 2011/02/24.

All the assurance components required by the level EAL3 have been assigned a "PASS" verdict. Consequently, the laboratory (LGAI-APPLUS) assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL3 methodology, as define by of the Common Criteria [CC-P3] and the Common Methodology [CEM].

Comments & Recommendations from the Evaluation Team

There are no recommendations.

Certifier Recommendations

Considering the obtained evidences during the instruction of the certification request of the product Huawei NetEngine40E/CX600 Universal Service Router V600R001, a positive resolution is proposed.

This certification is recognised under the terms of the Recognition Agreement [CCRA] for components up to EAL3 according to the mutual recognition levels of it and the accreditation status of the Spanish Scheme.

The assurance derived from this CR also is covered by the [SOGIS] agreement but only for components until EAL2.

Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Acronyms

CC	Common Criteria
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functionalities Interface
PP	Protection Profile
SFR	Security Functional Requirement
LMT	Local Maintenance Terminal
RMT	Remote Maintenance Terminal
NE	NetEngine
CLI	Command Line Interface
GUI	Graphical User Interface
SRU	Switch Router Unit
MPU	Main Process Unit
LPU	Line Process Unit
SFU	Switching Fabric Unit
SPU	Service Process Unit

Bibliography

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

Common Criteria

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r3, July 2009.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r3, July 2009.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r3, July 2009.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r3, July 2009.

Security Target

It is published jointly with this certification report the security target,

"Huawei NetEngine40E/CX600 Universal Service Router V600R001 Security Target v0.68", 2011/02/24.