Reference: 2017-10-INF-2789-v1
Target: Interno OC
Date: 23.05.2019

Created by: CERT9
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2017-10**
TOE	**openNAC Enterprise v1.2**
Applicant	**B86566189 - Opencloud Factory S.L.**
References	

[EXT-3314] Solicitud Certificaci—n OPENNAC Enterprise

Certification report of the product openNAC Enterprise v1.2, as requested in [EXT-3314] dated 09/03/2017, and evaluated by Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-4598] received on 20/05/2019.

CONTENTS

EXECUTIVE SUMMARY 3
TOE SUMMARY 3
SECURITY ASSURANCE REQUIREMENTS 4
SECURITY FUNCTIONAL REQUIREMENTS 5
IDENTIFICATION 6
SECURITY POLICIES 6
ASSUMPTIONS AND OPERATIONAL ENVIRONMENT 6
CLARIFICATIONS ON NON-COVERED THREATS 6
OPERATIONAL ENVIRONMENT FUNCTIONALITY 6
ARCHITECTURE 7
LOGICAL ARCHITECTURE 7
PHYSICAL ARCHITECTURE 7
DOCUMENTS 7
PRODUCT TESTING 7
EVALUATED CONFIGURATION 8
EVALUATION RESULTS 9
COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM 9
CERTIFIER RECOMMENDATIONS 9
GLOSSARY 9
BIBLIOGRAPHY 10
SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE) 10
RECOGNITION AGREEMENTS 11
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA) 11
International Recognition of CC – Certificates (CCRA) 11

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product openNAC Enterprise v1.2.

OpenNAC Enterprise is a solution that provides Network Access Control for corporate networks (LAN/WAN) by authenticating, authorizing and auditing accesses to the network. It is a software solution and its components execute on general purpose computing hardware, always in a virtualized environment, which is provided by the Operational Environment.

Developer/manufacturer: Opencloud Factory S.L.

Sponsor: Opencloud Factory S.L..

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 R5 EAL2.

Evaluation end date: 20/05/2019.

All the assurance components required by the evaluation level EAL2 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 EAL2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

Considering the obtained evidences during the instruction of the certification request of the product openNAC Enterprise v1.2, a positive resolution is proposed.

TOE SUMMARY

As opposed to specific network equipment, openNAC is a software product, so it does not have the capability to perform the control of network accesses itself. Instead, it relies on an environment configuration where the network devices such as switches are configured to "talk" to the TOE by sending RADIUS requests. When a client (i.e. user computer) requests access to the network, the network device in the environment send RADIUS requests to the TOE. Upon receiving these requests, the TOE performs access control policy evaluation tasks and determines if it grants or denies access to the network for the client, providing such information in the RADIUS response. Then, the network device enforces the access control on the network, by granting or denying access to the client based on the RADIUS response returned by the TOE.

The access control of user and devices to the network resources TOE is based on policies, these policies indicate the rules for granting or denying access of users to the network. To establish and

configure the access control policies, the TOE provides an interface in the form of a REST API, that can be used directly or through a web portal, which is included in the set of services contained in the TOE virtual machine. Through this interface, an administrator can authenticate in order to establish policies, register or edit user or devices, among other administrative tasks. This interface also allows to view the audit data generated by the TOE in response to management or security events.

For regular users, those that try to access to resources in the local area network without being involved in management functions, the use of the TOE is transparent. They operate normally without any direct interaction with the TOE, and the configured network devices enforce the access control for them, in collaboration with the TOE, in charge of policy evaluation.

The TOE is deployed as a virtual machine running on a general purpose computer connected to the local area network. Once the operating environment is properly prepared, including the configuration of the network devices in a way that all authentication and authorization requests are set to the TOE, the TSF can be deployed. The TOE major security features are the following:

- Audit generation. The TOE generates audit data related to management events (administrative actions), and events related to network access, where access control policy to the network is enforced.
- Management functions: via the web interface, it is possible for administrators to manage of user, devices, policies, etc. Audit data can be consulted through this interface as well.
- Network Access Control for users and devices to networks. The TOE attends authorization and authentication requests from the configured network devices in the operational environment that result in the evaluation of the access control policies and it providing responses to the devices that they will use to grant or deny access.
- Role-based access control to management functions. The different management functions, provided via web interface, are available with a different level of permissions depending on the user roles. Different roles are defined in the TOE and they have different sets of permissions for performing management actions. Assignment of roles to users is possible via the web interface.
- Protection of communications. The web interface (REST API) communications, used for TOE management, are protected since HTTPS is used in the TOE evaluated configuration.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL2, according to Common Criteria v3.1 R5.

Assurance class	Assurance components
ASE	ASE_INT.1 ASE_CCL.1 ASE_SPD.1 ASE_OBJ.2 ASE_ECD.1 ASE_REQ.2 ASE_TSS.1
ADV	ADV_ARC.1 ADV_FSP.2 ADV_TDS.1
AGD	AGD_OPE.1 AGD_PRE.1
ALC	ALC_CMC.2 ALC_CMS.2 ALC_DEL.1
ATE	ATE_COV.1 ATE_FUN.1 ATE_IND.2
AVA	AVA_VAN.2

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R5:

Security functional requirements
FAU_GEN.1
FAU_GEN.2
FCP_ACC.1
FDP_ACC.3
FDP_ACF.1
FDP_ACF.2
FIA_ATD.1
FIA_UAU.1
FIA_UID.1
FMT_MSA.1
FMT_MSA.3
FMT_SMF.1
FMT_SMR.1
FPT_STM.1
FTP_ITC.1

IDENTIFICATION

Product: openNAC Enterprise v1.2

Security Target: openNAC Enterprise Security Target, v1.7 (06 May 2019).

Protection Profile: None.

Evaluation Level: Common Criteria v3.1 R5 EAL2.

SECURITY POLICIES

The use of the product openNAC Enterprise v1.2 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in [ST], chapter 3.4 (Organizational security policies).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The assumptions detailed in [ST], chapter 3.5 (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.

CLARIFICATIONS ON NON-COVERED THREATS

The threats detailed in [ST], chapter 3.3 (Threats to security) do not suppose a risk for the product openNAC Enterprise v1.2, although the agents implementing attacks have the attack potential according to the Basic of EAL2 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.

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 detailed in [ST], chapter 4.2 (Security objectives for the operational environment).

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

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE consists of a virtual machine, which contains a series of logical components that provide the security functionality described in the Security Target. The logical scope of the TOE is the whole virtual machine, which consists of a CentOS operating system with a set of services, libraries and configuration required by the TOE core components. The TOE is subdivided in three main subsystems:

- Web
- RADIUS-NAC
- Database

PHYSICAL ARCHITECTURE

The TOE is a virtual machine file compatible with VirtualBox distributed as an OVA file.

DOCUMENTS

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

Document title	Version
openNAC Enterprise - AGD_OPE (openNAC Enterprise Operational User Guidance)	1.6
openNAC Enterprise - AGD_PRE (openNAC Enterprise Preparative Procedures)	1.7
openNAC Enterprise - REST API Specification	1.2

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 openNAC Enterprise v1.2 it is necessary the disposition of the following software components:

- A single instance of openNAC Enterprise 1.2 configured in the local network. There are cluster configurations, but they don't belong to the evaluated TOE configuration.

The TOE is delivered as a virtual machine image, which must be run by a Virtual Machine Hypervisor running on a general purpose computer. To run the virtual machine image containing the TOE, Oracle VirtualBox software is required. Below is the list of compatible versions of Oracle VirtualBox that can run the TOE:

- VirtualBox 5.2.8
- VirtualBox 5.2.6
- VirtualBox 5.2.4
- VirtualBox 5.2.2
- VirtualBox 5.2.0

An operating system compatible with the above versions of VirtualBox is required in order to run the software. The list of compatible operating systems is the following:

- Windows 10
- Linux:
  - Ubuntu 14.04 LTS, 16.04 LTS, and 17.04
  - Debian GNU/Linux 7 ("Wheezy"), 8 ("Jessie") and 9 ("Stretch")
  - Oracle Enterprise Linux 5, Oracle Linux 6 and 7
  - Redhat Enterprise Linux 5, 6 and 7 or CentOS
  - Fedora 25 and 26
  - Gentoo Linux: Gentoo Profile 13.0 or higher
  - openSUSE 13.2
- MacOS X 10.10 (Yosemite) or higher.

One of the above operating systems is required to be installed in the computer running the TOE. As for the hardware required to run the TOE, it is required a general purpose computer with one of the listed operating system installed. The hardware requirements for the computer are the following:

- Reasonably powerful x86 hardware. Any recent Intel or AMD processor should do.
- Memory. At least 4 GB of RAM, but recommended 8 GB of RAM.
- Hard disk space. The virtual machine files could grow up to 40 GB.
- A network interface card to be connected to the corporate network.

In order to achieve the above-described configuration, the TOE preparative guide must be thoroughly followed for the TOE installation and configuration.

EVALUATION RESULTS

The product openNAC Enterprise v1.2 has been evaluated against the Security Target openNAC Enterprise Security Target, v1.7 (06 May 2019).

All the assurance components required by the evaluation level EAL2 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 EAL2, as defined by the Common Criteria v3.1 R5 and the CEM v3.1 R5.

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 Epoche & Espri S.L.U., 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, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[ST] openNAC Enterprise Security Target, v1.7 (06 May 2019).

SECURITY TARGET / SECURITY TARGET LITE (IF APPLICABLE)

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: openNAC Enterprise Security Target, v1.7 (06 May 2019).

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.org.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification)of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognized under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.