openNAC Enterprise Security Target v1.7

Opencloud Factory

2019-05-06

Created by

Table of contents

1 ST Introduction

1.1 ST Reference

Title: openNAC Enterprise Security Target

Version: v1.7

Author: Opencloud Factory

Evaluation Lab: Epoche & Espri

Date of publication: 2019-05-06

1.2 TOE Reference

TOE Name: openNAC Enterprise

TOE Developer: Opencloud Factory

TOE Version: v1.2

1.3 TOE Overview

1.3.1 Introduction

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 developed by opencloud Factory S.L. 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.

openNAC Enterprise solution is the next step in the evolution of data Network Access Control Solutions. openNAC is a simple but feature-rich and flexible solution to build and control enterprise Network Access, which combines existing OpenSource technologies with advanced features for multi-tenancy, automatic provision and elasticity. openNAC follows a bottom-up approach driven by sysadmins, developers and user's real needs.

1.3.2 TOE Type

openNAC Enteprise is a Network Access Control product.

1.3.3 TOE Usage & Major Security Features

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, that 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:

- Generation of auditory. The TOE generates auditory 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.

1.3.4 Non-TOE Security Features

The TOE provides some security features that are not in the scope of the evaluation and, therefore, they are not part of the TSF. Such functionality is related to other entities in the local area network that can indirectly interact with the TOE. The following non-TOE security functionality is considered:

- **Interoperability with Active Directory/LDAP**. In order to avoid manual registration of the users or devices in a corporate network, the TOE can send LDAP queries to an Active Directory Server in order to get the list of user or devices of the organization. This way, automatic registration of users and devices is possible.
- **Active configuration of network devices.** The TOE is capable of establishing configuration of the compatible network devices (see Appendix A of this ST) in order to allow them to communicate with the TOE.

1.3.5 Non-TOE Hardware/Software/Firmware

1.3.5.1 TOE required hardware and software

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.

1.3.5.2 Network environment

Interaction of external entities with the TOE is carried out by communications through a local network, to which the TOE must be connected. For this purpose, the TOE has a network interface controller, connected to the local network, and it is used to communicate with other entities in the network.

The following non-TOE elements exist in the TOE environment and interact with communications through the local network**:**

- **Management clients.** Web browsers or REST clients that establish a connection through HTTPS in order to access or modify the TOE configuration elements, such as policies, CMDB, etc.
- **Network devices**. Network equipment devices connected to the same local network as the TOE. Some of them are in charge of enforcing access control on network resources and for such purpose, they communicate to the TOE to request authentication or authorization of clients. Depending on the TOE response, whose calculation is part of the TSF, these devices will allow or deny access to the requested resources. Other devices are part of the network but do not participate in access control tasks. Some of the of possible network devices that exist in the TOE environment are:
  - Switches
  - Network Access Points
  - Firewalls
  - Other network elements 802.1x capable
  - IDS/IPS sensors
  - DNS servers

- DHCP servers

- **Client computers**. These are the devices that request access to network resources. Access is denied or granted according to the above-explained mechanism.

- **User Data Sources.** Elements involved in the access control policies used to determine if network access is granted or denied to a resource can be retrieved by the TOE from external sources. For instance, if an Active Directory is in place, the TOE may send LDAP queries to the Domain Controller in order to retrieve the list of users of the domain. Then, these users can be assigned to policies that will grant or deny access to network resources.

- **Products complementary to openNAC**. These products are part of a product suite where the TOE is included, and they provide additional funcionality, for utility or convenience. This additional functionality of not part of the TOE and therefore is not included in the evaluated TSF. These non- TOE components are:

  - **openNAC Agent**. A software that is installed in client devices and communicates to the TOE via REST API, in order to register users and end-user devices.

  - **openNAC Analytics**. A product distributed as virtual machine that communicates to the TOE via REST API, in order to obtain data and generate analytics information.

  - **openNAC Sensor**. A product distributed as virtual machine that collects and decoding network protocols and sends it to OpenNAC Analytics. It allows to complement the vision of the behaviour of the entities through the inspection and classification of the network traffic arriving at the application level (layer 7). It also allows visibility over network segments that are not managed by the NAC

1.4 TOE Description

1.4.1 Introduction

1.4.1.1 TOE Evaluated Configuration

openNAC Enterprise supports multiple configurations in different scenarios, some of them relying on external environment elements described in section 1.3.4.2 of this ST. For instance, openNAC Enterprise can be configured to retrieve users from a LDAP server and register them, or a client program (openNAC Agent) can be installed in client computers to automatically register users and end-user devices in openNAC.

Although features as the above-mentioned ones are technically available in openNAC Enterprise, they are not included in the evaluated configuration of the TOE. Such TOE evaluated configuration is intended to provide a scenario with an essential setup with the indispensable settings that are required for the TOE to deploy the security functionality described in this Security Target.

The TOE evaluated configuration can be described as follows:

- A single instance of openNAC Enterprise is configured in the local network. There are cluster configurations, but they don't belong to the evaluated TOE configuration.
- Registration of users in the TOE is carried out using the web interface, introducing their data in the interface available in the Web Administration Portal or using the REST API. The TOE is not configured to retrieve users from external data sources, such as an Active Directory.
- Authentication of users as consequence of incoming RADIUS requests to the TOE is carried out against the internal list of users that the TOE maintains. No authentication is performed as external user sources, such as Active Directory, or any other method different that the previously described.
- Network devices that send authentication / authorization petitions via RADIUS requests are configured manually to interact with the TOE. In the evaluated configuration, the TOE does not actively configure them by any possible interface available.
- Network devices that send authentication / authorization petitions via RADIUS requests are introduced in the TOE using the web interface (Web Administration Portal or REST API). The TOE does not rely on any external source for importing them and it does not automatic discovery of such devices in the network.
- No external plugins that OpenNAC Enterprise may support are installed.
- TOE configuration is performed in a way that only those TOE interfaces required for deploying the TSF are configured. These are the web interface and the RADIUS interface. This includes the following features available in openNAC Enterprise product are **disabled or not configured** (default configuration is kept):
    - Notification checks.
    - SNMP trap monitoring.
    - DHCP Server.
    - DNS Server.
    - Network configuration backups.
    - Statistics or analytics generation for an external data-collection server.
- The described scenario has been tested using a free software implementation of a RADIUS client (NTRadPing Test Utility), although any supported device of those listed in Appendix A of this ST can be configured to send RADIUS requests to the TOE.
- In the TOE evaluated configuration, for obtaining reliable time sources, the TOE Virtual Machine is configured so that it synchronizes its system clock with the clock of the host machine, instead of using an external secure NTP server.

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

1.4.2 TOE Logical Scope

The following diagram depicts a typical scenario where the TOE is deployed in a local area network. The TOE runs on a virtual machine, which contains part of the required operating environment in the form of operating system, services, libraries and configuration.

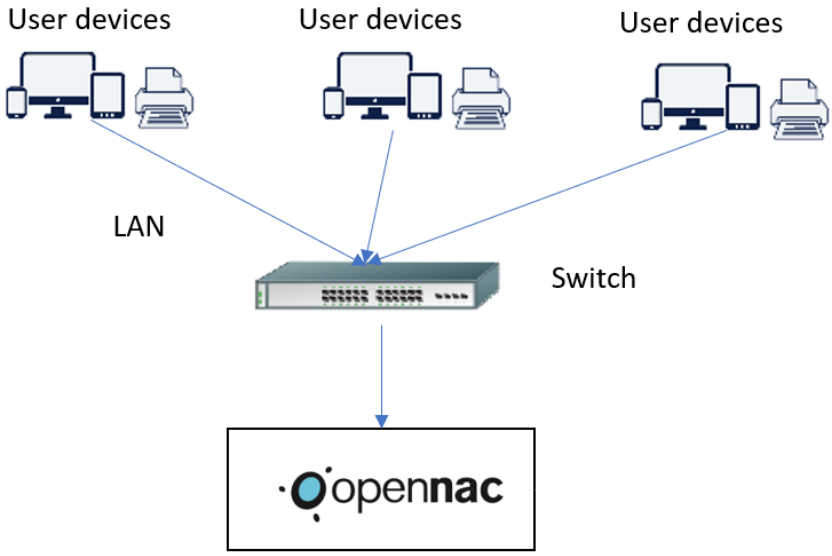


Figure 1 *Typical deployment diagram of openNAC in a Local Area Network*

While it is possible to have different setups and more complex scenarios, the above one summarizes the basic deployment case that illustrates how the TOE functions in relation with its environment.

The TOE consists of a virtual machine which contains a series of logical components that provide the security functionality described in this Security Target. The logical scope of the TOE is the whole virtual machine.

The TOE virtual machine consists of a CentOS operating system with a set of services, libraries and configuration required by the TOE core components.

1.4.2.1 Network Access Control details

The main security functionality of the TOE consists on to perform access control to a network for users and devices. As mentioned in previous sections, the TOE as a software product cannot fully enforce access control itself. The actual enforcement of access control is performed by the network devices in the local area network, e.g. managed switches. It is the TOE who, by evaluating access control policies, determines if the network device will allow or deny the access to the network resource for a given access attempt. Below is a detailed explanation of how this process occurs:

- The TOE includes a freeRADIUS server with an openNAC specific module. This server listens to RADIUS requests in ports 1812 UDP (authentication) and 1813 UDP (authorization).
- An administrator user, via the web management interface, configures the network access control policies of the TOE, defining rules for access in terms of users, devices, networks, etc. This information is stored in an internal database of the TOE.

- During the preparation of the operational environment, the network devices in the local area network (e.g. managed switches) are configured to use the TOE as RADIUS server. As part of their configuration, a pre-shared key is established for communication with the TOE freeRADIUS server. This way, when a user device (e.g. user computer) requests access to the network, the switches send authentication / authorization RADIUS requests to the TOE.
- As response to the incoming RADIUS requests, the TOE evaluates the policies established by the administrator, considering which user or device is trying to access which network resource. Depending on the result of the policy evaluation, the TOE returns different responses to the network device that sent the RADIUS request. These responses indicate if the access will be granted or denied.

The following figure depicts how the authorization process occurs:

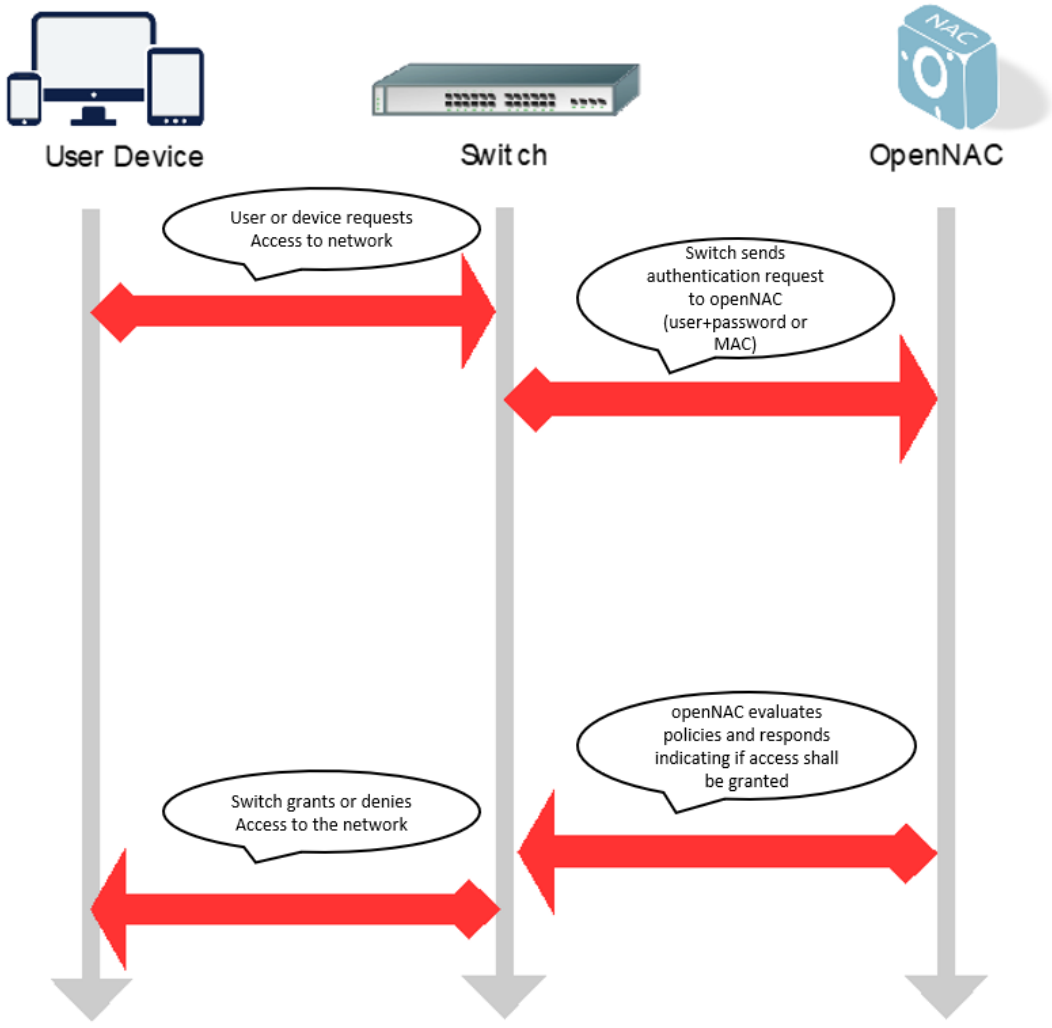


Figure 2 Network Access Control scheme

Authentications are carried out in two ways:

- 802.1x user auth request: user credentials are used for authentication.

- 802.1x MAB request: device MAC is used for authentication.

1.4.2.1.1 Access Control using Virtual Local Area Networks

In order to effectively enforce access control to the network, the network devices in the LAN do not simply "allow" or "deny" access to the network to a client device, but Virtual Local Area Networks (VLANs) are used to implement a more complex mechanism. During the preparation of the operational environment, the network devices are configured to support multiple VLAN networks. These networks are being used to segregate the devices requesting access to the network based on the access control policies. This way, when a switch sends an authorization RADIUS request to the TOE, depending on its answer, the switch will assign a different VLAN to the client based on the TOE response.

Once the switches assign clients to different VLAN networks, effective segregation of authenticated and authorized clients is achieved, since they are separated to those that are not correctly authenticated or authorized given that they are in different VLANs.

1.4.2.2 Management functions

In order to carry out management functions of the TOE, a REST API is provided which contains the required functions for the different tasks required for TOE administration. The TOE listens to HTTPS requests in port 443 TCP and it performs the management activities as response to petitions sent via this interface. Some of the TSF related activities related to this REST API are:

- Authentication of users
- Management of users
- Management of devices
- Management of policies
- Management of roles and permissions
- View audit data generated by the TOE

While any REST client can be used to use this API, the TOE also provides a Web Administration Portal that can be used with a web browser and whose purpose is to facilitate the use of the REST API. This portal user interfaces that, upon their usage, they internally invoke the REST API by means of HTTPS requests.

1.4.2.3 Role Based Access Control to Management Functions

Different roles with different privileges to exercise management functions exist in the TOE. The security functionalities related to management, detailed in previous section, are available in different level of permissions depending roles associated to the user performing them. Depending on the role of the user, for instance, management actions involving read operations may be allowed while those involving modification, creation or deletion operations may be forbidden. Different sets of permissions assigned to roles determine the management actions allowed for them.

These roles can be managed via the web interface, where they can be also assigned or unassigned to users of the TOE.

1.4.2.4 Protection of Communications

The TOE implements protection of communications through the web interface, that occurs using an HTTPS channel for encryption of the communications through this channel. TLS version used is v1.2.

1.4.2.5 Generation of Audit Data

The TOE generates audit data for two different kind of events:

- Events related to management actions that occur through the web interface.
- Events related to network accesses that take place through a RADIUS authentication / authorization request that triggers a policy evaluation. The result of the action (granted or blocked) is logged.

Audit data is available to be read through the web interface.

1.4.3 TOE Physical Scope

The Target of Evaluation (TOE) is purely a software TOE and includes the following components:

Name	Type	Version	Distribution format	Description
openNAC Enterprise	Software	1.2	OVA file	Virtual machine file compatible with VirtualBox
openNAC Enterprise - AGD_PRE v1.7.pdf	Guidance	1.7	PDF document	Guide for installation of the TOE and preparation of the operational environment
openNAC Enterprise - AGD_OPE v1.6.pdf	Guidance	1.6	PDF document	Guide for operational use of the TOE
openNAC Enterprise - REST	Guidance	1.2	PDF document	Specification and instruction usage

API specification v1.2.pdf				of the REST API functions

2 Conformance Claims

This Security Target and the TOE described are in accordance with the requirements of Common Criteria 3.1R5.

This Security Target claims conformance with the following parts of Common Criteria:

- Conformance with [CC31R5P2] extended.
- Conformance with [CC31R5P3].

The methodology to be used for the evaluation is described in the "Common Evaluation Methodology" of the Common Criteria standard of April 2017, version 3.1 revision 5 with an evaluation assurance level of EAL2.

This Security Target does not claim conformance with any protection profile.

3 Security Problem Definition

This section describes the security aspects of the operational environment and its expected use in said environment. It includes the declaration of the TOE operational environment that identifies and describes:

- The alleged known threats that will be countered by the TOE
- The organizational security policies that the TOE has to adhere to
- The TOE usage assumptions in the suggested operational environment.

We will begin defining Assets and Agents of threats.

3.1 Assets

NETWORK RESOURCE: A resource (e.g. network share) located in the network managed by the network devices configured by the TOE.

TOE MANAGEMENT CONFIGURATION: TOE stored configuration: users, devices configuration, etc, stored in the TOE database.

TOE INTERNAL CONFIGURATION: The configuration of the TOE environment that is stored internally, for instance, in system configuration files of the Virtual Machine. Examples are SSH configuration, web server configuration, internal database connection, etc.

AUTHENTICATION DATA: Authentication credentials to access the network, or to use the administration interfaces of the TOE.

3.2 Threat Agents

DEVICE: A device trying to access a resource in the network managed by network devices configured by the TOE.

USER: A user trying to access the TOE configuration data.

3.3 Threats to Security

This section identifies the threats to assets that require protection by the TOE. The threats are defined in terms of assets concerned, attackers and the adverse action that materializes the threat.

T.NETWORK_ACCESS: A **Device** tries to access a **Network resource** without authorization.

T.MANAGEMENT_ACCESS: A **User** tries to access or modify **TOE Management configuration** without authentication, or authenticated but without enough privileges.

T.INTERNAL_CONFIGURATION: A **User** tries to modify the **TOE Internal Configuration** so that part of the TSF can be bypassed, for instance, modifying configuration of services inside the Virtual Machine.

T.EAVESDROP: A **User** listens to the traffic in the local network to capture **Authentication data** through the communication interface of the TOE with the outside, used for TOE management.

3.4 Organizational Security Policies

The organizational Security policies are defined as follows.

P.AUDIT: Audit data will be available, so user activities in their interaction with the TOE can be monitored.

3.5 Assumptions

The assumptions when using the TOE are the following:

A.TRUSTED_ADMIN: Administrators of the TOE are appropriately trained to undertake the installation, configuration and management of the TOE in a secure trusted manner, and they are not careless, willfully negligent or hostile.

A.SECURE_LOCATION: The processing platforms on which the TOE resides are located within a facility that provides controlled access, ensuring that the organizational network infrastructure that interacts with the TOE is physically protected in a way that all communications with the TOE take place in a secure environment (this includes RADIUS messages).

A.CONFIG: The Operational Environment shall allow the TOE to receive all passwords and associated data from network-attached systems.

A.VLAN_SEGREGATION: The network equipment supports the creation of Virtual Local Area Networks (VLANs) in order to segregate the devices connected to the LAN. Bypassing the segregation established by setting different VLAN is not feasible.

A.TIMECONFIG: The hardware and the hosting OS where the TOE runs provide accurate time to the TOE.

4 Security Objectives

The security objectives are high level declarations, concise and abstract of the solution to the problem exposed in the former section, which counteracts the threats and fulfills the security policies and the assumptions. These consist of:

- the security objectives for the operational environment.
- the security objectives for the TOE

4.1 Security objectives for the TOE

The security objectives for the TOE must determine (to the desired extent) the responsibility of the TOE in countering the threats and in enforcing the OSPs. Each objective must be traced back to aspects of identified threats to be countered by the TOE and to aspects of OSPs to be met by the TOE.

O.MANAGEMENT: The TOE shall enforce authentication and authorization to users on the TOE management interfaces.

O.NAC: The TOE shall enforce authentication and access control policies to network access requests coming from network devices.

O.AUDIT: The TOE will generate audit data on management operations and network access requests.

O.COMM: The intercommunication channel between the TOE and external entities, used for TOE management shall be protected to avoid capturing sensitive data.

4.2 Security objectives for the operational environment

The security objectives for the Operational Environment determine the responsibility of the environment in countering the threats, enforcing the OSPs and upholding the assumptions. Each objective must be traced back to aspects of identified threats to be countered by the environment, to aspects of OSPs to be enforced by the environment and to assumptions to be uphold by the environment.

OE.PERSONNEL: Authorized administrators are non-hostile and follow all administrator guidance and must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains the TOE security objectives. Any operator of the TOE must be trusted not to disclose their authentication credentials to any individual not authorized for access to the TOE.

OE.PHYSEC: The facility surrounding the processing platform in which the TOE resides must provide a controlled means of access to the facility. This ensures that the organizational network infrastructure that interacts with the TOE is physically protected in a way that all communications with the TOE take place in a secure environment (this includes RADIUS messages).

OE.NETWORK_PROTECT: The network devices in the operational environment are configured in a way that network access is not granted to clients except through authorization carried out by the TOE.

OE.NETWORK_EQUIPMENT: Network devices in the operating environment that interact with the TOE for authentication and authorization requests belong to the list of supported devices specified in Appendix A of this Security Target.

Application Note

Network equipment meeting the operational and security requirements needed to interoperate with the TOE are those devices listed in Annex A of this ST.

OE.TIME: The TOE environment must ensure that the IT environment will provide a reliable time source to the TOE

4.3 Security Objectives Rationale

The following table provides a mapping of security objectives tracing each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective, and each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective. This illustrates that the security objectives counter all threats, the security objectives enforce all OSPs and the security objectives for the operational environment uphold all assumptions.

	O.MANAGEMENT	O.NAC	O.AUDIT	O.COMM	OE.PERSONNEL	OE.PHYSEC	OE.NETWORK_PROTECT	OE.NETWORK_EQUIPMENT	OE.TIME
T.NETWORK_ACCESS		X					X		
T.MANAGEMENT_ACCESS	X				X				
T.INTERNAL_CONFIGURATION					X	X			
T.EAVESDROP				X					
P.AUDIT			X						
A.TRUSTED_ADMIN					X				
A.SECURE_LOCATION						X			
A.CONFIG							X		
A.VLAN_SEGREGATION								X	
A.TIMECONFIG									X

Table 1 *Security Objectives vs Security Problem Definition*

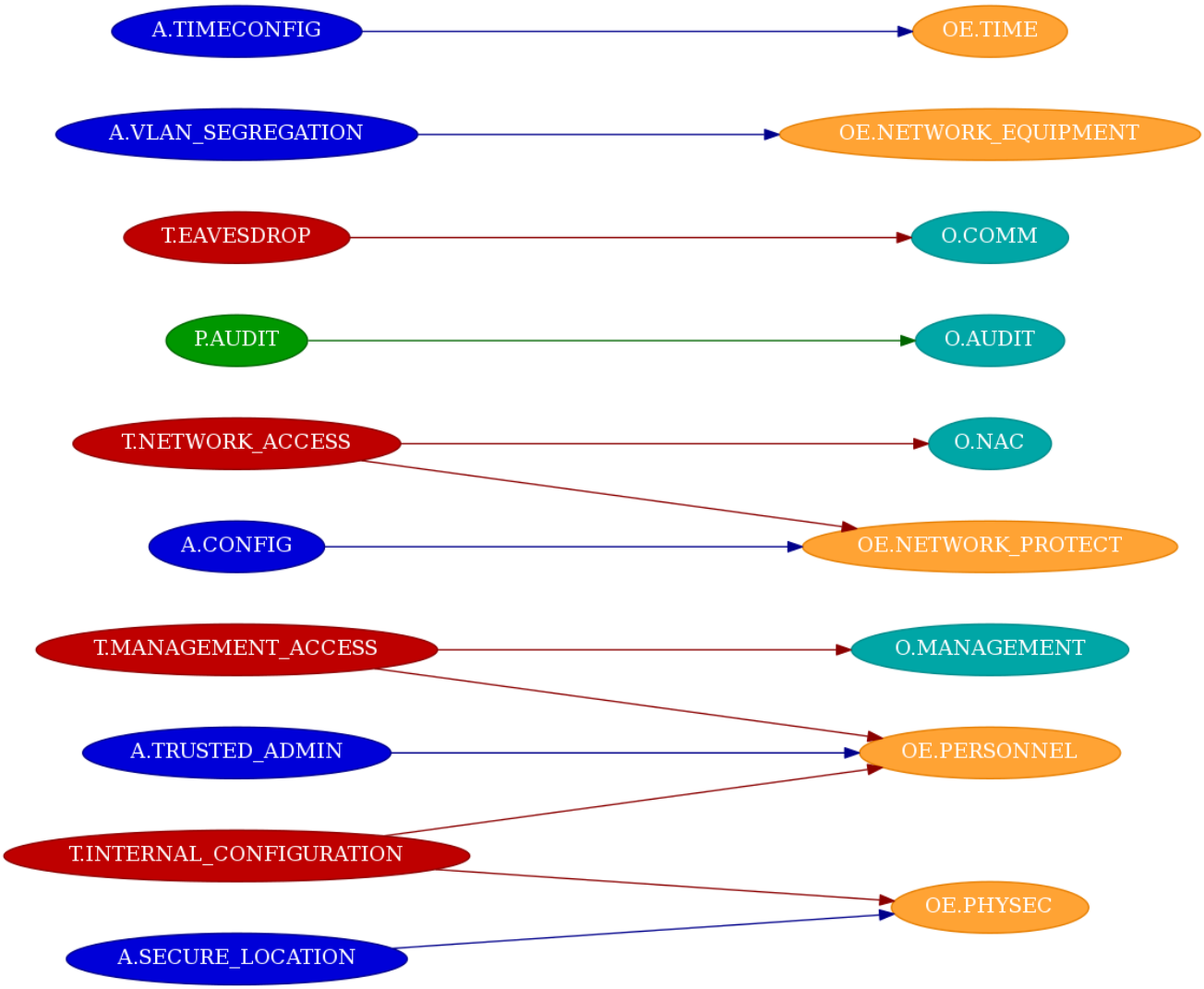


Figure 3 Mapping of Security Problem Definition to Security Objectives

4.3.1 Threats

T.NETWORK_ACCESS: Clients will allow network access only through authorization carried out by the TOE, due to the configuration of the network devices in the operational environment, given by **OE.NETWORK_PROTECT**.

Network access authorization is performed after the TOE enforces access control policies as required by **O.NAC**.

T.MANAGEMENT_ACCESS: Management of the TOE configuration objects is carried out through the HTTPS interface. It requires user authentication and authorization, as required by **O.MANAGEMENT**. It is assumed that the users that can access the management TOE interface have been properly established, given **OE.PERSONNEL**.

T.INTERNAL_CONFIGURATION: An internal configuration of the TOE is possible only during its installation, through an SSH interface that is closed after the initial configuration, given by **OE.PERSONNEL**

Other ways to alter the internal configuration of the TOE or the services of the system where it runs are not possible (e.g. physically accessing the computer to alter configuration files) due to **OE.PHYSEC**.

T.EAVESDROP: Sensitive data sent in authentication requests for TOE management, through the web interface, is not sent in plain data due to **O.COMM** and, thus, it is not possible to capture it by eavesdropping.

The following table maps the threats of the security problem established to the security objectives of the TOE and the security objectives of the operational environment.

Threats	Security Objectives
T.NETWORK_ACCESS	O.NAC OE.NETWORK_PROTECT
T.MANAGEMENT_ACCESS	O.MANAGEMENT OE.PERSONNEL
T.INTERNAL_CONFIGURATION	OE.PERSONNEL OE.PHYSEC
T.EAVESDROP	O.COMM

Table 2 Threats vs Security Objectives

4.3.2 Organizational Security Policies

P.AUDIT: This policy is addressed by **O.AUDIT**

The following table maps the organizational security policies of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

OSPs	Security Objectives
P.AUDIT	O.AUDIT

Table 3 OSPs vs Security Objectives

4.3.3 Assumptions

A.TRUSTED_ADMIN: This assumption is supported by **OE.PERSONNEL**, which requires that the personnel configuring the TOE are trusted and trained personnel that properly follow the TOE preparative guides.

A.SECURE_LOCATION: This assumption is supported by **OE.PHYSEC**, which requires that the infrastructure where the TOE is deployed has physical control access.

A.CONFIG: This assumption is supported by **OE.NETWORK_PROTECT**, which requires that the network infrastructure is configured in a way that network devices communicate to the TOE for network authentication and authorization requests, therefore the operational environment must support the communication between the network devices and the TOE.

A.VLAN_SEGREGATION: This assumption is supported by **OE.NETWORK_EQUIPMENT**, which requires that the network equipment is capable of setting-up reliable VLAN networks to achieve segregation of users or devices in the local area network.

A.TIMECONFIG: This assumption is supported by **OE.TIME**, which requires that the environment provides a reliable time source to the TOE

The following table maps the assumptions of the problem established to the security objectives of the TOE and the security objectives of the operational environment.

Assumptions	Security Objectives
A.TRUSTED_ADMIN	OE.PERSONNEL
A.SECURE_LOCATION	OE.PHYSEC
A.CONFIG	OE.NETWORK_PROTECT
A.VLAN_SEGREGATION	OE.NETWORK_EQUIPMENT

Assumptions	Security Objectives
A.TIMECONFIG	OE.TIME

Table 4 Assumptions vs Security Objectives for the Operational Environment

5 Extended Components Definition

5.1 Class FDP: User data protection

This class contains families specifying requirements related to protecting user data. FDP is split into four groups of families (listed below) that address user data within a TOE, during import, export, and storage as well as security attributes directly related to user data.

The families in this class are organised into four groups:

- User data protection security function policies:
- Forms of user data protection:
- Off-line storage, import and export:
- Inter-TSF communication:

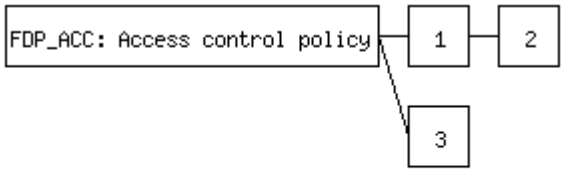
An access control policy needs to be established on the network it can be controlled which clients have rights to access to the network where the TOE is operating.
The TOE itself cannot carry out the network access control functionality, but it needs to be delegated to the network devices. These devices, such as managed switches, can effectively control the access of the clients to the network. To achieve this, the network devices configuration is established by the TOE.

5.1.1 Access control policy (FDP_ACC)

Family behavior

This family identifies the access control SFPs (by name) and defines the scope of control of the policies that form the identified access control portion of the SFRs related to the SFP. This scope of control is characterised by three sets: the subjects under control of the policy, the objects under control of the policy, and the operations among controlled subjects and controlled objects that are covered by the policy. The criteria allows multiple policies to exist, each having a unique name. This is accomplished by iterating components from this family once for each named access control policy. The rules that define the functionality of an access control SFP will be defined by other families such as FDP_ACF and FDP_ETC. The names of the access control SFPs identified here in FDP_ACC are meant to be used throughout the remainder of the functional components that have an operation that calls for an assignment or selection of an ``access control SFP.''

Component levelling



Access control to the network needs to be enforced by the network devices, based on authorization requests to the TOE.

Management: FDP_ACC.3

There are no management activities foreseen.

Audit: FDP_ACC.3

There are no auditable events foreseen.

FDP_ACC.3: Delegated access control

Hierarchical to:

No other components.

Dependencies:

No dependencies.

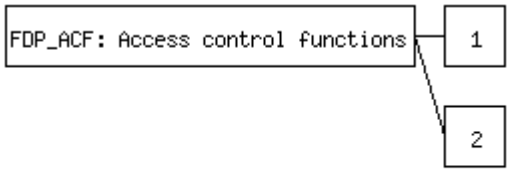
FDP_ACC.3.1: ***In response to requests from the network devices, the TSF shall evaluate the [assignment: access control SFP] on [assignment: list of subjects, objects and operations among subjects and objects covered by the SFP], providing the evaluation result in the response to the configured network devices so they can enforce the SFP***

5.1.2 Access control functions (FDP_ACF)

Family behavior

This family describes the rules for the specific functions that can implement an access control policy named in FDP_ACC. FDP_ACC specifies the scope of control of the policy.

Component levelling



The TOE shall listen and attend requests from the network devices, providing them a response based on the security attributes that they will use to carry out network access control.

Management: FDP_ACF.2

There are no management activities foreseen.

Audit: FDP_ACF.2

There are no auditable events foreseen.

FDP_ACF.2: Delegated Security attribute based access control

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_ACF.2.1: ***In response to requests from the network devices, the TSF shall evaluate the [assignment: access control SFP] to objects based on the following: [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes] , providing the evaluation result to the network devices so they can enforce the SFP.***

FDP_ACF.2.2: ***In response to requests from network devices, The TSF shall consider the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects] , providing the evaluation result to the network devices so they can enforce the SFP.***

FDP_ACF.2.3: ***In response to requests from network devices, the TSF shall evaluate the explicit authorisation of access of subjects to objects based on the following additional rules [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects] , providing the evaluation result to the network devices so they can enforce the SFP.***

FDP_ACF.2.4: ***In response to requests from network devices, the TSF shall evaluate the explicit denial of access of subjects to objects based on the following additional rules: [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects] , providing the evaluation result to the network devices so they can enforce the SFP.***

6 Security Requirements

This section defines the Security functional requirements (SFRs) and the Security assurance requirements (SARs) that fulfill the TOE. Assignment, selection, iteration and refinement operations have been made, adhering to the following conventions:

- Assignments. They appear between square brackets. The word “assignment” is maintained and the resolution is presented in ***boldface, italic and blue color.***
- Selections. They appear between square brackets. The word “selection” is maintained and the resolution is presented in ***boldface, italic and blue color.***
- Iterations. It includes “/” and an “identifier” following requirement identifier that allows to distinguish the iterations of the requirement. Example: FCS_COP.1/XXX.
- Refinements: the text where the refinement has been done is shown ***bold, italic, and light red color.*** Where part of the content of a SFR component has been removed, the removed text is shown in ~~***bold, italic, light red color and crossed out.***~~

6.1 Security Functional Requirements

6.1.1 FAU: Security audit

6.1.1.1 FAU_GEN.1: Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the ***[selection: not specified]*** level of audit; and

c) ***[assignment: events related to management and to network access control as follows:***
a) All create, update and delete actions over the following objects:
- Policy objects
- CMDB objects
b) Network access events, attempt to connect and its result: granted or blocked] .

Application Note

Audit functions cannot be shutdown, they are mandatory.

Application Note

Although read operations on the objects specified in this requirement are also subject to the access control policy, they don't generate audit data because of the potential high volume of the information generated.

Application Note

See first application note on FDP_ACC.1 for a detailed listing of CMDB items.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, ***[assignment: no other audit relevant information]*** .

6.1.1.2 FAU_GEN.2: User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.2 FDP: User data protection

6.1.2.1 FDP_ACC.1: Subset access control

FDP_ACC.1.1 The TSF shall enforce the ***[assignment: Access control SFP]*** on ***[assignment: Subjects: All users***
Objects: Policy objects and CMDB objects
Operations: CRUD operations] .

Application Note

The term "CMDB objects", when used in the context of this assignment and in the rest of this ST, refer to those items maintained in the TOE database that are related to TSF. Multiple item categories are maintained in the TOE database, but only a subset of them is related and relevant to the security functionality declared in this ST.

The following table lists the items that are considered CMDB:

Item	Description
Network devices	Devices in the operating network of the TOE that send RADIUS requests to the TOE for authentication and authorization.
Networks	Networks that can be registered in the TOE
VLANs	VLANs are registered in the TOE and later used in responses to authorization requests to indicate to the network devices which VLAN must be used for the connection associated to the request.

Security Profiles	Profiles that can be associated to evaluation of policies
Brands	Brands of network devices
Models	Models of network devices
Users	Users that can interact with the TOE for performing management functions or involved in network access control operative.
User roles	Asignation of users to roles, for performing management functions.
Roles	List of roles maintained in the TOE for role-based access control to management functions.
ACLs	List of allowed actions (read, create, update, delete) that users can perform on CMDB objects and policy objects, given as access control lists.
API Keys	API keys can be established so that, instead of using user authentication in REST API operations, a key can be used.

Table 5 *List of CMDB objects*

Application Note

CRUD (create, read, update, delete) operations on the above objects are exercised through the REST API.

6.1.2.2 FDP_ACC.3: Delegated access control

FDP_ACC.3.1 In response to requests from the network devices, the TSF shall evaluate the ***[assignment: Access Control SFP]*** on ***[assignment: subjects, objects and operations described in the next application note]*** , providing the evaluation result in the response to the configured network devices so they can enforce the SFP

Application Note

Subjects, objects and operations for **FDP_ACC.3**

Subjects	Objects	Operations
Clients (MAC address or user/pass)	VLAN networks	Access

Table 6 Subjects, objects and operations for FDP_ACC.3

6.1.2.3 FDP_ACF.1: Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** to objects based on the following: ***[assignment: Subjects: All users***
Objects: Policy objects and CMDB objects
Operations: CRUD Operations] .

Application Note

CRUD (create, read, update, delete) operations on the above objects are exercised through the REST API.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[assignment: see application note below]*** .

Application Note

The following table indicates which are the allowed operations (create, read, update or delete) on policy objects and CMDB objects that users are entitled to perform, depending on their role. In each cell, it is indicated which roles have rights to perform the associated operation.

Object	Read	Create	Update	Delete
ACL	administrator readonly user otpmanager		administrator	
Device brands	administrator readonly			

Network device	administrator readonly	administrator	administrator	administrator
User device	administrator readonly	administrator	administrator	administrator
Device models	administrator readonly	administrator	administrator	administrator
Network	administrator readonly	administrator	administrator	administrator
Policy	administrator readonly	administrator	administrator	administrator
Role	administrator readonly	administrator	administrator	administrator
User	administrator readonly	administrator	administrator	administrator
User/Role associations	administrator readonly user otpmanager		administrator	

VLAN	administrator readonly	administrator	administrator	administrator
Security profiles	administrator readonly	administrator	administrator	administrator
API Keys	administrator readonly	administrator	administrator	administrator
Log files (audit data)	administrator readonly			

Table 7 ACL rules

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: ***[assignment: none]*** .

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: ***[assignment: none]*** .

6.1.2.4 FDP_ACF.2: Delegated Security attribute based access control

FDP_ACF.2.1 In response to requests from the network devices, the TSF shall evaluate the ***[assignment: Access Control SFP]*** to objects based on the following: ***[assignment: table of subjects, objects and operations in the following application note]*** , providing the evaluation result to the network devices so they can enforce the SFP.

Application Note

Subjects, objects and operations for **FDP_ACF.2**

Subjects	Objects	Operations

Clients (device MAC, user/password)	VLAN networks	Access

Table 8 Subjects, objects and operations for FDP_ACF.2

FDP_ACF.2.2 In response to requests from network devices, The TSF shall consider the following rules to determine if an operation among controlled subjects and controlled objects is allowed: ***[assignment: none]*** , providing the evaluation result to the network devices so they can enforce the SFP.

FDP_ACF.2.3 In response to requests from network devices, the TSF shall evaluate the explicit authorisation of access of subjects to objects based on the following additional rules ***[assignment: none]*** , providing the evaluation result to the network devices so they can enforce the SFP.

FDP_ACF.2.4 In response to requests from network devices, the TSF shall evaluate the explicit denial of access of subjects to objects based on the following additional rules: ***[assignment: none]*** , providing the evaluation result to the network devices so they can enforce the SFP.

6.1.3 FIA: Identification and authentication

6.1.3.1 FIA_ATD.1: User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: ***[assignment: ID, Name, Source, Mail, Role]*** .

6.1.3.2 FIA_UAU.1: Timing of authentication

FIA_UAU.1.1 The TSF shall allow ***[assignment: none]*** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.3 FIA_UID.1: Timing of identification

FIA_UID.1.1 The TSF shall allow ***[assignment: none]*** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 FMT: Security management

6.1.4.1 FMT_MSA.1: Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** to restrict the ability to ***[selection: [assignment: create, update, delete]]*** the security attributes ***[assignment: user roles]*** to ***[assignment: Administrator]***.

Application Note

By default, only administrators have the ability of modifying user roles. User roles can be read by both Administrator and readonly roles, but readonly role doesn't have permissions to create, delete or update user roles. Nevertheless, one of the TOE management functions allows administrators to modify the rules for access control of users to policy objects and CMDB objects. In consequence, an administrator could modify an access control list in a way that another role is able to modify user roles.

6.1.4.2 FMT_MSA.3: Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the ***[assignment: Access Control SFP]*** to provide ***[selection: restrictive]*** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the ***[assignment: Administrator]*** to specify alternative initial values to override the default values when an object or information is created.

6.1.4.3 FMT_SMF.1: Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: ***[assignment: a) Assign roles to users***
b) Manage machine, system and user policies
c) View audit logs].

6.1.4.4 FMT_SMR.1: Security roles

FMT_SMR.1.1 The TSF shall maintain the roles ***[assignment: administrator, readonly, user, otpmanager]*** .

Application Note

The TOE includes a role named *otpmanager*, which is related to one time password functionality, which is out of the scope of the TSF. However, this role is included and described in this ST to detail its relationship with the Role Based Access Control functionality of the TOE, since some of the TOE management functions are available to *otpmanager* role.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5 FPT: Protection of the TSF

6.1.5.1 FPT_STM.1: Reliable time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.6 FTP: Trusted path/channels

6.1.6.1 FTP_ITC.1: Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit ***[selection: another trusted IT product]*** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for ***[assignment: none]*** .

6.2 Security Assurance Requirements

The development and the evaluation of the TOE shall be done in accordance to the following security assurance requirements: **EAL2**

The following table shows the assurance requirements by reference the individual components in [CC31R5P3]

Assurance Class	Assurance Components
ASE: Security Target evaluation	ASE_CCL.1: Conformance claims ASE_ECD.1: Extended components definition ASE_INT.1: ST introduction ASE_TSS.1: TOE summary specification ASE_OBJ.2: Security objectives ASE_REQ.2: Derived security requirements ASE_SPD.1: Security problem definition
ALC: Life-cycle support	ALC_CMC.2: Use of a CM system ALC_CMS.2: Parts of the TOE CM coverage ALC_DEL.1: Delivery procedures
ADV: Development	ADV_ARC.1: Security architecture description ADV_FSP.2: Security-enforcing functional specification ADV_TDS.1: Basic design
AGD: Guidance documents	AGD_OPE.1: Operational user guidance AGD_PRE.1: Preparative procedures
ATE: Tests	ATE_COV.1: Evidence of coverage ATE_FUN.1: Functional testing ATE_IND.2: Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2: Vulnerability analysis

Table 9 Security Assurance Requirements

6.3 Security Requirements Rationale

6.3.1 Necessity and sufficiency analysis

SFR / TOE Security Objective	O.MANAGEMENT	O.NAC	O.AUDIT	O.COMM
FAU_GEN.1			X	
FDP_ACC.3		X		
FDP_ACF.2		X		
FMT_MSA.1	X			
FMT_MSA.3	X			
FMT_SMF.1	X			
FMT_SMR.1	X			
FTP_ITC.1	X			X
FIA_ATD.1	X			
FIA_UID.1	X			
FIA_UAU.1	X			
FAU_GEN.2			X	
FDP_ACC.1	X			
FDP_ACF.1	X			
FPT_STM.1			X	

Table 10 *SFRs / TOE Security Objectives coverage*

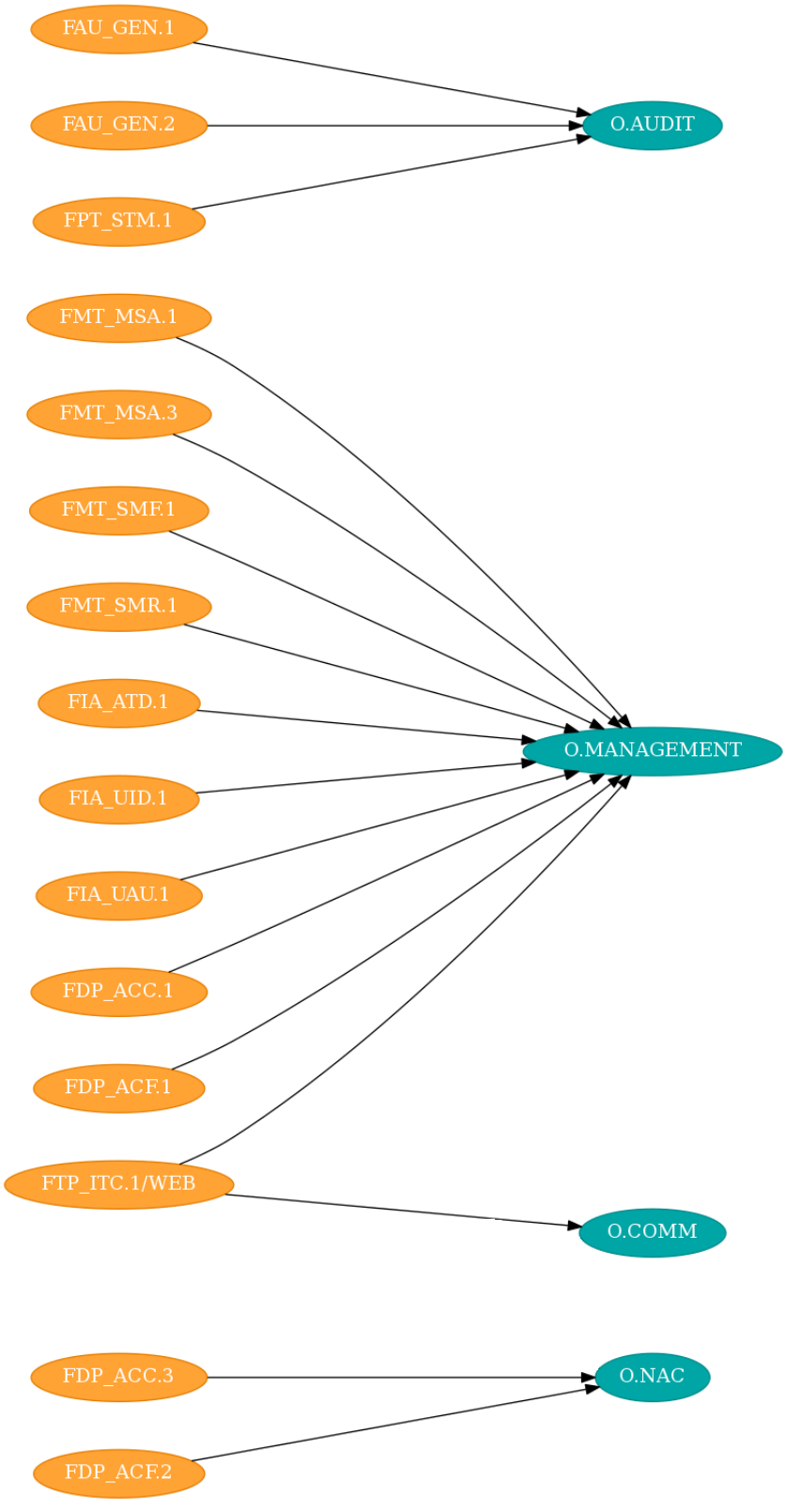


Figure 4 Mapping of SFRs to TOE Security Objectives

6.3.2 Security Requirement Sufficiency

O.MANAGEMENT: This objective ensures that the management of the TOE configuration through the administration interfaces is done enforcing authentication and authorization.

FDP_ACC.1 requires that the access to the management functions of the TOE for is controlled.

FDP_ACF.1 supports **FDP_ACC.1** ensuring that access to management functions of the TOE is based on the user privilege level and their allowable actions.

FIA_ATD.1 specifies the security attributes for users of the TOE.

FIA_UID.1 requires the TOE to enforce identification of all users prior to performing TSF-initiated actions on behalf of the user.

FIA_UAU.1 requires the TOE to enforce authentication of all users prior to performing TSF-initiated actions on behalf of the user.

FMT_MSA.1 specifies that only privileged administrators can access the TOE security functions and related configuration data.

FMT_MSA.3 ensures that the default values of the security attributes are restrictive in nature as to enforce the access control policy for the TOE.

FTP_ITC.1 ensures that a trusted inter-communication channel exists to perform the management functions of the TOE. This channel is established between the management client (web browser or REST API client) and the TOE

FMT_SMR.1 ensures that the TOE maintain different roles associated to users involved in management functions.

FMT_SMF.1 specifies the list of management functions available through the interface administration.

O.NAC: **FDP_ACC.3** requires that the access control SFP to the network resources is enforced by the network devices, based on policy evaluations performed by the TOE upon requests from the network devices.

FDP_ACF.2 supports **FDP_ACC.3** ensuring that the access control to the network is performed based on evaluation of policies carried out by the TOE.

O.AUDIT: **FAU_GEN.1** ensures the generation of audit data, and determines what is audited.

FAU_GEN.2 ensures that each audit data event is associated to the identity of an user, related to the generation of the event.

FPT_STM.1 ensures that reliable timestamps are associated to any audit data generated by the TOE.

O.COMM: **FTP_ITC.1** ensures the protection of the communications between the TOE and the client that uses the REST API. This communication is carried out using HTTPS protocol, preventing attackers to capture sensitive data in traffic.

6.3.3 SFR Dependency Rationale

6.3.3.1 Table of SFR dependencies

The following table lists the dependencies for each requirement, indicating how they have been satisfied. The abbreviation "h.a." indicates that the dependency has been satisfied by a SFR that is hierarchically above the required dependency.

SFR	Required	Fulfilled	Missing
FAU_GEN.1	FPT_STM.1	FPT_STM.1	None
FDP_ACC.3	None	None	None
FDP_ACF.2	None	None	None
FMT_MSA.1	FMT_SMR.1, FMT_SMF.1, [FDP_ACC.1 or FDP_IFC.1]	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1	None
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1	None
FMT_SMF.1	None	None	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1	None
FTP_ITC.1	None	None	None
FIA_ATD.1	None	None	None
FIA_UID.1	None	None	None
FIA_UAU.1	FIA_UID.1	FIA_UID.1	None
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.1	None
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1	None
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3	None
FPT_STM.1	None	None	None

Table 11 *SFR Dependencies*

6.3.4 SAR Rationale

The SARs were chosen according to the market expected evaluation assurance level for the TOE type.

6.3.5 SAR Dependency Rationale

6.3.5.1 Table of SAR dependencies

SAR	Required	Fulfilled	Missing
ASE_CCL.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.1	ASE_INT.1, ASE_ECD.1, ASE_REQ.2 (hierarchically above ASE_REQ.1)	None
ASE_ECD.1	None	None	None
ASE_INT.1	None	None	None
ASE_OBJ.2	ASE_SPD.1	ASE_SPD.1	None
ASE_REQ.2	ASE_OBJ.2, ASE_ECD.1	ASE_OBJ.2, ASE_ECD.1	None
ASE_TSS.1	ASE_INT.1, ASE_REQ.1, ADV_FSP.1	ASE_INT.1, ASE_REQ.2 (hierarchically above ASE_REQ.1), ADV_FSP.2 (hierarchically above ADV_FSP.1)	None
ALC_CMC.2	ALC_CMS.1	ALC_CMS.2 (hierarchically above ALC_CMS.1)	None
ALC_CMS.2	None	None	None
ADV_FSP.2	ADV_TDS.1	ADV_TDS.1	None
AGD_OPE.1	ADV_FSP.1	ADV_FSP.2 (hierarchically above ADV_FSP.1)	None
AGD_PRE.1	None	None	None
ATE_IND.2	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	ADV_FSP.2, AGD_OPE.1, AGD_PRE.1, ATE_COV.1, ATE_FUN.1	None
AVA_VAN.2	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	ADV_ARC.1, ADV_FSP.2, ADV_TDS.1, AGD_OPE.1, AGD_PRE.1	None
ASE_SPD.1	None	None	None
ALC_DEL.1	None	None	None
ADV_ARC.1	ADV_FSP.1, ADV_TDS.1	ADV_FSP.2 (hierarchically above ADV_FSP.1), ADV_TDS.1	None
ADV_TDS.1	ADV_FSP.2	ADV_FSP.2	None
ATE_COV.1	ADV_FSP.2, ATE_FUN.1	ADV_FSP.2, ATE_FUN.1	None
ATE_FUN.1	ATE_COV.1	ATE_COV.1	None

Table 12 SAR dependencies

7 TOE Summary Specification

This section presents the security functions implemented by the TOE. They are the following:

- Security Audit (SF.Audit)
- User Data Protection (SF.User_Data_Protection)
- Identification and Authentication (SF.Identification_Authentication)
- Security Management (SF.Security_Management)
- Trusted Path/Channels (SF.Trusted_Path)

7.1 SF.Audit

FAU_GEN.1 provides the generation of audit data by the TOE, for all the auditable events specified by such security functional requirement. Each event generated is associated with a user identification, as indicated by **FAU_GEN.2**. Besides, **FPT_STM.1** is met by ensuring that each audit event generated has a reliable timestamp associated.

7.2 SF.User_Data_Protection

Protection of user data is implemented by the TOE for a) management functions via HTTPS interface and b) access control of the devices/users in the network to the different network resources.

For management functions via HTTPS interface, the TOE implements an Access Control Policy to define what roles can access particular functions related to TOE management. **FDP_ACC.1** provides enforcement of the access control policy on subjects related to TOE management, and **FDP_ACF.1** defines the rules used for access control.

For access to network resources, user data protection is enforced by the network devices by sending RADIUS requests to the TOE, which is able to receive them thanks to the RADIUS component with the openNAC module. These requests are attended by the TOE by performing policy evaluation and, depending on the evaluation result, RADIUS responses are provided to the network devices. Such responses contain the authorization or non-authorization to the required network resource. This way is how **FDP_ACC.3** and **FDP_ACF.2** extended requirements are met by the TOE.

7.3 SF.Identification_Authentication

Identification and authentication are required for users in order to access the management of TOE functions, via the HTTPS interface from a web browser or REST client. To exercise any of the management functions available through this interface, the users first need to be authenticated, sending an authentication request that contains the user identifier and password, thus meeting **FIA_UAU.1**. Once authenticated, each management action requested by the user needs to be accompanied by its identifier, typically using an authentication token that was returned in the response to a successful authentication request. This token is required to be included in each request associated with a management action sent to the TOE via HTTPS interface, otherwise, the action request is denied. Therefore, **FIA_UID.1** is met this way.

Once authenticated, the user is able to carry out those management functions allowed to the user roles associated to him. The TOE maintains a role for each individual user, therefore implementing role-based access control to provide a convenient way to assign a user to a particular job function or set of permissions. The TOE can sign users to roles, based on attributes of their identity, and then associate permissions to the role, therefore meeting **FIA_ATD.1**.

7.4 SF.Security_Management

All management related functions of the TOE are carried out via the web (HTTPS) interface. An user authenticates against the TOE using a web browser or REST client, and then he is able to perform management functions. All the management functions described in this section refer to actions performed this way, via web interface.

For management purposes, the TOE maintains three user roles: administrator, readonly, user and otpmanager. These roles can be assigned to users from the management interfaces. This way, **FMT_SMR.1** is met.

Only users with the Administrator role can create, modify or delete roles, and only users with the Administrator role can assign roles to users. Users with the readonly role have only read rights on roles. This way, **FMT_MSA.1** is met.

Besides, The TOE ensures that only secure values are accepted for the security attributed listed with Access Control SFP, and these values are set by the users with Administrator role. This way, **FMT_MSA.3** is met.

The TOE management functions include assigning roles to users, managing policies and viewing audit logs, therefore meeting **FMT_SMF.1**.

7.5 SF.Trusted_Path

A trusted communication channel for TOE management functions is provided between the management client, a web browser or REST client, and the TOE itself via port 443, provided by **FTP_ITC.1**. This communication channel occurs using HTTPS protocol, thus all communications are encrypted.

8 Appendices

8.1 Appendix A. List of compatible network devices

The devices listed in this section fulfill the technical requirements needed to interoperate with the TOE for network access control operative.

Wired devices

- 3COM NJ220
- 3COM SS4200
- 3COM SS4500
- 3COM 4200G
- 3COM E4800G
- 3COM E5500G
- Accton ES3526XA
- Accton ES3528M
- AlcatelLucent6250/5450/6860
- Allied Telisis AT8000GS
- Amer SS2R24i
- Avaya (see Nortels)
- Brocade ICX64XX
- Brocade ICX66XX
- Brocade FastIron 4802
- Brocade FCXXXXX
- Brocade FI-SXXXX
- Cisco Catalyst iOS XE
- Cisco 2900XL
- Cisco 2900XL
- Cisco 2950
- Cisco 2960 / 2970

- Cisco 3500XL Series
- Cisco 3550
- Cisco 3560
- Cisco 3750
- Cisco 4500
- Cisco 6500
- Cisco ISR 1800 Series
- Cisco IOS XE (all switches)
- Dell PowerConnect 3424
- Dell/Force 10
- D-Link DES3526
- D-Link DES3550
- D-Link DGS3100
- D-Link DGS3200
- Edge-corE 4510
- Enterasys D2
- Enterasys Matrix N3
- Enterasys SecureStack C2
- Enterasys SecureStack C3
- Extreme Networks Summit (XOS)
- Extreme Networks EAS
- HP E4800G
- HP E5500G
- HP Procurve 2500 Series
- HP Procurve 2600 Series
- HP Procurve 2920 Series
- HP Procurve 3400cl Series
- HP Procurve 4100 Series
- HP Procurve 5300 Series
- HP Procurve 5400 Series

- HP/H3C S5120
- Huawei S2700
- Huawei S3700
- Huawei S5700
- Huawei S6700
- Huawei S7700
- Huawei S9700
- IBM/Lenovo StackSwitch G8052
- Intel Express 460
- Intel Express 530
- Juniper Networks EX Series
- LG iPecs Series
- Linksys SRW224G4
- Netgear FGS Series
- Nortel BayStack 470
- Nortel BayStack 4550
- Nortel BayStack 5500 Series
- Nortel ERS 2500 Series
- Nortel ERS 4000 Series
- Nortel ERS 4500 Series
- Nortel ERS 5500 Series
- Nortel ES325
- Nortel BPS2000
- SMC TS6128L2
- SMC TS6224M
- SMC SMC8824M - SMC8848M
- Ubiquiti EdgeSwitch

Wireless devices

- Aerohive AP Series
- Aruba Networks(200,600,800,2400,3000,6000,7000,7200)

- AnyFi Controller
- Avaya Wireless controllers
- BelAir Networks (Ericsson)
- Brocade Mobility Wireless LAN controllers
- Cisco Wireless Services Module (WiSM, WiSM2)
- Cisco WLC (all models)
- D-Link DWS 3026
- Enterasys V2110 wireless controller
- Extreme Networks Summit Wireless controllers
- Extricom EXSW Wireless Switches (controllers)
- HP ProCurve MSM710 Mobility controller
- Huawei AC6605 wireless controller
- Juniper (Trapeze) Wireless controllers
- Meraki
- Meru Networks Wireless controllers
- MikroTik
- Mojo Networks
- Motorola/Zebra RF Switches (controllers)
- Ruckus Wireless controllers MAC Auth
- Xirrus WiFi Arrays

Access points

- Aerohive AP Series
- Aruba Instant Access Points
- Cisco 1130AG
- Cisco 1240AG
- Aruba Instant Access Points
- Cisco 1250
- D-Link DWL Access Points
- HP ProCurve
- OpenWRT with hostapd or CoovaChilli

- HP ProCurve
- Xirrus WiFi Arrays

VPN server supported devices

All the VPNs concentrator that support Radius protocol are suitable to be integrated with openNAC Technologies:

- Juniper Networks
- Netscaler
- Cisco ASA
- PaloAlto
- FortiGate

9 Acronyms

The following table shows the acronyms used in this document.

Acronym	Meaning
ST	Security Target
PP	Protection Profile
CC	Common Criteria
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFi	TSF Interface
IT	Information Technology
OSP	Organizational Security Policy
EAL	Evaluation Assurance Level
TSC	TSF Scope of Control
TSS	TOE Summary Specification
RADIUS	Remote Authentication Dial-In User Service
NAC	Network Access Control
WAN	Wide Area Network
LAN	Local Area Network
VLAN	Virtual Local Area Network
MAC	Media Access Control
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
UDS	User Data Source
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol

Table 13 *Abbreviations*

10 Glossary of Terms

Term	Meaning
Augmentation	Addition of one or more requirement(s) to a package
Evaluation Assurance Level	Set of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale, that form an assurance package
Operational Environment	Environment in which the TOE is operated
Protection Profile	Implementation-independent statement of security needs for a TOE type
Security Target	Implementation-dependent statement of security needs for a specific identified TOE
Target Of Evaluation	Set of software, firmware and/or hardware possibly accompanied by guidance
Authenticator Source	Authentication sources are repositories that allow importing and/or authenticate users and groups
Managed Device	Device whose support and security is responsibility of the corporate IT department
Network Device	Network devices are physical devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data in a computer network. Network devices may include gateways, routers, network bridges, modems, wireless access points, networking cables, line drivers, switches, hubs, and repeaters.
Policy	A set of conditions that define how devices can enter, and operate within, an organization's network.
Quarantined Device	Device isolated from the network through a security policy that automatically reconfigures the network restricting device network access
Radius	Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service.
Registered Device	Known user device
Tags	Text label with the form of a keyword used to classify or organize devices and to facilitate profiling and policy generation
Unmanaged Device	Device whose support and security is responsibility of the user
User Device	Computing resource that communicates on a network, i.e. laptop, desktop machine, printer, E-mail server, etc. Entity at one end of a point-to-point LAN segment that seeks to be authenticated by an authenticator attached to the other end of that link.

Table 14 *Glossary of terms*

11 Document References

The following table shows the documents referenced in this document.

Reference	Document
CC31R5P1	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 1: Introduction and general model
CC31R5P2	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 2: Security functional components
CC31R5P3	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, Part 3: Security assurance components
CEM31R5P3	Common Criteria Evaluation methodology, Version 3.1, Revision 5
API-DOC	openNAC Enterprise - REST API specification v1.2
RFC-2865	Specificaton of RADIUS protocol, RFC 2865
OPENNAC-ONLINE-GUIDES	Online user guides of OpenNAC, covering for multiple openNAC products, including openNAC Enterprise (it includes configurations and features outside the TOE evaluated configuration). Available at http://doc-opennac.opencloudfactory.com
RFC1918	RFC 1918, Address Allocation for Private Internets

Table 15 *List of document references*