OPNsense Business Edition

Security Target

v0.8

29/07/2024

Created by   

Version control

Version	Comment	Date
0.1	Initial version	14/11/2023
0.2	Changes after CPSTIC comments	22/12/2023
0.3	Changes after CPSTIC comments	22/02/2024
0.4	Changes after CPSTIC comments	18/03/2024
0.5	Changes after client given information	17/04/2024
0.6	Changes after CPSTIC comments	13/05/2024
0.7	Audit logs clarifications	03/07/2024
0.8	Syslog configuration added	29/07/2024

Table of contents

1 Introduction

This document is the Security Target for **OPNsense Business Edition**. This document includes the following information:

1. Information about this document.
2. Description of the functionality of the solution and use cases, which allows organizations or public services to address the threats and risks described in the document.
3. Description of the execution environment.
4. Threat and risk analysis of the product.
5. Fundamental security requirements covered by this solution and how they are covered to implement each security function.
6. Acronyms, Glossary of terms and Document references.

1.1 Sponsor, TOE and evaluation information

Applicant data	Deciso B.V.
Developer data	Deciso B.V.
Contact information of developer	Ad Schellevis +31(0)187744020 a.a.schellevis@deciso.com Edison 43, 3241 LS Middelharnis, The Netherlands.
TOE name	OPNsense Business Edition
TOE version	23.10.2
Evaluation type	LINCE
User guidance and version	See *2.2: Identification of the TOE secure use, installation and configuration guides*
Taxonomy according to CCN-STIC-140	N/A

1.2 Methodology and evaluation criteria

CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Evaluation Methodology for National Essential Security Certification March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Security Target template for National Essential Security Certification March 2022 version 2.0).

2 TOE description

2.1 TOE Functional description

OPNsense Business Edition, from now on referred as TOE, is a stateful software-based firewall. It is in charge of interconnecting two or more networks, channelling all communications between them through itself to examine each message and block those that do not meet the specified security criteria.

The TOE includes both the firewall application and the platform/operating system on which it operates. The underlying operating system, based on FreeBSD, is an essential component of the TOE, as it provides the necessary capabilities for the secure execution of the TOE. The TOE is thus considered as an integrated solution comprising:

1. Firewall application: implements traffic filtering and security policy management functionality
2. Platform/Operating System: FreeBSD, specifically configured to support the security operations required by the TOE.
3. Management Interface: Includes both the command line interface (CLI) and the graphical user interface (GUI), through which the administration of the TOE is performed.

Although the TOE offers a wide range of additional functionalities, such as VPN, proxy, intrusion detection, among others, the scope of evaluation focuses on the firewall functionality (traffic filtering and policy management).

In this context, the TOE interconnect two or more networks so that all communications between these networks pass through it, in order to examine each message and filtering those that do not meet the specified security criteria.

Filtering is implemented at various levels within the layers defined by the Open Systems Interconnection model (ISO/IEC 7498-1), specifically addressing network (Layer 3) and transport (Layer 4).

Regarding to the TOE management, the TOE can be managed by two different interfaces:

- **CLI interface:**
  - Local access: Available directly on the machine where the TOE is installed, allowing administrators to perform the initial configuration, maintenance and management of the system without the need for a network connection.
  - Remote access: which allows remote TOE management via SSHv2. The use of this interface is not allowed to the *root* user.
- **GUI interface:** it is a web interface which allows TOE management via HTTPS (over TLS v1.2 or higher).

Figure 1 TOE CLI interface

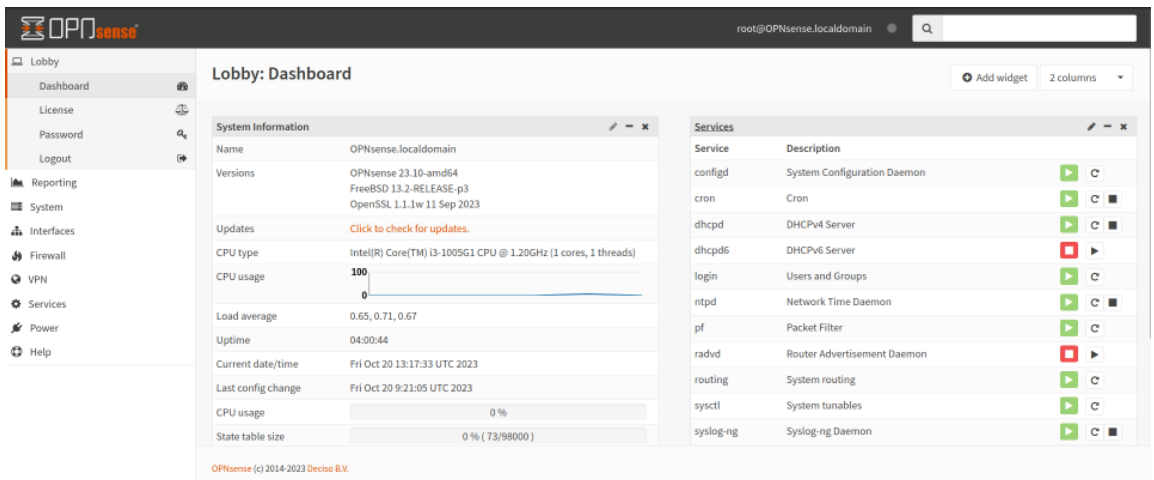


Figure 2 TOE GUI interface

In relation with the specific functionalities of the TOE, it can be defined the following:

- **SF. Trusted Administration:** The TOE defines users and groups, permissions can be specified for groups and for individual users. The TOE defines a default root user with all permissions. Only administrator users or users with the necessary permissions set can perform management functions.
- **SF. Identification and Authentication:** The TOE is in charge of identifying and authenticating every user, apart from implementing mechanisms to prevent brute-force attacks and a password policy. In addition, the TOE is capable to close a user's session after a determined inactivity time.
- **SF. Trusted Communication Channels:** The TOE protects the information in transit for management purposes by establishing secure communications channels using SSHv2 and HTTPS (over TLS v1.2 or higher). In addition, the TOE establishes secure communication channels using TLS v1.2 when exchanging information with external syslog servers and using TLS v1.3 with the endpoints for OPNsense updates.

- **SF. Cryptography:** The TOE supports only cryptographic algorithms and functions accepted for ENS MEDIUM category of CCN-STIC-807 guide.
- **SF. Trusted Installation and Updates:** The TOE shall verify the authenticity of updates using a digital signature RSA-4096 with RSASSA-PKCS#1 padding and the SHA-256 checksum. Furthermore, the TOE allows to check if any new updates are available.
- **SF. Audit:** The TOE produces a range of audit records based on various events and behaviours detected during its operation. An access control policy is applied to the audit records. Finally, the audit data can be sent to an external syslog server.
- **SF. Protection of Credentials and Sensitive Data:** Credentials and private keys are protected by access control (read/write permissions only for the root user and read permission for wheel user group).
- **SF. Firewalls:** The TOE allows to configure rules with actions to allow, block or reject traffic, based on attributes such as IP addresses, protocols and ports.

2.2 Identification of the TOE secure use, installation and configuration guides

The following table lists the documents and user's guides necessary to carry out the configuration of the TOE properly:

Document's type	Document's name	Document's version (update-history-date)
Installation, Configuration and Operation **Guide**	OPNsense Documentation	Version d971b9d

2.3 TOE usage description

The following steps shall be followed in order to bring the TOE to the evaluated configuration:

2.3.1 OPNsense Business Initial Configuration

In the evaluated configuration, an installation image of type "dvd" (ISO image) is used. To performs the installation, the steps needed are the following:

1. Open VMware and click on Create a new virtual machine.
2. Select the TOE ISO and click on “Next”
3. Give a name to the virtual machine and click on “Next”.
4. Set 30GB as disk size.
5. Click on Customize Hardware > Memory and set 1GB of RAM memory. Also, add network adapters according to your network needs.
6. Press “Close”.
7. Click on “Finish”.
8. Wait for the TOE to boot up.
9. In order to install the TOE, log in with the user “installer” and authenticate with the password “opnsense”.
10. Select the Keyboard layout.
11. Indicate “Continue with…”
12. Select “Install (UFS)” and press Enter.
13. Select "stripe" and press Enter.
14. Select the virtual disk and press OK.
15. Select Yes and press Enter.
16. Select “Change root password” and press OK.
17. Define a new password for the root user, the password shall be in compliance with the password policy declared in SF. Identification and Authentication, specifically in the **IAU.3** requirement.
18. Select "Complete Install" and Press OK.
19. Wait for the TOE to reboot and navigate to the web interface.
20. Log in with the root user credentials
21. Follow the wizard setup, press Next.
22. Give a hostname and domain to the TOE and press Next
23. Set the NTP servers and the time zone. In this case the NTP servers configured are the ones offered by default. Press Next.
24. Leave the default parameters for the configuration related to the WAN interface and press Next.
25. Leave the default parameters for the configuration related to the LAN interface and press Next.
26. Set a new root password if it was not changed before. The password shall be in compliance with the password policy declared in SF. Identification and Authentication, specifically in the **IAU.3** requirement.
27. Click on reload to apply the changes

The TOE is now configured and ready.

2.3.2 Update to the evaluated version

The TOE is provided for version 23.10 and it must be updated to version 23.10.2 in order to reach the evaluated version. Therefore, the following steps must be executed:

1. Log in through the web interface with the root user.
2. Go to System > Firmware > Settings and toggle "Advanced mode".
3. Indicate "23.10/MINT/23.10.2/latest" in the Flavour parameter and introduce the Subscription key.
4. Go to the Status tab and click Check for updates.
5. Click Update.
6. Wait for the update to be installed.

2.3.3 Security Considerations

The following factors shall be considered to achieve the security functions outlined in Section *5 Security Functional Requirements*:

- By default, the TOE uses a self-signed certificate. It shall be replaced with a customized certificate, which can be configured in the *System → Trust → Certificates* menu. This user-configured certificate shall be generated with RSA-3072 or higher.
- Check that the *enable access log* parameter is activated in the *System > Settings > Administration* menu. This parameter allows to record all accesses to the TOE.
- The user shall configure a 2FA in the user configuration process, following section *"Configure 2FA TOTP & Google Authenticator"* from *OPNsense Documentation* guide declared in section 2.2.

2.3.4 Idle timeout configuration

In order to configure the GUI and CLI idle timeout, this field has to be modified through GUI interface in *System → Settings → Administration* and establishing the value "5" (5 minutes) to the parameters *Session Timeout* (for GUI interface) and *Inactivity timeout* (for CLI interface).

In order to accurately configure the CLI idle timeout, the Login shell must be modified to one of last the three options (/bin/csh, /bin/sh, /bin/tcsh). This configuration can be performed in the User information for each user via GUI interface. If the Login shell is maintained to "/usr/local/sbin/opnsense-shell" (the default value), the idle timeout will not be applied to CLI interface.

2.3.5 Access control configuration

By default, the file containing the credentials and private keys of TOE users can be viewed by any user. To limit access to the file so that only the administrator users have permissions, it is necessary to execute the command ***chmod 640 /conf/config.xml*** through the CLI interface with a root user. This command will apply the following configuration:

- *root* user will be able to read and write the credentials and private keys.
- *wheel* user group will be able to read the credentials and private keys. The *wheel* user group includes both the *root* user and users considered as administrators (equivalent to the *sudoers* group on Linux systems but applied to FreeBSD).

2.3.6 Password Policy

The product includes the functionality of modifying the local account password policy. In order to comply with the security requirements, it is necessary to do the following steps for the users:

Enter the TOE GUI and go to the following menu *System* → *Access* → *Servers*, then choose the *Local Database* option and configure the following values as indicated:

- **Policy**. Enable password policy constraints.
- **Length**. Minimum password length to require. From the options provided by the TOE, a minimum length of 12 characters should be set.
- **Complexity**. Enforce password complexity checks.

2.3.7 Cipher suites configuration

The TOE shall be configured only with the following cipher suites and SSH parameters to allow the communication with the GUI and CLI interfaces, the external syslog server and the external update server:

GUI interface (*TLS v1.2 or higher)*

In order to meet the cryptographic requirements, it is required to configure the ciphersuites for TLS through the web interface. The steps below are needed to be followed:

1. Log in through the web interface with the root user.
2. Navigate to System > Settings > Administration.
3. In the Web GUI section, use the dropdown menu for "SSL Ciphers" to select valid ciphersuites:
   - *TLS_AES_128_GCM_SHA256*
   - *TLS_AES_256_GCM_SHA384*
   - *TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256*
   - *TLS_CHACHA20_POLY1305_SHA256*
   - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256*
   - *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384*

External syslog server (*TLS v1.2 or higher)*

In order to meet the cryptographic requirements, it is required to configure accepted cipher suites through the command line interface. This configuration affects the TLS connection when the TOE communicates with a remote syslog server. The steps below are needed to be followed:

1) Log in through the CLI interface with the root user.

2) Edit the file:
   `/etc/local/opnsense/service/templates/OPNsense/Syslog/syslog-ng-destinations.conf`
3) In the network parameters, inside the TLS parameters, add the following lines:

```
ssl-options(no-sslv2, no-sslv3, no-tlsv1, no-tlsv11)
cipher-suite("ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-
SHA256s:TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_AES_128_GC
```

```
M_SHA256:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-
SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-
ECDSA-AES128-CCM")
```

4) Save the file.

CLI interface *(SSHv2)*

In order to meet the cryptographic requirements, it is required to configure accepted cryptographic parameters for SSH through the web interface. The steps below are followed:

1) Log in through the web interface with the root user.
2) Navigate to System > Settings > Administration.
3) In the Secure Shell section, use the dropdown menu for "Key exchange algorithms", "Ciphers", "MACs" and "Public key signature algorithms" to select valid cryptographic parameters.
   - **SSH Key Exchange Method**
     - diffie-hellman-group16-sha512
     - diffie-hellman-group18-sha512
     - ecdh-sha2-nistp256
     - ecdh-sha2-nistp384
     - ecdh-sha2-nistp521
   - **SSH Encryption Algorithms**
     - aes128-ctr
     - aes192-ctr
     - aes256-ctr
   - **SSH Public Key Algorithm**
     - ecdsa-sha2-nistp256
   - **SSH MAC Algorithm**
     - hmac-sha2-256
     - hmac-sha2-512

2.3.8 Log rules configuration

To log the packets managed by a firewall rule (passed, blocked or rejected), it is necessary to enable the option ***Log*** in the menu *Firewall → Rules → LAN* for each rule that is considered relevant.

2.3.9 Logs Traceability

The TOE allows accurate identification of configuration changes, extending the audit log, via the menu *System > Configuration > History* in the GUI interface. In this menu, the current configuration is compared with the previous one, as shown in the following image:

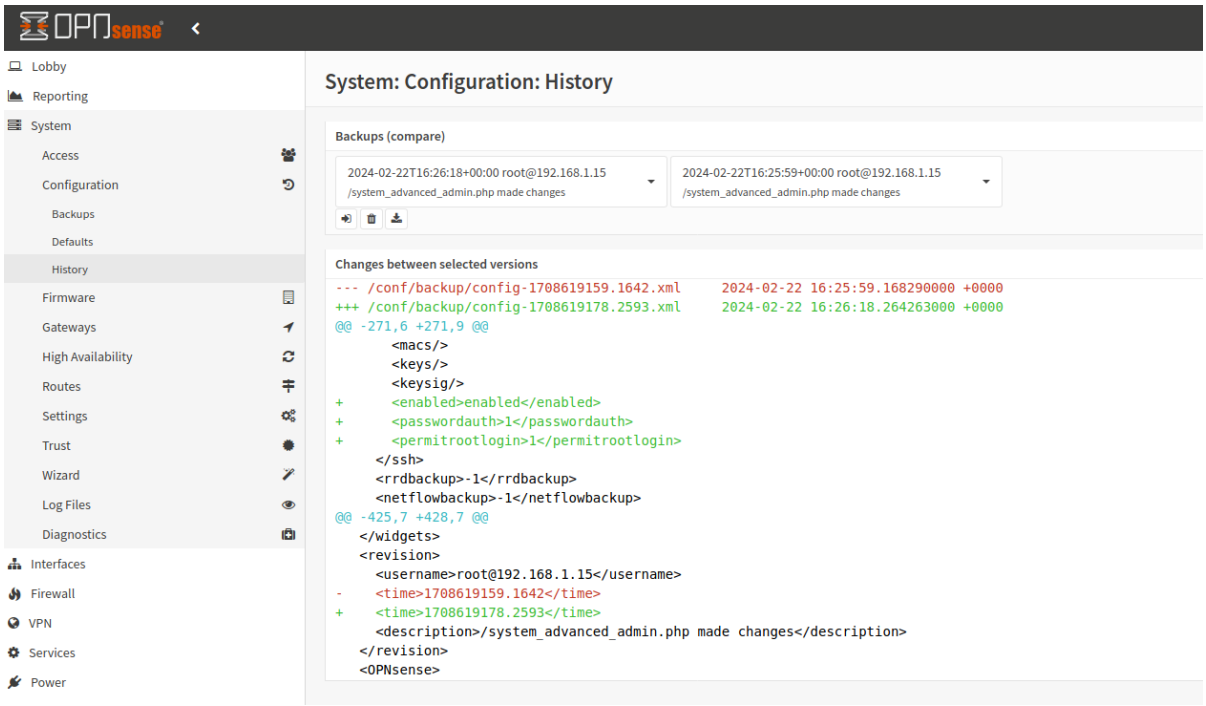


Figure 3 TOE configuration diff

This section is included in the document to be in compliance with the **AUD.2** requirement. Therefore, the type of event information of the audit records related to the following events shall be consulted as indicated in this section:

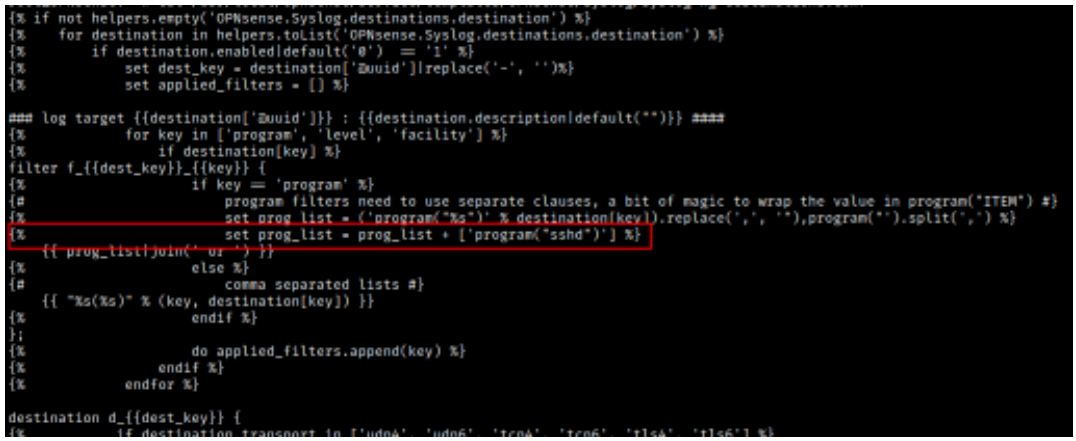
- Configuration of the session termination when inactivity is detected.
- Changes in user credentials.
- Delete user groups.
- Associate permissions to groups or users.
- Load SSL certificate for GUI.
- Enabling to connect to the TOE by SSH.
- Allowing the root user to connect by SSH.
- Create, modify or delete Firewall rules.

It is important to notice that this functionality is comparing system backups, no logs or audit data. When the TOE sends its audit data to a syslog server, it will send the log that states that the TOE configuration has changed or that a firewall rule has changed, but the information of what has changed is detailed in this functionality that compares backups (these backups are automatically generated every time the TOE configuration is changed or a firewall rule is changed, created or deleted).

2.3.10Syslog configuration

By default, all the audit records are not sent to the Syslog server. Therefore, the following configuration shall be performed:

- Edit the file */usr/local/opnsense/service/templates/OPNsense/Syslog/syslog-ng-destinations.conf* adding the following line: `{% set prog_list = prog_list + ['program("sshd")'] %}`



- Save the file.
- Restart the *syslog-ng* service.

2.3.11ACL configuration

By default, the TOE allows to assign view audit logs permission to users. However, this permission also allows user to remove audit logs. In order to prevent that the users (other than the root user) from deleting the audit logs, the following configuration shall be followed.

A new ACL shall be created to assign log view-only permissions to non-root users:

1) Create a new directory that will store the new ACL by executing this command in CLI interface:
   `mkdir -p /usr/local/opnsense/mvc/app/models/security/security/ACL`
2) Copy the following code lines into an XML file called “ACL.xml” and store it in the previously created directory:

```
<acl>
    <page-diagnostics-logs-read-only>
        <name>read only logs</name>
        <patterns>
            <!-- System: Log Files: Backend -->
            <pattern>ui/diagnostics/log/core/configd</pattern>
            <pattern>api/diagnostics/log/core/configd</pattern>
            <pattern>api/diagnostics/log/core/configd/export*</pattern>
            <!-- System: Log Files: Audit -->
            <pattern>ui/diagnostics/log/core/audit</pattern>
            <pattern>api/diagnostics/log/core/audit</pattern>
            <pattern>api/diagnostics/log/core/audit/export*</pattern>
            <!-- System: Log Files: Boot -->
            <pattern>ui/diagnostics/log/core/boot</pattern>
            <pattern>api/diagnostics/log/core/boot</pattern>
            <pattern>api/diagnostics/log/core/boot/export*</pattern>
            <!-- System: Log Files: General -->
            <pattern>ui/diagnostics/log/core/system</pattern>
            <pattern>api/diagnostics/log/core/system</pattern>
            <pattern>api/diagnostics/log/core/system/export*</pattern>
            <!-- System: Log Files: Web GUI -->
            <pattern>ui/diagnostics/log/core/lighttpd</pattern>
            <pattern>api/diagnostics/log/core/lighttpd</pattern>
```

<pattern>api/diagnostics/log/core/lighttpd/export</pattern>*
<!-- Firewall: Log Files: General -->
<pattern>ui/diagnostics/log/core/firewall</pattern>
<pattern>api/diagnostics/log/core/firewall</pattern>
<pattern>api/diagnostics/log/core/firewall/export</pattern>*
<!-- Firewall: Log Files: Live View -->
<pattern>ui/diagnostics/firewall/log</pattern>
<pattern>api/diagnostics/firewall/log/</pattern>*
<!-- Firewall: Log Files: Overview -->
<pattern>ui/diagnostics/firewall/stats</pattern>
<pattern>api/diagnostics/firewall/stats</pattern>*
<!-- Firewall: Log Files: Plain View -->
<pattern>ui/diagnostics/log/core/filter</pattern>
<pattern>api/diagnostics/log/core/filter</pattern>
<pattern>api/diagnostics/log/core/filter/export</pattern>*
</patterns>
</page-diagnostics-logs-read-only>
</acl>

3) Clear the cache to prevent old ACL's still being used with the following command:
`rm /tmp/opnsense_acl_cache.json`

With this configuration, a new permission called "read only logs" will be available. This permission will be assigned by the root to users which will be able to view audit logs.

Therefore, the only one who can delete the logs will be the root user who has been assigned the `/allpages` permission, which grants the possibility of executing all the TOE functionalities.

2.3.12Configd configuration

The following configuration must be performed in order to do not allow non-wheel group users to interact with configd functionality:

1) Create a new directory that will store the new configuration to allow only the wheel group users to interact with configd functionality:
`mkdir /usr/local/opnsense/service/conf/configd.conf.d`
2) Copy the following code lines into a file called "lockdown.conf" and store it in the previously created directory:
[actions_defaults]
allowed_groups = wheel
3) Restart the configd service in order to apply the changes:
`service configd restart`

2.3.13System Back-ups

It is necessary to define in System>Configuration>Backups a number of **5** Backup Count or higher. In this way, the TOE will generate a configuration backup every time the configuration changes or firewall rule is created, modified or deleted.

In this way, the TOE stores its last 5 configurations, establishing a rotation policy following the oldest criteria.

***Note**: Through these configurations, it is possible to see in detail the TOE configuration changes or Firewall rules changes.*

2.3.14SSH root login disabling

It is necessary to disable the *root* access to the CLI interface through SSH, only allowing local access to the *root* user via the CLI interface. Access *System > Settings > Administration > Secure Shell* in GUI interface and uncheck the option "*Permit Root Login*".

3 Operational environment

3.1 Operational environment description

The following diagram shows the operational environment where the TOE is typically deployed:

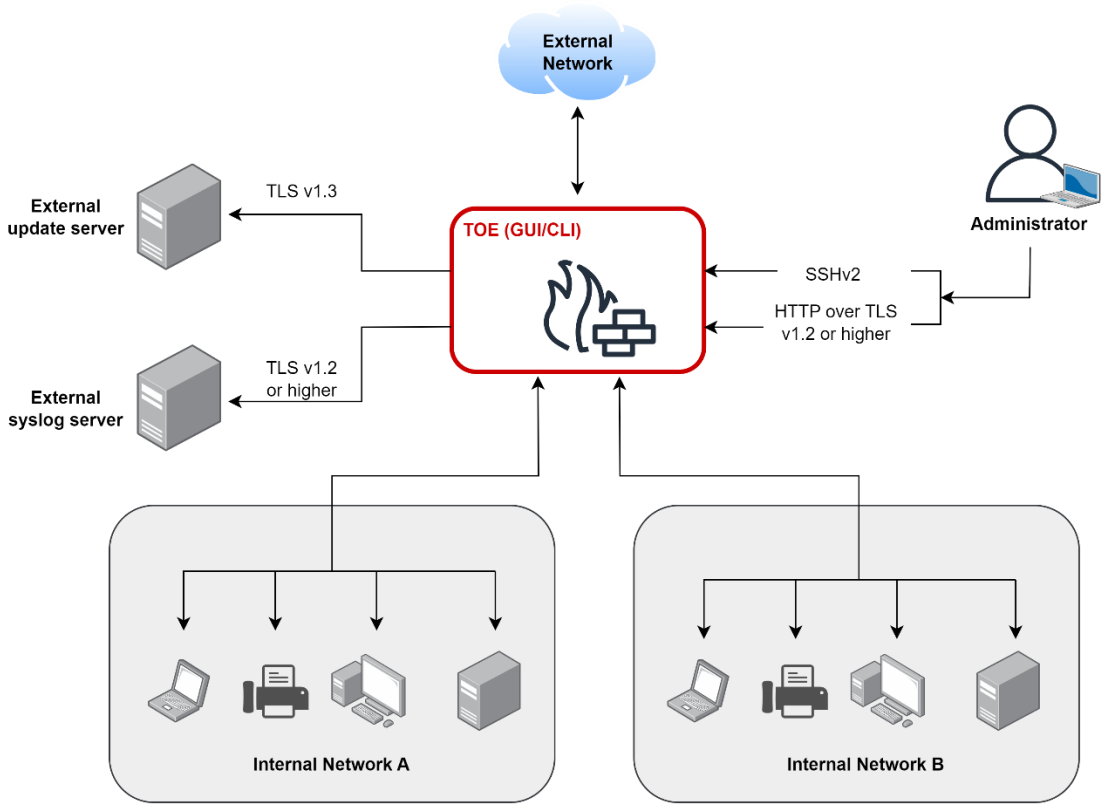


Figure 4 TOE operational environment

The main entities that compose the operational environment are described below:

- **Administrator**: The Administrator user has the permissions to configure and manage the TOE. In order to access the GUI and CLI interfaces, the administrator's PC requires a web browser and a command prompt respectively.
- **Internal Network**: This network contains several connected devices, such as computers, servers and other devices. The TOE protects this network by filtering the incoming and outgoing traffic.
- **External network**: The set of networks and devices that communicate with the internal network in both directions (ingoing and outgoing). The incoming and outgoing traffic to the internal networks is filtered by the TOE.
- **External syslog server**: This server receives and stores the log files generated by the TOE.
- **External update server**: This server is listening for petitions from the TOE for updating purposes (requests to know if new updates are available, updates delivery…).

Hardware requirements

To install the TOE the virtual machine should have the following hardware prerequisites:

- Minimum required RAM is 1GB
- Minimum recommended virtual disk size of 8 GB.

4 Security Problem Definition

4.1 Operational Environment Assumptions

Assumption	Description
A.PHYSICAL PROTECTION	The product shall be physically protected by its environment and not subject to physical attacks that could compromise its security or interfere with its proper operation.
A.LIMITED FUNCTIONALITY	The product shall only provide network access control functionality as its primary function and shall not provide any other functionality or service.
A.TRUSTED ADMINISTRATOR	Administrators shall be members of the organization who are fully trusted and have the best security interests for the organization. They shall be properly trained and shall be free of any malicious intent or conflict of interest in managing the product.
A.PERIODIC UPDATES	The software of the product is updated when new updates that fix known vulnerabilities appear.
A. PROTECTION OF THE CREDENTIALS	All credentials, especially the administrator's, must be properly protected by the organization using the product be properly protected by the organization.

4.2 Assets to protect

This section describes the assets that the TOE's security features protect.

Asset	Description	Security Dimensions
AS.ADMINISTRATION	Product management interfaces and the information transmitted through them, in both directions.	Confidentiality, Traceability, Authenticity and Integrity.
AS.PSS	Configuration data and audit records from the TOE.	Integrity.
AS.PSC	Credentials and private keys.	Confidentiality and Integrity.
AS.UPDATES	Updates that may affect TOE's configuration and functionality.	Integrity and Authenticity.
AS.COMMUNICATIONS	TOE's communications, established between its own components and with its operational environment.	Confidentiality, Integrity and Authenticity.

4.3 Threat descriptions

Threat	Description	Assets
T.NOAUT - UNAUTHORIZED ADMINISTRATOR ACCESS	An attacker can gain access as a product administrator by one of the following scenarios: • Impersonating as an administrator to the product. • Impersonating as the product to an administrator. • Replaying an administration session. • Performing man-in-the-middle attacks.	*AS.ADMINISTRATION* *AS.PSS*
T.CRYPTO - WEAK CRYPTOGRAPHIC MECHANISMS	Use of cryptographic mechanisms or weak key lengths in the product that allow an attacker to compromise it, primarily through brute force attacks.	*AS.PSC* *AS.COMMUNICATIONS* *AS.UPDATES* *AS.ADMINISTRATION*
T.COM - UNAUTHORIZED COMMUNICATION PROTOCOLS	Use of unauthorized protocols that allow an attacker to compromise the integrity and confidentiality of critical product communications.	*AS.COMMUNICATIONS* *AS.ADMINISTRATION*
T.ACT - MALICIOUS UPDATE	An attacker can perform a malicious update that weakens the product's security features.	*AS.UPDATES*
T.AUD - UNDETECTED ACTIVITIES	An attacker may attempt to access, change or modify the product's security functionality without the administrator's knowledge.	*AS.ADMINISTRATION* *AS.PSS*
T.PSC - COMPROMISE OF CRITICAL SECURITY PARAMETERS	An attacker can compromise critical security parameters and continuously access the product and its critical data.	*AS.PSC*
T.NOAUTUSR - UNAUTHORIZED USER ACCESS	An attacker can gain unauthorized access by one of the following scenarios: • Impersonating a user to the product. • Impersonating the product to a user. • Replaying a user session. • Performing man-in-the-middle attacks.	*AS.ADMINISTRATION* *AS.PSS*
T.CRE - COMPROMISE OF CREDENTIALS	An attacker can exploit the use of weak or unprotected credentials to gain privileged access to the product.	*AS.PSC*
T.NET - NETWORK ATTACK	An attacker gains access to the network by mapping the machines residing on it and obtaining IP address data, services or any other	*AS.COMMUNICATIONS*

	information that allows him to launch attacks on those machines and services.	

4.3.1 Traceability threats/security requirements

The following table maps the Fundamental Security Requirements defined in section *5: Security Functional Requirements* that address the defined threats:

	T.NOAUT	T. CRYPTO	T.COM	T.ACT	T.AUD	T.PSC	T.NOAUTUSR	T.CRE	T.NET
ADM.1	X								
ADM.2	X								
ADM.3	X								
IAU.1	X						X		
IAU.2								X	
IAU.3								X	
IAU.4	X								
COM.1		X	X						
COM.2			X						
COM.3	X	X	X				X		
COM.4	X	X	X				X		
CIF.1	X	X	X	X			X		
ACT.1				X					
ACT.2		X		X					
ACT.3	X			X					
AUD.1					X				
AUD.2					X				

	T.NOAUT	T. CRYPTO	T.COM	T.ACT	T.AUD	T.PSC	T.NOAUTUSR	T.CRE	T.NET
AUD.3					X				
AUD.4		X	X		X				
AUD.5					X				
PSC.1						X			
FWL.1									X
FWL.2									X
FWL.3									X
FWL.4									X

5 Security Functional Requirements

5.1 SF. Trusted Administration

Requirement	Description
ADM.1	The TOE define a default root user and provide the ability to create new users or groups of users. The TOE also allows modifying the privileges assigned to a given user or group of users.

ADM.2	The TOE shall allow the authorized users to perform the following functionalities remotely:
	• Configuration of the session termination when inactivity is detected.
	• Configuration of the TOE:
	  ○ Update the TOE.
	  ○ Create, modify and delete users.
	  ○ Create, modify and delete user groups.
	  ○ Associate permissions to groups or users.
	  ○ Load SSL certificate for GUI.
	  ○ Enabling to connect to the TOE by SSH.
	  ○ Allowing the root user to connect by SSH.
	• Functionalities of the TOE:
	  ○ Create, modify or delete Firewall rules.
	  ○ Change the order of existing Firewall rules.

ADM.3	The TOE shall ensure only specific entities are capable of perform the **ADM.2** functions:
	• Root user.
	• Another user/group with the specific permissions:
	  ○ Update the TOE: "System: Firmware"
	  ○ Create, modify and delete users: "System: User Manager"
	  ○ Create, modify and delete user groups: "System: Group Manager"
	  ○ Associate permissions to groups or users: "System: Group Manager: Add Privileges" | "System: User Manager: Add Privileges"
	  ○ Load SSL certificate for GUI: "System Advanced: Admin Access Page"
	  ○ Enabling to connect to the TOE by SSH: "System: Advanced: Admin Access Page"
	  ○ Allowing the root user to connect by SSH: "System: Advanced: Admin Access Page"
	  ○ Create, modify or delete Firewall rules: "Firewall: Rules: Edit" and "Firewall: Rules"
	  ○ Change the order of existing Firewall rules: "Firewall: Rules"
	  ○ Configuration of the session termination when inactivity is detected: "System: Advanced: Admin Access Page".
	• Also, with the permission *"All pages"*, the user could have all the permissions to all the previously defined administrable functions.

5.2 SF. Identification and Authentication

Requirement	Description
IAU.1	The TOE shall identify and authenticate every user through username and password before grating access to the GUI and CLI interfaces.
IAU.2	The TOE shall implement a 2FA mechanism to protect against authentication brute-force attacks.
IAU.3	The password policy of the TOE shall be as follows: • The password shall be configurable with a minimum or equal length of 12 characters. • The password shall be able to be composed of 3 of the following 4 parameters: ○ Lowercase letters ○ Uppercase letters ○ Numbers ○ Special characters "!", "@", "#", "$", "%", "^", "&", "*", "(", ")".
IAU.4	The TOE shall close a user session established through CLI and GUI interfaces after 5 minutes of inactivity.

5.3 SF. Trusted Communication Channels

The ciphersuites listed in this section include the (R) nomenclature, that refers to the recommended cryptographic algorithms that are considered secure and suitable in the context of HIGH ENS Category.

Requirement	Description
COM.1	The TOE shall establish secure channels when exchanging sensitive information with authorized entities: • The TOE with an external syslog server using TLS v1.2 or higher, with ECDHE key exchange method, with 25519 (R), secp256r1 (R), 448 (R), secp521r1 (R) and secp384r1 (R) curves and the following cipher suites: ○ *TLS_AES_256_GCM_SHA384 (R)* ○ *TLS_AES_128_GCM_SHA256 (R)* ○ *TLS_CHACHA20_POLY1305_SHA256 (R)* ○ *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R)* ○ *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R)* ○ *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (R)* ○ *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (R)* ○ *TLS_ECDHE_ECDSA_WITH_AES_256_CCM (R)* ○ *TLS_ECDHE_ECDSA_WITH_AES_128_CCM (R)* • The TOE with the update server using TLS v1.3, with ECDHE key exchange method, with 25519 (R), secp256r1 (R), 448 (R), secp521r1 (R) and secp384r1 (R) curves and the following cipher suites: ○ *TLS_AES_256_GCM_SHA384 (R)* ○ *TLS_CHACHA20_POLY1305_SHA256 (R)* ○ *TLS_AES_128_GCM_SHA256 (R)*
COM.2	The TOE shall allow secure communications channels to be initiated by itself or by authorized entities. These secure communication channels are the following: 1. **Communication between the TOE and the external syslog server** through TLS v1.2 or higher, initialized by the TOE. 2. **Communication between the TOE and the update server** through TLS v1.3, initialized by the TOE.
COM.3	The TOE shall use digital certificates RSA-3072 or higher when the users use the HTTPS protocol to access the TOE's web interface.
COM.4	The TOE shall establish secure communication channels when exchanging information with the authorized user, using algorithms accepted according to the ENS MEDIUM category of the CCN-STIC-807 guide: • The Administrator with the TOE via the GUI interface through HTTPS (over TLS v1.2 or higher), with ECDHE key exchange method, with 25519 (R), secp256r1 (R), 448 (R), secp521r1 (R) and secp384r1 (R) curves and the following cipher suites:

	○ *TLS_AES_128_GCM_SHA256 (R)* ○ *TLS_AES_256_GCM_SHA384 (R)* ○ *TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (R)* ○ *TLS_CHACHA20_POLY1305_SHA256 (R)* ○ *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R)* ○ *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R)* • The Administrator with the TOE via the CLI interface through SSHv2 using: • **SSH Key Exchange Method** ○ diffie-hellman-group16-sha512 *(R)* ○ diffie-hellman-group18-sha512 *(R)* ○ ecdh-sha2-nistp256 *(R)* ○ ecdh-sha2-nistp384 *(R)* ○ ecdh-sha2-nistp521 *(R)* • **SSH Encryption Algorithms** ○ aes128-ctr *(R)* ○ aes192-ctr *(R)* ○ aes256-ctr *(R)* • **SSH Public Key Algorithm** ○ ecdsa-sha2-nistp256 *(R)* • **SSH MAC Algorithm** ○ hmac-sha2-256 *(R)* ○ hmac-sha2-512 *(R)*

5.4 SF. Cryptography

Requirement	Description
CIF.1	The TOE shall use the following cryptographic mechanisms in compliance in accordance with the provisions of guide ENS MEDIUM CCN-STIC-807: • Cipher suites of the communication channels defined in **COM.1** and **COM.4**. • The certificates as specified in **COM.3**. • The cryptographic algorithm for software updates integrity, as defined in **ACT.2**.

5.5 SF. Trusted Installation and Updates

The padding mention in this section include the Legacy (L) nomenclature which refers to the cryptographic algorithms, in the context of MEDIUM ENS Category, that are considered with acceptable security in the short term, valid until 2025.

Requirement	Description
ACT.1	The TOE shall provide the ability to query the current software version through the *System* → *Firmware* menu of the GUI interface, initiate updates manually and check for new updates available.
ACT.2	The TOE shall use RSA-4096 digital signatures with RSASSA-PKCS#1 (L) padding and SHA-256 hashing to authenticate software updates before installation.
ACT.3	Software update shall be allowed only to the followings users/group of users: • Root user. • Another user/group of users with *"System: Firmware"* permission.

5.6 SF. Audit

Requirement	Description

AUD.1	The TOE shall generate audit records when any of the following events occur:
	• Login and logout of the remote users.
	• Changes in user credentials.
	• Changes in TOE configurations and functionalities:
	  ○ Configuration of the session termination when inactivity is detected.
	  ○ Update the TOE.
	  ○ Create, modify and delete users.
	  ○ Create, modify and delete user groups.
	  ○ Associate permissions to groups or users.
	  ○ Load SSL certificate for GUI.
	  ○ Enabling to connect to the TOE by SSH.
	  ○ Allowing the root user to connect by SSH.
	  ○ Create, modify or delete Firewall rules.
	• Events related with TOE functionality when a rule is applied to incoming or outcoming traffic is allowed, blocked or rejected.

AUD.2	Audit records shall contain at least the following information: • Date and time of the event. • Type of identified event (as section 2.3.9 states). • Result of the event. • User producing the event (if applicable).

AUD.3	The following access policy shall apply to audit records:
	• **Read:**
	  ○ root user,
	  ○ Users or group of users with *"read only logs"* permission
	• **Modify**: Root user, only locally by CLI interface.
	• **Delete**: Root user, locally by CLI interface or remotely by GUI interface.

AUD.4	The TOE shall be able to store the generated audit information in itself and transmit the generated audit information to an external Syslog server using a secure TLS v1.2 or higher channel described in **COM.1**.
AUD.5	The TOE shall implement a rotation mechanism based on two main configurations: ▪ 'preservelogs': Determines the number of logs to be kept before deletion. ▪ 'maxfilessize': Sets a limit on the maximum size allowed for each log file. If a log file exceeds the 'maxfilesize' limit, an early log rotation will be forced, preserving the integrity of the logs without compromising the available storage space.

5.7 SF. Protection of Credentials and Sensitive Data

Requirement	Description
PSC.1	The TOE shall ensure that the specific directory where are stored credentials (login passwords) and private keys has read/write permissions only for the root user and read permissions for the administrator users included in *wheel* user group by a previously defined control access.

5.8 SF. Firewalls

Requirement	Description
FWL.1	The TOE shall allow the definition of stateful traffic filtering rules using the following settings: • Source and destination address. • Source and destination ports. • Type. • Interface.
FWL.2	The TOE shall have the ability to process and inspect packets from the following network protocols: ICMPv4, ICMPv6, IPv4, IPv6, TCP, UDP in a way that allows: 1. Define packet filtering rules based on the settings defined in **FWL.1.** 2. Use the following basic filtering operations: pass, block, and reject. Also allowing to save the operation performed in the activity log. 3. Assign rules in a specific order to network interfaces of the TOE, defined by an authorized user.
FWL.3	The TOE shall drop traffic if no rule applies. This behaviour is set by default.
FWL.4	The TOE shall consider that a session between devices connected to the TOE has been terminated when there is inactivity in the session for specific time depending on the protocol: • TCP connection: When a TCP connection is established the TOE uses a state timeout value of 86400 seconds. • UDP connection: When UDP packets are transmitted, the TOE generates a session with a timeout of 60 seconds. The subsequent UDP packets transmitted before the timeout value expires refresh the initial value to 30 seconds.

6 Acronyms

The following table shows the acronyms used in this document.

Acronym	Meaning
CCN	Centro Criptológico Nacional (National Cryptologic Centre).
CNI	Centro Nacional de Inteligencia (Spanish National Intelligence Centre).
ENS	Esquema Nacional de Seguridad (National Security Scheme).
LINCE	Certificación Nacional Esencial de Seguridad
MCF	Módulo Revisión de Código Fuente
MEB	Módulo de Evaluación Biométrica
MEC	Módulo de Evaluación Criptográfica
ST	Security Target – Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y la Comunicación (Security of Information and Communication Technologies).
TICs	Tecnologías de la Información y la Comunicación (Information and Communication Technologies).
TOE	Target Of Evaluation - Objeto a evaluar.
SSH	Secure Shell
HTTPS	Hypertext Transfer Protocol Secure
CLI	Command Line Interface
TLS	Transport Layer Security
CPU	Central Processing Unit
RAM	Random Access Memory
SSD	Solid State Drive
UFS	Universal Flash Storage
GUI	Graphical User Interface
AES	Advanced Encryption Standard
RSA	Rivest, Shamir y Adleman
SHA	Secure Hash Algorithm
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

ICMP	Internet Control Message Protocol
IP	Internet Protocol
ACL	Access Control List

Table 1 *Abbreviations*

7 Document references

The following table shows the documents referenced in this document.

Reference	Document
CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Evaluation Methodology for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Security Target template for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-2004	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Evaluation Technical Report template for National Essential Security Certification, March 2022 version 2.0).
CCN-STIC-807	Criptología de empleo en el Esquema Nacional de Seguridad, mayo 2022 (National Security Scheme employment cryptology, May 2022).

Table 2 List of document references

8 Annex

8.1 Third party libraries used by the TOE

Library Name	Version	Vendor
ca_root_nss	3.93	Mozilla
cyrus-sasl	2.1.28	Cyrus team, Carnegie Mellon University
cyrus-sasl-gssapi	2.1.28_1	Cyrus team, Carnegie Mellon University
suricata	6.0.15	Open Information Security Foundation (OISF)
easy-rsa	3.1.7	OpenVPN Technologies Inc
openssl	1.1.1w	The OpenSSL Project
py39-openssl	23.2.0,1	The OpenSSL Project
libnet	1.3,1	The libnet Developer Community
syslog-ng	4.4.0	Balabit
openvpn	2.6.8_1	OpenVPN Technologies Inc
openssh-portable	9.3.p1_1,1	The OpenSSH Project
strongswan	5.9.13	The strongSwan Team
squid	6.6	The Squid Team