jtsec
BEYOND IT SECURITY

STIC Evaluation Technical Report

STIC_OPNSENSE_IAD-2504 (CUA-2023-118)

1.0

2025/05/16

CHANGELOG

Version	Date	Author	Reason	Changes
1.0	2025/05/16	AGL	Document Creation	First version

INDEX

1 INTRODUCTION

This document is the Information and Communications Technology Security (STIC) Evaluation Technical Report (ETR) for the TOE OPNsense Business Edition according to the method described in [CCN-STIC-2001] and [CCN-STIC-2002]. The results only affect the tested TOE, so they may not be representative of other manufacturer developments.

1.1 EVALUATION TECHNICAL REPORT INFORMATION

ETR reference	STIC_OPNSENSE_IAD-2504-ETR-v1.0
ETR version	1.0
Author or authors	AGL
Reviewer	DAT
Approved by	JTG
Start date of the works	2025/04/22
End date of the works	2025/05/16
CB dossier code	CUA-2023-118
Laboratory project code	STIC_OPNSENSE_IAD-2504
Type of evaluation	Complementary STIC
Product Taxonomy	N/A
Evaluation Laboratory holding the accreditation	jtsec Beyond IT Security SLU (ESB93551422)
Laboratory address	Avenida de la Constitución 20 Oficina 208. CP 18012 Granada, España.
Address where the work is done	Avenida de la Constitución 20 Oficina 208. CP 18012 Granada, España.

1.2 TOE DEVELOPER INFORMATION

Applicant data	Deciso B.V.
Applicant's contact information	Ad Schellevis +31(0)187744020 a.a.schellevis@deciso.com Edison 43, 3241 LS Middelharnis, The Netherlands.
Developer data	Deciso B.V.
TOE name	OPNsense Business Edition
TOE version	25.4
Operating manuals of the product	[TOE-DOCS-7AC0BF1]

2 TOE DESCRIPTION

The information in this section is provided by the manufacturer online or in its delivered evidence.

2.1 FUNCTIONAL DESCRIPTION OF THE TOE

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.

2.2 INVENTORY OF SECURITY FUNCTIONS

This evaluation uses as its baseline the complementary STIC evaluation previously conducted for the same TOE, OPNsense Business Edition. The STIC evaluation is referenced by qualification dossier CUA-2023-118.

The requirements to be tested are associated with test cases that resulted in FAIL verdicts during the prior STIC evaluation. Additionally, as required in the previous evaluation, testing of the requirements (FCS_CKM.4.1, FCS_RBG_EXT.1.1, FCS_RBG_EXT.1.2) from the Collaborative Protection Profile for Network Devices [cPP-ND-30e] will be performed. The supporting document associated with this protection profile ([cPP-ND-30e-SD]) will be followed by the evaluator when conducting the tests, although it will not be followed strictly but rather as a guide to orientate the tests.

The following table includes the Security Functions that will be retested in this evaluation:

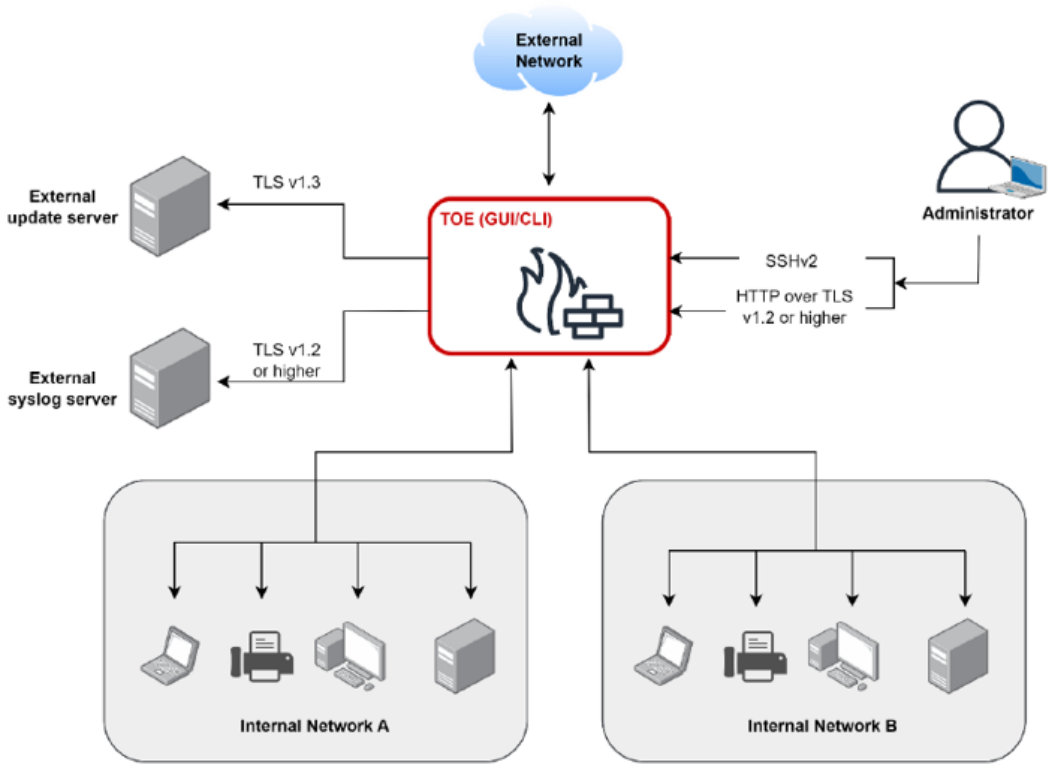
Security Function	Test Code	Brief description
FFW_RUL_EXT.1.6	[STIC_OPNSENSE_IAD-2504-TST-0010]	The firewall functionality of the TOE will be tested to ensure it drops and logs IPv4 network packets with invalid source or destination addresses, such as unspecified addresses or addresses reserved for future use.
FFW_RUL_EXT.1.6	[STIC_OPNSENSE_IAD-2504-TST-0020]	The firewall functionality of the TOE will be tested to ensure it drops and logs IPv6 network packets with invalid source or destination addresses, such as unspecified addresses or addresses reserved for future use.
FCS_CKM.4.1	[STIC_OPNSENSE_IAD-2504-TST-0030]	The cryptographic key destruction functionality of the TOE will be tested to ensure it destroys cryptographic keys in accordance with a specified

		cryptographic key destruction method.
FCS_RBG_EXT.1.1 FCS_RBG_EXT.1.2	[STIC_OPNSENSE_IAD-2504-TST-0040]	The random bit generation functionality of the TOE will be tested in order to verify that comply with ISO/IEC 18031:2011.

3 OPERATIONAL ENVIRONMENT

3.1 DESCRIPTION OF THE OPERATIONAL ENVIRONMENT

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



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.

3.2 OPERATIONAL ENVIRONMENT ASSUMPTIONS

This section contains the assumptions presented by the manufacturer in the latest version of his Security Target. They are described below:

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 EXECUTIVE SUMMARY OF THE EVALUATION

This assessment is a STIC evaluation of the OPNsense Business Edition. First, an Impact Analysis Report was conducted to analyse the changelogs from version 24.10.1 to version 25.4 of the TOE to identify newly added functionality, as well as existing and fixed functionality. The results of the analysis are recorded in [IAR-10].

This evaluation dismisses the analysis of the Security Target, as this STIC evaluation does not involves its own Security Target, and the sections related to such tasks are not included in the present report.

Concerning this evaluation, the installation of the TOE was carried out following the guides and the documentation of the product. The installation was straightforward and flawless; therefore, no non-conformities were generated through this phase of the evaluation.

Once the TOE was installed, the evaluator proceeded with functional testing. The functional tests conducted are specifically related to the firewall logging capabilities. This was a previously evaluated requirement (FFW_RUL_EXT.1.6) and had been identified as an issue in a prior evaluation; therefore, the corresponding tests were performed.

Additionally, following the guidelines from CPSTIC provided in the previous evaluation, the testing of the requirements (FCS_CKM.4.1, FCS_RBG_EXT.1.1, FCS_RBG_EXT.1.2) from the Collaborative Protection Profile for Network Devices [cPP-ND-30e] is performed in the current evaluation. The analysis and results of these requirements are summarized in [STIC_OPNSENSE_IAD-2504-TST-0030] and [STIC_OPNSENSE_IAD-2504-TST-0040] functional tests.

As a result of the execution of the functional tests documented in section *13 Annex B: Functional test plan and report*, no non-conformities were generated through this phase of the evaluation.

Following the completion of the functional tests, the next step was to perform the analysis of the TOE's vulnerabilities. This phase mainly involves the review of public vulnerabilities related to the TOE and its third-party libraries or components. Some CVEs were identified as applicable but after further analysis and some testing these were deemed not exploitable, mainly because the affected code of the third-party libraries was not being used by the TOE. This analysis does not reveal public vulnerabilities (CVE) that could affect the TOE at the date this report is developed. In addition, an analysis was conducted to identify vulnerabilities applicable to each OWASP Top 10 category for the TOE web interface.

It is worth noting that vulnerability analysis has been focused on new functionality or previously tested functionality that may have been implicitly affected by changes in the TOE, given that OPNsense is a product that is under continuous qualification and runs several evaluations through the year it is considered that it is not required to examine thoroughly the functionality regarding completeness.

Afterwards, the penetration tests were carried out in order to identify and exploit potential vulnerabilities in the TOE. The set of penetration tests can be found in *Annex D: Penetration test plan and report*.

The execution of the penetration tests did not reveal any issue.

Since there are not OPEN non-conformities, the laboratory determines that the verdict is **PASS**.

5 VERDICT OF THE EVALUATION

After analyzing the results of the evaluation, the laboratory determines that the verdict is **PASS**.

No non-conformities were reported during the evaluation.

6 TOE INSTALLATION AND REVIEW OF THE INSTALLATION, CONFIGURATION AND OPERATION GUIDES

Documents used during installation	[TOE-DOCS-7AC0BF1]
Evaluator	AGL
Days required	1
Date	2025/05/16
Results of the evaluator's work	**PASS**

6.1 EVALUATION ACTIVITIES

This section contains the evaluation activities defined in section 4.2 of [CCN-STIC-2002] as well as a brief description of the result of these tasks on the TOE and its documentation.

TE.2.1. Verify that the applicant has provided the required test platform to perform the tests on the product.

PASS The manufacturer has provided the evaluator with the platform required for testing, as well as the necessary documentation to make use of it within the conditions of the evaluation.

TE.2.2. Check that the installation and operation guides describe the roles and privileges for the different user roles defined in the TOE that allow the TOE to be installed and operated in a secure manner.

PASS The guides provided by the manufacturer clearly describe the roles and privileges of the various TOE users that allow the TOE to be installed and operated safely.

TE.2.3. Check that, according to the product installation or configuration guides, it is possible to install the product according to the configuration(s) described in the ~~Security Target~~.

- **In the case of products that can be installed on several operating system versions, the operating system used and its version must be indicated as precisely as possible (patch, service pack, etc.).**
- **If the product allows several mounting/configuration (set-up) modes, the guides must clearly indicate which mode is evaluated. ~~The identification of this mode shall be indicated in the Security Target.~~**
- **If the product supports different settings in its configuration, the guides must clearly differentiate between those that are part of the scope of the evaluation and those that are not.**

- **If the product requires installation, the product shall be installed in the configuration specified in the installation guide. Additionally, the applicant shall provide documentation related to the different configuration modes existing in the product.**

PASS The evaluator has been able to install the product exclusively following the contents of the manufacturer's documentation, provided through [TOE-DOCS-7AC0BF1].

TE.2.4. Check that the version of the TOE installed corresponds to the one declared in the ~~Security Target~~ and that the guides describe the TOE identification procedure to the TOE consumers.

PASS The evaluator has followed the guidelines provided by the manufacturer and has been able to correctly verify that the version of the TOE installed corresponds to the version subject to the current evaluation as can be seen in *6.4 Verification of the installed TOE version.*

TE.2.5. The evaluator shall register the relevant information to successfully install the TOE.

PASS The information necessary to carry out the complete installation of the product, under the same conditions as those used for this evaluation, can be found in the sections *6.2 Detailed configuration of the operational environment* and *6.3 Description of the installation and configuration of the TOE*.

TE.2.6. The evaluator shall register all system's configuration specific data when appropriate.

PASS/ The specific data used during the TOE preparation and configuration process is reflected in the *6.5 Used installation options*.

TE.2.7. The evaluator shall register every non-conformity in regards to the installation and configuration of the TOE or the test environment.

PASS No non-conformities were found regarding the installation process of the TOE and its documentation. The results are summarized in the section 6.6 Results.

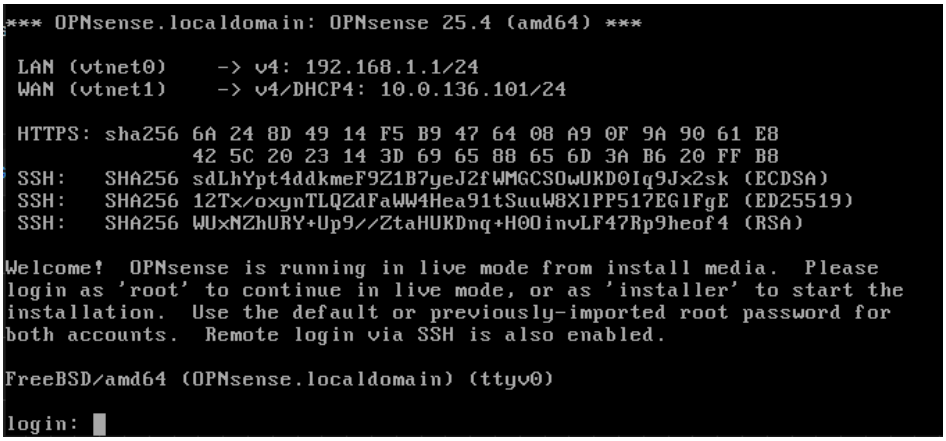
6.2 DETAILED CONFIGURATION OF THE OPERATIONAL ENVIRONMENT

The test scenarios are described in section *12 Annex A: Test scenarios.*

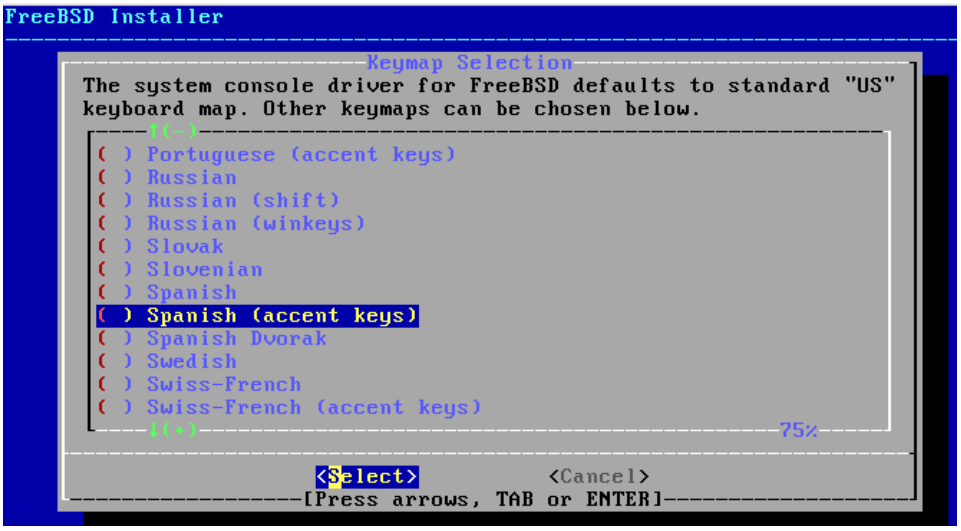
6.3 DESCRIPTION OF THE INSTALLATION AND CONFIGURATION OF THE TOE

Before starting the installation steps for [TOE-254], a virtual machine with [TOE-ISO-254] is required, and it must meet the minimum hardware requirements (1 GB RAM and 8 GB disk space). The following steps are followed to install [TOE-254]:

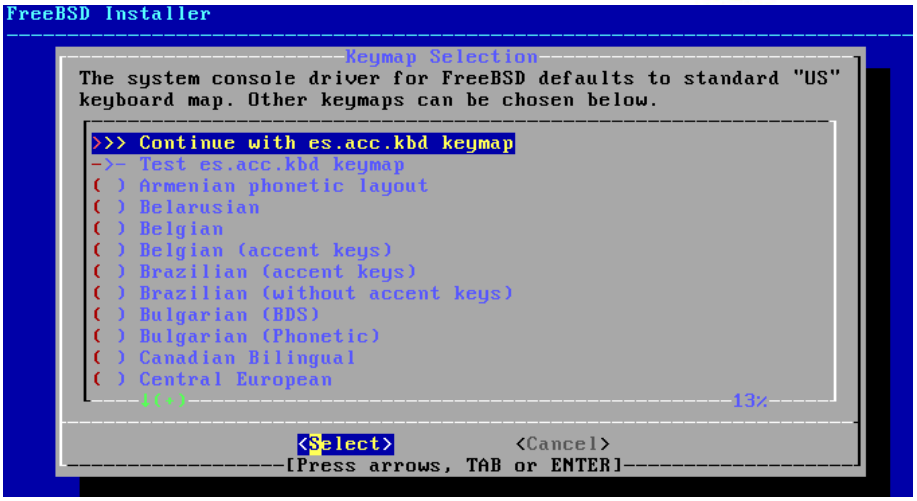
1. Start the virtual machine.
2. Wait for [TOE-254] to boot up.
3. Log in with the user “installer” and authenticate with the password “opnsense”:



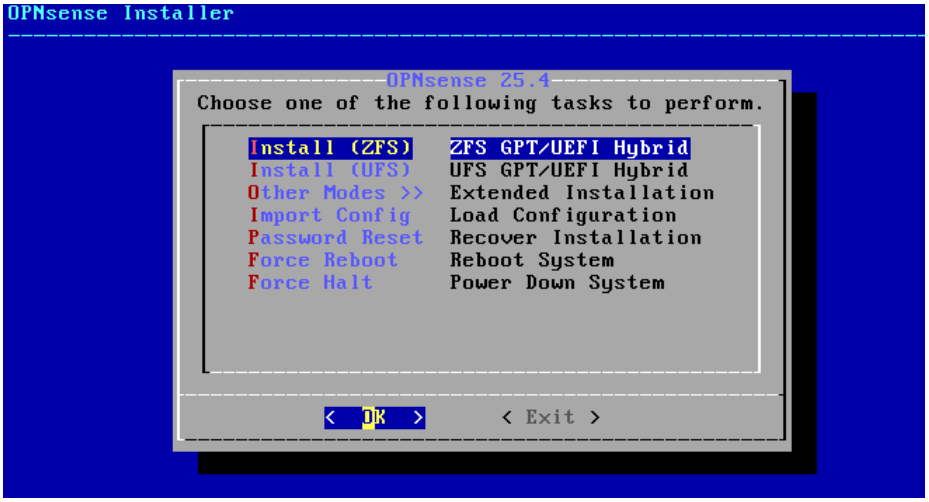
4. Select the keyboard layout and press Enter:



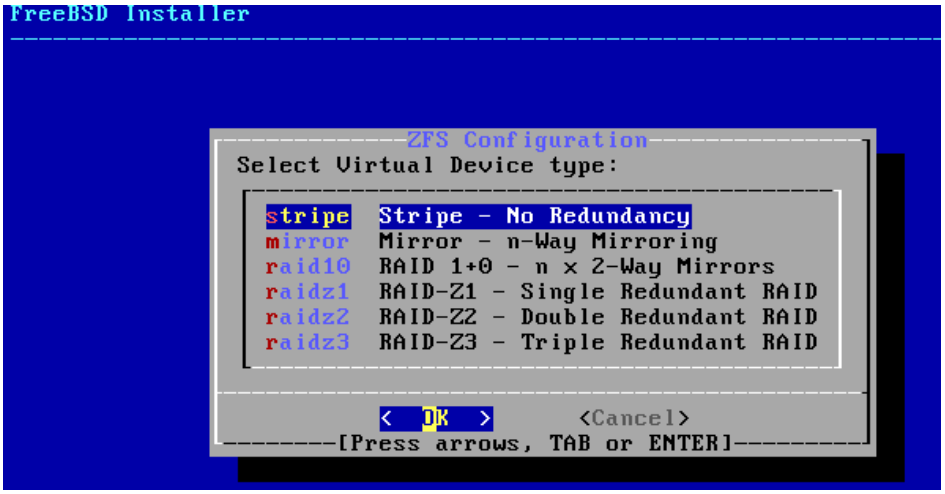
5. Select “Continue with…” and press Enter:



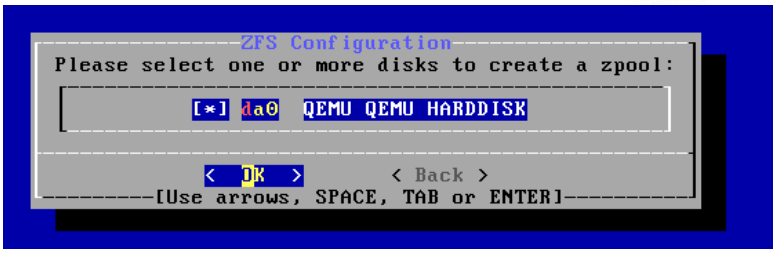
6. Select “Install (ZFS)” and press Enter:



7. Select “Stripe” and press Enter:

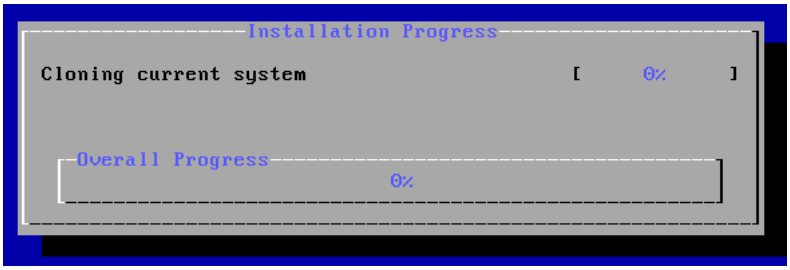


8. Press “Space” to select the virtual disk and press “OK”:

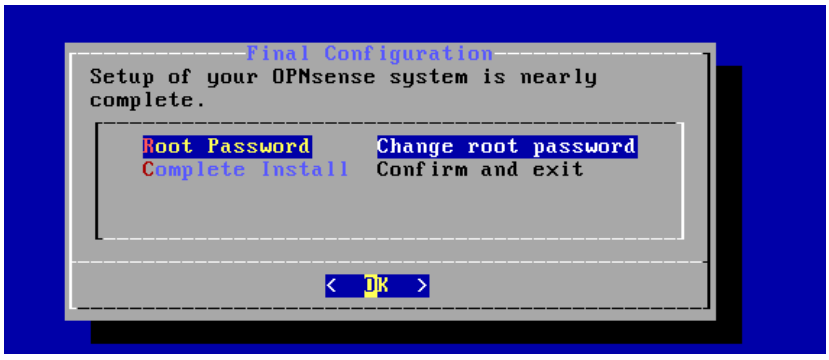


9. Select “Yes” and press Enter:

10. Wait for the installation process to finish:

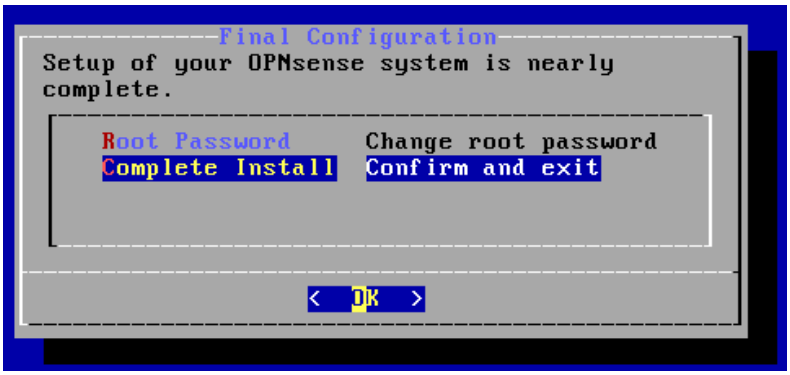


11. Select “Change root password” and press “OK”:

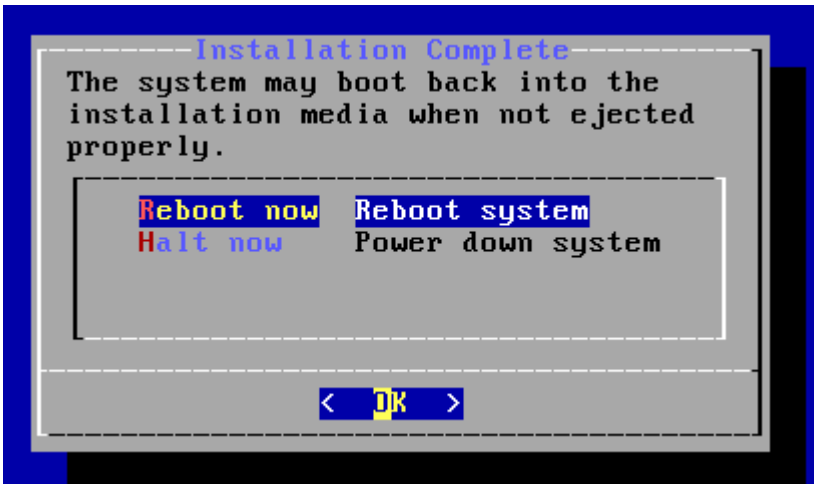


12. Define a new password for the root user and press “OK”:

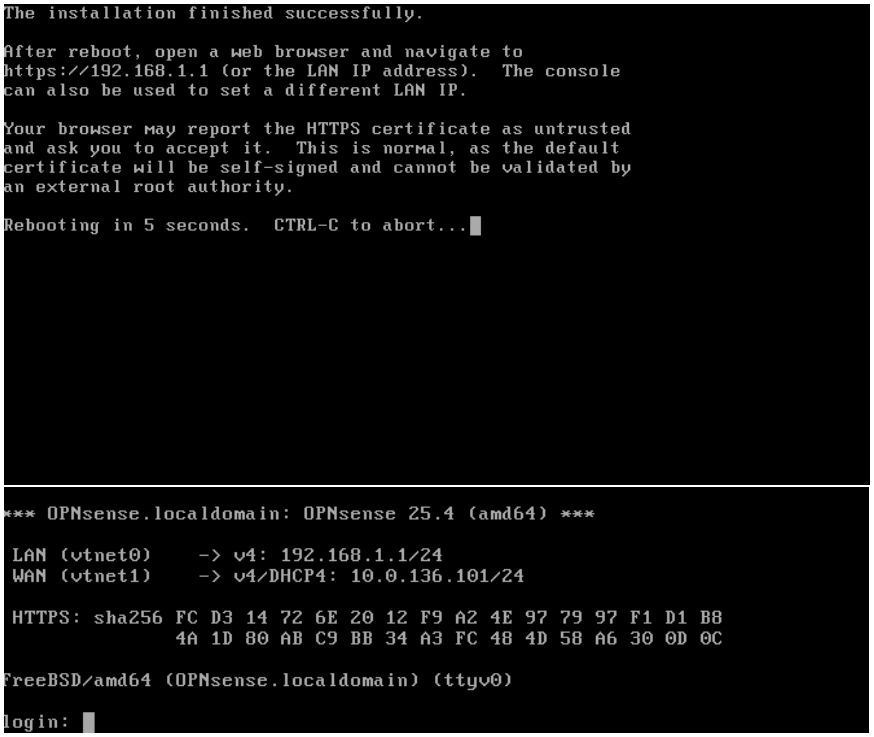
13. Select “Complete Install” and press “Enter”:



14. Select “Reboot now” and press “Enter”:



15. Wait for [TOE-254] to reboot:



16. Log in with root credentials.

17. Enter “1” and press “Enter” to assign the interfaces.

```
*** OPNsense.localdomain: OPNsense 25.4 (amd64) ***

LAN (vtnet0)    -> v4: 192.168.1.1/24
WAN (vtnet1)    -> v4/DHCP4: 10.0.136.101/24

HTTPS: sha256 FC D3 14 72 6E 20 12 F9 A2 4E 97 79 97 F1 D1 B8
              4A 1D 80 AB C9 BB 34 A3 FC 48 4D 58 A6 30 0D 0C

 0) Logout                              7) Ping host
 1) Assign interfaces                   8) Shell
 2) Set interface IP address            9) pfTop
 3) Reset the root password            10) Firewall log
 4) Reset to factory defaults          11) Reload all services
 5) Power off system                   12) Update from console
 6) Reboot system                      13) Restore a backup

Enter an option: 1
```

18. Enter “N” when prompted to configure LAGGs and VLANs:

```
Do you want to configure LAGGs now? [y/N]: N
Do you want to configure VLANs now? [y/N]: N
```

19. Enter the WAN interface name. In this case is “vtnet0”.
20. Enter the LAN interface name. In this case is “vtnet1”. This interface will be the LAN1 interface.
21. Enter the Optional interface name. In this case is “vtnet2”. This interface will be the LAN2 interface.
22. Enter “y” and press “Enter”:

```
If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: vtnet0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): vtnet1

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished): vtnet2

Enter the Optional interface 2 name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> vtnet0
LAN  -> vtnet1
OPT1 -> vtnet2

Do you want to proceed? [y/N]:
```

23. In the [TOE-254] menu, select option 2 and press “Enter.
24. Select “vtnet1” interface”:

```
Enter an option: 2

Available interfaces:

1 - LAN (vtnet1 - static, track6)
2 - OPT1 (vtnet2)
3 - WAN (vtnet0 - dhcp, dhcp6)

Enter the number of the interface to configure: 1
```

25. Enter “n” and press “Enter” when prompted to configure IPv4 address LAN interface via DHCP. Then enter the LAN IPv4 address and the subnet mask bit count:

```
Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.136.101


Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

26. Enter “Y” and press “Enter” when prompted to configure IPv6 address LAN interface via WAN tracking.
27. Enter “N” and press “Enter” when prompted to enable the DHCP server on LAN and change the web GUI protocol from HTTPS to HTTP.
28. Enter “Y” and press “Enter” when prompted to generate a new self-signed web GUI certificate and restore web GUI access defaults.

```
Configure IPv6 address LAN interface via WAN tracking? [Y/n] y

Do you want to enable the DHCP server on LAN? [y/N] n

Do you want to change the web GUI protocol from HTTPS to HTTP? [y/N] n
Do you want to generate a new self-signed web GUI certificate? [y/N] y
Restore web GUI access defaults? [y/N] y
```

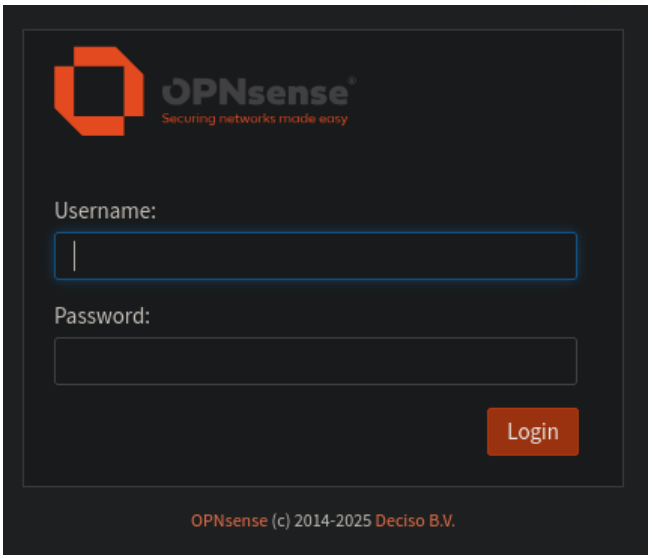
29. Verify the IP of the network interface has been set correctly:

```
*** OPNsense.localdomain: OPNsense 25.4 (amd64) ***

 LAN (vtnet1)     -> v4: 10.0.136.101/24
```

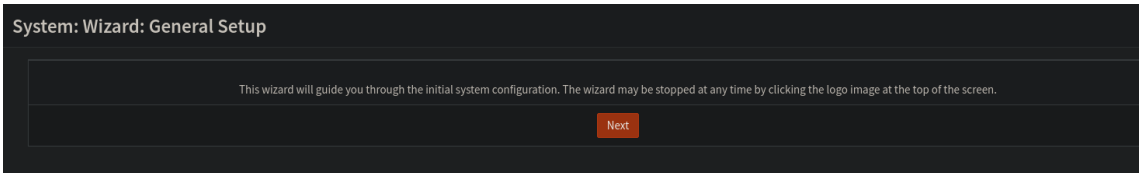
30. Repeat the process with “vtnet2” interface, setting a static IPv4 address and network mask.

```
*** OPNsense.localdomain: OPNsense 25.4 (amd64) ***

 LAN (vtnet1)     -> v4: 10.0.136.101/24
 OPT1 (vtnet2)    -> v4: 10.0.137.101/24
 WAN (vtnet0)     -> v4/DHCP4: 10.0.135.100/24
```

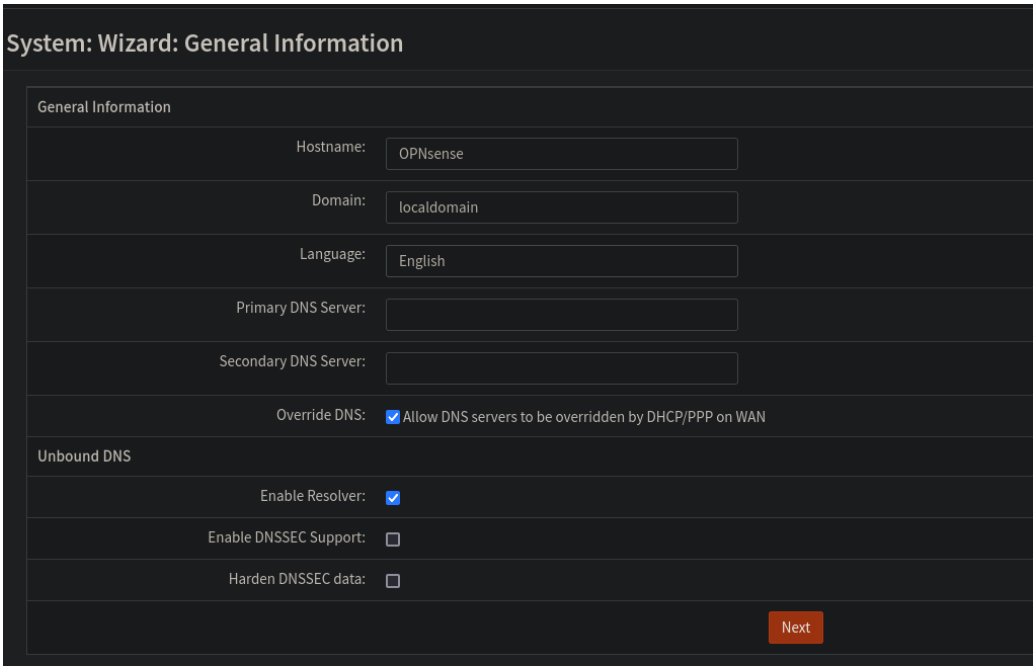
31. In [KALI1], access the LAN IP address through HTTPS using a web browser and log in with the root user credentials:



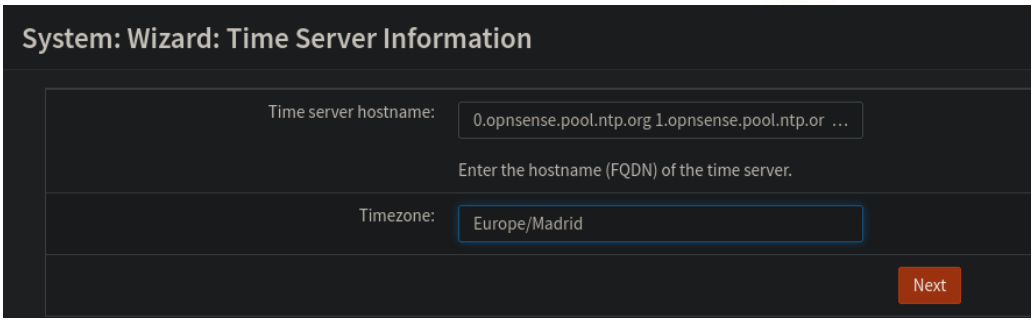
32. Follow the wizard setup, press Next:



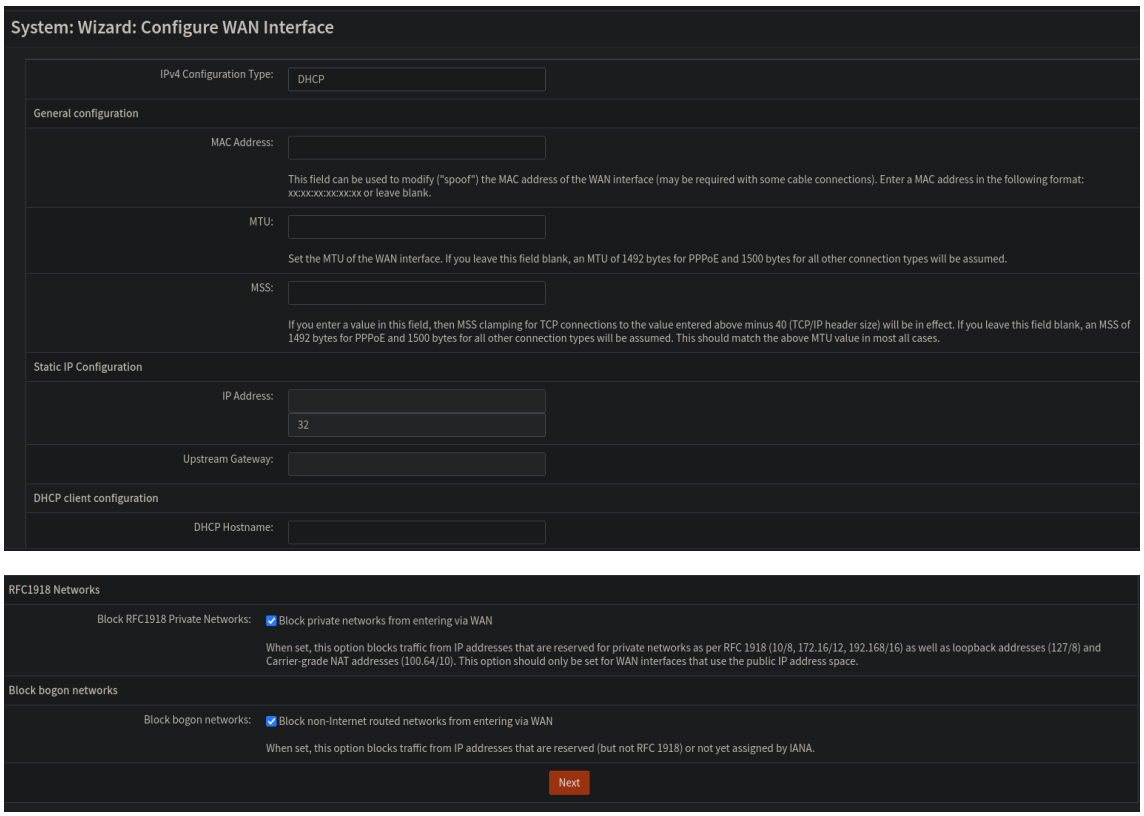
30. Give a hostname and a domain to the TOE and press “Next”:



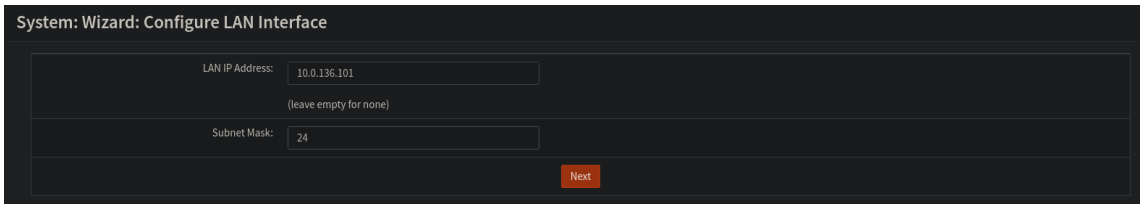
33. Set NTP servers and the time zone. In this case the NTP servers configured are the ones offered by default. Press “Next”:



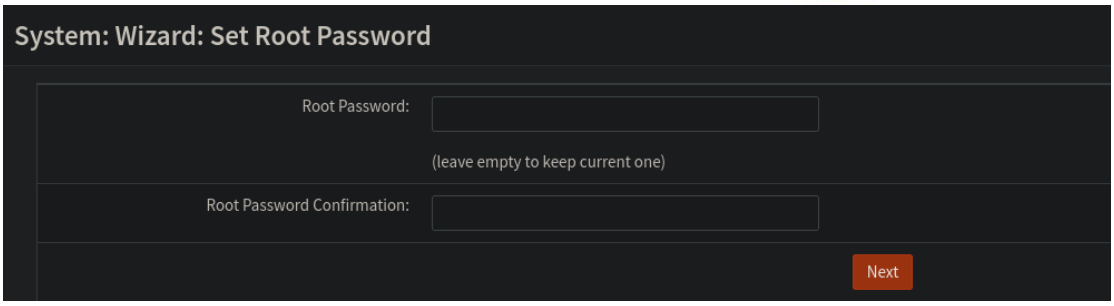
34. Leave the default configuration for the WAN interface and press “Next”:



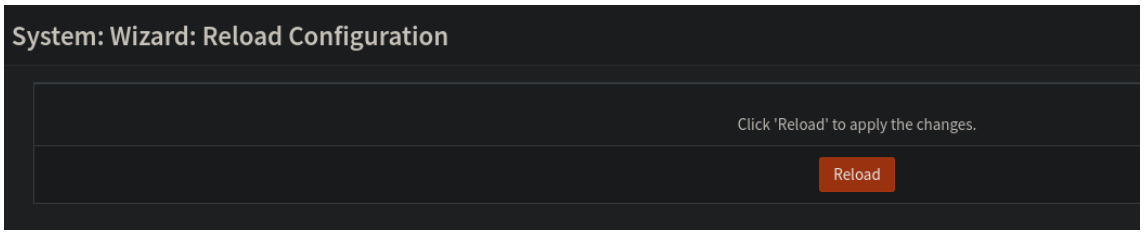
35. Leave the default configuration for the LAN interface. Press “Next”:



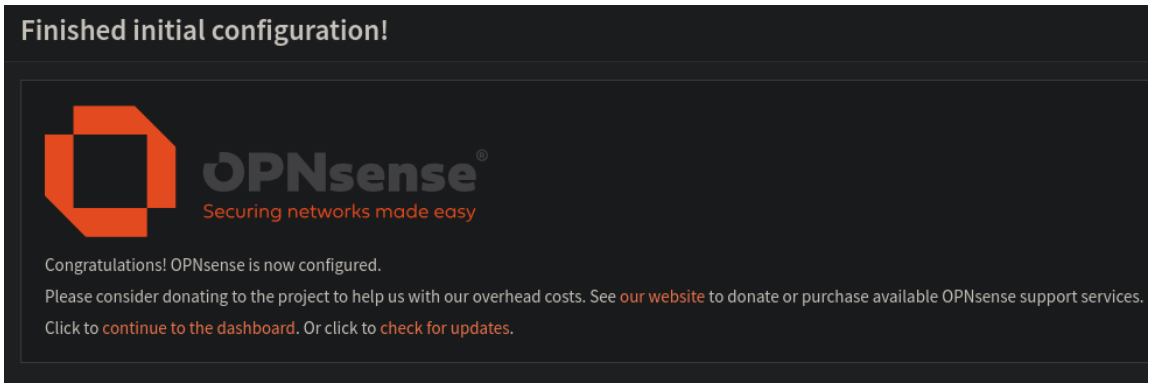
36. Set a new root password if it was not changed before:



37. Click on “Reload” to apply the changes:



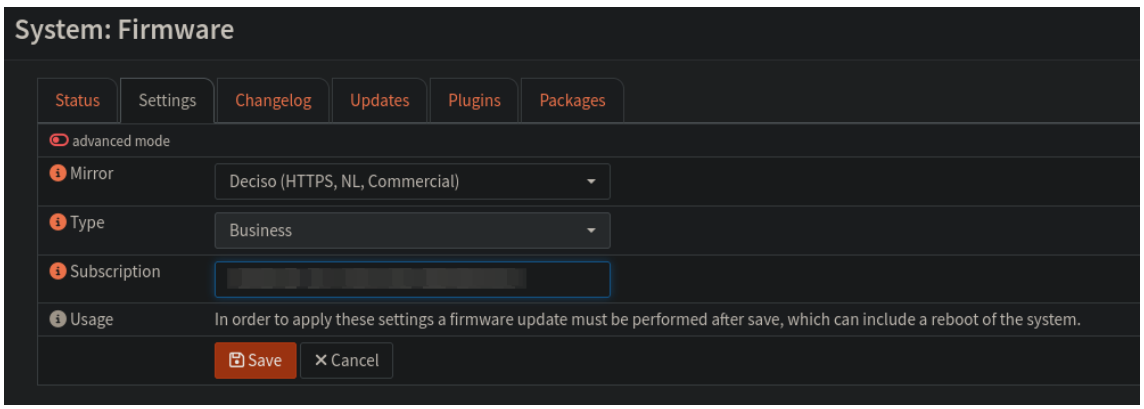
38. Wait for the configuration to finish:



6.3.1 SETTING A SUBSCRIPTION KEY

The following steps are followed in order to configure a subscription key:

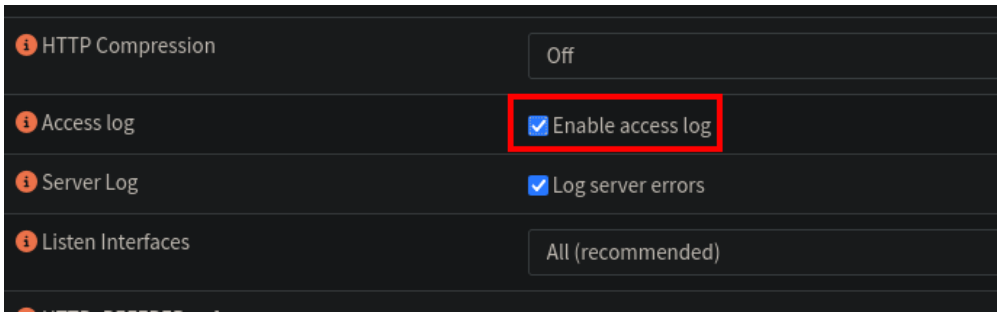
1. Log in through the TOE web interface with root credentials.
2. Go to “System → Firmware → Settings”.
3. Indicate the subscription key in the Subscription text box and click “Save”:



6.3.2 ENABLING ACCESS LOGS

To enable access logs, the following steps are required:

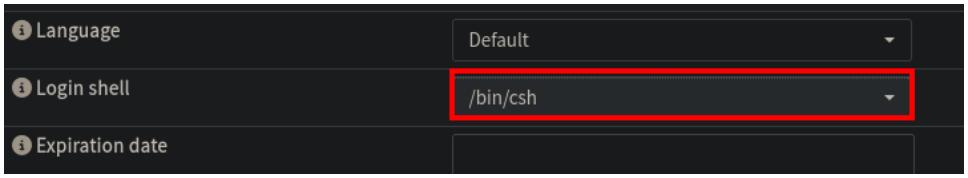
1. Log in through the TOE web interface with root credentials.
2. Enable the access log parameter in the Settings menu. In the left panel go to "System → Settings → Administration" and select "Enable access log":



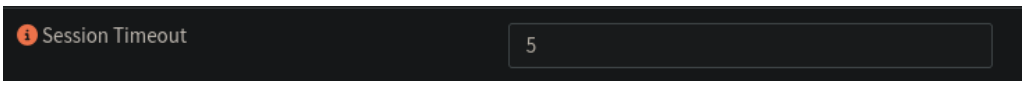
6.3.3 CONFIGURING SHELL TYPE AND INACTIVITY TIMEOUT

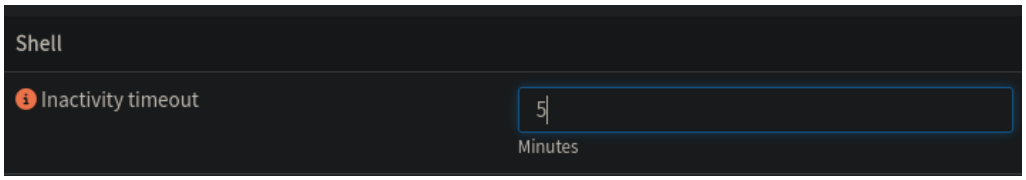
For the inactivity session timeout to work, it is required to change the login shell assigned to the user. The steps below are followed:

1. Log in through the TOE web interface with root credentials.
2. Go to "System → Access → Users".
3. For each user, change the Login shell assigned from /usr/local/sbin/opnsense-shell to "/bin/csh". Then click on "Save" to apply the changes:



4. Go to "System → Settings → Administration".
5. Set the "Session Timeout" and "Inactivity timeout" parameters to 5 minutes in order to set the inactivity timeout for the GUI and CLI interfaces Then click on "Save" to apply the changes:

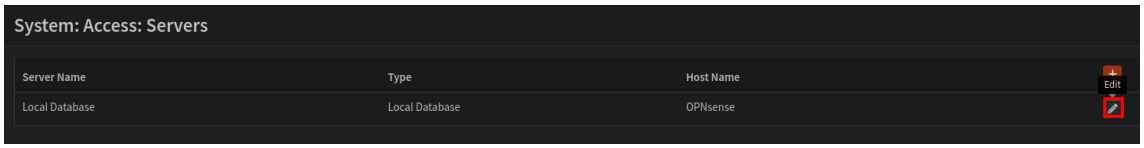




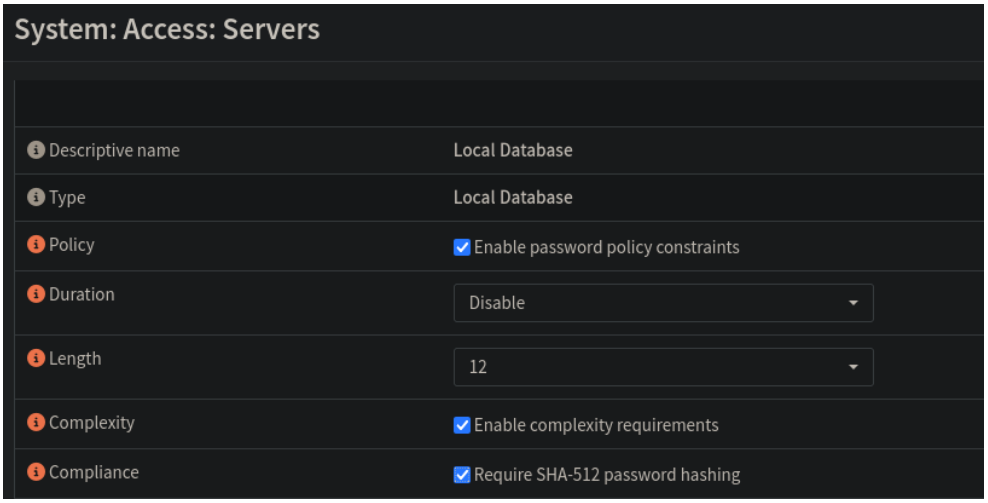
6.3.4 DEFINING A PASSWORD POLICY

1. Log in through the TOE web interface with root credentials.
2. Go to "System → Access → Servers".

3. Edit the “Local Database” server.



4. Enable “Password policy constraints”. Then, add a duration for passwords, the minimum length, enable complexity requirements and compliance settings:



5. Click on “Save” to save the changes.

6.3.5 ADDING A READ-ONLY AUDIT ROLE

In order to prevent any user (other than the root user) with read access to audit records from deleting the logs, the following steps must be followed:

1. Log in through the TOE CLI interface with root credentials.
2. Create a new directory that will store the new ACL by executing the following command:

```
mkdir -p /usr/local/opnsense/mvc/app/models/security/security/ACL
```

3. Create the file ACL.xml in the previous created directory with the following content in order to create the new read-only audit role:

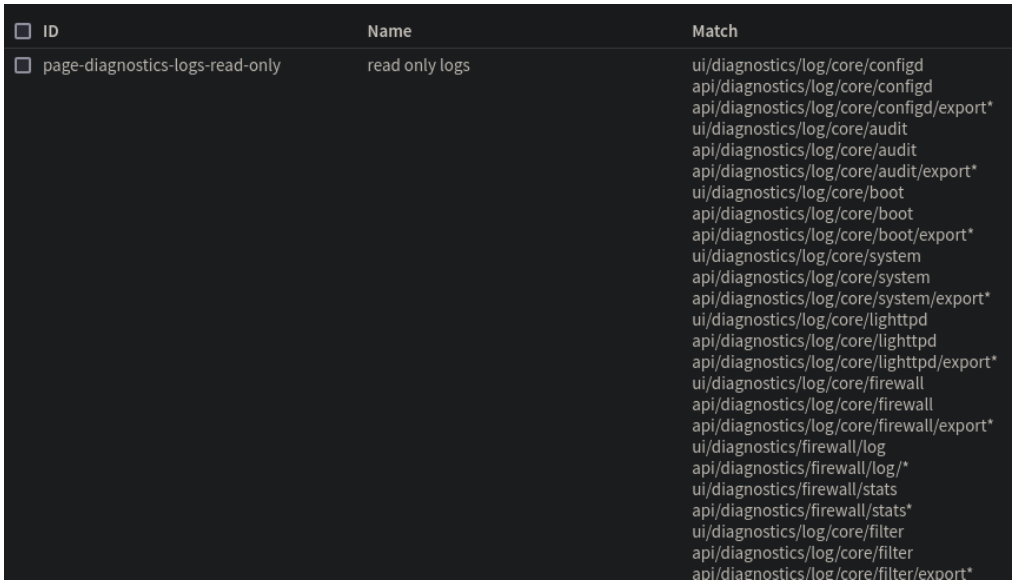
```
<acl>
    <page-diagnostics-logs-read-only>
        <name>read only logs</name>
        <patterns>
            <!-- System: Log Files: Backend -->
                <pattern>ui/diagnostics/log/core/configd</pattern>
                <pattern>api/diagnostics/log/core/configd</pattern>
```

```
                <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>
```

4. Clear the cache to prevent old ACL-s still being used with the following command:

```
rm /tmp/opnsense_acl_cache.json
```

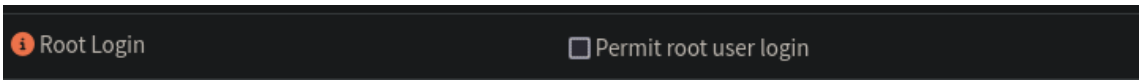
After this, the new role shall appear when assigning privileges to a user or group.



6.3.6 DISABLING ROOT USER FOR SSH

To disable root access to the CLI through SSH, the steps below are followed:

1. Log in through the TOE web interface with root credentials.
2. Go to “System→ Settings → Administration → Secure Shell”.
3. Uncheck the option “Permit root login”:

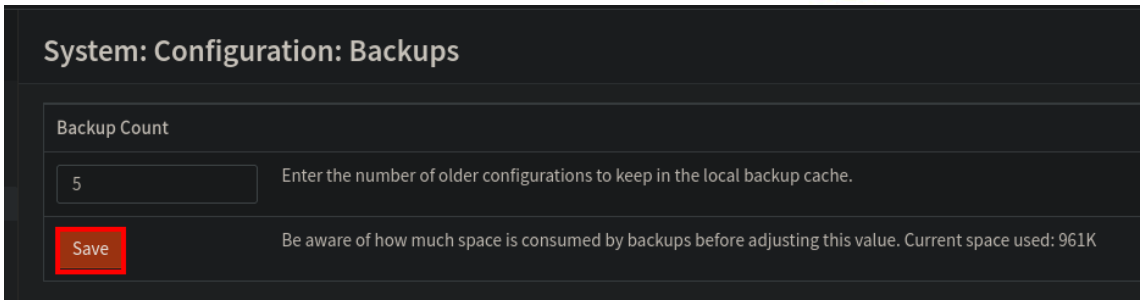


4. Click on “Save” to save the changes.

6.3.7 CONFIGURING SYSTEM BACKUPS ROTATION

In order to preserve a specific number of configuration backups the steps below are followed:

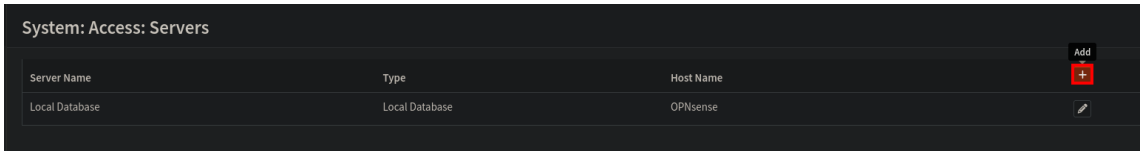
1. Log in through the TOE web interface with root credentials.
2. Go to “System → Configuration → Backups”.
3. Configure the “Backup Count” parameter to 5. Then click on “Save” to apply the changes:



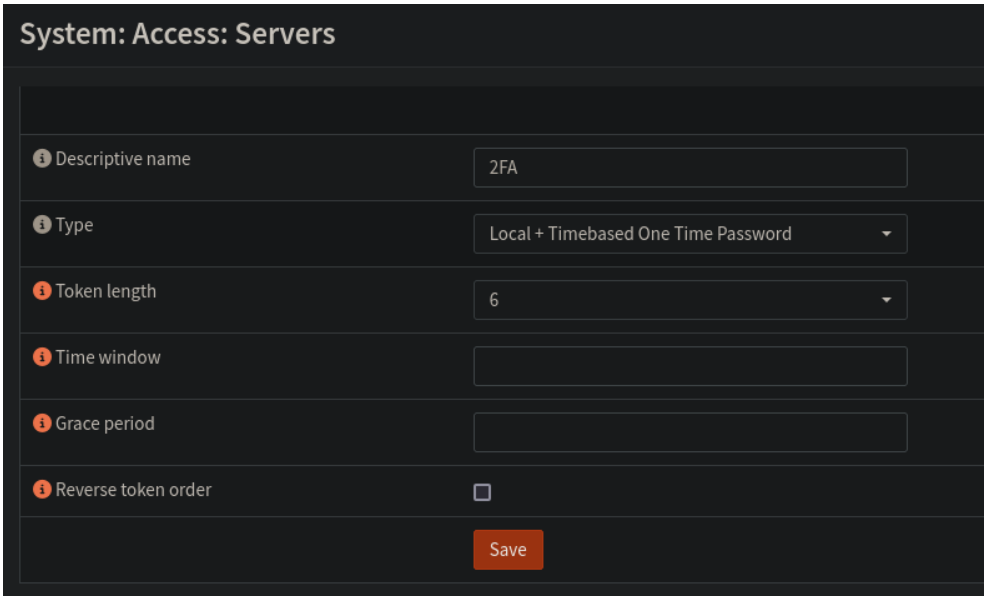
6.3.8 CONFIGURING TWO-FACTOR AUTHENTICATION

In order to configure a 2FA the steps below are followed:

1. Log in through the TOE web interface with root credentials.
2. Go to "System → Access → Servers".
3. Click "Add server" in the top right corner:

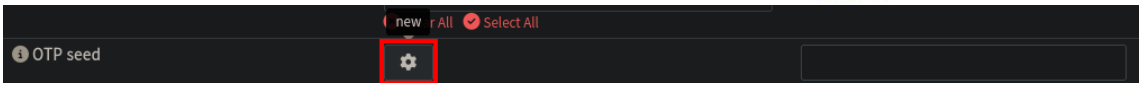


4. Create a new server with the following parameters:

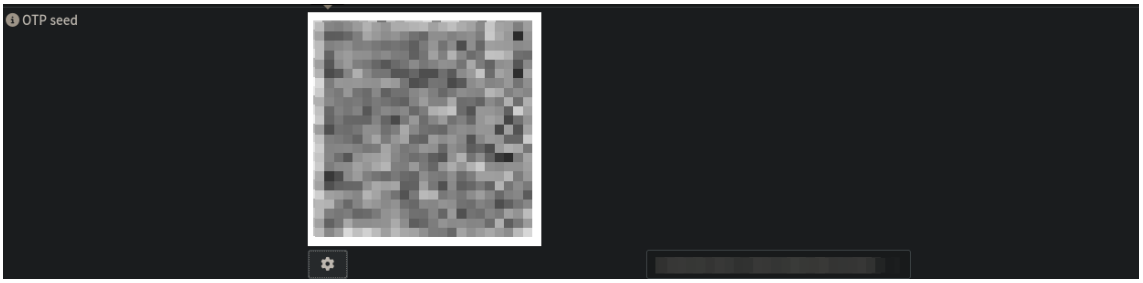


5. Install a Google Authenticator compatible app on your device.
6. Go to "System → Access → Users".
7. Edit the root user.
8. Click on "Show" in the OTP seed parameter:

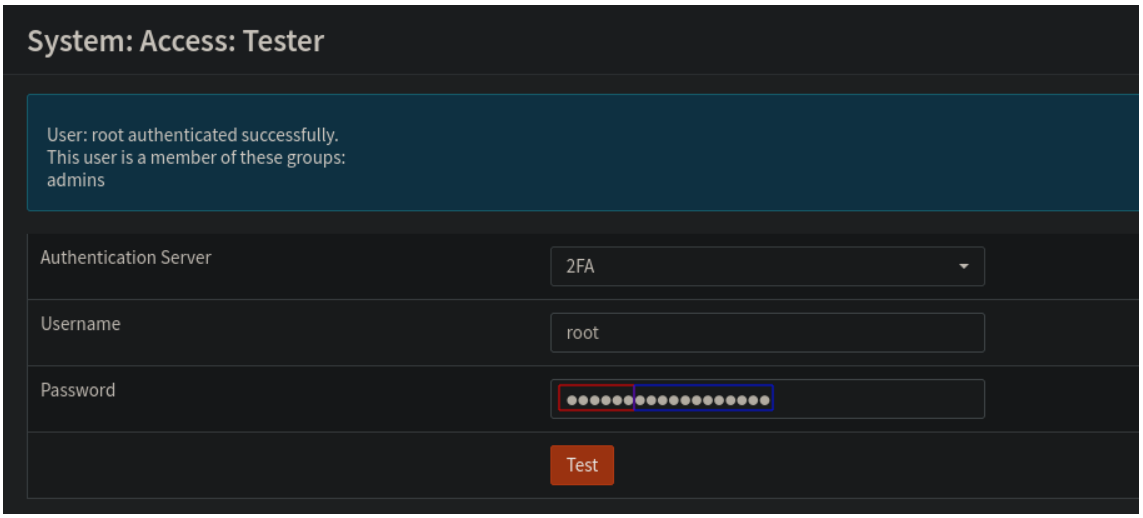
9. Click on "New" in the OTP seed parameter:



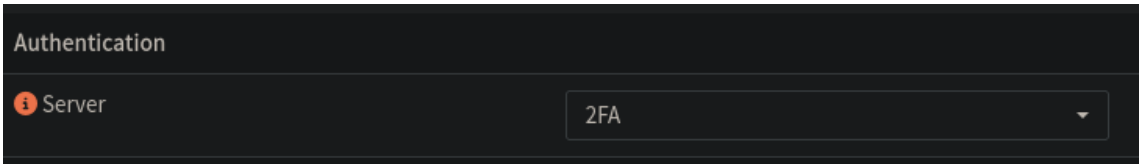
10. Register the token generated or QR code in the Goggle Authenticator compatible app:



11. Click on “Save” to save the changes.
12. Go to “System → Access → Tester”.
13. Verify that the 2FA authentication is properly configured concatenating the authenticator code and the user password “<CODE><PASSWORD>”:



14. Go to “System → Settings → Administration”.
15. Change the Authentication server by selecting the “2FA” server that was just created in the dropdown menu:



16. Click on “Save” to apply the changes.

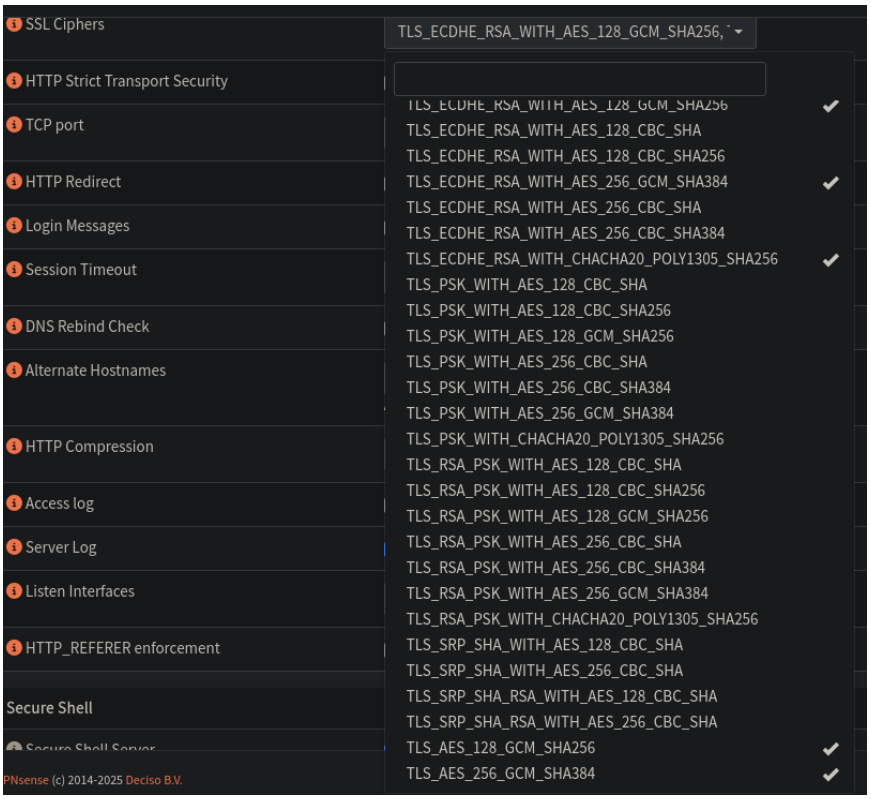
Note: The 2FA is configured for each user. In this case, it was configured for the root user. The steps shall be repeated for each desired user to use 2FA.

6.3.9 CONFIGURING WEB INTERFACE TLS CIPHER SUITES

It is required to configure cipher suites for TLS through the web interface. This configuration affects the web portal used to manage and administrate the TOE. The steps below are followed:

1. Log in through the TOE web interface with root credentials.
2. Navigate to "System → Settings → Administration".
3. In the Web GUI section, use the dropdown menu for "SSL Ciphers" to select valid cipher suites:

TLS_AES_128_GCM_SHA256
TLS_AES_256_GCM_SHA384
TLS_CHACHA20_POLY1305_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256



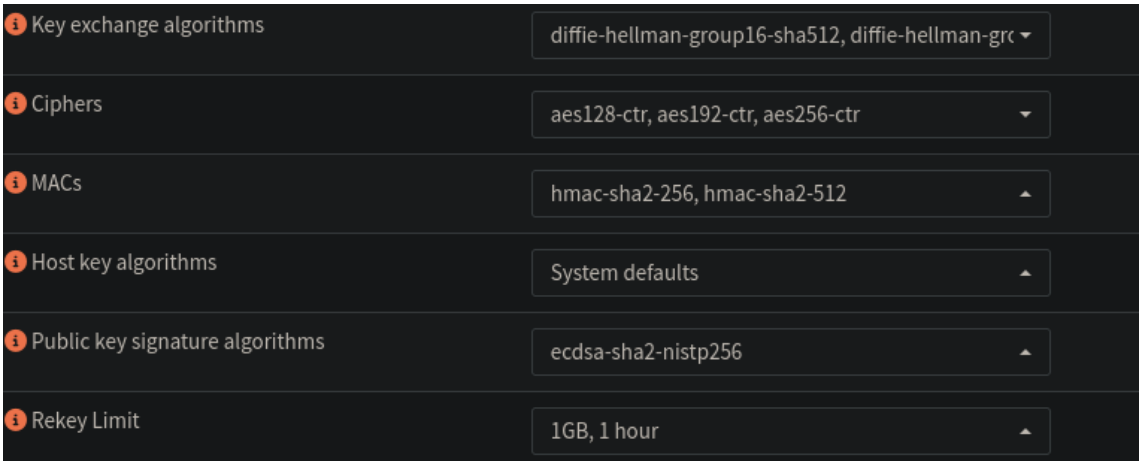
4. Scroll down and click "Save" to apply the configuration.

6.3.10 CONFIGURING SSH CRYPTOGRAPHIC PARAMETERS

It is required to configure cryptographic parameters for SSH through the web interface. This configuration affects the SSH connections that users establish with the TOE. The steps below are followed:

1. Log in through the TOE web interface with root credentials.
2. Navigate to "System → Settings → Administration".
3. In the Secure shell section, click on "Show cryptographic overrides":

4. Use the dropdown menu for "Key exchange algorithms", "Ciphers", "MACs", "Public key signature algorithms" and "Rekey Limit" to select valid cryptographic parameters:
    a. Key exchange algorithms:
        i. diffie-hellman-group16-sha512
        ii. diffie-hellman-group18-sha512
        iii. ecdh-sha2-nistp256
        iv. ecdh-sha2-nistp384
        v. ecdh-sha2-nistp521
    b. Ciphers:
        i. aes128-ctr
        ii. aes192-ctr
        iii. aes256-ctr
    c. MACs:
        i. hmac-sha2-256
        ii. hmac-sha2-512
    d. Public key signature algorithms:
        i. ecdsa-sha2-nistp256
    e. Rekey Limit:
        i. 1GB, 1 hour



5. Scroll down and click on "Save" to apply the changes.

6.3.11 INSTALLING CERTIFICATES FROM TRUSTWORTHY CA

A self-signed certificate generated by [TOE-254] itself is used in this evaluation, as it does not imply a degradation in the quality level at the functionality or testing of [TOE-254]. This matter is considered by the evaluator when conducting the testing.

6.3.12 DISABLING NTP SERVICE.

In order to disable the NTP service the steps below are followed:

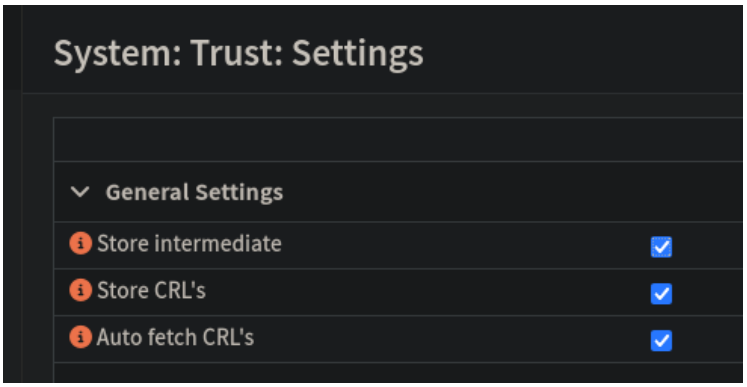
1. Log in through the TOE web interface with root credentials.
2. Go to “Services → Network Time → General”.
3. Remove all the Time servers specified:

4. Click on “Save” to apply the changes.

6.3.13 MODIFYING TRUST SETTINGS

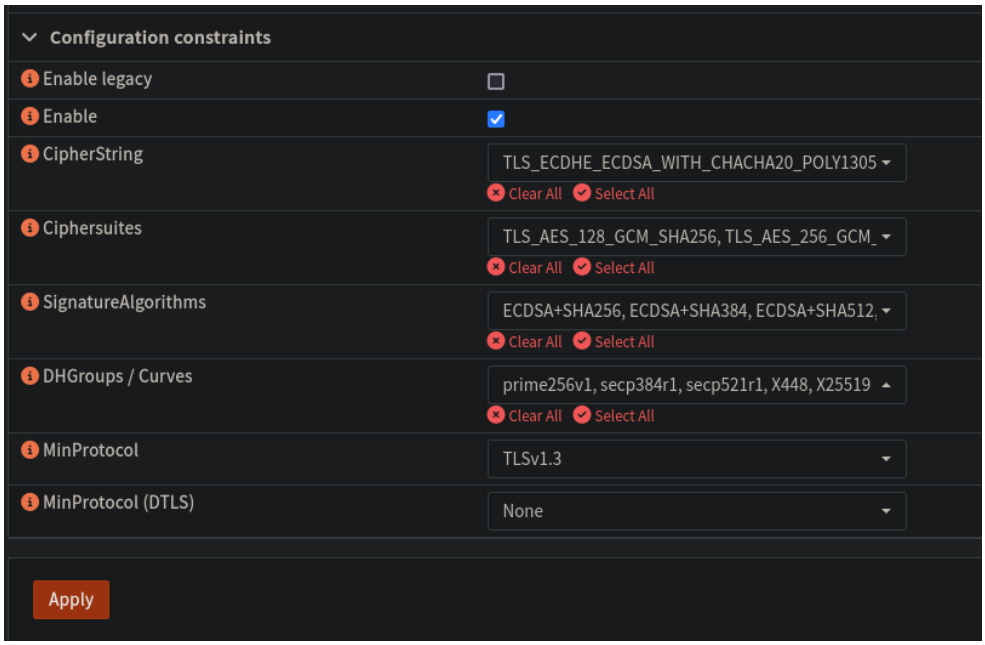
The steps followed are defined below:

1. Log in through the TOE web interface with root credentials.
2. Go to “System → Trust → Settings”.
3. Enable the “Store intermediate”, “Store CRL’s” and “Auto fetch CRL’s” checkboxes:



4. Under Configuration constraints, select Enable checkbox, which is disabled by default, uncheck the “Enable Legacy” option and indicate the following configuration:

a. CipherString:
   TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
   TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
b. Ciphersuites:
   TLS_AES_128_GCM_SHA256, TLS_AES_256_CGM_SHA384, TLS_CHACHA20_POLY1305_SHA256
c. SignatureAlgorithms:
   ECDSA+SHA256, ECDSA+SHA384, ECDSA+SHA512, rsa_pss_pss_sha256, rsa_pss_pss_sha384, rsa_pss_pss_sha512, rsa_pss_rsae_sha256, rsa_pss_rsae_sha384, rsa_pss_rsae_sha512.
d. DHGroups / Curves: prime256v1, secp384r1, secp521r1, x448, x25519
e. MinProtocol: TLSv1.3

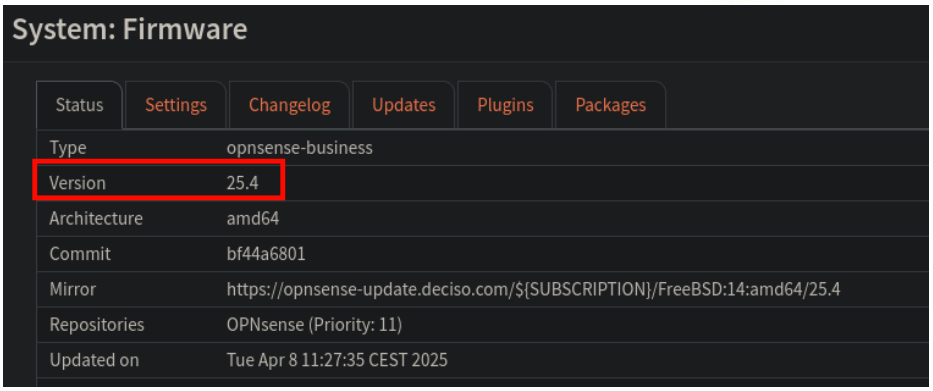


5. Click on “Apply” to apply the changes.

6.4 VERIFICATION OF THE INSTALLED TOE VERSION

In order to check the verification of the installed TOE version, the steps below are followed:

1. Log in through the TOE web interface with the root user.
2. Go to “System → Firmware → Status”.
3. Check the version number identifier:



6.5 USED INSTALLATION OPTIONS

The selection of different installations options in order to achieve the secure configuration was not considered or required.

6.6 RESULTS

ID	Non-conformity	State
N/A	None.	N/A

ID	Comments	State
N/A	None.	N/A

7 CONFORMITY ASSESSMENT

7.1 FUNCTIONAL TESTS

Evaluator	AGL
Days required	1 days.
Date	2025/05/16
Results of the evaluator's work	**PASS**

7.1.1 EVALUATION ACTIVITIES

The information presented in this section covers the result of carrying out the evaluation activities specified in section 4.3 of [CCN-STIC-2002], with regard to functional testing of the TOE.

TE.4.1. The evaluator shall check and test the product's security functions and mechanisms to a level of detail that allows checking that the declared security functionality has been correctly implemented in the product. The evaluator must justify the sample using as a reference Annex A.2 of [CEM].

PASS Information concerning this task of the evaluator can be found in the section 7.1.2 List of functional tests. This information is presented in more detail in the section *12 Annex B: Functional test plan and report.*

TE.4.2. The evaluator shall register every non-conformity in regards to any test performed.

PASS Information concerning this task of the evaluator can be found in the section *7.1.3 Results*.

7.1.2 LIST OF FUNCTIONAL TESTS

Security function	Test code	Objective	Result
FFW_RUL_EXT.1.6	[STIC_OPNSENSE_IAD-2504-TST-0010]	Verify if the TOE drops and is capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address "reserved for the future use" (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4.	**PASS**
FFW_RUL_EXT.1.6	[STIC_OPNSENSE_IAD-2504-TST-0020]	Verify if the TOE drops and is capable of logging network	**PASS**

		packets where the source or destination address of the network packet is defined as being unspecified or an address “reserved for the future use” (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6.	
FCS_CKM.4.1	[STIC_OPNSENSE_IAD-2504-TST-0030]	Verify that the TSF destroys cryptographic keys in accordance with a specified cryptographic key destruction method. - For plaintext keys in volatile storage, the destruction shall be executed by a single overwrite consisting of zeroes. - For plaintext keys in non-volatile storage, destruction shall be performed by invoking a TSF-provided interface that instructs another part of the TSF to destroy the abstraction representing the key.	**PASS**
FCS_RBG_EXT.1.1 FCS_RBG_EXT.1.2	[STIC_OPNSENSE_IAD-2504-TST-0040]	Verify that the TOE performs all deterministic random bit generation services in accordance with ISO/IEC 18031:2011. In addition, verify that the deterministic RBG is seeded by at least one entropy source that accumulates entropy from software-based noise source or platform-based noise source with a minimum of entropy at least equal to the greatest security strength,	**PASS**

		according to ISO/IEC 18031:2011.	

7.1.3 RESULTS

ID	Non-conformity	State
N/A	None.	N/A

ID	Comments	State
N/A	None.	N/A

8 VULNERABILITY ANALYSIS

Evaluator	DAT
Days required	1 day
Date	2025/05/16
Results of the evaluator's work	**PASS**

8.1 EVALUATION ACTIVITIES

The information presented in this section covers the result of carrying out the Evaluation activities specified in section 4.4 of [CCN-STIC-2002], with regard to the analysis of vulnerabilities present in the TOE.

TE.5.1. The evaluator shall perform a methodic vulnerability analysis by using any means within their technical competence, using at least the following sources of information:

(a) Documentation provided by the applicant (e.g., Security Target, user's guides, etc.).

b) Available information on the technology.

c) Public vulnerability databases for the type of the product. taking into account in such analysis the relation of third-party libraries defined in the Security Target by the applicant.

d) The product itself, which is installed on a test platform as representative as possible with respect to environment of the product.

PASS The TOE vulnerability analysis is described in the *8.3 TOE vulnerability analysis*. The result of this analysis is detailed in the section *14 Annex C: Vulnerability Analysis.*

TE.5.2 The evaluator shall document the devised vulnerability analysis methodology.

PASS The method followed to carry out the vulnerability analysis is described in the section *8.2 Methodology used for the analysis*.

TE.5.3. Document all potential vulnerabilities found within the applicable attack potential and document possible attack scenarios based on those vulnerabilities.

PASS Information regarding the vulnerabilities found is summarized in section *8.4 List of potential vulnerabilities* and described in more detail in section *14 Annex C: Vulnerability Analysis.* The scenarios are detailed in section *12 Annex A: Test scenarios.*

TE.5.4. Calculate the attack potential for each of the attack scenarios designed by the evaluator according to the scoring system described in section 4.4.1.1.1 Calculation of Attack Potential of [CCN-STIC-2002].

PASS Information concerning this task of the evaluator can be found in the section *8.4 List of potential vulnerabilities.*

This information is described in more detail in the section *14 Annex C: Vulnerability Analysis.*

TE.5.5. The evaluator shall register every non-conformity in relation to the Security Target.

PASS Information regarding this task of the evaluator can be found in section *8.5 Results.*

8.2 METHODOLOGY USED FOR THE ANALYSIS

The methodology used follows the spirit of the Common Criteria [CC] methodology for vulnerability analysis [CEM].

Firstly, the changelogs collected in the [IAR-10] were analysed to determine potential vulnerabilities related to newly added functionality or fixed functionality of the TOE.

Secondly, the evaluator referred to the OWASP TOP 10 2021 standard [OWASP], which delineates the most prevalent vulnerabilities. Following an analysis of the vulnerabilities outlined in OWASP what apply to the Target of Evaluation (TOE), the traceability of each vulnerability to OWASP TOP 10 has been proved in the next section, next to each vulnerability.

Then, a survey of the TOE information available has been carried out to identify potential vulnerabilities that can be exploited by an attacker with low attack potential.

An extensive analysis of the state of the art regarding the different vectors of attack on TOE-like tools has been carried out from different points of view. Based on the results of these tools and the analysis of the most common weaknesses of this type of tools, the vulnerabilities of the TOE have been identified.

As part of this initial analysis, a search for public vulnerabilities in third-party components and in older versions of the TOE, if any, is performed. For each public vulnerability, its applicability is determined and a brief rationale is provided. If a public vulnerability is considered applicable, a calculation of the attack potential required to exploit the vulnerability will be performed.

Next, an assessment and analysis of the vulnerabilities found has been made by performing tests that provide more information on the vulnerabilities and give rise to more sophisticated attacks.

The evaluator employed a set of criteria to determine the nature of the tests conducted, which comprised two main components. Firstly, the evaluator relied on a thorough examination of the security functionalities inherent to the product. Secondly, the evaluator referred to the OWASP TOP 10-2021 standard [OWASP], which delineates the most prevalent vulnerabilities. Following an analysis of the vulnerabilities outlined in

OWASP that apply to the Target of Evaluation (TOE), the traceability of each vulnerability to OWASP TOP 10 has been provided below, next to each vulnerability.

In a third step, penetration tests have been carried out based on the vulnerabilities found to check the degree of exploitability of the vulnerabilities.

Finally, comprehensive and more complex penetration tests on the exploitable vulnerabilities present in the TOE have been developed as proofs of concept to illustrate the possibilities of an attacker exploiting these vulnerabilities.

To calculate the distribution of the time dedicated to each vulnerability, it has been done taking into account the degree of difficulty to be exploited, as well as the severity for the integrity of the TOE that a successful attack would entail.

8.3 TOE VULNERABILITY ANALYSIS

The vulnerability analysis process includes reviewing all security features affected by the changes identified in [IAR-10], as well as testing the most relevant vulnerabilities listed in the OWASP Top 10 (2021). This process aims to identify potential weaknesses that could affect the TOE.

The analysis process continues with the clear definition of the context of vulnerability to serve as a basis for understanding its severity and subsequent consideration. On the basis of this information, the different routes of attack on the vulnerable element are established, which, if appropriate, will be tested for penetration later.

The tools used in the identification of the vulnerabilities present in the TOE are developed from information present in the TOE are developed from public information always under the requirements of time and effort marked by the methodology and developing small scripts from public information and based on the functional tests performed in the previous stage.

All the changelogs reflected in the [IAR-10] have been analysed, with special attention paid to threats that could compromise communication between the TOE and other entities, the integrity of the information stored within it, and its ability to maintain functionality under extreme workloads or attempts to bypass its traffic restrictions.

8.4 LIST OF POTENTIAL VULNERABILITIES

Code	Resistance level
[STIC_OPNSENSE_IAD-2504-VUL-0000]	6
[STIC_OPNSENSE_IAD-2504-VUL-0100]	3
[STIC_OPNSENSE_IAD-2504-VUL-0110]	3
[STIC_OPNSENSE_IAD-2504-VUL-0120]	3
[STIC_OPNSENSE_IAD-2504-VUL-0200]	3
[STIC_OPNSENSE_IAD-2504-VUL-0300]	3
[STIC_OPNSENSE_IAD-2504-VUL-0400]	3
[STIC_OPNSENSE_IAD-2504-VUL-0410]	3

[STIC_OPNSENSE_IAD-2504-VUL-0500]	3
[STIC_OPNSENSE_IAD-2504-VUL-0600]	3
[STIC_OPNSENSE_IAD-2504-VUL-0700]	3

8.5 RESULTS

ID	Non-conformity	State
N/A	None.	N/A

ID	Comments	State
N/A	None.	N/A

9 TOE PENETRATION TESTS

This section presents a summary of the tests carried out and the results obtained.

Evaluator	AGL
Days required	8 days.
Date	2025/05/16
Results of the evaluator's work	**PASS**

9.1 EVALUATION ACTIVITIES

The information presented in this section covers the result of carrying out the evaluation activities specified in section 4.5 of [CCN-STIC-2002], with regard to the TOE penetration tests.

TE.6.1. Provide a list of all penetration tests performed in the TOE, including at least the steps necessary to reproduce the test, the expected result, the result obtained, and whether the attack is successful or not. In addition, indicate to which of the vulnerabilities identified in the previous phase this penetration test is associated.

PASS The list of penetration tests performed can be found summarized in the section *9.2 List of penetration tests* and described in more detail and with the information indicating the evaluator's task in the section *15 Annex D: Penetration test plan and report.*

TE.6.2. The evaluator shall document all non-conformities related to any successful attack.

PASS The results of the penetration tests are collected on the basis of the non-conformities and comments in the section *9.3 Results*.

9.2 LIST OF PENETRATION TESTS

Penetration tests are performed from the perspective of a potential attacker and, based on the vulnerabilities found in the TOE, aim to cover the most relevant and promising attack vectors.

Time constraints mean that the methodology used in penetration testing is focused on determining whether the objective established in each test is feasible, thus determining the severity of the identified vulnerabilities.

Some tests were not identified during the preliminary vulnerability analysis and are the result of the creativity of the evaluator, who looks for new possible attacks in an exploratory way based on the knowledge gained during the tests.

For these tests it will be necessary to create an applicable vulnerability and calculate the attack potential.

The PASS/FAIL criteria for establishing the result of the penetration tests will be that if a FAIL penetration test is performed because the TOE does not behave safely according to the security functionality and assets declared by the manufacturer in his Security Target. For those penetration tests whose objective is not directly the violation of the security properties of the TOE but rather the collection of information for further testing or that by their characteristics do not violate any asset or contradict the security functionality declared by the manufacturer in an evident way, the verdict will be assigned to PASS.

In those cases where the TOE presents vulnerabilities that are not exploitable in the operational environment of the TOE, either because of the action of the environmental hypotheses or because the time or capabilities required to exploit them exceed the time and effort restrictions of this certification, a PASS result will be established and the verdict of the PASS will be justified, creating a comment that will allow the manufacturer to improve the security of the product if he so wishes.

Security function	Test code	Objective	Result
All security functions	[STIC_OPNSENSE_IAD-2504-PT-0000]	Verify if it is possible to exploit CVE-2025-32728	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2504-PT-0100]	Verify if it is possible to bypass the 2FA verification performed by the TOE in the login page.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2504-PT-0110]	Verify if the “low” user (unprivileged user) is capable of perform actions (such as user management, firewall rules management…) that only administrator is allowed to.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2504-PT-0120]	Verify if it is possible to perform path traversal attacks on the TOE web interface.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2504-PT-0130]	Verify if the TOE web interface is vulnerable to IDOR.	**PASS**
SF. Trusted Communication Channels SF. Cryptographic requirements	[STIC_OPNSENSE_IAD-2504-PT-0200]	Verify if the TOE uses insecure communication mechanisms, weak cipher suites or weak key exchange groups when exchanging information through its communication channels	**PASS**

		with the TOE web GUI, update server and audit server.	
SF. Trusted Communication Channels SF. Trusted Administration SF. Identification and Authentication	[STIC_OPNSENSE_IAD-2504-PT-0210]	Verify if it is possible to bypass the restrictions to access the TOE through its SSH interface.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2504-PT-0300]	Verify if it is possible to perform XSS attacks on the TOE web interface.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2504-PT-0310]	Verify if it is possible to perform SSTI attacks on the TOE web interface.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2504-PT-0320]	Verify if it is possible to perform SQLI attacks on the TOE web interface.	**PASS**
SF. Protection of Credentials and Sensitive Data	[STIC_OPNSENSE_IAD-2504-PT-0400]	Verify if the JavaScript files stored in the TOE leak any sensitive information.	**PASS**
SF. Protection of Credentials and Sensitive Data	[STIC_OPNSENSE_IAD-2504-PT-0410]	Verify if it is possible to perform cache poisoning attacks on the TOE web interface.	**PASS**
SF. Trusted Administration SF. Identification and Authentication	[STIC_OPNSENSE_IAD-2504-PT-0500]	Verify if it is possible to change the TOE user's password without knowing the current password.	**PASS**
SF. Audit SF. Trusted administration	[STIC_OPNSENSE_IAD-2504-PT-0600]	Verify if it is possible to perform client IP spoofing attack on the TOE web interface.	**PASS**

SF. Identification and Authentication			
SF. Trusted Administration	[STIC_OPNSENSE_IAD-2504-PT-0700]	Verify if it is possible to perform a SSRF attack on the TOE web interface.	**PASS**

9.3 RESULTS

ID	Non-conformity	State
N/A	None.	N/A

ID	Comments	State
N/A	None.	N/A

10 REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation.

The last approved version must be considered which is published in the website of the Certification Body. (https://oc.ccn.cni.es).

[CCN-STIC-2001] Definition of the National Essential Security Certification (LINCE), version 2.0. March 2022.

[CCN-STIC-2002] Evaluation Methodology for the National Essential Security Certification (LINCE), version 2.0. March 2022.

[CCN-STIC-2003] Template for the Security Target of the National Essential Security Certification (LINCE), version 2.0. March 2022.

[CCN-STIC-807] Use of cryptology within the National Security Scheme (Esquema Nacional de Seguridad). May 2022.

[CEM] Common Methodology for Information Technology Security Evaluation: Evaluation Methodology.

The last approved version must be considered which is published in the website of the Certification Body. (https://oc.ccn.cni.es).

[listado_de_evidencias] List of evidence in which are included the reference, title, version, path and SHA-256 hash of the different evidence provided by the manufacturer for the evaluation.

[cPP-ND-30e] Collaborative Protection Profile for Network Devices Version 3.0e

[cPP-ND-30e-SD] Evaluation Activities for Network Device cPP Version 3.0e Supporting Document.

[IAR-10] Impact Analysis Report version 1.0

10.1 DEVELOPER EVIDENCES

The applicable developer evidence is listed in the latest version of the attached document [listado_de_evidencias].

11 ACRONYMS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
HTTPS	Hyper Text Transfer Protocol Secure
IDOR	Insecure Direct Object Reference
LINCE	National Essential Security Certification
MCF	Source Code Module
MEB	Biometric Evaluation Module
MEC	Cryptographic Evaluation Module
SQLI	SQL Injection
SSH	Secure Shell
SSRF	Server-Side Request Forgery
SSTI	Server-Side Template Injection
TIC	Information and Communications Technology
TLS	Transport Layer Security
TOE	Target Of Evaluation
XSS	Cross-Site Scripting