jtsec
BEYOND IT SECURITY

STIC Evaluation Technical Report

STIC_OPNSENSE_MEDIUM-2404
1.0
2024/08/29

jtsec
BEYOND IT SECURITY

CHANGELOG

Version	Date	Author	Reason	Changes
1.0	2024/08/29	DAT	Document creation.	First version.

INDEX

1 INTRODUCTION

This document is the National Essential Security Certification (LINCE) 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_MEDIUM-2404-ETR-v1.0
ETR version	1.0
Author or authors	DAT
Reviewer	ACP
Approved by	JTG
Start date of the works	2024/08/27
End date of the works	2024/08/29
CB dossier code	N/A
Laboratory project code	STIC_OPNSENSE_MEDIUM-2404
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	24.4.1_3
Operating manuals of the product	[OPNSENSE-DOCS-D971B9D]

2 TOE DESCRIPTION

The information in this section is provided by the manufacturer in the latest version of its Security Target.

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 (over TLSv1.2 or higher).

2.2 INVENTORY OF SECURITY FUNCTIONS

This evaluation takes as a baseline the LINCE evaluation carried out for the same TOE that is the subject of this STIC evaluation, OPNsense Business Edition. This LINCE evaluation has been carried out in accordance with the Security Target [ST-08], which is essentially based on [CCN-STIC-140-D3M].

The evaluator has considered the Impact Analysis Report [IAR-10] when defining the requirements to be tested in this evaluation. Those requirements that have been affected by changes in the product from the version evaluated in the LINCE to the initial version of this STIC evaluation will be retested.

Therefore:

1. A coverage analysis has been carried out, considering [ST-08] and [IAR-10].
2. The SFRs to be evaluated have been defined according to the TOE version of this assessment.

The analysis performed is included in the following table:

Requirement from [ST-08]	Retested in the present evaluation?
ADM.1	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
ADM.2	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
ADM.3	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
IAU.1	**Not covered**, requirement to test in the present STIC evaluation. Functionality was evaluated in LINCE evaluation (IAU.1 requirement) but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity. Related change is described as "*system: prevent activating shell for non-admins*".
IAU.2	Considered covered since changes introduced and described in [IAR-10] are not related to the

	functionality described; therefore, retesting is not considered necessary.
IAU.3	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
IAU.4	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
COM.1	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
COM.2	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
COM.3	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
COM.4	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
CIF.1	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
ACT.1	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
ACT.2	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
ACT.3	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
AUD.1	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.

AUD.2	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
AUD.3	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
AUD.4	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
AUD.5	**Not covered**, requirement to test in the present STIC evaluation. Related requirement AUD.5 was evaluated in LINCE evaluation but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity. Related changes are described as "*system: fix maximum log file size being ignored when there is only one file*" and "*system: make log rotate action available to Cron*".
PSC.1	**Not covered**, requirement to test in the present STIC evaluation. Functionality was evaluated in LINCE evaluation (PSC.1 requirement) but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity. Related change is described as "*system: limit file system /conf/config.xml and backups access to administrators*".
FWL.1	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
FWL.2	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
FWL.3	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.
FWL.4	Considered covered since changes introduced and described in [IAR-10] are not related to the functionality described; therefore, retesting is not considered necessary.

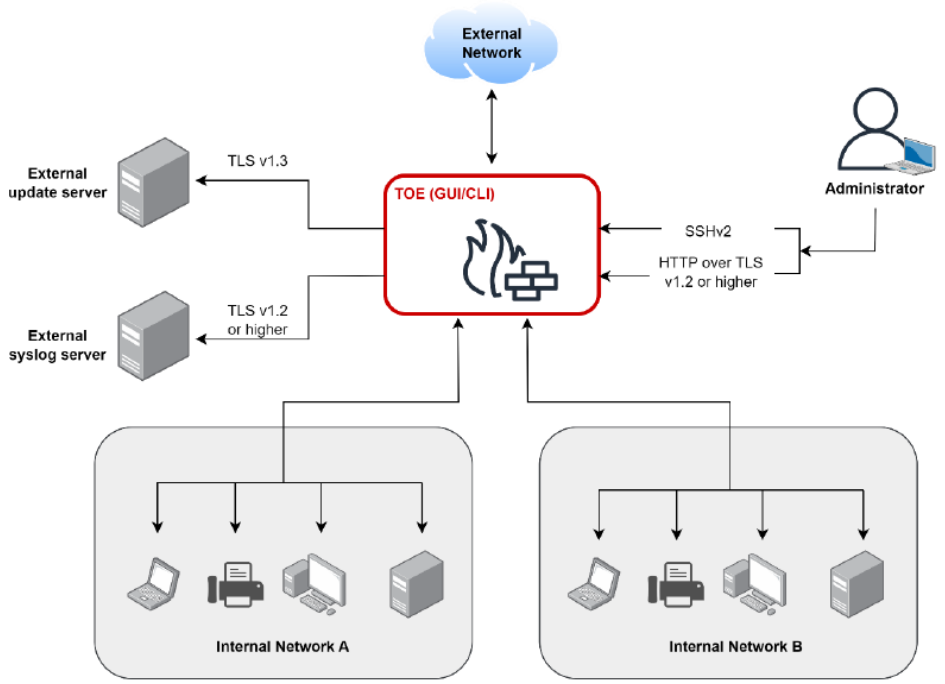
Given the previous analysis, the requirements to verify in the present report are the following:

Requirement	Description
IAU.1	The TOE shall identify and authenticate every user through username and password before grating access to the GUI and administrative users through the CLI interfaces.
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.
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.

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

The present STIC evaluation for the product OPNsense Business Edition has been carried out following the LINCE methodology in order to verify if the product covers a set of requirements declared in the Security Target from a past LINCE evaluation. The main purpose of the present evaluation is to verify if such requirements are still met in the version 24.04.1_3 of the TOE and identify any deviation.

In order to define the requirements to retest in the present STIC evaluation, the evaluation has taken the Security Target from the previous LINCE evaluation for OPNsense Business Edition version 23.10 ([ST-08]) as a baseline. Given the requirements in such Security Target, the changes introduced in the product are analysed with the objective of determining which requirements need to be retested; these are the ones whose functionality are impacted by a change included throughout product versions up to the TOE version in the current evaluation [TOE-2441_3]. The analysis and definition of the requirements is included in section 2.2 Inventory of security functions. Briefly, only the requirements IAU.1, AUD.5 and PSC.1 are considered in need of retesting, given a few changes included in the product as defined in the manufacturer's changelogs.

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.

The installation procedure does not reveal any non-conformities, the procedure remains the same as described in LINCE Security Target [ST-08]. It just differs in one aspect, the indications related to the modification of permissions related to the configuration file /conf/config.xml are not followed as it would not make sense to manually change such permissions since [IAR-10] reveals a change that suggests that such permissions are applied by default. Therefore, the permissions are unmodified, and they are analysed in the functional test related to the pertinent requirement.

Since most of the changes reviewed and defined in [IAR-10] are deemed not related to most of the requirements, only a few requirements are considered in necessity of retesting. The execution of these functional tests reveals the following:

- [TOE-2441_3] does not meet the requirement IAU.1 as described in the Security Target [ST-08] which is taken as an initial reference for the present evaluation. The test reveals that not every user is now able to access all interfaces, local access through the CLI/SSH interface is not allowed for non-administrator users. This behaviour is deemed not consistent with IAU.1; therefore, the non-conformity OR01.NC01 is generated. This behaviour is not considered conflictive security-wise since it is more restrictive, only administrative users are allowed to access the TOE locally. In order to address this inconsistency, the definition of the requirement declared in section 2.2 Inventory of security functions of the present report is refined to express accurately the behaviour of the TOE and the non-conformity is deemed closed.

After executing the functional tests, the vulnerability analysis was conducted. This phase mainly involves the review of public vulnerabilities related to the TOE and its third-party components or libraries. This analysis does not reveal public vulnerabilities (CVE) that could affect the TOE at the date this report is developed.

It is worth noting that vulnerabilities related to the evaluated functionality have not been considered or identified, given that the functionality tested in the present evaluation is minimal and most functionality remains the same as in the previous LINCE evaluation and additional functionality has not been added. For this reason, penetration tests have been dismissed in the present evaluation. Since no penetration tests are performed, the sections related to such tasks are not included in the present report.

Given the results obtained in the present evaluation, it is deemed that [TOE-2441_3] meets ENS medium category and the evaluation is assigned a **PASS** verdict.

5 VERDICT OF THE EVALUATION

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

The TOE installation phase does not reveal any non-conformity.

The functional test phase does not reveal any non-conformity.

The vulnerability analysis does not reveal any non-conformity.

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

Documents used during installation	[OPNSENSE-DOCS-D971B9D]
Evaluator	DAT
Days required	1 day.
Date	2024/08/29
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 [ST-08] and [OPNSENSE-DOCS-D971B9D].

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

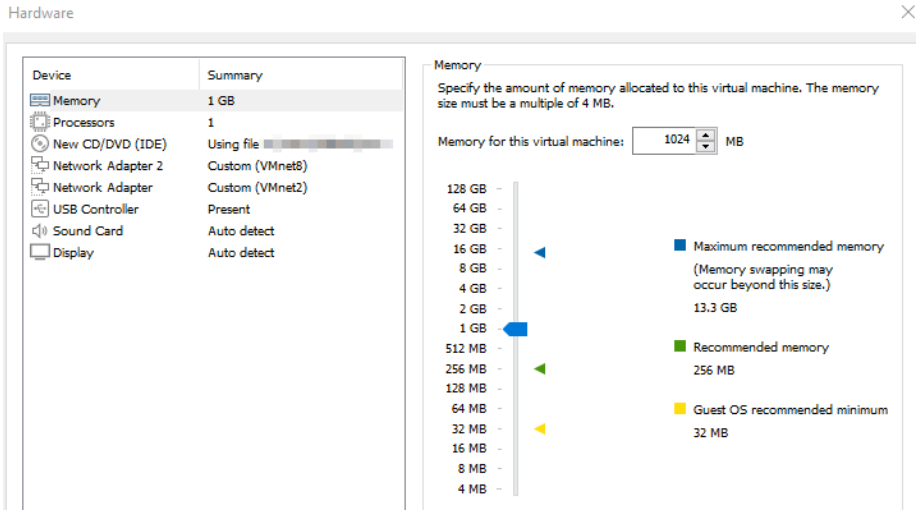
The test scenarios are described in section *11 Annex A: Test scenarios*.

6.3 DESCRIPTION OF THE INSTALLATION AND CONFIGURATION OF THE TOE INSTALLATION

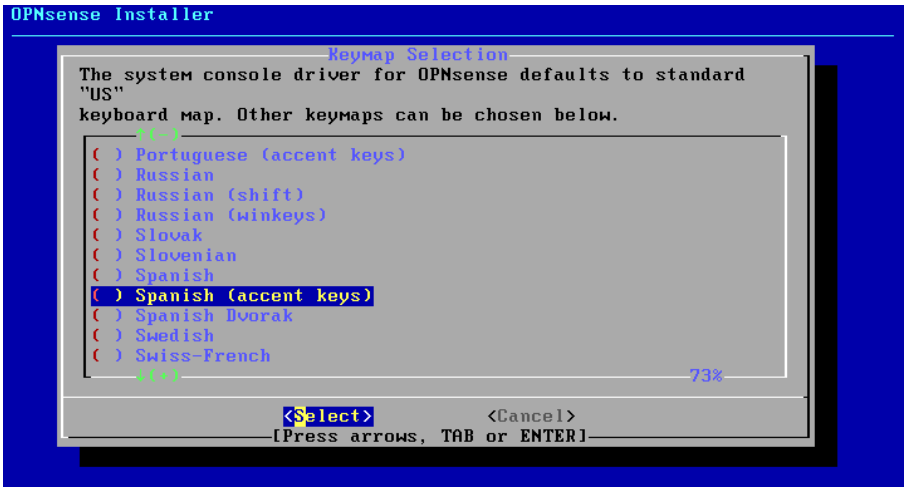
To perform the installation, the steps needed are the following:

1. Open VMware and click on Create a new virtual machine.

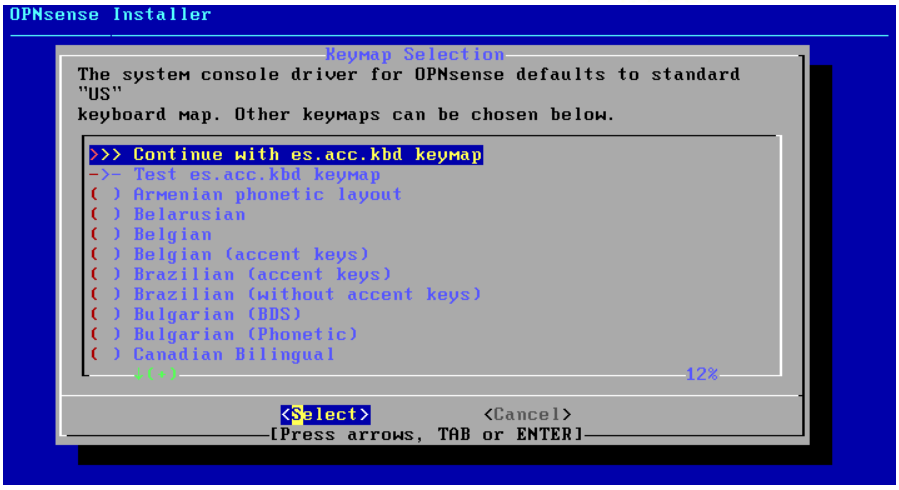
2. Select [TOE-ISO-2404] and click on “Next”.
3. Give a name to the virtual machine and click on “Next”.
4. Set 30GB as disk size.
5. Click on Customize Hardware → Memory and set 1GB of RAM memory. Add a network adapter and configure the virtual networks as shown (“Network Adapter” set to VMnet2 and “Network Adapter 2” set to VMnet8).



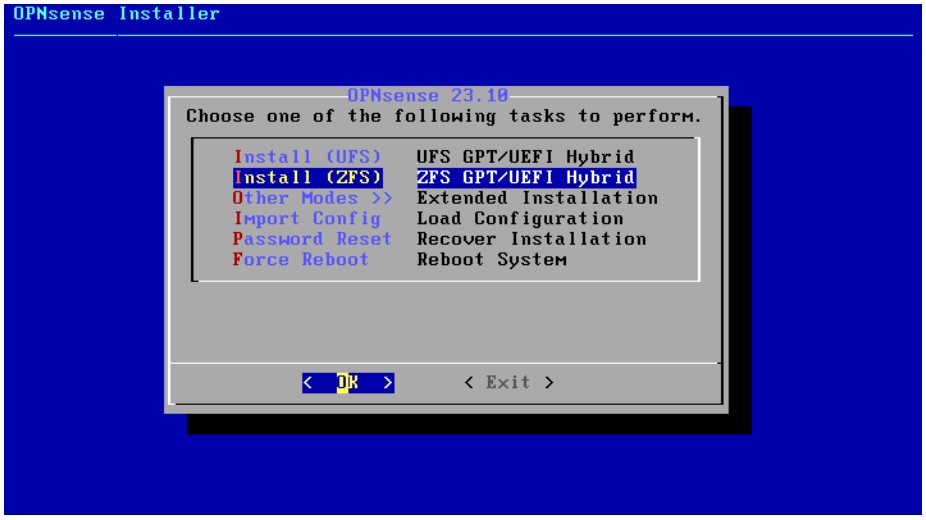
6. Press “Close”.
7. Click on “Finish”.
8. Wait for the TOE to boot up.
9. In order to install the TOE, log in with the user “installer” and authenticate with the password “opnsense”.
10. Select the keyboard layout.



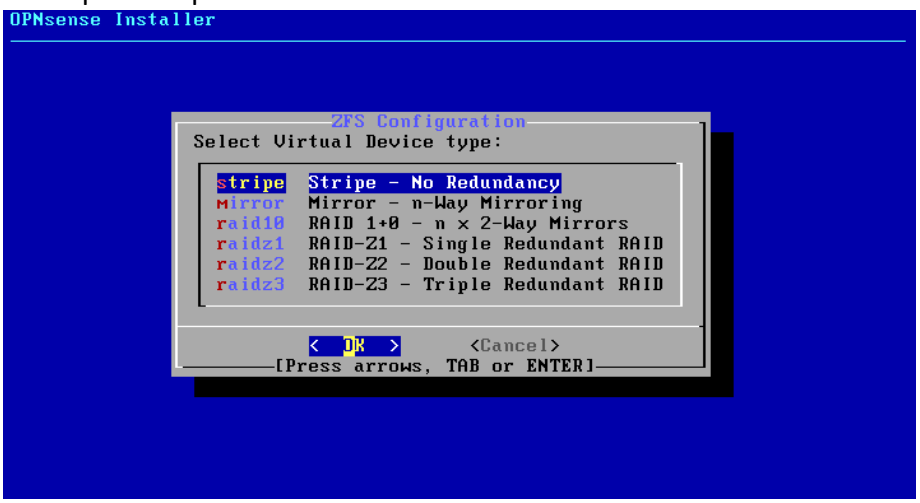
11. Indicate “Continue with…”.



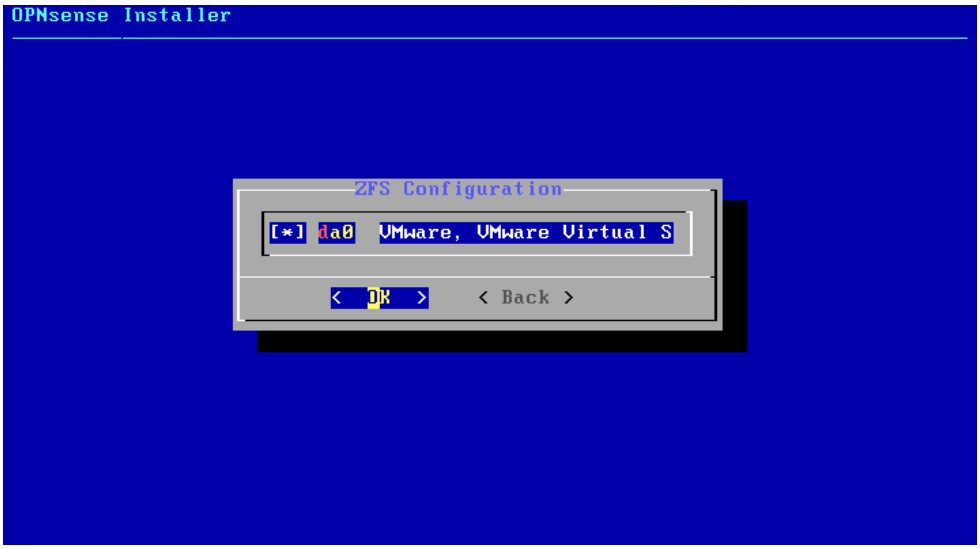
12. Select “Install (ZFS)” and press Enter.



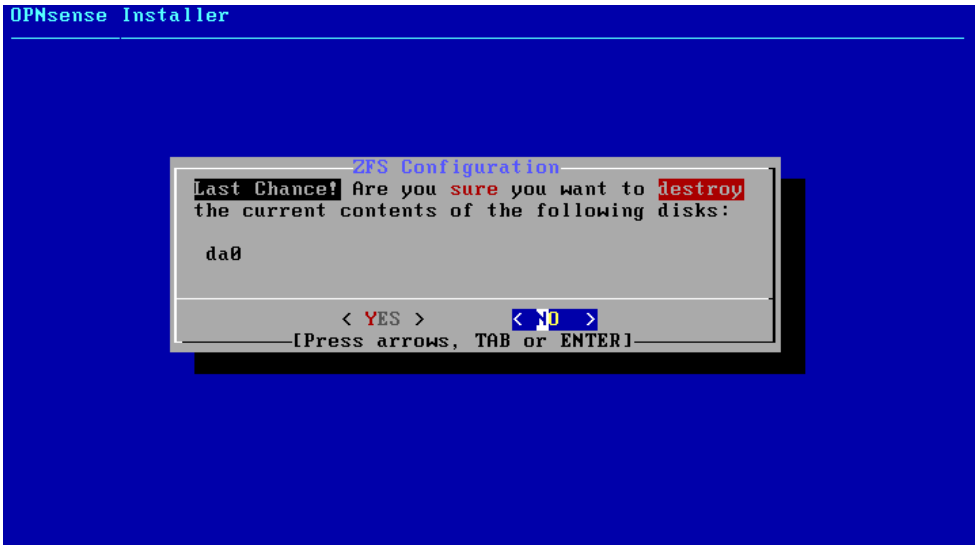
13. Select “stripe” and press Enter.



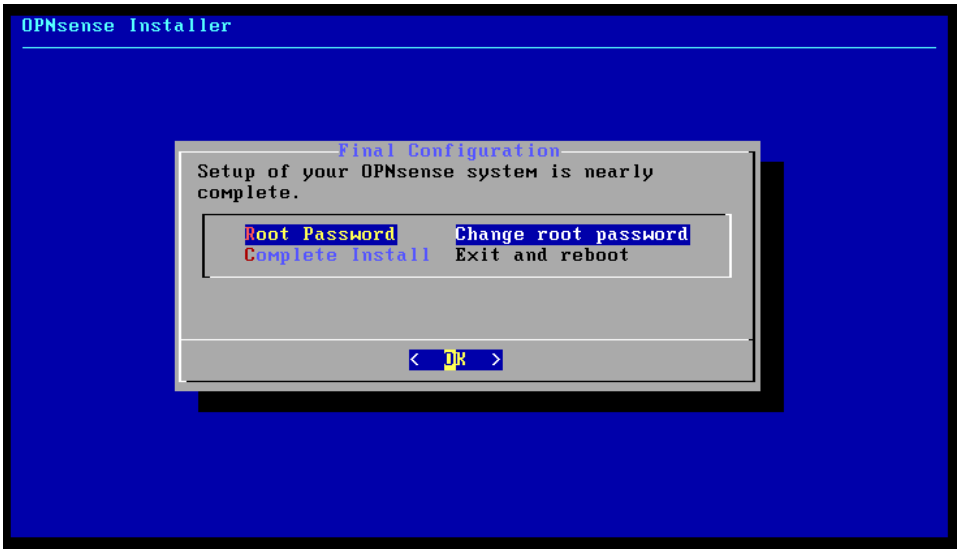
14. Select the virtual disk and press OK.



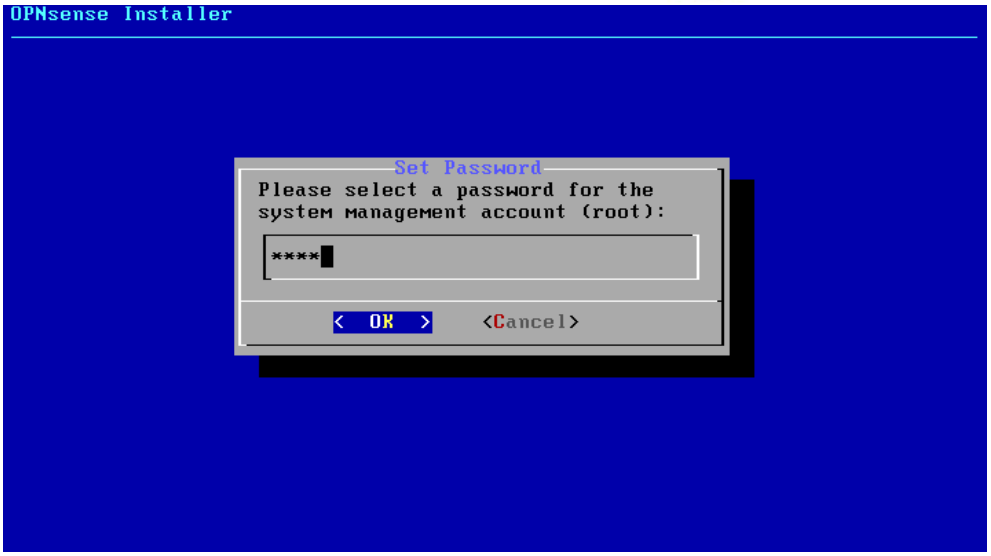
15. Select Yes and press Enter.



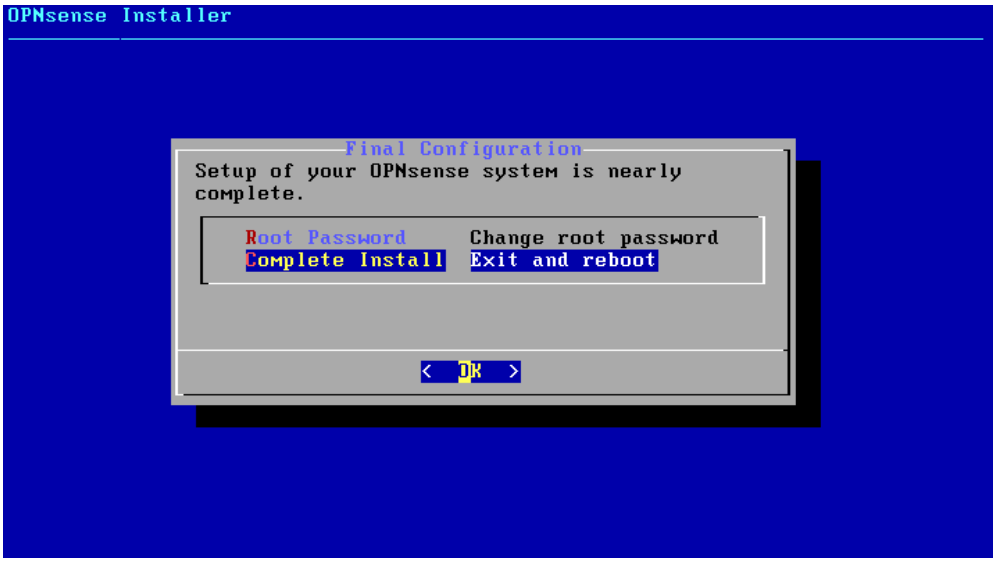
16. Select “Change root password” and press OK.



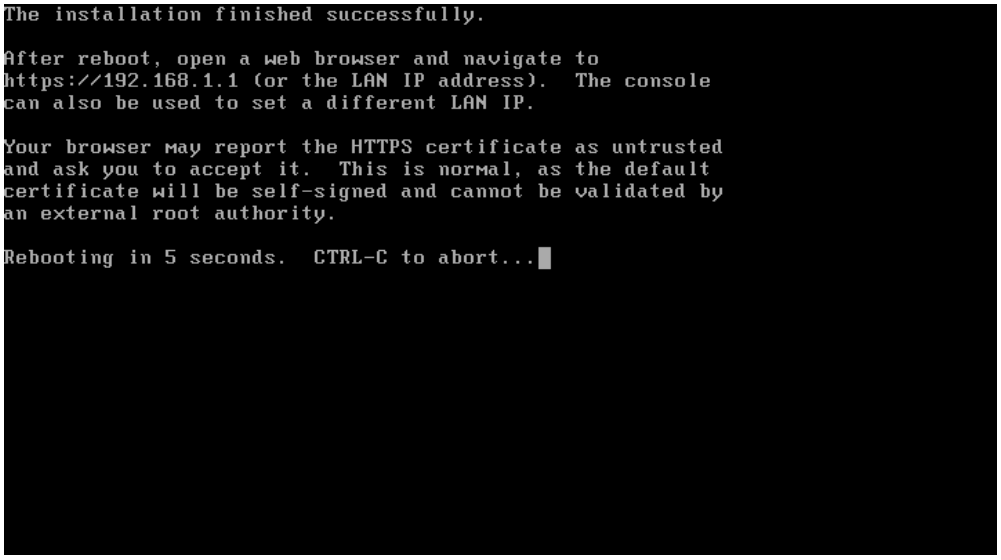
17. Define a new password for the root user.

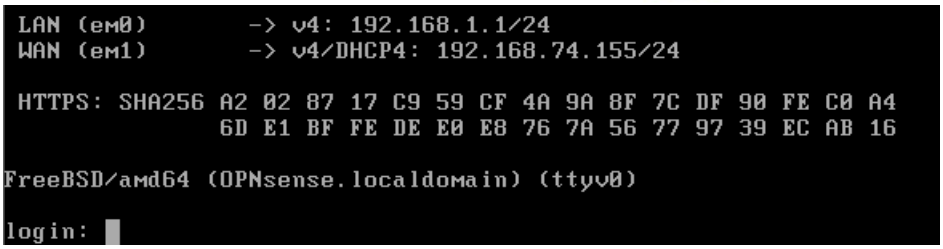


18. Select “Complete Install” and press OK.

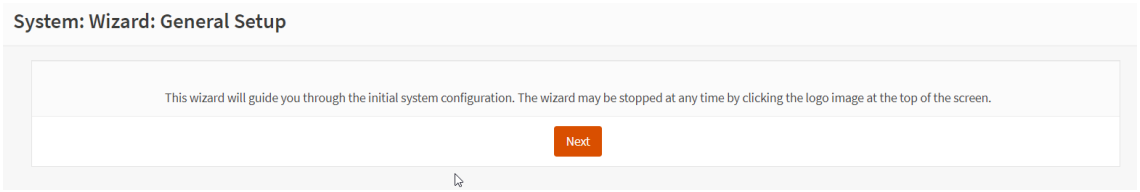


19. Wait for the TOE to reboot and navigate to the web interface.

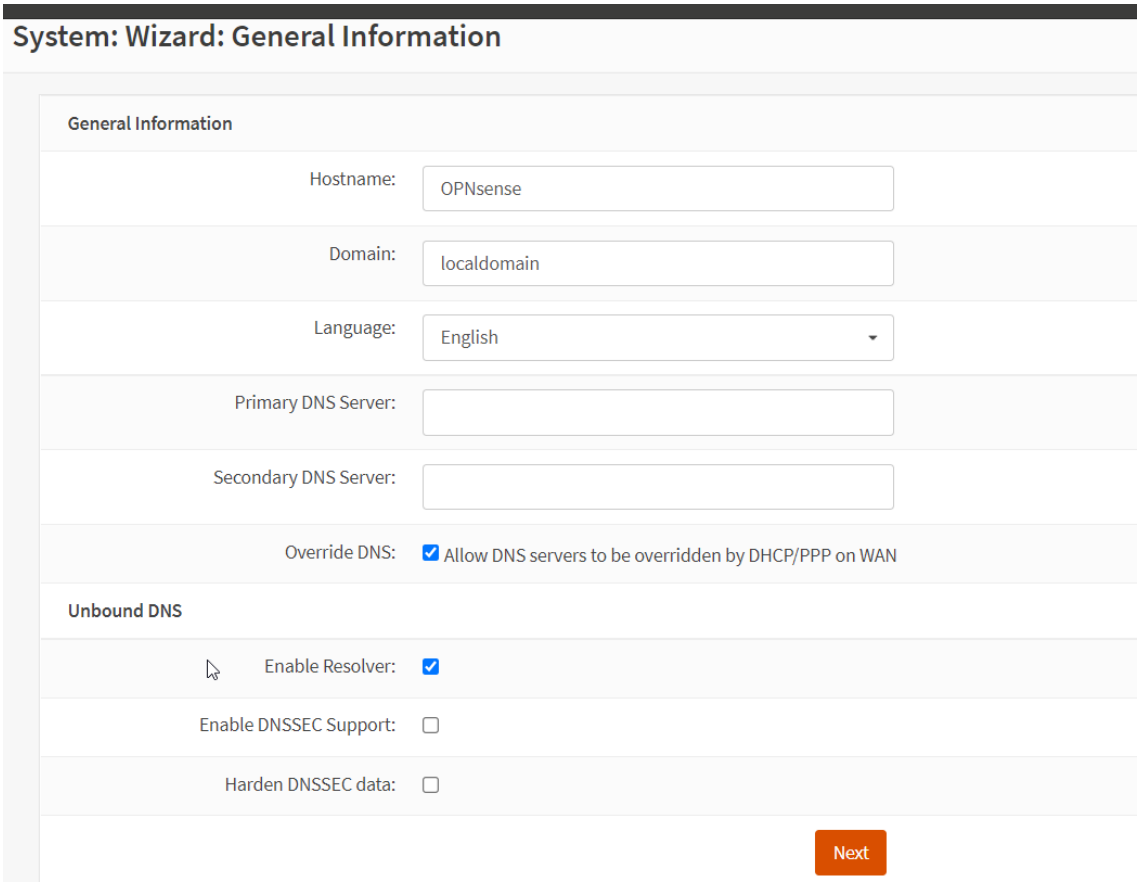




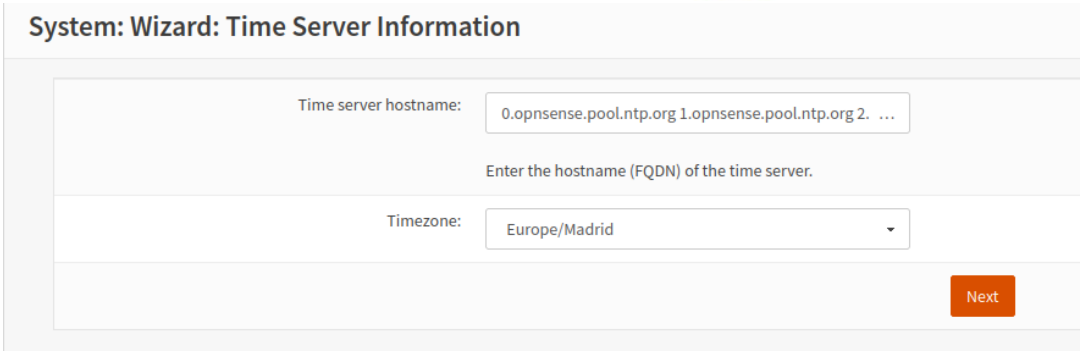
20. Access the LAN IP address through HTTPS using a web browser and log in with the root user credentials.
21. Follow the wizard setup, press Next.



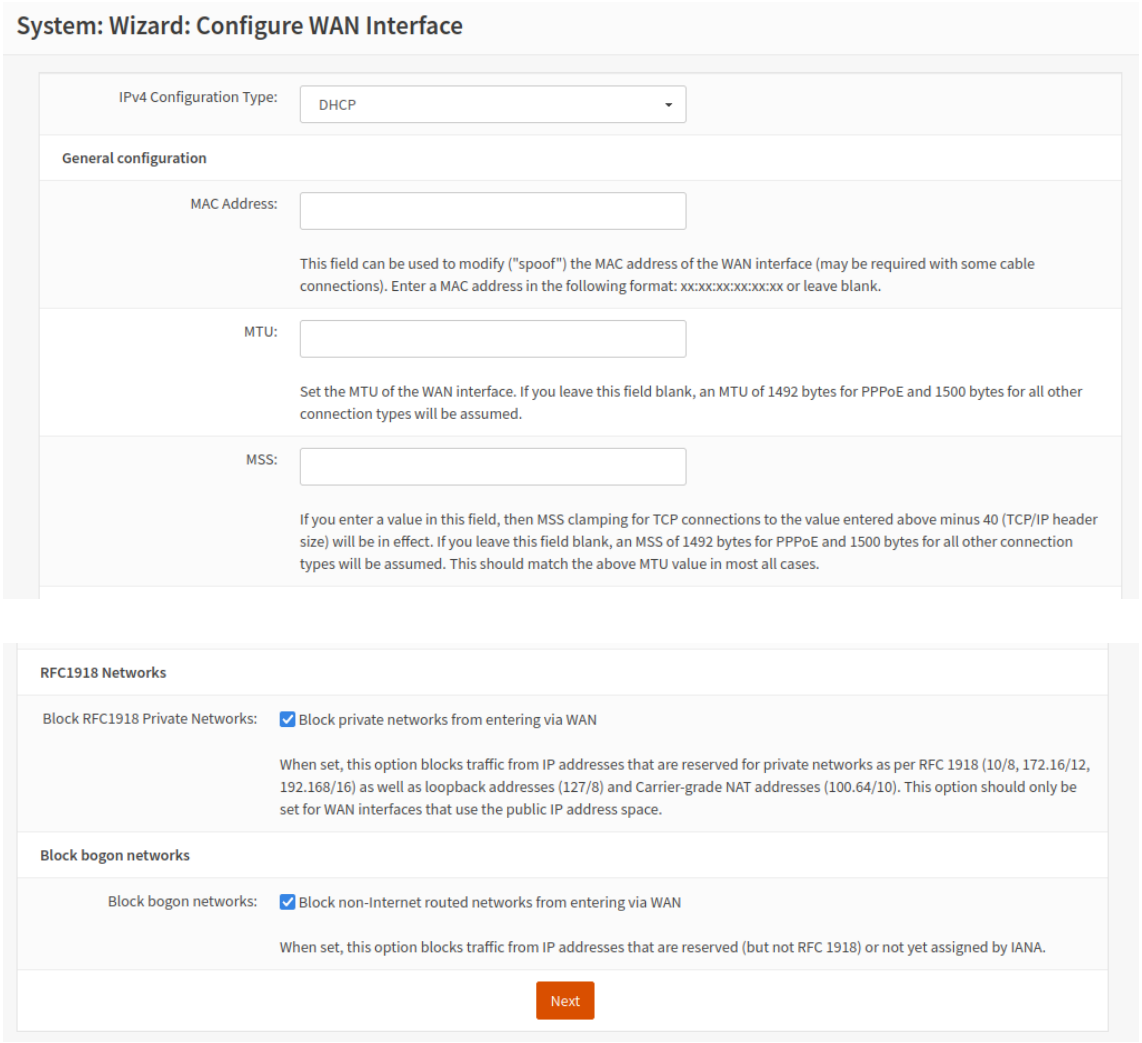
22. Give a hostname and a domain to the TOE and press Next.



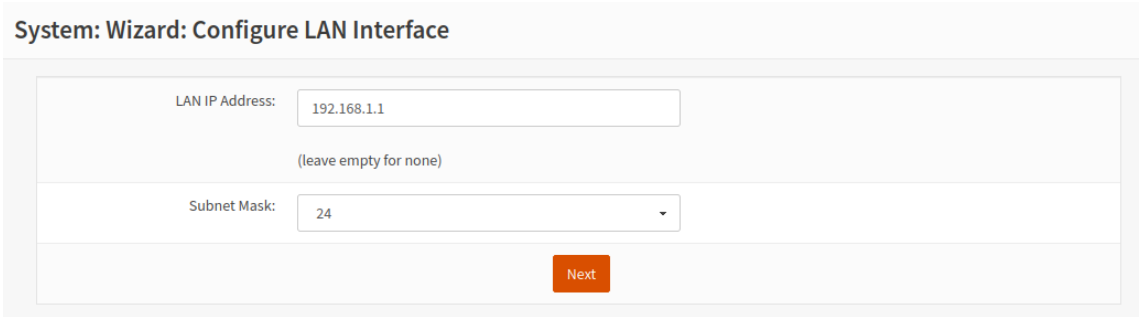
23. Set NTP servers and the time zone. In this case the NTP servers configured are the ones offered by default. Press Next.



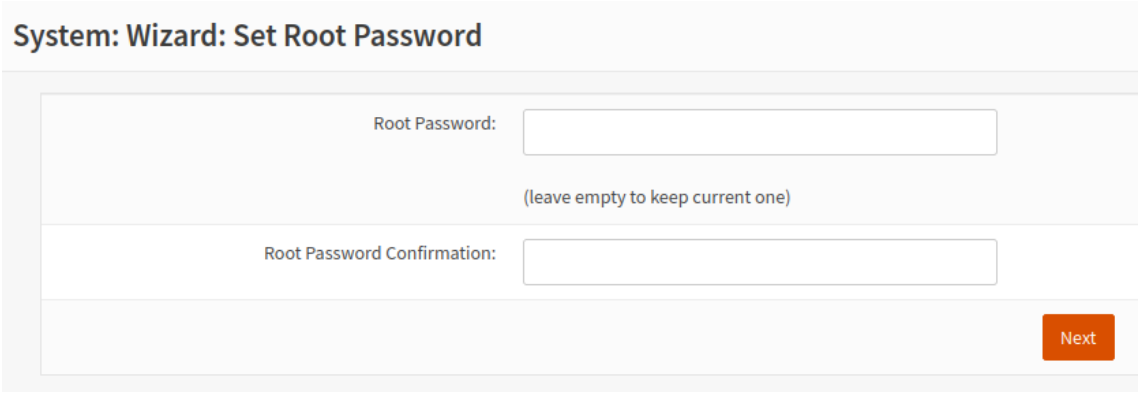
24. Leave the default configuration for the WAN interface and press Next.



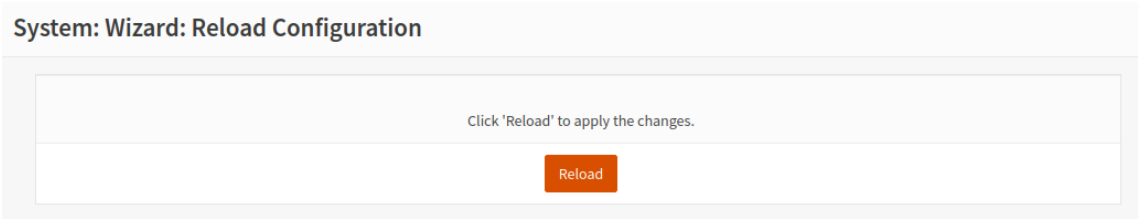
25. Leave the default configuration for the LAN interface and press Next.



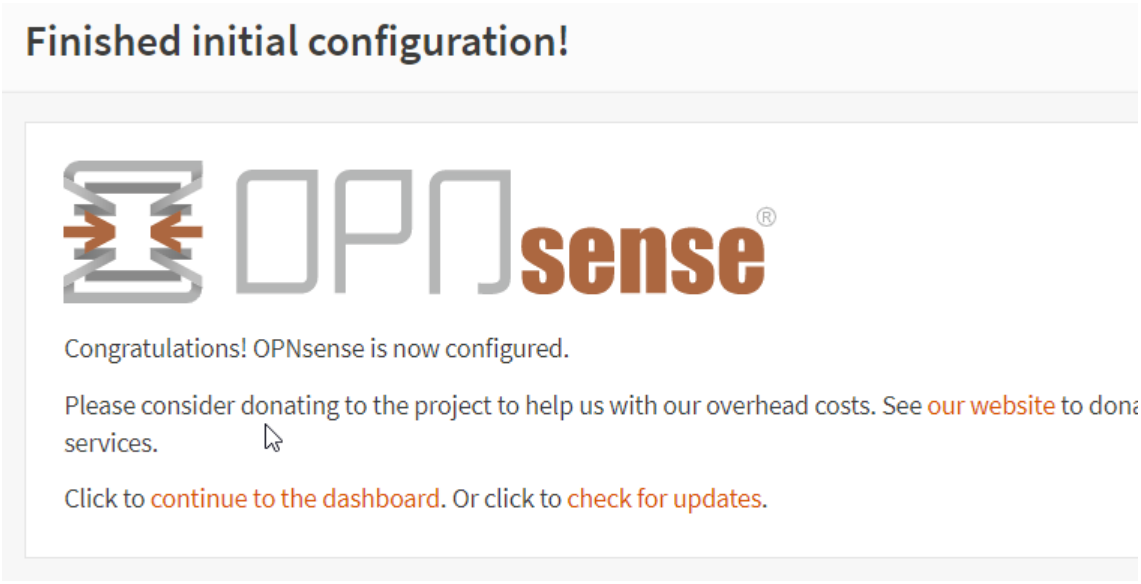
26. Set a new root password if it was not changed before.



27. Click on reload to apply the changes.



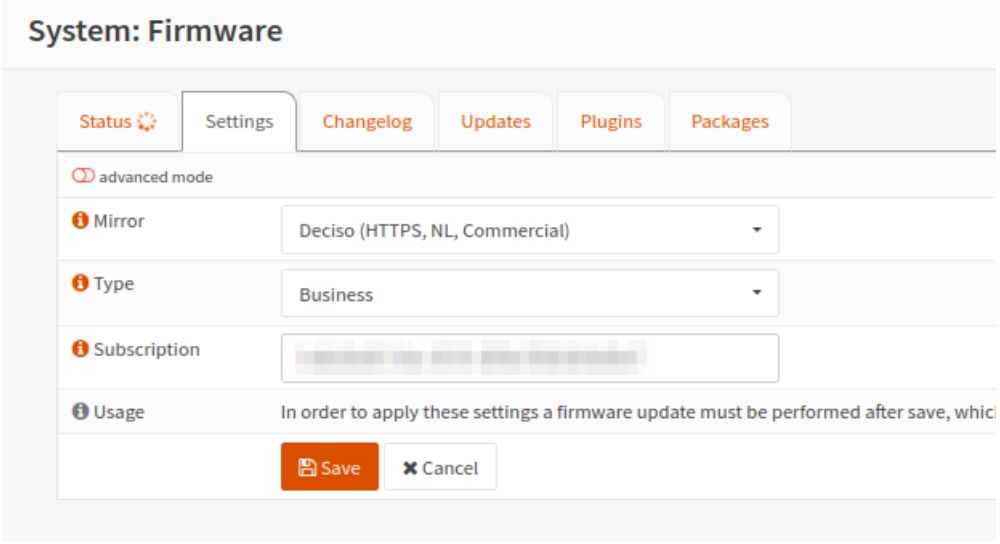
28. The TOE is now configured and ready.



6.3.1 SETTING A SUBSCRIPTION KEY

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

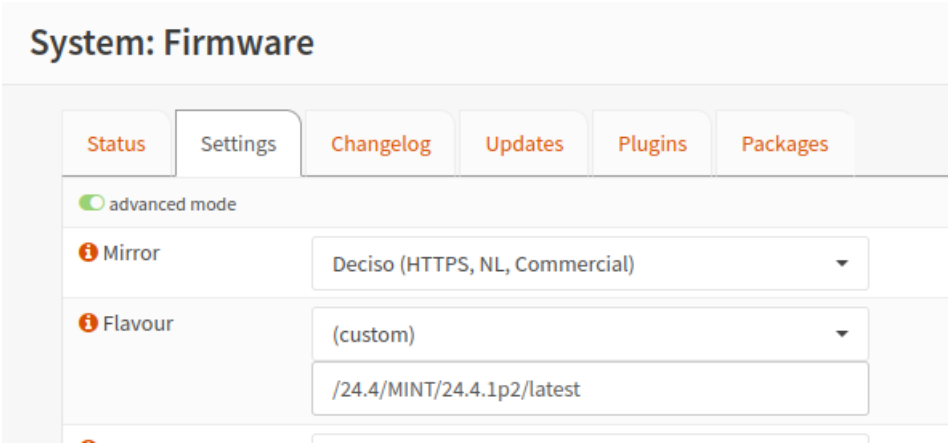
1. Log in through the TOE web interface with the root user.
2. Go to System → Firmware → Settings.
3. Indicate the Subscription key in the Subscription text box and click Save.



6.3.2 UPDATING TO 24.04.1_3 VERSION

The TOE version in the present evaluation is 24.04.1_3, after installing the TOE it is required to update to such version:

1. Log in through the TOE web interface with the root user.
2. Go to System → Firmware → Settings.
3. Toggle "Advanced mode".
4. Indicate "/24.4/MINT/24.4.1p2/latest" in the Flavour parameter and click Save.

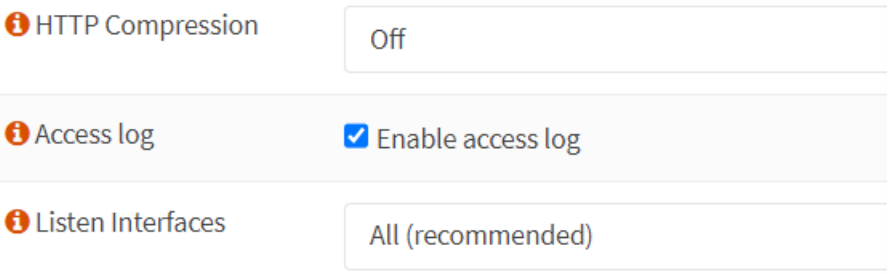


5. Go to the Status tab and click Check for updates.
6. Click Update.
7. Wait for the update to be installed.

6.3.3 ENABLING ACCESS LOGS

After installing the TOE, given the indications in the Security Target, the following steps are required through the web interface:

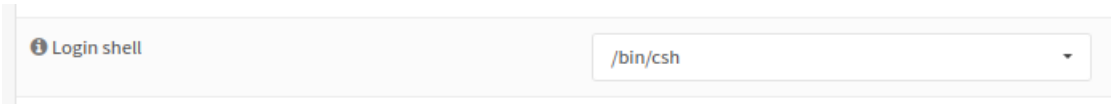
1. Enable the access log parameter in the Settings menu. In the left panel go to System → Settings → Administration and select “Enable access log”.



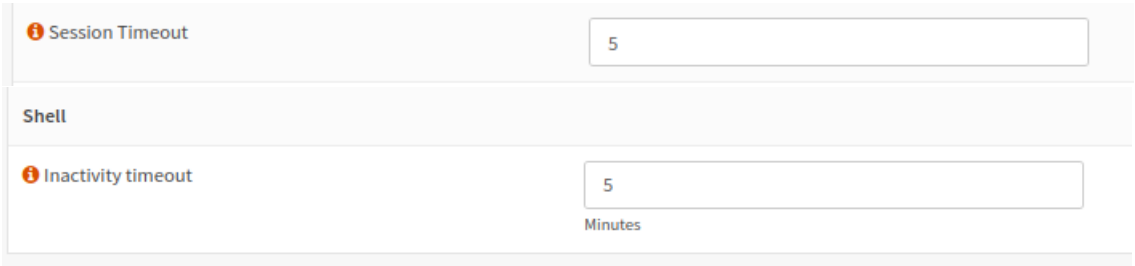
6.3.4 CHANGE SHELL TYPE AND INACTIVITY TIMEOUT

For the inactivity session timeout to work, it is required to change the login shell assigned to the user as indicated in the Security Target. The Security Target also indicates to change the session/inactivity timeout to 5 minutes. The steps below are followed:

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

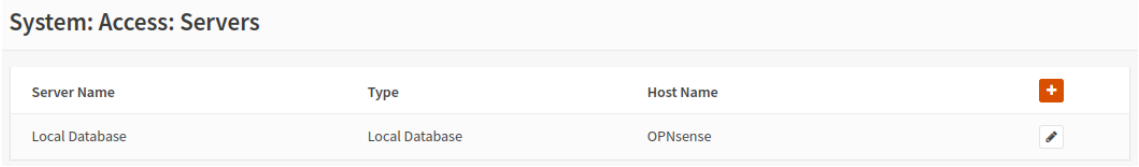


4. Go to System → Settings → Administration.
5. Set the "Session Timeout" and "Inactivity timeout" parameters to 5 minutes in order to set the inactivity timeout for the GUI and CLI interfaces.

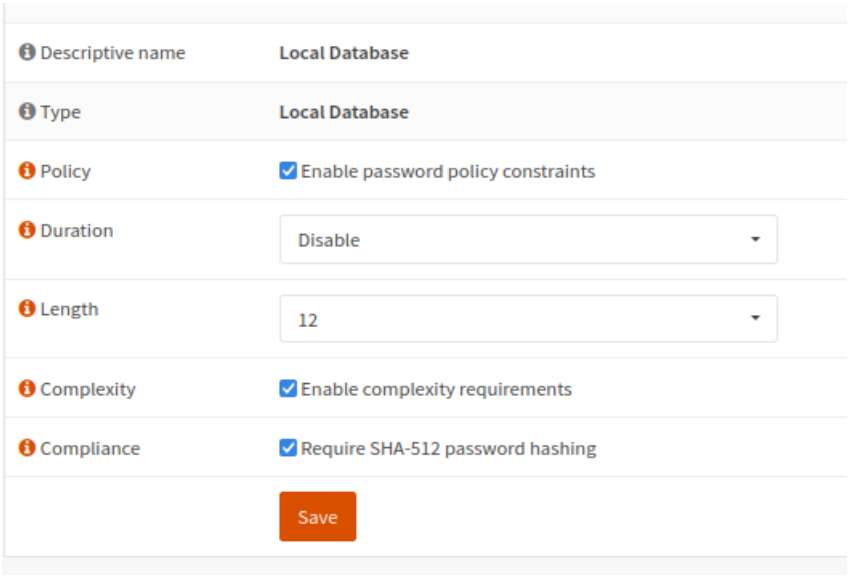


6.3.5 DEFINING A PASSWORD POLICY

1. Log in through the TOE web interface with the root user.
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 and enable complexity requirements.



5. Save the changes.

6.3.6 ADD 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 as described in the Security Target:

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. Create the file ACL.xml with the following content in order to create the new read-only audit role.

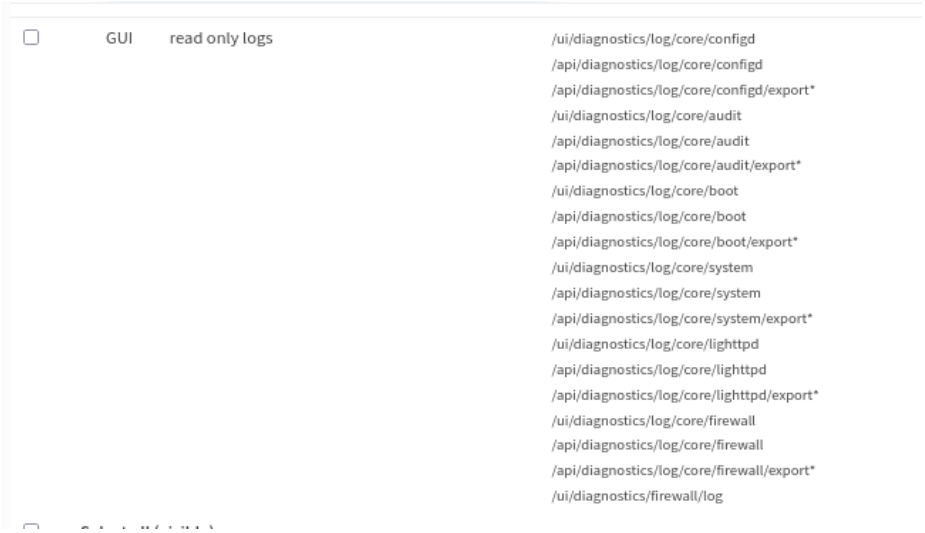
```
<acl>
    <page-diagnostics-logs-read-only>
        <name>read only logs</name>
        <patterns>
            <!-- System: Log Files: Backend -->
                <pattern>ui/diagnostics/log/core/configd</pattern>
                <pattern>api/diagnostics/log/core/configd</pattern>
              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

3. 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.



6.3.7 DISABLE ROOT USER FOR SSH

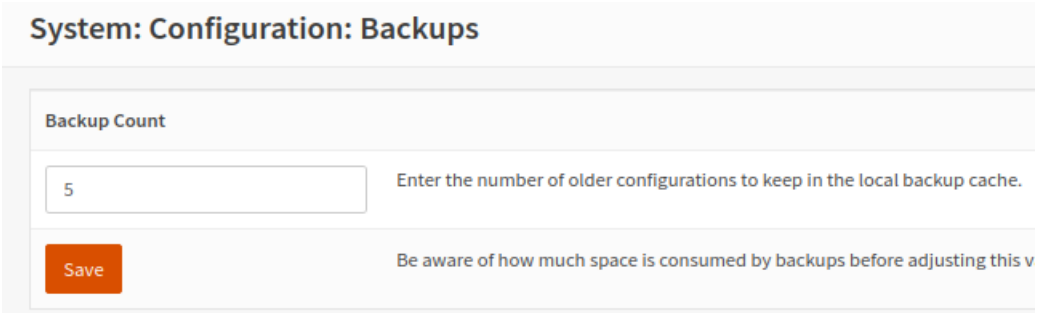
The Security Target indicates that it is required to disable root access to the CLI through SSH. The steps below are followed:

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

6.3.8 CONFIGURE SYSTEM BACKUPS ROTATION

The Security Target indicates that it is necessary to define a specific number of configuration backups to preserve. The steps below are followed:

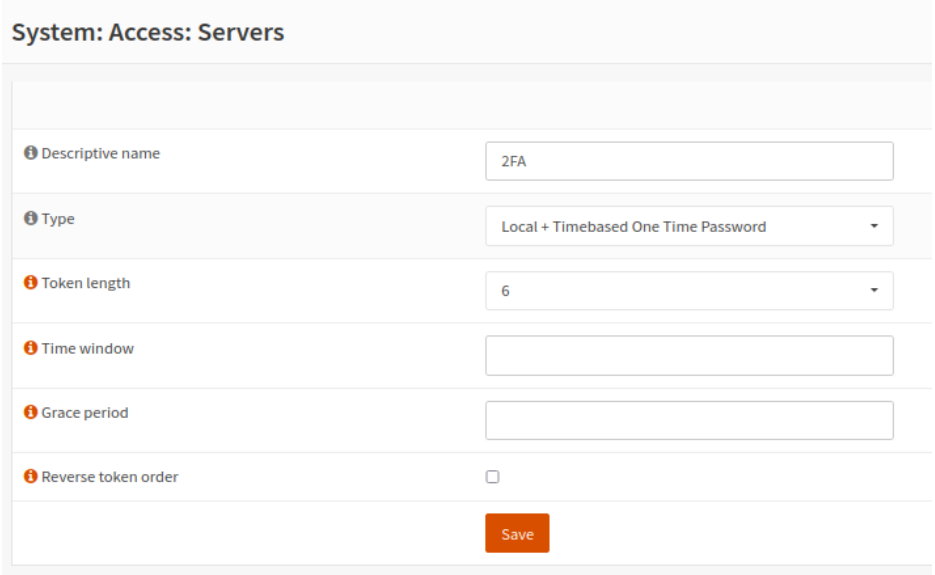
1. Log in through the TOE web interface with the root user.
2. Go to System → Configuration → Backups.
3. Configure the "Backup Count" parameter to 5.



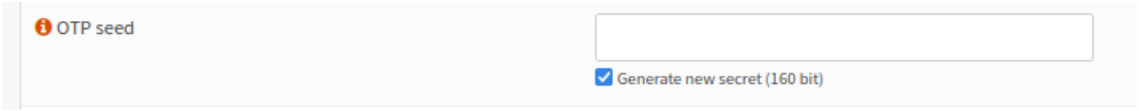
6.3.9 CONFIGURE TWO-FACTOR AUTHENTICATION

The Security Target indicates that it is required to configure a 2FA as part of the user configuration process. The steps below are followed:

1. Go to System → Access → Servers
2. Click Add server in the top right corner.
3. Create a new server with the following parameters.

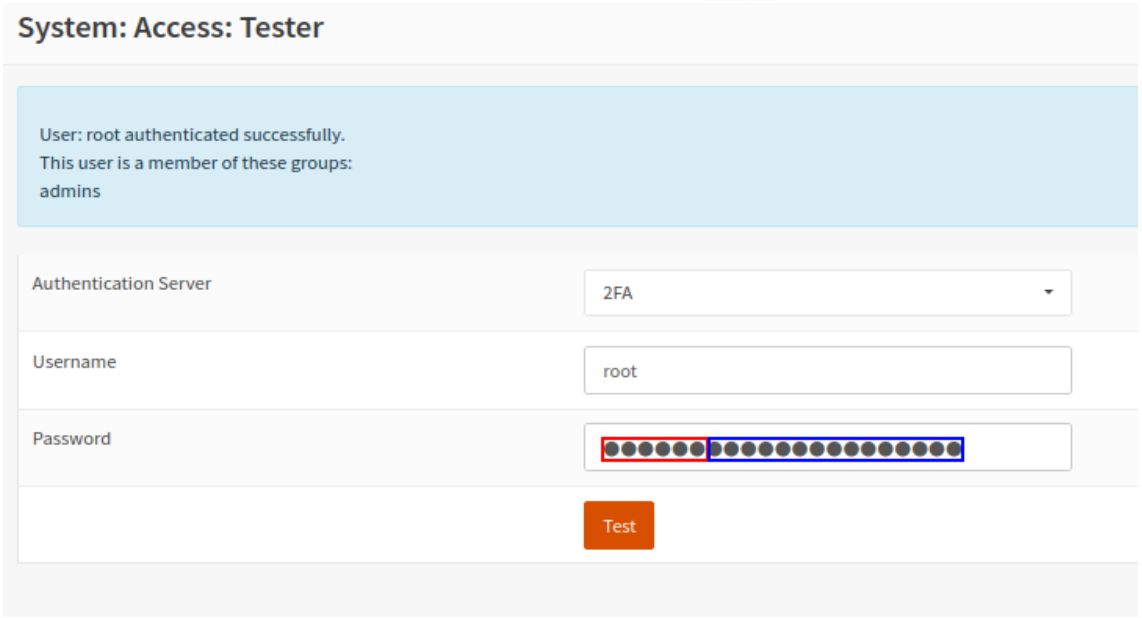


4. Install a Google Authenticator compatible app on your device.
5. Go to System → Access → Users.
6. Edit the root user.
7. Select "Generate a new secret (160 bit)" in the OTP parameter and click Save

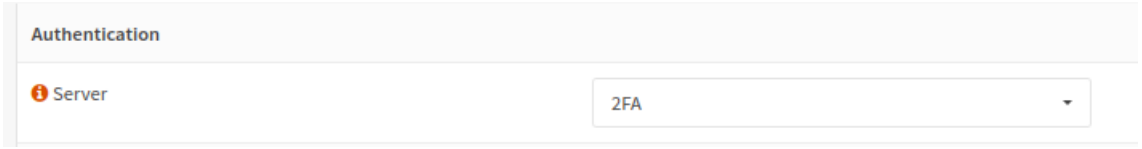


8. Edit again the root user to view the seed and QR, register such token or QR code in the Google Authenticator compatible app.

9. Go to System → Access → Tester.
10. Verify that the 2FA authentication is properly configured concatenating the authenticator code and the user password "<CODE><PASSWORD>".



11. Go to System → Settings → Administration.
12. Change the Authentication server by selecting the "2FA" server that was just created in the dropdown menu.



6.3.10CONFIGURING CONFIGD ACCESS CONTROL

In order to prevent local non-authorized interaction with the configd backend service, the steps below are followed as described in the Security Target:

1. Log in through the TOE CLI interface with the root user.
2. Execute the following command to create a new directory:

```
mkdir /usr/local/opnsense/service/conf/configd.conf.d
```

3. Add the file lockdown.conf in the previous directory with the following content:

```
[action_defaults]

allowed_groups = wheel
```

4. After the file is created, run the following command:

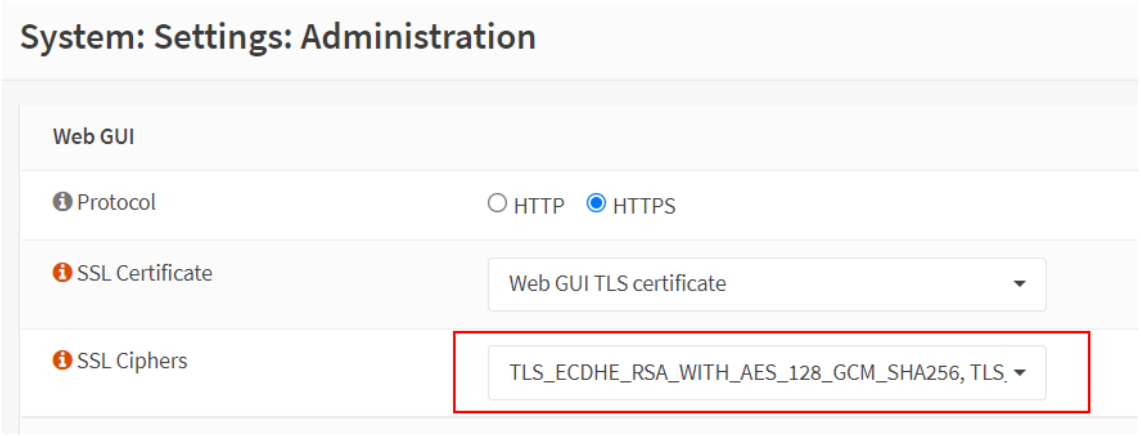
```
service configd restart
```

6.3.11WEB INTERFACE TLS CIPHER SUITES CONFIGURATION

In order to meet the cryptographic requirements and conform [CCN-STIC-807] as declared in the Security Target, it is required to configure accepted 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 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 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.

6.3.12SSH CRYPTOGRAPHIC PARAMETERS CONFIGURATION

In order to meet the cryptographic requirements and conform [CCN-STIC-807] as declared in the Security Target, it is required to configure accepted 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 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.
   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

2. Scroll down and click Save.

6.3.13SYSLOG CLIENT TLS CIPHER SUITES CONFIGURATION

In order to meet the cryptographic requirements and conform [CCN-STIC-807] as declared in the Security Target, it is required to configure accepted cipher suites through the local command line interface. This configuration affects the TLS connections when the TOE communicates with a remote syslog server. The steps below are followed:

1. Log in through the TOE local command line and select the Shell option.

```
 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: 8
```

2. Edit the file `/usr/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-SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES128-CCM")`

```
{%            if destination.transport in ['tls4', 'tls6'] %}
        tls(
                ca-file("/etc/ssl/cert.pem")
                key-file("/usr/local/etc/syslog-ng/cert.d/{{dest_key}}.key")
                cert-file("/usr/local/etc/syslog-ng/cert.d/{{dest_key}}.crt")
                ssl-options(no-sslv2, no-sslv3, no-tlsv1, no-tlsv11)
                cipher-suite("ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:TLS_AES_128_GCM_SHA25
6:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES128-CCM")
        )
{%            endif %}
    );
{%          endif %}
};
```

4. Save the file.

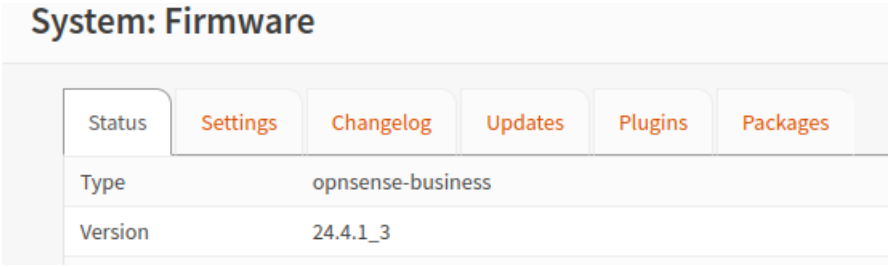
6.3.14INSTALLING CERTIFICATES FROM TRUSTWORTHY CA

In the Security Target, it is recommended to install a digital certificate signed by a trusted CA. However, a self-signed certificate generated by [TOE-2441_3] itself is used in this evaluation, as it does not imply a degradation in the quality level at the functionality or testing of [TOE-2441_3]. This matter is considered by the evaluator when conducting the testing.

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.
3. Check the version number identifier.



6.5 USED INSTALLATION OPTIONS

The selection of different installation 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	DAT
Days required	1 day.
Date	2024/08/29
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
SF. Identification and Authentication IAU.1	[STIC_OPNSENSE_MEDIUM-2404-TST-ND-0010]	Verify that the TOE identifies and authenticates users through username and password as defined in the description of the requirement.	**PASS**
SF. Audit AUD.5	[STIC_OPNSENSE_MEDIUM-2404-TST-ND-0020]	Verify that the TOE overwrites previous audit records according to the maximum log file size and	**PASS**

		number of logs to be kept defined.	
SF. Protection of credentials and sensitive data PSC.1	[STIC_OPNSENSE_MEDIUM-2404-TST-ND -0030]	Verify that the TOE stores credentials and private keys as declared in the requirement.	**PASS**

7.1.3 RESULTS

ID	Non-conformity	State
OR01.NC01	[STIC_OPNSENSE_MEDIUM-2404-TST-ND-0010] SF. Identification and Authentication IAU.1 The requirement IAU.1 of [ST-08] declares the following: "*The TOE shall identify and authenticate every user through username and password before grating access to the GUI and CLI interfaces.*". The test related to the present non-conformity reveals that [TOE-2441_3] does not allow every user to access the CLI/SSH interface, such access is now completely disabled and cannot be reenabled. Therefore, the requirement is considered inconsistent with the behaviour of the TOE. The description of the requirement was refined to express the behaviour of [TOE-2441_3] accurately, the requirement now differentiates between administrative and normal users. This behaviour is not considered conflictive security-wide since it is more restrictive, only administrative users are allowed to access the TOE locally. Since results obtained are now consistent with the definition of the requirement; therefore, this issue is deemed closed.	**CLOSED**

ID	Comments	State
N/A	None.	N/A

8 VULNERABILITY ANALYSIS

Evaluator	DAT
Days required	1 day.
Date	2024/08/29
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 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 *13 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 *13 Annex C: Vulnerability Analysis*. The scenarios are detailed in section *11 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 *13 Annex C: Vulnerability Analysis.*

TE.5.5. The evaluator shall register every non-conformity in relation to the Vulnerability Analysis.

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, 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.

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 involves checking all security features declared in the TOE, identifying potential TOE vulnerabilities.

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 security functions are analyzed, paying special attention to threats that could damage the communication between the TOE and other entities, the information stored in it and its ability to maintain the quality of its functionality in the face of attempts to circumvent the restrictions it places on the traffic.

8.4 LIST OF POTENTIAL VULNERABILITIES

Code	Attack potential
N/A	N/A

8.5 RESULTS

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

ID	Comments	State
N/A	None.	N/A

9 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.

[CCN-STIC-140-D3M] Reference Taxonomy for ICT Security Products - Annex D.3M: Firewall. 2020 August.

[ST-08] OPNsense Business Edition Security Target version 0.8 (LINCE)

[IAR-10] OPNsense Business Edition IAR version 1.0

9.1 DEVELOPER EVIDENCES

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

10 ACRONYMS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
LINCE	National Essential Security Certification
STIC	Seguridad en las Tecnologías de Información y la Comunicación
TIC	Information and Communications Technology
TOE	Target Of Evaluation
HTTPS	Hypertext Transfer Protocol Secure
TLS	Transport Layer Security
SSH	Secure Socket Shell
CLI	Command-line interface
GUI	Graphical User Interface
VPN	Virtual Private Network
PC	Personal Computer
RAM	Random Access Memory
GB	GigaByte
MB	MegaByte
CVE	Common Vulnerabilities and Exposures
LAN	Local Area Network
WAN	Wide Area Network
NTP	Network Time Protocol
OTP	One-Time Password
MAC	Message Authentication Code
RSA	Rivest-Shamir-Adleman
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral

ECDSA	Elliptic Curve Digital Signature Algorithm
SHA	Secure Hash Algorithm
AES	Advanced Encryption Standard
CA	Certificate Authority
XML	Extended Markup Language