jtsec
BEYOND IT SECURITY

STIC Evaluation Technical Report

STIC_OPNSENSE_CQ (CUA-2022-46)
2.0
12/12/2022

CHANGELOG

Version	Date	Author	Reason	Changes
0.1	08/06/2022	DHA	First version	Creation of the document
0.2	09/06/2022	DAT	Comments by CPSTIC	Added additional information related to the differences between Community and Business Edition.
1.0	28/07/2022	DAT	Performed pertinent testing effort for BE 22.4	Added sections 4 to 11. Added annexes A, B, C, D.
2.0	12/12/2022	JAL	Performed pertinent testing effort for BE 22.10	Updated security requirements from the previous evaluation. Updated sections 4 to 11. Updated annexes A, B, C, D. Deleted section related to bootup sequence hardening from installation procedure.

TABLE OF CONTENTS

1 Introduction 5
1.1 Evaluation Technical Report information 5
1.2 TOE developer information 5
2 TOE description 7
2.1 Functional description of the TOE 7
2.2 Inventory of security functions 8
2.2.1 ADM (Reliable installation) 8
2.2.2 IAU (Identification and authentication) 9
2.2.3 COM (Reliable communication channels) 9
2.2.4 ACT (Reliable Installation and upgrades) 10
2.2.5 AUD (Audit) 11
2.2.6 CIF (Cryptographic requirements) 12
2.2.7 FW (Firewall) 13
3 Operational environment 15
3.1 Description of the operational environment 15
3.2 Operational environment assumptions 15
4 Executive summary of the evaluation 17
4.1 Version 1.0 17
4.2 Version 2.0 20
5 Verdict of the evaluation 22
6 TOE preparation and configuration 23
6.1 Evaluation activities 23
6.2 Detailed configuration of the operational environment 24
6.3 Description of the installation and configuration of the TOE 24
6.3.1 OPNSense installation 24
6.3.2 Web interface TLS cipher suites configuration 37
6.3.3 SSH cryptographic parameters configuration 38
6.3.4 Syslog client TLS cipher suites configuration 40
6.3.5 License Activation 41
6.3.6 Patch Installation 42
6.4 Used installation options 43
6.5 Results 43

7 Conformity assessment 44
7.1 Documentation analysis 44
7.1.1 Evaluation activities 44
7.1.2 Results 44
7.2 Functional tests 46
7.2.1 Evaluation activities 46
7.2.2 List of functional tests 46
7.2.3 Results 50
8 Vulnerability analysis 51
8.1 Evaluation activities 51
8.2 Methodology used for the analysis 51
8.3 TOE vulnerability analysis 52
8.4 List of potential vulnerabilities 52
8.5 Results 53
9 TOE penetration tests 54
9.1 Evaluation activities 54
9.2 List of penetration tests 54
9.3 Results 57
10 References 58
10.1 Developer Evidences 58
11 Acronyms 59

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_CQ-ETR-v2.0
ETR version	2.0
Author or authors	JAL
Reviewer	DAT
Approved by	
Start date of the works	22/11/2022
End date of the works	12/12/2022
CB dossier code	CUA-2022-46
Laboratory project code	STIC_OPNSENSE_CQ
Type of evaluation	STIC
Product Taxonomy	Communications Protection/Firewall
Evaluation Laboratory holding the accreditation	jtsec Beyond IT Security SL
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

Sponsor data	Deciso B.V Edison 43, 3241 LS Middelharnis, Netherlands.
Developer data	Deciso B.V Edison 43, 3241 LS Middelharnis, Netherlands.
Contact information of developer	Deciso B.V. project@opnsense.org
TOE name	OPNsense Business Edition
TOE version	22.10

Operating manuals of the product	[OPNSENSE-LINCE-ST16] [DOC-74b13d1]

2 TOE DESCRIPTION

2.1 FUNCTIONAL DESCRIPTION OF THE TOE

OPNsense is an open-source, easy-to-use, and easy-to-build FreeBSD based firewall (stateful firewall) and routing platform. A stateful firewall is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The product offers a grouping of Firewall Rules by Category, an excellent feature for more demanding network setups. OPNsense includes most of the features available in commercial firewalls and more in many cases. It brings the rich feature set of commercial offerings with the benefits of open and verifiable sources.

The TOE, as any firewall, has the following basic security features:

- Protection against network traffic outside the network they protect by limiting incoming packets according to the policy applied.
- Access restriction to the outside network for elements of the internal network. Only those devices or users specified in the applied policy are allowed to leave.

The feature set of OPNsense includes high-end features. Those features are intended to make possible that an administrator role performs secure and centralized management and configuration of the product itself and administer the key functionalities for the security of the product and the network it protects. This will make possible the existence of only one type of role capable of performing this type of highly relevant tasks for the product and the network in which it is deployed.

The product also allows users to properly authenticate themselves before accessing the product's configuration through its interfaces, preventing the reading and modification of unauthorized personnel parameters. The product also permits the establishment of a password complexity policy to improve security in the authentication process.

The product offers the possibility of establishing secure communication channels by using SSH and HTTPS protocols so that only authorized entities can establish secure communication channels.

Moreover, the product allows performing a reliable installation and updating, protecting integrity and authenticity during the product's installation. The product also has several types of audit reports grouped according to the set of functionalities recorded. These records allow the detection and traceability of any event that occurs during the operation of the product.

Finally, the product allows the creation of rules providing the possibility of performing packet filtering according to the protocol used, the source network, and the destination network and allowing to decide what type of action to take for each rule. The product also records all the events that occur related to the rules created.

2.2 INVENTORY OF SECURITY FUNCTIONS

2.2.1 ADM (RELIABLE INSTALLATION)

After analyzing [CCN-STIC-140-D3] and [OPNSENSE-LINCE-ST16] in relation to this security function, the following coverage has been considered:

SFR	Retested
ADM.1	No
ADM.2	Yes
ADM.3	No

Equivalent requirements are included in [OPNSENSE-LINCE-ST16], [OPNSENSE-IAR-20] does not present changes that may affect this security functionality. In any case, although no changes are considered relevant for this security function, the evaluator has considered that ADM.2 should be retested in order to verify that it is still possible to configure the required parameters.

Requirement	Description	Objective
ADM.2	The product must be able to manage the following functionalities: • Administration of the product locally and remotely. • Configuration of session termination time or blocking when inactivity is detected. • Other product configuration parameters.	Verify that it is possible to configure session termination by inactivity time for the web interface and SSH console. Verify that it is possible to configure through the web interface: • Protocols • SSL Certificate • SSL Ciphers • TCP Port • Alternate hostnames • Listen interfaces • HTTP Compression Verify that it is possible to configure parameters related to the SSH connection: • Enable secure Shell • Login group • Permit root user login

		• Permit password login • SSH Port • Listen interfaces

2.2.2 IAU (IDENTIFICATION AND AUTHENTICATION)

After analyzing [CCN-STIC-140-D3] and [OPNSENSE-LINCE-ST16] in relation to this security function, the following coverage has been considered:

SFR	Retested
IAU.1	No
IAU.2	Yes
IAU.3	No
IAU.4	No
IAU.5	Yes

Equivalent requirements are included in [OPNSENSE-LINCE-ST16], [OPNSENSE-IAR-20] does not present changes that may affect this security functionality. In any case, although no changes are considered relevant for this security function, the evaluator has considered that IAU.2 and IAU.5 should be retested in order to verify that the brute-force protection is still present and the product block or log off a user after a certain period of inactivity.

Requirement	Description	Objective
IAU.2	The product must implement mechanisms that prevent brute-force authentication attacks.	Verify if the TOE blocks the attacker's IP address after a determined number of failed attempts.
IAU.5	The product must block or log off a user after a certain period of inactivity.	Verify if the TOE block or log off a user after a certain period of inactivity.

2.2.3 COM (RELIABLE COMMUNICATION CHANNELS)

After analyzing [CCN-STIC-140-D3] and [OPNSENSE-LINCE-ST16] in relation to this security function, the following coverage has been considered:

SFR	Retested
COM.1	Yes
COM.2	Yes
COM.3	No

Equivalent requirements are included in [OPNSENSE-LINCE-ST16], [OPNSENSE-IAR-20] does not present changes that may affect this security functionality. In any case, although no changes are considered relevant for this security function, the evaluator has considered that COM.1 and COM.2 should be retested in order to verify that the secure protocols are still being used and the communications are initiated by itself or by authorized entities.

Requirement	Description	Objective
COM.1	Protection of information in transit. The TOE shall establish secure channels when exchanging sensitive information with authorized entities or between different parts of the product using functions, algorithms and protocols by following the [CCN-STIC-807] guide (e.g., HTTPS/TLS 1.2, TLS 1.2 or higher, IPSec, etc.).	Verify that the TOE establishes secure channels using: • SSH, via remote console • HTTPS, via web interface • TLS, with external syslog server
COM.2	The TOE must allow these secure communication channels to be initiated by itself or by authorized entities.	Verify that the TOE still uses secure channels when stablishes communications with different services in the network where it is running.

2.2.4 ACT (RELIABLE INSTALLATION AND UPGRADES)

After analyzing [CCN-STIC-140-D3] and [OPNSENSE-LINCE-ST16] in relation to this security function, the following coverage has been considered:

SFR	Retested
ACT.1	Yes
ACT.2	No
ACT.3	No
ACT.4	Yes

Equivalent requirements are included in [OPNSENSE-LINCE-ST16], [OPNSENSE-IAR-20] does not present changes that may affect this security functionality. In any case, although no changes are considered relevant for this security function, the evaluator has considered that ACT.1 and ACT.4 should be retested in order to verify that the product offer the possibility to check the current version and to verify that it is possible to start updates manually.

Requirement	Description	Objective

ACT.1	The product must offer the possibility to check the current version of the firmware/software.	Verify that the TOE allow to check the current version of the firmware/software.
ACT.4	The product must offer the possibility to start updates manually and to check if there are new updates available.	Verify that the TOE allow to start updates manually and to check if there are new updates available.

2.2.5 AUD (AUDIT)

After analyzing [CCN-STIC-140-D3] and [OPNSENSE-LINCE-ST16] in relation to this security function, the following coverage has been considered:

SFR	Retested
AUD.1	Yes
AUD.2	Yes
AUD.3	No
AUD.4	No
AUD.5	No

Equivalent requirements are included in [OPNSENSE-LINCE-ST16], since [OPNSENSE-IAR-20] does not present changes that may affect this security functionality, the evaluator has considered that AUD.1 and AUD.2 should be retested in order to verify that the product register audit events related to specific actions and contains at least certain information about events.

Requirement	Description	Objective
AUD.1	The product must generate audit information at the beginning and termination of the audit functions and when any of the following events: a) Login and logout of registered users b) Change in user credentials c) Changes in the product configuration d) Events related to product functionality e) Generation, import, change or deletion of cryptographic keys	Verify that the TOE generate audit events when the mentioned actions are performed.
AUD.2	The audit records shall contain at least the following information: date and time of the event, type of event	Verify that the events logs generated by TOE when the listed actions are

	identified, result of the event, user producing the event (if applicable).	performed contains at least date and time of the event, type of event, result of the event and user producing the event.

2.2.6 CIF (CRYPTOGRAPHIC REQUIREMENTS)

After analyzing [CCN-STIC-140-D3] and [OPNSENSE-LINCE-ST16] in relation to this security function, the following coverage has been considered:

SFR	Retested
CIF.1	Yes

Equivalent requirements are included in [OPNSENSE-LINCE-ST16], [OPNSENSE-IAR-20] does not present changes that may affect this security functionality. In any case, although no changes are considered relevant for this security function, the evaluator has considered that CIF.1 should be retested in order to verify that the TOE uses protocols and cipher suites agreed in [CCN-STIC-807].

Requirement	Description	Objective
CIF.1	All symmetric and asymmetric encryption algorithms, key agreement protocols and summary functions used by the product must be within those accredited by the CCN for use in the ENS. The list of these algorithms is included in the [CCN-STIC-807] Cryptology for use in the ENS (MEDIUM Category).	Verify that the TOE uses agreed cryptographic mechanisms such as communication protocols, cipher suites or summary functions. To do so, the evaluator will mainly inspect the communication channels.

2.2.7 FW (FIREWALL)

After analyzing [CCN-STIC-140-D3] and [OPNSENSE-LINCE-ST16] in relation to this security function, the following coverage has been considered:

SFR	Retested
FW.1	No
FW.2	No
FW.3	No
FW.4	Yes
FW.5	Yes
FW.6	No
FW.7	No
FW.8	Yes

Equivalent requirements are included in [OPNSENSE-LINCE-ST16], [OPNSENSE-IAR-20] does not present changes that may affect this security functionality. In any case, although no changes are considered relevant for this security function, the evaluator has considered that some fundamental requirements should be tested again in order to verify that the firewall functionality is still met.

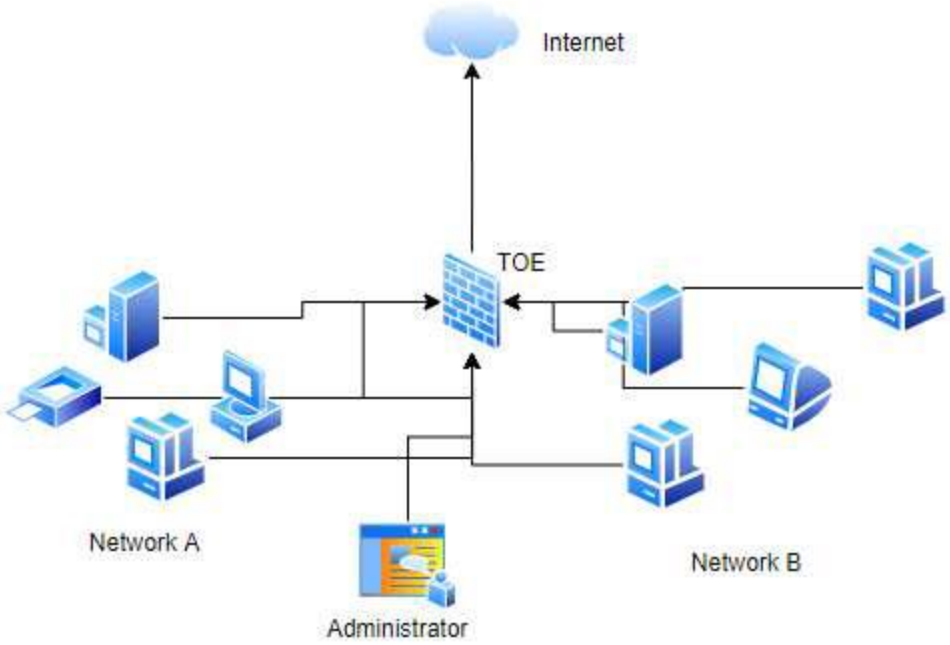
Requirement	Description	Objective
FW.4	The product allows: a) Drop or be capable of counting and/or add to the log packets which are invalid fragments. b) Drop or be capable of counting and/or add to the log fragmenting packets which cannot be re-assembled completely. c) Drop or be capable of adding to the log packets where the source address of the network packet is defined as being on a broadcast network. d) Drop or be capable of adding to the log packets where the source address of the network packet is defined as being on a multicast network. e) Drop or be capable of adding to the log packets where the source or destination address of the network packet is defined as being unspecified	Verify if the TOE still allows to register the required information related to packets.

	(i.e. 0.0.0.0) or an address "reserved for future use" (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4. f) Drop or be capable of adding to the log packets where the source or destination address of the network packet is defined as an "unspecified address" or on address "reserved for future definition and use" (i.e. unicast addresses not in this address range: 2000::(/3) as specified in RFC 3515 for IPv6. g) Drop or be capable of adding to the log packets with the IP options: Loose Source Routing (LSR) and Record Route Specified (SSR).	
FW.5	The product is capable of dropping and logging according to the following rules: • Network packets where the source address of the network packet is equal to the address of the network interface where the network packet was received; • Network packets where the source or destination address of the network packet is a link-local address; • Network packets where the source address of the network packet does not belong to the networks associated with the network interface where the network packet was received.	Verify if the TOE still allows to drop and log network packets according to the specified rules.
FW.8	The product is capable of limiting an administratively defined number of *half-open TCP* connections. In the event that the configured limit is reached, new connection attempts will be dropped and the drop event will be counted and/or logged.	Verify if the TOE still able to limit an administratively defined number of half-open TCP connections and this type of event is logged and showed in the corresponding audit interface.

3 OPERATIONAL ENVIRONMENT

3.1 DESCRIPTION OF THE OPERATIONAL ENVIRONMENT

The product is designed to run on a network to protect interconnections by allowing and/or limiting traffic to or from a network that is protected based on a set of rules established by an administrator. The TOE provides a Dashboard or graphical interface which offers a list of features to check the status of the product and the network quickly.



According to its features, the product is capable of being deployed according to the use cases described in the firewall taxonomy:

- *Border device.* The product is able to be deployed in an operational environment where protects a network from an external network, as the Internet.
- *Network segmentation.* The device is located in an area where it protects two internal networks from each other, i.e., it segments both networks and allows only authorized traffic to flow from one to the other.

3.2 OPERATIONAL ENVIRONMENT ASSUMPTIONS

This section contains the assumptions presented by the manufacturer. They are described below:

Reference	Description
A.Physical Protection	The product must be installed in an area where access is only possible for authorized personnel and under suitable environmental conditions.

A.Limited functionality	The product must be used for network routing and filtering as its basic function and not provide any other functionality, except for certain compatible communication protection-oriented ones.
A.Reliable Administration	The Administrator will be a trusted member and will look after getting the best security interests on behalf of the organization. It is therefore assumed that such an administrator is trained and free from any harmful intent in handling the product. The product will not be able to protect itself against and administrator user with bad intentions.
A.Periodic Updates	The product's firmware and software will be updated as updates that correct known vulnerabilities are released.
A.Credential Protection	All credentials, especially the administrator's credentials, must be properly protected by the organization who uses the product.
A.Security Policy	A security policy should reflect the set of principles, organization and procedures required by an organization to address its information security needs, included the use of ICT.

4 EXECUTIVE SUMMARY OF THE EVALUATION

4.1 VERSION 1.0

This is a STIC evaluation for the product OPNsense Business Edition 22.4. The evaluation has been carried out following the LINCE methodology to verify that the Business Edition of the previously evaluated and certified product still meets a series of requirements.

The previous evaluated version was the community edition and though the evaluated edition is the business edition and there are differences (showed in the table below), the security functions that are going to be evaluated are the same, since the additional functionality is not relevant. The main difference is that business edition is intended for companies, enterprises and professionals looking for a more stable upgrade path (this version lags 4 releases behind the community edition) and additional commercial features.

Features	Community Edition	Business Edition
Stateful Firewall	✓	✓
Various authentication options	✓	✓
Two-Factor Authentication	✓	✓
Certificates (Let's encrypt)	✓	✓
Link Aggregation & Failover	✓	✓
Traffic Shaping	✓	✓
Multi WAN	✓	✓
Load Balancer	✓	✓
Intrusion Detection & Prevention	✓	✓
Captive Portal	✓	✓
VPN Services (Ipsec, OpenVPN, WireGuard)	✓	✓
High Availability	✓	✓
Virus scanner	✓	✓
Tested Updates (Business Edition Update Repository)	✗	✓
Access to GeoIP database	✗	✓
Access to the official OPNsense OVA image	✗	✓
Business-Plugins (OPNcentral (in development))	✗	✓
Support of the active development with the license fee	✗	✓

Given that the Business Edition version 22.4 is based on the Community Edition 22.1.4 as mentioned by the manufacturer in https://docs.opnsense.org/releases/BE_22.4.html#april-26-2022. The changes introduced from the evaluated version of the Community Edition (21.7.1) to the version 22.1.4 have been examined in order to determine what security functionality could have been affected and, therefore, must be retested. This changelog is provided in the document [OPNSENSE-IAR-10].

Moreover, as a consequence of a further analysis requested by CPSTIC given the manufacturer's statement "This business release is based on the OPNsense 22.1.4 community version with additional reliability improvements.", the evaluator has requested the manufacturer more detail in relation to the aforementioned additional reliability improvements.

These additional reliability improvements are documented in [OPNSENSE-IAR-10] and are described by the manufacturer as bug fixes and minor changes backported from superior versions (22.1.5 and 22.1.6) of the Community Edition 22.1.4 into the Business Edition version 22.4. Such improvements, included in [OPNSENSE-IAR-10], were analysed and are considered to not affect the requirements tested and declared in [OPNSENSE-LINCE-ST16].

The changes between the versions, included in [OPNSENSE-IAR-10], were analysed by the evaluator, determining that, with the information given in the changelog, none of the requirements were considered affected by the changes. Given this, the evaluator has sampled the tests performed in the previous LINCE evaluation and has determined a set of tests to repeat for the Business edition. The section 2.2 Inventory of security functions delves deeper on the tests that are going to be carried out and they can be found in Annex B: Functional test plan and report.

Regarding this evaluation, after analyzing the scope of the tests and determining the requirements to retest, the installation of the TOE was carried following the manuals and taking into account the indications included in the security target [OPNSENSE-LINCE-ST16]) for the version of the product included in CPSTIC.

The installation was straightforward and flawless; therefore, no non-conformities were generated through this phase of the evaluation.

Apart from the installation procedure, in order to meet the cryptographic requirements, additional steps were followed in order to configure TLS cipher suites for the web interface, SSH cryptographic parameters and TLS cipher suites offered when connecting to a remote syslog server. These steps are documented in sections 6.3.2 Web interface TLS cipher suites configuration, 6.3.3 SSH cryptographic parameters configuration and 6.3.4 Syslog client TLS cipher suites configuration.

Following with the evaluation, the set of functional tests was conducted revealing that [TOE-224] passes the set of tests determined. Given the results experienced, the evaluator has not required to perform additional functional testing effort as the behavior showed by [TOE-224] demonstrate a high level of confidence. As all the functional tests passed, no non-conformities were generated during this phase.

Leading the completion of the functional tests, it was proceeded to perform the analysis of the TOE vulnerabilities. The evaluator followed the type of vulnerabilities documented in the previous LINCE evaluation as the TOE is the same. Given the vulnerabilities, the evaluator selected a set of penetration tests carried out in the LINCE evaluation, alongside others considered adequate, conducting them to verify that the

product maintains the security warranties from the LINCE evaluation. These tests can be found in Annex B: Functional test plan and report.

During this phase, only one test failed and a non-conformity was generated and reported to the manufacturer:

- [STIC_OPNSENSE_CQ-PT-7010]: The evaluator identified an issue with the bootup procedure causing the transmission of packets without the application of the filtering rules defined in [TOE-224] during a temporal window. The root cause of this is that the network interfaces were configured and up before configuring the filtering rules.
  This issue, labeled as OR01.NC01, was communicated to the manufacturer. A solution to this issue was provided which consists on a small change related to the file that defines the bootup sequence. This change is documented in section 6.3.5 Bootup Sequence Hardening.

Once the indications were provided by the manufacturer, the evaluator repeated the related test and verified that the solution was valid and working, closing the associated non-conformity OR01.NC01.

Therefore, since all the registered non-conformities were solved, the laboratory concludes the evaluation with the verdict **PASS**.

4.2 VERSION 2.0

This is a STIC evaluation for the product OPNsense Business Edition 22.10. The evaluation has been carried out following the LINCE methodology to verify that the requirements evaluated in previous testing rounds are still met by the TOE, as part of a contiguous qualification procedure.

The approach to OPNsense Bussiness Edition 22.10 evaluation is the same as for OPNsense Bussiness Edition 22.4, which was tested in the previous testing round, determine a set of tests to perform and verify if the results still met the requirements. In this case, the coverage considered slightly differs from the last STIC evaluation with the objective to verify a different group of requirements that were not tested in the previous round.

The changes introduced from the latest evaluated version of the Business Edition (22.4) to the version 22.10 have been examined in order to determine what security functionality could have been affected and, therefore, must be retested. This changelog is provided in the document [OPNSENSE-IAR-20].

Moreover, as a consequence of the manufacturer's statement "This business release is based on the OPNsense 22.7.6 community version with additional reliability improvements.", the evaluator has requested the manufacturer more detail in relation to the aforementioned additional reliability improvements.

These additional reliability improvements are documented in [OPNSENSE-IAR-20] and are described by the manufacturer as bug fixes and minor changes backported into the Business Edition version 22.10. Such improvements, included in [OPNSENSE-IAR-20], were analysed and are considered to not affect the requirements tested and declared in [OPNSENSE-LINCE-ST16].

The changes between the versions, included in [OPNSENSE-IAR-20], were analysed by the evaluator, determining that, with the information given in the changelog, none of the requirements were considered affected by the changes. Given this, and taking into account the tests performed in the previous STIC evaluation, the evaluator has determined a set of tests to repeat for OPNsense Business edition 22.10. The section 2.2 Inventory of security functions delves deeper on the tests that are going to be carried out and they can be found in Annex B: Functional test plan and report.

Regarding this evaluation, after analyzing the scope of the tests and determining the requirements to retest, the installation of the TOE was carried following the manuals and taking into account the indications included in the security target [OPNSENSE-LINCE-ST16]) for the version of the product included in CPSTIC.

The installation was straightforward and flawless; therefore, no non-conformities were generated through this phase of the evaluation.

Apart from the installation procedure, in order to meet the cryptographic requirements, additional steps were followed in order to configure TLS cipher suites for the web

interface, SSH cryptographic parameters and TLS cipher suites offered when connecting to a remote syslog server. These steps are documented in sections 6.3.2 Web interface TLS cipher suites configuration, 6.3.3 SSH cryptographic parameters configuration and 6.3.4 Syslog client TLS cipher suites configuration.

Following with the evaluation, the set of functional tests was conducted revealing an issue related to the brute force protection for the GUI and SSH:

- [STIC_OPNSENSE_CQ-TST-2020]/ [STIC_OPNSENSE_CQ-TST-2021]: The evaluator determined that the brute force protection was not working properly given the behavior of [TOE-2210]. Firstly, performing the brute force attack was possible if the connection remained open as [TOE-2210] did not seem to be killing the state of such connection when the limit failed attempts was reached. Secondly, regarding SSH, the protection was not complete since only the username enumeration was protected, failed login attempts for registered users were not properly monitored. The authentication error generated when an existing user indicates a wrong password was not taken into account.

This issue is registered as OR02.NC01 and was communicated to the manufacturer. The developer response was quick and confirmed the finding, providing a solution for the issue. The change performed is present in the publicly-available Github repository (https://github.com/opnsense/core/commit/ae8e0ce4a4a2c0c96f6f561b85a59a0b71eba828).

Given the results of the functional tests experienced, the evaluator has not required to perform additional functional testing effort as the behavior showed by [TOE-2210] demonstrate a high level of confidence.

Leading the completion of the functional tests, it was proceeded to perform the analysis of the TOE vulnerabilities. The evaluator followed the type of vulnerabilities documented in previous evaluations as the TOE is the same. Given the vulnerabilities, the evaluator selected a set of penetration tests to conduct, alongside others considered adequate. These tests can be found in Annex D: Penetration test plan and report.

Therefore, since all the registered non-conformities were solved, the laboratory concludes the evaluation with the verdict **PASS**.

5 VERDICT OF THE EVALUATION

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

The installation of the product does not reveal any non-conformity.

The documentation analysis does not reveal any non-conformity.

The functional tests do not reveal any non-conformity.

The vulnerability analysis does not reveal any non-conformity.

The penetration tests do not reveal any non-conformity.

6 TOE PREPARATION AND CONFIGURATION

Documents used during installation	[OPNSENSE-LINCE-ST16] [DOC-74b13d1]
Evaluator	JAL
Days required	1 day.
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. The evaluator shall check that, according to the TOE operative and preparative guidance, it is possible to securely install the product using the configuration or configurations referenced in the Security Target.

PASS The evaluator has been able to install the product exclusively following the contents of the manufacturer's documentation, provided through [OPNSENSE-LINCE-ST16] and [DOC-74b13d1].

TE.2.2. The evaluator shall check that the manufacturer has provided the testing platforms required to carry out the TOE evaluation activities.

PASS The manufacturer has provided the evaluator with a platform on which to develop the tests, as well as the necessary documentation to make use of it within the conditions of the evaluation.

TE.2.3. 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* y *6.3 Description of the installation and configuration of the TOE*.

TE.2.4. 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 section *6.4 Used installation options*.

TE.2.5. 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 6.5 Results.

6.2 DETAILED CONFIGURATION OF THE OPERATIONAL ENVIRONMENT

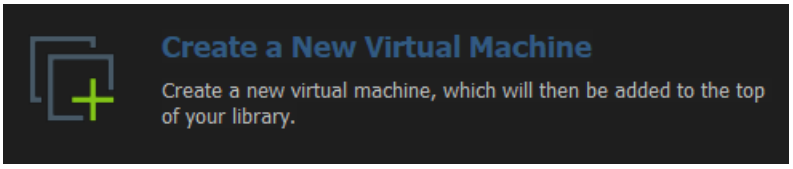
The test scenarios are described in section 12 Annex A: Test scenarios.

6.3 DESCRIPTION OF THE INSTALLATION AND CONFIGURATION OF THE TOE

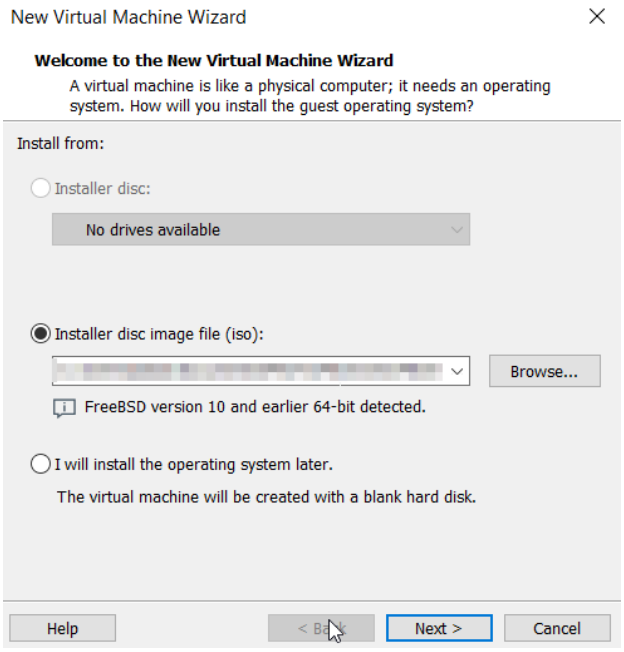
6.3.1 OPNSENSE INSTALLATION

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

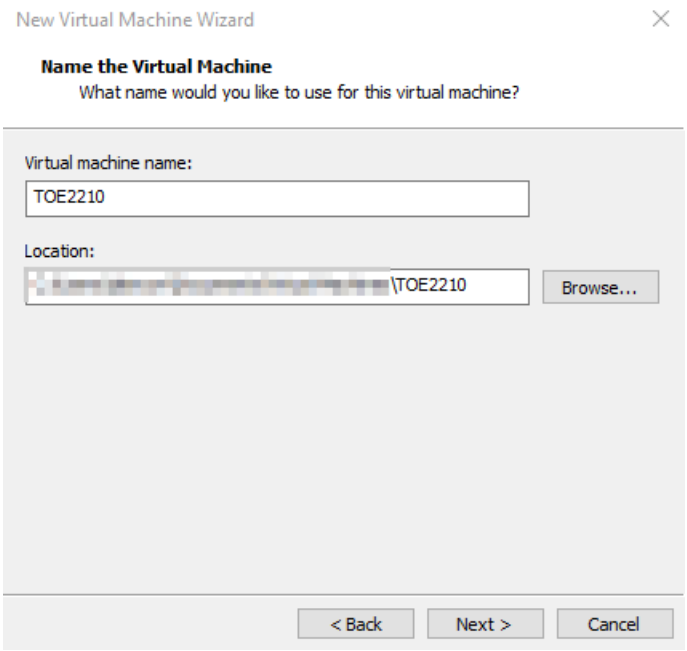
1. Open VMware and click on Create a new virtual machine.



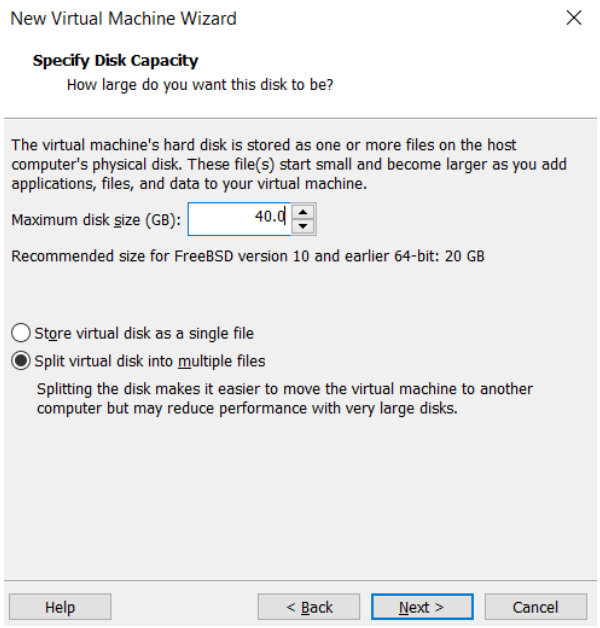
2. Select [TOE-ISO-2210] and click on “Next”.



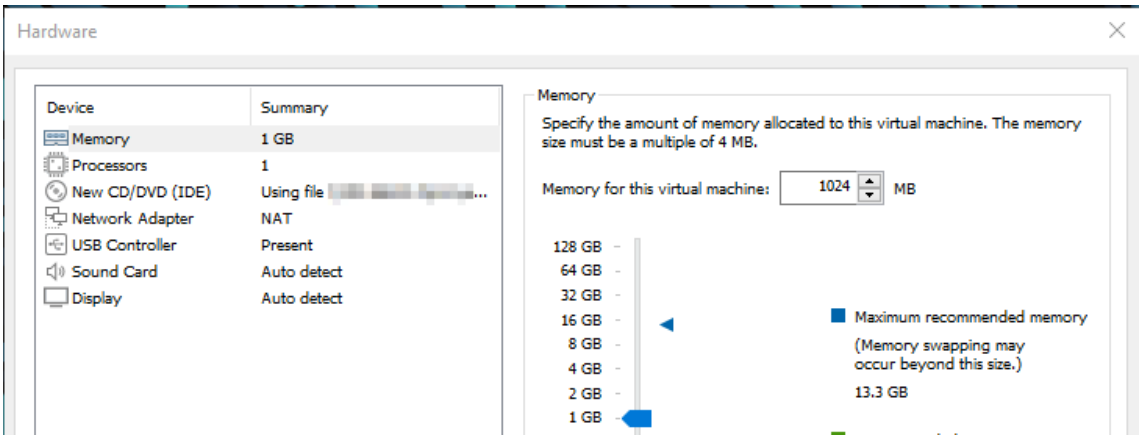
3. Give a name to the virtual machine and click on “Next”.



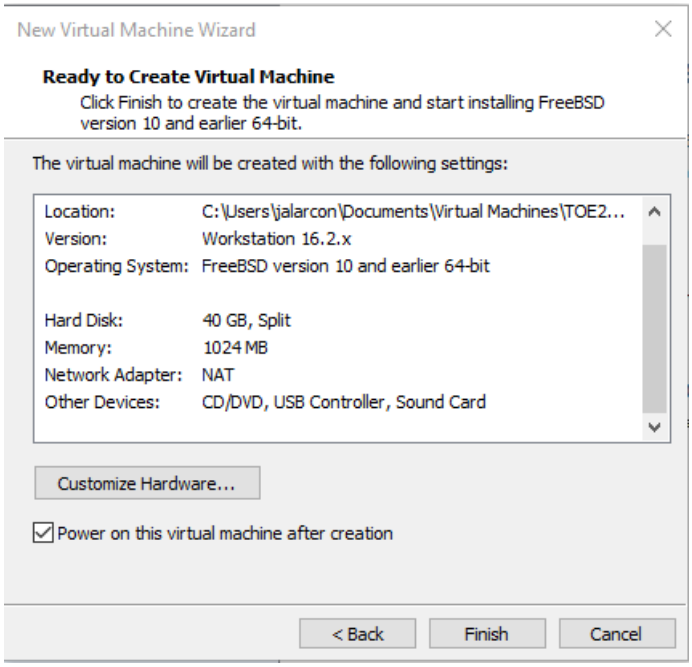
4. Set 40GB as disk size.



5. Click on Customize Hardware > Memory and set 1GB of RAM memory. Then, press “Close”.



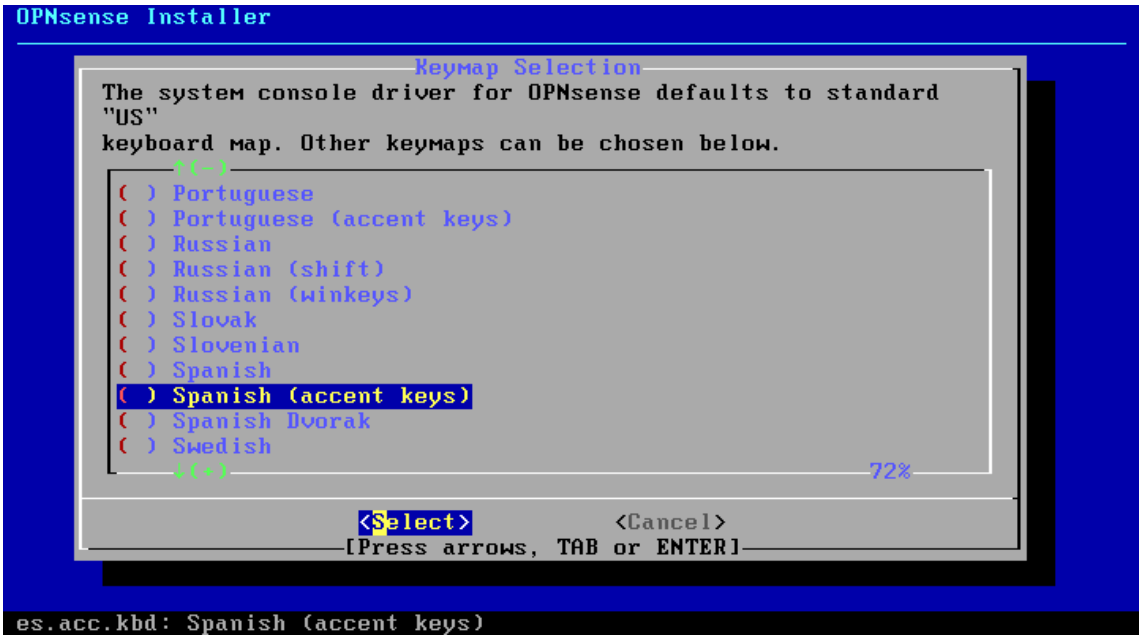
6. Click on “Finish”.



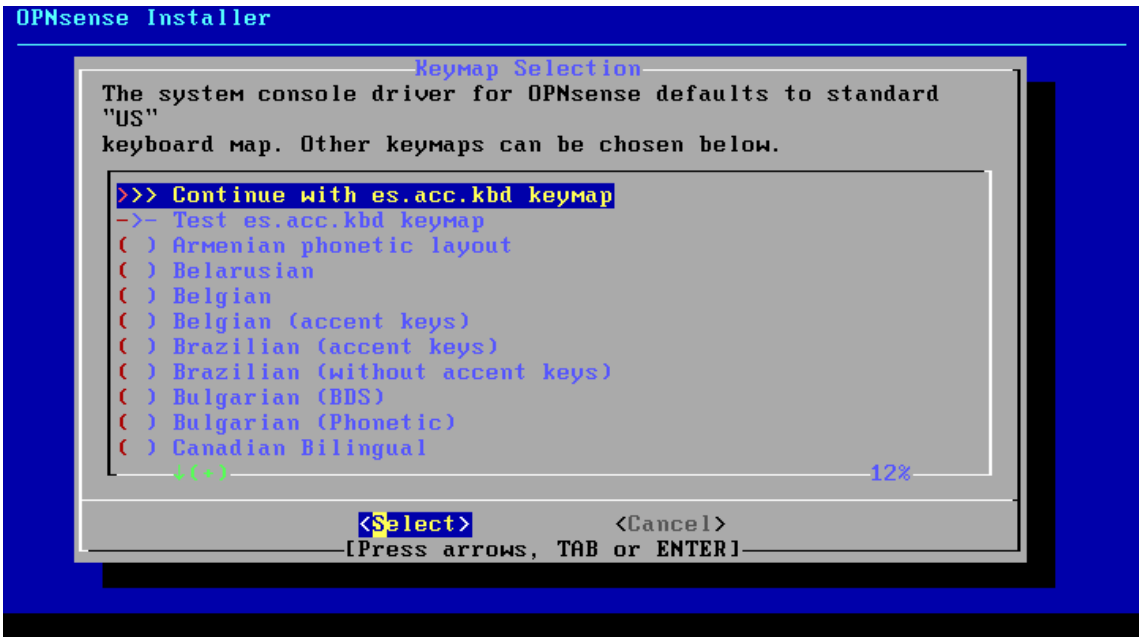
7. Wait for [TOE-2210] to boot up.
8. In order to install [TOE-2210], log in with the user “installer” and authenticate with the password “opnsense”.

```
Starting Cron: OK
>>> Invoking start script 'beep'
Root file system: /dev/iso9660/OPNSENSE_INSTALL
Tue Nov 22 11:35:49 UTC 2022

*** OPNsense.localdomain: OPNsense 22.10 (amd64/OpenSSL) ***

 LAN (em0)       -> v4: 192.168.1.1/24

 HTTPS: SHA256 87 C2 5C C3 1D 3D 85 69 B1 B6 B2 90 49 30 39 56
               5A EB 59 72 38 81 C2 9F 4A 2C 23 87 51 83 49 63
 SSH:   SHA256 L9cO/2/oNzHYdJkx/QcFAN1JuED13PkuUtSD4xmkSyA (ECDSA)
 SSH:   SHA256 /13xTdUBjfw3IcBt4eIOuMNiOgq5PI4eiVPWNC0UK8w (ED25519)
 SSH:   SHA256 IKsaiXcF0DeM9wdTt+84mMoY/a/Bed8s3VXpsa0Nnbc (RSA)
pw: no such user 'installer'

Welcome!  OPNsense is running in live mode from install media.  Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation.  Use the default or previously-imported root password for
both accounts.  Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)

login: installer
Password:
```

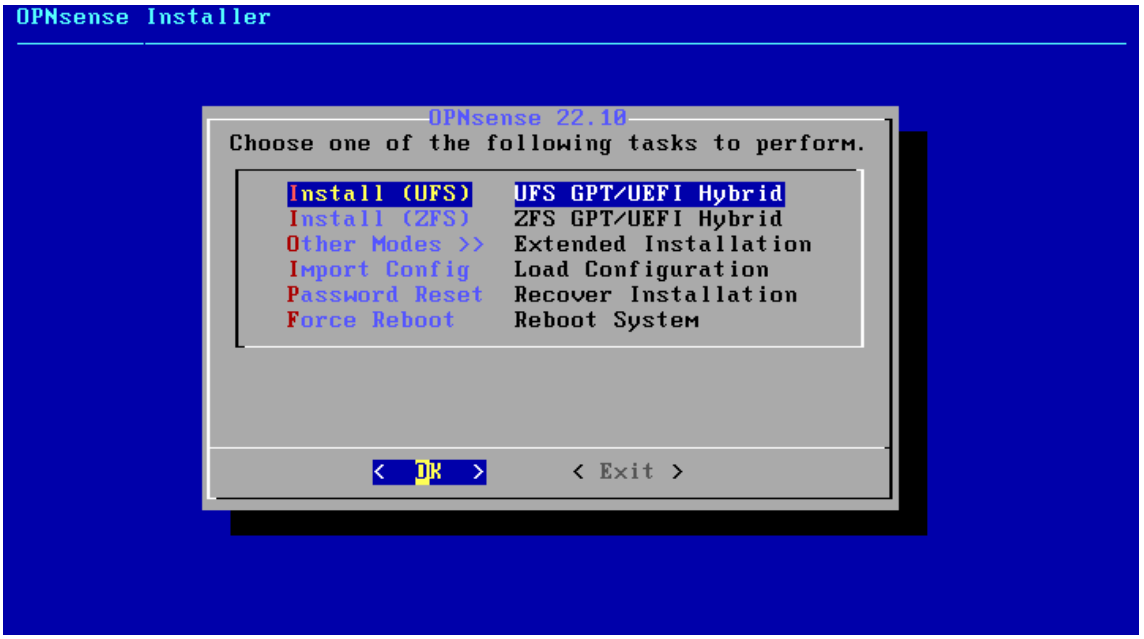
9. Select the keyboard layout.



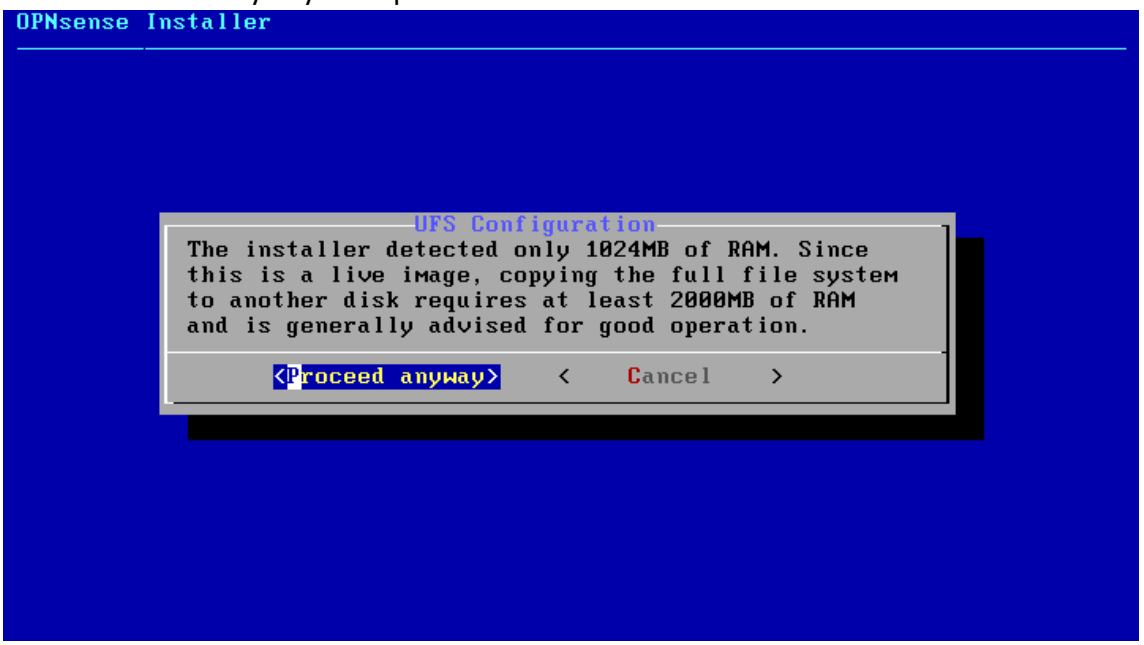
10. Indicate “Continue with…”.



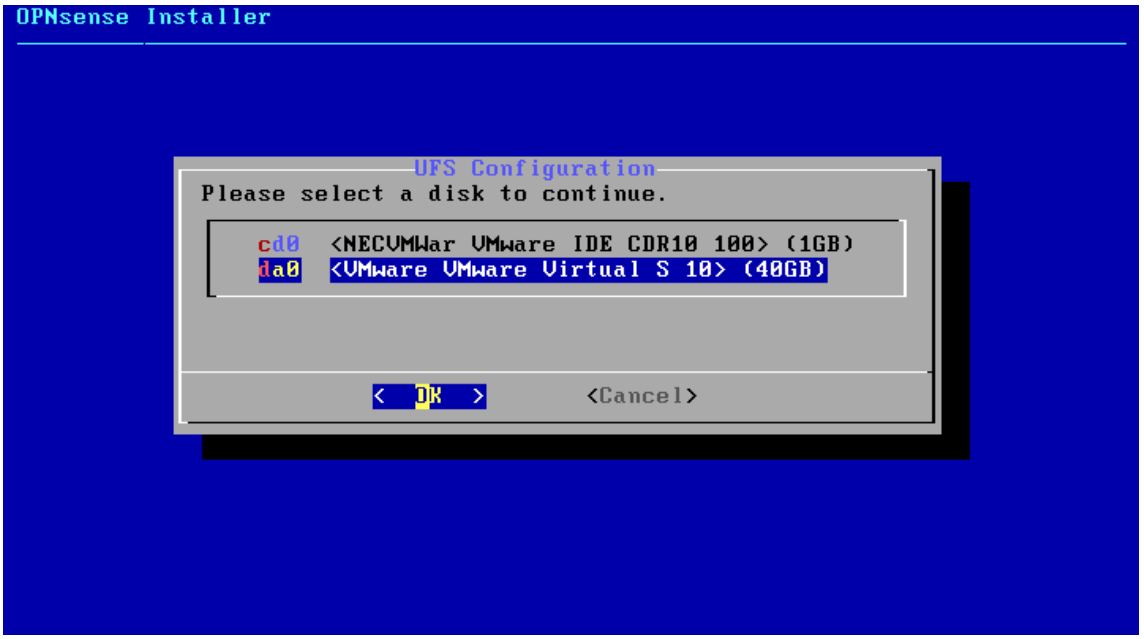
11. Select “Install (UFS)” and press Enter.



12. Select “Proceed anyway” and press Enter.

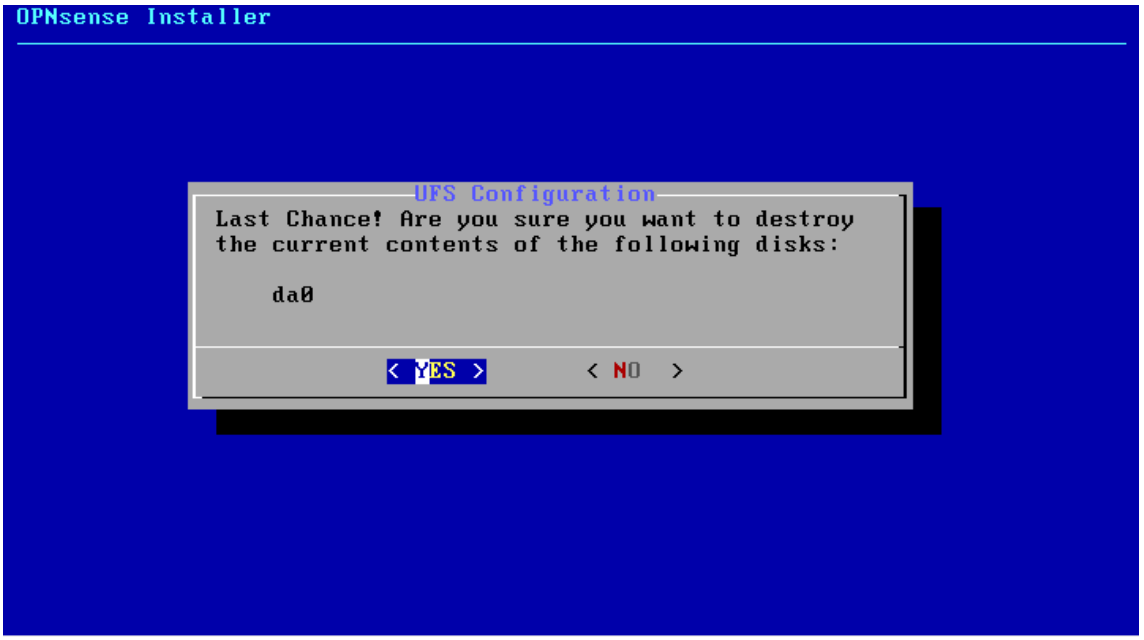


13. Select the 40GB virtual disk and press OK.

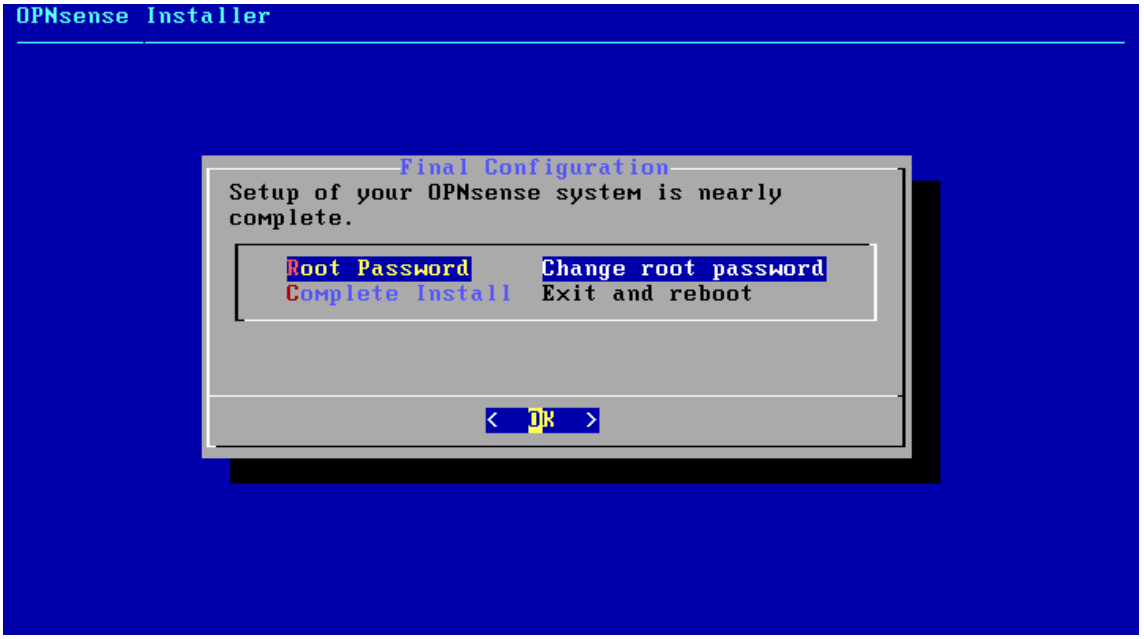


14. Select Yes and press Enter.

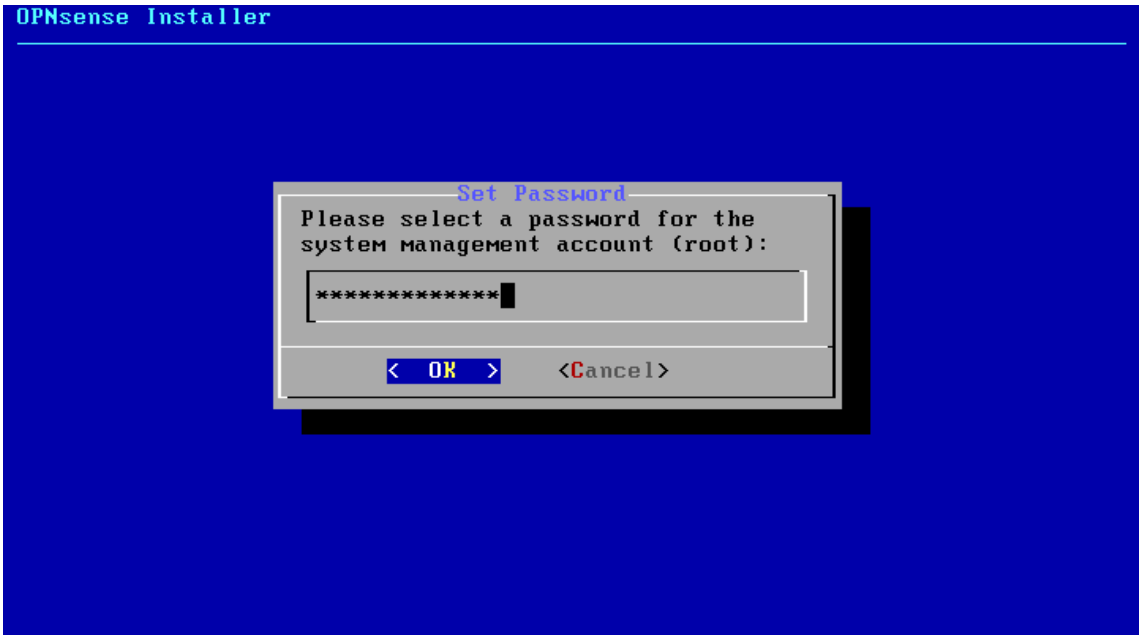
15. Select Yes and press Enter.



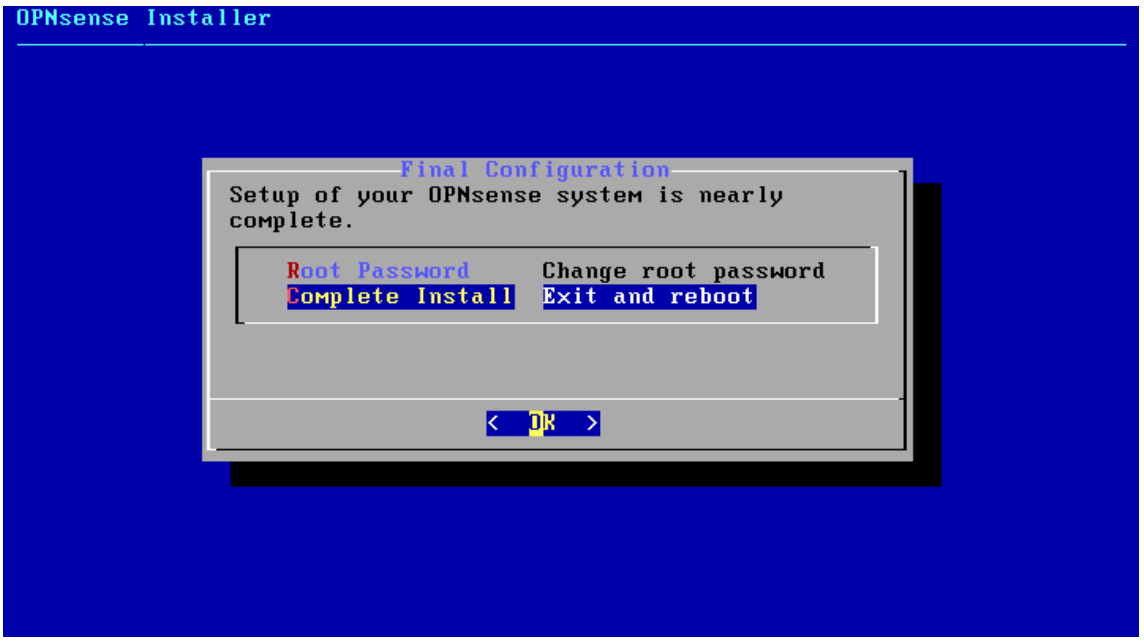
16. Select “Change root password” and press OK.



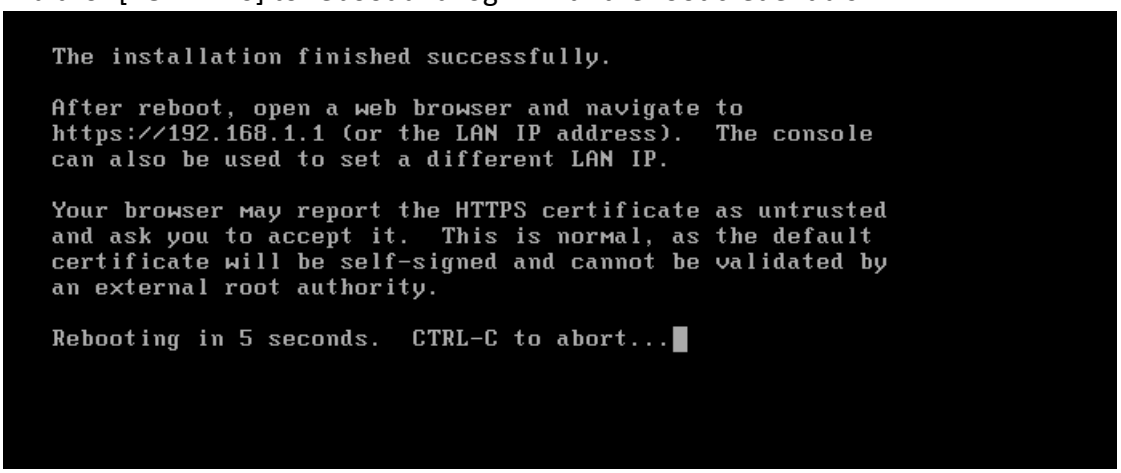
17. Define a new password for the root user, the password shall be at least 10 characters long and have capital letters, numbers and special characters.



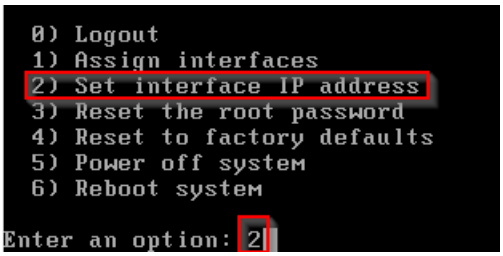
18. Select Exit and Press OK.



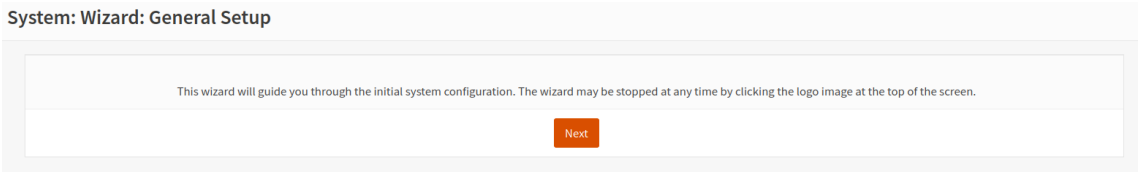
19. Wait for [TOE-2210] to reboot and log in with the root credentials.



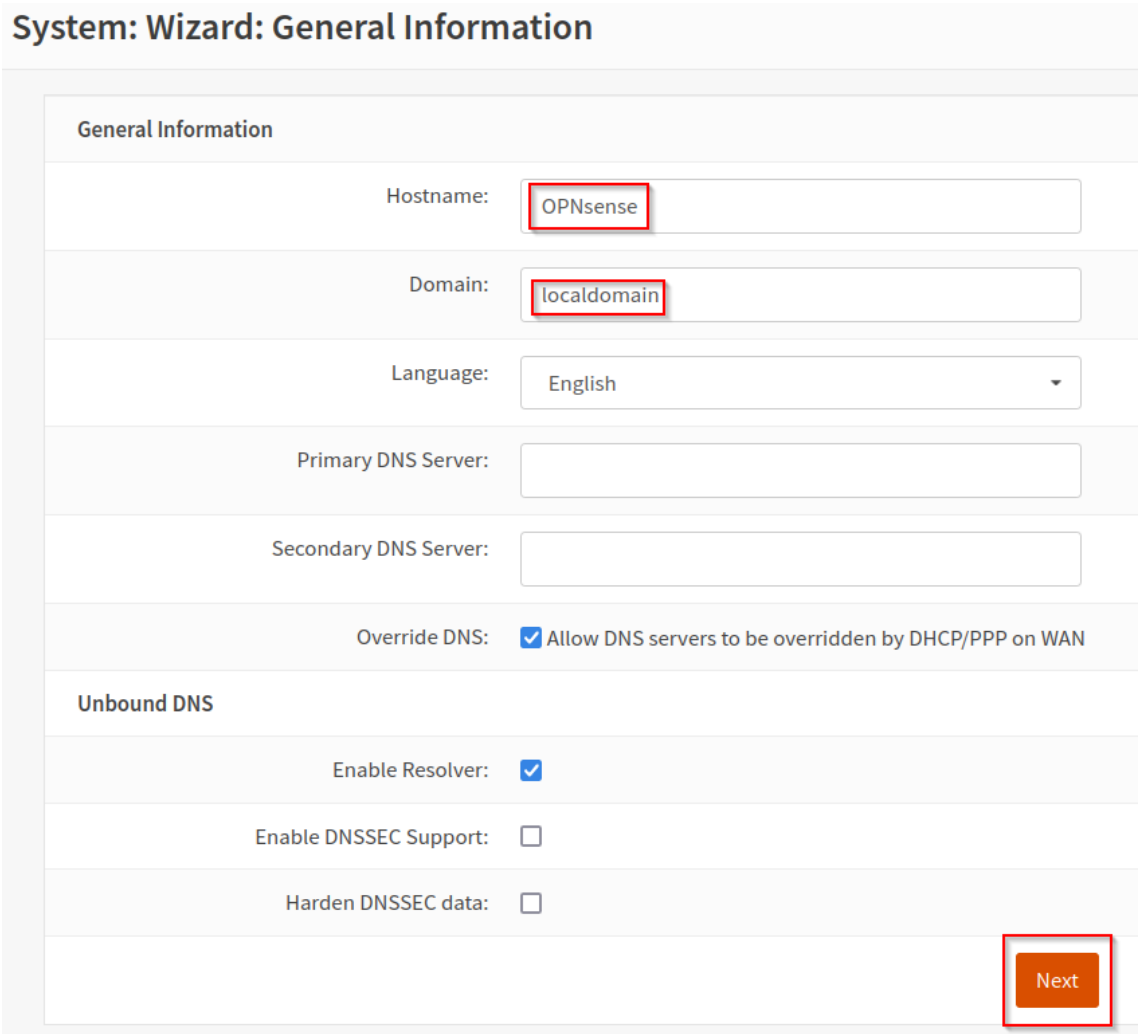
20. Select option 2 “Set interface IP address” and press Enter.



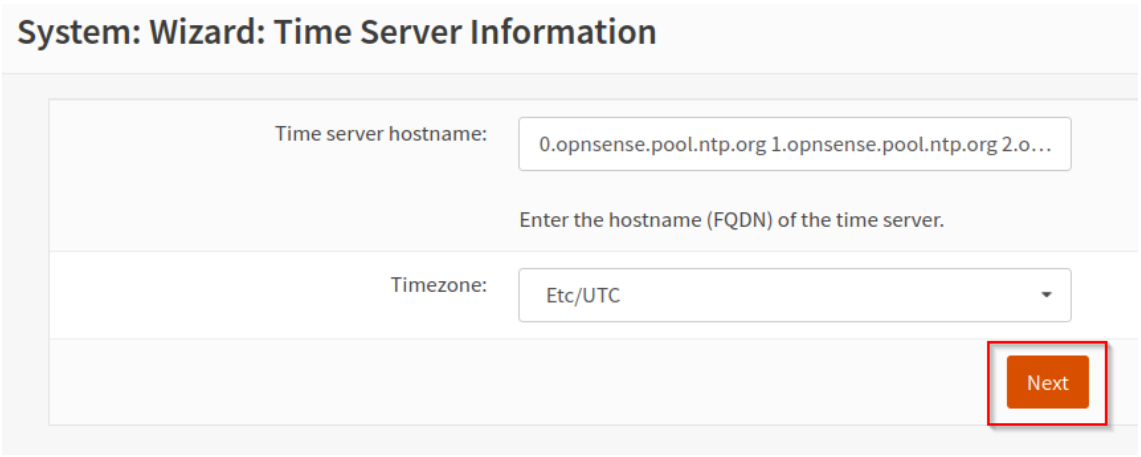
21. Set an IP Address for the TOE in the LAN network:
    a. Select No for DHCP configuration.
    b. Add an IP Address to <IP-TOE_LAN1>
    c. Enter the LAN subnet, in this case 24.
22. Select No for all the following options regarding IPv6 and new configurations to the Web Interface.
23. Access the <IP-TOE_LAN1>
24. Log in with the root user credentials.
25. Follow the wizard setup, press Next.



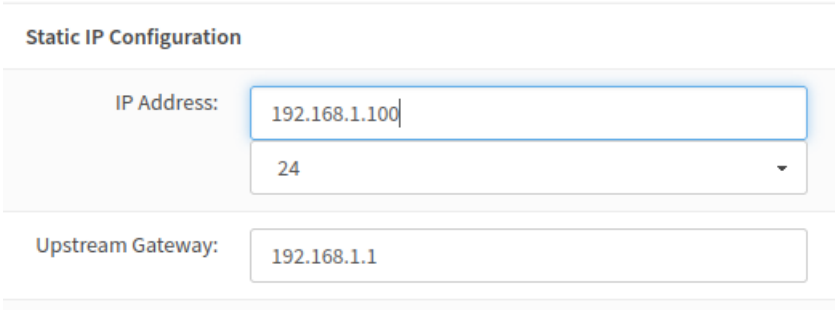
26. Give a hostname and a domain to the TOE and press Next.



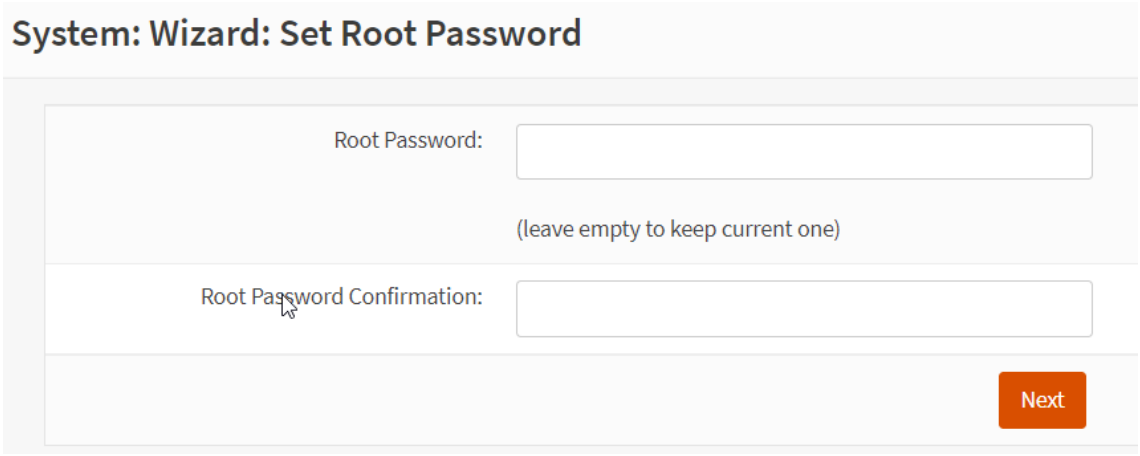
27. Set NTP servers and the time zone. In this case the NTP servers configured are the ones offered by default. Press Next.



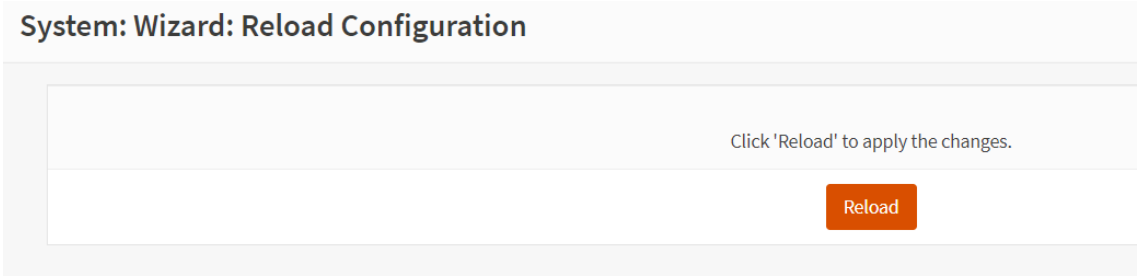
28. Do not configure any field in “Configure WAN interface”.
29. In “Configure LAN interface” check that the IP address and the subnet mask are the same as configured in previous steps. Press Next.



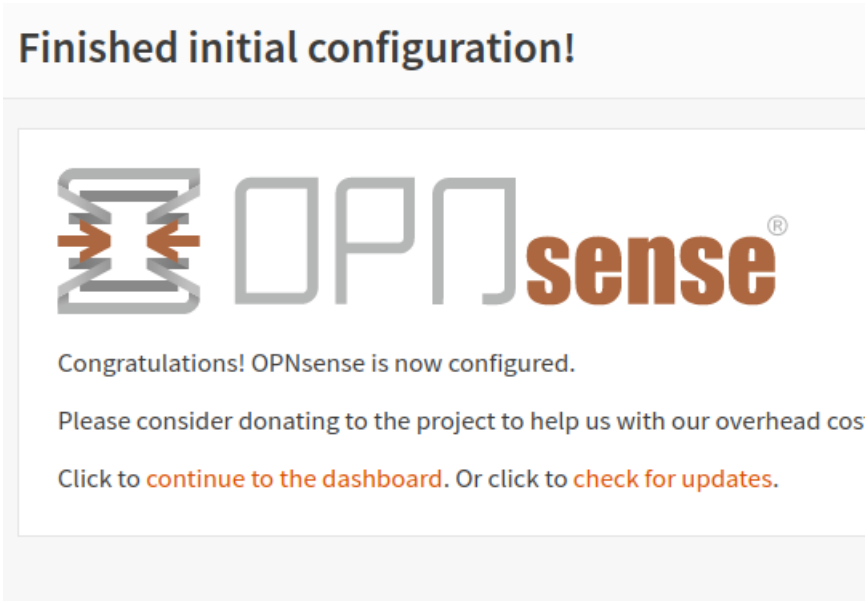
30. Set a new root password if it was not changed before.



31. Click on reload to apply the changes.

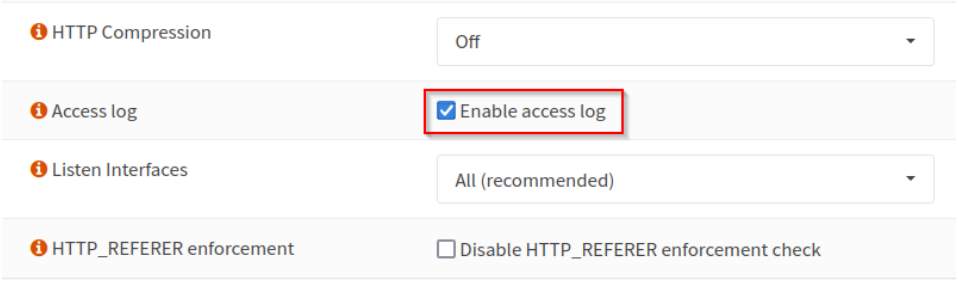


32. [TOE-2210] is now configured and ready, click to the dashboard.

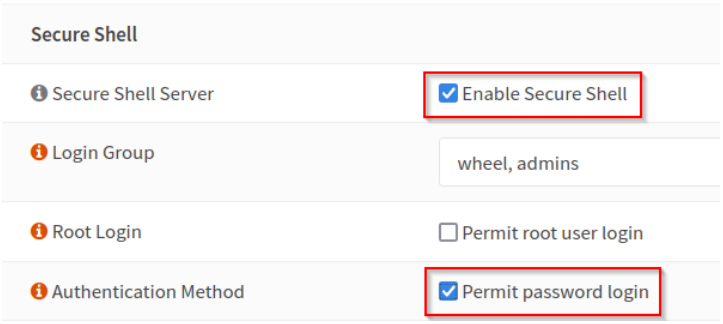


After installing the TOE, given the indications in the security target [OPNSENSE-LINCE-ST16], the following steps are required through the web interface:

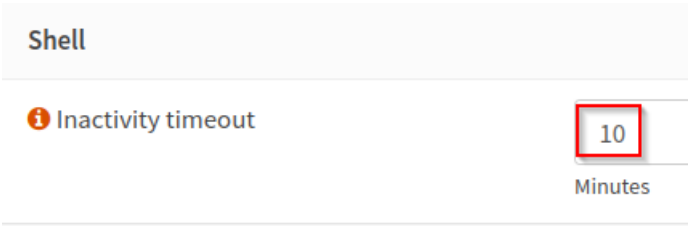
1. Enable the access log parameter in the Settings menu. In the left panel go to System > Settings > Administration and select “enable access log”.



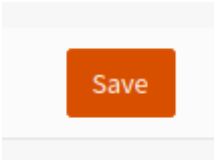
2. Enable SSH by password for admin users, do not allow root user login.



3. Define an “Inactivity timeout” of 10 minutes for the SSH shell.

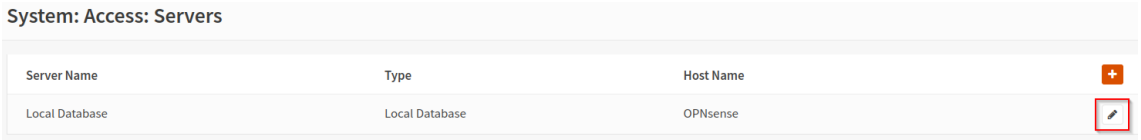


4. Press “Save”.

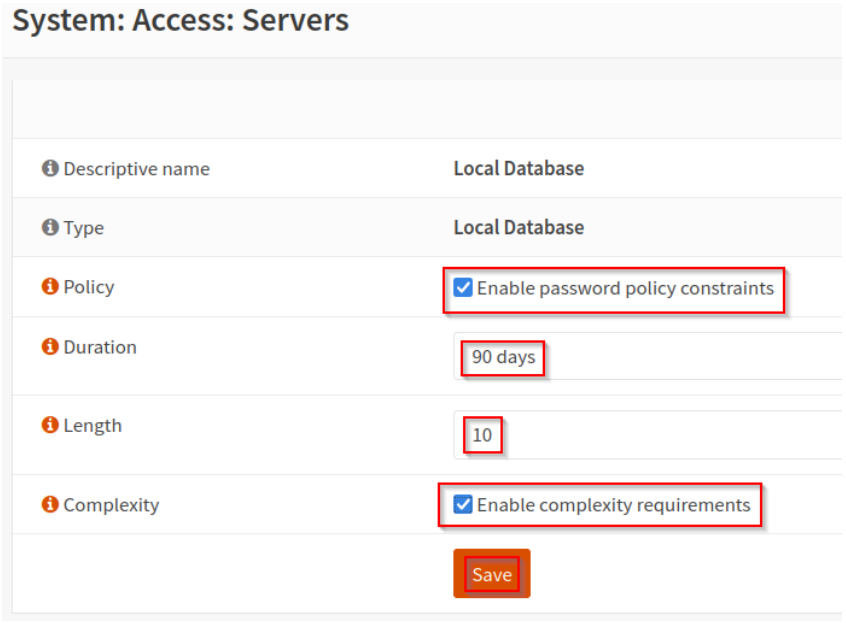


5. Define a password policy. In the left panel, go to System > Access > Servers.

6. Press the edit button.

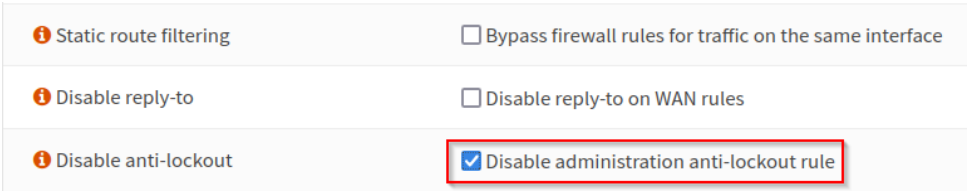


7. Enable “Password policy constraints”. Then, add a duration for passwords, the minimum length and enable complexity requirements. Finally, press “Save”.

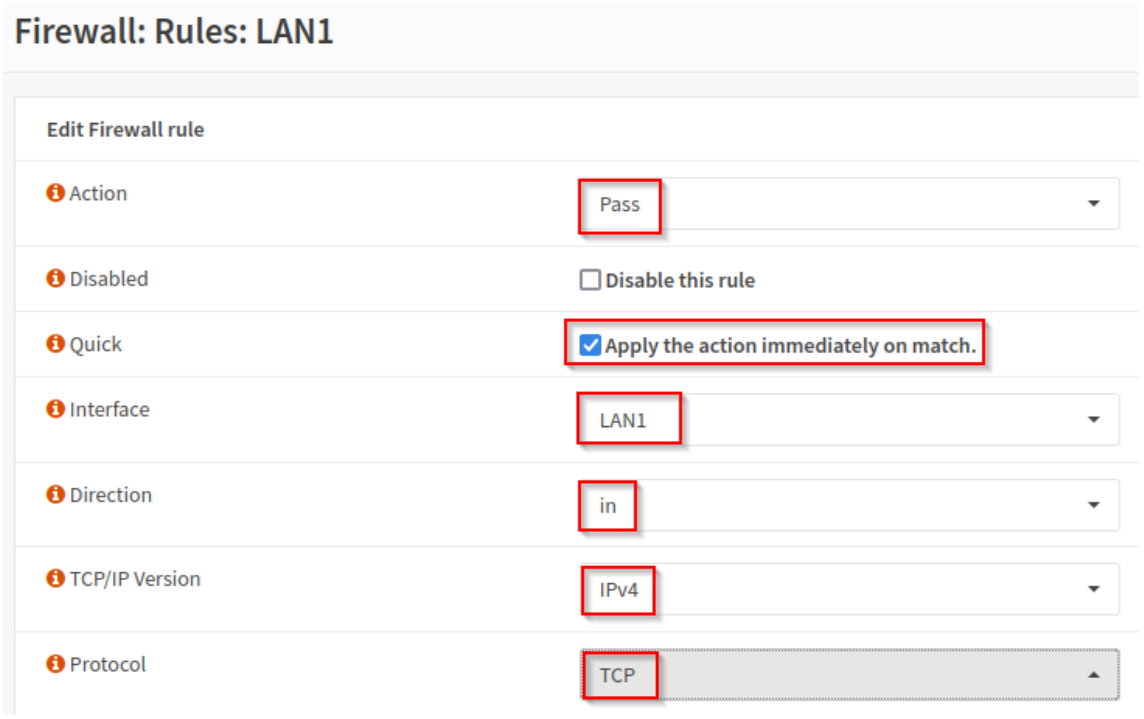


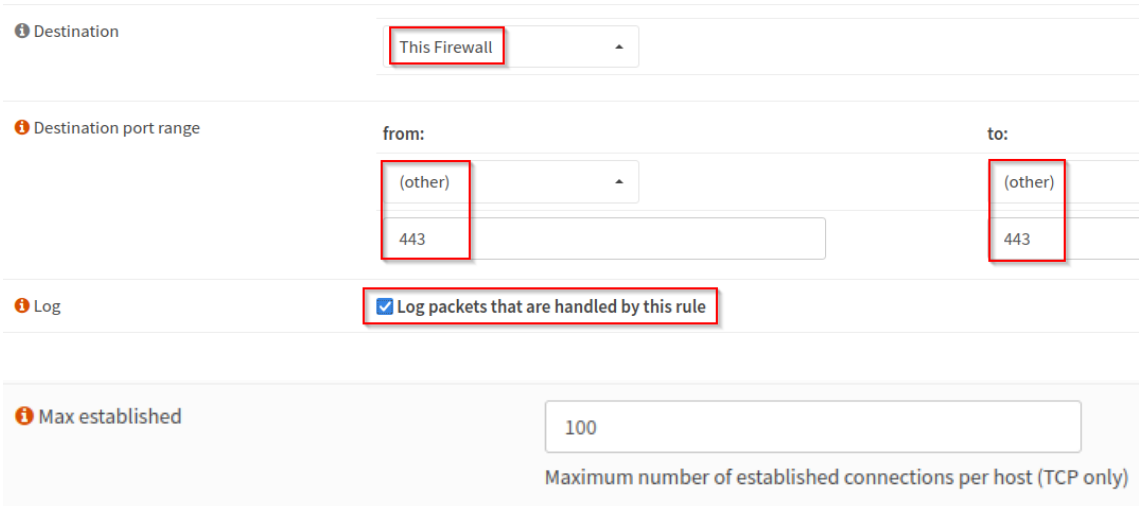
To protect the TOE against DoS attacks, log in into [TOE-2210] through the web interface and follow the next steps:

1. Go to Firewall > Settings > Advanced and mark the "Disable anti-lockout" option.



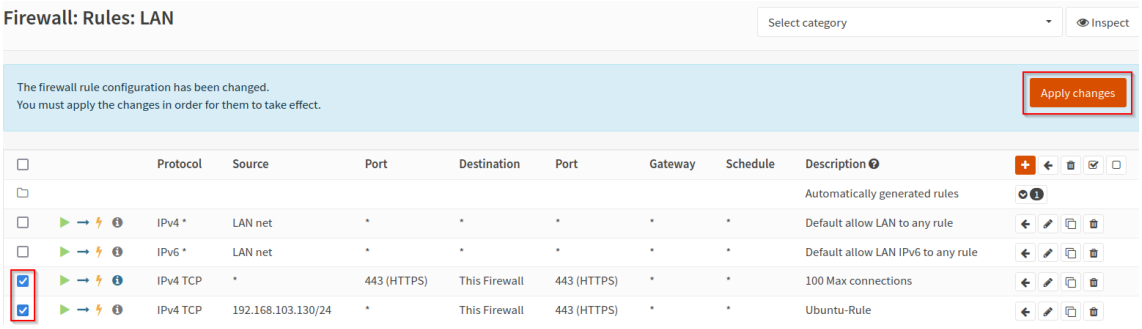
2. Go to Firewall > Rules > LAN and create a new rule for allowing a maximum of 100 simultaneous connections to the Firewall administration web page.





3. Create another with the same parameters, but only allowing <IP-UBUNTU> as source address.

4. Select both rules in the top and click on “Apply changes”.

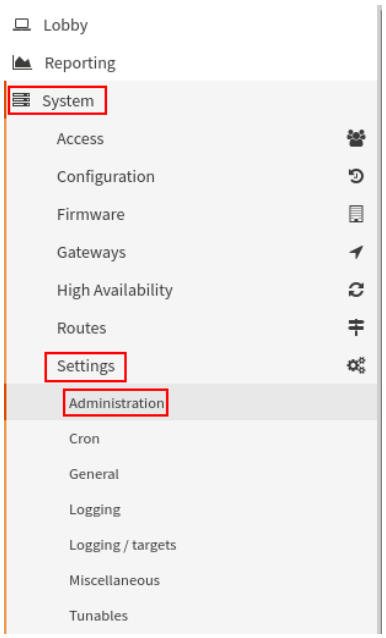


Finally, it is recommended to install a digital certificate signed by a trusted CA. However, a self-signed certificate generated by [TOE-2210] itself is used in this evaluation, as it does not imply a degradation in the quality level at the functionality or testing of [TOE-2210]. This matter is taken into account by the evaluator when conducting the testing.

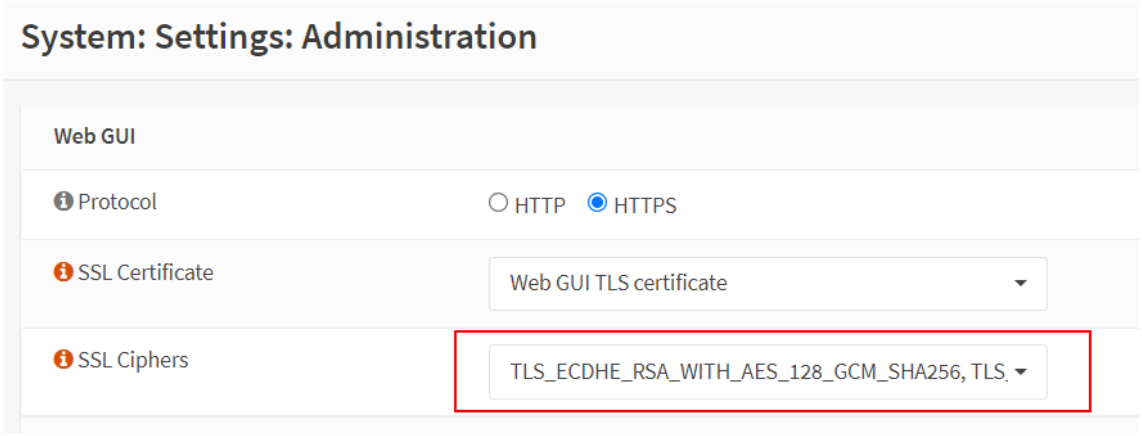
6.3.2 WEB INTERFACE TLS CIPHER SUITES CONFIGURATION

In order to meet the cryptographic requirements and conform [CCN-STIC-807], 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 [TOE-2210]. The steps below are followed:

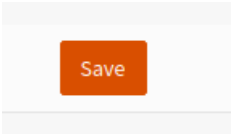
1. Log in through the web interface for [TOE-2210] with the root user.
2. Navigate to System > Settings > Administration.



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



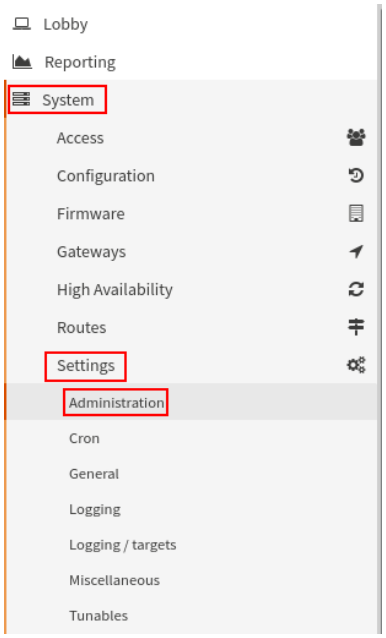
4. Scroll down and click Save.



6.3.3 SSH CRYPTOGRAPHIC PARAMETERS CONFIGURATION

In order to meet the cryptographic requirements and conform [CCN-STIC-807], it is required to configure accepted cryptographic parameters for SSH through the web interface. This configuration affects the SSH connections that users establish with [TOE-2210]. The steps below are followed:

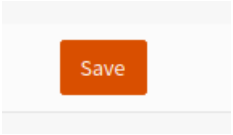
1. Log in through the web interface for [TOE-2210] with the root user.
2. Navigate to System > Settings > Administration.



3. In the Secure Shell section, click “Show cryptographic overrides”.

4. 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-group14-sha256
        ii. diffie-hellman-group16-sha512
        iii. diffie-hellman-group18-sha512
        iv. ecdh-sha2-nistp256
        v. ecdh-sha2-nistp384
        vi. ecdh-sha2-nistp521
    b. Ciphers:
        i. aes128-gcm@openssh.com
        ii. aes256-gcm@openssh.com
    c. MACs:
        i. hmac-sha2-256
        ii. hmac-sha2-512
    d. Public key signature algorithms:
        i. ecdsa-sha2-nistp256
        ii. ecdsa-sha2-nistp384
        iii. ecdsa-sha2-nistp521

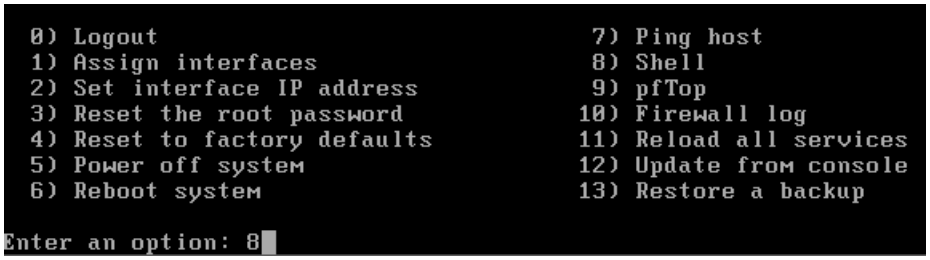
5. Scroll down and click Save.



6.3.4 SYSLOG CLIENT TLS CIPHER SUITES CONFIGURATION

In order to meet the cryptographic requirements and conform [CCN-STIC-807], it is required to configure accepted cipher suites through the local command line interface. This configuration affects the TLS connections when [TOE-2210] communicates with a remote syslog server. The steps below are followed:

1. Log in through the local command line for [TOE-2210] and select the Shell option.



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")`

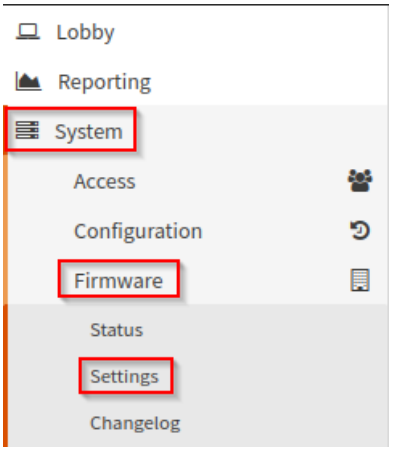
```
    network(
        "{{destination.hostname}}"
        transport("tls")
        port({{destination.port}})
        ip-protocol({{destination.transport[3]}})
        persist-name("{{dest_key}}")
        tls(
                ca-file("/etc/ssl/cert.pem")
                key-file("/usr/local/etc/syslog-ng/cert.d/{{dest_key}}.key")
                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_
SHA256:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-A
ES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES128-CCM")
        )
    );
```

4. Save the file.
5. Restart the syslog-ng service.

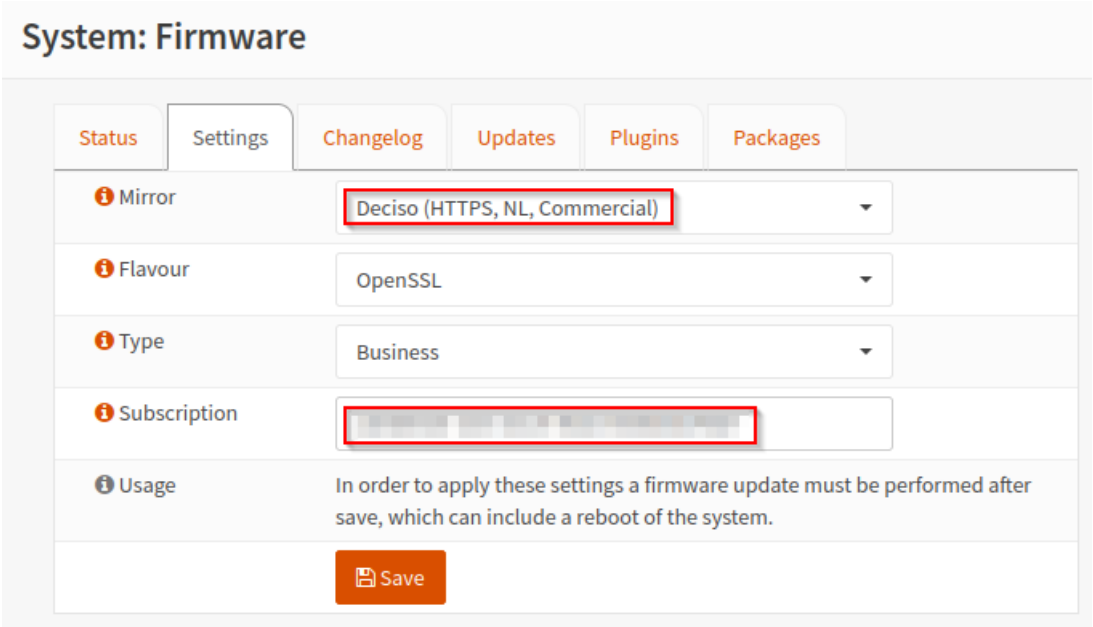
6.3.5 LICENSE ACTIVATION

In order to download updates of [TOE-2210], must be specified the license key in the product configuration.

1. Go to [TOE-2210] web interface and log in.
2. Navigate to “System > Firmware > Status”.



3. Specify the “Mirror” and “Subscription”.

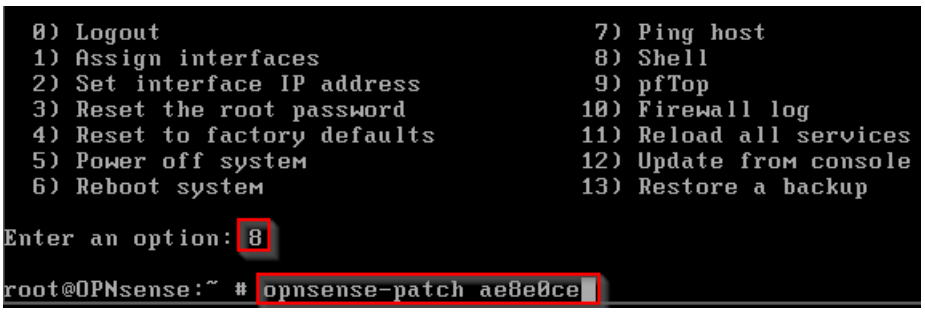


4. Save the changes.

6.3.6 PATCH INSTALLATION

In order to [TOE-2210] works correctly is necessary to install a new patch provided by the vendor.

1. Go to [TOE-2210].
2. Select option 8 and execute the following command to apply the patch.



3. Wait for the patch to finish.

```
;
;As the client still might have a state when being kicked-out, we should kill an
y state the client has while adding it to the alias. Apparantly our ssh messages
 are only catched partially, so add ".*Authentication error for .*" to the list
as well. To ease testing, better detect the location of the timestamp so we can
use a construction like this to feed amn existing log:
;
;lockout_handler < /var/log/audit/audit_20221205.log
;---
; src/opnsense/scripts/syslog/lockout_handler | 9 ++++++---
; 1 file changed, 6 insertions(+), 3 deletions(-)
;
;diff --git a/src/opnsense/scripts/syslog/lockout_handler b/src/opnsense/scripts
/syslog/lockout_handler
;index 75d55bf441..c6eb045030 100755
;--- a/src/opnsense/scripts/syslog/lockout_handler
;+++ b/src/opnsense/scripts/syslog/lockout_handler
--------------------------
Patching file opnsense/scripts/syslog/lockout_handler using Plan A...
Hunk #1 succeeded at 41 (offset -2 lines).
Hunk #2 succeeded at 95 (offset -1 lines).
Hunk #3 succeeded at 104 (offset -1 lines).
done
All patches have been applied successfully.  Have a nice day.
root@OPNsense:~ #
```

4. Reboot the system.

6.4 USED INSTALLATION OPTIONS

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

6.5 RESULTS

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

ID	Comments	State
N/A	None.	N/A

7 CONFORMITY ASSESSMENT

7.1 DOCUMENTATION ANALYSIS

Documents analyzed	[OPNSENSE-LINCE-ST16] [DOC-74b13d1]
Evaluator	JAL
Days required	1 days.
Results of the evaluator's work	**PASS**

7.1.1 EVALUATION ACTIVITIES

The information presented in this section covers the requirements of the standard, in section 4.3 of [CCN-STIC-2002], with respect to the evaluation activities on documentation analysis.

TE.3.1. The evaluator shall list the analyzed documents.

PASS The list of analyzed documents is presented in the row *Documents analyzed* of the table in the *7.1 Documentation analysis.*

TE.3.2. The evaluator shall check that the provided information meets the requirements related to content and presentation (section 3 of [CCN-STIC-2002]), providing a verdict about its completeness and legibility. If there is a big a volume of information to be reviewed, the evaluator may, after notifying the Certification Body, implement a sampling strategy in accordance to the following priorities:

- **The Security Target provided by the manufacturer;**
- **TOE preparative and operative guidance;**

PASS The documentation provided by the manufacturer complies with section 3 of [CCN-STIC-2002].

TE.3.3. The evaluator shall register every non-conformity in regards to any deviation of the evaluated documentation.

PASS The results of the analysis of the documentation provided by the manufacturer are reflected in the section 7.1.2 *Results*.

7.1.2 RESULTS

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

ID	Comments	State
N/A	None.	N/A

7.2 FUNCTIONAL TESTS

Evaluator	JAL
Days required	3 days.
Results of the evaluator's work	**PASS**

7.2.1 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 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. If the tests are not complete, the evaluator shall provide a rationale regarding the used sampling strategy.

PASS Information concerning this task of the evaluator can be found in the section 7.2.2 List of functional tests. This information is presented in more detail in the section 13 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 *7.2.3 Results*.

7.2.2 LIST OF FUNCTIONAL TESTS

The evaluator has sampled the tests performed in the previous LINCE evaluation and has determined a set of tests to repeat for the Business edition. This set of tests have been approved by CPSTIC.

Security function	Test code	Objective	Result
SF. Reliable Administration	[STIC_OPNSENSE_CQ-TST-1020]	Verify that [TOE-2210] allows to set a session termination by inactivity time in the Web Interface.	**PASS**
SF. Reliable Administration	[STIC_OPNSENSE_CQ-TST-1021]	Verify that [TOE-2210] allows to set a session termination by inactivity time in the SSH server.	**PASS**
SF. Reliable Administration	[STIC_OPNSENSE_CQ-TST-1022]	Verify that [TOE-2210] allows to configure the following	**PASS**

		parameters in the Web Interface: • Protocols • SSL Certificate • SSL Ciphers • TCP Port • Alternate Hostnames • Listen Interfaces • HTTP Compression	
SF. Reliable Administration	[STIC_OPNSENSE_CQ-TST-1023]	Verify that [TOE-2210] allows to configure the following parameters for SSH server: • Enable secure shell • Login group • Permit root user login • Permit password login • SSH Port • Listen interfaces	**PASS**
SF. Identification and authentication	[STIC_OPNSENSE_CQ-TST-2020]	Verify that [TOE-2210] does not allow brute force attacks targeting its Web Interface, blocking the attacker's IP address.	**PASS**
SF. Identification and authentication	[STIC_OPNSENSE_CQ-TST-2021]	Verify that [TOE-2210] does not allow brute force attacks through SSH.	**PASS**
SF. Reliable communication channels SF. Cryptographic requirements	[STIC_OPNSENSE_CQ-TST-3010]	Verify that [TOE-2210] establishes a secure channel via SSH when a user establishes a connection in accordance with [CCN-STIC-807].	**PASS**

SF. Reliable communication channels SF. Cryptographic requirements	[STIC_OPNSENSE_CQ-TST-3011]	Verify that [TOE-2210] establishes a secure channel via HTTPS/TLS v1.2 when a user establishes a connection in accordance with [CCN-STIC-807].	**PASS**
SF. Reliable communication channels SF. Cryptographic requirements	[STIC_OPNSENSE_CQ-TST-3012]	Verify that [TOE-2210] establishes a secure channel via TLS v1.2 when sending information to an external syslog server in accordance with [CCN-STIC-807].	**PASS**
SF. Reliable installation and upgrades	[STIC_OPNSENSE_CQ-TST-4010]	Verify that the [TOE-2210] allows to check its current version of the firmware/software.	**PASS**
SF. Reliable installation and upgrades	[STIC_OPNSENSE_CQ-TST-4040]	Verify that the [TOE-2210] allows to start updates manually and to check if there are new updates available.	**PASS**
SF. Audit	[STIC_OPNSENSE_CQ-TST-5010]	Verify that the [TOE-2210] generates audit data for login and logout of registered users and contains at least date and time of the event, type of event identified, result of the event and user producing the event.	**PASS**
SF. Audit	[STIC_OPNSENSE_CQ-TST-5011]	Verify that the [TOE-2210] generates audit data when the user credentials are modified and contains at least date and time of the event, type of event identified, result of the event and user producing the event.	**PASS**
SF. Audit	[STIC_OPNSENSE_CQ-TST-5012]	Verify that the [TOE-2210] generates audit data when the [TOE-2210] configuration is modified and contains at least date and time of the event, type of event identified, result of the event and user producing the event.	**PASS**
SF. Audit	[STIC_OPNSENSE_CQ-TST-5013]	Verify that the [TOE-2210] generates audit data for events related to product functionality	**PASS**

		and contains at least date and time of the event, type of event identified, result of the event and user producing the event.	
SF. Audit	[STIC_OPNSENSE_CQ-TST-5014]	Verify that the [TOE-2210] generates audit data for generation, import, change or deletion of cryptographic keys and contains at least date and time of the event, type of event identified, result of the event and user producing the event.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-TST-6040]	Verify that the [TOE-2210] count and/or add to the logs packets which are invalid packet fragments.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-TST-6041]	Verify that the [TOE-2210] counts the fragmenting packets which cannot be re-assembled.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-TST-6042]	Verify that the [TOE-2210] drops and/or registers packets where its source address is a broadcast IP address.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-TST-6043]	Verify that the [TOE-2210] drops and/or registers packets where its source address is a multicast IP address.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-TST-6044]	Verify that the [TOE-2210] drops and/or adds to the log packets where the source or destination address of the network packet is defined as being unspecified or an address reserved for future use in IPv4.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-TST-6045]	Verify that the [TOE-2210] drops and/or to the log packets where the source or destination address of the network packet is defined as being unspecified or an address reserved for future use in IPv6.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-TST-6046]	Verify that [TOE-2210] is able to drop and also to add to the log the packets with IP options.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-TST-6047]	Verify that the [TOE-2210] counts and/or add to the logs	**PASS**

		packets which are invalid packet fragments.	
SF. Firewall	[STIC_OPNSENSE_CQ-TST-6080]	Verify that the [TOE-2210] is capable of limiting a defined number of half-open TCP connections, dropping all the new connections that overpass this limit logging the event.	**PASS**

7.2.3 RESULTS

ID	Non-conformity	State
OR02.NC01	[STIC_OPNSENSE_CQ-TST-2020] [STIC_OPNSENSE_CQ-TST-2021] [TOE-2210] is not properly providing brute force protection. It seems that [TOE-2210] is not killing the current state when the maximum limit of attempts is reached by the same connection. Moreover, SSH login protection seems insufficient as the lockout is only working if the username is also being brute forced. Password failed login attempts for an existing user does seem to be properly monitored. The developer implemented changes in the lockout handler and the protection is now being provided as expected.	**CLOSED**

ID	Comments	State
N/A	None.	N/A

8 VULNERABILITY ANALYSIS

Evaluator	JAL
Days required	2 days.
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 4.5 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.

PASS The TOE vulnerability analysis is described in the *8.3 TOE vulnerability* del TOE. The result of this analysis is detailed in the section

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. The evaluator shall document every identified potential vulnerability applicable to the TOE scope.

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.5.4. The evaluator shall compute the attack potential for every potential vulnerability in accordance to the punctuation system presented in the section 4.5.1 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.

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.

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.

8.4 LIST OF POTENTIAL VULNERABILITIES

Code	Resistance level
[STIC_OPNSENSE_CQ-VUL-1010]	BASIC
[STIC_OPNSENSE_CQ-VUL-1020]	BASIC
[STIC_OPNSENSE_CQ-VUL-1030]	BASIC
[STIC_OPNSENSE_CQ-VUL-1050]	BASIC
[STIC_OPNSENSE_CQ-VUL-1060]	BASIC
[STIC_OPNSENSE_CQ-VUL-1120]	BASIC

[STIC_OPNSENSE_CQ-VUL-1130]	BASIC
[STIC_OPNSENSE_CQ-VUL-2010]	BASIC
[STIC_OPNSENSE_CQ-VUL-2030]	BASIC
[STIC_OPNSENSE_CQ-VUL-2040]	BASIC
[STIC_OPNSENSE_CQ-VUL-3010]	BASIC
[STIC_OPNSENSE_CQ-VUL-3020]	BASIC
[STIC_OPNSENSE_CQ-VUL-3030]	BASIC
[STIC_OPNSENSE_CQ-VUL-4010]	BASIC
[STIC_OPNSENSE_CQ-VUL-5010]	BASIC
[STIC_OPNSENSE_CQ-VUL-6010]	BASIC
[STIC_OPNSENSE_CQ-VUL-7010]	BASIC
[STIC_OPNSENSE_CQ-VUL-8010]	BASIC

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	JAL
Days required	3 days.
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 4.6 of [CCN-STIC-2002], with regard to the TOE penetration tests.

TE.6.1. The evaluator shall provide a list with all the penetration tests performed on the TOE including, at least, the required steps to reproduce each test, the expected result, the actual result and whether the attack is successful or not.

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
SF. Reliable Administration	[STIC_OPNSENSE_CQ-PT-1010]	Verify that [TOE-2210] does not allow non-privileged users to perform privileged users' actions with specified URLs.	PASS
SF. Reliable Administration	[STIC_OPNSENSE_CQ-PT-1020]	Verify that [TOE-2210] does not allow to gain access to the management interfaces with the default credentials.	PASS
SF. Reliable Administration	[STIC_OPNSENSE_CQ-PT-1030]	Verify that the [TOE-2210] is not vulnerable to SQL injection.	PASS
SF. Reliable Administration	[STIC_OPNSENSE_CQ-PT-1050]	Verify that [TOE-2210] does not allow user enumeration by Web Interface messages.	PASS
SF. Reliable Administration	[STIC_OPNSENSE_CQ-PT-1060]	Verify that the [TOE-2210] is not vulnerable to directory traversal.	PASS
SF. Reliable Administration	[STIC_OPNSENSE_CQ-PT-1120]	Verify that the user root is not allowed to manage the [TOE-2210] via SSH.	PASS
SF. Reliable Administration	[STIC_OPNSENSE_CQ-PT-1130]	Verify that [TOE-2210] does not allow non-privileged user to access through SSH.	PASS
SF. Reliable Administration	[STIC_OPNSENSE_CQ-PT-2010]	Verify that the [TOE-2210] does not allow bypassing of password policies.	PASS

SF. Identification and authentication	[STIC_OPNSENSE_CQ-PT-2030]	Verify that [TOE-2210] does not store password in plain-text.	**PASS**
SF. Identification and authentication	[STIC_OPNSENSE_CQ-PT-2040]	Verify that [TOE-2210] does not allow an attacker to block the root account by brute-force in the Web Interface.	**PASS**
SF. Reliable communication channels	[STIC_OPNSENSE_CQ-PT-3010]	Verify that [TOE-2210] does not allow to downgrade HTTPS to HTTP.	**PASS**
SF. Reliable Communications channels	[STIC_OPNSENSE_CQ-PT-3020]	Verify that the [TOE-2210] does not allow to establish a SSH connection with insecure SSH versions.	**PASS**
SF. Reliable communication channels	[STIC_OPNSENSE_CQ-PT-3030]	Verify if [TOE-2210] authenticates the external syslog server.	**PASS**
SF. Reliable communication channels	[STIC_OPNSENSE_CQ-PT-3031]	Verify that [TOE-2210] properly verifies the certificate from the external syslog server.	**PASS**
SF. Reliable communication channels	[STIC_OPNSENSE_CQ-PT-3032]	Verify if it is possible to exploit a XSS vulnerability by indicating the payload in the fields from a certificate of a remote syslog server.	**PASS**
SF. Reliable communication channels SF. Cryptographic requirements	[STIC_OPNSENSE_CQ-PT-3033]	Verify that [TOE-2210] does not allow to use TLS versions lower that TLSv1.2 in the communication with an external syslog server.	**PASS**
SF. Reliable communication channels SF. Reliable installation and upgrades	[STIC_OPNSENSE_CQ-PT-4010]	Verify if an attacker is able to spoof the update server when [TOE-2210] is checking for updates.	**PASS**
SF. Audit	[STIC_OPNSENSE_CQ-PT-5010]	Verify that it is not possible to inject fake audit events in the [TOE-2210] log file or modify it.	**PASS**

SF. Firewall	[STIC_OPNSENSE_CQ-PT-7010]	Verify that [TOE-2210] correctly applies filtering rules on boot.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-PT-7011]	Verify that the [TOE-2210] correctly applies a rule that blocks UDP on boot.	**PASS**
SF. Firewall	[STIC_OPNSENSE_CQ-PT-7012]	Verify that [TOE-2210] does not allow rule bypassing when packets are fragmented.	**PASS**
All security functions	[STIC_OPNSENSE_CQ-PT-8010]	Verify that [TOE-2210] does not present exploitable vulnerabilities identified performing a scan with the tool Nessus.	**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 0.1. January 2020.

[CCN-STIC-2002] Evaluation Methodology for the National Essential Security Certification (LINCE), version 0.1. January 2020

[CCN-STIC-2003] Template for the Security Target of the National Essential Security Certification (LINCE), version 0.1. January 2020

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

[OPNSENSE-LINCE-ST16] LINCE Security Target v1.6.

[OPNSENSE-IAR-10] Impact analysis report v1.0 for [TOE-224].

[OPNSENSE-IAR-20] Impact analysis report v2.0 for [TOE-2210].

[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.

10.1 DEVELOPER EVIDENCES

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

11 ACRONYMS

CBS	Basic Security Certification
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
LINCE	National Essential Security Certification
MCF	Source Code Module
MEC	Cryptographic Evaluation Module
TIC	Information and Communications Technology
TOE	Target Of Evaluation
LAN	Local Area Network
WAN	Wide Area Network
IP	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
TLS	Transport Layer Security
SSH	Secure Shell
UFS	Unix File System
NTP	Network Time Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
DoS	Denial of Service
CA	Certification Authority
GUI	Graphical User Interface
CLI	Command Line Interface

SSL	Secure Sockets Layer
MAC	Message Authentication Code