jtsec
BEYOND IT SECURITY

STIC Evaluation Technical Report

STIC_OPNSENSE_IAD-2604 (CUA-2023-118)
1.0
25/05/2026

CHANGELOG

Version	Date	Author	Reason	Changes
1.0	25/05/2026	AGL	Document creation	N/A

TABLE OF CONTENTS

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.

No part of this report may be reproduced without the express permission of the laboratory.

1.1 EVALUATION TECHNICAL REPORT INFORMATION

ETR reference	STIC_OPNSENSE_IAD-2604-ETR-v1.0
ETR version	1.0
Author or authors	AGL
Reviewer	AMM
Approved by	JPC
Start date of the works	20/04/2026
End date of the works	25/05/2026
CB dossier code	CUA-2023-118
Laboratory project code	STIC_OPNSENSE_IAD-2604
Type of evaluation	Complementary STIC
Product Taxonomy	N/A
Evaluation Laboratory holding the accreditation	jtsec Beyond IT Security S.L (Unipersonal)
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	26.4
Operating manuals of the product	[TOE-DOCS-a95e580]

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 to as the TOE, is a stateful software-based firewall. It is in charge of interconnecting two or more networks, channeling 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 complete OPNsense Business edition solution offers a wide range of additional functionalities, such as VPN, proxy, intrusion detection, among others, the scope of evaluation (TOE) 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, to examine each message and filter 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 the TOE management, the TOE can be managed by two different interfaces:

- CLI interface:
    - Local access: Available directly on the machine where the TOE is installed, allowing administrators to perform the initial configuration, maintenance and management of the system without the need for a network connection.

- Remote access: which allows remote TOE management via SSHv2. The use of this interface is not allowed to the root user.

- GUI interface: it is a web interface which allows TOE management via HTTPS.

2.2 INVENTORY OF SECURITY FUNCTIONS

This evaluation uses as its baseline the latest complementary STIC evaluation previously conducted for the same TOE, **OPNsense Business Edition version 25.10** (Such evaluation will be named [STIC-2510]).

[STIC-2510] took as a baseline a previous complementary STIC evaluation. Such evaluation will be named [STIC-254], which in turn is based on a previous complementary STIC evaluation that was performed to pass from a LINCE certification to a ENS HIGH STIC qualification (Such evaluation will be named **[STIC-24101]**).

[STIC-2510], [STIC-254] and [STIC-24101] have CB dossier number **2024-13** and **qualification dossier [CUA-2023-118]**, and were carried out in accordance with the **Security Target [LINCE-ST-08].**

For [STIC-24101], the defined security functions and the pool of security requirements were extracted from different protection profiles and taxonomies. These are [cPP-ND-30e] and [PPMOD-FW-14e]. These supporting documents associated with these protection profiles ([cPP-ND-30e-SD] and [PPMOD-FW-14e-SD]) were followed by the evaluator when conducting the tests.

[STIC-254] **added additional testing and retesting** of some requirements (FCS_CKM.4.1, FCS_RBG_EXT.1.1, FCS_RBG_EXT.1.2) from the Collaborative Protection Profile for Network Devices [cPP-ND-30e] and FFW_RUL_EXT.1.6 from the Protection Profile Module for Stateful Traffic Filter Firewalls (PPMOD-FW-14e).

[STIC-2510] **did not add additional testing and retesting** as the changelogs did not reveal any change to the security functionalities of the TOE.

This evaluation (**[STIC-264]**) bumps the TOE OPNsense Business Edition **from version 25.10 to 26.4**. The associated Security Target for the TOE OPNsense ([LINCE-ST-08]) has not been updated since the previous STIC evaluation, and therefore, the inventory of Security Functions and Security Requirements remain the same. Given this rationale, the laboratory has attached in this section all the **Security Requirements evaluated in** [STIC-2510], [STIC-254] and [STIC-24101] to have more visibility about the continuous qualification.

To detect the security requirements that need to be retested, the laboratory developed the **Impact Analysis Report [IAR-10]** document, based on analyzing the changelogs between the latest evaluated version (25.10) from the actual evaluated version (26.4). Such Impact Analysis Report leveraged that **there are no security requirements that need to be retested**, as none of the changes from one version to another affect the

security functionalities of the TOE. Therefore, no functional tests were performed during this evaluation.

2.2.1 COLLABORATIVE PROTECTION PROFILE FOR NETWORK DEVICES

The following table includes the coverage analysis for the [cPP-ND-30e] Protection Profile:

Requirement in [cPP-ND-30e]	Covered?
FAU_GEN.1.1	**Partially covered** by the requirement AUD.1 included in the LINCE Security Target as some points defined in the requirement from the PP are mentioned in AUD.1 The features tested of this requirement are defined in the SFR definition included after this table.
FAU_GEN.1.2	**Partially covered** by the requirement AUD.2 included in the LINCE Security Target. The features tested of this requirement are defined in the SFR definition included after this table and are tied to the events declared in FAU_GEN.1.1.
FAU_GEN.2.1	**Partially covered** by the requirement AUD.2 included in the LINCE Security Target. The audit features tested are verified alongside the tests related to FAU_GEN.1.1 and FAU_GEN.1.2.
FAU_STG_EXT.1.1	Covered by AUD.4.
FAU_STG_EXT.1.2	Covered by AUD.4.
FAU_STG_EXT.1.3	Covered by AUD.4.
FAU_STG_EXT.1.4	The features tested of this requirement are defined in the SFR definition included after this table.
FAU_STG_EXT.1.5	The features tested of this requirement are defined in the SFR definition included after this table.
FAU_STG_EXT.1.6	Covered by AUD.4.
FCS_CKM.1.1	Dismissed for the present STIC evaluation, will be covered in future evaluation rounds.
FCS_CKM.2.1	Dismissed for the present STIC evaluation, will be covered in future evaluation rounds.
FCS_CKM.4.1	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_COP.1.1/DataEncryption	Dismissed for the present STIC evaluation, will be covered in future evaluation rounds.
FCS_COP.1.1/SigGen	Dismissed for the present STIC evaluation, will be covered in future evaluation rounds.
FCS_COP.1.1/Hash	Dismissed for the present STIC evaluation, will be covered in future evaluation rounds.

FCS_COP.1.1/KeyedHash	Dismissed for the present STIC evaluation, will be covered in future evaluation rounds.
FCS_RBG_EXT.1.1	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_RBG_EXT.1.2	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_UIA_EXT.1.1	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_UIA_EXT.1.2	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_UIA_EXT.1.3	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_UIA_EXT.1.4	The features tested of this requirement are defined in the SFR definition included after this table.
FMT_MOF.1.1/ManualUpdate	Covered by ADM.2, ADM.3 and ACT.3.
FMT_MTD.1.1/CoreData	Covered by ADM.3.
FMT_SMF.1.1	**Partially covered** by the requirement ADM.2 included in the LINCE Security Target. The management features to test are defined in the SFR definition included after this table.
FMT_SMR.2.1	Covered by ADM.1.
FMT_SMR.2.2	Covered by ADM.1.
FMT_SMR.2.3	Covered by ADM.2.
FPT_SKP_EXT.1.1	Covered by PSC.1.
FPT_STM_EXT.1.1	The features tested of this requirement are defined in the SFR definition included after this table.
FPT_STM_EXT.1.2	The features tested of this requirement are defined in the SFR definition included after this table.
FPT_TST_EXT.1.1	The features tested of this requirement are defined in the SFR definition included after this table.
FPT_TST_EXT.1.2	The features tested of this requirement are defined in the SFR definition included after this table.
FPT_TUD_EXT.1.1	Covered by ACT.1.
FPT_TUD_EXT.1.2	Covered by ACT.1.
FPT_TUD_EXT.1.3	Covered by ACT.2.
FTA_SSL.3.1	Covered by IAU.4.
FTA_SSL.4.1	Covered by AUD.1
FTA_TAB.1.1	The features tested of this requirement are defined in the SFR definition included after this table.
FTP_ITC.1.1	Covered by COM.1 and COM.2.
FTP_ITC.1.2	Covered by COM.2.
FTP_ITC.1.3	Covered by COM.2.
FTP_TRP.1.1/Admin	Covered by COM.4.
FTP_TRP.1.2/Admin	Covered by COM.4.
FTP_TRP.1.3/Admin	Covered by COM.4.

FCS_HTTPS_EXT.1.1	Covered by COM.1 and COM.4.
FCS_HTTPS_EXT.1.1	Covered by COM.1 and COM.4.
FCS_TLSS_EXT.1.1	Covered by COM.4 and CIF.1. The only TOE HTTPS/TLS server is the web management interface. TLS protocol version and cipher suites were verified in tests for such requirements.
FCS_TLSS_EXT.1.2	Covered by COM.3. The only TOE HTTPS/TLS server is the web management interface. The size of the key for the certificate in such HTTPS/TLS server was verified in the test related to such requirement.
FCS_TLSS_EXT.1.3	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_TLSS_EXT.1.4	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_TLSS_EXT.1.5	Covered by installation/configuration process. The configuration of a specific set of cipher suites is indicated in the LINCE Security Target as part of the TOE configuration process. As it has been possible to exercise the functionality related to this requirement through the installation, the requirement is considered fulfilled.
FCS_TLSS_EXT.1.6	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_TLSS_EXT.1.7	Functional testing not required as defined in the supporting document for [cPP-ND-30e], [cPP-ND-30e-SD].
FCS_TLSS_EXT.1.8	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_SSH_EXT.1.1	Covered by COM.4. Requirement from Functional Package [PKG-SSH-10].
FCS_SSH_EXT.1.2	Covered by COM.4 and IAU.1. Requirement from Functional Package [PKG-SSH-10].
FCS_SSH_EXT.1.3	The features tested of this requirement are defined in the SFR definition included after this table. Requirement from Functional Package [PKG-SSH-10].
FCS_SSH_EXT.1.4	Covered by COM.4. Requirement from Functional Package [PKG-SSH-10].
FCS_SSH_EXT.1.5	Covered by COM.4.

	Requirement from Functional Package [PKG-SSH-10].
FCS_SSH_EXT.1.6	Covered by COM.4. Requirement from Functional Package [PKG-SSH-10].
FCS_SSH_EXT.1.7	Functional testing not required as defined in the supporting document for [cPP-ND-30e], [cPP-ND-30e-SD].
FCS_SSH_EXT.1.8	The features tested of this requirement are defined in the SFR definition included after this table. Requirement from Functional Package [PKG-SSH-10].
FCS_SSHS_EXT.1.1	Covered by COM.4.
FCS_TLSC_EXT.1.1	Covered by COM.1 and CIF.1. The TOE acts as a TLS client when establishing a connection with the syslog server and with the update repository. TLS protocol version and cipher suites were verified in tests for such requirements for both communication channels.
FCS_TLSC_EXT.1.2	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_TLSC_EXT.1.3	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_TLSC_EXT.1.4	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_TLSC_EXT.1.5	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_TLSC_EXT.1.6	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_TLSC_EXT.1.7	The features tested of this requirement are defined in the SFR definition included after this table.
FCS_TLSC_EXT.1.8	Functional testing not required as defined in the supporting document for [cPP-ND-30e], [cPP-ND-30e-SD].
FCS_TLSC_EXT.1.9	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_X509_EXT.1.1/Rev	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_X509_EXT.1.2/Rev	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_X509_EXT.2.1	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_X509_EXT.2.2	The features tested of this requirement are defined in the SFR definition included after this table.

FIA_X509_EXT.3.1	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_X509_EXT.3.2	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_AFL.1.1	Covered by IAU.2, the configuration instructions included in the LINCE Security Target urge the user to configure a 2FA mechanism. This mechanism, that was tested in the LINCE evaluation, is deemed valid to cover the SFR defined in the PP.
FIA_AFL.1.2	Covered by IAU.2, the configuration instructions included in the LINCE Security Target urge the user to configure a 2FA mechanism. This mechanism, that was tested in the LINCE evaluation, is deemed valid to cover the SFR defined in the PP.
FIA_UAU.7.1	The features tested of this requirement are defined in the SFR definition included after this table.
FIA_PMG_EXT.1.1	Covered by IAU.3.
FPT_APW_EXT.1.1	The features tested of this requirement are defined in the SFR definition included after this table.
FPT_APW_EXT.1.2	The features tested of this requirement are defined in the SFR definition included after this table.
FMT_MOF.1.1/Functions	The features tested of this requirement are defined in the SFR definition included after this table.
FMT_MTD.1.1/CryptoKeys	The features tested of this requirement are defined in the SFR definition included after this table.
FTA_SSL_EXT.1.1	Covered by IAU.4.

Therefore, given the previous analysis, the Security Functional Requirements tested from the PP [cPP-ND-30e] were the following:

Requirement	SFR PP Description	Final description
FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a. Start-up and shut-down of the audit functions; b. All auditable events for the not specified level of audit; and c. All administrative actions comprising: •Administrative login and logout (name of Administrator account shall be logged if individual accounts are required for Administrators).	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shut-down of the audit functions; b) All administrative actions comprising: • Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged). • [selection: no other actions];

	•Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed). •Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged). •[selection: Resetting passwords (name of related Administrator account shall be logged), no other actions, [assignment: list of other uses of privileges]]; d. Specifically defined auditable events listed in Table 2.	c) Specifically defined auditable events: • Management of the TOE's trust store. • Discontinuous changes to time. • Initiation/termination/failure of the trusted channel with the remote audit server.
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (~~if applicable~~), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the cPP/ST, information specified in column three of Table 2.	Same description as in PP.
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.	Same description as in PP.

FAU_STG_EXT.1.4	The TSF shall be able to store [selection: persistent, nonpersistent] audit records locally with a minimum storage size of [assignment: number of records and/or file/buffer size(s)].	The TSF shall be able to store [selection: persistent] audit records locally with a minimum storage size of [assignment: maximum log file size * number of logs to be kept as defined].
FAU_STG_EXT.1.5	The TSF shall [selection: drop new audit data, overwrite previous audit records according to the following rule: [assignment: rule for overwriting previous audit records], [assignment: other action]] when the local storage space for audit data is full.	The TSF shall [selection: overwrite previous audit records according to the following rule: [assignment: maximum log file size and number of logs to be kept as defined]] when the local storage space for audit data is full.
FCS_CKM.4	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: • For plaintext keys in volatile storage, the destruction shall be executed by a [selection: single overwrite consisting of [selection: a pseudo-random pattern using the TSF's RBG, zeroes, ones, a new value of the key, [assignment: a static or dynamic value that does not contain any CSP]], destruction of reference to the key directly followed by a request for garbage collection]; • For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [selection: logically addresses the storage location of the key and performs a [selection: single, [assignment: number of	Verify that the TSF destroys cryptographic keys in accordance with a specified cryptographic key destruction method. • For plaintext keys in volatile storage, the destruction shall be executed by a single overwrite consisting of zeroes. • For plaintext keys in non-volatile storage, destruction shall be performed by invoking a TSF-provided interface that instructs another part of the TSF to destroy the abstraction representing the key.

	passes]-pass] overwrite consisting of [selection: a pseudo-random pattern using the TSF's RBG, zeroes, ones, a new value of the key, [assignment: a static or dynamic value that does not contain any CSP]]; instructs a part of the TSF to destroy the abstraction that represents the key]	
FCS_RBG_EXT.1.1	The TSF shall perform all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using [selection: Hash_DRBG [selection: SHA-256, SHA-384, SHA-512], HMAC_DRBG [selection: SHA-256, SHA384, SHA-512], CTR_DRBG (AES)].	Verify that the TSF performs all deterministic random bit generation services in accordance with ISO/IEC 18031:2011.
FCS_RBG_EXT.1.2	The deterministic RBG shall be seeded by at least one entropy source that accumulates entropy from [selection: [assignment: number of software-based sources] software-based noise source, [assignment: number of platform-based sources] platform-based noise source] with a minimum of [selection: 128 bits, 192 bits, 256 bits] of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011 Table C.1 "Security Strength Table for Hash Functions", of the keys and hashes that it will generate.	Verify that the deterministic RBG is seeded by at least one entropy source that accumulates entropy from software-based noise source or platform-based noise source with a minimum of entropy at least equal to the greatest security strength, according to ISO/IEC 18031:2011.
FCS_SSH_EXT.1.3	The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: number of bytes between 35,000 and 1 GB (inclusive)] in an SSH transport connection are dropped.	The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: 262135 bytes] in an SSH transport connection are dropped.

FCS_SSH_EXT.1.8	The TSF shall ensure that [selection: • a rekey of the session keys, • connection termination] occurs when any of the following thresholds are met: • one hour connection time • no more than one gigabyte of transmitted data, or • no more than one gigabyte of received data.	The TSF shall ensure that [selection: • a rekey of the session keys] occurs when any of the following thresholds are met: • one hour connection time • no more than one gigabyte of transmitted data, or • no more than one gigabyte of received data.
FCS_TLSC_EXT.1.2	The TSF shall verify that the presented identifier matches [selection: the reference identifier per RFC 6125 Section 6, IPv4 address in the CN or in the SAN, IPv6 address in the CN or in the SAN, IPv4 address in the SAN, IPv6 address in the SAN, the identifier per RFC 5280 Appendix A using [selection: id-atcommonName, id-at-countryName, id-at-dnQualifier, id-at-generationQualifier, idat-givenName, id-at-initials, id-at-localityName, id-at-name, id-atorganizationalUnitName, id-at-organizationName, id-at-pseudonym, id-atserialNumber, id-at-stateOrProvinceName, id-at-surname, id-at-title] and no other attribute types].	The TSF shall verify that the presented identifier matches [selection: the reference identifier per RFC 6125 Section 6, IPv4 address in the CN or in the SAN, and no other attribute types]. NOTE: SFR tested for the communication channel of the TOE with the audit server and the update repository.
FCS_TLSC_EXT.1.3	The TSF shall not establish a trusted channel if the server certificate is invalid [selection: • without any administrator override mechanism • except with the following administrator override: If the TSF fails to determine the revocation status the TSF shall allow the administrator to provide override authorization to	The TSF shall not establish a trusted channel if the server certificate is invalid [selection: • without any administrator override mechanism]. NOTE: SFR tested for the communication channel of the TOE with the audit server and the update repository.

	establish the connection on a per certificate basis.].	
FCS_TLSC_EXT.1.4	The TSF shall [selection: not present the Supported Groups Extension, present the Supported Groups Extension with the following curves/groups: [selection: secp256r1, secp384r1, secp521r1, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192] and no other curves/groups] in the Client Hello.	For the communication channel with the remote audit server: The TSF shall [selection: present the Supported Groups Extension with the following curves/groups: [selection: secp256r1, secp384r1, secp521r1], ~~and no other curves/groups~~ x448 and x25519] in the Client Hello. For the communication channel with the update repository: The TSF shall [selection: present the Supported Groups Extension with the following curves/groups: [selection: secp256r1, secp384r1, secp521r1], ~~and no other curves/groups~~ x448 and x25519] in the Client Hello.
FCS_TLSC_EXT.1.5	The TSF shall [selection: • present the signature_algorithms extension with support for the following algorithms: ○ rsa_pkcs1 with sha256(0x0401), ○ rsa_pkcs1with sha384(0x0501), ○ rsa_pkcs1 with sha512(0x0601), ○ ecdsa_secp256r1 with sha256(0x0403), ○ ecdsa_secp384r1 with sha384(0x0503), ○ ecdsa_secp521r1 with sha512(0x0603), ○ rsa_pss_rsae with sha256(0x0804),	For the communication channel with the audit server: The TSF shall [selection: • present the signature_algorithms extension with support for the following algorithms: [selection: ○ ecdsa_secp256r1 with sha256(0x0403), ○ ecdsa_secp384r1 with sha384(0x0503), ○ ecdsa_secp521r1 with sha512(0x0603), ○ rsa_pss_rsae with sha256(0x0804), ○ rsa_pss_rsae with sha384(0x0805), ○ rsa_pss_rsae with sha512(0x0806),

	○ rsa_pss_rsae with sha384(0x0805), ○ rsa_pss_rsae with sha512(0x0806), ○ rsa_pss_pss with sha256(0x0809), ○ rsa_pss_pss with sha384(0x080a), ○ rsa_pss_pss with sha512(0x080b) ○] and no other algorithms;	○ rsa_pss_pss with sha256(0x0809), ○ rsa_pss_pss with sha384(0x080a), ○ rsa_pss_pss with sha512(0x080b) ○] and no other algorithms;]. For the communication channel with the update repository: The TSF shall [selection: • present the signature_algorithms extension with support for the following algorithms: [selection: ○ ecdsa_secp256r1 with sha256(0x0403), ○ ecdsa_secp384r1 with sha384(0x0503), ○ ecdsa_secp521r1 with sha512(0x0603), ○ rsa_pss_rsae with sha256(0x0804), ○ rsa_pss_rsae with sha384(0x0805), ○ rsa_pss_rsae with sha512(0x0806), ○ rsa_pss_pss with sha256(0x0809), ○ rsa_pss_pss with sha384(0x080a), ○ rsa_pss_pss with sha512(0x080b) ○] and no other algorithms;].
FCS_TLSC_EXT.1.6	The TSF [selection: provides, does not provide] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.	The TSF [selection: provides] the ability to configure the list of supported ciphersuites as defined in FCS_TLSC_EXT.1.1.
FCS_TLSC_EXT.1.7	The TSF shall prohibit the use of the following extensions:	Same description as in PP.

	• Early data extension • Post-handshake client authentication according to RFC 8446, Section 4.2.6.	NOTE: SFR tested for the communication channel of the TOE with the audit server and the update repository.
FCS_TLSC_EXT.1.9	The TSF shall [selection: support TLS 1.2 secure renegotiation through use of the "renegotiation_info" TLS extension in accordance with RFC 5746, reject [selection: TLS 1.2, TLS 1.3] renegotiation attempts].	For the communication channel with the remote audit server: The TSF shall [selection: reject [selection: TLS 1.3] renegotiation attempts For the communication channel with the update repository: The TSF shall [selection: reject [selection: TLS 1.3] renegotiation attempts].
FCS_TLSS_EXT.1.3	The TSF shall perform key exchange using: [selection: • RSA key establishment with key size [selection: 2048, 3072, 4096] bits; • EC Diffie-Hellman key agreement over NIST curves [selection: secp256r1, secp384r1, secp521r1] and no other curves; • Diffie-Hellman parameters [selection: of size 2048 bits, of size 3072 bits, of size 4096 bits, of size 6144 bits, of size 8192 bits, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192]].	The TSF shall perform key exchange using: [selection: • EC Diffie-Hellman key agreement over NIST curves [selection: secp256r1, secp384r1, secp521r1], ~~and no other curves~~ x25519 and x448;].
FCS_TLSS_EXT.1.4	The TSF shall support [selection: no session resumption, session resumption based on session IDs according to RFC 5246 (TLS 1.2), session resumption based on session tickets according to RFC 5077 (TLS 1.2), session resumption according to RFC 8446 (TLS 1.3)].	The TSF shall support [selection: session resumption based on session tickets according to RFC 5077 (TLS 1.2), session resumption according to RFC 8446 (TLS 1.3)].

FCS_TLSS_EXT.1.6	The TSF shall prohibit the use of the following extensions: • Early data extension	Same description as in PP.
FCS_TLSS_EXT.1.8	The TSF shall [selection: support secure renegotiation in accordance with RFC 5746 by always including the "renegotiation_info" TLS extension in TLS 1.2 ServerHello messages, reject [selection: TLS 1.2, TLS 1.3] renegotiation attempts].	The TSF shall [selection: support secure renegotiation in accordance with RFC 5746 by always including the "renegotiation_info" TLS extension in TLS 1.2 ServerHello messages, reject [selection: TLS 1.3] renegotiation attempts].
FIA_UAU.7.1	The TSF shall provide only obscured feedback to the administrative user while the authentication is in progress at the local console.	Same description as in PP.
FIA_UIA_EXT.1.1	The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process: • Display the warning banner in accordance with FTA_TAB.1; • [selection: no other actions, automated generation of cryptographic keys, [assignment: list of services, actions performed by the TSF in response to non-TOE requests]].	The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process: • Display the warning banner in accordance with FTA_TAB.1; • [selection: no other actions].
FIA_UIA_EXT.1.2	The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.	Same description as in PP.
FIA_UIA_EXT.1.3	The TSF shall provide the following remote authentication mechanisms [selection: Web GUI password, SSH password, SSH public key, X.509 certificate, [assignment:	The TSF shall provide the following remote authentication mechanisms [selection: Web GUI password, SSH password] and local

	other authentication mechanism]] and local authentication mechanisms [selection: none, password-based, [assignment: other authentication mechanism]].	authentication mechanisms [selection: password-based].
FIA_UIA_EXT.1.4	The TSF shall authenticate any administrative user's claimed identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.	Same description as in PP.
FIA_X509_EXT.1.1/Rev	The TSF shall validate certificates in accordance with the following rules: • RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates. • The certification path must terminate with a trusted CA certificate designated as a trust anchor. • The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE. • The TSF shall validate the revocation status of the certificate using [selection: the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5, ~~no revocation method~~]. • The TSF shall validate the extendedKeyUsage field	The TSF shall validate certificates in accordance with the following rules: • RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates. • The certification path must terminate with a trusted CA certificate designated as a trust anchor. • The TSF shall validate a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE. • The TSF shall validate the revocation status of the certificate using [selection: a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3]. • The TSF shall validate the extendedKeyUsage field according to the following rules: ○ Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-

	according to the following rules: ○ Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. ○ Server certificates presented for DTLS/TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field. ○ Client certificates presented for DTLS/TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. ○ OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field.	kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. ○ Server certificates presented for DTLS/TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field. ○ Client certificates presented for DTLS/TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. ○ OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the extendedKeyUsage field. NOTE: SFR tested for the communication channel of the TOE with the audit server and the update repository.
FIA_X509_EXT.1.2/Rev	The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.	Same description as in PP. NOTE: SFR tested for the communication channel of the TOE with the audit server and the update repository.
FIA_X509_EXT.2.1	The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: DTLS, HTTPS, IPsec, SSH, TLS, no protocols] and [selection: code signing for system software updates	The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: HTTPS, TLS] and [selection: no additional uses]. NOTE: SFR tested for the communication channel of the

	[assignment: other uses], no additional uses].	TOE with the audit server and the update repository.
FIA_X509_EXT.2.2	When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: allow the Administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate].	When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: accept the certificate]. NOTE: SFR tested for the communication channel of the TOE with the audit server and the update repository.
FIA_X509_EXT.3.1	The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [selection: device-specific information, Common Name, Organization, Organizational Unit, Country].	The TSF shall generate a Certificate Request as specified by RFC 2986 and be able to provide the following information in the request: public key and [selection: Common Name, Organization, Organizational Unit, Country].
FIA_X509_EXT.3.2	The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.	Same description as in PP.
FMT_MOF.1.1/Functions	The TSF shall restrict the ability to [selection: determine the behaviour of, modify the behaviour of] the functions [selection: transmission of audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full] to Security Administrators.	The TSF shall restrict the ability to [selection: determine the behaviour of] the functions [selection: transmission of audit data to an external IT entity] to Security Administrators and authorized users with the "System: Logging: Logging" privilege.
FMT_MTD.1.1/CryptoKeys	The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators.	The TSF shall restrict the ability to manage the cryptographic keys to Security Administrators and authorized users with the "System: CA Manager" and "System: Certificate Manager" privileges.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions:	The TSF shall be capable of performing the following management functions:

	• Ability to administer the TOE remotely; • Ability to configure the access banner; • Ability to configure the remote session inactivity time before session termination; • Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates; • [selection: ○ Ability to start and stop services; ○ Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full); ○ Ability to modify the behaviour of the transmission of audit data to an external IT entity; ○ Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1; ○ Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full, changes to local audit storage size); ○ Ability to manage the cryptographic keys; ○ Ability to configure the cryptographic functionality;	• Ability to configure the access banner; • [selection: ○ Ability to manage the cryptographic keys; ○ Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors; ○ Ability to set the time which is used for time-stamps; ○ Ability to modify the behaviour of the transmission of audit data to an external IT entity;].

	○ Ability to configure thresholds for SSH rekeying; ○ Ability to configure the lifetime for IPsec SAs; ○ Ability to configure the list of supported (D)TLS ciphers; ○ Ability to configure the interaction between TOE components; ○ Ability to enable or disable automatic checking for updates or automatic updates; ○ Ability to re-enable an Administrator account; ○ Ability to set the time which is used for time-stamps; ○ Ability to configure NTP; ○ Ability to configure the reference identifier for the peer; ○ Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors; ○ Ability to generate Certificate Signing Request (CSR) and process CA certificate response; ○ Ability to administer the TOE locally; ○ Ability to configure the local session inactivity time before session termination or locking; ○ Ability to configure the authentication failure parameters for FIA_AFL.1; ○ Ability to manage the trusted public keys database; ○ Ability to manage the public key or certificate	

	used to validate the digital update; ○ No other capabilities].	
FPT_APW_EXT.1.1	The TSF shall store administrative passwords in non-plaintext form.	Same description as in PP.
FPT_APW_EXT.1.2	The TSF shall prevent the reading of plaintext administrative passwords.	Same description as in PP.
FPT_STM_EXT.1.1	The TSF shall be able to provide reliable time stamps for its own use.	Same description as in PP.
FPT_STM_EXT.1.2	The TSF shall [selection: allow the Security Administrator to set the time, synchronise time with an NTP server, obtain time from the underlying virtualization system].	The TSF shall [selection: allow the Security Administrator to set the time].
FTA_TAB.1.1	Before establishing a an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding unauthorised use of the TOE.	Before establishing an administrative user session the TSF shall display a Security Administrator-specified advisory notice and consent warning message regarding use of the TOE.

2.2.2 PP-MODULE FOR STATEFUL TRAFFIC FILTER FIREWALLS

The following table includes the coverage analysis for the [PPMOD-FW-14e] Protection Profile:

Requirement in [PPMOD-FW-14e]	Covered?
FAU_GEN.1	Covered by AUD.1 and AUD.2.
FDP_RIP.2.1	Functional testing is not required as defined in the supporting document for [PPMOD-FW-14e], [PPMOD-FW-14e-SD].
FFW_RUL_EXT.1.1	Covered by FWL.1.
FFW_RUL_EXT.1.2	Covered by FWL.1 and FWL.2.
FFW_RUL_EXT.1.3	Covered by FWL.2.
FFW_RUL_EXT.1.4	Covered by FWL.1 and FWL.2.
FFW_RUL_EXT.1.5	Covered by FWL.1 and FWL.4.
FFW_RUL_EXT.1.6	**Partially covered** by penetration tests executed in the LINCE evaluation. Paragraphs a), b), e), h) are considered covered in the LINCE evaluation.

	The paragraphs c), d), f) and g) are tested in the present STIC evaluation. Requirement was updated to ensure it drops and logs IPv4 and IPv6 network packets with invalid source or destination addresses, such as unspecified addresses or addresses reserved for future use.
FFW_RUL_EXT.1.7	**Not covered**, SFR to test in the present STIC evaluation.
FFW_RUL_EXT.1.8	Covered by FWL.2.
FFW_RUL_EXT.1.9	Covered by FWL.3.
FFW_RUL_EXT.1.10	**Not covered**, SFR to test in the present STIC evaluation.
FMT_SMF.1.1/FFW	Covered by ADM.2, FWL.1 and FWL.2.

Therefore, given the previous analysis, the Security Functional Requirements to test from this PP module [PPMOD-FW-14e] are the following:

Requirement	SFR PP Description	Final description
FFW_RUL_EXT.1.6	The TSF shall enforce the following default stateful traffic filtering rules on all network traffic: a) The TSF shall drop and be capable of [selection: counting, logging] packets which are invalid fragments; b) The TSF shall drop and be capable of [selection: counting, logging] fragmented packets which cannot be re-assembled completely; c) The TSF shall drop and be capable of logging packets where the source address of the network packet is defined as being on a broadcast network; d) The TSF shall drop and be capable	The TSF shall enforce the following default stateful traffic filtering rules on all network traffic: c) The TSF shall drop and be capable of [selection: logging] packets where the source address of the network packet is defined as being on a broadcast network; d) The TSF shall drop and be capable of [selection: logging] packets where the source address of the network packet is defined as being on a multicast network; f) The TSF shall drop and be capable of [selection: logging] network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4; g) The TSF shall drop and be capable of [selection: logging] network packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” (i.e.

	of logging packets where the source address of the network packet is defined as being on a multicast network; e) The TSF shall drop and be capable of logging network packets where the source address of the network packet is defined as being a loopback address; f) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4; g) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is defined as an “unspecified address” or an address “reserved for future definition and use” (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6;	unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6; i) [selection: no other rules].

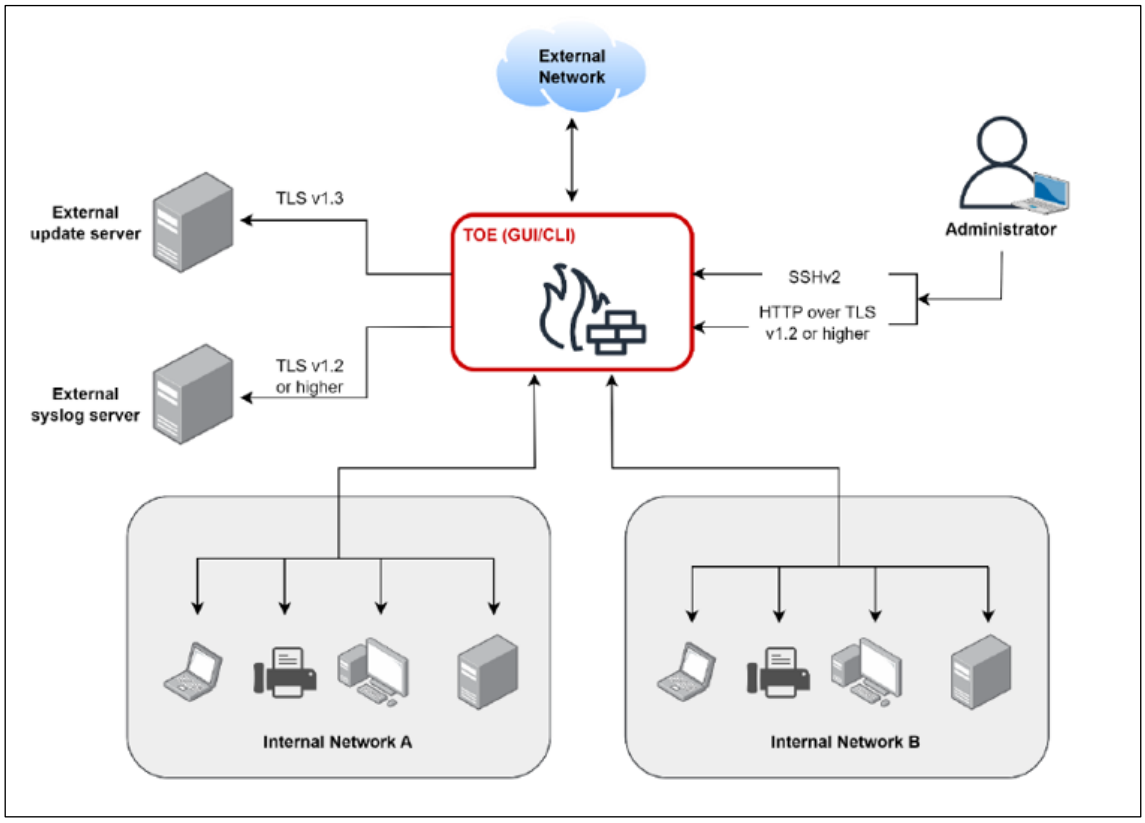
	h) The TSF shall drop and be capable of logging network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified; and i) [selection: [assignment: other default rules enforced by the TOE], no other rules].	
FFW_RUL_EXT.1.7	The TSF shall be capable of dropping and logging according to the following rules: a) The TSF shall drop and be capable of logging 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; b) The TSF shall drop and be capable of logging network packets where the source or destination address of the network packet is a link-local address; c) The TSF shall drop and be capable of logging network packets where the source address of the network packet does not belong to the networks associated with the network interface where the	Same description as in PP.

	network packet was received.	
FFW_RUL_EXT.1.10	The TSF shall be capable of limiting an administratively defined number of half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped and the drop event shall be [selection: counted, logged].	The TSF shall be capable of limiting an administratively defined number of half-open TCP connections. In the event that the configured limit is reached, new connection attempts shall be dropped and the drop event shall be [selection: logged].

3 OPERATIONAL ENVIRONMENT

3.1 DESCRIPTION OF THE OPERATIONAL ENVIRONMENT

The operational environment described by the manufacturer that is required to make the product possible is set out below:



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

- **Administrator**: The Administrator user has the permissions to configure and manage the TOE. 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 must only provide erase functionality as its primary function and must not provide any other functionality or service.
A. TRUSTED ADMINISTRATION	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. TRUSTED PLATFORM	In the case of a software product, it shall run on a trusted platform, including the operating system or any runtime environment provided by the platform.
A. ACCESS	The tool has access to all the system information necessary to carry out all its functionalities.

4 EXECUTIVE SUMMARY OF THE EVALUATION

This assessment is a STIC evaluation of the OPNsense Business Edition version 26.4

This evaluation uses as its baseline the latest complementary STIC evaluation previously conducted for the same TOE, **OPNsense Business Edition version 25.10** (Such evaluation will be named **[STIC-2510]).**

[STIC-2510] took as a baseline a previous complementary STIC evaluation. Such evaluation will be named [STIC-254], which in turn is based on a previous complementary STIC evaluation that was performed to pass from a LINCE certification to a ENS HIGH STIC qualification (Such evaluation will be named **[STIC-24101]**).

[STIC-2510], [STIC-254] and [STIC-24101] have CB dossier number **2024-13** and **qualification dossier [CUA-2023-118]** and were carried out in accordance with the **Security Target [LINCE-ST-08].**

For [STIC-24101], the defined security functions and the pool of security requirements were extracted from different protection profiles and taxonomies. These are **[cPP-ND-30e]** and **[PPMOD-FW-14e]**. These supporting documents associated with these protection profiles ([cPP-ND-30e-SD] and [PPMOD-FW-14e-SD]) were followed by the evaluator when conducting the tests.

[STIC-254] **added additional testing and retesting** of some requirements (FCS_CKM.4.1, FCS_RBG_EXT.1.1, FCS_RBG_EXT.1.2) from the Collaborative Protection Profile for Network Devices [cPP-ND-30e] and FFW_RUL_EXT.1.6 from the Protection Profile Module for Stateful Traffic Filter Firewalls (PPMOD-FW-14e).

[STIC-2510] **did not add additional testing and retesting** as the changelogs did not reveal any change to the security functionalities of the TOE.

This evaluation (**[STIC-264]**) bumps the TOE OPNsense Business Edition **from version 25.10 to 26.4**. The associated Security Target for the TOE OPNsense ([LINCE-ST-08]) has not been updated since the previous STIC evaluation, and therefore, the inventory of Security Functions and Security Requirements remain the same. Given this rationale, the laboratory has attached in section ***2.2 Inventory of security functions*** all the **Security Requirements evaluated in** [STIC-2510], [STIC-254] and [STIC-24101] to have more visibility about the continuous qualification.

The laboratory received the TOE OPNSense Business Edition 26.4 ISO at the start of the evaluation ([TOE-264]), and the associated documentation ([TOE-DOCS-a95e580]).

To detect the security requirements that need to be retested, the laboratory developed the **Impact Analysis Report [IAR-10]** document, based on analyzing the changelogs between the latest evaluated version (25.10) from the actual evaluated version (26.4). Such Impact Analysis Report leveraged that **there are no security requirements that need to be retested**, as none of the changes from one version to another affect the security functionalities of the TOE. Therefore, the section related to the security requirements testing is not included in the present report.

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

This evaluation dismisses the Security Target Analysis phase as it does not involve its own Security Target and depends on a previously evaluated security target ([LINCE-ST-08]).

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

Afterwards, the penetration tests were carried out to identify and exploit potential vulnerabilities in the TOE.

The execution of the penetration test revealed the following non-conformity:

- **OR01.NC01**: It was verified that it is possible to perform open redirect attacks through the [TOE-264] OPNcentral plugin login functionality. [TOE-264] does not properly validate the “page” parameter, allowing to redirect users to an external website.

A comment has been registered to problem found that do not currently affect the security of the TOE. The following comment was found:

- **OR01:CO01**: It is possible to perform a stored XSS attack by creating a custom Monit service in “Services → Monit → Settings” that relies on a file containing the XSS payload. When navigating to “Services → Monit → Status”, [TOE-264] displays the Monit status and the XSS payload is rendered and executed in the browser. To perform this attack, the user requires the “WebCfg – Services: Monit System Monitoring page”, and both the **Monit and HTTPD services must be enabled, which are not part of the default configuration**.

The identified non-conformity and comment were notified to the manufacturer and recorded in the Observation Report 01 version 1.0 (**[OR01-10]**).

Since there was an OPEN non-conformity, the laboratory determined that the verdict of the evaluation was **FAIL**.

The manufacturer notified about a plugin update to fix **OR01.NC01** and a patch to fix **OR01.CO01**. The laboratory updated the plugin (os-OPNBEcore) to version 1.8_2 and installed https://github.com/opnsense/core/commit/0bb5afb3aed39 patch. These steps have been added in the sub-section **6.2.15** ***Updating os-OPNBEcore plugin to version 1.8_2 and installing patch***.

Afterwards, the laboratory proceeded to perform the tests that generated the non-conformity and the comment to verify if they have been fixed correctly.

After repeating the tests, the non-conformity and comment from **[OR-01]** were deemed addressed by the manufacturer:

- **OR01.NC01**: In the updated [TOE-264] os-OPNBEcore plugin it is included a session validation functionality, in which the "page" parameter is only processed when the session exists. In addition, an ACL is implemented to check if the user is allowed to access the destination path generated. For low privileged users, the ACL is enforced and the user is redirected to the internal lobby dashboard. However, for a highly privileged user such as "root", the destination is accepted and it is possible to perform an open redirect. This is not considered a non-conformity due to to Assumption A.Trusted Administration.
- **OR01.CO01**: The updated [TOE-264] patch (https://github.com/opnsense/core/commit/0bb5afb3aed39) uses the "strip_tags()" function which return a string with all NULL bytes, HTML and PHP tags stripped from a given string, preventing the creating of HTML tags containing XSS payloads. Therefore, it is not possible to perform a stored XSS attack by creating a custom Monit service.

Nevertheless, a new comment was generated from **OR01.NC01**, as it is still possible to perform open redirect attacks using high privileged users such as root. The following comment was registered:

- **OR01.CO02**: It is possible to perform an open redirect attack through the [TOE-264] OPNcentral plugin login functionality. [TOE-264] does not properly validate the "page" parameter, allowing to redirect users to an external website. However, due to an ACL, only highly privileged users such as "root" are allowed to perform this attack.

The status of non-conformities and comments was updated by the evaluator and the Observation Report **[OR01-11]** was generated.

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

5 VERDICT OF THE EVALUATION

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

The TOE preparation and configuration process of the TOE does not reveal any non-conformity.

The Security Target analysis tasks do not reveal any non-conformity.

The penetration tests do not reveal any non-conformity.

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

Documents used during installation	[TOE-DOCS-a95e580]
Evaluator	AGL
Days required	2 days
Date	25/05/2026
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 for these tasks on the TOE and its documentation.

TE.2.1. Check 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 functions 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 in a secure manner.

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 multiple versions of the operating system, the operating system used and its version must be indicated as precisely as possible (patch, service pack, etc.).**
- **If the product allows for multiple modes of assembly/configuration (set-up), the guides must clearly indicate which mode is evaluated. ~~The identification of this mode shall be indicated in the Security Target~~.**
- **If the product allows for 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 available in the product.**

PASS The evaluator has been able to install the product exclusively following the contents of the manufacturer's documentation, provided through [TOE-DOCS-a95e580].

TE.2.4. Check that the installed TOE version 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 section 6.3 *Verification of the installed TOE version*.

TE.2.5. Describe 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 section 6.2 *Description of the installation and configuration of the TOE*.

TE.2.6. Describe all specific system configuration data, when applicable.

PASS The specific system configuration data used during the TOE preparation and configuration process is reflected in section 6.4 *Used installation options*.

TE.2.7. Register every non-conformity in relation to the installation and configuration of the TOE or the test environment.

PASS No non-conformities remain open regarding the installation process of the TOE and its documentation. The results are summarized in section 6.5*6.5 Results*.

6.2 DESCRIPTION OF THE INSTALLATION AND CONFIGURATION OF THE TOE

Before starting the installation steps for the TOE OPNsense, a virtual machine with [TOE-ISO-264] (the TOE OPNsense ISO installer) is required, and it must meet the minimum hardware requirements (1 GB RAM and 8 GB disk space). Also, another virtual machine with a web browser and connectivity to the TOE OPNsense virtual machine must be used to access the TOE OPNsense console.

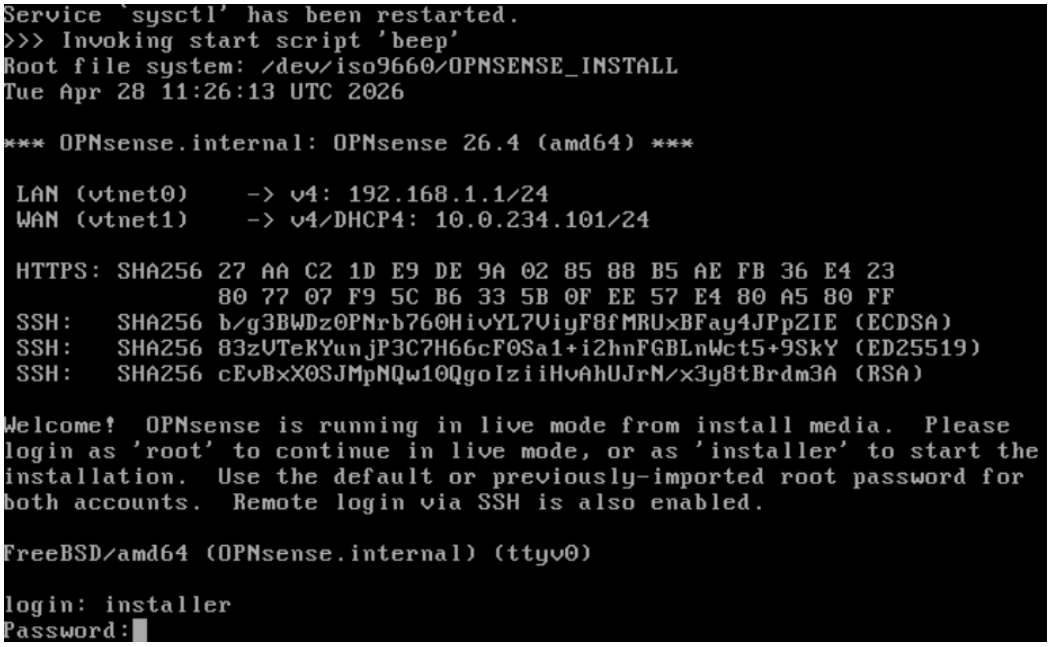
6.2.1 ISO INSTALLATION

The following steps are followed to install the TOE OPNsense:

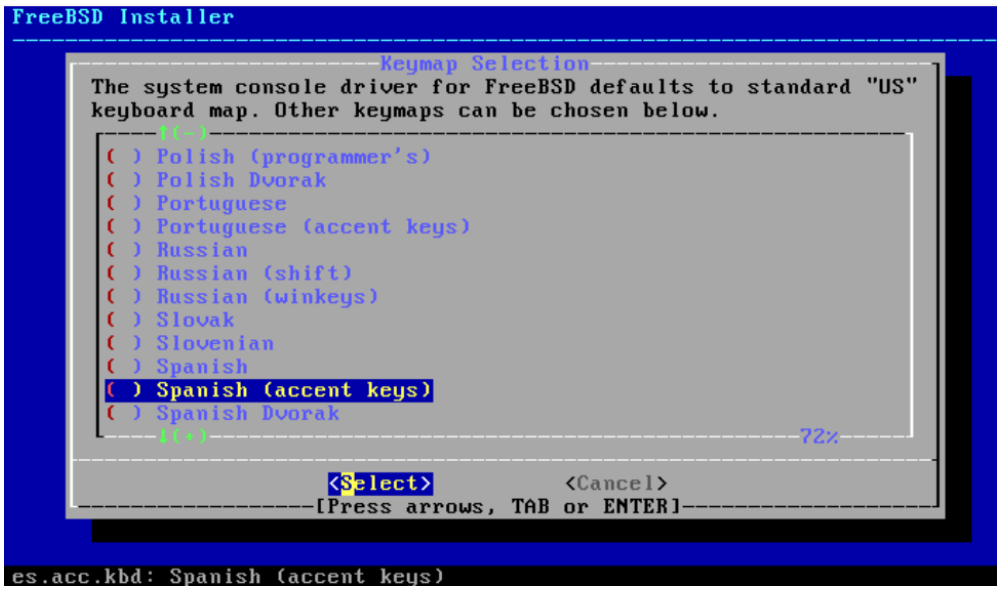
1. Start the virtual machine with [TOE-ISO-264] as the main boot order.

2. Wait for the TOE OPNsense to boot up.

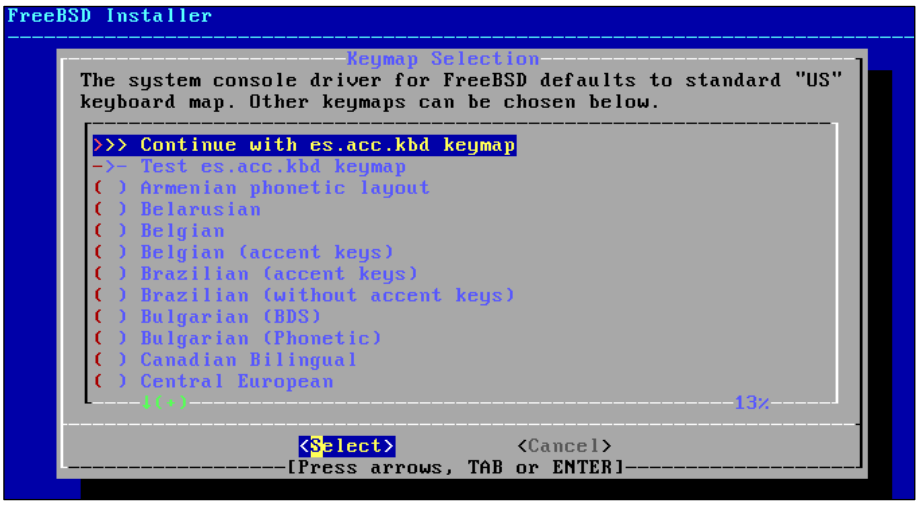
3. Log in with the user “installer” and authenticate with the password “opnsense”:



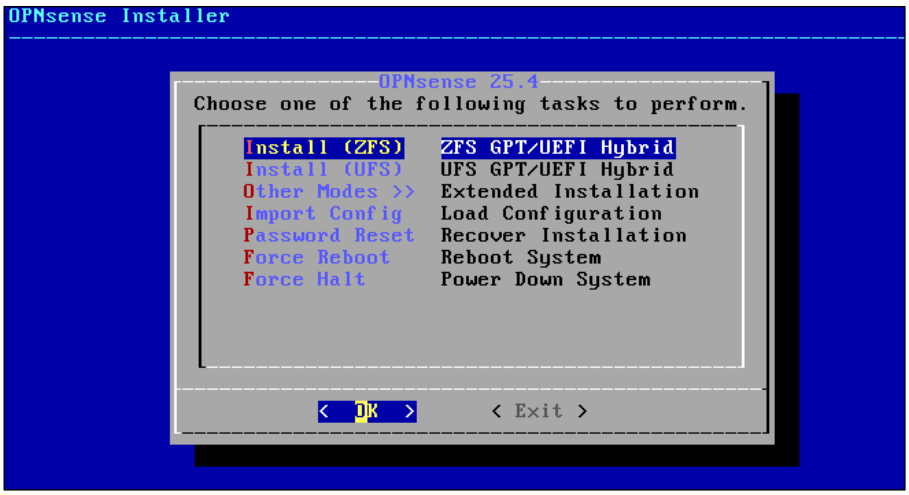
4. Select the keyboard layout and press Enter:



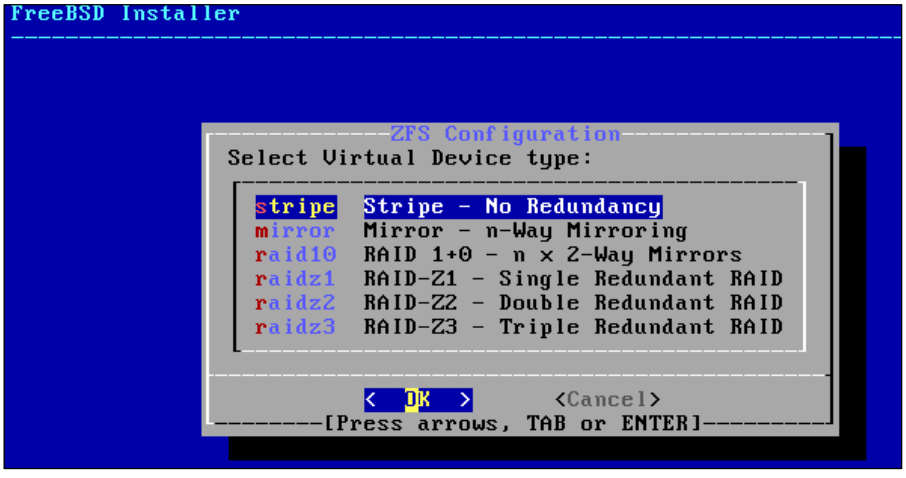
5. Select “Continue with es.acc.kbd.keymap” and press Enter:



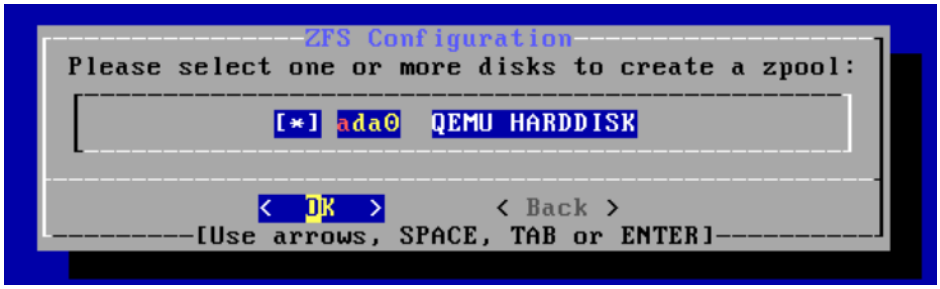
6. Select “Install (ZFS) and press Enter:



7. Select “Stripe” and press Enter:

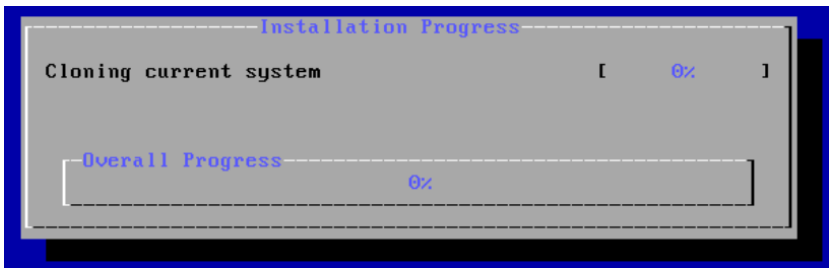


8. Press “Space” to select the virtual disk and press “OK”:

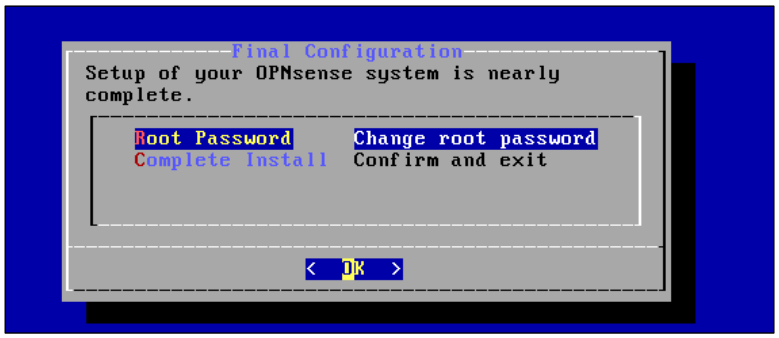


9. Select “Yes” and press “Enter”:

10. Wait for the installation process to finish:

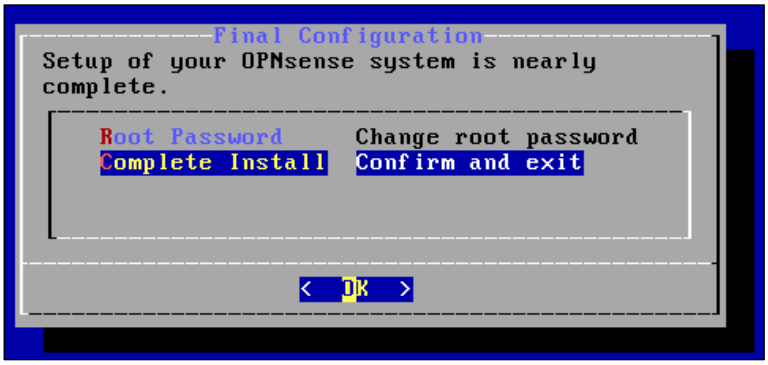


11. Select “Change root password” and press “OK”:

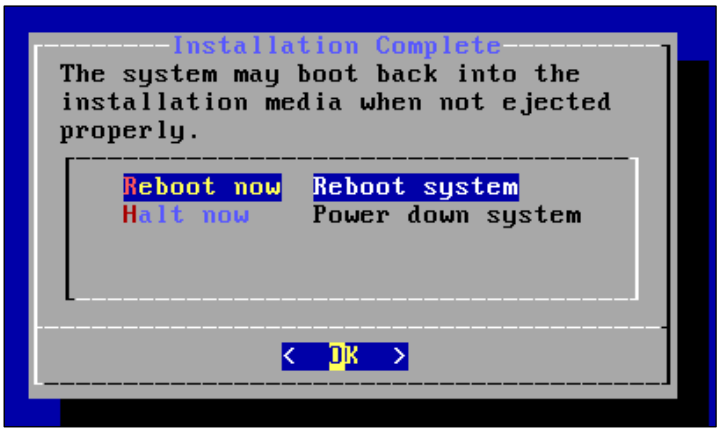


12. Define the password for the root user and press “OK”:

13. Select “Complete install” and press Enter:



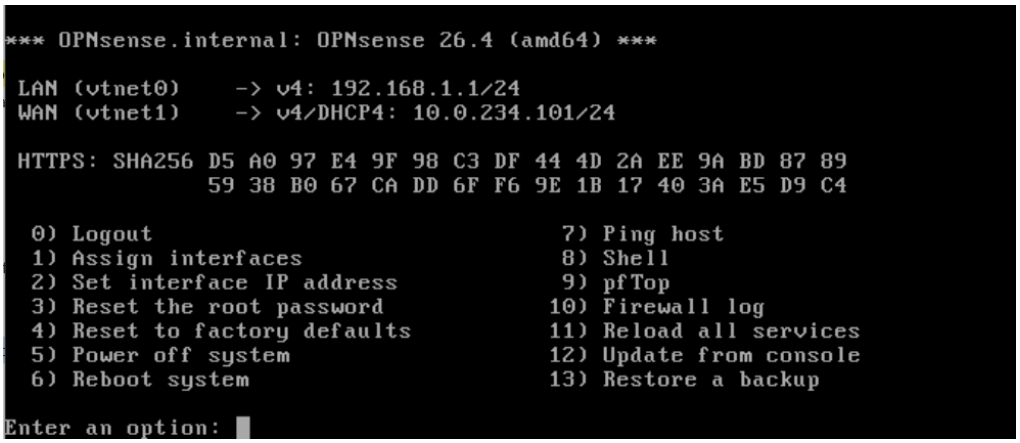
14. Select “Reboot now” and press Enter:



15. Change the boot order for the hard disk instead of the ISO disk. Reboot the TOE OPNsense.

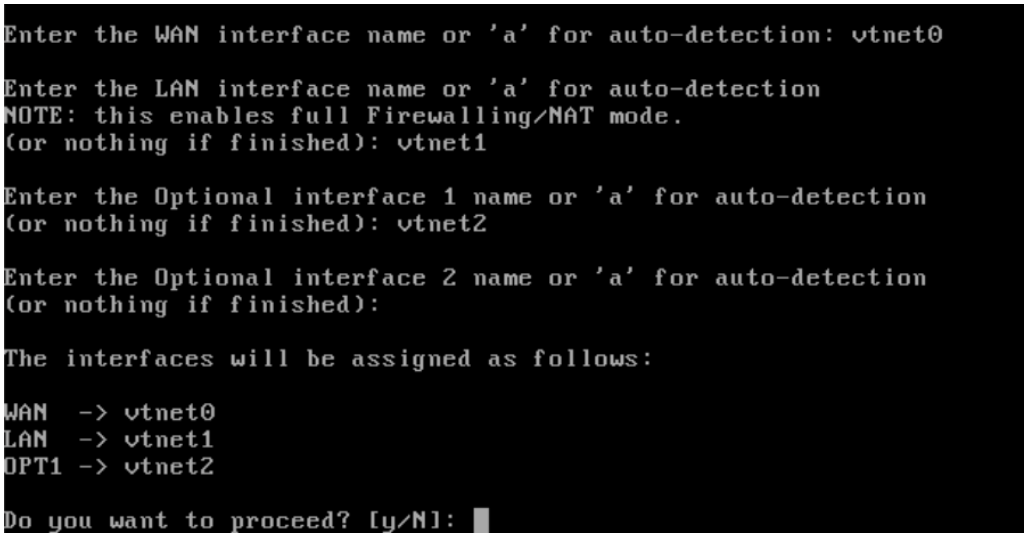
16. Log in with root credentials.

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

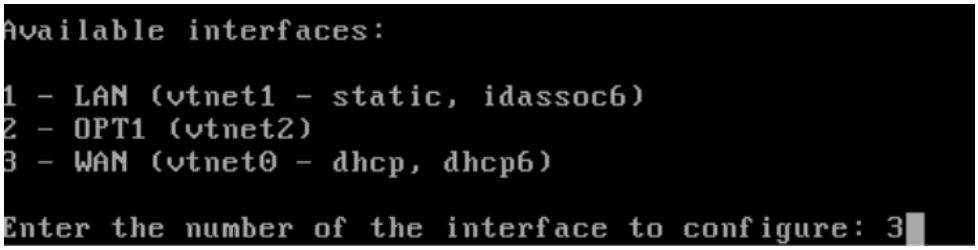


18. Enter “N” when prompted to configure LAGGs and VLANs:

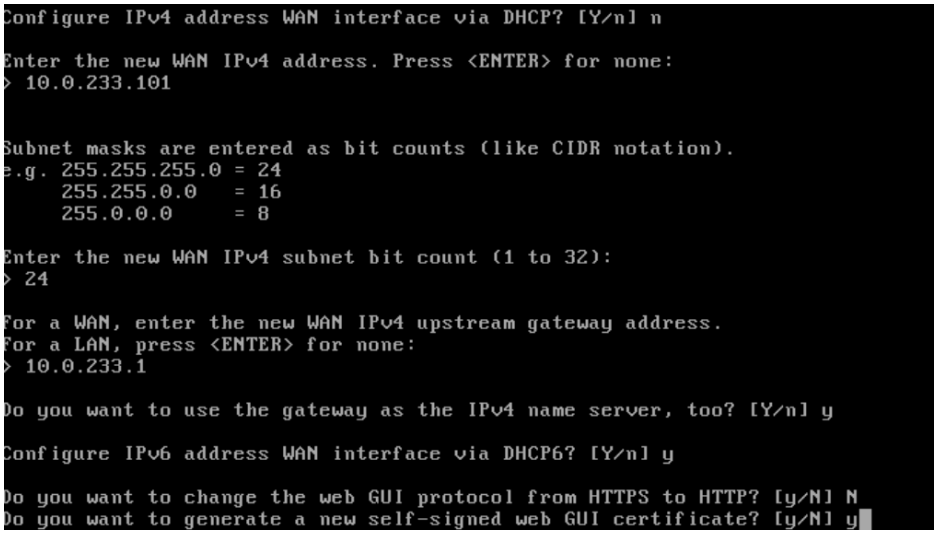
19. Enter the WAN interface name. In this case is “vtnet0”.
20. Enter the LAN interface name. In this case is “vtnet1”. This interface will be the LAN1 interface.
21. Enter the Optional interface name. In this case is “vtnet2”. This interface will be the LAN2 interface.
22. Enter “y” and press “Enter”:



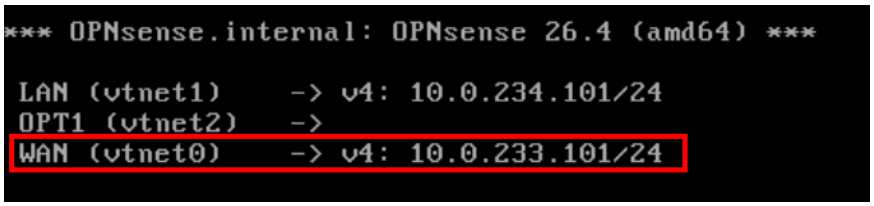
23. In the TOE OPNsense CLI menu, select option 2 and press Enter.
24. Select “vtnet0” interface.



25. Enter “n”.
26. Enter the WAN IPv4 address. Then enter “24” as subnet mask bit count. Then enter the WAN IPv4 gateway address.
27. Enter “y” when prompted to use the gateway as the IPv4 name server.
28. Enter “y” and press “Enter” when prompted to configure IPv6 address WAN interface via DHCP6.
29. Enter “N” and press “Enter” when prompted to change the web GUI protocol from HTTPS to HTTP.
30. Enter “y” and press enter when prompted to generate a new self-signed web GUI certificate and restore web GUI access defaults.



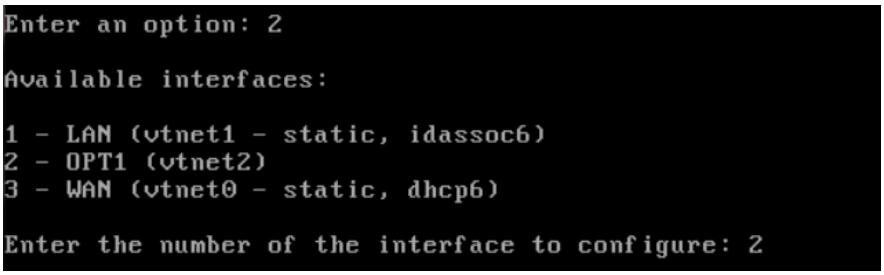
31. Verify that the IP network interface has been set correctly:



32. As the LAN1 interface is properly configured, no further configuration is needed.

33. In the TOE OPNsense CLI menu, select option 2 and press Enter.

34. Select LAN2 (vtnet2) interface:



35. Enter “n” and press “Enter” when prompted to configure IPv4 address LAN interface via DHCP. Then enter a valid IPv4 address for such LAN and the “24” subnet mask bit count.

36. Press “Enter” when prompted to skip the upstream gateway address.

37. Enter “Y” and press “Enter” when prompted to configure IPv6 address LAN interface via WAN tracking.

38. Enter “Y” and press “Enter” when prompted to enable the DCHP server on LAN and change the web GUI protocol from HTTPS to HTTP.

39. Enter “Y” and press “Enter” when prompted to generate new self-signed web GUI certificate and restore web GUI access defaults.

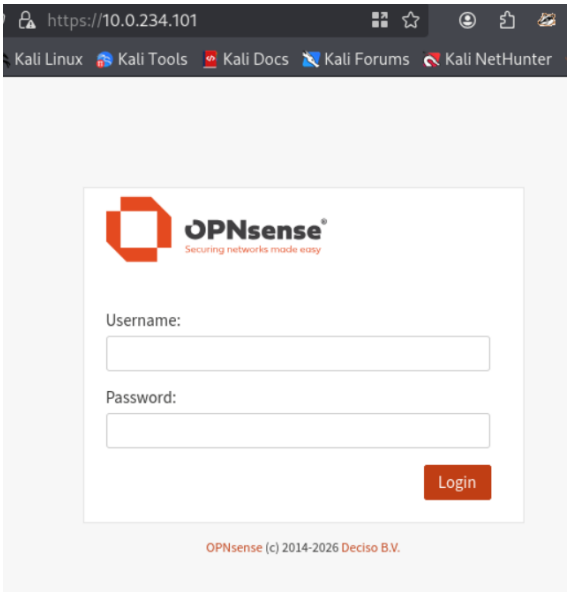
```
Configure IPv4 address OPT1 interface via DHCP? [y/N] N

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 10.0.235.101


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

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address OPT1 interface via WAN tracking? [Y/n] Y

Do you want to enable the DHCP server on OPT1? [y/N] N
```

```
Do you want to enable the DHCP server on OPT1? [y/N] N

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

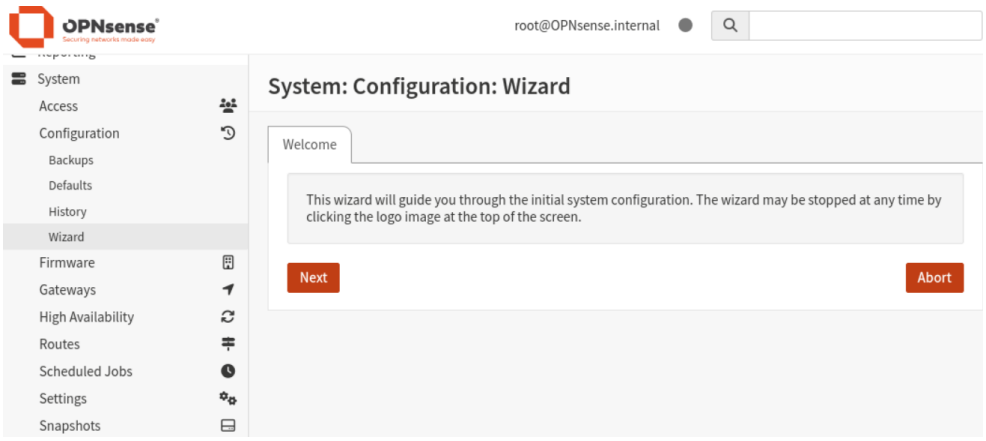
40. Verify the network IP interface has been set correctly:

```
OPT1 (vtnet2)    -> v4: 10.0.235.101/24
```

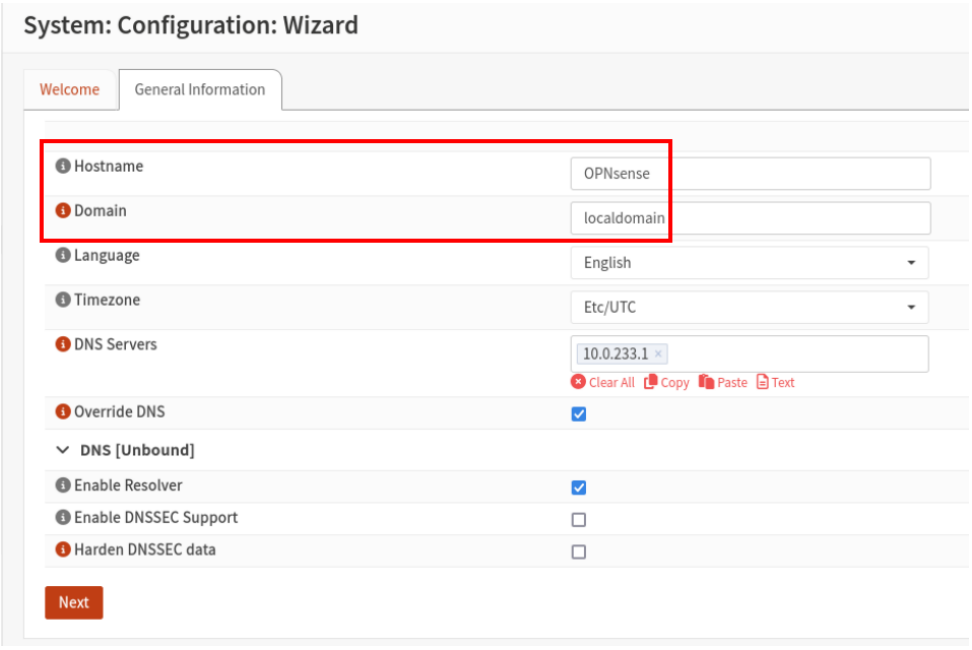
41. In another device in the same LAN as “vtnet1” interface, in this case KALI1 machine, access the TOE OPNsense IP address through HTTPS using a web browser and log in with root user credentials:



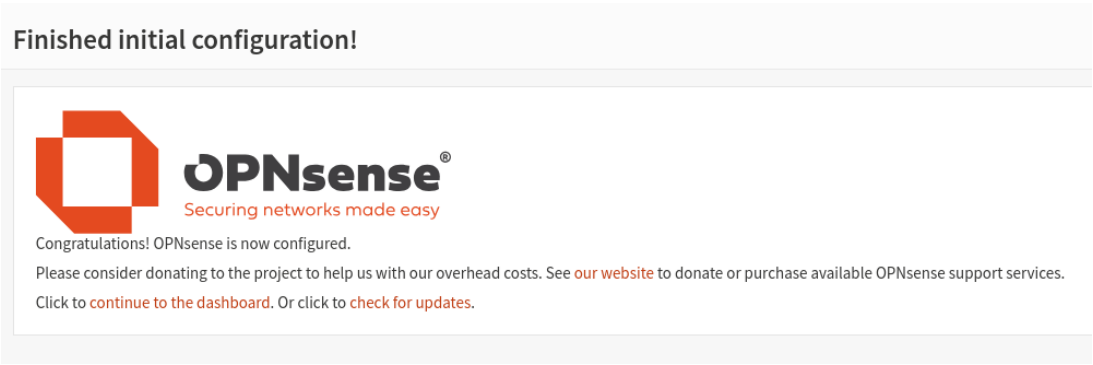
42. Click on “Next” in the configuration wizard:



43. Insert a hostname and domain and press “Next”:



44. Click on “Next” for the following sections until the configuration has finished:

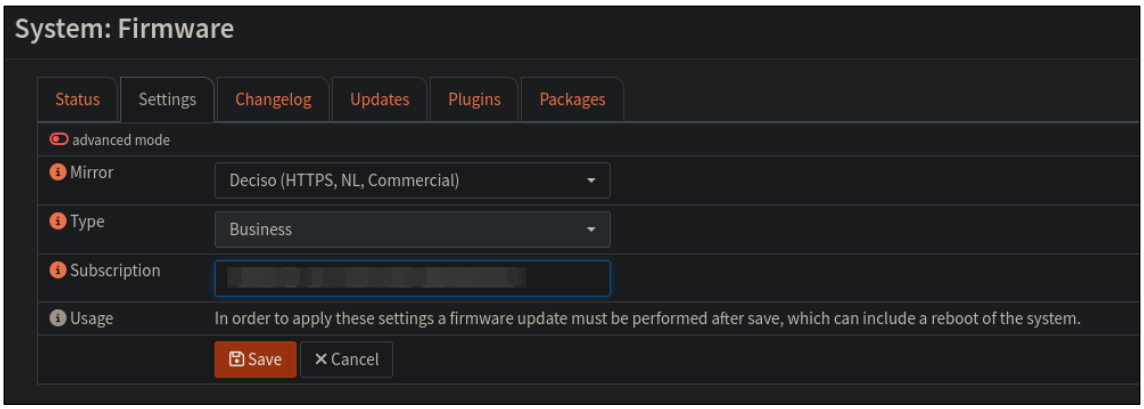


The following steps were performed in TOE OPNsense web console to complete the configuration:

6.2.2 SETTING A SUBSCRIPTION KEY

The following steps were followed to configure a subscription key:

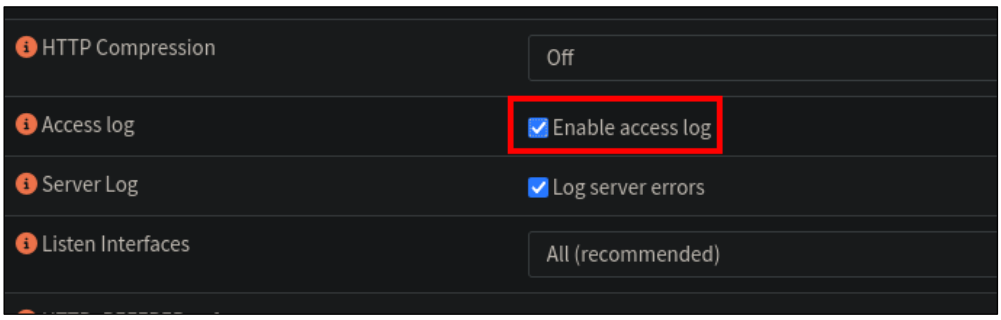
1. Go to "System > Firmware > Settings".
2. Indicate the subscription key in the Subscription text box and click "Save":



6.2.3 ENABLING ACCESS LOGS

To enable access logs, the following steps are required:

1. In the left panel go to "System > Settings > Administration" and select "Enable access log". Scroll down and click on "Save":

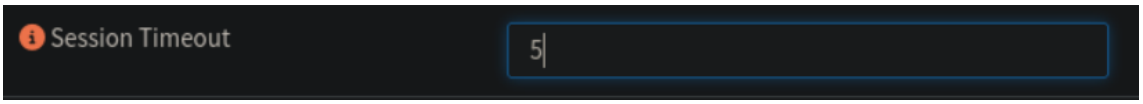


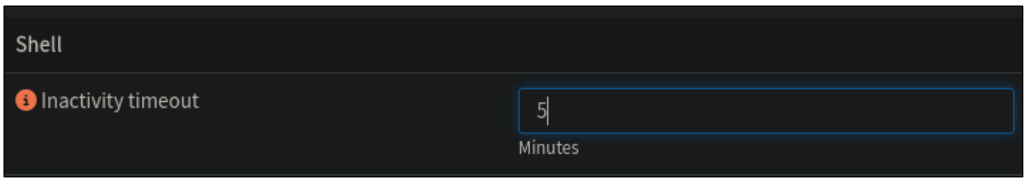
6.2.4 CONFIGURING SHELL TYPE AND INACTIVITY TIMEOUT

For the inactive session timeout to work, it is required to change the login shell assigned to the user. The steps below were performed:

1. Go to "System > Access > Users".
2. For each user, click on the "pen" icon next to its name. Change the Login shell assigned from /usr/local/sbin/opnsense-shell to "/bin/csh". Then click on "Save" to apply the changes:

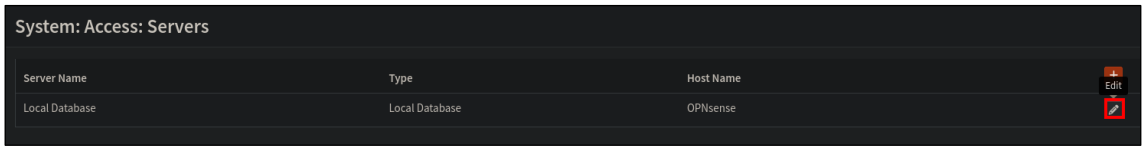
3. Go to "System > Settings > Administration".
4. Set the "Session Timeout" to 5 minutes and "Inactivity timeout" to 5 minutes to set the inactivity timeout for the GUI and CLI interfaces Then click on "Save" to apply the changes:



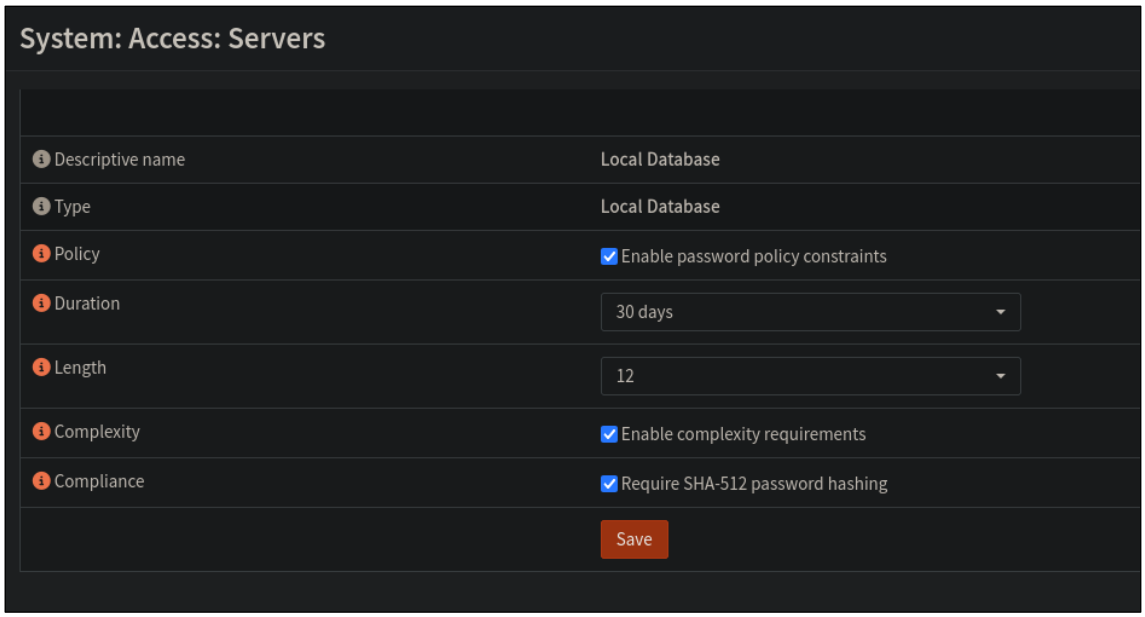


6.2.5 DEFINING A PASSWORD POLICY

1. Go to "System > Access > Servers".
2. Click on "Edit" button next to the "Local Database" server.



3. Enable "Password policy constraints". Then, add the following constraints:
   a. 30 days of duration for passwords.
   b. 12 characters as the minimum length.
   c. Enable complexity requirements.
   d. Enable compliance settings.



4. Click on "Save" to save the changes. **Note: after rebooting the TOE OPNsense, a new password using the specified policy must be set up.**

6.2.6 ADDING A READ-ONLY AUDIT ROLE

To prevent any user (other than the root user) with read access to audit records from deleting the logs, the following steps were followed:

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

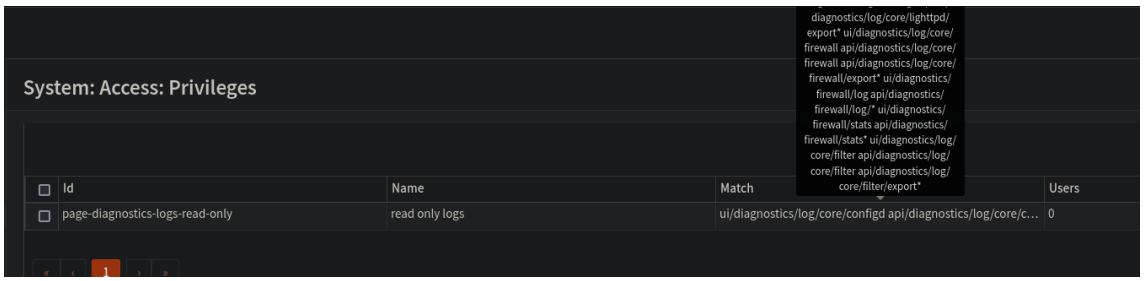
```
mkdir -p /usr/local/opnsense/mvc/app/models/security/security/ACL
```

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

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

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

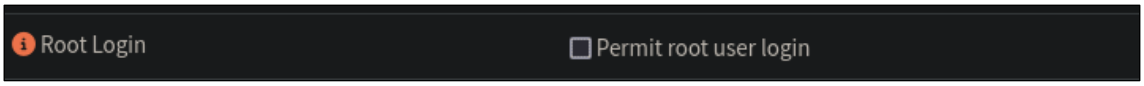
4. Reboot the TOE OPNsense.
5. Navigate to the TOE OPNsense web GUI and log in using root user credentials.
6. Navigate to "System > Access > Privileges".
7. Search for the "page-diagnostics-logs-read-only" user and verify that it appears:



6.2.7 DISABLING ROOT USER FOR SSH

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

1. Go to "System > Settings > Administration"
2. In the "Secure Shell" option, uncheck the option "Permit root login".

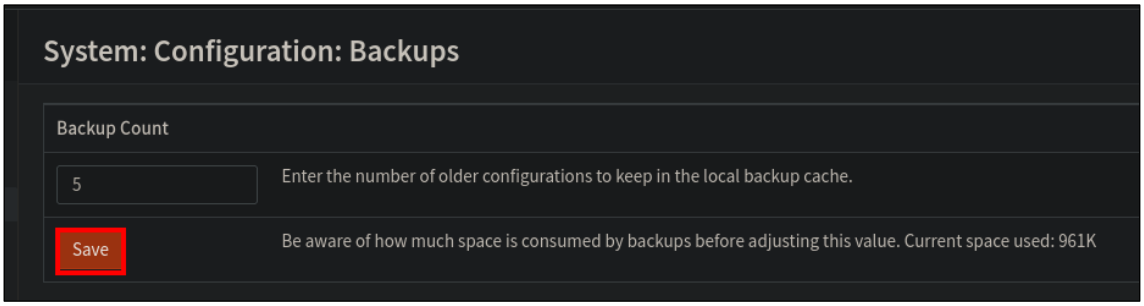


3. Click on "Save" to save the changes.

6.2.8 CONFIGURING SYSTEM BACKUPS ROTATION

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

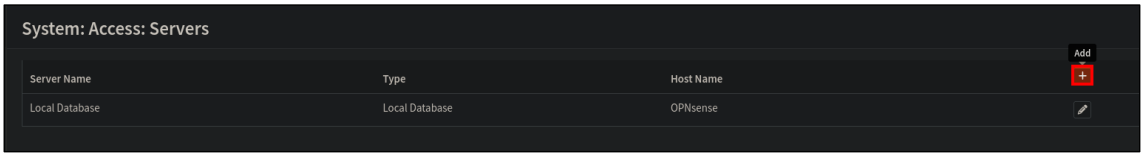
1. Go to "System > Configuration > Backups".
2. Configure the "Backup Count" parameter to 5. Then click on "Save" to apply the changes:



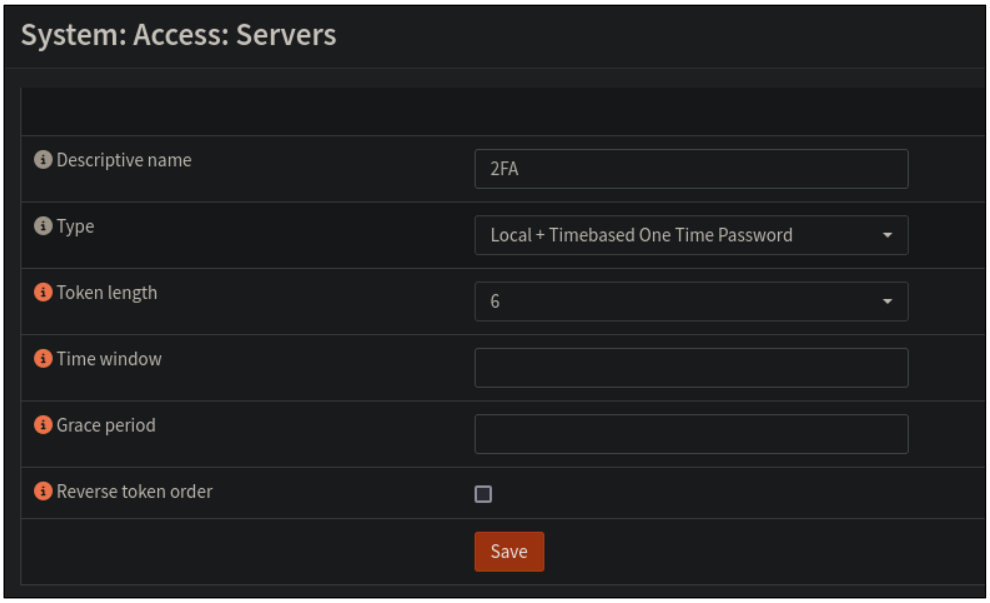
6.2.9 CONFIGURING TWO-FACTOR AUTHENTICATION

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

1. Go to "System > Access > Servers".
2. Click "Add server" in the top right corner:

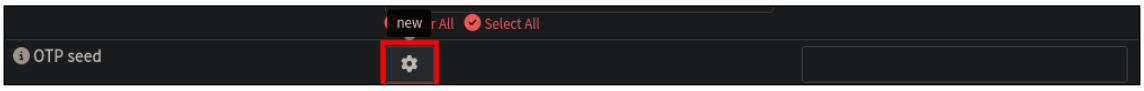


3. Create a new server with the following parameters:

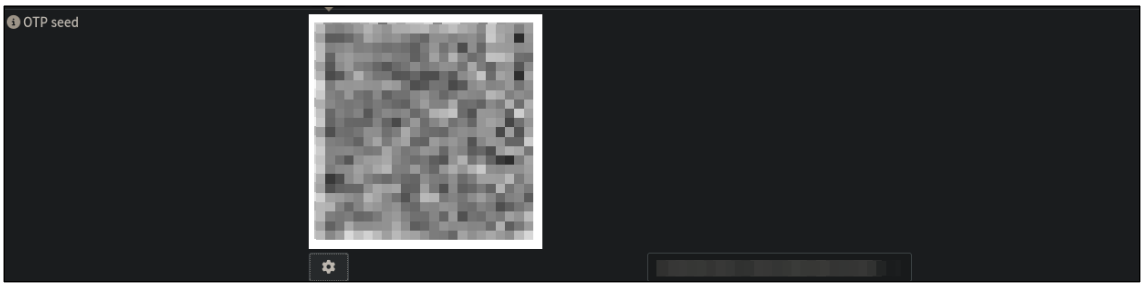


4. Install a Google Authenticator compatible app on your device.
5. Go to "System > Access > Users".
6. Edit the root user.
7. Click on "Show" in the OTP seed parameter:

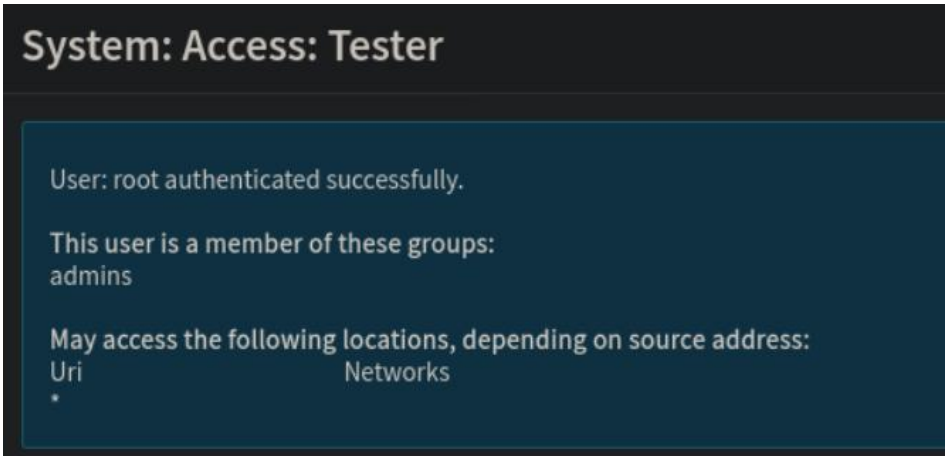
8. Click on "New" in the OTP seed parameter:



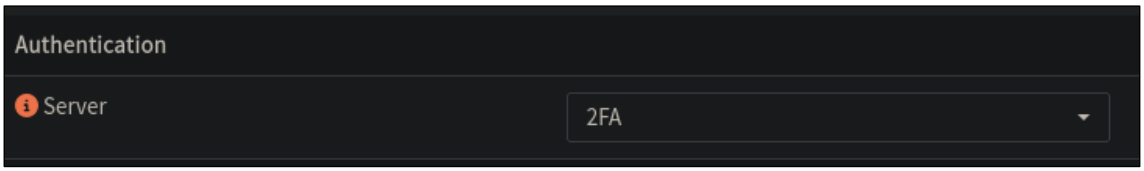
9. Register the token generated or QR code in the Goggle Authenticator compatible app:



10. Click on "Save" to save the changes.
11. Go to "System > Access > Tester".
12. Select the previously created 2FA server and verify that the 2FA authentication is properly configured concatenating the authenticator code and the user password "<CODE><PASSWORD>":



13. Go to "System > Settings > Administration".
14. Change the Authentication server by selecting the "2FA" server that was just created in the dropdown menu:



15. Click on "Save" to apply the changes.

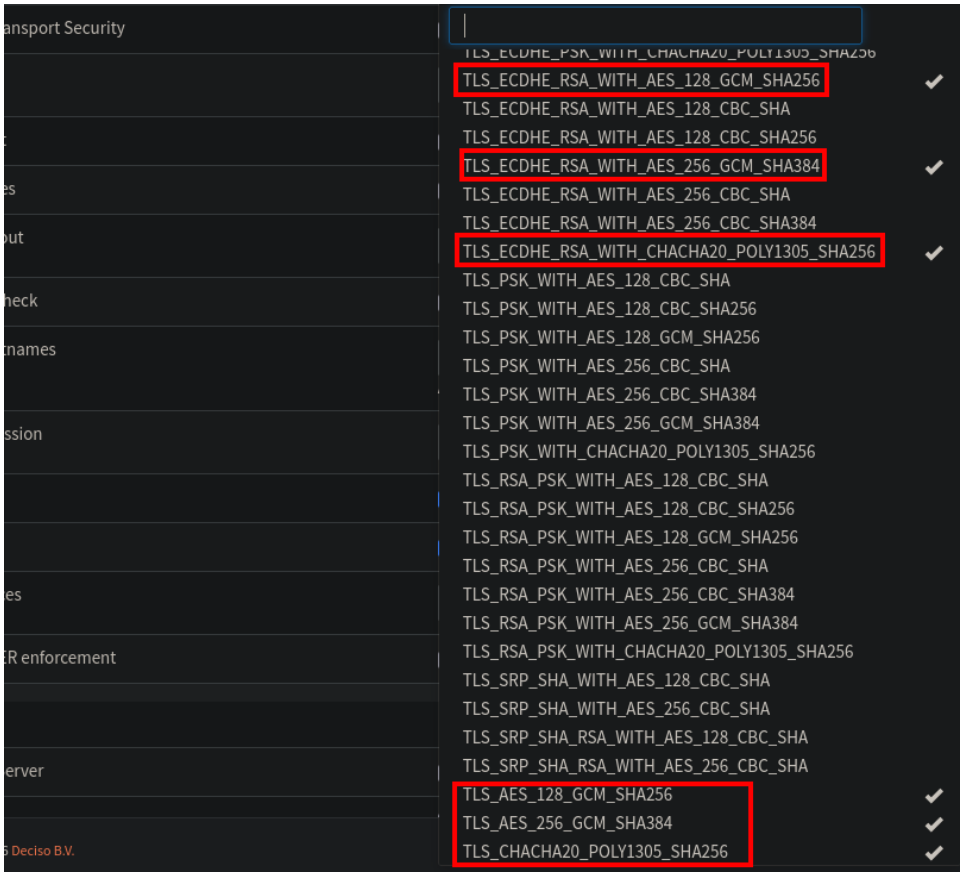
Note: The 2FA is configured for each user. In this case, it was configured for the root user. The steps shall be repeated for each desired user to use 2FA.

6.2.10 CONFIGURING WEB INTERFACE TLS CIPHER SUITES

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

1. Navigate to "System > Settings > Administration".
2. In the Web GUI section, use the dropdown menu for "SSL Ciphers" to select the following 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



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

6.2.11 CONFIGURING SSH CRYPTOGRAPHIC PARAMETERS

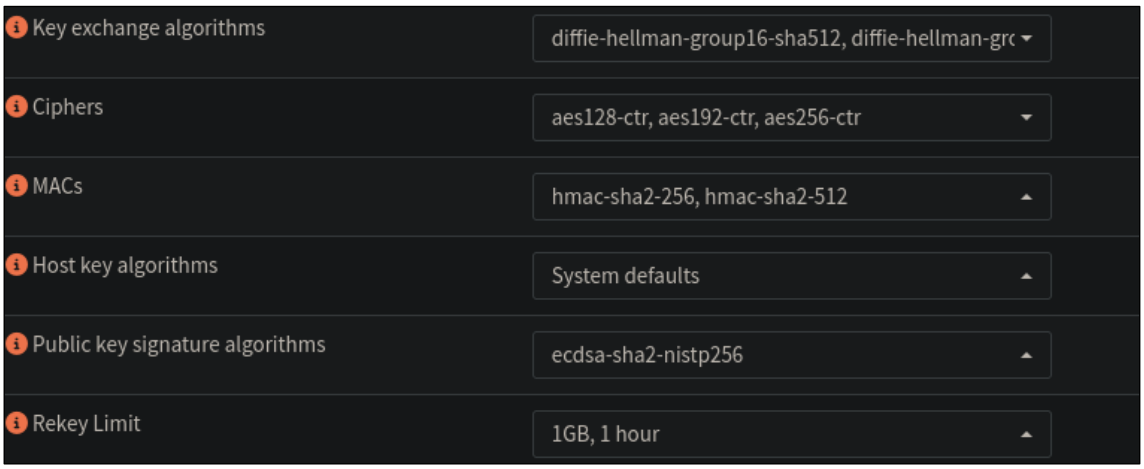
It is required to configure cryptographic parameters for SSH through the web interface. This configuration affects the SSH connections that users establish with the TOE. The steps below were followed:

1. Navigate to "System > Settings > Administration".
2. In the Secure shell section, click on "Show cryptographic overrides":

3. Use the dropdown menu for "Key exchange algorithms", "Ciphers", "MACs", "Public key signature algorithms" and "Rekey Limit" to select valid cryptographic parameters:
    a. Key exchange algorithms:
        i. diffie-hellman-group16-sha512
        ii. diffie-hellman-group18-sha512
        iii. ecdh-sha2-nistp256

iv. ecdh-sha2-nistp384
v. ecdh-sha2-nistp521

b. Ciphers:
   i. aes128-ctr
   ii. aes192-ctr
   iii. aes256-ctr
c. MACs:
   i. hmac-sha2-256
   ii. hmac-sha2-512
d. Public key signature algorithms:
   i. ecdsa-sha2-nistp256
e. Rekey Limit:
   i. 1GB, 1 hour



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

6.2.12 INSTALLING CERTIFICATES FROM TRUSTWORTHY CA

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

6.2.13 DISABLING NTP SERVICE

To disable the NTP service the steps below were followed:

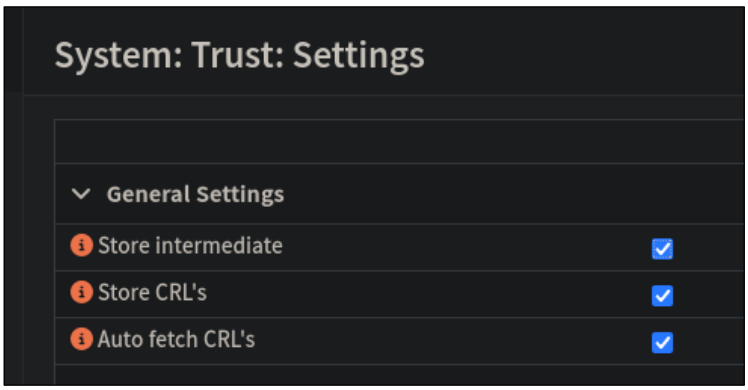
1. Log in through the TOE web interface with root credentials.
2. Go to "Services > Network Time > General".
3. Remove all the Time servers specified:

4. Click on "Save" to apply the changes.

6.2.14 MODIFYING TRUST SETTINGS

The steps followed were defined below:

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

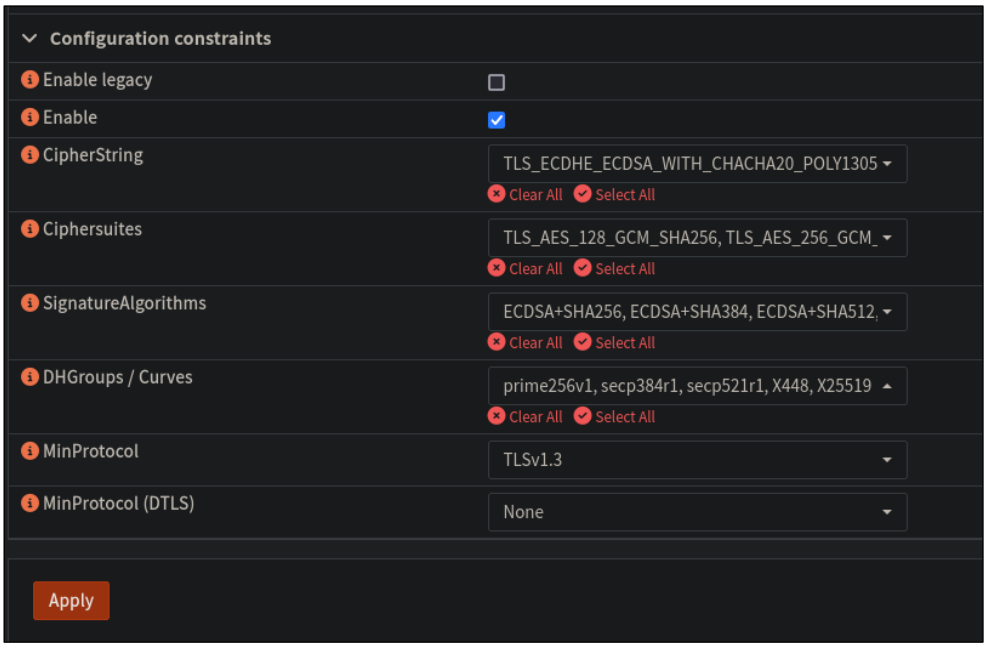


4. Under Configuration constraints, select Enable checkbox, which is disabled by default, uncheck the "Enable Legacy" option and indicate the following configuration:

   a. CipherString:
   TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
   TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,
   TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,
   TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
   b. Ciphersuites:
   TLS_AES_128_GCM_SHA256, TLS_AES_256_CGM_SHA384,
   TLS_CHACHA20_POLY1305_SHA256
   c. SignatureAlgorithms:

ECDSA+SHA256, ECDSA+SHA384, ECDSA+SHA512, rsa_pss_pss_sha256, rsa_pss_pss_sha384, rsa_pss_pss_sha512, rsa_pss_rsae_sha256, rsa_pss_rsae_sha384, rsa_pss_rsae_sha512.

d. DHGroups / Curves: prime256v1, secp384r1, secp521r1, x448, x25519
e. MinProtocol: TLSv1.3

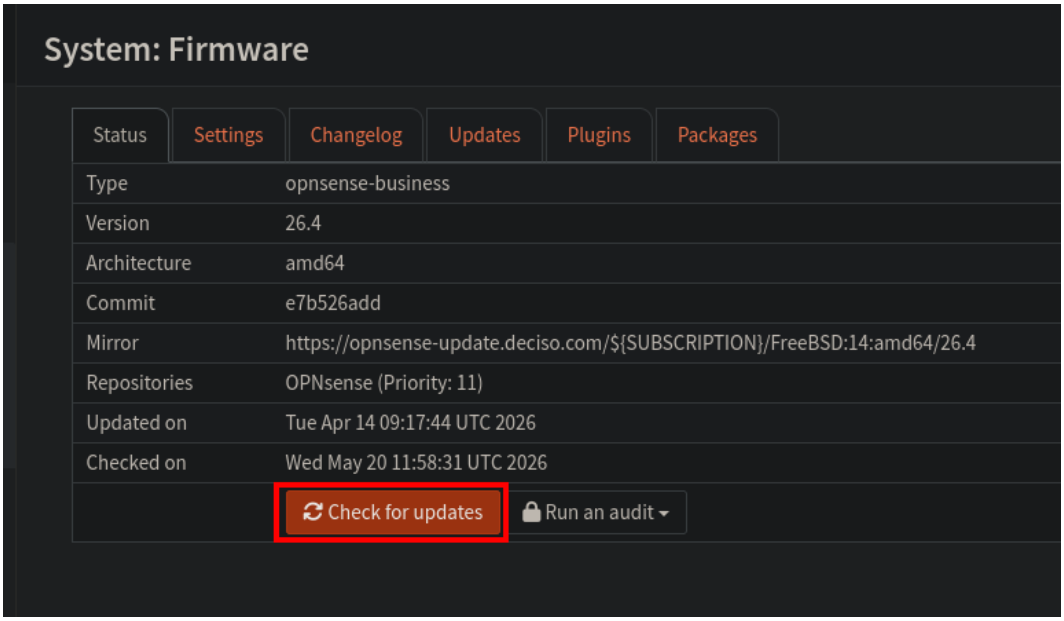


5. Click on "Apply" to apply the changes.

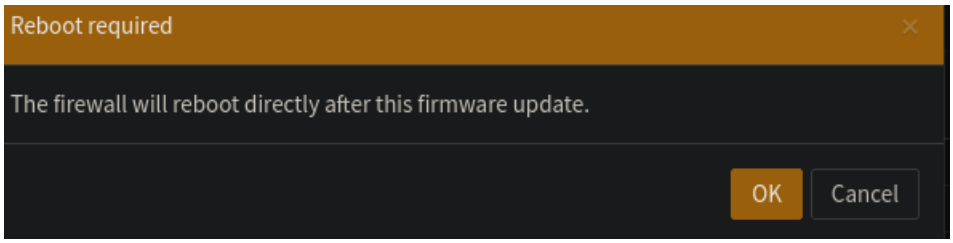
6.2.15 UPDATING OS-OPNBECORE PLUGIN TO VERSION 1.8_2 AND INSTALLING PATCH

The steps below show how to update THE os-OPNBEcore plugin and how to install the https://github.com/opnsense/core/commit/0bb5afb3aed39 patch:

1. Log in through the TOE web interface.
2. Go to “System → Firmware → Status”.
3. Click on “Check for updates”:



4. Click on “Update” and then click on “OK”:



5. Log in to the TOE OPNsense CLI as root.

6. Run the following command to install the patch:

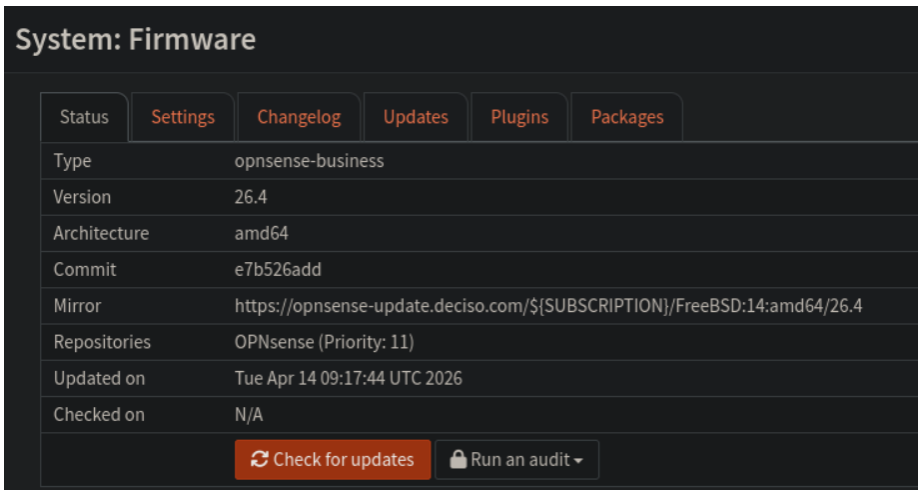
```
opnsense-patch
https://github.com/opnsense/core/commit/0bb5afb3aed39
```

```
From 0bb5afb3aed398eb11b59cdd6f006ec6069d98e9 Mon Sep 17 00:00:00 2001
From: Ad Schellevis <ad@opnsense.org>
Date: Tue, 19 May 2026 11:39:45 +0200
Subject: [PATCH] Services: Monit: Status - sanitize monit output before
 offering it.

---
 .../app/controllers/OPNsense/Monit/Api/StatusController.php    | 3 ++-
 1 file changed, 2 insertions(+), 1 deletion(-)

diff --git a/src/opnsense/mvc/app/controllers/OPNsense/Monit/Api/StatusControll
er.php b/src/opnsense/mvc/app/controllers/OPNsense/Monit/Api/StatusController.ph
p
index 12399827bc5..95040e69e12 100644
--- a/src/opnsense/mvc/app/controllers/OPNsense/Monit/Api/StatusController.php
+++ b/src/opnsense/mvc/app/controllers/OPNsense/Monit/Api/StatusController.php
--------------------------
Patching file opnsense/mvc/app/controllers/OPNsense/Monit/Api/StatusController.p
hp using Plan A...
Hunk #1 succeeded at 72.
Hunk #2 succeeded at 84.
done
All patches have been applied successfully.  Have a nice day.
```

6.3 VERIFICATION OF THE INSTALLED TOE VERSION

To verify the installed TOE version, the steps below were as follows:

1. Log in to the TOE OPNsense web GUI as root.
2. Go to "System > Firmware > Status".
3. Check the version number identifier:



6.4 USED INSTALLATION OPTIONS

No additional installation options were included in order to achieve the secure configuration.

6.5 RESULTS

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

ID	Comment	State
N/A	None.	N/A

7 VULNERABILITY ANALYSIS

Evaluator	AGL
Days required	1 day
Date	25/05/2026
Results of the evaluator's work	**PASS**

7.1 EVALUATION ACTIVITIES

The information presented in this section covers the results 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. Conduct a methodical vulnerability analysis by using any means within the technical competence of the evaluator, 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 TOE type, taking into account in said analysis the list of third-party libraries defined in the Security Target by the applicant.**

d) **The TOE itself, which is installed on a test platform as representative as possible of the TOE's operational environment.**

PASS The TOE vulnerability analysis is described in section 7.3 *TOE vulnerability analysis*.

TE.5.2 Document the devised vulnerability analysis methodology.

PASS The method followed to carry out the vulnerability analysis is described in section 7.2 *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 *7.4 List of potential vulnerabilities*.

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. Calculation of Attack Potential of [CCN-STIC-2002].

PASS Information concerning this task can be found in section 7.4 *List of potential vulnerabilities.*

TE.5.5. Register every non-conformity in relation to the Vulnerability Analysis.

PASS No non-conformities remain open remaining the Vulnerability Analysis phase. Information regarding this task can be found in section *7.5 Results*.

7.2 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.

Secondly, the evaluator referred to the OWASP TOP 10 2025 standard [OWASP], which delineates the most prevalent vulnerabilities. Following an analysis of the vulnerabilities outlined in OWASP which apply to the Target of Evaluation (TOE), the traceability of each vulnerability to OWASP TOP 10 has been proved in the next section, next to each vulnerability.

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.

The distribution of the time dedicated to each vulnerability has been calculated 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.

7.3 TOE VULNERABILITY ANALYSIS

The vulnerability analysis process includes reviewing all security features affected by the changes identified in [IAR-10], as well as testing the most relevant vulnerabilities listed

in the OWASP TOP 10 (2025). This process aims to identify potential weaknesses that could affect the TOE.

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

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

All the security functions are analyzed, paying special attention to threats that could damage the communications 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.

7.4 LIST OF POTENTIAL VULNERABILITIES

Code	Attack Potential
[STIC_OPNSENSE_IAD-2604-VUL-0010]	3
[STIC_OPNSENSE_IAD-2604-VUL-0020]	21
[STIC_OPNSENSE_IAD-2604-VUL-0030]	21
[STIC_OPNSENSE_IAD-2604-VUL-0040]	21
[STIC_OPNSENSE_IAD-2604-VUL-0050]	21
[STIC_OPNSENSE_IAD-2604-VUL-0060]	21
[STIC_OPNSENSE_IAD-2604-VUL-0070]	3
[STIC_OPNSENSE_IAD-2604-VUL-0080]	3
[STIC_OPNSENSE_IAD-2604-VUL-0090]	3

7.5 RESULTS

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

ID	Comment	State
N/A	None.	N/A

8 TOE PENETRATION TESTS

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

Evaluator	AGL
Days required	10 days.
Date	25/05/2026
Results of the evaluator's work	**PASS**

8.1 EVALUATION ACTIVITIES

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

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

PASS The list of penetration tests performed can be found summarized in section *8.2 List of penetration tests*.

TE.6.2. Register all non-conformities related to any successful attack.

PASS No non-conformities corresponding to the penetration tests phase remain open. The results of the penetration tests are collected on the basis of the non-conformities and comments in section *8.3 Results*.

8.2 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.

Due to the time constraints, 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 a penetration test is assigned a FAIL verdict because the TOE does not behave safely according to the security functionality and assets declared by the manufacturer in the

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 assumptions or because the time or capabilities required to exploit them exceed the time and effort restrictions of this methodology, a PASS result will be assigned alongside the corresponding rationale, resulting in a comment that will allow the manufacturer to improve the security of the product if they so wish.

Security function	Test code	Objective	Result
All security functions	[STIC_OPNSENSE_IAD-2604-PT-0010]	Verify if the TOE is vulnerable to CVE-2026-35387	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2604-PT-0020]	Verify if the TOE is vulnerable to SQL injection attacks by analyzing the source code.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2604-PT-0030]	Verify if the TOE is vulnerable to command injection attacks using PHP functions by analyzing the source code.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2604-PT-0040]	Verify if the TOE is vulnerable to command injection attacks in the diagnostics section.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2604-PT-0050]	Verify if the TOE is vulnerable to XSS attacks by performing a TCP connection in the Port Probe section and creating a Monit service.	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2604-PT-0060]	Verify if the TOE is vulnerable to path traversal attacks.	**PASS**
SF. Identification and Authentication	[STIC_OPNSENSE_IAD-2604-PT-0070]	Verify if the TOE is vulnerable to open redirect attacks	**PASS**
All security functions	[STIC_OPNSENSE_IAD-2604-PT-0080]	When inspecting how the TOE includes the response headers, it is not possible to trick the TOE to create HTTP response headers.	**PASS**

8.3 RESULTS

ID	Non-conformity	State
OR01.NC01	[STIC_OPNSENSE_IAD-2604-PT-0070]	**CLOSED**

ID	Non-conformity	State
	It was verified that it is possible to perform open redirect attacks through the [TOE-264] OPNcentral plugin login functionality. [TOE-264] does not properly validate the "page" parameter, allowing to redirect users to an external website. In the updated [TOE-264] os-OPNBEcore plugin it is included a session validation functionality, in which the "page" parameter is only processed when the session exists. In addition, an ACL is implemented to check if the user is allowed to access the destination path generated. For low privileged users, the ACL is enforced and the user is redirected to the internal lobby dashboard. However, for a highly privileged user such as "root", the destination is accepted and it is possible to perform an open redirect. This is not considered a non-conformity due to to Assumption A.Trusted Administration.	

ID	Comment	State
OR01.CO01	[STIC_OPNSENSE_IAD-2604-PT-0050] It is possible to perform a stored XSS attack by creating a custom Monit service in "Services → Monit → Settings" that relies on a file containing the XSS payload. When navigating to "Services → Monit → Status", [TOE-264] displays the Monit status and the XSS payload is rendered and executed in the browser. To perform this attack, the user requires the "WebCfg – Services: Monit System Monitoring page", and both the **Monit and HTTPD services must be enabled, which are not part of the default configuration**. The updated [TOE-264] patch (https://github.com/opnsense/core/commit/0bb5afb3aed39) uses the "strip_tags()" function which return a string with all NULL bytes, HTML and PHP tags stripped from a given string, preventing the creating of HTML tags containing XSS payloads. Therefore, it is not possible to perform a stored XSS attack by creating a custom Monit service.	**CLOSED**
OR01.CO02	[STIC_OPNSENSE_IAD-2604-PT-0070] It is possible to perform an open redirect attack through the [TOE-264] OPNcentral plugin login functionality. [TOE-264] does not properly validate the "page" parameter, allowing to redirect users to an external website. However, due to an ACL, only	**OPEN**

ID	Comment	State
	highly privileged users such as “root” are allowed to perform this attack.	

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.
[cPP-ND-30e]	Collaborative Protection Profile for Network Devices Version 3.0e
[cPP-ND-30e-SD]	Evaluation Activities for Network Device cPP Version 3.0e Supporting Document.
[IAR-10]	Impact Analysis Report version 1.0
[OR01-10]	Observation Report 01 - Version 1.0
[OR01-11]	Observation Report 01 - Version 1.1
[OWASP]	OWASP Top 10 2025 document that identifies and categorizes the most critical web application security risks according to vendors by trade, bug bounty vendors, and organizations that contribute internal testing data. (https://owasp.org/Top10/).

9.1 DEVELOPER EVIDENCE

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
CVE	Common Vulnerabilities and Exposures
DNS	Domain Name System
ENS	Esquema Nacional de Seguridad
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
ID	Identifier
LAN	Local Area Network
LINCE	National Essential Security Certification
MCF	Source Code Module
MEB	Biometric Evaluation Module
MEC	Cryptographic Evaluation Module
SQL	Structured Query Language
TIC	Information and Communications Technology
TOE	Target Of Evaluation
XSS	Cross-Site Scripting