jtsec
BEYOND IT SECURITY

STIC Evaluation Technical Report

STIC_OPNSENSE_HIGH-2404 (CUA-2023-118)
1.0
2025/01/28

CHANGELOG

Version	Date	Author	Reason	Changes
1.0	2025/01/28	DAT	Document creation.	First version.

INDEX

1 INTRODUCTION

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

1.1 EVALUATION TECHNICAL REPORT INFORMATION

ETR reference	STIC_OPNSENSE_HIGH-2404-ETR-v1.0
ETR version	1.0
Author or authors	DAT
Reviewer	ACP
Approved by	JTG
Start date of the works	2024/07/03
End date of the works	2025/01/28
CB dossier code	CUA-2023-118
Laboratory project code	STIC_OPNSENSE_HIGH-2404
Type of evaluation	Complementary STIC
Product Taxonomy	N/A
Evaluation Laboratory holding the accreditation	jtsec Beyond IT Security SLU (ESB93551422)
Laboratory address	Avenida de la Constitución 20 Oficina 208. CP 18012 Granada, España.
Address where the work is done	Avenida de la Constitución 20 Oficina 208. CP 18012 Granada, España.

1.2 TOE DEVELOPER INFORMATION

Applicant data	Deciso B.V.
Applicant's contact information	Ad Schellevis +31(0)187744020 a.a.schellevis@deciso.com Edison 43, 3241 LS Middelharnis, The Netherlands.
Developer data	Deciso B.V.
TOE name	OPNsense Business Edition
TOE version	24.10.1
Operating manuals of the product	[OPNSENSE-DOCS-D971B9D]

2 TOE DESCRIPTION

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

2.1 FUNCTIONAL DESCRIPTION OF THE TOE

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

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

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

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

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

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

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

- CLI interface:
  - Local access: Available directly on the machine where the TOE is installed, allowing administrators to perform the initial configuration, maintenance and management of the system without the need for a network connection.
  - Remote access: which allows remote TOE management via SSHv2. The use of this interface is not allowed to the root user.

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

2.2 INVENTORY OF SECURITY FUNCTIONS

For this evaluation, the defined security functions and the pool of security requirements are 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]) will be followed by the evaluator when conducting the tests, although they will not be followed strictly but rather as a guide to orientate the tests.

It is worth noting that although the CPSTIC taxonomy [CCN-STIC 140-D3] refers to these taxonomies but to versions v2.2e and v1.3 respectively, the laboratory has decided to use the most up to date versions available.

This evaluation takes as a baseline the LINCE evaluation carried out for the same TOE that is the subject of this STIC evaluation, OPNsense Business Edition. This LINCE evaluation, with CB dossier number 2024-13 and qualification dossier CUA-2023-118, has been carried out in accordance with the Security Target [LINCE-ST-08].

Given this, the evaluator has carried out an analysis of the requirements included in the protection profiles [cPP-ND-30e] and [PPMOD-FW-14e] with the purpose of determining and omitting for the present STIC evaluation those that are covered by the work carried out and requirements evaluated in the LINCE evaluation.

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

Therefore, for each protection profile:

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

These two points are included in the following sections, for each protection profile separately.

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 audit features to test 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 audit features to test 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 to test 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	**Not covered**, SFR to test in the present STIC evaluation. Related requirement AUD.5 was evaluated in LINCE evaluation but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity.
FAU_STG_EXT.1.5	**Not covered**, SFR to test in the present STIC evaluation. Related requirement AUD.5 was evaluated in LINCE evaluation but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity.
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	Dismissed for the present STIC evaluation, will be covered in future evaluation rounds.
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	Dismissed for the present STIC evaluation, will be covered in future evaluation rounds.
FCS_RBG_EXT.1.2	Dismissed for the present STIC evaluation, will be covered in future evaluation rounds.
FIA_UIA_EXT.1.1	**Not covered**, SFR to test in the present STIC evaluation.
FIA_UIA_EXT.1.2	**Not covered**, SFR to test in the present STIC evaluation. Functionality was evaluated in LINCE evaluation (IAU.1 requirement) but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity.
FIA_UIA_EXT.1.3	**Not covered**, SFR to test in the present STIC evaluation. Functionality was evaluated in LINCE evaluation (IAU.1 requirement) but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity.
FIA_UIA_EXT.1.4	**Not covered**, SFR to test in the present STIC evaluation. Functionality was evaluated in LINCE evaluation (IAU.1 requirement) but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity.
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	**Not covered**, SFR to test in the present STIC evaluation.
FPT_STM_EXT.1.2	**Not covered**, SFR to test in the present STIC evaluation.
FPT_TST_EXT.1.1	**Not covered**, SFR to test in the present STIC evaluation.
FPT_TST_EXT.1.2	**Not covered**, SFR to test in the present STIC evaluation.
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	**Not covered**, SFR to test in the present STIC evaluation.
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	**Not covered**, SFR to test in the present STIC evaluation. Curves are specified in COM.4 but retesting is considered just to determine if they remain the same and are suitable for HIGH category, this decision comes from detecting deviations after superficial testing.
FCS_TLSS_EXT.1.4	**Not covered**, SFR to test in the present STIC evaluation.
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	**Not covered**, SFR to test in the present STIC evaluation.
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	**Not covered**, SFR to test in the present STIC evaluation.
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	**Not covered**, SFR to test in the present STIC evaluation. 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	**Not covered**, SFR to test in the present STIC evaluation. 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	**Not covered**, SFR to test in the present STIC evaluation.
FCS_TLSC_EXT.1.3	**Not covered**, SFR to test in the present STIC evaluation.
FCS_TLSC_EXT.1.4	**Not covered**, SFR to test in the present STIC evaluation. Curves are specified in COM.1 but retesting is considered just to determine if they remain the same and are suitable for HIGH category, this decision comes from detecting deviations after superficial testing.
FCS_TLSC_EXT.1.5	**Not covered**, SFR to test in the present STIC evaluation.
FCS_TLSC_EXT.1.6	Communication channel with the syslog server 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. The communication channel with the update repository is **not covered** by that rationale.
FCS_TLSC_EXT.1.7	**Not covered**, SFR to test in the present STIC evaluation.
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	**Not covered**, SFR to test in the present STIC evaluation.
FIA_X509_EXT.1.1/Rev	**Not covered**, SFR to test in the present STIC evaluation.
FIA_X509_EXT.1.2/Rev	**Not covered**, SFR to test in the present STIC evaluation.
FIA_X509_EXT.2.1	**Not covered**, SFR to test in the present STIC evaluation.
FIA_X509_EXT.2.2	**Not covered**, SFR to test in the present STIC evaluation.
FIA_X509_EXT.3.1	**Not covered**, SFR to test in the present STIC evaluation.
FIA_X509_EXT.3.2	**Not covered**, SFR to test in the present STIC evaluation.
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	**Not covered**, SFR to test in the present STIC evaluation.
FIA_PMG_EXT.1.1	Covered by IAU.3.
FPT_APW_EXT.1.1	**Not covered**, SFR to test in the present STIC evaluation. Functionality was evaluated in LINCE evaluation (PSC.1 requirement) but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity.
FPT_APW_EXT.1.2	**Not covered**, SFR to test in the present STIC evaluation. Functionality was evaluated in LINCE evaluation (PSC.1 requirement) but changes (as indicated in [IAR-10]) introduced in the product affect such functionality; therefore, retesting is a necessity.
FMT_MOF.1.1/Functions	**Not covered**, SFR to test in the present STIC evaluation.
FMT_MTD.1.1/CryptoKeys	**Not covered**, SFR to test in the present STIC evaluation.
FTA_SSL_EXT.1.1	Covered by IAU.4.

Therefore, given the previous analysis, the Security Functional Requirements to test from the PP [cPP-ND-30e] are 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	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

	be logged if individual accounts are required for Administrators). •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.	addition to the action itself a unique key name or key reference shall be logged). • [selection: no other actions]; 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	The TSF shall be able to store [selection: persistent] audit records

	locally with a minimum storage size of [assignment: number of records and/or file/buffer size(s)].	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.
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: other authentication mechanism]] and local authentication mechanisms [selection: none, password-based, [assignment: other authentication mechanism]].	The TSF shall provide the following remote authentication mechanisms [selection: Web GUI password, SSH password] and local authentication mechanisms [selection: password-based].
FIA_UIA_EXT.1.4	The TSF shall authenticate any administrative user's claimed	Same description as in PP.

	identity according to each authentication mechanism specified in FIA_UIA_EXT.1.3.	
FMT_SMF.1.1	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;	The TSF shall be capable of performing the following management functions: • 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_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.
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	The TSF shall [selection: support secure renegotiation in

	always including the "renegotiation_info" TLS extension in TLS 1.2 ServerHello messages, reject [selection: TLS 1.2, TLS 1.3] renegotiation attempts].	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].
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-	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.

	surname, id-at-title] and no other attribute types].	
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 establish the connection on a per certificate basis.].	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.
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	For the communication channel with the audit server: The TSF shall [selection:

	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), ○ 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;	• 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;]. 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. NOTE: SFR only tested for the communication channel with the update repository. Other TOE TLS client channel is considered covered.
FCS_TLSC_EXT.1.7	The TSF shall prohibit the use of the following extensions: • Early data extension • Post-handshake client authentication according to RFC 8446, Section 4.2.6.	Same description as in PP. 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].

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 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.	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-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. ○ Server certificates presented for

	○ 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.	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	The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection: HTTPS, TLS] and

	[selection: code signing for system software updates [assignment: other uses], no additional uses].	[selection: no additional uses]. NOTE: SFR tested for the communication channel of the 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.
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.
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.

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.

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 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.
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	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

	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 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	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. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6; i) [selection: no other rules].

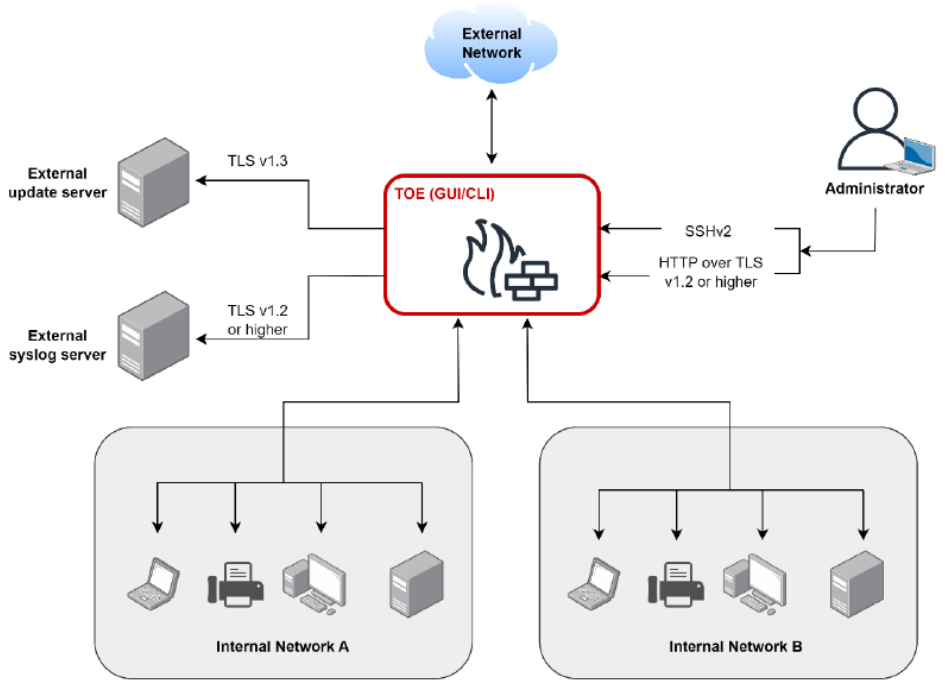
	address of the network packet is defined as an "unspecified address" or an address "reserved for future definition and use" (i.e. unicast addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6; h) The TSF shall drop and be capable of logging network packets with the IP options: 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	Same description as in PP.

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



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

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

Hardware requirements

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

- Minimum required RAM is 1GB

- Minimum recommended virtual disk size of 8 GB.

3.2 OPERATIONAL ENVIRONMENT ASSUMPTIONS

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

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

4 EXECUTIVE SUMMARY OF THE EVALUATION

This is a STIC evaluation for the TOE OPNsense Business Edition, which has been evaluated previously with a LINCE evaluation as defined in the Security Target [LINCE-ST-08] provided by the manufacturer. The goal of the present evaluation is to conduct testing according to the HIGH category taxonomy [CCN-STIC-140-D3] which references the collaborative Protection Profile for Network Devices [cPP-ND-30e] and PP-Module for Stateful Traffic Filter Firewalls [PPMOD-FW-14e].

Since the TOE has undergone a LINCE evaluation, before starting the testing effort, the laboratory has analysed the requirements included in the LINCE evaluation to determine if there are any requirements from the aforementioned Protection Profiles that are already covered and therefore do not need to be tested. This analysis is depicted in section *2.2 Inventory of security functions*. Because of the analysis, the laboratory concludes that, given [LINCE-ST-08], although some SFRs are covered, testing will still be done for most requirements.

The version previously certified through the LINCE evaluation is 23.10.2. In the case of this evaluation, the version to be evaluated in the first instance is 24.4.1_3. Given this, the laboratory has requested from the manufacturer the Impact Analysis Report [IAR-10] in which the changes introduced in the product from the LINCE certified version up to the current one are analysed. The requirements from [LINCE-ST-08] affected by any of these changes will be tested again, this analysis complements the definition of requirements mentioned in the previous paragraph.

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

The TOE was configured and prepared to conduct the functional testing effort according to the guides provided, which were analyzed too, this did not reveal any non-conformities related to the installation of the TOE and guidance documents.

The execution of the functional tests for [TOE-2441_3] revealed the following non-conformities:

- When the date/time is manually changed by a user through the CLI making use of the "date" command, [TOE-2441_3] registers the event in the Audit log with the following entry: "date set by root". The entry contains a timestamp, type of event and user associated with the user but not the old and new values for the time (OR01.NC01).
- [TOE-2441_3] stores administrative passwords in non-plaintext form and prevents its reading. The hash algorithm is identified as bcrypt which uses blowfish. This algorithm is not complied according to [CCN-STIC-807] (OR01.NC02).
- [TOE-2441_3] supports the finite field group ffdhe2048 in the TOE GUI interface, which is considered LEGACY by [CCN-STIC-807]; given this, it is deemed not

suitable for ENS HIGH category (OR01.NC03). This finite field group is also offered when establishing a connection with the remote audit server (OR01.NC06).

- [TOE-2441_3] does not seem to define a RekeyLimit for the SSH connections. After establishing the SSH connection and waiting for one hour, the rekey of the connection is not carried out by [TOE-2441_3]. Furthermore, the rekey of the connection is also not carried out by [TOE-2441_3] after having received or sent more than 1GB of data (OR01.NC04).
- [TOE-2441_3] fails to properly verify the reference identifier included in the certificate presented by the remote audit server when wildcards are included (OR01.NC05).
- [TOE-2441_3] offers signature algorithms when establishing a connection with the remote audit server that do not comply [CCN-STIC-807] ENS HIGH category (OR01.NC07).
- [TOE-2441_3], as a client, seems to support TLS renegotiation when establishing a connection with the remote audit server since it offers the suite TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff). Despite this, it has been identified that the TOE ignores Hello Request messages sent by the server and renegotiation does not occur, the TOE continues to send data instead of sending a Client Hello message as a follow up to the Hello Request message and the connection is not renegotiated (OR01.NC08).
- [TOE-2441_3] does not properly handle certificate revocation lists (CRLs) when establishing a connection with the remote audit server (OR01.NC09, OR01.NC10, OR01.NC11).
- [TOE-2441_3] offers signature algorithms when establishing a connection with the update repository that do not comply [CCN-STIC-807] ENS HIGH category (OR01.NC12).
- [TOE-2441_3] does not properly handle certificate revocation lists (CRLs) when establishing a connection with the update repository (OR01.NC13, OR01.NC14, OR01.NC15).
- [TOE-2441_3] does not seem to validate the trustworthiness of the CSR response when it is uploaded and associated with its Certificate Signing Request in the System > Trust > Certificate menu. The CSR response is pasted and uploaded but no feedback is provided regarding its validity; therefore, it is not clear that [TOE-2441_3] is validating the trustworthiness of the CA that issued that response to the CSR (OR01.NC16).
- [TOE-2441_3] does not drop network packets:
    - whose source address is defined as a broadcast address (e.g.: 192.168.2.255 in a 192.168.2.0/24 network). The network packet is identified by [TOE-2441_3] and transmitted to the destination (OR01.NC17).
    - where the source address of the network packet is defined as a multicast address (from 224.0.0.0 to 239.255.255.255). The network packet is identified by [TOE-2441_3] and transmitted to the destination (OR01.NC18).

- whose source or destination address are 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 (OR01.NC19).
- whose source or destination address are defined as being "unspecified address" (0:0:0:0:0:0:0:0) 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 (OR01.NC20).
- whose source address of the network packet is equal to the address of the network interface where the network packet was received (OR01.NC21).
- whose source or destination address of the network packet is a IPv4 link-local address (169.254.0.0/16) (OR01.NC22).
- whose source address of the network packet does not belong to the networks associated with the network interface where the network packet was received (OR01.NC23).

- [TOE-2441_3] provides the capability to limit the maximum number of states to an administratively defined number (Max states parameter available in the firewall rules), limiting the number of half-open connections that can be forwarded through the firewall. When such threshold is met, the remaining packets which are dropped and never reach their destination are not logged or counted. It is expected that [TOE-2441_3] logs or counts the packets that are dropped after the maximum number of states is reached (OR01.NC24).

After executing the functional tests, the vulnerability analysis was conducted. This phase mainly involves the review of public vulnerabilities related to the TOE and its third-party components or libraries. Some CVEs were identified as applicable but after further analysis and some testing these were deemed not exploitable, mainly because the affected code of the third-party libraries was not being used by the TOE. This analysis does not reveal public vulnerabilities (CVE) that could affect the TOE at the date this report is developed.

It is worth noting that vulnerabilities and penetration tests related to the evaluated functionality have not been considered, given that most functionality remains the same as in the previous LINCE evaluation, which was recently executed. A dedicated effort to re-analyse the functionality of the TOE and re-testing has not been undertaken in the current evaluation but it is considered for future evaluation rounds agreed for the present year as part of the continuous qualification process.

At this point, the non-conformities identified by the laboratory were registered and delivered to the manufacturer through [OR01-10].

After some time, the manufacturer provided the laboratory with [TOE-24101], which attempted to address most of the points identified throughout the evaluation.

The tests related to functionality that was added or modified in [TOE-24101], the ones related to non-conformities, were repeated by the laboratory in order to verify the fixes developed by the manufacturer. In summary, this version of the TOE solved all non-

conformities identified in relation to the requirements of the [cPP-ND-30e]. Moreover, in order to address the non-conformities related to [PPMOD-FW-14e], the manufacturer introduced some changes in [TOE-24101] and provided instructions to configure filtering rules in order to perform the required traffic filtering; these were documented as part of the configuration of the TOE.

After repeating the tests and reviewing the results carefully, the laboratory deems that there are a couple of small gaps related to the requirement FFW_RUL_EXT.1.6 from [PPMOD-FW-14e] that are not strictly met.

- The laboratory identifies that [TOE-24101] successfully drops the network packets whose destination address is unspecified (0.0.0.0 / 0:0:0:0:0:0:0:0) but does not log the drop event; therefore, the non-conformities OR01.NC19 and OR01.NC20 are considered open. This is caused given that [TOE-24101] marks this type of packets as invalid and discards them before they are even evaluated by the filtering rules.

In any case, since the product is properly dropping these packets, the non-conformity is not considered critical since the usage of these packets would not work in any scenarios since these are being discarded.

5 VERDICT OF THE EVALUATION

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

The non-conformities OR01.NC19 and OR01.NC20 identified through the functional tests are considered open since the requirement FFW_RUL_EXT.1.6 is not completely met.

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

Documents used during installation	[OPNSENSE-DOCS-D971B9D]
Evaluator	DAT
Days required	1 day.
Date	2025/01/28
Results of the evaluator's work	**PASS**

6.1 EVALUATION ACTIVITIES

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

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

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

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

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

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

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

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

PASS The evaluator has been able to install the product exclusively following the contents of the manufacturer's documentation, provided through [LINCE-ST-08] and [OPNSENSE-DOCS-D971B9D].

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

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

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

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

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

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

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

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

6.2 DETAILED CONFIGURATION OF THE OPERATIONAL ENVIRONMENT

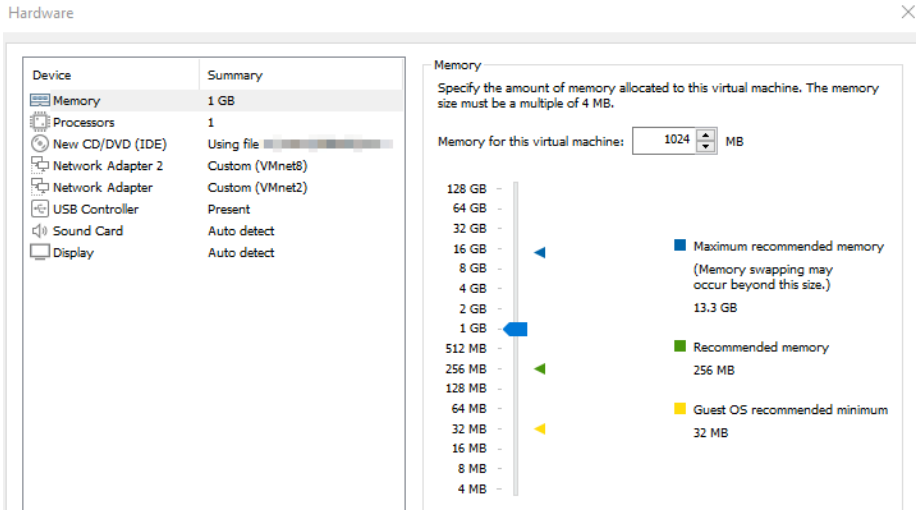
The test scenarios are described in section *12 Annex A: Test scenarios*.

6.3 DESCRIPTION OF THE INSTALLATION AND CONFIGURATION OF THE TOE

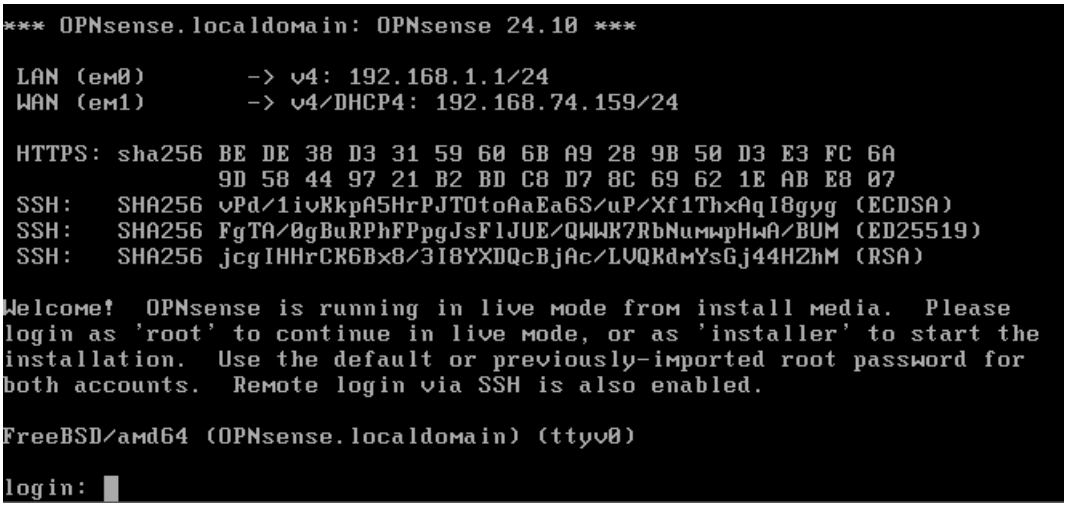
To perform the installation, the steps needed are the following:

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

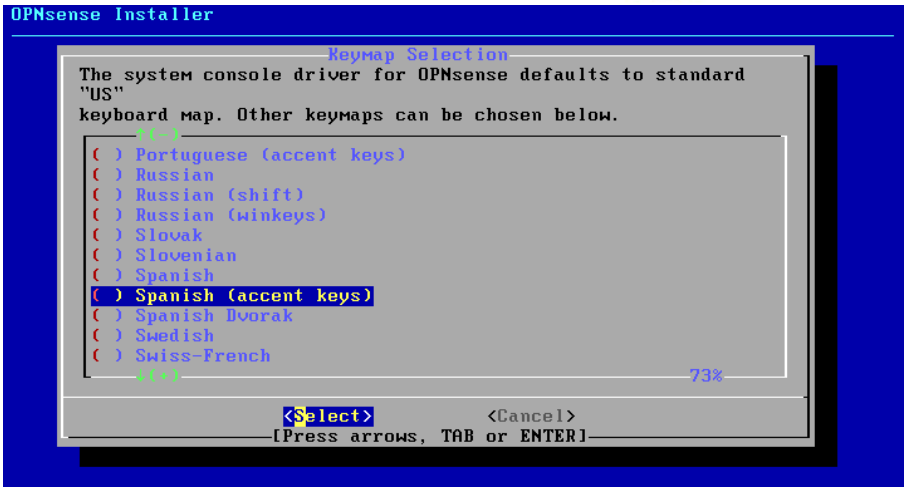
2. Select [TOE-ISO-2410] and click on “Next”.
3. Give a name to the virtual machine and click on “Next”.
4. Set 30GB as disk size.
5. Click on Customize Hardware → Memory and set 1GB of RAM memory. Add a network adapter and configure the virtual networks as shown (“Network Adapter” set to VMnet2 and “Network Adapter 2” set to VMnet8).



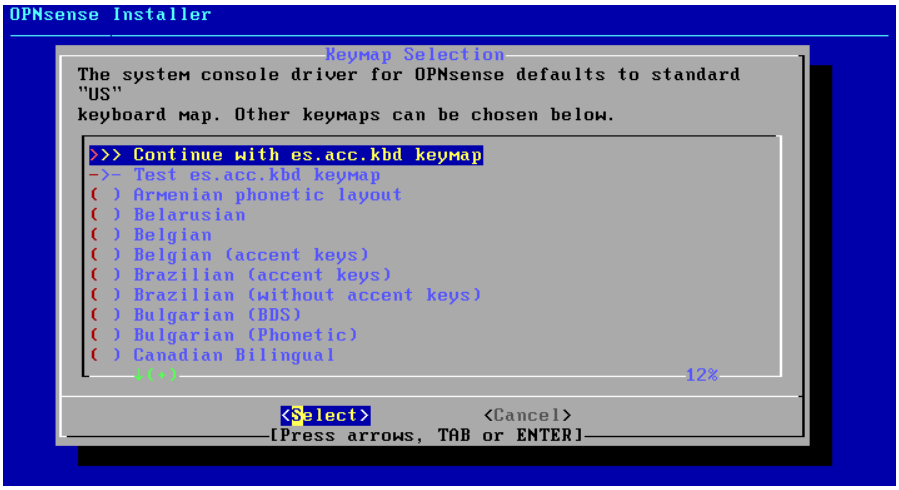
6. Press “Close”.
7. Click on “Finish”.
8. Wait for the TOE to boot up.
9. In order to install the TOE, log in with the user “installer” and authenticate with the password “opnsense”.



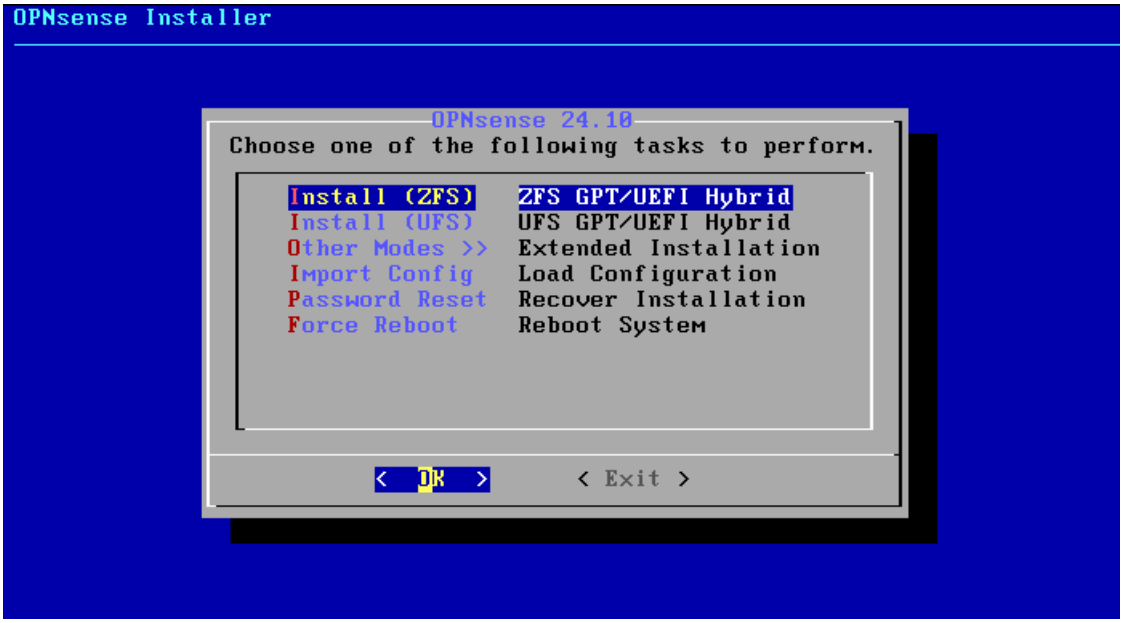
10. Select the keyboard layout.



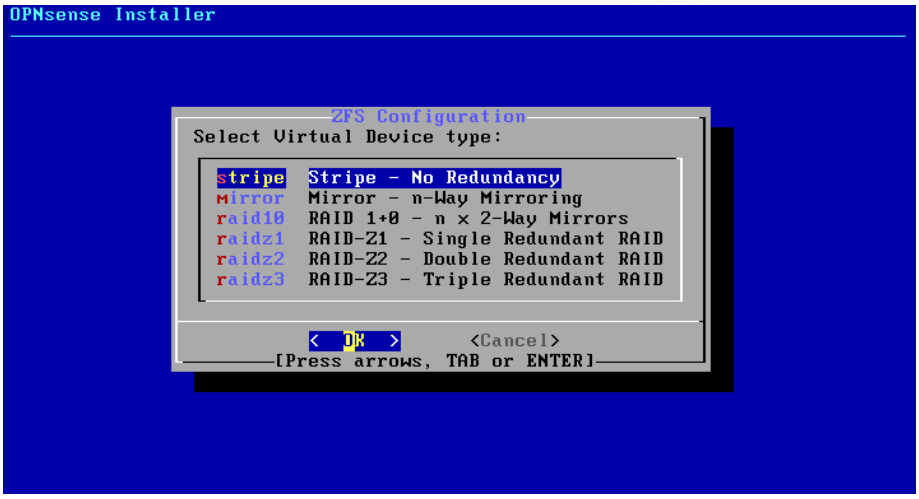
11. Indicate “Continue with…”.



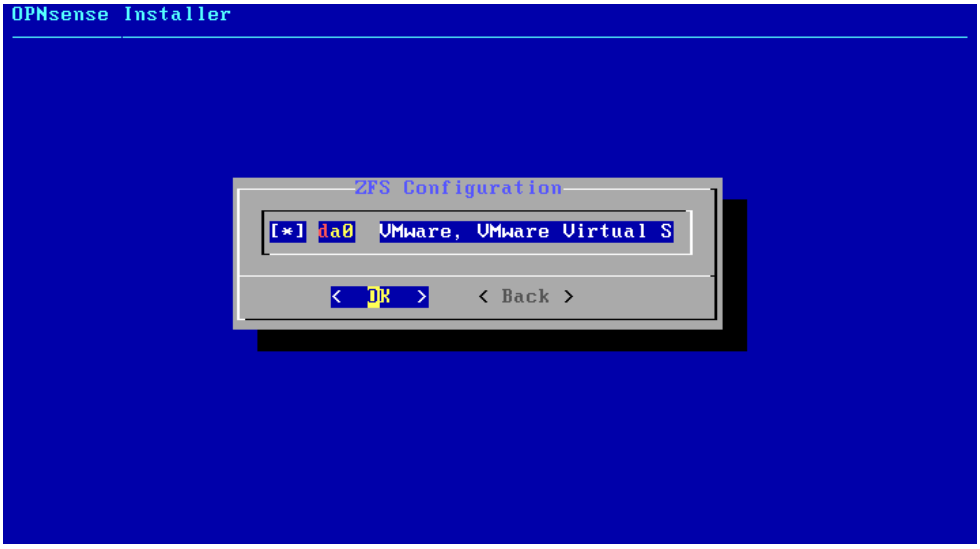
12. Select “Install (ZFS)” and press Enter.



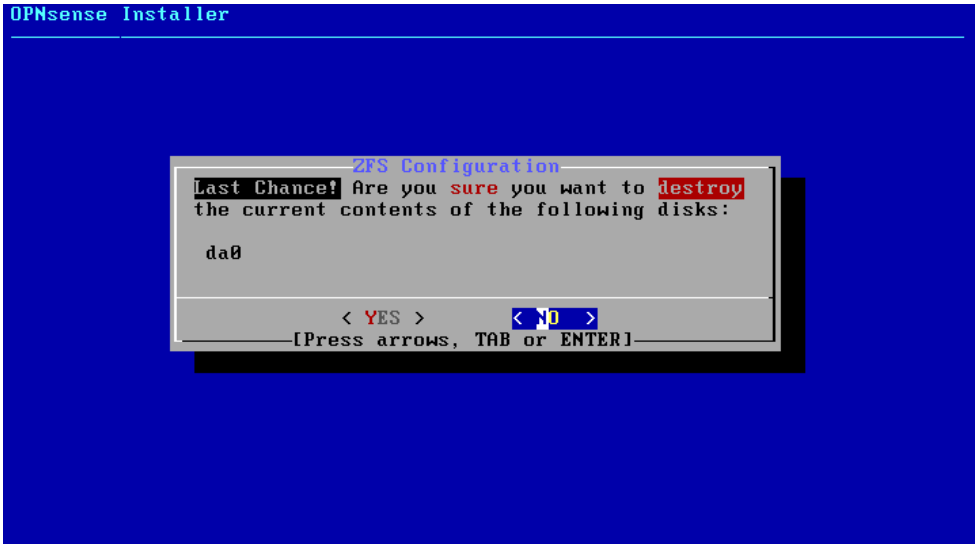
13. Select “stripe” and press Enter.



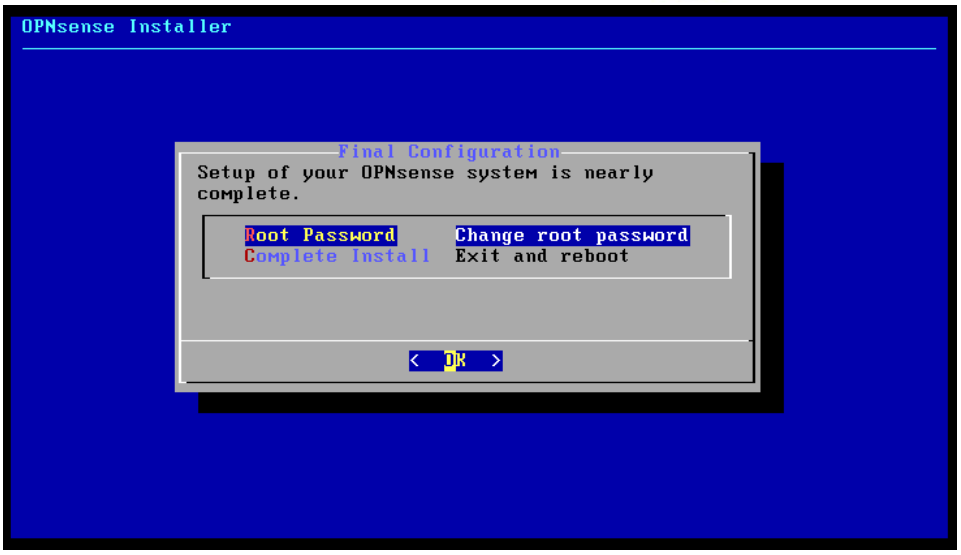
14. Select the virtual disk and press OK.



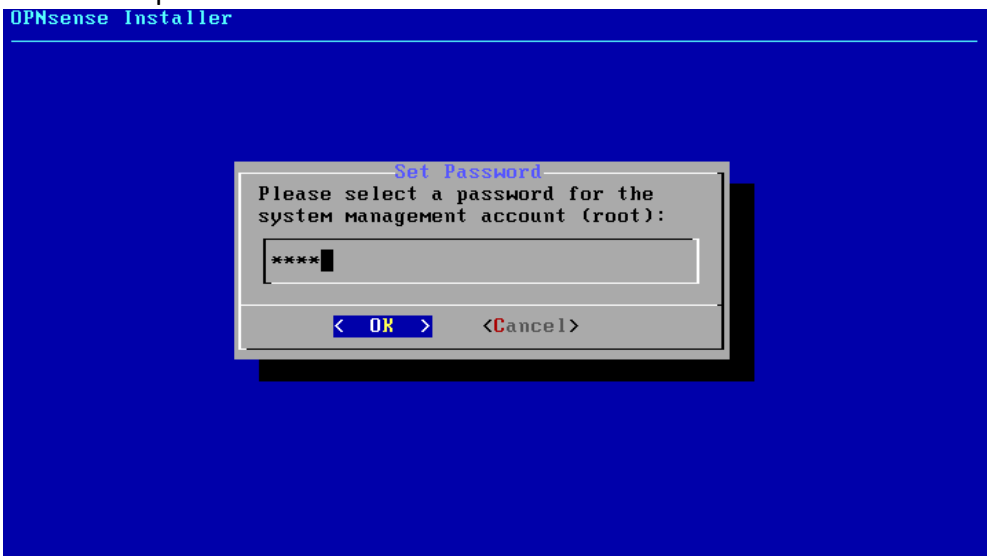
15. Select Yes and press Enter.



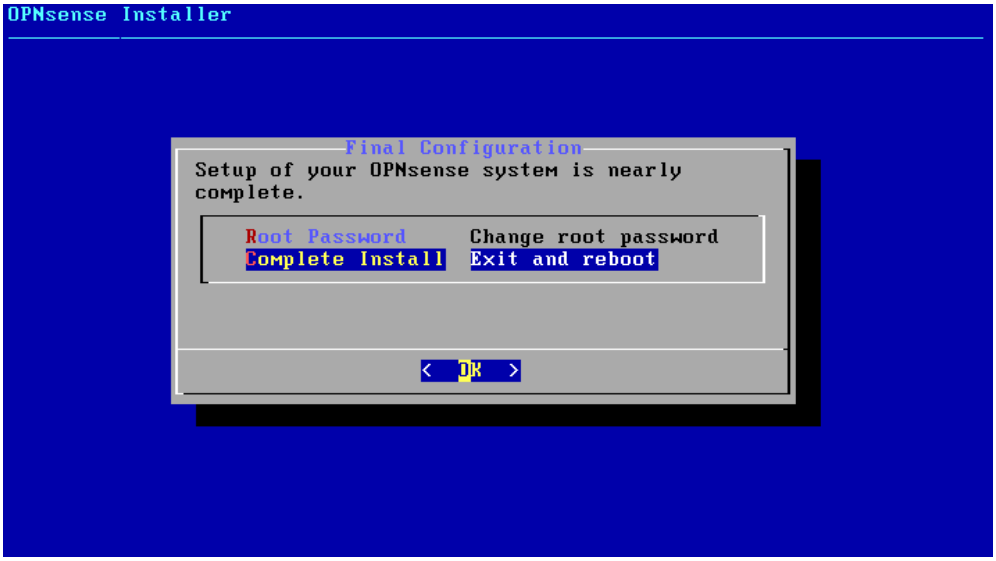
16. Select “Change root password” and press OK.



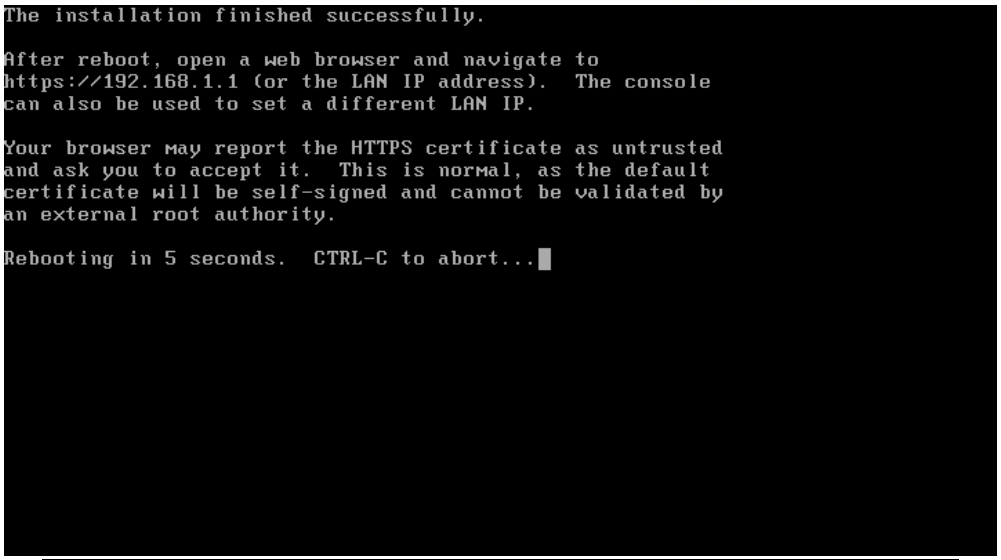
17. Define a new password for the root user.

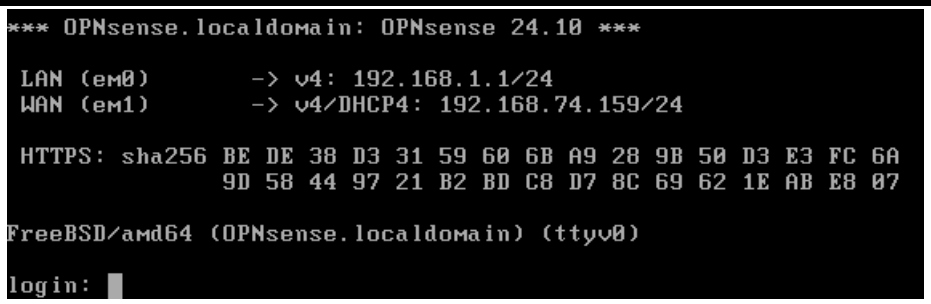


18. Select “Complete Install” and press OK.

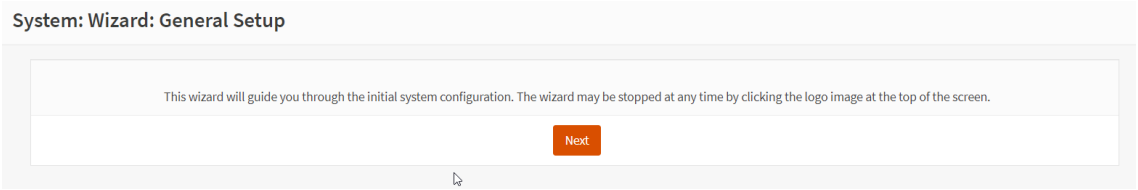


19. Wait for the TOE to reboot and navigate to the web interface.

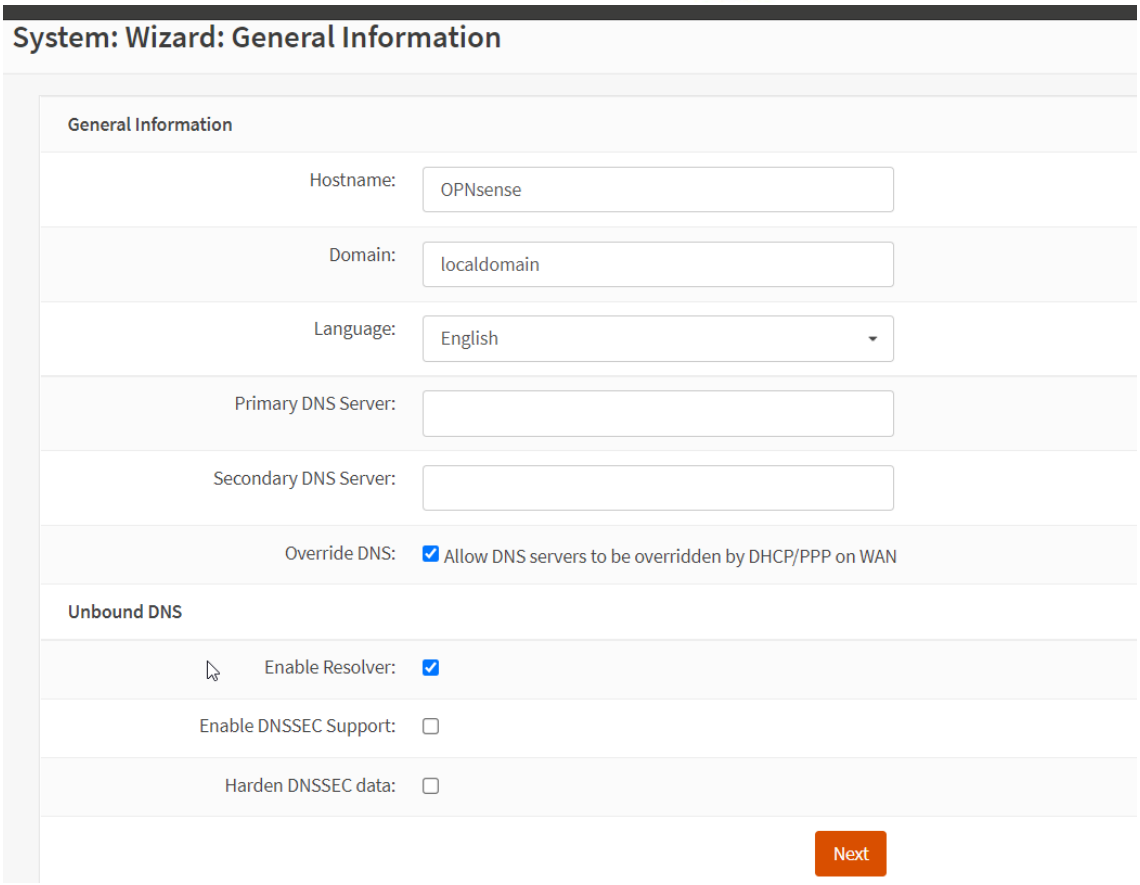




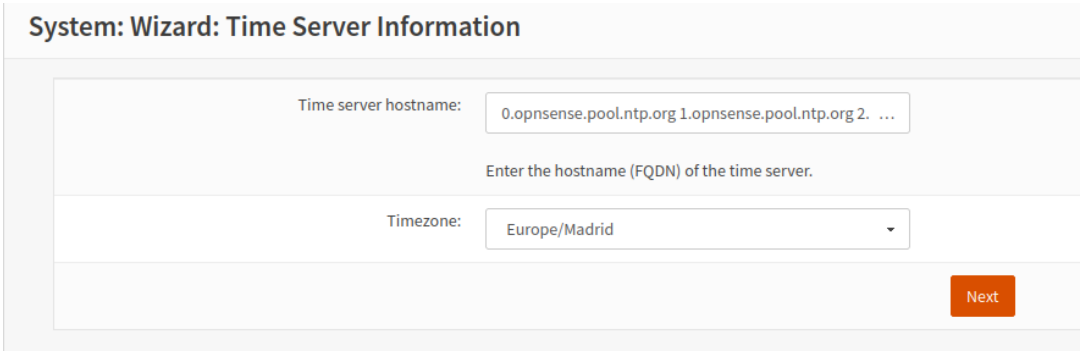
20. Access the LAN IP address through HTTPS using a web browser and log in with the root user credentials.
21. Follow the wizard setup, press Next.



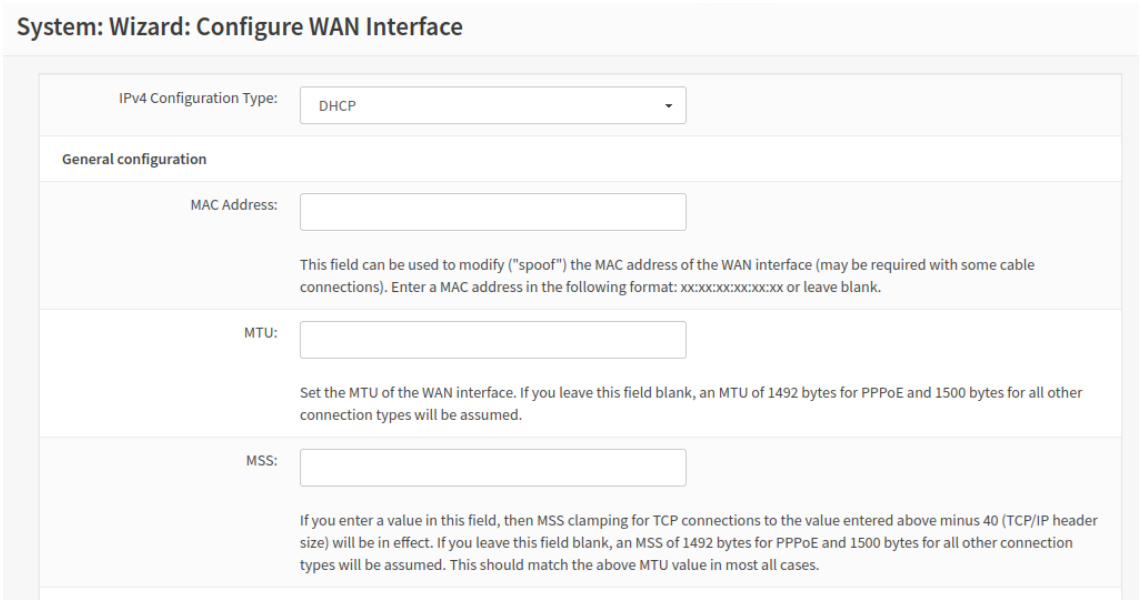
22. Give a hostname and a domain to the TOE and press Next.



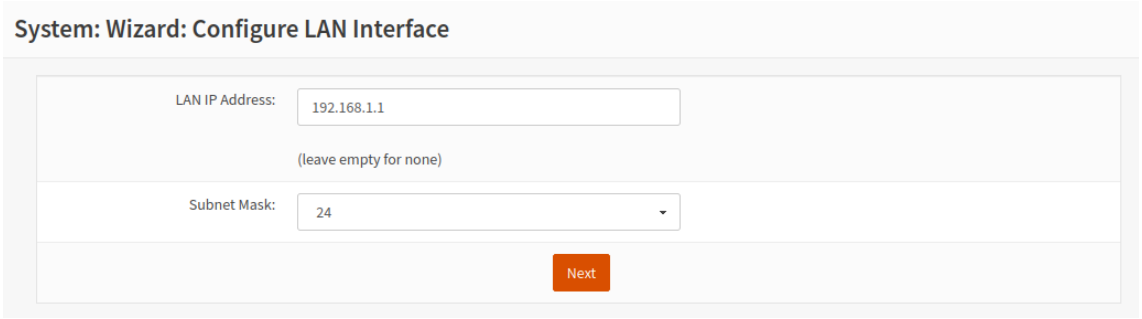
23. Set NTP servers and the time zone. In this case the NTP servers configured are the ones offered by default. Press Next.



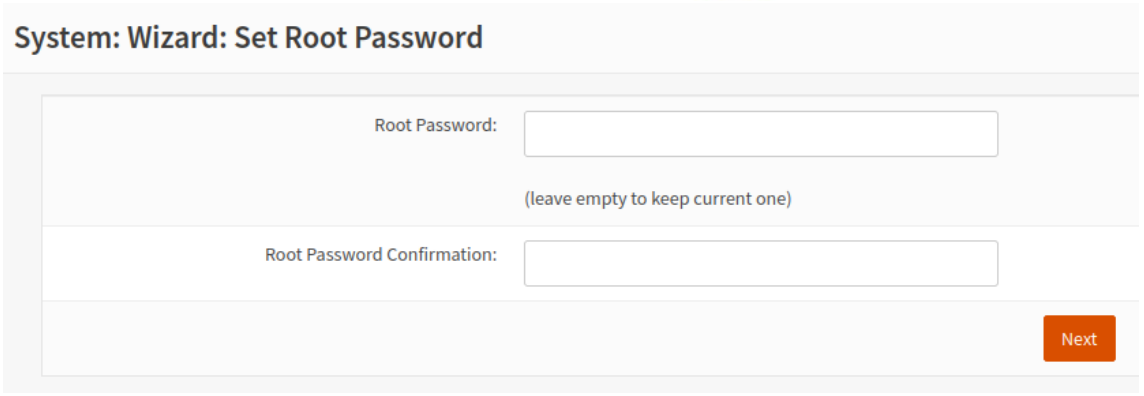
24. Leave the default configuration for the WAN interface and press Next.



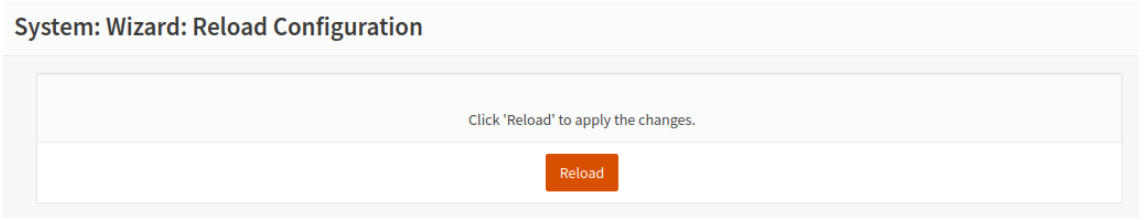
25. Leave the default configuration for the LAN interface and press Next.



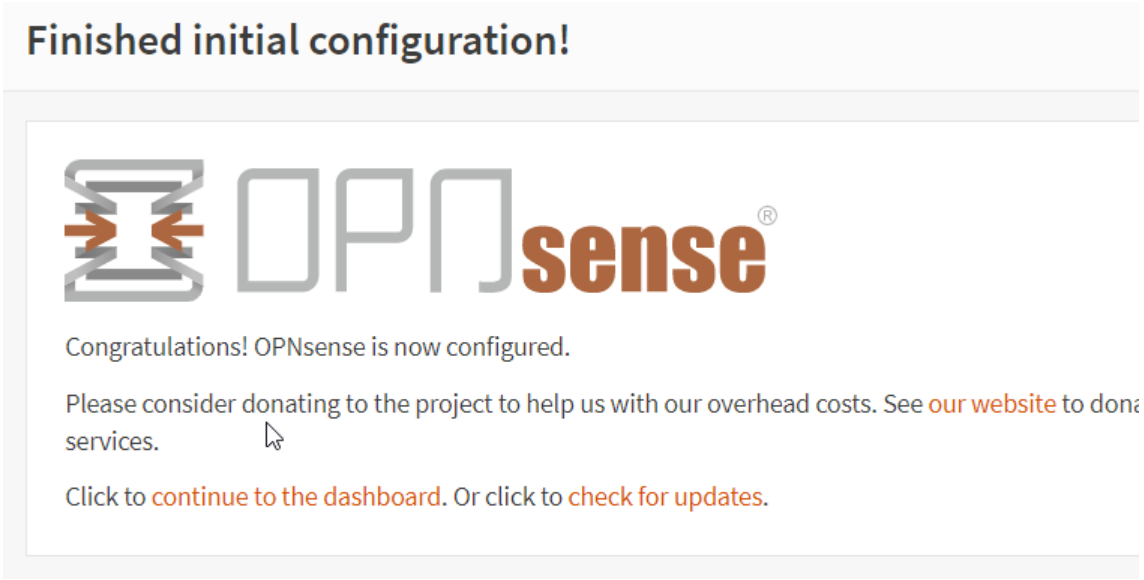
26. Set a new root password if it was not changed before.



27. Click on reload to apply the changes.



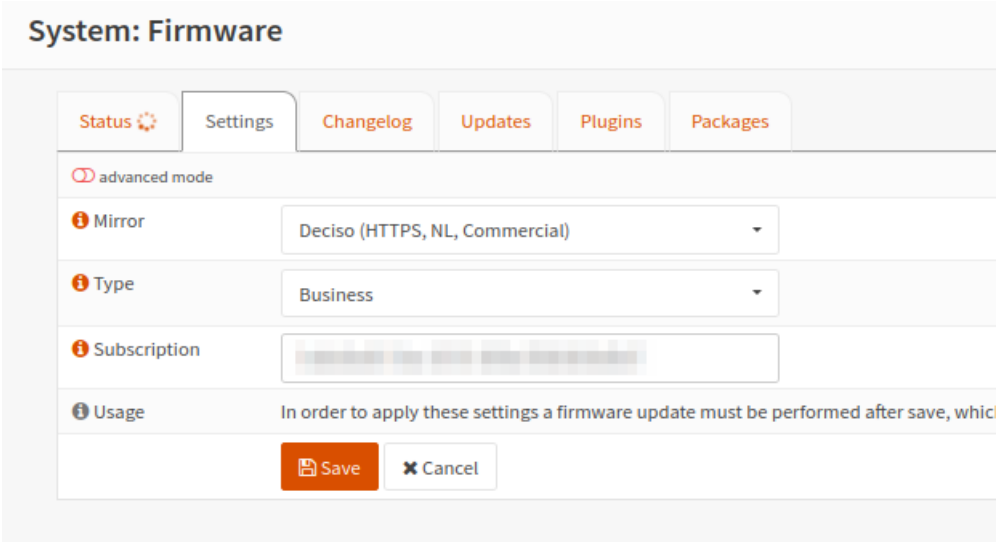
28. The TOE is now configured and ready.



6.3.1 SETTING A SUBSCRIPTION KEY

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

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



6.3.2 UPDATING TO VERSION 24.10.1

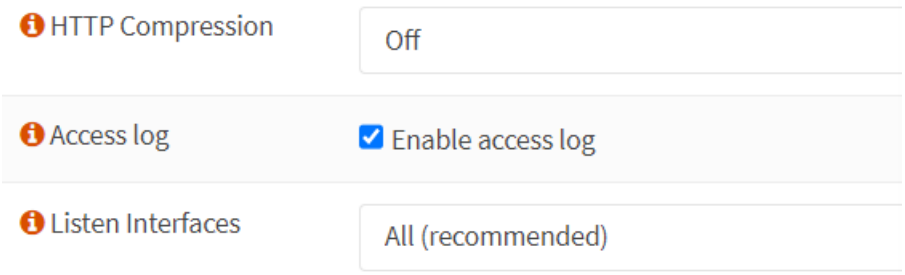
The steps below are followed:

1. Log in through the TOE web interface with the root user.
2. Go to System → Firmware → Settings.
3. Toggle “Advanced mode”.
4. Indicate “/24.10/MINT/24.10.1/latest” in the Flavour parameter and click Save.
5. Go to the Status tab and click Check for updates.
6. Click Update.
7. Wait for the update to be installed.

6.3.3 ENABLING ACCESS LOGS

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

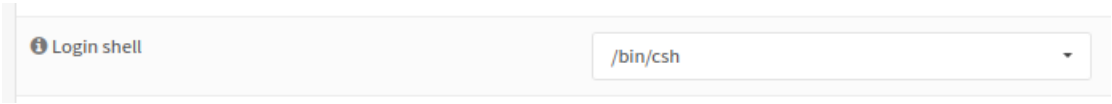
1. Enable the access log parameter in the Settings menu. In the left panel go to System → Settings → Administration and select “Enable access log”.



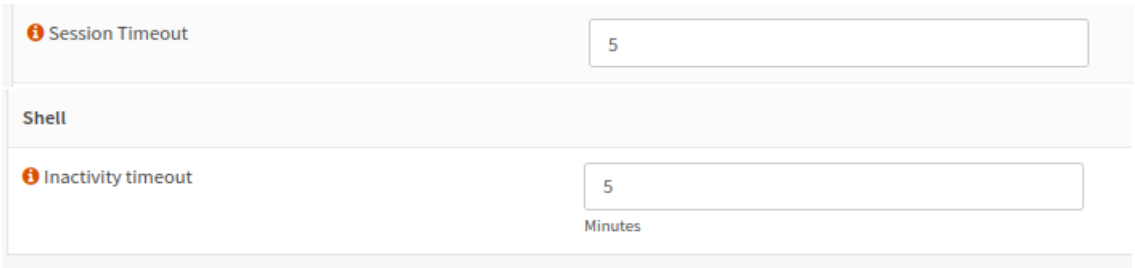
6.3.4 CHANGE SHELL TYPE AND INACTIVITY TIMEOUT

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

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



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



6.3.5 CHANGE PERMISSIONS OF /CONF/CONFIG.XML

In order to prevent that any user is able to view the critical /conf/config.xml local file, as indicated in the Security Target, the steps below are followed:

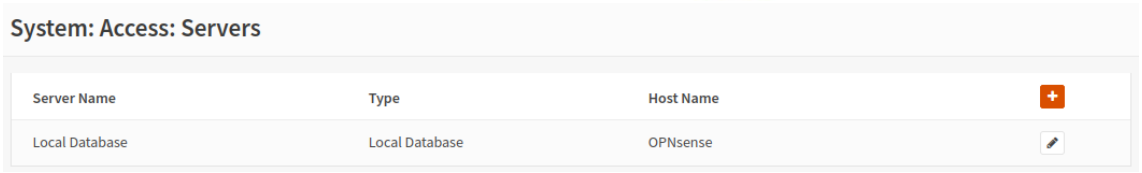
1. Log in through the TOE CLI interface with the root user.
2. Execute the following command in order to change the permissions associated with the config.xml file:

```
chmod 640 /conf/config.xml
```

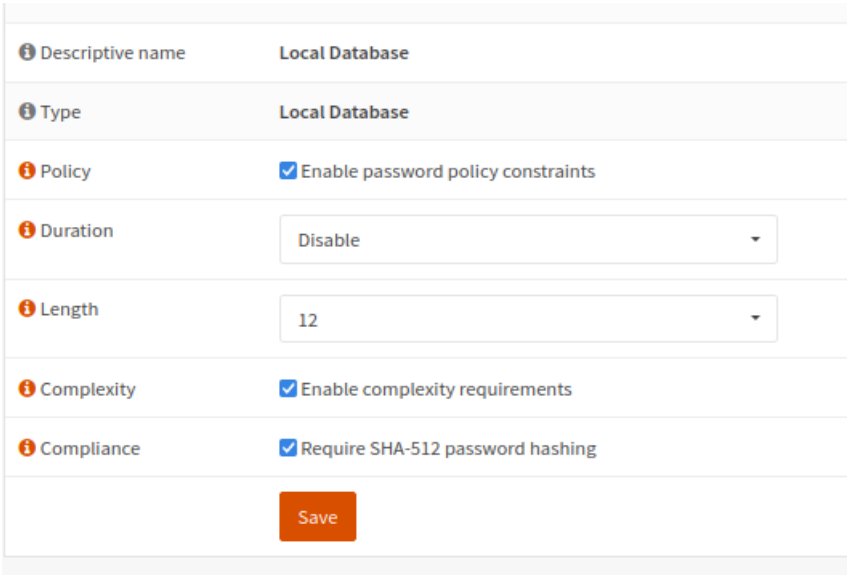
NOTE: Although this is included in the LINCE Security Target, these are deemed no longer necessary for the TOE version evaluated in the present report. The current version prevents non-administrative users from accessing the TOE locally.

6.3.6 DEFINING A PASSWORD POLICY

1. Log in through the TOE web interface with the root user.
2. Go to System → Access → Servers.
3. Edit the "Local Database" server.



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



5. Save the changes.

6.3.7 ADD A READ-ONLY AUDIT ROLE

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

1. Create a new directory that will store the new ACL by executing this command in CLI interface.

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

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

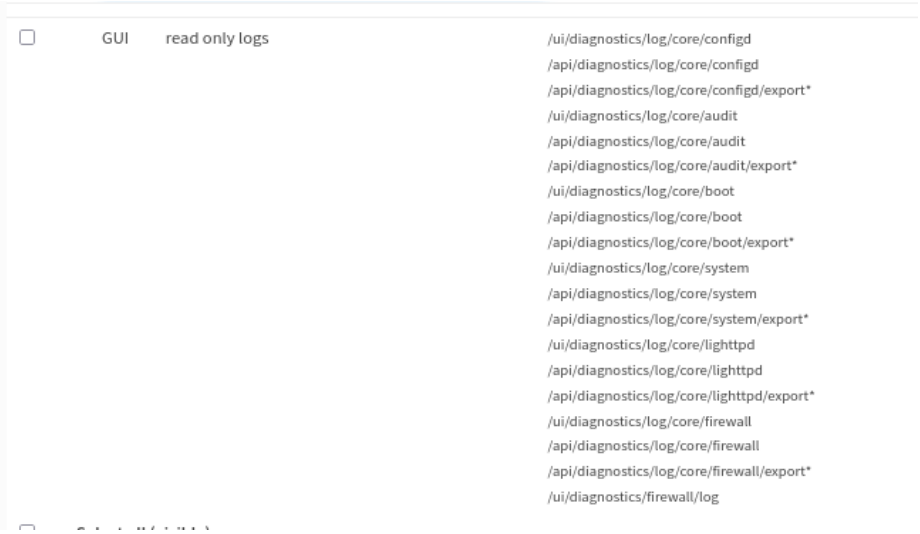
```
<acl>
    <page-diagnostics-logs-read-only>
        <name>read only logs</name>
        <patterns>
            <!-- System: Log Files: Backend -->
                <pattern>ui/diagnostics/log/core/configd</pattern>
                <pattern>api/diagnostics/log/core/configd</pattern>
              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

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

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

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

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



6.3.8 DISABLE ROOT USER FOR SSH

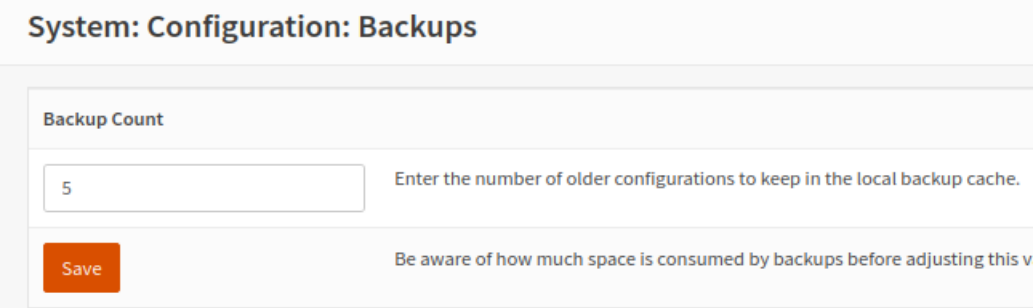
The Security Target indicates that it is required to disable root access to the CLI through SSH. The steps below are followed:

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

6.3.9 CONFIGURE SYSTEM BACKUPS ROTATION

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

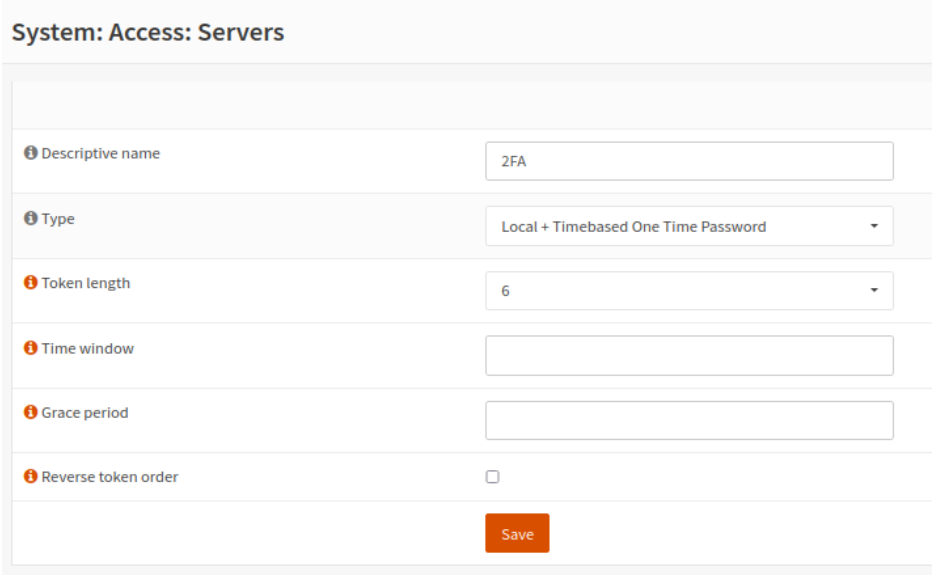
1. Log in through the TOE web interface with the root user.
2. Go to System → Configuration → Backups.
3. Configure the "Backup Count" parameter to 5.



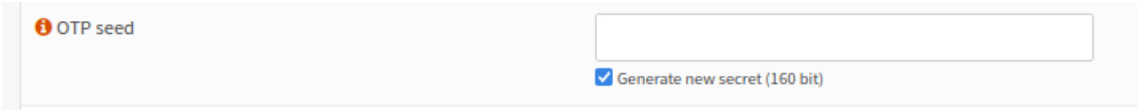
6.3.10CONFIGURE TWO-FACTOR AUTHENTICATION

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

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

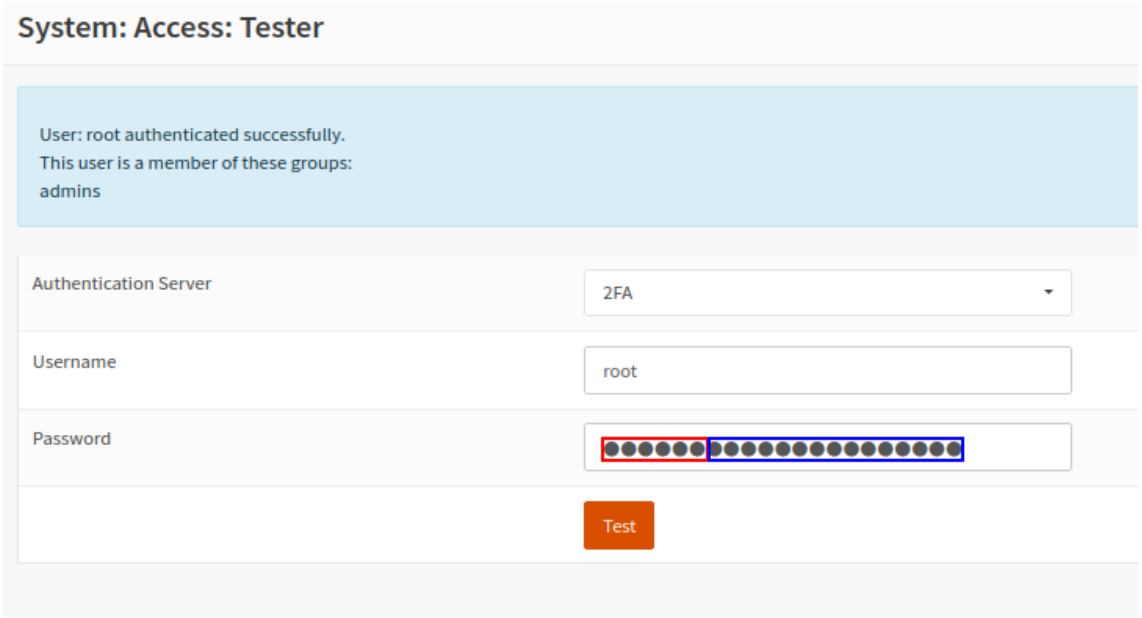


4. Install a Google Authenticator compatible app on your device.
5. Go to System → Access → Users.
6. Edit the root user.
7. Select "Generate a new secret (160 bit)" in the OTP parameter and click Save

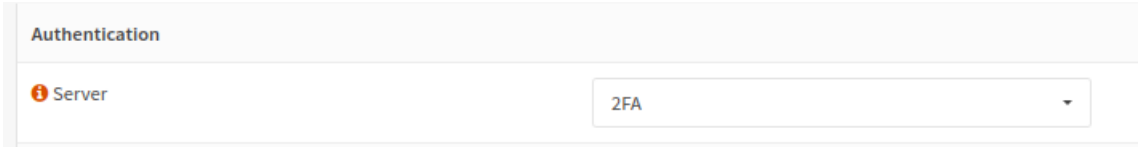


8. Edit again the root user to view the seed and QR, register such token or QR code in the Google Authenticator compatible app.

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



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



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

6.3.11CONFIGURING CONFIGD ACCESS CONTROL

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

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

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

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

```
[action_defaults]

allowed_groups = wheel
```

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

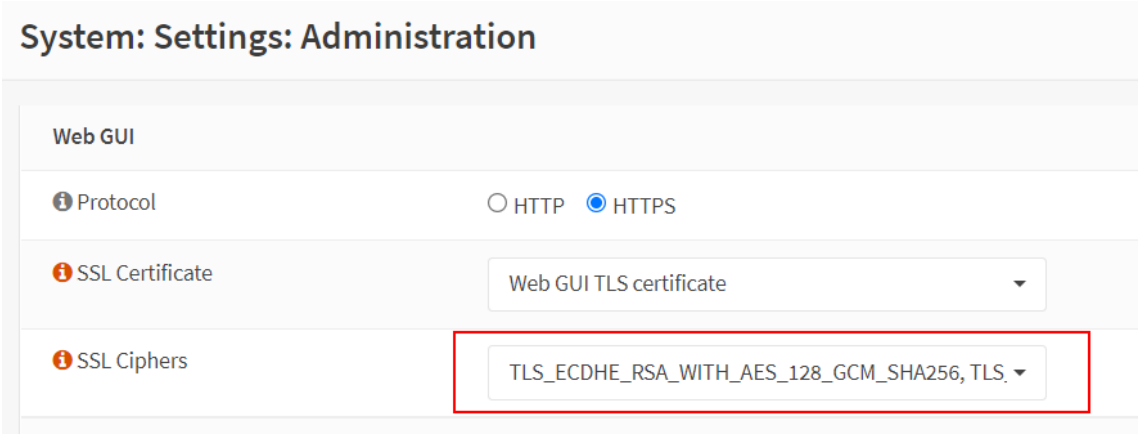
```
service configd restart
```

NOTE: Although this is included in the LINCE Security Target, these are deemed no longer necessary for the TOE version evaluated in the present report. The current version prevents non-administrative users from accessing the TOE locally.

6.3.12WEB INTERFACE TLS CIPHER SUITES CONFIGURATION

In order to meet the cryptographic requirements and conform [CCN-STIC-807] as declared in the Security Target, it is required to configure accepted cipher suites for TLS through the web interface. This configuration affects the web portal used to manage and administrate the TOE. The steps below are followed:

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



4. Scroll down and click Save.

6.3.13SSH CRYPTOGRAPHIC PARAMETERS CONFIGURATION

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

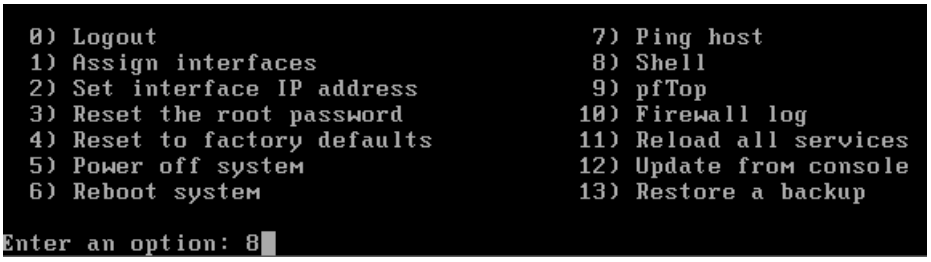
1. Log in through the TOE web interface with the root user.
2. Navigate to System → Settings → Administration.

3. In the Secure Shell section, use the dropdown menu for “Key exchange algorithms”, “Ciphers”, “MACs” and “Public key signature algorithms” to select valid cryptographic parameters.
    a. Key exchange algorithms:
        i. diffie-hellman-group16-sha512
        ii. diffie-hellman-group18-sha512
        iii. ecdh-sha2-nistp256
        iv. ecdh-sha2-nistp384
        v. ecdh-sha2-nistp521
    b. Ciphers:
        i. aes128-ctr
        ii. aes192-ctr
        iii. aes256-ctr
    c. MACs:
        i. hmac-sha2-256
        ii. hmac-sha2-512
    d. Public key signature algorithms:
        i. ecdsa-sha2-nistp256
    e. Rekey Limit:
        i. 1GB, 1 hour
2. Scroll down and click Save.

6.3.14SYSLOG CLIENT TLS CIPHER SUITES CONFIGURATION

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

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



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

```
ssl-options(no-sslv2, no-sslv3, no-tlsv1, no-tlsv11)
cipher-suite("ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-
AES128-GCM-
SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_GCM_SHA256:TLS_C
HACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-
```

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

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

4. Save the file.

NOTE: Although this is included in the LINCE Security Target, these are deemed no longer necessary for the TOE version evaluated in the present report. The current version allows to configure these parameters through the System > Trust > Settings menu.

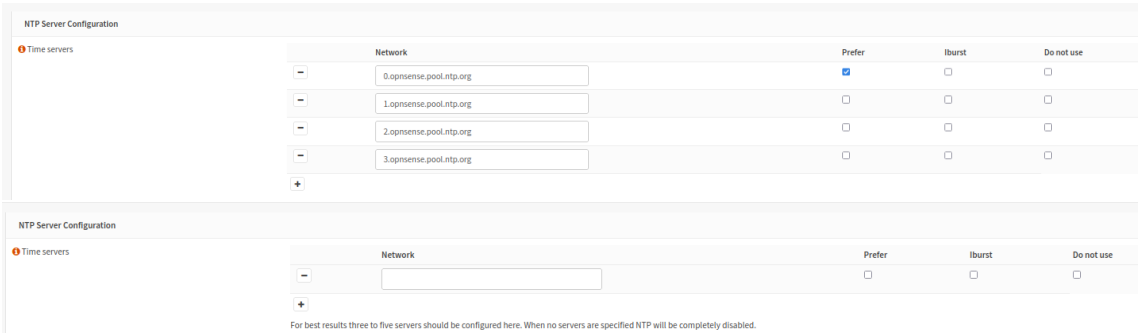
6.3.15INSTALLING CERTIFICATES FROM TRUSTWORTHY CA

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

6.3.16DISABLING NTP SERVICE

The steps below are followed:

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

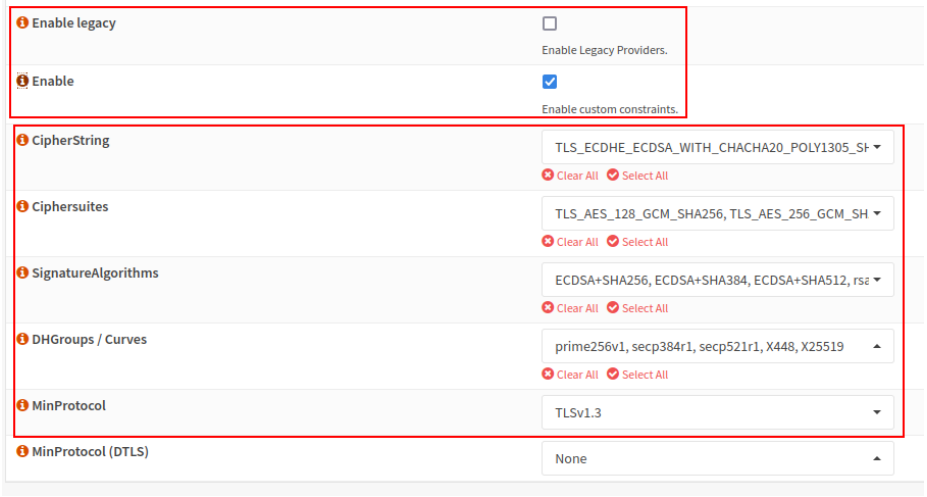


4. Click Save.

6.3.17MODIFYING TRUST SETTINGS

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

4. Under Configuration constraints, select the 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_sha514.
   d. DHGroups / Curves: prime256v1, secp384r1, secp521r1, x448, x25519
   e. MinProtocol: TLSv1.3

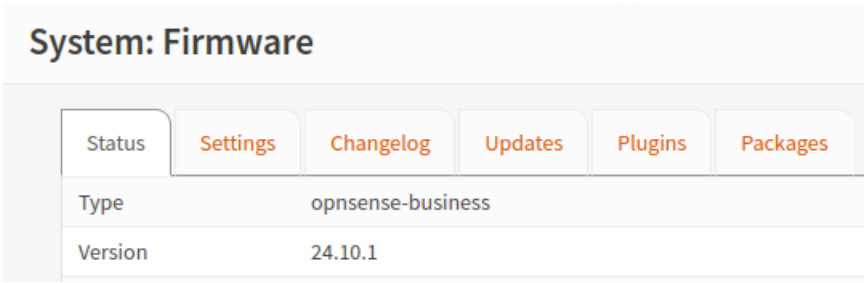


5. Save the changes and reboot the TOE.

6.4 VERIFICATION OF THE INSTALLED TOE VERSION

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

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



6.5 USED INSTALLATION OPTIONS

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

6.6 RESULTS

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

ID	Comments	State
N/A	None.	N/A

7 CONFORMITY ASSESSMENT

7.1 FUNCTIONAL TESTS

Evaluator	DAT
Days required	20 days.
Date	2025/01/28
Results of the evaluator's work	**FAIL**

7.1.1 EVALUATION ACTIVITIES

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

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

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

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

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

7.1.2 LIST OF FUNCTIONAL TESTS

Security function	Test code	Objective	Result
FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0010]	Verify that the TSF generates audit information for the declared events: • Start-up and shut-down of the audit functions.	**PASS**
FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1 FMT_SMF.1.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0011]	Verify that the TSF generates audit information for the declared events:	**PASS**

		• Generating/import of, changing, or deleting of cryptographic keys. • Management of the TOE's trust store.	
FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0013]	Verify that the TSF generates audit information for the declared events: • Discontinuous changes to time.	**PASS**
FAU_GEN.1.1 FAU_GEN.1.2 FAU_GEN.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0014]	Verify that the TSF generates audit information for the declared events: • Initiation/termination/ failure of the trusted channel with the remote audit server.	**PASS**
FAU_STG_EXT.1.4 FAU_STG_EXT.1.5	[STIC_OPNSENSE_HIGH-2404-TST-ND-0020]	Verify that the TSF overwrites previous audit records according to the maximum log file size and number of logs to be kept defined.	**PASS**
FMT_SMF.1.1 FIA_UIA_EXT.1.1 FTA_TAB.1.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0030]	Verify that the TSF provides the ability to configure the access banner and that the banner is shown when initiating an identification and authentication process.	**PASS**
FMT_SMF.1.1 FMT_MOF.1.1/Functions	[STIC_OPNSENSE_HIGH-2404-TST-ND-0032]	Verify that the TSF provides the ability to modify the behaviour of the transmission of audit data to an external IT entity and that this is restricted to administrator users.	**PASS**
FMT_SMF.1.1 FMT_MTD.1.1/CryptoKeys	[STIC_OPNSENSE_HIGH-2404-TST-ND-0033]	Verify that the TSF provides the ability to manage the cryptographic keys and that this is restricted to the administrator users.	**PASS**
FMT_SMF.1 FPT_STM_EXT.1.1 FPT_STM_EXT.1.2	[STIC_OPNSENSE_HIGH-2404-TST-ND-0034]	Verify that the TSF provides the ability to set the time which is used for time-stamps.	**PASS**

FIA_UIA_EXT.1.2 FIA_UIA_EXT.1.3 FIA_UIA_EXT.1.4	[STIC_OPNSENSE_HIGH-2404-TST-ND-0035]	Verify that the TSF identifies and authenticates administrative users using Web GUI password, SSH password and local CLI password.	**PASS**
FIA_UAU.7.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0040]	Verify that the TSF provides only obscured feedback to the administrative user while the authentication is in progress at the local console.	**PASS**
FPT_APW_EXT.1.1 FPT_APW_EXT.1.2	[STIC_OPNSENSE_HIGH-2404-TST-ND-0050]	Verify that the TSF stores administrative passwords in non-plaintext form and that it prevents reading.	**PASS**
FCS_TLSS_EXT.1.3	[STIC_OPNSENSE_HIGH-2404-TST-ND-0100]	Verify that the TSF performs key exchange using the declared curves for EC Diffie-Hellman and Diffie-Hellman parameters.	**PASS**
FCS_TLSS_EXT.1.4	[STIC_OPNSENSE_HIGH-2404-TST-ND-0110]	Verify that the TSF supports session resumption based on session tokens for TLSv1.2 according to RFC 5077 and does not support the early data extension.	**PASS**
FCS_TLSS_EXT.1.4 FCS_TLSS_EXT.1.6	[STIC_OPNSENSE_HIGH-2404-TST-ND-0120]	Verify that the TSF supports session resumption for TLSv1.3 according to RFC 8446 and does not support the early data extension.	**PASS**
FCS_TLSS_EXT.1.8	[STIC_OPNSENSE_HIGH-2404-TST-ND-0150]	Verify that the TSF supports secure renegotiation by including the "renegotiation_info" extension for TLSv1.2 and that rejects TLSv1.3 renegotiation attempts.	**PASS**
FCS_SSH_EXT.1.3	[STIC_OPNSENSE_HIGH-2404-TST-ND-0200]	Verify that the TSF ensures that packets greater than 262135 bytes in an SSH transport connection are dropped.	**PASS**
FCS_SSH_EXT.1.8	[STIC_OPNSENSE_HIGH-2404-TST-ND-0202]	ify that the TSF ensures that a rekey of the session keys occurs when one hour connection time is reached, no	**PASS**

		more than one gigabyte of transmitted data or no more than one gigabyte of received data.	
FCS_TLSC_EXT.1.2	[STIC_OPNSENSE_HIGH-2404-TST-ND-0300]	Verify that the TSF verifies that the identifier provided by the remote audit server when establishing a connection matches the reference identifier defined.	**PASS**
FCS_TLSC_EXT.1.3	[STIC_OPNSENSE_HIGH-2404-TST-ND-0310]	Verify that the TSF does not establish a trusted channel with the remote audit server if the server certificate is deemed invalid and that the TSF does not implement any administrator override mechanism.	**PASS**
FCS_TLSC_EXT.1.4	[STIC_OPNSENSE_HIGH-2404-TST-ND-0320]	Verify that the TSF presents the Supported Groups Extension with the declared curves/groups when establishing a connection with the remote audit server.	**PASS**
FCS_TLSC_EXT.1.5	[STIC_OPNSENSE_HIGH-2404-TST-ND-0330]	Verify that the TSF offers the declared signature algorithms when establishing a connection with the remote audit server.	**PASS**
FCS_TLSC_EXT.1.7	[STIC_OPNSENSE_HIGH-2404-TST-ND-0350]	Verify that the TSF does not use the early data extension and post-handshake client authentication according to RFC 8446 when establishing a connection with the remote audit server.	**PASS**
FCS_TLSC_EXT.1.9	[STIC_OPNSENSE_HIGH-2404-TST-ND-0370]	Verify that the TSF supports secure renegotiation as declared when establishing a connection with the remote audit server.	**PASS**
FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0380]	Verify that the TSF properly validates the certificate trust chain of the certificate presented by the remote audit server and that does not	**PASS**

		establish a connection when this chain is broken.	
FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0381]	Verify that the TSF does not establish a connection with the remote audit server when an expired certificate is presented.	**PASS**
FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0382]	Verify that the TSF properly handles and verifies the revocation status of the certificate presented when establishing a connection with the remote audit server.	**PASS**
FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0383]	Verify that the TSF does not establish a connection with the remote audit server when the CRL involved in the communication channel is signed by a CA that does not includes cRLsign key usage.	**PASS**
FIA_X509_EXT.1.1/Rev	[STIC_OPNSENSE_HIGH-2404-TST-ND-0384]	Verify that the TSF does not establish a connection with the remote audit server when any byte of the in the first eight bytes of the certificate is modified.	**PASS**
FIA_X509_EXT.1.1/Rev	[STIC_OPNSENSE_HIGH-2404-TST-ND-0385]	Verify that the TSF does not establish a connection with the remote audit server when any byte of the signatureValue field of the certificate is modified.	**PASS**
FIA_X509_EXT.1.1/Rev	[STIC_OPNSENSE_HIGH-2404-TST-ND-0386]	Verify that the TSF does not establish a connection with the remote audit server when any byte of the public key of the certificate is modified.	**PASS**
FIA_X509_EXT.1.2/Rev	[STIC_OPNSENSE_HIGH-2404-TST-ND-0387]	Verify that the TSF does not establishes a connection with the remote audit server when the certificate chain presented includes a CA that does not contain the basicConstraints extension or it is included with a FALSE value.	**PASS**

FIA_X509_EXT.2.2	[STIC_OPNSENSE_HIGH-2404-TST-ND-0390]	Verify that the TSF behaves as declared when establishing a connection with the remote audit server and it cannot to determine the revocation status of the presented certificate due to being unable to establish a connection with the endpoint that distributes the CRL.	**PASS**
FCS_TLSC_EXT.1.2	[STIC_OPNSENSE_HIGH-2404-TST-ND-0400]	Verify that the TSF verifies that the identifier provided by the update repository when establishing a connection matches the reference identifier defined.	**PASS**
FCS_TLSC_EXT.1.3	[STIC_OPNSENSE_HIGH-2404-TST-ND-0410]	Verify that the TSF does not establish a trusted channel with the update repository if the server certificate is deemed invalid and that the TSF does not implement any administrator override mechanism.	**PASS**
FCS_TLSC_EXT.1.4	[STIC_OPNSENSE_HIGH-2404-TST-ND-0420]	Verify that the TSF presents the Supported Groups Extension with the declared curves/groups when establishing a connection with the update repository.	**PASS**
FCS_TLSC_EXT.1.5	[STIC_OPNSENSE_HIGH-2404-TST-ND-0430]	Verify that the TSF offers the declared signature algorithms when establishing a connection with the update repository.	**PASS**
FCS_TLSC_EXT.1.6	[STIC_OPNSENSE_HIGH-2404-TST-ND-0440]	Verify that the TSF does not allow the configuration of the ciphersuites used when establishing a connection with the update repository.	**PASS**
FCS_TLSC_EXT.1.7	[STIC_OPNSENSE_HIGH-2404-TST-ND-0450]	Verify that the TSF does not use the early data extension and post-handshake client authentication according to RFC 8446 when establishing a connection with the update repository.	**PASS**

FCS_TLSC_EXT.1.9	[STIC_OPNSENSE_HIGH-2404-TST-ND-0470]	Verify that the TSF rejects secure renegotiation for TLSv1.3 as declared when establishing a connection with the update repository.	**PASS**
FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0480]	Verify that the TSF properly validates the certificate trust chain of the certificate presented by the update repository and that does not establish a connection when this chain is broken.	**PASS**
FIA_X509_EXT.1.1/Rev FIA_X509_EXT.1.2/Rev	[STIC_OPNSENSE_HIGH-2404-TST-ND-0481]	Verify that the TSF does not establish a connection with the update repository when an expired certificate is presented.	**PASS**
FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0482]	Verify that the TSF properly handles and verifies the revocation status of the certificate presented when establishing a connection with the update repository.	**PASS**
FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1	[STIC_OPNSENSE_HIGH-2404-TST-ND-0483]	Verify that the TSF does not establish a connection with the update repository the CRL involved in the communication channel is signed by a CA that does not includes cRLsign key usage.	**PASS**
FIA_X509_EXT.1.1/Rev	[STIC_OPNSENSE_HIGH-2404-TST-ND-0484]	Verify that the TSF does not establish a connection with the update repository when any byte of the in the first eight bytes of the certificate is modified.	**PASS**
FIA_X509_EXT.1.1/Rev	[STIC_OPNSENSE_HIGH-2404-TST-ND-0485]	Verify that the TSF does not establish a connection with the update repository when any byte of the signatureValue field of the certificate is modified.	**PASS**
FIA_X509_EXT.1.1/Rev	[STIC_OPNSENSE_HIGH-2404-TST-ND-0486]	Verify that the TSF does not establish a connection with the update repository when any byte of the public key of the certificate is modified.	**PASS**

FIA_X509_EXT.1.2/Rev	[STIC_OPNSENSE_HIGH-2404-TST-ND-0487]	Verify that the TSF does not establishes a connection with the update repository when the certificate chain presented includes a CA that does not contain the basicConstraints extension or it is included with a FALSE value.	**PASS**
FIA_X509_EXT.2.2	[STIC_OPNSENSE_HIGH-2404-TST-ND-0490]	Verify that the TSF behaves as declared when establishing a connection with the update repository and it cannot to determine the revocation status of the presented certificate due to being unable to establish a connection with the endpoint that distributes the CRL.	**PASS**
FIA_X509_EXT.3.1 FIA_X509_EXT.3.2	[STIC_OPNSENSE_HIGH-2404-TST-ND-0500]	Verify that the TSF generates Certificate Requests including the public key, common name, organization, organizational unit and country and that properly validates the response to the Certificate Request.	**PASS**
FFW_RUL_EXT.1.6	[STIC_OPNSENSE_HIGH-2404-TST-FW-0100]	Verify that the TSF drops and is capable of logging packets where the source address of the network packet is defined as a broadcast network address.	**PASS**
FFW_RUL_EXT.1.6	[STIC_OPNSENSE_HIGH-2404-TST-FW-0101]	Verify that the TSF drops and be capable of logging packets where the source address of the network packet is defined as a multicast address.	**PASS**
FFW_RUL_EXT.1.6	[STIC_OPNSENSE_HIGH-2404-TST-FW-0102]	Verify that the TSF drops and is capable of logging network packets where the source or destination address of the network packet is defined as being unspecified (i.e. 0.0.0.0) or an address “reserved for future use” (i.e. 240.0.0.0/4) as specified in RFC 5735 for IPv4.	**FAIL**

FFW_RUL_EXT.1.6	[STIC_OPNSENSE_HIGH-2404-TST-FW-0103]	Verify that the TSF drops and is 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.	**FAIL**
FFW_RUL_EXT.1.7	[STIC_OPNSENSE_HIGH-2404-TST-FW-0200]	Verify that the TSF drops and is 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.	**PASS**
FFW_RUL_EXT.1.7	[STIC_OPNSENSE_HIGH-2404-TST-FW-0201]	Verify that the TSF drops and is capable of logging network packets where the source or destination address of the network packet is a link-local address.	**PASS**
FFW_RUL_EXT.1.7	[STIC_OPNSENSE_HIGH-2404-TST-FW-0202]	Verify that the TSF drops and is 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 network packet was received.	**PASS**
FFW_RUL_EXT.1.10	[STIC_OPNSENSE_HIGH-2404-TST-FW-0300]	Verify that the TSF can limit an administratively defined number of half-open TCP connections and that after the limit is reached, new connections attempts are dropped and logged or counted	**PASS**

7.1.3 RESULTS

ID	Non-conformity	State
OR01.NC01	[STIC_OPNSENSE_HIGH-2404-TST-ND-0013] FAU_GEN.1.1 FAU_GEN.1.2	**CLOSED**

	FAU_GEN.2.1 When the date/time is manually changed by a user through the CLI making use of the "date" command, [TOE-2441_3] registers the event in the Audit log with the following entry: "date set by root". The entry contains a timestamp, type of event and user associated with the user. It is determined that, given the SFR FAU_GEN.1.2 requirement from [cPP-ND-30e], this type of event is missing the following piece of information in the log entry: old and new values for the time. The manufacturer provided [TOE-24101]; after repeating the associated test it is deemed that the issue is fixed since the audit register related to changes in date/time properly includes the timestamps before and after the change.	
OR01.NC02	[STIC_OPNSENSE_HIGH-2024-TST-ND-0050] FPT_APW_EXT.1.1 FPT_APW_EXT.1.2 [TOE-2441_3] stores administrative passwords in non-plaintext form and prevents its reading. The hash algorithm is identified as bcrypt which uses blowfish. This algorithm is not complied according to [CCN-STIC-807]. The manufacturer provides instructions to configure the usage of SHA-512 instead of blowfish. This option is available in the password policy menu, and it is verified in the associated functional test.	**CLOSED**
OR01.NC03	[STIC_OPNSENSE_HIGH-2404-TST-ND-0100] FCS_TLSS_EXT.1.3 [TOE-2441_3] supports the following elliptic curves and finite field groups in the TOE GUI interface: prime256v1 (also known as secp256r1), secp384r1, secp521r1, x25519, x448, ffdhe2048, ffdhe3072, ffdhe4096, ffdhe6144, ffdhe8192. The finite field group ffdhe2048 is considered LEGACY by [CCN-STIC-807]; given this, it is deemed not suitable for ENS HIGH category. Only cryptographic mechanisms identified as recommended by [CCN-STIC-807] shall be used for ENS HIGH category.	**CLOSED**

	The manufacturer provided [TOE-24101], after repeating the test associated with the non-conformity, it is revealed that only the elliptic curves are offered, not a single finite field group is supported; therefore, the issue is considered addressed and closed.	
OR01.NC04	[STIC_OPNSENSE_HIGH-2404-TST-ND-0202] FCS_SSH_EXT.1.8 [TOE-2441_3] does not seem to define a RekeyLimit for the SSH connections. After establishing the SSH connection and waiting for one hour, the rekey of the connection is not carried out by [TOE-2441_3]. Furthermore, the rekey of the connection is also not carried out by [TOE-2441_3] after having received or sent more than 1GB of data. [TOE-2441_3] must rekey the connection when any of the following thresholds happen: one hour connection time, no more than one gigabyte of transmitted data, or no more than one gigabyte of received data. The manufacturer provided [TOE-24101]; after repeating the associated test it is deemed that the issue is fixed, the SSH service is properly configured to perform rekey after 1 hour of the creation of the session, after 1GB of data has been sent and after 1GB of data has been received.	**CLOSED**
OR01.NC05	[STIC_OPNSENSE_HIGH-2404-TST-ND-0300] FCS_TLSC_EXT.1.2 [TOE-2441_3] fails to properly verify the reference identifier included in the certificate presented by the remote audit server when wildcards are included. When using IP reference identifiers, [TOE-2441_3] establishes a connection when the Common Name of the certificate includes a wildcard. For example, [TOE-2441_3] is configured to connect to the remote audit server "192.168.1.2" and the CN of the certificate is "*.168.1.2". It is expected that [TOE-2441_3] differentiates between identifiers with and without wildcards and the connection is not established. When using a DNS identifier: • [TOE-2441_3] establishes a connection when it is configured to connect to "foo.bar.example.com" and the remote audit server includes a wildcard not in the left-most position of the label (foo.*.example.com).	**CLOSED**

	It is expected that [TOE-2441_3] differentiates between identifiers with and without wildcards and the connection is not established. The manufacturer provided [TOE-24101]; after repeating the associated test it is deemed that the issue is fixed; the edge cases identified in the non-conformity are correctly addressed and the certificates are rejected and determined as invalid before establishing a connection.	
OR01.NC06	[STIC_OPNSENSE_HIGH-2404-TST-ND-0320] FCS_TLSC_EXT.1.4 [TOE-2441_3] offers the following group in the supported_groups TLS extension included in the Client Hello message when establishing a connection with the remote audit server: ffdhe2048. Such group is considered a LEGACY cryptographic mechanism according to [CCN-STIC-807]. Legacy cryptographic mechanisms are not suitable for HIGH category. The manufacturer provided [TOE-24101], after repeating the test associated with the non-conformity, it is revealed that only the elliptic curves are offered, not a single finite field group is supported; therefore, the issue is considered addressed and closed.	**CLOSED**
OR01.NC07	[STIC_OPNSENSE_HIGH-2404-TST-ND-0330] FCS_TLSC_EXT.1.5 [TOE-2441_3] offers signature algorithms when establishing a connection with the remote audit server that do not comply [CCN-STIC-807] ENS HIGH category. rsa_pkcs1_sha256, rsa_pkcs1_sha384, rsa_pkcs1_sha512: RSASSA-PKCS1 signature scheme is considered legacy according to [CCN-STIC-807]. SHA224 ECDSA, SHA224 RSA, SHA224 DSA: SHA224 hashing algorithm is considered legacy according to [CCN-STIC-807]. LEGACY cryptographic mechanisms are not suitable for ENS HIGH category. The manufacturer provided [TOE-24101], after repeating the test associated with the non-conformity, it is revealed that the TOE only offers digital signature algorithms that	**CLOSED**

	comply with ENS high category; therefore, addressing the non-conformitiy.	
OR01.NC08	[STIC_OPNSENSE_HIGH-2404-TST-ND-0370] FCS_TLSC_EXT.1.9 [TOE-2441_3], as a client, seems to support TLS renegotiation when establishing a connection with the remote audit server since it offers the suite TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff). Despite this, it has been identified that the TOE ignores Hello Request messages sent by the server and renegotiation does not occur, the TOE continues to send data instead of sending a Client Hello message as a follow up to the Hello Request message and the connection is not renegotiated. If TLS renegotiation is indeed supported in such communication channel, it is expected that Hello Request messages from the remote server are not ignored, and renegotiation shall occur. If TLS renegotiation is not supported, [TOE-2441_3] must terminate the connection after receiving the Hello Request message. The manufacturer provided [TOE-24101], with instructions to configure TLSv1.3 through the new System > Trust > Settings. These settings were applied (and documented as part of the installation/configuration of the TOE) and the associated test was repeated; the issue is deemed addressed and the non-conformity is closed.	**CLOSED**
OR01.NC09	[STIC_OPNSENSE_HIGH-2404-TST-ND-0382] FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1 [TOE-2441_3] does not properly handle certificate revocation lists (CRLs) when establishing a connection with the remote audit server. A certificate chain with a CA, an intermediate CA and a leaf certificate was generated. After revoking the intermediate CA and uploading the pertinent CRL file to System > Trust > Revocation, the connection is still established; [TOE-2441_3] does not seem to identify that the certificate chain presented by the remote audit server includes a revoked certificate. It is expected that [TOE-2441_3] verifies the revocation of certificates when establishing a connection with the remote audit server.	**CLOSED**

	The manufacturer provided [TOE-24101]; this version included new functionality that implemented the CRL handling and verification. The tests related to CRLs were repeated by the evaluator to properly verify the functionality, revealing that the tests passed; therefore, closing the non-conformity.	
OR01.NC10	[STIC_OPNSENSE_HIGH-2404-TST-ND-0383] FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1 [TOE-2441_3] does not properly handle certificate revocation lists (CRLs) when establishing a connection with the remote audit server. A certificate chain with a CA, an intermediate CA without the cRLsign key usage and a leaf certificate were generated. After revoking the leaf certificate using the intermediate CA and uploading the pertinent CRL file to System > Trust > Revocation, the connection is still established. It is expected that [TOE-2441_3] does not accept the certificate since the CRL was signed by a certificate that does not include the cRLsign key usage. Moreover, [TOE-2441_3] does not establish a remote connection to retrieve the certificate revocation list. The manufacturer provided [TOE-24101]; this version included new functionality that implemented the CRL handling and verification. The tests related to CRLs were repeated by the evaluator to properly verify the functionality, revealing that the tests passed; therefore, closing the non-conformity.	**CLOSED**
OR01.NC11	[STIC_OPNSENSE_HIGH-2404-TST-ND-0390] FIA_X509_EXT.2.2 [TOE-2441_3] does not retrieve CRLs remotely, connections related to the CRL are not established; [TOE-2441_3] does not follow and query the CRL URI included in the certificate presented by the remote audit server. It is expected that [TOE-2441_3] reaches an external entity to retrieve the CRL as part of the certificate revocation. A local revocation store can be used to verify and manage the revocation of certificates, but it shall not work as a replacement for remote retrieval of CRLs but an additional mechanism, this is indicated in the related SFR from the PP.	**CLOSED**

	The manufacturer provided [TOE-24101]; this version included new functionality that implemented the CRL handling and verification. The tests related to CRLs were repeated by the evaluator to properly verify the functionality, revealing that the tests passed; therefore, closing the non-conformity.	
OR01.NC12	[STIC_OPNSENSE_HIGH-2404-TST-ND-0430] FCS_TLSC_EXT.1.5 [TOE-2441_3] offers signature algorithms when establishing a connection with the update repository that do not comply [CCN-STIC-807] ENS HIGH category. • rsa_pkcs1_sha256, rsa_pkcs1_sha384, rsa_pkcs1_sha512: RSASSA-PKCS1 signature scheme is considered legacy. The manufacturer provided [TOE-24101], after repeating the test associated with the non-conformity, it is revealed that the TOE only offers digital signature algorithms that comply with ENS high category; therefore, addressing the non-conformitiy.	**CLOSED**
OR01.NC13	[STIC_OPNSENSE_HIGH-2404-TST-ND-0482] FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1 [TOE-2441_3] does not properly handle certificate revocation lists (CRLs) when establishing a connection with the update repository. A certificate chain with a CA, an intermediate CA and a leaf certificate were generated. After revoking the intermediate CA and uploading the pertinent CRL file to System > Trust > Revocation, the connection is still established; [TOE-2441_3] does not seem to identify that the certificate chain presented by the server includes a revoked certificate. It is expected that [TOE-2441_3] verifies the revocation of certificates when establishing a connection with the update repository. The manufacturer provided [TOE-24101]; this version included new functionality that implemented the CRL handling and verification. The tests related to CRLs were repeated by the evaluator to properly verify the	**CLOSED**

	functionality, revealing that the tests passed; therefore, closing the non-conformity.	
OR01.NC14	[STIC_OPNSENSE_HIGH-2404-TST-ND-0483] FIA_X509_EXT.1.1/Rev FIA_X509_EXT.2.1 [TOE-2441_3] does not properly handle certificate revocation lists (CRLs) when establishing a connection with the update repository. A certificate chain with a CA, an intermediate CA without the cRLsign key usage and a leaf certificate were generated. After revoking the leaf certificate using the intermediate CA and uploading the pertinent CRL file to System > Trust > Revocation, the connection is still established. It is expected that [TOE-2441_3] does not accept the certificate since the CRL was signed by a certificate that does not include the cRLsign key usage. Moreover, [TOE-2441_3] does not establish a remote connection to retrieve the certificate revocation list. The manufacturer provided [TOE-24101]; this version included new functionality that implemented the CRL handling and verification. The tests related to CRLs were repeated by the evaluator to properly verify the functionality, revealing that the tests passed; therefore, closing the non-conformity.	**CLOSED**
OR01.NC15	[STIC_OPNSENSE_HIGH-2404-TST-ND-0490] FIA_X509_EXT.2.2 [TOE-2441_3] does not retrieve CRLs remotely, connections related to the CRL are not established; [TOE-2441_3] does not follow and query the CRL URI included in the certificate presented by the update repository. It is expected that [TOE-2441_3] reaches an external entity to retrieve the CRL as part of the certificate revocation. A local revocation store can be used to verify and manage the revocation of certificates, but it shall not work as a replacement for remote retrieval of CRLs but an additional mechanism. The manufacturer provided [TOE-24101]; this version included new functionality that implemented the CRL handling and verification. The tests related to CRLs were repeated by the evaluator to properly verify the	**CLOSED**

	functionality, revealing that the tests passed; therefore, closing the non-conformity.	
OR01.NC16	[STIC_OPNSENSE_HIGH-2404-TST-ND-0500] FIA_X509_EXT.3.1 FIA_X509_EXT.3.2 [TOE-2441_3] does not seem to validate the trustworthiness of the CSR response when it is uploaded and associated with its Certificate Signing Request in the System > Trust > Certificate menu. The CSR response is pasted and uploaded but no feedback is provided regarding its validity; therefore, it is not clear that [TOE-2441_3] is validating the trustworthiness of the CA that issued that response to the CSR. It is expected that [TOE-2441_3] validates the response to the CSR and determines if the certification path of the response to the CSR is valid upon the upload by the user. The manufacturer provided [TOE-24101]; after repeating the associated test, it is deemed that the TOE includes the proper checks when validating a CSR response, rejecting responses that are signed by an unknown CA. Given this, the issue is considered addressed, and the non-conformity is closed.	**CLOSED**
OR01.NC17	[STIC_OPNSENSE_HIGH-2404-TST-FW-0100] FFW_RUL_EXT.1.6 [TOE-2441_3] does not drop network packets whose source address is defined as a broadcast address (e.g.: 192.168.2.255 in a 192.168.2.0/24 network). The network packet is identified by [TOE-2441_3] and transmitted to the destination. It is expected that [TOE-2441_3] drops and logs (or counts) such type of network packets. The manufacturer delivered [TOE-24101] alongside instructions to configure filtering rules in the firewall to properly filter out and log the pertinent packets. The associated test was repeated to verify the fix, closing the present non-conformity.	**CLOSED**
OR01.NC18	[STIC_OPNSENSE_HIGH-2404-TST-FW-0101] FFW_RUL_EXT.1.6 [TOE-2441_3] does not drop network packets where the source address of the network packet is defined as a	**CLOSED**

	multicast address (from 224.0.0.0 to 239.255.255.255). The network packet is identified by [TOE-2441_3] and transmitted to the destination. It is expected that [TOE-2441_3] drops and logs (or counts) such type of network packets. The manufacturer delivered [TOE-24101] alongside instructions to configure filtering rules in the firewall to properly filter out and log the pertinent packets. The associated test was repeated to verify the fix, closing the present non-conformity.	
OR01.NC19	[STIC_OPNSENSE_HIGH-2404-TST-FW-0102] FFW_RUL_EXT.1.6 [TOE-2441_3] does not drop network packets whose source or destination address are 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. It is expected that, in addition to dropping these types of network packets, the dropping action is logged or counted by [TOE-2441_3]. The manufacturer delivered [TOE-24101] alongside instructions to configure filtering rules in the firewall to properly filter out the pertinent packets. The test was repeated revealing that: • Packets with a source or destination "reserved for future use" address are properly dropped, and the event is logged. • Packets with unspecified (0.0.0.0) source address are properly dropped and the event is logged. • Packets with unspecified (0.0.0.0) destination address are dropped but the event is NOT logged. Therefore, although most of the points identified in the description of the non-conformity are addressed, given that the drop of packets with unspecified destination address is not logged, the non-conformity remains open.	**OPEN**
OR01.NC20	[STIC_OPNSENSE_HIGH-2404-TST-FW-0103] FFW_RUL_EXT.1.6 [TOE-2441_3] does not drop network packets whose source or destination address are defined as being "unspecified address" (0:0:0:0:0:0:0:0) or an address "reserved for future definition and use" (i.e. unicast	**OPEN**

	addresses not in this address range: 2000::/3) as specified in RFC 3513 for IPv6. It is expected that, in addition to dropping these types of network packets, the dropping action is logged or counted by [TOE-2441_3]. The manufacturer delivered [TOE-24101] alongside instructions to configure filtering rules in the firewall to properly filter out the pertinent packets. The test was repeated revealing that: • Packets with a source or destination "reserved for future use" address are properly dropped, and the event is logged. • Packets with unspecified (0:0:0:0:0:0:0:0) source address are properly dropped, and the event is logged. • Packets with unspecified (0:0:0:0:0:0:0:0) destination address are dropped but the event is NOT logged. Therefore, although most of the points identified in the description of the non-conformity are addressed, given that the drop of packets with unspecified destination address is not logged, the non-conformity remains open.	
OR01.NC21	[STIC_OPNSENSE_HIGH-2404-TST-FW-0200] FFW_RUL_EXT.1.7 [TOE-2441_3] does not drop network packets whose source address of the network packet is equal to the address of the network interface where the network packet was received. It is expected that, in addition to dropping these types of network packets, the dropping action is logged or counted by [TOE-2441_3]. The manufacturer delivered [TOE-24101] alongside instructions to configure filtering rules in the firewall to properly filter out and log the pertinent packets. The associated test was repeated to verify the fix, closing the present non-conformity.	**CLOSED**
OR01.NC22	[STIC_OPNSENSE_HIGH-2404-TST-FW-0201] FFW_RUL_EXT.1.7 [TOE-2441_3] does not drop network packets whose source or destination address of the network packet is a IPv4 link-local address (169.254.0.0/16).	**CLOSED**

	It is expected that, in addition to dropping these types of network packets, the dropping action is logged or counted by [TOE-2441_3]. When the source address is a link-local address, [TOE-2441_3] filtering logs show that the packet is forwarded but somehow it does not reach the destination. In any case, network packet does not seem to be drop according to [TOE-2441_3]. The manufacturer delivered [TOE-24101] alongside instructions to configure filtering rules in the firewall to properly filter out and log the pertinent packets. The associated test was repeated to verify the fix, closing the present non-conformity.	
OR01.NC23	[STIC_OPNSENSE_HIGH-2404-TST-FW-0202] FFW_RUL_EXT.1.7 [TOE-2441_3] does not drop network packets whose source address of the network packet does not belong to the networks associated with the network interface where the network packet was received. It is expected that, in addition to dropping these types of network packets, the dropping action is logged or counted by [TOE-2441_3]. The manufacturer delivered [TOE-24101] alongside instructions to configure filtering rules in the firewall to properly filter out and log the pertinent packets. The associated test was repeated to verify the fix, closing the present non-conformity.	**CLOSED**
OR01.NC24	[STIC_OPNSENSE_HIGH-2404-TST-FW-0300] FFW_RUL_EXT.1.10 [TOE-2441_3] provides the capability to limit the maximum number of states to an administratively defined number (Max states parameter available in the firewall rules), limiting the number of half-open connections that can be forwarded through the firewall. When such threshold is met, the remaining packets which are dropped and never reach their destination are not logged or counted. It is expected that [TOE-2441_3] logs or counts the packets that are dropped after the maximum number of states is reached.	**CLOSED**

	The manufacturer delivered [TOE-24101]. The associated test was repeated to verify the fix, closing the present non-conformity since it was verified that the packets are logged after the defined threshold is reached.	

ID	Comments	State
N/A	None.	N/A

8 VULNERABILITY ANALYSIS

Evaluator	DAT
Days required	2 days.
Date	2025/01/28
Results of the evaluator's work	**PASS**

8.1 EVALUATION ACTIVITIES

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

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

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

b) **Available information on the technology.**

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

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

PASS The TOE vulnerability analysis is described in the *8.3 TOE vulnerability analysis*. The result of this analysis is detailed in the section *13 Annex C: Vulnerability Analysis.*

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

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

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

PASS Information regarding the vulnerabilities found is summarized in section *8.4 List of potential vulnerabilities* and described in more detail in section *13 Annex C: Vulnerability Analysis*. The scenarios are detailed in section *11 Annex A: Test scenarios*.

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

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

This information is described in more detail in the section *13 Annex C: Vulnerability Analysis.*

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

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

8.2 METHODOLOGY USED FOR THE ANALYSIS

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

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

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

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

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

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

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

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

8.3 TOE VULNERABILITY ANALYSIS

The vulnerability analysis process involves checking all security features declared in the TOE, identifying potential TOE vulnerabilities.

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

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

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

8.4 LIST OF POTENTIAL VULNERABILITIES

Code	Attack potential
[STIC_OPNSENSE_HIGH-2404-VUL-0000]	6
[STIC_OPNSENSE_HIGH-2404-VUL-0001]	6
[STIC_OPNSENSE_HIGH-2404-VUL-0002]	6
[STIC_OPNSENSE_HIGH-2404-VUL-0003]	30

8.5 RESULTS

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

ID	Comments	State
N/A	None.	N/A

9 TOE PENETRATION TESTS

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

Evaluator	DAT
Days required	2 days.
Date	2025/01/28
Results of the evaluator's work	**PASS**

9.1 EVALUATION ACTIVITIES

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

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

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

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

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

9.2 LIST OF PENETRATION TESTS

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

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

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

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

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

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

Security function	Test code	Objective	Result
All security functions	[STIC_OPNSENSE_HIGH-2404-PT-0000]	Verify if it is possible to exploit CVE-2024-11236 and CVE-2024-8932.	**PASS**
All security functions	[STIC_OPNSENSE_HIGH-2404-PT-0001]	Verify if it is possible to exploit CVE-2024-11234.	**PASS**
All security functions	[STIC_OPNSENSE_HIGH-2404-PT-0002]	Verify if it is possible to exploit CVE-2024-11233.	**PASS**

9.3 RESULTS

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

ID	Comments	State
N/A	None.	N/A

10 REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation.

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

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

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

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

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

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

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

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

[CCN-STIC 140-D3] Reference Taxonomy for ICT Security Products - Annex D.3: Firewall. 2020 August.

[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.

[PKG-SSH-10] Functional Package for SSH Version 1.0

[PKG-TLS-11] Functional Package for TLS Version 1.1

[PPMOD-FW-14e] collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625

[PPMOD-FW-14e-SD]	collaborative Protection Profile Module for Stateful Traffic Filter Firewalls v1.4 + Errata 20200625 Supporting Document
[LINCE-ST-08]	OPNsense Business Edition Security Target version 0.7 (LINCE)
[IAR-10]	OPNsense Business Edition IAR version 1.0

10.1 DEVELOPER EVIDENCES

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

11 ACRONYMS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
LINCE	National Essential Security Certification
MCF	Source Code Module
MEB	Biometric Evaluation Module
MEC	Cryptographic Evaluation Module
TIC	Information and Communications Technology
TOE	Target Of Evaluation
SSH	Secure Shell
NTP	Network Time Protocol
TLS	Transport Layer Security
CLI	Command Line Interface
GUI	Graphical User Interface
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CA	Certification Authority
CVE	Common Vulnerabilities and Exposures