



jtsec
BEYOND IT SECURITY

LINCE Evaluation Technical Report

LINCE_OPNSENSE_BE (2024-13)

1.0

2024/06/24





CHANGELOG

Version	Date	Author	Reason	Changes
V1.0	2024/06/24	DAT	First version.	Document creation.

TABLE OF CONTENTS

1	Introduction.....	5
1.1	Evaluation Technical Report information	5
1.2	TOE developer information	5
2	TOE description	6
2.1	Functional description of the TOE	6
2.2	Inventory of security functions	8
2.2.1	SF. Trusted Administration	8
2.2.2	SF. Identification and Authentication.....	9
2.2.3	SF. Trusted Communication Channels.....	10
2.2.4	SF. Cryptography	11
2.2.5	SF. Trusted Installation and Updates.....	12
2.2.6	SF. Audit.....	12
2.2.7	SF. Protection of Credentials and Sensitive Data	14
2.2.8	SF. Firewalls	14
3	Operational environment.....	16
3.1	Description of the operational environment.....	16
3.2	Operational environment assumptions.....	17
4	Executive summary of the evaluation	18
5	Verdict of the evaluation	23
6	TOE installation and review of the installation, configuration and operation guides 24	
6.1	Evaluation activities	24
6.2	Detailed configuration of the operational environment.....	25
6.3	Description of the installation and configuration of the TOE.....	26
6.3.1	OPNsense installation.....	26
6.3.2	Setting a subscription key.....	33
6.3.3	Updating to 23.10.2 version	34
6.3.4	Enabling access logs.....	35
6.3.5	Change shell type and inactivity timeout.....	35
6.3.6	Change permissions of /conf/config.xml.....	35
6.3.7	Defining a password policy	36
6.3.8	Add a read-only audit role.....	36
6.3.9	Disable root user for SSH.....	38

6.3.10	Configure system backups rotation.....	39
6.3.11	Configure two-factor authentication	39
6.3.12	Configuring configd access control.....	41
6.3.13	Web interface TLS cipher suites configuration	41
6.3.14	SSH cryptographic parameters configuration	42
6.3.15	Syslog client TLS cipher suites configuration.....	43
6.3.16	Installing certificates from trustworthy CA	43
6.4	Verification of the installed TOE version	43
6.5	Used installation options	44
6.6	Results.....	44
7	Conformity assessment	45
7.1	Security Target assessment	45
7.1.1	Evaluation activities.....	45
7.1.2	Results.....	47
7.2	Functional tests.....	51
7.2.1	Evaluation activities.....	51
7.2.2	List of functional tests	51
7.2.3	Results.....	56
8	Vulnerability analysis.....	60
8.1	Evaluation activities	60
8.2	Methodology used for the analysis	61
8.3	TOE vulnerability analysis	62
8.4	List of potential vulnerabilities	62
8.5	Results.....	62
9	TOE penetration tests.....	64
9.1	Evaluation activities	64
9.2	List of penetration tests.....	64
9.3	Results.....	69
10	References	71
10.1	Developer Evidences	71
11	Acronyms.....	73

1 INTRODUCTION

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

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

1.1 EVALUATION TECHNICAL REPORT INFORMATION

ETR reference	LINCE_OPNSENSE_BE-ETR-v1.0
ETR version	1.0
Author or authors	DAT
Reviewer	ACP
Approved by	JTG
Start date of the works	2024/06/04
End date of the works	
CB dossier code	2024-13
Laboratory project code	LINCE_OPNSENSE_BE
Type of evaluation	LINCE
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	23.10.2
Operating manuals of the product	[OPNSENSE-DOCS-D971B9D]

2 TOE DESCRIPTION

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

2.1 FUNCTIONAL DESCRIPTION OF THE TOE

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

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

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

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

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

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

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

- **CLI interface:**
 - Local access: Available directly on the machine where the TOE is installed, allowing administrators to perform the initial configuration, maintenance and management of the system without the need for a network connection.
 - Remote access: which allows remote TOE management via SSHv2. The use of this interface is not allowed to the *root* user.
- **GUI interface**: it is a web interface which allows TOE management via HTTPS (over TLSv1.2 or higher).

```

Hello, this is OPNsense 23.10

Website:      https://opnsense.org/
Handbook:     https://docs.opnsense.org/
Forums:       https://forum.opnsense.org/
Code:         https://github.com/opnsense
Twitter:      https://twitter.com/opnsense

*** OPNsense.localdomain: OPNsense 23.10 ***

LAN (em0)      -> v4: 192.168.1.1/24

HTTPS: SHA256 C1 4D 0C 16 79 BA 99 DF 9E 56 05 2E 71 AD D6 04
              AF 1D 50 D5 B7 11 12 B9 0F 0E 68 85 78 4F 62 62

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

Enter an option:

```

Figure 1 TOE CLI interface

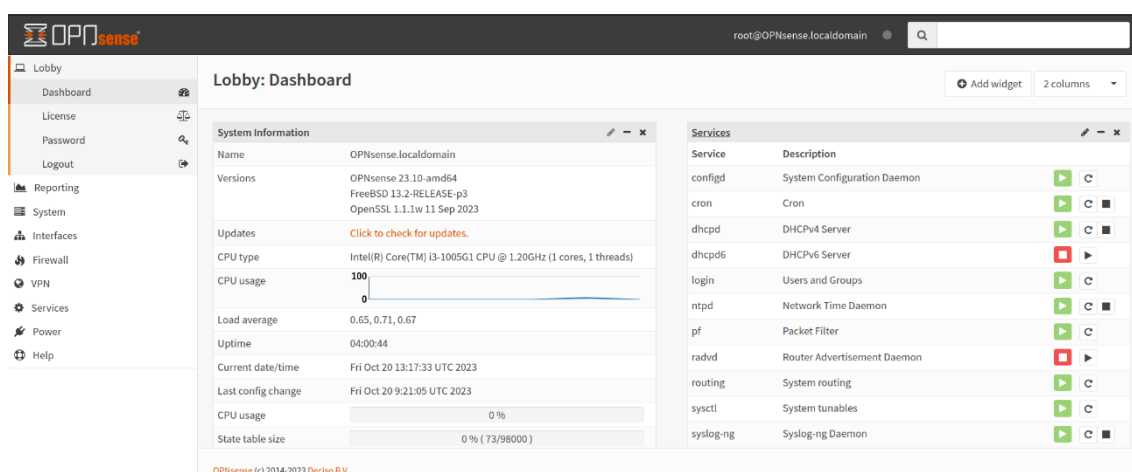


Figure 2 TOE GUI interface

In relation with the specific functionalities of the TOE, it can be defined the following:

- **SF. Trusted Administration:** The TOE defines users and groups, permissions can be specified for groups and for individual users. The TOE defines a default root user with all permissions. Only administrator users or users with the necessary permissions set can perform management functions.
- **SF. Identification and Authentication:** The TOE is in charge of identifying and authenticating every user, apart from implementing mechanisms to prevent brute-force attacks and a password policy. In addition, the TOE is capable to close a user's session after a determined inactivity time.
- **SF. Trusted Communication Channels:** The TOE protects the information in transit for management purposes by establishing secure communications channels using SSHv2 and HTTPS (over TLS v1.2 or higher). In addition, the TOE

establishes secure communication channels using TLS v1.2 when exchanging information with external syslog servers and using TLS v1.3 with the endpoints for OPNsense updates.

- **SF. Cryptography:** The TOE supports only cryptographic algorithms and functions accepted for ENS MEDIUM category of CCN-STIC-807 guide.
- **SF. Trusted Installation and Updates:** The TOE shall verify the authenticity of updates using a digital signature RSA-4096 with RSASSA-PKCS#1 padding and the SHA-256 checksum. Furthermore, the TOE allows to check if any new updates are available.
- **SF. Audit:** The TOE produces a range of audit records based on various events and behaviours detected during its operation. An access control policy is applied to the audit records. Finally, the audit data can be sent to an external syslog server.
- **SF. Protection of Credentials and Sensitive Data:** Credentials and private keys are protected by access control (read/write permissions only for the root user).
- **SF. Firewalls:** The TOE allows to configure rules with actions to allow, block or reject traffic, based on attributes such as IP addresses, protocols and ports.

2.2 INVENTORY OF SECURITY FUNCTIONS

2.2.1 SF. TRUSTED ADMINISTRATION

Requirement	Description
ADM.1	The TOE define a default root user and provide the ability to create new users or groups of users. The TOE also allows modifying the privileges assigned to a given user or group of users.
ADM.2	<p>The TOE shall allow the authorized users to perform the following functionalities remotely:</p> <ul style="list-style-type: none"> • Configuration of the session termination when inactivity is detected. • Configuration of the TOE: <ul style="list-style-type: none"> ○ Update the TOE. ○ Create, modify and delete users. ○ Create, modify and delete user groups. ○ Associate permissions to groups or users. ○ Load SSL certificate for GUI. ○ Enabling to connect to the TOE by SSH. ○ Allowing the root user to connect by SSH. • Functionalities of the TOE: <ul style="list-style-type: none"> ○ Create, modify or delete Firewall rules. ○ Change the order of existing Firewall rules.
ADM.3	The TOE shall ensure only specific entities are capable of perform the ADM.2 functions:

	<ul style="list-style-type: none"> • Root user. • Another user/group with the specific permissions: <ul style="list-style-type: none"> ○ <u>Update the TOE: "System: Firmware"</u> ○ <u>Create, modify and delete users: "System: User Manager"</u> ○ <u>Create, modify and delete user groups: "System: Group Manager"</u> ○ <u>Associate permissions to groups or users: "System: Group Manager: Add Privileges" "System: User Manager: Add Privileges"</u> ○ <u>Load SSL certificate for GUI: "System Advanced: Admin Access Page"</u> ○ <u>Enabling to connect to the TOE by SSH: "System: Advanced: Admin Access Page"</u> ○ <u>Allowing the root user to connect by SSH: "System: Advanced: Admin Access Page"</u> ○ <u>Create, modify or delete Firewall rules: "Firewall: Rules: Edit" and "Firewall: Rules"</u> ○ <u>Change the order of existing Firewall rules: "Firewall: Rules"</u> ○ <u>Configuration of the session termination when inactivity is detected: "System: Advanced: Admin Access Page"</u>. • Also, with the permission <i>"All pages"</i>, the user could have all the permissions to all the previously defined administrable functions.
--	---

2.2.2 SF. IDENTIFICATION AND AUTHENTICATION

Requirement	Description
IAU.1	The TOE shall identify and authenticate every user through username and password before granting access to the GUI and CLI interfaces.
IAU.2	The TOE shall implement a 2FA mechanism to protect against authentication brute-force attacks.
IAU.3	<p>The password policy of the TOE shall be as follows:</p> <ul style="list-style-type: none"> • The password shall be configurable with a minimum or equal length of 12 characters. • The password shall be able to be composed of 3 of the following 4 parameters: <ul style="list-style-type: none"> ○ Lowercase letters ○ Uppercase letters ○ Numbers

	<ul style="list-style-type: none"> ○ Special characters "!", "@", "#", "\$", "%", "^", "&", "*", "(", ")".
IAU.4	The TOE shall close a user session established through CLI and GUI interfaces after 5 minutes of inactivity.

2.2.3 SF. TRUSTED COMMUNICATION CHANNELS

Requirement	Description
COM.1	<p>The TOE shall establish secure channels when exchanging sensitive information with authorized entities:</p> <ul style="list-style-type: none"> • The TOE with an external syslog server using TLS v1.2 or higher, using the following cipher suites: <ul style="list-style-type: none"> ○ TLS_AES_256_GCM_SHA384 (R) ○ TLS_AES_128_GCM_SHA256 (R) ○ TLS_CHACHA20_POLY1305_SHA256 (R) ○ TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R) ○ TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R) ○ TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (R) ○ TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (R) ○ TLS_ECDHE_ECDSA_WITH_AES_256_CCM (R) ○ TLS_ECDHE_ECDSA_WITH_AES_128_CCM (R) • The TOE with the update server using TLS v1.3, with ECDHE key exchange method, with 25519 (R), secp256r1 (R), 448 (R), secp521r1 (R) and secp384r1 (R) curves and the following ciphersuites: <ul style="list-style-type: none"> ○ TLS_AES_256_GCM_SHA384 (R) ○ TLS_CHACHA20_POLY1305_SHA256 (R) ○ TLS_AES_128_GCM_SHA256 (R)
COM.2	<p>The TOE shall allow secure communications channels to be initiated by itself or by authorized entities. These secure communication channels are the following:</p> <ol style="list-style-type: none"> 1. Communication between the TOE and the external syslog server through TLS v1.2 or higher, initialized by the TOE. 2. Communication between the TOE and the update server through TLS v1.3, initialized by the TOE.
COM.3	The TOE shall use digital certificates RSA-3072 or higher when the users use the HTTPS protocol to access the TOE's web interface.
COM.4	The TOE shall establish secure communication channels when exchanging information with the authorized user, using algorithms accepted according to the ENS MEDIUM category of the CCN-STIC-807 guide:

- The Administrator with the TOE via the GUI interface through HTTPS (over TLS v1.2 or higher), using the following cipher suites:
 - *TLS_AES_128_GCM_SHA256 (R)*
 - *TLS_AES_256_GCM_SHA384 (R)*
 - *TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (R)*
 - *TLS_CHACHA20_POLY1305_SHA256 (R)*
 - *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R)*
 - *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R)*
- The Administrator with the TOE via the CLI interface through SSHv2 using:
 - **SSH Key Exchange Method**
 - *diffie-hellman-group16-sha512 (R)*
 - *diffie-hellman-group18-sha512 (R)*
 - *ecdh-sha2-nistp256 (R)*
 - *ecdh-sha2-nistp384 (R)*
 - *ecdh-sha2-nistp521 (R)*
 - **SSH Encryption Algorithms**
 - *aes128-ctr (R)*
 - *aes192-ctr (R)*
 - *aes256-ctr (R)*
 - **SSH Public Key Algorithm**
 - *ecdsa-sha2-nistp256 (R)*
 - **SSH MAC Algorithm**
 - *hmac-sha2-256 (R)*
 - *hmac-sha2-512 (R)*

2.2.4 SF. CRYPTOGRAPHY

Requirement	Description
CIF.1	<p>The TOE shall use the following cryptographic mechanisms in compliance in accordance with the provisions of guide ENS MEDIUM CCN-STIC-807:</p> <ul style="list-style-type: none"> • Cipher suites of the communication channels defined in COM.1 and COM.4. • The certificates as specified in COM.3. • The cryptographic algorithm for software updates integrity, as defined in ACT.2.

2.2.5 SF. TRUSTED INSTALLATION AND UPDATES

Requirement	Description
ACT.1	The TOE shall provide the ability to query the current software version through the <i>System</i> → <i>Firmware</i> menu of the GUI interface, initiate updates manually and check for new updates available.
ACT.2	The TOE shall use RSA-4096 digital signatures with RSASSA-PKCS#1 (L) padding and SHA-256 hashing to authenticate software updates before installation.
ACT.3	Software update shall be allowed only to the followings users/group of users: <ul style="list-style-type: none"> • Root user. • Another user/group of users with “<i>System: Firmware</i>” permission.

2.2.6 SF. AUDIT

Requirement	Description
AUD.1	The TOE shall generate audit records when any of the following events occur: <ul style="list-style-type: none"> • Login and logout of the users. • Changes in user credentials. • Changes in TOE configurations and functionalities: <ul style="list-style-type: none"> ○ Events described in ADM.2. • Events related with TOE functionality when a rule is applied to incoming or outgoing traffic is allowed, blocked or rejected.
AUD.2	Audit records shall contain at least the following information: <ul style="list-style-type: none"> • Date and time of the event. • Type of identified event, depending on the specific event, the TOE will display a specific type of log output: <ul style="list-style-type: none"> ✓ “user [user@<IP>] changed configuration to /conf/backup/config*.xml in /system_usermanager.php?act=edit&userid=<user ID> [user “[name of the user]” changed]”, for the following administrable function: <ul style="list-style-type: none"> ▪ Changes in user credentials.

	<ul style="list-style-type: none"> ✓ “/system_advanced_admin.php made changes”, for the following administrable functions: <ul style="list-style-type: none"> ▪ Session termination. ▪ Delete groups. ▪ Associate permissions to users/groups. ▪ Load SSL certificate for GUI. ▪ Enable to connect the TOE by SSH. ✓ “opnsense-business upgraded”, for the following administrable function: <ul style="list-style-type: none"> ▪ Update the TOE ✓ “The user “user” was successfully removed”, for the deletion of users ✓ “/firewall_rules_edit.php made changes”, for the following administrable functions: <ul style="list-style-type: none"> ▪ Create, modify or delete Firewall rules. ▪ Change the order of existing Firewall rules • Result of the event • User producing the event (if applicable).
AUD.3	<p>The following access policy shall apply to audit records:</p> <ul style="list-style-type: none"> • Read: <ul style="list-style-type: none"> ○ root user, ○ Users or group of users with “<i>read only logs</i>” permission • Modify: Root user, only locally by CLI interface. • Delete: Root user, only locally by CLI interface.
AUD.4	<p>The TOE shall be able to store the generated audit information in itself and transmit the generated audit information to an external Syslog server using a secure TLS v1.2 or higher channel described in COM.1.</p>
AUD.5	<p>The TOE shall implement a rotation mechanism based on two main configurations:</p> <ul style="list-style-type: none"> ▪ <u>‘preservelogs’</u>: Determines the number of logs to be kept before deletion. ▪ <u>‘maxfilesize’</u>: Sets a limit on the maximum size allowed for each log file.

	If a log file exceeds the 'maxfilesize' limit, an early log rotation will be forced, preserving the integrity of the logs without compromising the available storage space.
--	---

2.2.7 SF. PROTECTION OF CREDENTIALS AND SENSITIVE DATA

Requirement	Description
PSC.1	The TOE shall ensure that the specific directory where are stored credentials (login passwords) and private keys has read/write permissions only for the root user by a previously defined control access.

2.2.8 SF. FIREWALLS

Requirement	Description
FWL.1	The TOE shall allow the definition of stateful traffic filtering rules using the following settings: <ul style="list-style-type: none"> • Source and destination address. • Source and destination ports. • Type. • Interface.
FWL.2	The TOE shall have the ability to process and inspect packets from the following network protocols: ICMPv4, ICMPv6, IPv4, IPv6, TCP, UDP in a way that allows: <ol style="list-style-type: none"> 1. Define packet filtering rules based on the settings defined in FWL.1. 2. Use the following basic filtering operations: pass, block, and reject. Also allowing to save the operation performed in the activity log. 3. Assign rules in a specific order to network interfaces of the TOE, defined by an authorized user.
FWL.3	The TOE shall drop traffic if no rule applies. This behaviour is set by default.
FWL.4	The TOE shall consider that a session between devices connected to the TOE has been terminated when there is inactivity in the session for specific time depending on the protocol: <ul style="list-style-type: none"> • <u>TCP connection</u>: When a TCP connection is established the TOE uses a state timeout value of 86400 seconds. • <u>UDP connection</u>: When UDP packets are transmitted, the TOE generates a session with a timeout of 60 seconds. The

	subsequent UDP packets transmitted before the timeout value expires refresh the initial value to 30 seconds.
--	--

3 OPERATIONAL ENVIRONMENT

3.1 DESCRIPTION OF THE OPERATIONAL ENVIRONMENT

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

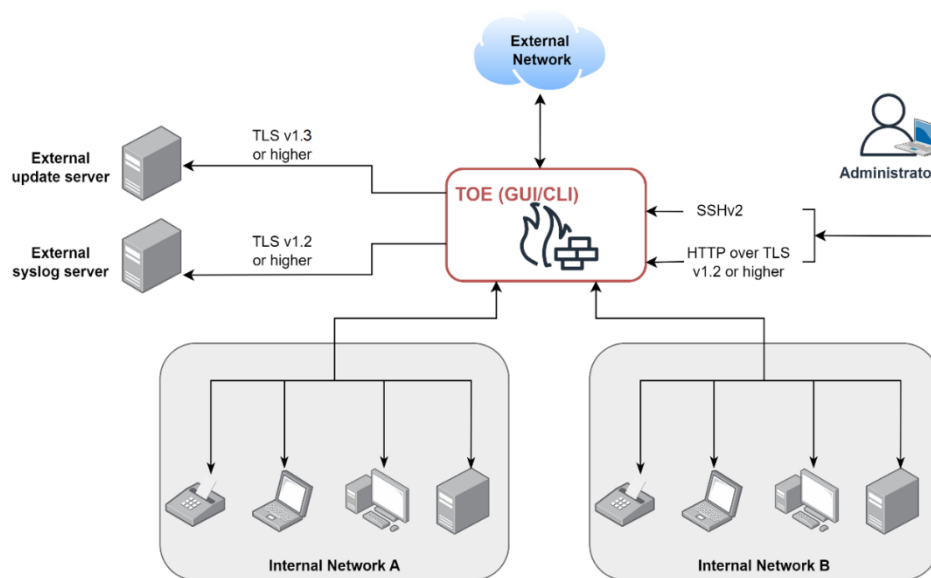


Figure 3 TOE operational environment

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 PLATFORM ADMINISTRATOR	Administrators of the platform where the TOE runs 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 environment.
A.PERIODIC UPDATES	The software of the product is updated when new updates that fix known vulnerabilities appear.
A.PROTECTION OF CREDENTIALS	All credentials, especially the administrator's, must be properly protected by the organization using the product be properly protected by the organization.

4 EXECUTIVE SUMMARY OF THE EVALUATION

The evaluation for the product OPNsense Business Edition has been carried out following the LINCE methodology in order to verify if the product covers a set of requirements declared in the Security Target document provided by the manufacturer.

The evaluation started after a kick-off meeting with the manufacturer which included a brief demonstration of the capabilities and functionalities offered by the product, which was delivered to the laboratory through [TOE-ISO-2310].

Firstly, as the Security Target [ST-04] was delivered to the laboratory, the pertinent analysis was performed. The analysis of [ST-04] revealed several issues that were registered in the pertinent documental Observation Report. Following, there is a summarized description of the opened non-conformities.

- [ST-04] includes some inconsistencies when referring to the TLS protocol version related to the TOE web interface. In section 2.1 TOE Functional description, “over TLSv1.3” is mentioned, while in other sections such as the description of the requirement COM.4, “TLSv1.2 or higher” is defined. This is considered contradictory and confusing (OR01.NC01).
- According to the documentation of the TOE, there are several different options in relation to what image to choose for installation. Four types of installation are defined: “dvd”, “vga”, “serial”, “nano”. It is considered that the installation method is not well identified or indicated to the user in [ST-04]; therefore, the installation procedure included is not properly defined (OR01.NC03).
- The section 2.3 TOE usage description of [ST-04], includes the subsection OPNsense Business Edition installer which includes some steps with the purpose to defined the installation procedure of the TOE. The steps are poorly documented and most of the steps are missing. It is required for the author to properly defined the installation procedure with the complete steps (OR01.NC04).
- The section 2.3 TOE usage description of [ST-04], includes the subsection CLI interface idle timeout configuration which indicates the reader to navigate to the “System → Settings → Administration” in order to change the Login shell of a user. These instructions are deemed incorrect, it is not possible to change the Login shell parameter in such menu, this parameter is associated with each user uniquely and it is changed in the profile of each user. In the same paragraph, the author states that the default session timeout for the GUI interface is 5 minutes. This is wrong, the default time is 4 hours. Instructions to change such timeout seem to be missing (OR01.NC05).
- The section 2.3 TOE usage description of [ST-04], includes the subsection Password Policy which instructs the reader to navigate to “System → Access → Servers where it is possible to change the following available settings”. It is deemed that such menu does not allow the user to change the pertinent settings, further indications are required for users to find the proper menu (OR01.NC06).

- The section 2.3 TOE usage description of [ST-04], includes information related to the “History” menu that allows users to identify changes applied to the configuration. It is not clear what the purpose of this information is as context seems to be lacking. It is required for the author to properly redact such information and provide enough context to justify its inclusion in [ST-04] and correctly define its relation with other sections of the document (OR01.NC07).
- The section 2.3 TOE usage description of [ST-04] includes information related to a “new ACL” and provides XML content for the reader to use. Such XML lines are not properly formatted and some tags are missing; therefore, making it impossible for a reader to apply the proper configuration. The author must review such information and provide the user with accurate steps and information (OR01.NC08).
- The section 2.3 TOE usage description of [ST-04], includes the subsection Access control configuration which instructs the user to execute a command in order to change the permissions associated with the core configuration file. The command is “chmod 640 ...”. In relation to this, the requirement PSC.1 indicates that, for example, the login credentials are protected according to the access control defined, mentioning that “... read/write permissions only for the root user”. This is not accurate since the permissions assigned are “640”, this means that read permissions are also given to the group associated with the file, “wheel” group. This is the “sudoers”-like group in FreeBSD systems; therefore, it is considered that users in this group are administrators and their read access to the file is not problematic but it is considered that the description of the requirement must be more accurate to properly represent the behaviour of the TOE (OR01.NC09).

The issues mentioned above were registered as non-conformities, along another minor issues registered as comments, in the Observation Report [OR01-10].

After the analysis of the Security Target, the installation and configuration of [TOE-2310] alongside the review of the provided guides [GUIDE-INSTALL-13AEB027], [GUIDE-FIRMWARE-8D335784], [GUIDE-OPERATIONAL-5486375E5], [GUIDE-FWMNGMT-3452BF16], [GUIDE-2FA-387EFC28] was performed. Such review revealed some issues regarding the guides were registered in the pertinent documental Observation Report. Following, there is a summarized description of the opened non-conformities.

- The guidance documents declared in section 2.2 Identification of the TOE secure use, installation and configuration guides are not well formatted. Some of the sections do not fit in the pages and are chopped off. Moreover, some administration functionally declared in the requirements and the pertinent operational guidance is missing from the declared guides. Moreover, the firewall management guide and 2FA configuration guide are defined with the same “Document’s name” (OR01.NC02).

The issues mentioned above were registered as non-conformities, along the issues related to the Security Target analysis, in the Observation Report [OR01-10].

Afterwards, to verify if [TOE-2310] satisfied the requirements declared in [ST-04], the functional testing was conducted. Such requirements were grouped in eight security functions; in summary, the following security functions presented non-conformities:

- SF. Identification and authentication.
 - [TOE-2310] does not terminates the session according to the Shell Inactivity time defined in the web interface (System > Administration menu). This timeout only applies to tcsh/csh/sh type shells but does not apply to the default shell assigned to users (/usr/local/sbin/opnsense-shell), which is defined in the configuration page for each user in the parameter (Login shell). Therefore, given this behaviour and that the users or administrators are not instructed documentarily to use or configure any specific type of shell, it is determined that the requirement is not complied (OR02NC01).
- SF. Cryptography and SF. Trusted communication channels.
 - [TOE-2310] offers TLSv1.0 and TLSv1.1 apart from the compliant protocol versions TLSv1.2 and TLSv1.3. TLSv1.0 and TLSv1.1 do not comply [CCN-STIC-807] ENS MEDIUM Category when establishing a connection with the remote update server "opnsense-update.deciso.com". Moreover, [TOE-2310] offers the cipher suites which are identified as Legacy and Not recommended according to [CCN-STIC-807] (OR02.NC02).
- SF. Cryptography and SF. Trusted Installation and Updates.
 - The signature scheme involved in the digital signature of the updates is RSASSA-PKCS#1 which is considered legacy by [CCN-STIC-807]. The use of such legacy mechanism is not declared in the Security Target by the manufacturer which is required by [IT-012]. The author must declare the use of all the legacy cryptographic mechanisms (OR02.NC03).
- SF. Audit.
 - [TOE-2310] does not overwrite older audit entries when the storage space for the logs reaches its limit. According to the analysis of the configuration available in the web interface and the documentation available it is not possible to configure circular logging. A similar functionality is offered which consists on preserving the logs for a determined number of days configurable through the System > Settings > Logging menu in the web interface. In any case, the results obtained are not consistent with the declaration of the requirement AUD.5 in the Security Target (OR02.NC04).
 - The description of the requirement AUD.3 states that the root user is only able to remove the audit records locally through the CLI interface. The pertinent functional test reveals that the behaviour of the TOE is not consistent with such description since it is also possible to clear the audit records through the TOE web interface in [TOE-2310] (OR02.NC05).
 - [TOE-2310] registers an event when the password of a user is changed but the audit record generated in deemed ambiguous as the type of event is not properly described. It is not possible to identify if the

password was changed or other parameter related to the user, it just indicates that the user has changed (OR02.NC06).

- [TOE-2310] registers the declared events in the logs, but some inconsistencies have been identified according to the declared information in the Security Target. The audit entries for the following events are considered to be generic, not allowing users to properly distinguish between the type of event as most of them are registered with the same entry: Session termination timeout, Deletion of groups, Change permissions of users/groups, GUI Certificate change, SSH configuration change, Creation, modification and deletion of firewall rules, Change in order of firewall rules (OR02.NC07).

After completing the functional testing, it was proceeded to perform the analysis of the product vulnerabilities. Subsequently, the penetration tests were carried out in order to vulnerate and find flaws in the capabilities and functionalities of the product. The penetration tests revealed the following issues:

- Given the publicly documented CVE-2023-39005, the configd.socket related to the configd service was examined. It is determined that a low privileged user with local access to [TOE-2310] is able to issue commands (e.g.: auth add user test1) through configd.socket since the permissions assigned to such socket file are lax, allow read and write permissions for everyone. Among other administrator declared functionality, the non-authorized user is able to create new users (OR02.NC06).
- Given the publicly documented CVE-2023-39003, the usage of /tmp was examined. It is determined that a low privileged user with local access to [TOE-2310] is able to create symbolic links to restricted files and view its contents through the web interface in the crash reporter menu (for example, creating the symbolic link /tmp/PHP_errors.log that points to /conf/config.xml). This is possible because the symbolic link is interpreted as a PHP error file that is directly loaded in the crash reported menu as part of a diagnostic functionality, allowing the low privileged to read non-authorized files (OR02.NC07).
- A stored cross site scripting vulnerability was identified in wizard.php through the “language” POST parameter used in the System: Wizard: General Information step of the wizard in System > Wizard menu. The user-controlled input is sanitized using the PHP function addslashes inside the “update_config_field” function defined in wizard.php but such measure is not enough to prevent XSS payloads; validation of such parameter is therefore deemed insufficient (OR02.NC08).

The following comments were also registered:

- It is determined that some services and processes hosted in [TOE-2310] are running with root privileges (e.g.: php-cgi or ntpd). This finding could be conflictive in case a hypothetical vulnerability in such processes is exploited since it would provide the attacker with root privileges. It is advised to the

manufacturer that the permissions for such services are segregated and that they are only run using the minimum-required privileges in order to mitigate the consequences of vulnerabilities affecting the processes (OR02.CO01).

The non-conformities and comments registered during the execution of the functional and penetration testing were collected in the Observation Report [OR02-10]. Both observation reports, [OR01-10] and [OR02-10] were handed to the manufacturer in order to communicate the issues that required to be solved.

After the manufacturer reviewed the non-conformities, new evidences were provided in order to suffice the non-conformities identified. These are [ST-07], [TOE-23102] and [OPNSENSE-DOCS-D971B9D].

The analysis of [ST-07] did not reveal any additional non-conformities. Also, the new guidance evidence, [OPNSENSE-DOCS-D971B9D], was reviewed. These evidences are deemed to solve the non-conformities registered in [OR01-10]. Given this, all the non-conformities from such Observation Report were closed and [OR01-20] was generated.

[TOE-2310] was updated to [TOE-23102] following the update procedure included in the Security Target [ST-07]. Other installation and configuration instructions defined by the manufacturer in the Security Target were followed, as documented in section 6.3 *Description of the installation and configuration of the TOE*, the deployment of the new version of the TOE did not reveal any additional non-conformities.

After updating the TOE, functional tests related to non-conformities were repeated to determine if the issues were solved according to [ST-07].

After completing the functional testing, the vulnerability analysis was reviewed in case it needed refinement or addition of new vulnerabilities. Since the listing of the third-party libraries was updated, the analysis of CVEs was updated and documented in the pertinent section of the present report.

Considering the same philosophy followed for the functional tests, only the penetration tests with a non-conformity associated were repeated ([LINCE_OPNSENSE_BE-PT-0001], [LINCE_OPNSENSE_BE-PT-0003] and [LINCE_OPNSENSE_BE-PT-1101]).

The execution of the functional and penetration related to non-conformities revealed that the non-conformities from [OR02-10] were solved according to [ST-07] and the updated version of the TOE [TOE-23102]. Given this, all the non-conformities from such Observation Report were closed and [OR02-20] was generated.

Due to the TOE not having any open non-conformities, the evaluation result is **PASS**.

5 VERDICT OF THE EVALUATION

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

The Security Target assessment does not reveal any non-conformity.

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

The documentation analysis does not reveal any non-conformity.

The functional tests do not reveal any non-conformity.

The vulnerability analysis does not reveal any non-conformity.

The penetration tests do not reveal any non-conformity.

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

Documents used during installation	[OPNSENSE-DOCS-D971B9D] [ST-07]
Evaluator	DAT
Days required	3 days.
Date	2024/06/21
Results of the evaluator's work	PASS

6.1 EVALUATION ACTIVITIES

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

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

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

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

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

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

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

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

PASS The evaluator has been able to install the product exclusively following the contents of the manufacturer's documentation, provided through [ST-07] 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 declared in the Security Target [ST-07] as can be seen in 6.4 Verification of the installed TOE version. The manufacturer provides guidelines in the description of the ACT.1 requirement.

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 section 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

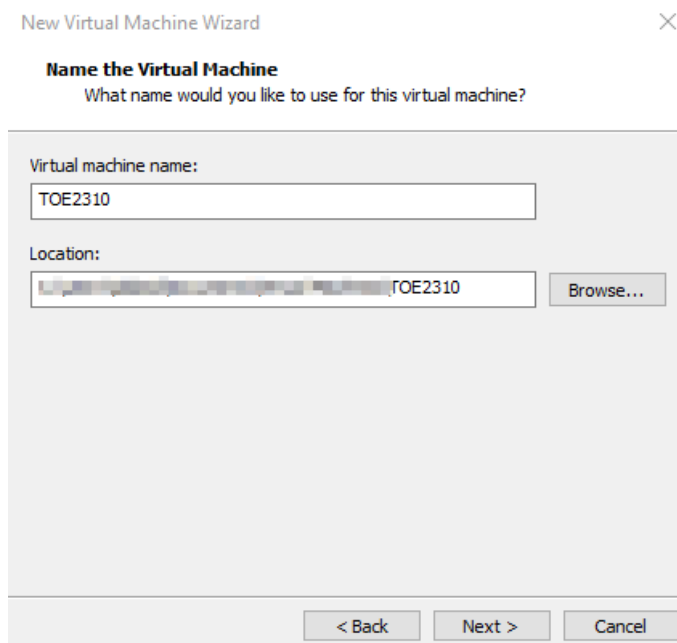
The test scenarios are described in section 12 Annex A: Test scenarios.

6.3 DESCRIPTION OF THE INSTALLATION AND CONFIGURATION OF THE TOE

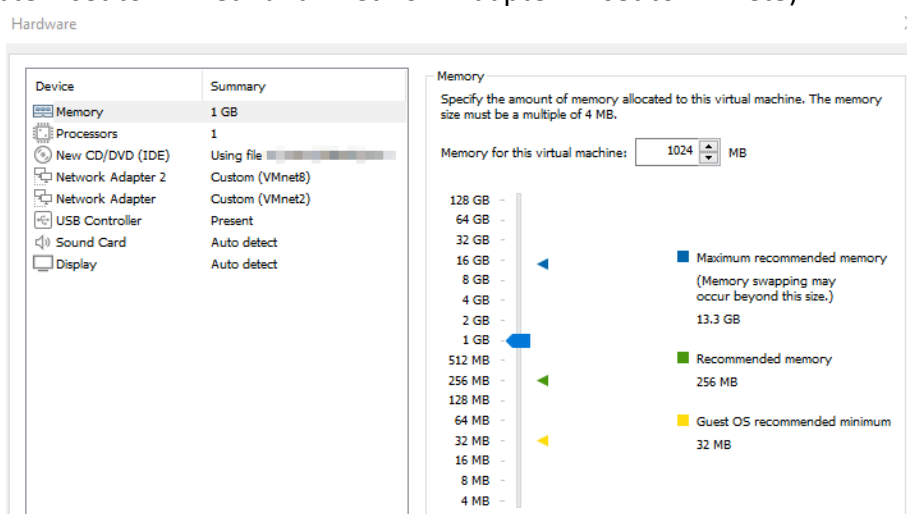
6.3.1 OPNSENSE INSTALLATION

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

1. Open VMware and click on Create a new virtual machine.
2. Select [TOE-ISO-2310] 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”.

```
*** OPNsense.localdomain: OPNsense 23.10 ***

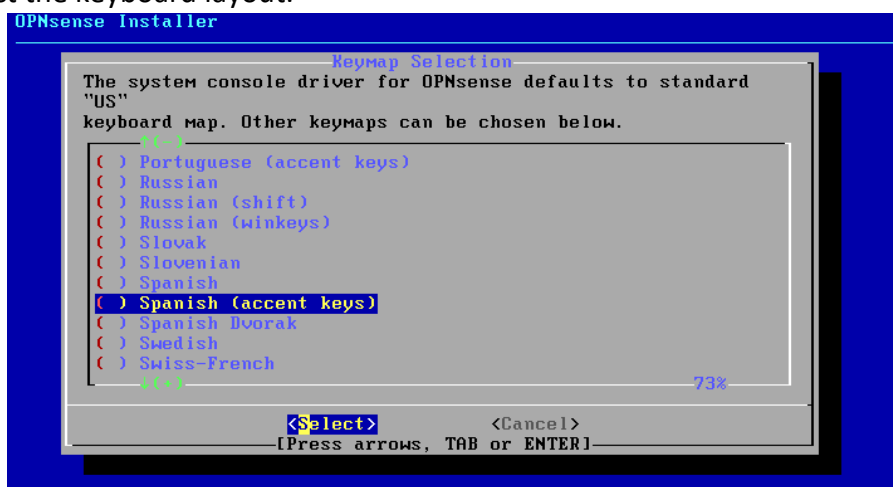
LAN (em0)      -> v4: 192.168.1.1/24
WAN (em1)      -> v4/DHCP4: 192.168.74.150/24

HTTPS: SHA256 E4 19 F7 F5 1A CC 6C 93 E5 AC F2 F7 94 7C AF 58
        61 BA A4 F9 99 9B 53 F5 AD 2E B8 D0 BA 61 14 ED
SSH:   SHA256 UJ0krxBYMip5lG0ga6+JXqXNnhB7glreRmcPej+fGvE (ECDSA)
SSH:   SHA256 vu2YnvkbbMYbn8lC9Ze4/XWB6W1U680f0d/7/o5fK7o (ED25519)
SSH:   SHA256 A42XDcvaJU5UkIY9p0DtVFD6UaF3db5ewD5PcUzQm8Y (RSA)

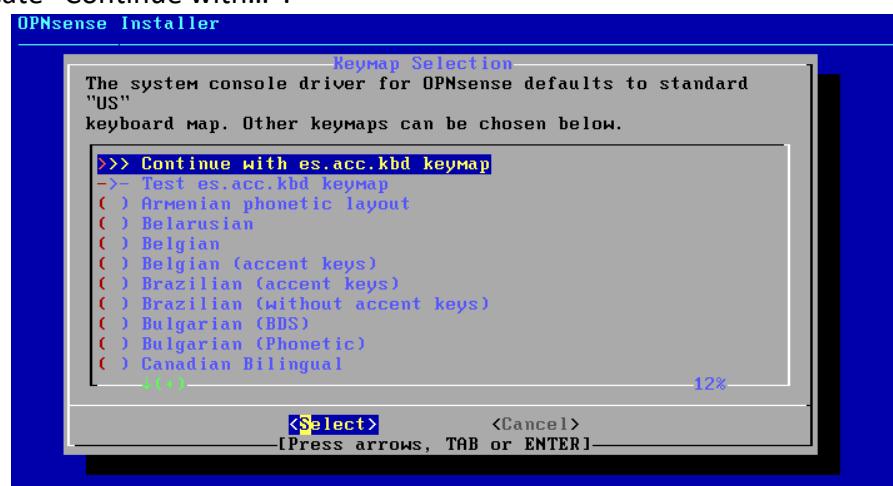
Welcome! OPNsense is running in live mode from install media. Please
login as 'root' to continue in live mode, or as 'installer' to start the
installation. Use the default or previously-imported root password for
both accounts. Remote login via SSH is also enabled.

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: 
```

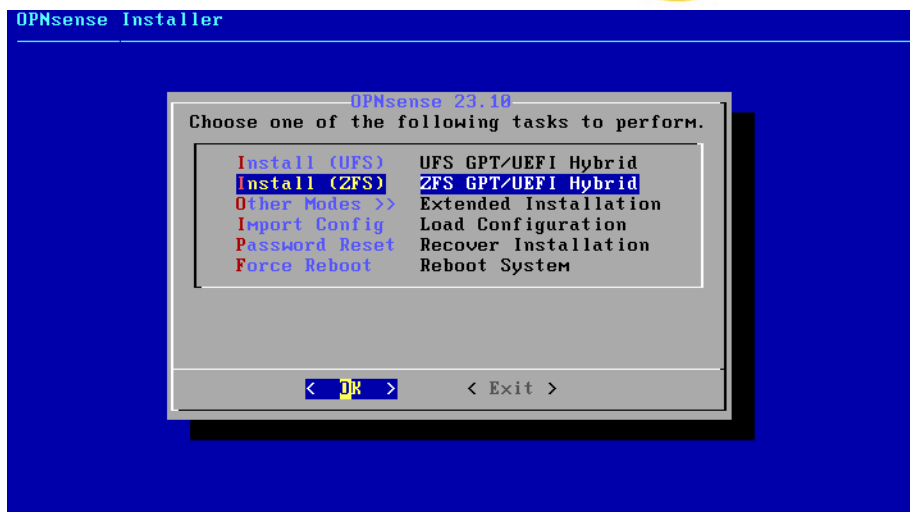
10. Select the keyboard layout.



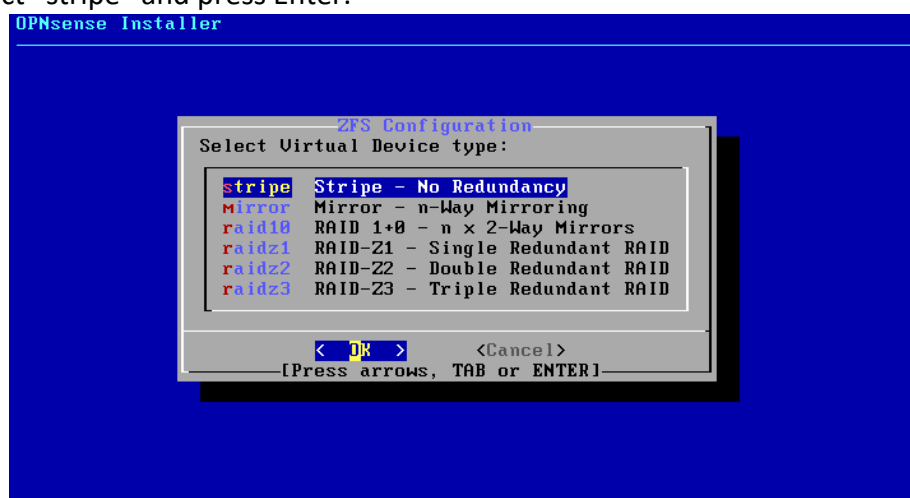
11. Indicate “Continue with...”.



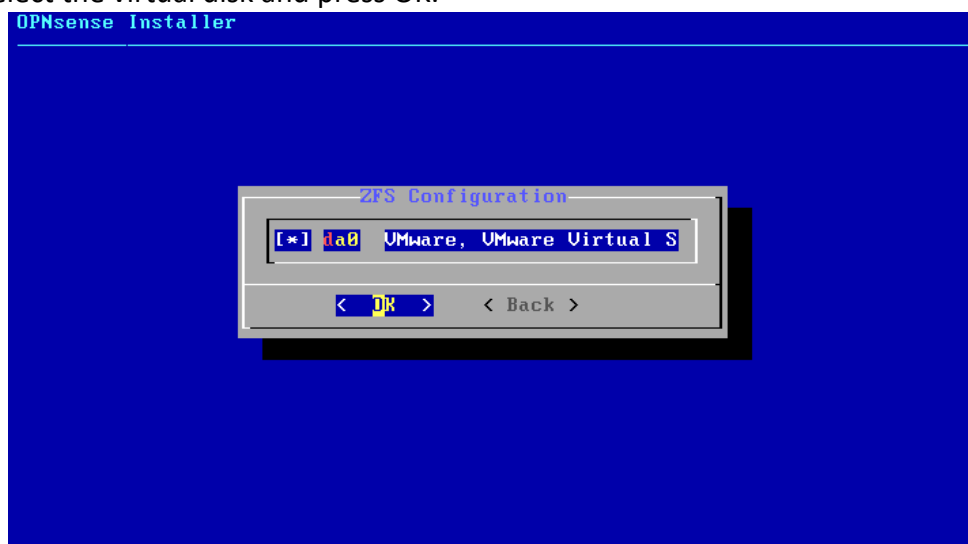
12. Select “Install (ZFS)” and press Enter.



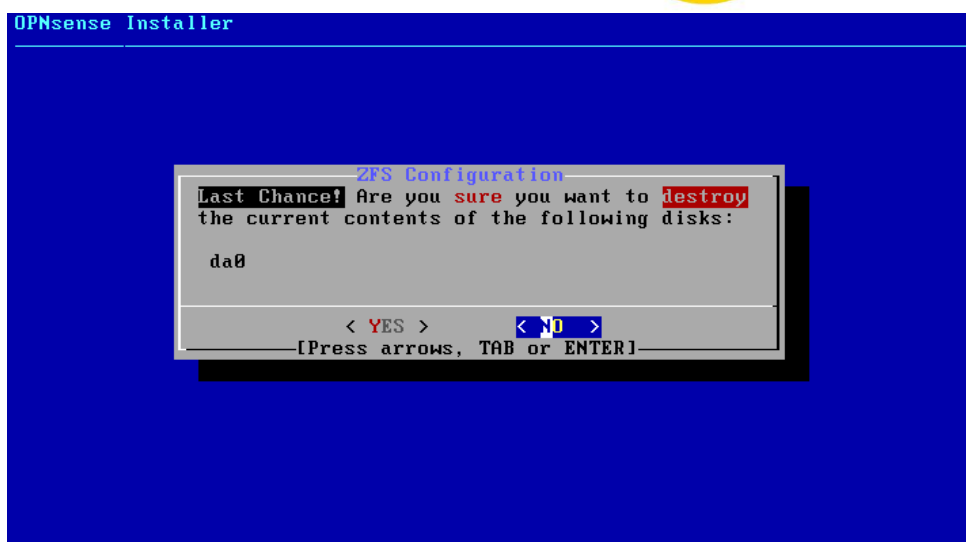
13. Select “stripe” and press Enter.



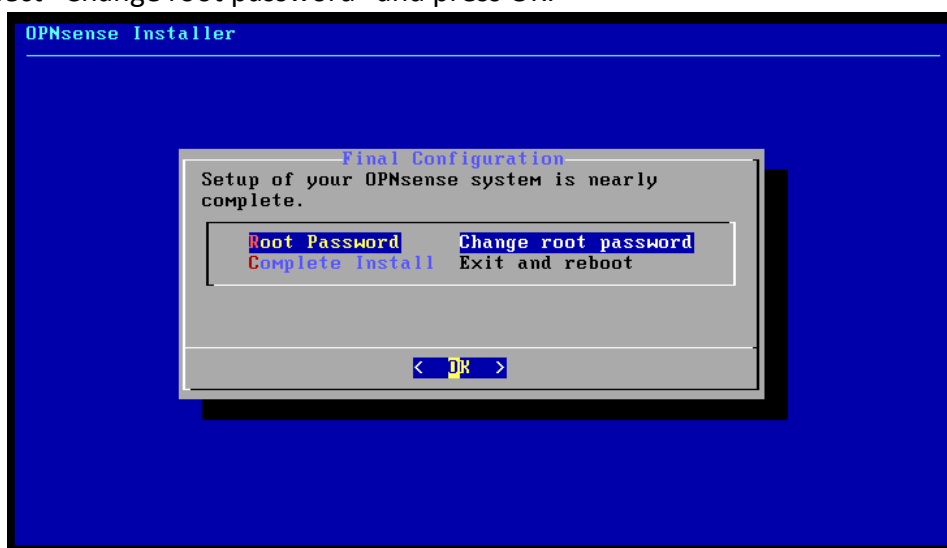
14. Select the virtual disk and press OK.



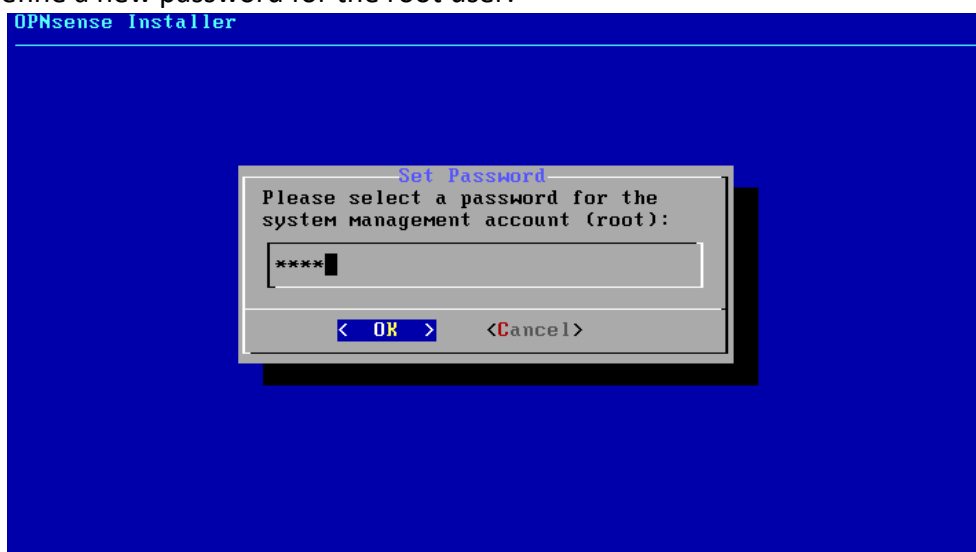
15. Select Yes and press Enter.



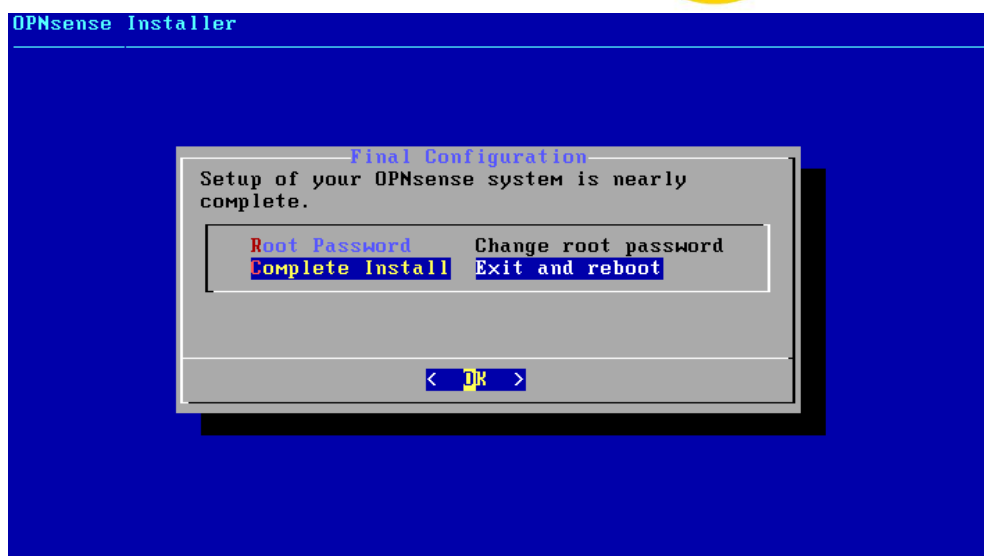
16. Select "Change root password" and press OK.



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.

```
The installation finished successfully.

After reboot, open a web browser and navigate to
https://192.168.1.1 (or the LAN IP address). The console
can also be used to set a different LAN IP.

Your browser may report the HTTPS certificate as untrusted
and ask you to accept it. This is normal, as the default
certificate will be self-signed and cannot be validated by
an external root authority.

Rebooting in 5 seconds. CTRL-C to abort...█
```

```
*** OPNsense.localdomain: OPNsense 23.10 ***

LAN (em0)      -> v4: 192.168.1.1/24
WAN (em1)      -> v4/DHCP4: 192.168.74.150/24

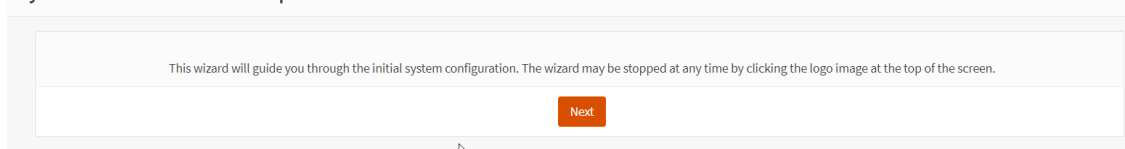
HTTPS: SHA256 E4 19 F7 F5 1A CC 6C 93 E5 AC F2 F7 94 7C AF 58
              61 BA A4 F9 99 9B 53 F5 AD 2E B8 D0 BA 61 14 ED

FreeBSD/amd64 (OPNsense.localdomain) (ttyv0)
login: █
```

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.

System: Wizard: General Setup



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

System: Wizard: General Information

General Information

Hostname: OPNsense

Domain: localdomain

Language: English

Primary DNS Server:

Secondary DNS Server:

Override DNS: ☒ Allow DNS servers to be overridden by DHCP/PPP on WAN

Unbound DNS

Enable Resolver: ☒

Enable DNSSEC Support: ☐

Harden DNSSEC data: ☐

Next

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

System: Wizard: Time Server Information

Time server hostname: 0.opnsense.pool.ntp.org 1.opnsense.pool.ntp.org 2. ...

Enter the hostname (FQDN) of the time server.

Timezone: Europe/Madrid

Next

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

System: Wizard: Configure WAN Interface

IPv4 Configuration Type:	DHCP
--------------------------	------

General configuration

MAC Address:	<input type="text"/>
--------------	----------------------

This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections). Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU:	<input type="text"/>
------	----------------------

Set the MTU of the WAN interface. If you leave this field blank, an MTU of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed.

MSS:	<input type="text"/>
------	----------------------

If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect. If you leave this field blank, an MSS of 1492 bytes for PPPoE and 1500 bytes for all other connection types will be assumed. This should match the above MTU value in most all cases.

RFC1918 Networks

Block RFC1918 Private Networks:	<input checked="" type="checkbox"/> Block private networks from entering via WAN
---------------------------------	--

When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8) and Carrier-grade NAT addresses (100.64/10). This option should only be set for WAN interfaces that use the public IP address space.

Block bogon networks

Block bogon networks:	<input checked="" type="checkbox"/> Block non-Internet routed networks from entering via WAN
-----------------------	--

When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA.

Next

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

System: Wizard: Configure LAN Interface

LAN IP Address:	192.168.1.1
-----------------	-------------

(leave empty for none)

Subnet Mask:	24
--------------	----

Next

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

System: Wizard: Set Root Password

Root Password:

(leave empty to keep current one)

Root Password Confirmation:

Next

27. Click on reload to apply the changes.

System: Wizard: Reload Configuration

Click 'Reload' to apply the changes.

Reload

28. The TOE is now configured and ready.

Finished initial configuration!



Congratulations! OPNsense is now configured.

Please consider donating to the project to help us with our overhead costs. See [our website](#) to donate services.

Click to [continue to the dashboard](#). Or click to [check for updates](#).

6.3.2 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.

System: Firmware

Status
Settings
Changelog
Updates
Plugins
Packages

☐ advanced mode

i Mirror
Deciso (HTTPS, NL, Commercial)

i Type
Business

i Subscription

i Usage
In order to apply these settings a firmware update must be performed after save, which

Save
Cancel

6.3.3 UPDATING TO 23.10.2 VERSION

In [ST-07], it is indicated that it is required to update to the TOE version 23.10.2, which is the version declared in that Security Target. 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 “23.10/MINT/23.10.2/latest” in the Flavour parameter and click Save.

System: Firmware

Status
Settings
Changelog
Updates
Plugins
Packages

☒ advanced mode

i Mirror
Deciso (HTTPS, NL, Commercial)

i Flavour
(custom)

/23.10/MINT/23.10.2/latest

i Type
Business

i Subscription

i Usage
In order to apply these settings a firmware update must be performed afi

Save
Cancel

5. Go to the Status tab and click Check for updates.
6. Click Update.

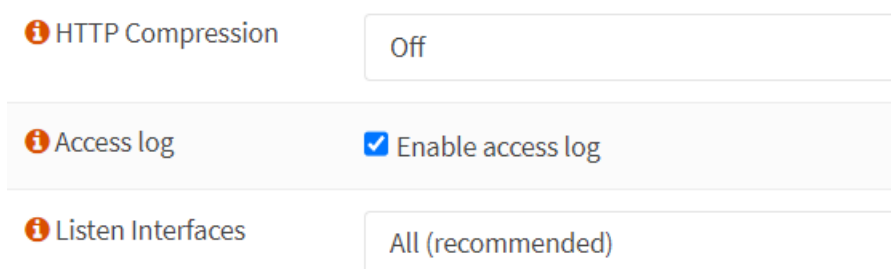
There are 97 updates available, total download size is 235.5MiB.

7. Wait for the update to be installed.

6.3.4 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”.

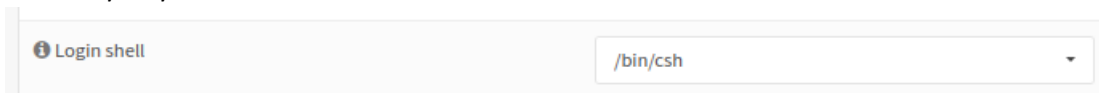


HTTP Compression	Off
Access log	<input checked="" type="checkbox"/> Enable access log
Listen Interfaces	All (recommended)

6.3.5 CHANGE SHELL TYPE AND INACTIVITY TIMEOUT

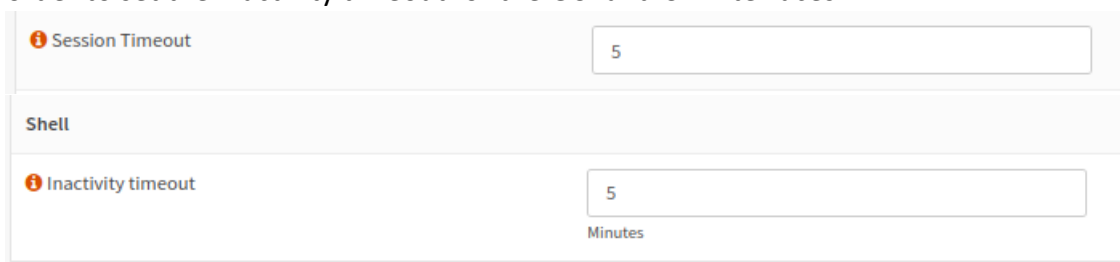
For the inactivity session timeout to work, it is required to change the login shell assigned to the user as indicated in the Security Target. The Security Target also indicates to change the session/inactivity timeout to 5 minutes. The steps below are followed:

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.



Login shell	/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.



Session Timeout	5
Shell	
Inactivity timeout	5
	Minutes

6.3.6 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
```

```
root@OPNsense:~ # ls -la /conf/config.xml
-rw-r----- 1 root wheel 62805 Apr 22 11:54 /conf/config.xml
```

6.3.7 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.

System: Access: Servers

Server Name	Type	Host Name	
Local Database	Local Database	OPNsense	

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

System: Access: Servers

 Descriptive name	Local Database
 Type	Local Database
 Policy	<input checked="" type="checkbox"/> Enable password policy constraints
 Duration	Disable
 Length	12
 Complexity	<input checked="" type="checkbox"/> Enable complexity requirements
<input type="button" value="Save"/>	

5. Save the changes.

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

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.

<input type="checkbox"/>	GUI	read only logs	/ui/diagnostics/log/core/configd /api/diagnostics/log/core/configd /api/diagnostics/log/core/configd/export* /ui/diagnostics/log/core/audit /api/diagnostics/log/core/audit /api/diagnostics/log/core/audit/export* /ui/diagnostics/log/core/boot /api/diagnostics/log/core/boot /api/diagnostics/log/core/boot/export* /ui/diagnostics/log/core/system /api/diagnostics/log/core/system /api/diagnostics/log/core/system/export* /ui/diagnostics/log/core/lighttpd /api/diagnostics/log/core/lighttpd /api/diagnostics/log/core/lighttpd/export* /ui/diagnostics/log/core/firewall /api/diagnostics/log/core/firewall /api/diagnostics/log/core/firewall/export* /ui/diagnostics/firewall/log
--------------------------	-----	----------------	--

6.3.9 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".

Root Login ☐ Permit root user login

6.3.10 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.

System: Configuration: Backups

Backup Count

Enter the number of older configurations to keep in the local backup cache.

Be aware of how much space is consumed by backups before adjusting this v

6.3.11 CONFIGURE TWO-FACTOR AUTHENTICATION

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

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

System: Access: Servers

Descriptive name

Type

Token length

Time window

Grace period

Reverse token order ☐

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

OTP seed

☒ Generate new secret (160 bit)

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

OTP seed

☐ Generate new secret (160 bit)

OTP QR code

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>".

System: Access: Tester

User: root authenticated successfully.
This user is a member of these groups:
admins

Authentication Server: 2FA

Username: root

Password:

Test

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

Authentication

Server: 2FA

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.

6.3.12 CONFIGURING CONFIGD ACCESS CONTROL

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

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

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

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

```
[action_defaults]  
allowed_groups = wheel
```

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

```
service configd restart
```

6.3.13 WEB 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
```

System: Settings: Administration

Web GUI

Protocol ☐ HTTP ☒ HTTPS

SSL Certificate Web GUI TLS certificate ▼

SSL Ciphers TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS ▼

4. Scroll down and click Save.

6.3.14 SSH CRYPTOGRAPHIC PARAMETERS CONFIGURATION

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

1. Log in through the TOE web interface with the root user.
2. Navigate to System → Settings → Administration.
3. In the Secure Shell section, use the dropdown menu for “Key exchange algorithms”, “Ciphers”, “MACs” and “Public key signature algorithms” to select valid cryptographic parameters.
 - a. Key exchange algorithms:
 - i. diffie-hellman-group16-sha512
 - ii. diffie-hellman-group18-sha512
 - iii. ecdh-sha2-nistp256
 - iv. ecdh-sha2-nistp384
 - v. ecdh-sha2-nistp521
 - b. Ciphers:
 - i. aes128-ctr
 - ii. aes192-ctr
 - iii. aes256-ctr
 - c. MACs:
 - i. hmac-sha2-256
 - ii. hmac-sha2-512
 - d. Public key signature algorithms:
 - i. ecdsa-sha2-nistp256
2. Scroll down and click Save.

6.3.15 SYSLOG CLIENT TLS CIPHER SUITES CONFIGURATION

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

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

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

2. Edit the file `/usr/local/opnsense/service/templates/OPNsense/Syslog/syslog-ng-destinations.conf`

3. In the network parameters, inside the TLS parameters, add the following lines:
`ssl-options(no-sslv2, no-sslv3, no-tls1, no-tls11)`
`cipher-suite("ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES128-CCM")`

```
{% if destination.transport in ['tls4', 'tls6'] %}
  tls(
    ca-file("/etc/ssl/cert.pem")
    key-file("/usr/local/etc/syslog-ng/cert.d/{{dest_key}}.key")
    cert-file("/usr/local/etc/syslog-ng/cert.d/{{dest_key}}.crt")
    ssl-options(no-sslv2, no-sslv3, no-tls1, no-tls11)
    cipher-suite("ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES128-GCM-SHA256:TLS_AES_128_GCM_SHA256:TLS_AES_128_GCM_SHA256:TLS_CHACHA20_POLY1305_SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-CCM:ECDHE-ECDSA-AES128-CCM")
  )
{% endif %}
);
{% endif %}
};
```

4. Save the file.

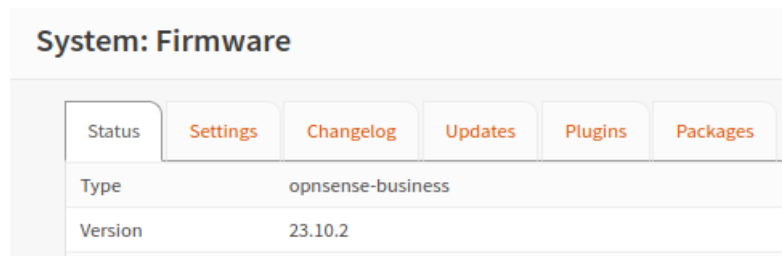
6.3.16 INSTALLING CERTIFICATES FROM TRUSTWORTHY CA

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-23102] itself is used in this evaluation, as it does not imply a degradation in the quality level at the functionality or testing of [TOE-23102]. This matter is taken into account by the evaluator when conducting the testing.

6.4 VERIFICATION OF THE INSTALLED TOE VERSION

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

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



6.5 USED INSTALLATION OPTIONS

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

6.6 RESULTS

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

ID	Comments	State
N/A	None.	N/A

7 CONFORMITY ASSESSMENT

7.1 SECURITY TARGET ASSESSMENT

Security Target identifier	[ST-07]
Evaluator	DAT
Days required	1 day.
Date	2024/06/21
Results of the evaluator's work	PASS

7.1.1 EVALUATION ACTIVITIES

This section contains the Evaluation activities defined in section 4.1 of [CCN-STIC-2002] as well as a brief description of the result of these tasks on [ST-07].

TE.1.1 The evaluator shall check that the Security Target includes all the elements described in chapter 3.1 of [CCN-STIC-2002] and in [CCN-STIC-2003].

PASS [ST-07] contains all the elements described in chapter 3.1 of [CCN-STIC-2002] and in [CCN-STIC-2003].

TE.1.2. Verify that the TOE can be uniquely identified.

PASS The TOE can be uniquely identified.

TE.1.3. Check that the Security Target strictly complies with all the Security Function Requirements of the declared product taxonomy.

PASS [ST-07] does not claim conformance to any product taxonomy; therefore, this task does not apply.

TE.1.4. Check that unique identification of operating guides or safe use procedures and configuration/installation guides is provided.

PASS [ST-07] provides sufficient information to allow the unique identification of the document [OPNSENSE-DOCS-D971B9D].

TE.1.5. The evaluator shall check that the description of the TOE is not misleading and that it describes at least the minimum security functionality in the TOE scope.

PASS The description of the TOE given in [ST-07] is clear and includes information about the functionality for which the TOE is designed.

TE.1.6. The evaluator shall check the existence of a correct delimitation of the parts that comprise the TOE and that those parts belonging to the operational environment, as well as an adequate description of how the operational environment supports the TOE's operation.

PASS The parts of the product that correspond to the TOE are clearly delimited from those that are part of the operational environment. In addition, a description of the operational environment is included.

TE.1.7. The evaluator shall check that the security functions and mechanisms mitigate or counter the threats described in the Security Target.

PASS The security features declared in [ST-07] mitigate all the threats described in the same document.

TE.1.8. The evaluator shall check that each one of the security functions or mechanisms are fully traced to threats included in the Security Target.

PASS All the security features described in [ST-07] mitigate at least one of the declared threats.

TE.1.9. The evaluator shall check that the assumptions of the operational environment are relevant in regards to the declared threats and the expected TOE use.

PASS The environmental hypotheses correspond to those established by the taxonomies considered and are relevant to the threats and the objective of the product.

TE.1.10. Check that the security functions are described to the level of detail necessary to enable the assessor to understand how the security functions are implemented by the TOE. The specification of the security functions should demonstrate how each of the functions counteracts or mitigates the stated threats.

PASS The security functions are described in sufficient detail so that the evaluator can carry out the tests for each of them. In addition, it shows how the stated threats are mitigated.

TE.1.11. Check that third-party libraries that implement security functionality are identified.

PASS Third-party libraries that implement security functionalities are correctly identified in section 8.1 *Third party libraries used by the TOE* from [ST-07].

TE.1.12. In case of declaring the optional modules (MCF), (MEC) or (MEB), the evaluator shall check that the functionalities that will be verified as part of the evaluation with these optional modules are detailed.

PASS N/A

TE.1.13. The evaluator shall register every non-conformity in relation to the Security Target.

PASS Information concerning this task of the evaluator can be found in the section 7.1.2 *Results*.

7.1.2 RESULTS

ID	Non-conformity	State
OR01.NC01	<p>[ST-04] includes some inconsistencies when referring to the TLS protocol version related to the TOE web interface. In section 2.1 TOE Functional description, “over TLSv1.3” is mentioned, while in other sections such as the description of the requirement COM.4, “TLSv1.2 or higher” is defined. This is considered contradictory and confusing.</p> <p>The manufacturer provides Security Target [ST-07]. This evidence fixes the non-conformity identified in previous version provided since the confusing information is amended by the author.</p>	CLOSED
OR01.NC02	<p>The guidance documents declared in section 2.2 Identification of the TOE secure use, installation and configuration guides are not well formatted. Some of the sections do not fit in the pages and are chopped off. Moreover, some administration functionally declared in the requirements and the pertinent operational guidance is missing from the declared guides. Moreover, the firewall management guide and 2FA configuration guide are defined with the same “Document’s name”.</p> <p>The manufacturer provides Security Target [ST-07] and [OPNSENSE-DOCS-D971B9D]. These evidences fix the non-conformity identified in previous version provided since the confusing information since a new guidance document that is considered complete ([OPNSENSE-DOCS-D971B9D]) and proper is delivered. Moreover, references to the guidance documents in section 2.2 of [ST-07] are now accurate, previous guides are dismissed.</p>	CLOSED
OR01.NC03	<p>According to the documentation of the TOE, there are several different options in relation to what image to choose for installation. Four types of installation are defined: “dvd”, “vga”, “serial”, “nano”. It is considered that the installation method is not well identified or indicated to the user in [ST-04]; therefore, the installation procedure included is not properly defined.</p> <p>The manufacturer provides Security Target [ST-07]. This evidence fixes the non-conformity identified in previous version provided since the author now states which image is chosen for installation.</p>	CLOSED

OR01.NC04	<p>The section 2.3 TOE usage description of [ST-04], includes the subsection OPNsense Business Edition installer which includes some steps with the purpose to defined the installation procedure of the TOE. The steps are poorly documented and most of the steps are missing. It is required for the author to properly defined the installation procedure with the complete steps.</p> <p>The manufacturer provides Security Target [ST-07]. This evidence fixes the non-conformity identified in previous version provided since a complete and properly documented installation procedure is provided by the author.</p>	CLOSED
OR01.NC05	<p>The section 2.3 TOE usage description of [ST-04], includes the subsection CLI interface idle timeout configuration which indicates the reader to navigate to the “System → Settings → Administration” in order to change the Login shell of a user. These instructions are deemed incorrect, it is not possible to change the Login shell parameter in such menu, this parameter is associated with each user uniquely and it is changed in the profile of each user. In the same paragraph, the author states that the default session timeout for the GUI interface is 5 minutes. This is wrong, the default time is 4 hours. Instructions to change such timeout seem to be missing.</p> <p>The manufacturer provides Security Target [ST-07]. This evidence fixes the non-conformity identified in previous version provided since the instructions related to the session timeout configuration is now deemed correct.</p>	CLOSED
OR01.NC06	<p>The section 2.3 TOE usage description of [ST-04], includes the subsection Password Policy which instructs the reader to navigate to “System → Access → Servers where it is possible to change the following available settings”. It is deemed that such menu does not allow the user to change the pertinent settings, further indications are required for users to find the proper menu.</p> <p>The manufacturer provides Security Target [ST-07]. This evidence fixes the non-conformity identified in previous version provided since the instructions related to the configuration of the password complexity policy is now deemed correct.</p>	CLOSED
OR01.NC07	<p>The section 2.3 TOE usage description of [ST-04], includes information related to the “History” menu that allows users</p>	CLOSED

	<p>to identify changes applied to the configuration. It is not clear what the purpose of this information is as context seems to be lacking. It is required for the author to properly redact such information and provide enough context to justify its inclusion in [ST-04] and correctly define its relation with other sections of the document.</p> <p>The manufacturer provides Security Target [ST-07]. This evidence fixes the non-conformity identified in previous version provided since the author now provides further context in relation to the “History” menu and what its purpose is in order for the TOE to meet the audit requirements.</p>	
OR01.NC08	<p>The section 2.3 TOE usage description of [ST-04] includes information related to a “new ACL” and provides XML content for the reader to use. Such XML lines are not properly formatted and some tags are missing; therefore, making it impossible for a reader to apply the proper configuration. The author must review such information and provide the user with accurate steps and information.</p> <p>The manufacturer provides Security Target [ST-07]. This evidence fixes the non-conformity identified in previous version provided since the author has amended the XML content included in the 2.3 TOE usage description section and it is now well structured and formatted.</p>	CLOSED
OR01.NC09	<p>The section 2.3 TOE usage description of [ST-04], includes the subsection Access control configuration which instructs the user to execute a command in order to change the permissions associated with the core configuration file. The command is “chmod 640 ...”. In relation to this, the requirement PSC.1 indicates that, for example, the login credentials are protected according to the access control defined, mentioning that “... read/write permissions only for the root user”. This is not accurate since the permissions assigned are “640”, this means that read permissions are also given to the group associated with the file, “wheel” group. This is the “sudoers”-like group in FreeBSD systems; therefore, it is considered that users in this group are administrators and their read access to the file is not problematic but it is considered that the description of the requirement must be more accurate to properly represent the behaviour of the TOE.</p>	CLOSED

	The manufacturer provides Security Target [ST-07]. This evidence fixes the non-conformity identified in previous version provided since the configuration indicated is now consistent with the description of the requirement.	
--	--	--

ID	Comments	State
N/A	None.	N/A

7.2 FUNCTIONAL TESTS

Evaluator	DAT
Days required	5 days.
Date	2024/06/21
Results of the evaluator's work	PASS

7.2.1 EVALUATION ACTIVITIES

The information presented in this section covers the result of carrying out the evaluation activities specified in section 4.3 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 7.2.2 *List of functional tests*. This information is presented in more detail in the section 13 *Annex B: Functional test plan and report*.

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

PASS Information concerning this task of the evaluator can be found in the section 7.2.3 *Results*.

7.2.2 LIST OF FUNCTIONAL TESTS

Security function	Test code	Objective	Result
SF. Trusted administration ADM.1	[LINCE_OPNSENSE_BE-TST-1000]	Verify that the TOE defines the default root user, provides the ability to create new users/groups and allows modifying the privileges of a given user or group.	PASS
SF. Trusted administration ADM.2	[LINCE_OPNSENSE_BE-TST-1100]	Verify that the TOE allows to remotely configure the session termination timeout.	PASS
SF. Trusted administration ADM.2	[LINCE_OPNSENSE_BE-TST-1101]	Verify that the TOE allows to remotely create, modify, delete users and groups and	PASS

		associate permissions with users and groups.	
SF. Trusted administration ADM.2	[LINCE_OPNSENSE_BE-TST-1102]	Verify that the TOE allows to remotely load a certificate for the TOE web interface.	PASS
SF. Trusted administration ADM.2	[LINCE_OPNSENSE_BE-TST-1103]	Verify that the TOE allows to remotely define the declared configuration parameters related to SSH service and its access.	PASS
SF. Trusted administration ADM.3 SF. Firewall FWL.2	[LINCE_OPNSENSE_BE-TST-1200]	Verify that the TOE only allows entities according to the declared access control policy to perform the declared management functionality.	PASS
SF. Identification and authentication IAU.1	[LINCE_OPNSENSE_BE-TST-2000]	Verify that the TOE identifies and authenticate users through a username and password before granting access through the GUI and CLI interfaces.	PASS
SF. Identification and authentication IAU.2	[LINCE_OPNSENSE_BE-TST-2100]	Verify that the TOE implements protection mechanisms against user authentication brute-force attacks as declared for the web interface.	PASS
SF. Identification and authentication IAU.2	[LINCE_OPNSENSE_BE-TST-2101]	Verify that the TOE implements protection mechanisms against user authentication brute-force attacks as declared for the SSH interface.	PASS
SF. Identification and authentication IAU.3	[LINCE_OPNSENSE_BE-TST-2200]	Verify that the TOE allows to configure passwords with a minimum or equal length of 12 characters and that the passwords can be composed of three of the following four sets of characters: lowercase letters, uppercase letters, numbers and the declared special characters.	PASS
SF. Identification and authentication	[LINCE_OPNSENSE_BE-TST-2300]	Verify that the TOE terminates the user session after the declared inactivity time window.	PASS

IAU.4			
SF. Trusted communication channels COM.1, COM.2 SF. Cryptography CIF.1 SF. Audit AUD.4	[LINCE_OPNSENSE_BE-TST-3000]	Verify that the TOE supports TLSv1.2 and TLSv1.3 with the declared cipher suites in compliance with [CCN-STIC-807] when exchanging information with the audit server.	PASS
SF. Trusted communication channels COM.1, COM.2 SF. Cryptography CIF.1	[LINCE_OPNSENSE_BE-TST-3001]	Verify that the TOE supports TLSv1.3 with the declared cipher suites in compliance with [CCN-STIC-807] when exchanging information with the update repository.	PASS
SF. Trusted communication channels COM.1, COM.2 SF. Cryptography CIF.1	[LINCE_OPNSENSE_BE-TST-3100]	Verify that the TOE web interface supports TLSv1.2 and TLSv1.3 with the declared cipher suites in compliance with [CCN-STIC-807] when exchanging information with the remote administrator.	PASS
SF. Trusted communication channels COM.4 SF. Cryptography CIF.1	[LINCE_OPNSENSE_BE-TST-3101]	Verify that the TOE SSH interface supports SSHv2 with the declared cryptographic mechanisms in compliance with [CCN-STIC-807] when exchanging information with the remote administrator.	PASS
SF. Trusted installation and updates ACT.1	[LINCE_OPNSENSE_BE-TST-5000]	Verify if the TOE allows to query the current version.	PASS
SF. Trusted installation and updates ACT.1	[LINCE_OPNSENSE_BE-TST-5001]	Verify if the TOE allows to check if there are any updates available.	PASS
SF. Trusted installation and updates ACT.1 SF. Trusted Administration ADM.2	[LINCE_OPNSENSE_BE-TST-5002]	Verify if the TOE allows initiate the installation of updates.	PASS

SF. Trusted installation and updates ACT.2 SF. Cryptography CIF.1	[LINCE_OPNSENSE_BE-TST-5100]	Verify if the TOE updates are digitally signed using the declared mechanisms.	PASS
SF. Trusted installation and updates ACT.2 SF. Cryptography CIF.1	[LINCE_OPNSENSE_BE-TST-5101]	Verify if the TOE authenticates the software updates before installing them.	PASS
SF. Trusted installation and updates ACT.3	[LINCE_OPNSENSE_BE-TST-5200]	Verify that the TOE only allows the declared users to perform software updates.	PASS
SF. Audit AUD.1, AUD.2	[LINCE_OPNSENSE_BE-TST-6001]	Verify that the TOE generates audit records related to the login and logout of users and that these are described with date and time, type of event, result of the event and user producing the event.	PASS
SF. Audit AUD.1, AUD.2	[LINCE_OPNSENSE_BE-TST-6002]	Verify that the TOE generates audit records related changes in user credentials and that these are described with date and time, type of event, result of the event and user producing the event.	PASS
SF. Audit AUD.1, AUD.2	[LINCE_OPNSENSE_BE-TST-6003]	Verify that the TOE generates audit records related changes in product configurations and that these are described with date and time, type of event, result of the event and user producing the event.	PASS
SF. Audit AUD.3	[LINCE_OPNSENSE_BE-TST-6100]	Verify that the TOE applies the declared access control policy to the audit records.	PASS
SF. Audit AUD.4	[LINCE_OPNSENSE_BE-TST-6200]	Verify that the TOE is able to store the audit information in itself.	PASS
SF. Audit AUD.4	[LINCE_OPNSENSE_BE-TST-6201]	Verify that the TOE is able to transmit the generated audit	PASS

		information to a remote audit server.	
SF. Audit AUD.5	[LINCE_OPNSENSE_BE-TST-6300]	Verify that the TOE overwrites the oldest logs as defined in the configuration related to the rotation mechanism.	PASS
SF. Protection of credentials and sensitive data PSC.1	[LINCE_OPNSENSE_BE-TST-7000]	Verify that the TOE stores credentials as declared in the Security Target.	PASS
SF. Protection of credentials and sensitive data PSC.1	[LINCE_OPNSENSE_BE-TST-7001]	Verify that the TOE stores private keys as declared in the Security Target.	PASS
SF. Firewall FWL.1	[LINCE_OPNSENSE_BE-TST-9000]	Verify that the TOE perform stateful traffic filtering of the network packets that processes.	PASS
SF. Firewall FWL.1, FWL.2 SF. Trusted Administration ADM.2	[LINCE_OPNSENSE_BE-TST-9100]	Verify that the TOE allows the definition of packet filtering rules for ICMPv4, ICMPv6, IPv4, IPv6, TCP and UDP based on source and destination addresses, source and destination ports, type and interface.	PASS
SF. Firewall FWL.2 SF. Audit AUD.1	[LINCE_OPNSENSE_BE-TST-9101]	Verify that the TOE allows the use of the declared filtering operations.	PASS
SF. Firewall FWL.2 SF. Trusted Administration ADM.2	[LINCE_OPNSENSE_BE-TST-9102]	Verify that the TOE allows the assignment of rules to network interfaces and that these are applied in the order established by an authorized user.	PASS
SF. Firewall FWL.3	[LINCE_OPNSENSE_BE-TST-9200]	Verify that the TOE denies by default all packets that do not match any rule.	PASS
SF. Firewall FWL.4	[LINCE_OPNSENSE_BE-TST-9300]	Verify that the TOE defines a state session as terminated according to the declared idle session time.	PASS

7.2.3 RESULTS

ID	Non-conformity	State
OR02.NC01	<p>[LINCE_OPNSENSE_BE-TST-2300] SF. Identification and authentication IAU.4</p> <p>[TOE-2310] does not terminates the session according to the Shell Inactivity time defined in the web interface (System > Administration menu). This timeout only applies to tcsh/csh/sh type shells but does not apply to the default shell assigned to users (/usr/local/sbin/opnsense-shell), which is defined in the configuration page for each user in the parameter (Login shell). Therefore, given this behaviour and that the users or administrators are not instructed documentarily to use or configure any specific type of shell, it is determined that the requirement is not complied.</p> <p>On the other hand, [TOE-2310] does terminates the session of users of web interface according to the defined time configured through the web interface, after the configured time value, the session is terminated and users are shown the login page.</p> <p>[ST-07] includes instructions ("CLI interface idle timeout configuration") for users to configure type of shells that the inactivity timeout apply to. After repeating the associated test, it is verified that the timeout is properly enforced; therefore, closing the non-conformity.</p>	CLOSED
OR02.NC02	<p>[LINCE_OPNSENSE_BE-TST-3001] SF. Trusted communication channels COM.1, COM.2 SF. Cryptography CIF.1</p> <p>[TOE-2310] offers TLSv1.0 and TLSv1.1 apart from the compliant protocol versions TLSv1.2 and TLSv1.3. TLSv1.0 and TLSv1.1 do not comply [CCN-STIC-807] ENS MEDIUM Category when establishing a connection with the remote update server "opnsense-update.deciso.com".</p> <p>Moreover, [TOE-2310] offers the following cipher suites which are identified as Legacy by [CCN-STIC-807]:</p> <ul style="list-style-type: none"> TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 	CLOSED

	<p> TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 </p> <p>Moreover, [TOE-2310] offers the following cipher suites which are identified not agreed by [CCN-STIC-807]:</p> <p> TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA </p> <p>The results obtained are not consistent with the declared cryptographic mechanisms and protocols and do not comply [CCN-STIC-807] ENS MEDIUM Category. According to ENS Category and threat level, legacy and not agreed mechanisms must not be used.</p> <p>[TOE-23102] introduces a fix that addresses this issue. After repeating the associated test, it is verified that the TOE offers proper suites and TLS versions; therefore, closing the non-conformity.</p>	
OR02.NC03	<p>[LINCE_OPNSENSE_BE-TST-5100]</p> <p>SF. Trusted installation and updates</p> <p>ACT.2</p> <p>SF. Cryptography</p> <p>CIF.1</p> <p>The signature scheme involved in the digital signature of the updates is RSASSA-PKCS#1 which is considered legacy by [CCN-STIC-807]. The use of such legacy mechanism is not declared in the Security Target by the manufacturer which is required by [IT-012]. The author must declare the use of all the legacy cryptographic mechanisms.</p> <p>[ST-07] clearly indicates the mentioned digital signature scheme and mechanism as legacy; therefore, closing the non-conformity.</p>	CLOSED
OR02.NC04	<p>[LINCE_OPNSENSE_BE-TST-6300]</p> <p>SF. Audit</p> <p>AUD.5</p>	CLOSED

	<p>[TOE-2310] does not overwrite older audit entries when the storage space for the logs reaches its limit.</p> <p>According to the analysis of the configuration available in the web interface and the documentation available it is not possible to configure circular logging.</p> <p>A similar functionality is offered which consists on preserving the logs for a determined number of days configurable through the System > Settings > Logging menu in the web interface. In any case, the results obtained are not consistent with the declaration of the requirement AUD.5 in the Security Target.</p> <p>In addition, according to the changelog of previous versions of the product, support for circular logging was dropped some releases ago and it is not available in the evaluated version.</p> <p>[ST-07] modifies the description of the requirement AUD.5 to address this issue. The requirement is now worded properly and it describes a behaviour consistent with the results obtained; therefore, closing the non-conformity.</p>	
OR02.NC05	<p>[LINCE_OPNSENSE_BE-TST-6100]</p> <p>SF. Audit</p> <p>AUD.3</p> <p>The description of the requirement AUD.3 states that the root user is only able to remove the audit records locally through the CLI interface. The pertinent functional test reveals that the behaviour of the TOE is not consistent with such description since it is also possible to clear the audit records through the TOE web interface in [TOE-2310].</p> <p>[ST-07] modifies the description of the requirement AUD.3 to address this issue. The requirement is now worded properly and it describes a behaviour consistent with the results obtained; therefore, closing the non-conformity.</p>	CLOSED
OR02.NC06	<p>[LINCE_OPNSENSE_BE-TST-6002]</p> <p>SF. Audit</p> <p>AUD.1, AUD.2</p> <p>[TOE-2310] registers an event when the password of a user is changed but the audit record generated in deemed ambiguous as the type of event is not properly described.</p> <p>it is not possible to identify if the password was changed or other parameter related to the user, it just indicates that the user has changed.</p>	CLOSED

	<p>[ST-07] includes extended instructions on how to verify the type of event making us of the System > Configuration > History menu in the TOE web interface. Through this menu it is possible to identify all changes and actions declared performed over the TOE configuration, as it displays the changes in the config.xml file which is the file that stores all the configuration parameters of the TOE.</p>	
OR02.NC07	<p>[LINCE_OPNSENSE_BE-TST-6003] SF. Audit AUD.1, AUD.2</p> <p>[TOE-2310] registers the declared events in the logs, but some inconsistencies have been identified according to the declared information in the Security Target.</p> <p>The audit entries for the following events are considered to be generic, not allowing users to properly distinguish between the type of event as most of them are registered with the same entry: Session termination timeout, Deletion of groups, Change permissions of users/groups, GUI Certificate change, SSH configuration change, Creation, modification and deletion of firewall rules, Change in order of firewall rules.</p> <p>[ST-07] includes extended instructions on how to verify the type of event making us of the System > Configuration > History menu in the TOE web interface. Through this menu it is possible to identify all changes and actions declared performed over the TOE configuration, as it displays the changes in the config.xml file which is the file that stores all the configuration parameters of the TOE.</p>	CLOSED

ID	Comments	State
N/A	None.	N/A

8 VULNERABILITY ANALYSIS

Evaluator	ACP
Days required	6 days.
Date	2024/06/21
Results of the evaluator's work	PASS

8.1 EVALUATION ACTIVITIES

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

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

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

b) Available information on the technology.

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

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

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

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

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

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

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

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

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

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

TE.5.5. The evaluator shall register every non-conformity in relation to the vulnerability analysis.

PASS Information regarding this task of the evaluator can be found in section 7.1.2 *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 established by the TOE, the information stored in it and its ability to maintain the quality of its functionality in the face of extreme workloads and attempts to circumvent the restrictions it places on the traffic.

8.4 LIST OF POTENTIAL VULNERABILITIES

Code	Attack potential
[LINCE_OPNSENSE_BE-VUL-0001]	3
[LINCE_OPNSENSE_BE-VUL-0002]	3
[LINCE_OPNSENSE_BE-VUL-0003]	3
[LINCE_OPNSENSE_BE-VUL-0004]	3
[LINCE_OPNSENSE_BE-VUL-1000]	6
[LINCE_OPNSENSE_BE-VUL-1100]	6
[LINCE_OPNSENSE_BE-VUL-1200]	6
[LINCE_OPNSENSE_BE-VUL-1300]	6
[LINCE_OPNSENSE_BE-VUL-1400]	6
[LINCE_OPNSENSE_BE-VUL-1500]	3
[LINCE_OPNSENSE_BE-VUL-3000]	11
[LINCE_OPNSENSE_BE-VUL-3010]	6
[LINCE_OPNSENSE_BE-VUL-6000]	3
[LINCE_OPNSENSE_BE-VUL-8000]	6
[LINCE_OPNSENSE_BE-VUL-9000]	3
[LINCE_OPNSENSE_BE-VUL-9001]	10

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	ACP, DAT
Days required	10 days.
Date	2024/06/21
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
SF. Trusted administration	[LINCE_OPNSENSE_BE-PT-0001]	Verify if it is possible to exploit the insecure permissions for configd.socket as described by CVE-2023-39005, determine the consequences and how the TOE is affected.	PASS
SF. Protection of credentials and sensitive data SF. Identification and authentication SF. Trusted administration	[LINCE_OPNSENSE_BE-PT-0002]	Verify if it is possible to exploit the insecure permissions in the /conf directory as described by CVE-2023-39004, determine the consequences and how the TOE is affected.	PASS
SF. Trusted administration	[LINCE_OPNSENSE_BE-PT-0003]	Verify if it is possible to exploit the insecure permissions in the /tmp directory as described by CVE-2023-39003, determine the consequences and how the TOE is affected.	PASS
SF. Identification and authentication	[LINCE_OPNSENSE_BE-PT-0004]	Examine the authentication brute-force protection functionality and determine if it is flawed as described by CVE-2023-27152.	PASS

SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1000]	Examine the CVEs related to reflective cross site scripting and their fixes to determine if they are completely fixed.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1001]	Examine the source code of the TOE to identify if similar reflective cross site scripting vulnerabilities related to the “act” parameter are present in other locations of the code.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1100]	Examine the CVEs related to stored cross site scripting and their fixes to determine if they are completely fixed.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1101]	Examine the source code of the TOE to determine if a stored cross site scripting vulnerability exists in wizard.php and verify its exploitability.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1200]	Examine the source code of the TOE to identify if the authentication mechanism is flawed and determine if it is possible to bypass it.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1201]	Determine if the PHP function password_verify used by the TOE in the authentication mechanism is affected by a publicly known bug that allows bypassing hash verification.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1202]	Verify if it is possible to bypass the OTP token used as a 2FA mechanism.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1203]	Verify if OTP tokens are invalidated after they expire in the Google authenticator compatible application.	PASS

SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1300]	Examine the source code of the TOE to determine if a code execution vulnerability exists and verify its exploitability.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1400]	Examine the source code of the TOE to determine if a local file inclusion vulnerability exists in wizard.php and verify its exploitability.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-1500]	Verify if it is possible to modify the structure of the /conf/config.xml file by injecting XML tags in the fields related to a user to determine if it is possible to change its permissions.	PASS
SF. Trusted Communication Channels SF. Cryptography SF. Trusted Installation and Updates	[LINCE_OPNSENSE_BE-PT-3000]	Verify the certificate validation performed by the TOE when establishing a connection with the remote update repository and determine if a remote attacker could intercept the communication.	PASS
SF. Trusted Communication Channels SF. Cryptography SF. Trusted Installation and Updates	[LINCE_OPNSENSE_BE-PT-3001]	Verify if, in case the communication channel with the remote update repository is compromised, the TOE properly verifies the packages to be installed through the update procedure by replacing the packagesite.pkg file, which contains metadata of the packages hosted in the repository, with one modified and digitally signed by the evaluator.	PASS
SF. Trusted Communication Channels SF. Cryptography	[LINCE_OPNSENSE_BE-PT-3002]	Verify if, in case the communication channel with the remote update repository is compromised, the TOE properly verifies the	PASS

SF. Trusted Installation and Updates		packages to be installed through the update procedure by replacing the package files downloaded with one modified by the evaluator.	
SF. Trusted Communication Channels SF. Cryptography SF. Audit	[LINCE_OPNSENSE_BE-PT-3010]	Verify the certificate validation performed by the TOE when establishing a connection with the remote audit repository and determine if a remote attacker could intercept the communication.	PASS
SF. Audit	[LINCE_OPNSENSE_BE-PT-6000]	Verify if it is possible to spoof the IP address registered in the audit logs when the login event is recorded.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-8000]	Verify if the services and processes of the TOE run with accurate permissions according to their purpose and determine the consequences and how the TOE is affected.	PASS
SF. Identification and authentication SF. Trusted Administration	[LINCE_OPNSENSE_BE-PT-8001]	Verify the permissions of the wizard files used by wizard.php to determine if non-administrative users would be able to perform modifications or read sensitive information.	PASS
SF. Firewall	[LINCE_OPNSENSE_BE-PT-9000]	Verify that the TOE properly enforces filtering rules on boot applying them before enabling the network interfaces.	PASS
SF. Firewall	[LINCE_OPNSENSE_BE-PT-9001]	Verify that the TOE drops network packets with the IP options: Loose Source Routing, Strict Source Routing, or Record Route specified.	PASS
SF. Firewall	[LINCE_OPNSENSE_BE-PT-9002]	Verify that the TOE drops network packets where the source address of the	PASS

		network packet is defined as being a loopback address.	
SF. Firewall	[LINCE_OPNSENSE_BE-PT-9003]	Verify that the TOE drops fragmented packets which cannot be re-assembled completely and that are considered invalid.	PASS

9.3 RESULTS

ID	Non-conformity	State
OR02.NC08	<p>[LINCE_OPNSENSE_BE-PT-0001]</p> <p>Given the publicly documented CVE-2023-39005, the configd.socket related to the configd service was examined. It is determined that a low privileged user with local access to [TOE-2310] is able to issue commands (e.g.: auth add user test1) through configd.socket since the permissions assigned to such socket file are lax, allow read and write permissions for everyone. Among other administrator declared functionality, the non-authorized user is able to create new users.</p> <p>[ST-07] introduces additional configuration that defines an access control policy that prevents the interaction of low-privileged users with the configd service. After repeating the associated test, it is verified that it does not allow such low privileged users to issue commands and execute administrative functionality; therefore, closing the non-conformity.</p>	CLOSED
OR02.NC09	<p>[LINCE_OPNSENSE_BE-PT-0003]</p> <p>Given the publicly documented CVE-2023-39003, the usage of /tmp was examined. It is determined that a low privileged user with local access to [TOE-2310] is able to create symbolic links to restricted files and view its contents through the web interface in the crash reporter menu (for example, creating the symbolic link /tmp/PHP_errors.log that points to /conf/config.xml). This is possible because the symbolic link is interpreted as a PHP error file that is directly loaded in the crash reported menu as part of a diagnostic functionality, allowing the low privileged to read non-authorized files.</p> <p>[TOE-23102] introduces a fix that addresses this issue. After repeating the test, it is verified that the symbolic links to</p>	CLOSED

	restricted files are no longer followed and that restricted local files are not embedded in the reporter menu; therefore, closing the non-conformity.	
OR02.NC10	<p>[LINCE_OPNSENSE_BE-PT-1101]</p> <p>A stored cross site scripting vulnerability was identified in wizard.php through the “language” POST parameter used in the System: Wizard: General Information step of the wizard in System > Wizard menu.</p> <p>The user-controlled input is sanitized using the PHP function addslashes inside the “update_config_field” function defined in wizard.php but such measure is not enough to prevent XSS payloads; validation of such parameter is therefore deemed insufficient.</p> <p>It is possible to achieve payload execution with the following simple payload "><script>alert(1);</script>".</p> <p>The value of the “language” parameter is stored in /conf/config.xml and then embedded in the <html lang="HERE"> tag present in all pages. Users with the permissions to access the wizard menu can exploit this vulnerability.</p> <p>[TOE-23102] introduces a fix that addresses this issue. After repeating the test, it is verified that the payload is addressed correctly and that proper filtering functions are used; therefore, closing the non-conformity.</p>	CLOSED

ID	Comments	State
OR02.CO01	<p>[LINCE_OPNSENSE_BE-PT-8000]</p> <p>It is determined that some services and processes hosted in [TOE-2310] are running with root privileges (e.g.: php-cgi or ntpd).</p> <p>This finding could be conflictive in case a hypothetical vulnerability in such processes is exploited since it would provide the attacker with root privileges. It is advised that the permissions for such services are segregated and that they are only run using the minimum-required privileges in order to mitigate the consequences of vulnerabilities affecting the processes.</p> <p>This comment is dismissed by the manufacturer and has not taken action; therefore, the comment remains open.</p>	OPEN

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).
- [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.
- [OR01-10] LINCE Observation Report 01 v1.0
- [OR01-20] LINCE Observation Report 01 v2.0
- [OR02-10] LINCE Observation Report 02 v1.0
- [OR02-20] LINCE Observation Report 02 v2.0
- [IT-012] Esquema de evaluación y certificación de la seguridad de las tecnologías de información. Instrucción Técnica 012: Mecanismos criptográficos en certificaciones. Versión 3. Fecha 27/04/2023.

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
LAN	Local Area Network
WAN	Wide Area Network
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
SSH	Secure Shell
TLS	Transport Layer Security
SSL	Secure Sockets Layer
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
NTP	Network Time Protocol
ICMP	Internet Control Message Protocol
CLI	Command Line Interface
GUI	Graphical User Interface
2FA	2-Factor Authentication

OTP	One-Time Password
QR	Quick Response
RSA	Rivest Shamir Adleman
AES	Advanced Encryption Standard
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Elliptic Curve Diffie-Hellman Ephimeral
ECDSA	Elliptic Curve Digital Signature Algorithm
SHA	Secure Hash Algorithm
HMAC	Hash-Based Message Authentication Codes
MAC	Message Authentication Codes
GCM	Galois Counter Mode
CTR	Counter
CCM	Counter with CBC-MAC
CBC	Cipher Block chaining
PKCS	Public Key Cryptography Standards
CA	Certification Authority
RAM	Random Access Memory
GB	GigaByte
ACL	Access Control List
CVE	Common Vulnerabilities and Exposures
UTF	Unicode Transformation Format
PHP	PHP: Hypertext Preprocessor
XML	Extended Markup Language
XSS	Cross-Site Scripting
LFI	Local File Inclusion

