AlliedWare Plus v5.5.4-1.8 and x930-52GPX Switch

Security Target

V1.1

10/06/2025

Created by jtsec Applus Allied Telesis

Version control

Version	Comment	Date
0.1	Initial draft version	02/11/2023
0.2	Corrections made for COM.1, PSC.1 and PRO.1, apart from some other minor corrections	08/11/2023
0.3	Corrections made for sections 2.1, 3.1, 5.3 and 5.7, apart from some other minor corrections.	21/11/2023
0.4	Comment answered regarding COM.1	24/11/2023
0.5	CPSTIC comments answered, and corrections made for sections 1.1, 5.6 and 5.9	08/01/2024
1.0	Corrections motivated by the OR01, OR02 and OR03 made in all sections.	19/03/2025
1.1	Corrections made for section 2.3.	10/06/2025

Table of contents

1 Introduction

This document is the Security Target for the **x930-52GPX Switch and its firmware AlliedWare Plus v5.5.4-1.8**. This document includes the following information:

1. Information about this document.
2. Description of the functionality of the solution and use cases, which allows organizations or public services to address the threats and risks described in the document.
3. Description of the execution environment.
4. Threat and risk analysis of the product.
5. Fundamental security requirements covered by this solution and how they are covered to implement each security function.
6. Acronyms, Glossary of terms and Document references.

1.1 Sponsor, TOE and evaluation information

Applicant data	Allied Telesis, Inc
Developer data	Allied Telesis Labs NZ Ltd
Contact information of developer	González, Luis Luis_Gonzalez@alliedtelesis.com Ruiz, Fernando Fernando_Ruiz@alliedtelesis.com
TOE name	x930-52GPX Switch and AlliedWare Plus
TOE version	Firmware AlliedWare Plus version 5.5.4.1.8 Hardware x930-52GPX Switch
Evaluation type	LINCE
User guidance and version	See *2.2: Identification of the TOE secure use, installation and configuration guides*
Taxonomy according to CCN-STIC-140	N/A

1.2 Methodology and evaluation criteria

CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (National Essential Security Certification Definition, March 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Evaluation Methodology for National Essential Security Certification March 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad marzo 2022 versión 2.0 (Security Target template for National Essential Security Certification March 2022 version 2.0).

2 TOE description

2.1 TOE Functional description

The TOE is composed of a stackable switch and its firmware. The TOE allows switching functionalities, allowing the segmentation of virtual networks by the creation of VLANs. Additionally, the TOE allows functionalities such as configuration of users, banners, idle session timeout and firmware upgrades.

Figure 1: TOE

The TOE's security functionalities are described below:

- **SF. Trusted Administration**: The functionalities of the TOE are carried out through local console, SSH or web-based administration interface, providing the capability to manage the TOE through them.
- **SF. Identification and Authentication**: The TOE identifies and authenticates users with administrative privilege levels, implementing measures to prevent access from unauthorized users.
- **SF. Trusted Communication Channels**: The TOE protects sensitive information in transit by establishing secure communication channels in the following manner:
    - Usage of TLS v1.2 and TLS v1.3 to encrypt communications with the Syslog server and communications between the administrator and the TOE's web-based administration interface.
    - Usage of SSHv2 implementation to login remotely to the CLI of the TOE.
    - Usage of HMAC-SHA1 to provide authenticity and integrity for the communications established between the TOE and the NTP server.
- **SF. Cryptography**: The cryptographic support used by the TOE to protect data includes functions, protocols and algorithms accepted by CCN-STIC-807.

- **SF. Trusted Installation and Updates**: The TOE ensures the integrity and authenticity of firmware/software updates which will only be performed by users with administrative privilege level.
- **SF. Audit**: The TOE generates audit logs for the different events that take place and behavior detected during the execution of its functionalities.
- **SF. Protection of Credentials and Sensitive Data**: The TOE protects credentials through hashing algorithms. Additionally, the TOE protects the private keys used to generate certificates for the communications by not providing access to the internal hardware memory in which they are stored.
- **SF. Protection of the product and its services**: The TOE performs an initialization process during startup to verify the integrity of the installed firmware, along with the TOE's different modules.
- **SF. Switch**: The TOE is able to manage ports, create VLANs and is capable of traffic forwarding on the data link layer of the OSI model.

2.2 Identification of the TOE secure use, installation and configuration guides

The following table lists the documents and user's guides necessary to carry out the configuration of the TOE properly:

Document's type	Document's name	Document's version (update-history-date)
Installation Guide (PDF)	Installation Guide for Standalone Switches x930 Series	2D83F87F3D6D0D720FE6ECEE0F0B5F2FC2E6CF7BE633FD05A19A96161B4E3A56
Reference Guide (PDF)	Command Reference for AlliedWare Plus™ Version 5.5.4-1.x	04EE921431374371CB2539D22EEF84317EA2EF9C592AC0EC9977DA6183790035
Technical Guide (PDF)	Getting Started with the AlliedWare Plus Command Line Interface	7FB8C19F82920AED8CC1177341C0ADA71E98772A97604BA45426E627A47DF9DB
Technical Guide (PDF)	Logging Feature Overview and Configuration Guide	1E168EED8BC78E736604CB84403CE46A608566AC15527DF977F56AECB71E4C9E
Technical Guide (PDF)	NTP Feature Overview and Configuration Guide	D0B2530FC2D8D56AC6EDB9438668BC000DEF632C7294FDE3165AD89D46FAEB01
Technical Guide (PDF)	PKI Feature Overview and Configuration Guide	9E5990815A534AEFBA0C39D552EB394EBD1829AD307E124A56A95173643302BA
Technical Guide (PDF)	Certificate and PKI setup for Syslog	3B101EA6440E2530DF540EF573CF39142A48896384AAD21F34BA028E8C58F5B7
Technical Guide (PDF)	Getting Started with the Device GUI on Switches	186E877CC6213918DD507B29EAFFE91B4518E5EA4BE7FB5C4AB03006A3B23E53

2.3 TOE usage description

Start a Local Management session as specified in "*How to login*" section of "*Getting Started with the AlliedWare Plus Command Line Interface*" referenced in *2.2 Identification of the TOE secure use, installation and configuration guides.*

Then, the user must follow the next steps to update the TOE to the evaluated version:

- Plug an USB to the TOE with the firmware and flash its content by executing:

```
1. dir usb
2. copy usb: <firmware-file> flash
```

- Execute the following commands to set the new firmware file and authenticate it using the HMAC-SHA256, provided by the manufacturer in a .sig file along with the firmware file.

```
1. configure terminal
2. crypto verify signed <FIRMWARE> <HMAC-SHA256>
3. boot system <FIRMWARE>
4. exit
5. write
```

- Reboot the device executing the `reboot` command.
- Once the update has finished, enter the `show version` command to display de firmware version and verify that it matches the evaluated version.
- Use the following commands while in Global Configuration mode (`awplus (config)#`) to enable Secure Mode:

```
1. crypto secure-mode
2. exit
3. write
4. reboot
```

- After this, to verify that the TOE has entered Secure Mode for the switch, the user must enter the `show secure-mode` command. The following message should be displayed: `Secure mode is enabled`.

Since, for the purpose of this evaluation, the TOE is to be used as a standalone unit, it must be configured as specified in the "*Installation Guide for Standalone Switches x930 Series*" referenced in *2.2 Identification of the TOE secure use, installation and configuration guides.*

- In order to make the device's configuration compliant in terms of password security, the following commands shall be introduced:

```
1. security-password minimum-length 12
2. security-password minimum-categories 4
3. security-password lifetime 10
4. security-password forced-change
```

As part of the pre-configuration, a user must be created and, thereafter, the default user "manager" shall be deleted so there is no default user. To do this, the following steps shall be performed:

- Enter `username <name> privilege <1-15> password <password>` to create a new user, where `<name>` is the name for the user to be created, `<1-15>` is the privilege level for the user, and `<password>` is the password for the specified user. With Secure Mode enabled, only privilege levels [1] and [15] are allowed by the TOE. In this case the new user shall be created with administrative privileges, so the privilege level shall be 15.
- Enter `ssh server allow-users <name>` to allow SSH access to the user created in the previous step.
- Enter `no username <name>` to delete a user. In this case, the user to be deleted is the "manager" user, so this value shall replace `<name>`.

In order to configure the TOE to send audit records to a remote syslog server, refer to the "PKI Feature Overview and Configuration Guide" referenced in *2.2 Identification of the TOE secure use, installation and configuration guides.*

To implement NTP on the switch, refer to the "NTP Feature Overview and Configuration Guide" referenced in *2.2 Identification of the TOE secure use, installation and configuration guides*. To configure authentication for this feature, refer to the mentioned guide, page 8.

To be able to create a management VLAN (to contain communications with the administrator via SSHv2 or web-based interface, with the NTP server and with the Syslog server), the switch shall be configured as follows:

```
vlan database
  vlan <VLAN_ID> name mgmt state management-only
!
acl-group ip port administrator
  eq 22
  eq 443
access-list hardware acl-test
  permit udp 169.254.8.101 255.255.255.0 eq 123 169.254.8.1
255.255.255.0 eq 123 vlan <VLAN_ID>
  permit udp 169.254.8.100 255.255.255.0 eq 6514 169.254.8.1
255.255.255.0 eq 6514 <VLAN_ID>
  permit tcp 169.254.8.220 255.255.255.0 range 1 65535 169.254.8.1
255.255.255.0 port-group administrator <VLAN_ID>
  deny tcp any range 1 65535 169.254.8.1 255.255.255.0 range 1 65535
vlan <VLAN_ID>
!
interface port1.0.1-1.0.5
  switchport
  switchport mode access
!
interface port1.0.6
  switchport
  switchport mode access
  switchport access vlan <VLAN_ID>
  access-group acl-test
!
interface port1.0.7-1.0.52
  switchport
  switchport mode access
```

To configure the IP address for the VLAN, the following commands shall be used:

```
1. interface vlan <VLAN_ID>
2. ip address <IP_ADDRESS> <SUBNET_MASK>
```

As for additional VLAN configuration, refer to chapter 15 “VLAN Commands” of the “Command Reference for AlliedWare Plus™ Version 5.5.4-1.x”, referenced in *2.2 Identification of the TOE secure use, installation and configuration guides.*

To configure a certificate for the TOE to use for its web interface (HTTPS), refer to page 32 and onwards of the “PKI Feature Overview and Configuration Guide”, referenced in *2.2 Identification of the TOE secure use, installation and configuration guides.*

To configure Spanning-Tree Protocol for the TOE, the following commands should be used:

```
1. configure terminal
2. spanning-tree enable
3. interface <PORT_ID>
4. spanning-tree priority <[0-240]>
```

To setup the certificate and PKI necessary for the Syslog connection, please follow the steps detailed in the “Certificate and PKI setup for Syslog“ guide, referenced in *2.2 Identification of the TOE secure use, installation and configuration guides.*

To close the HTTP port (port 80) of the TOE, the following commands should be used:

```
1. configure terminal
2. http port none
```

To protect the audit log system files from access, the following commands should be used:

```
1. configure terminal
2. strict-user-process-control
```

To set the log buffered level to informational, the following commands should be used:

```
1. configure terminal
2. log buffered level informational
```

Apart from these considerations, the TOE does not require any other pre-configuration or particular usage to obtain the security features described in section 5 Security Functional Requirements of this document beyond the TOE guide’s steps.

3 Operational environment

3.1 Operational environment description

The following diagram illustrates a common use case scenario where the TOE can be deployed:

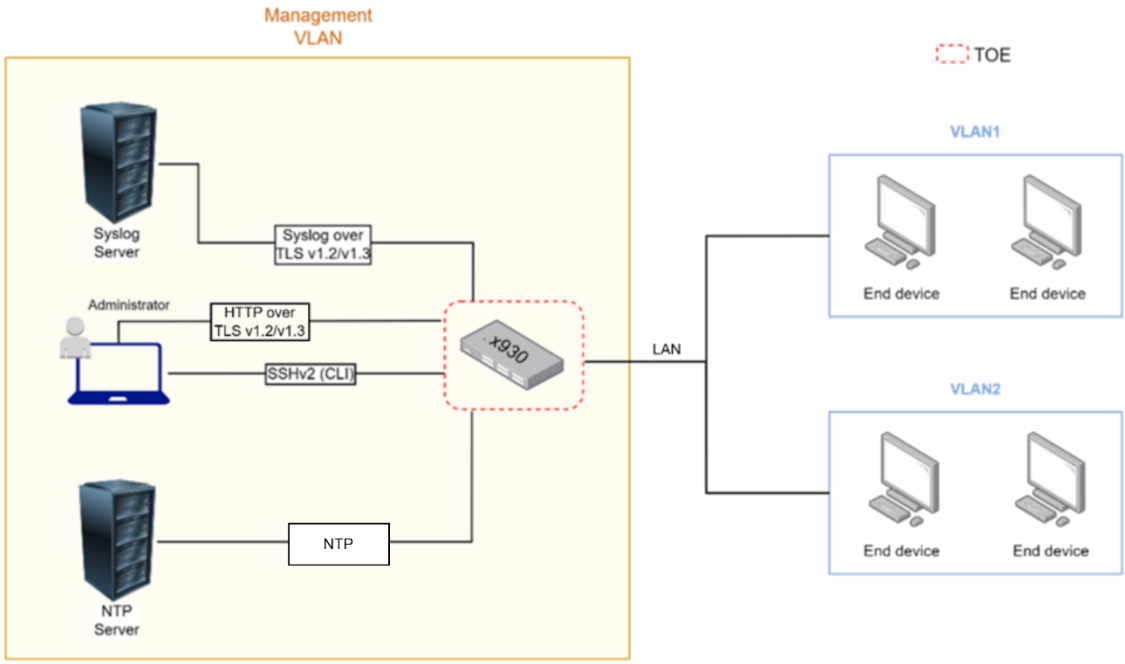

Figure 2: Operational environment

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

- **End devices**: Endpoints in the client's infrastructure that connects to services outside the network through the TOE via local communication.
- **Administrator**: User with administrative privilege level (15), as assigned by the TOE.
- **Syslog server**: It stores all the logs generated by the TOE. These logs are transmitted to the syslog server over TLS v1.2/v1.3.
- **NTP server**: The TOE can be configured to synchronize its clock with an NTP server in the network in order to get more accurate timestamps for audit records.

4 Security Problem Definition

4.1 Operational Environment Assumptions

Assumption	Description
A.PHYSICAL PROTECTION	The product must be physically protected by its operational 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 routing and filtering functionality as its primary function and shall not provide any other functionality or services that could be considered general purpose.
A.TRUSTED ADMINISTRATION	Administrators are members of full confidence and look after the best security interests of the organization. They must be properly trained and free of any malicious intent or conflict of interest in administering the product.
A.PERIODIC UPDATES	Product firmware/software is updated as updates are released to correct known vulnerabilities.
A.PROTECTION OF CREDENTIALS	All credentials, especially the administrator's, must be properly protected by the organization using the product.

4.2 Assets to protect

This section describes the assets that the TOE's security features protect.

Asset	Description	Security Dimensions
AS.Administration	Product management interfaces and the information transmitted through them, in both directions.	Confidentiality, integrity, authenticity and traceability
AS.PSS	Configuration data and audit trails.	Integrity
AS.PSC	Credentials and keys.	Confidentiality and integrity
AS.Updates	Updates to the device that may affect its configuration and functionality.	Authenticity and integrity
AS.Communications	Communications of the product, established between its own components, with the web-based interface, with the administrators via SSHv2 and with the Syslog server.	Confidentiality, integrity and authenticity
	Communications of the product, established between its own components and with the NTP server.	Integrity and authenticity

4.3 Threat descriptions

Threat	Description	Assets
T.NOAUT	**UNAUTHORIZED ADMINISTRATOR ACCESS.** An attacker can gain access as a product administrator by one of the following scenarios: Impersonating as an administrator to the product; Impersonating as the product to an administrator; Replaying an administration session; Performing man-in-the-middle attacks.	*AS.ADMINISTRATION* *AS.COMMUNICATIONS*
T.CRYPTO	**WEAK CRYPTOGRAPHIC MECHANISMS** Use of cryptographic mechanisms or weak key lengths in the product that allow an attacker to compromise it, primarily through brute force attacks.	*AS.PSC* *AS.COMMUNICATIONS* *AS.UPDATES*
T.COM	**UNAUTHORIZED COMMUNICATION PROTOCOLS** Use of unauthorized protocols that allow an attacker to compromise the integrity and confidentiality of critical product communications.	*AS.COMMUNICATIONS*
T.ACT	**MALICIOUS UPDATE** An attacker can perform a malicious update that weakens the product's security features.	*AS.UPDATES*
T.AUD	**UNDETECTED ACTIVITIES** An attacker may attempt to access, change or modify the product's security functionality without the administrator's knowledge.	*AS.ADMINISTRATION* *AS.PSS*
T.PSC	**COMPROMISE OF CRITICAL SECURITY PARAMETERS** An attacker can compromise critical security parameters and continuously access the product and its critical data.	*AS.PSC*

T.FUN	**FAILURE OF SECURITY FUNCTIONALITIES** An external attacker exploit weaknesses in the product's security functionalities and could access, change or modify information, security functionalities or network traffic in the product.	***AS.ADMINISTRATION*** ***AS.PSS***
T.NOAUTUSR	**UNAUTHORIZED USER ACCESS** An attacker can gain unauthorized access by one of the following scenarios: Impersonating a user to the product; Impersonating the product to a user; Replaying a user session; Performing man-in-the-middle attacks.	***AS.ADMINISTRATION*** ***AS.COMMUNICATIONS***
T.CRE	**COMPROMISE OF CREDENTIALS** An attacker can exploit the use of weak or unprotected credentials to gain privileged access to the product.	***AS.PSC***
T.NET	**UNAUTHORIZED NETWORK ACCESS** An attacker can exploit misconfigured or unmanaged network interfaces, or lack of network segmentation, to gain unauthorized access to sensitive areas of the network. This can lead to the interception or disruption of network traffic, potentially compromising sensitive data and affecting network integrity.	***AS.COMMUNICATIONS***

4.3.1 Traceability threats/security requirements

The following table maps the Fundamental Security Requirements defined in section *5: Security Functional Requirements* that address the defined threats:

	T.NOAUT	T.CRYPTO	T.COM	T.ACT	T.AUD	T.PSC	T.FUN	T.NOAUTUSR	T.CRE	T.NET
ADM.1	X									
ADM.2	X									
ADM.3	X									
IAU.1	X							X		
IAU.2									X	
IAU.3									X	
IAU.4	X									
COM.1	X	X	X					X		
COM.2	X		X					X		
COM.3	X		X					X		
COM.4	X	X	X					X		
CIF.1	X	X	X	X				X	X	
ACT.1				X						
ACT.2				X						
ACT.3				X						
AUD.1					X					

AUD.2					X					
AUD.3					X					
AUD.4					X					
AUD.5					X					
PSC.1	X	X	X			X		X	X	
PRO.1							X			
SWI.1										X
SWI.2										X
SWI.3										X

5 Security Functional Requirements

5.1 SF. Trusted Administration

Requirement	Description
ADM.1	The TOE shall define the privilege level 15 (administrative privileges) and shall allow the assignation of this privilege level to users.
ADM.2	The TOE shall allow management both locally through Console Port CLI and remotely through SSHv2. The TOE shall allow the following functionalities to users with privilege level 15: • Change user assigned roles. • Change users' passwords. • Create and delete users. • Create and delete VLANs. • Configuration of maximum inactivity time for remote terminal connections. • Configure banners on the device. • Disable and enable interfaces. • Set IPs to interfaces Additionally, the TOE shall allow management remotely through web-based management interface. The TOE shall allow the following functionalities to users with privilege level 15: • Change user assigned roles. • Change users' passwords. • Create and delete users. • Create and delete VLANs. • Disable and enable interfaces. • Set IPs to interfaces
ADM.3	The TOE shall ensure that only users with privilege level 15 are able to perform the functionalities described in ADM.2.

5.2 SF. Identification and Authentication

Requirement	Description
IAU.1	The TOE shall identify and authenticate each user before granting access to the TOE's functionalities via Console Port CLI, SSHv2 or web interface by prompting the user for their credentials.
IAU.2	The TOE shall establish a maximum authentication attempt limit of 5 attempts on Console Port CLI and SSHv2, and 3 attempts on web-based interface to prevent brute-force attacks. The TOE shall block the user account trying to log in via Console Port CLI, SSHv2 and web-based interface when the maximum authentication attempts limit is surpassed.
IAU.3	The TOE shall provide the ability to manage passwords as follows: • The password shall be configurable with a minimum length of 12 characters. • The password shall be able to be composed of lowercase letters, uppercase letters, numbers and special characters ["!", "@", "#", "$", "%", "^", "&", "*", "(", ")"].
IAU.4	The TOE shall log out a user's session after 10 minutes of inactivity in the case of the SSHv2 CLI, 5 minutes in the case of the web-based interface, and 10 minutes in the case of the Console Port CLI.

5.3 SF. Trusted Communication Channels

The cipher suites listed in this section include the following nomenclature:

- Recommended (R): Refers to the cryptographic algorithms that are considered secure and suitable in the context of HIGH ENS Category.
- Legacy (L): Refers to the cryptographic algorithms, in the context of MEDIUM ENS Category, that are considered with acceptable security in the short term, valid until 2025.

Requirement	Description
COM.1	The TOE shall establish secure channels when exchanging sensitive information with authorized entities, using accepted algorithms, protocols and functions according to the CCN-STIC-807 guide: • The authorized users communicate with the TOE through the web-based interface are carried out using HTTP over TLS v1.2 or TLS v1.3 with the following cryptographic mechanisms: ○ TLS v1.3: - TLS_AES_256_GCM_SHA384 (R) - TLS_AES_128_GCM_SHA256 (R) ○ TLS v1.2: - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R) - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R) ○ Key Exchange Groups: secp256r1 (R), secp384r1 (R), secp521r1 (R), Curve25519 (R), Curve448 (R), ffdhe4096 (R), ffdhe6144 (R), ffdhe8192 (R), ffdhe2048 (L). • The TOE communicates with the Syslog over TLS v1.2 or TLS v1.3, with the following cryptographic mechanisms: ○ TLS v1.3: - TLS_AES_256_GCM_SHA384 (R) - TLS_AES_128_GCM_SHA256 (R) ○ TLS v1.2: - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (R) - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (R) - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (R) - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (R) ○ Key Exchange Groups: Curve25519 (R), secp256r1 (R), Curve448 (R), secp521r1 (R), secp384r1 (R), ffdhe3072 (R), ffdhe4096 (R), ffdhe6144 (R), ffdhe8192 (R), ffdhe2048 (L). • The authorized users' communications with the TOE are carried out using SSHv2 (CLI):

	○ SSH Key Exchange Method: ecdh-sha2-nistp256 (R), ecdh-sha2-nistp384 (R) ○ SSH Encryption Algorithm: aes128-cbc (L), aes256-cbc (L), aes128-ctr (R), aes192-ctr (R), aes256-ctr (R) ○ SSH Public Key Algorithm: ecdsa-sha2-nistp384 (R). ○ SSH MAC Algorithm: hmac-sha2-256 (R). • The TOE communications with NTP server are carried out using HMAC-SHA1 (L) algorithms to authenticate NTP peers.
COM.2	The TOE shall allow the communication channels defined in COM.1 to be initiated by itself or by authorized entities: • The TOE initiates the communications with the Syslog server. • The TOE initiates the communications with the NTP server. • The authorized user initiates the communication with the TOE through the web-based interface. • The authorized user initiates the communication with the TOE via SSHv2.
COM.3	The TOE shall have RSA 2048 (L) digital certificates for the web-based interface (HTTPS) and 384 bits (R) public keys for the SSHv2 interface, so the authorized users connecting to the web interface (HTTPS) are able to authenticate the TOE.
COM.4	The TOE shall establish a secure communication channel with the administrator by using SSHv2 or HTTPS with the cryptographic algorithms defined in COM.1

5.4 SF. Cryptography

Requirement	Description
CIF.1	The TOE shall use the following authorized cryptographic mechanisms in accordance with the CCN-STIC-807 guide: • Cipher suites and cryptographic algorithms declared in COM.1. • The certificates as specified in COM.3. • The hash function used for software updates authentication, as defined in ACT.2. • Hash function for local passwords as defined in PSC.1.

5.5 SF. Trusted Installation and Updates

Requirement	Description
ACT.1	The TOE shall provide the ability to check the current firmware version, as well as to manually collect and initiate firmware updates via USB using the Command Line Interface.
ACT.2	The TOE shall authenticate the firmware updates before installing them using HMAC-SHA256, as authorized by the CCN-STIC-807 guide.
ACT.3	Users with privilege level 15 shall be the only ones allowed to update the TOE's firmware.

5.6 SF. Audit

Requirement	Description

AUD.1	The TOE shall generate audit records when any of the following events occur:
	• Login and logout of registered users.
	• Changes in user credentials.
	• Changes in product configurations:
	  ○ Banner configuration
	  ▪ Enabling and configuring message to display
	  ▪ Disabling the banner
	  ○ User management
	  ▪ Changes in users' assigned roles
	  ▪ Changes in users' passwords
	  ▪ Creation or removal of users
	  ○ Idle session timeout interval configuration
	  ○ Interfaces configuration
	  ▪ Disabling or enabling interfaces
	  ▪ Assigning IP addresses to interfaces
	• Events related with product functionalities:
	  ○ VLAN configuration
	  ▪ Creation of VLANs
	  ▪ Deletion of VLANs
	• Events related to the creation and removal of RSA cryptographic keys.

AUD.2	Audit records shall contain at least the following information: • Date and time of the event. • Type of identified event. • Result of the event (when the performed operation is successful). • User producing the event (if applicable).
AUD.3	The following access policy shall apply to audit records: • Read: users with privilege level 15. • Modify: no user. • Delete: users with privilege level 15.
AUD.4	The TOE shall be able to store the generated audit information in its memory and internal flash. It shall also store audit information externally via Syslog Server using the secure channel defined in **COM.1**.
AUD.5	The TOE shall overwrite the oldest logs if the storage space for the logs reaches its total storage limit of 50 kB in the following manner: • The TOE stores generated log entries internally in a series of log files, numbered sequentially by age. • Rotation increases the file number (eg. messages -> messages.1, messages.1 -> messages.2, etc.). • The oldest log file is deleted when the total size of these log files surpasses the limit of 50kB.

5.7 SF. Protection of Credentials and Sensitive Data

Requirement	Description
PSC.1	The TOE shall not provide access to the internal hardware memory where the private keys that the TOE uses to generate certificates for the communications are stored. Additionally, credentials shall be stored within the TOE using SHA-256 hashing algorithms.

5.8 SF. Protection of the product and its services

Requirement	Description

PRO.1	The TOE shall perform a test during product startup, to verify firmware version and proper operation of its different components:
	• Filesystem:
	  ○ Flash
	• Base components
	  ○ syslog
	  ○ inet

5.9 SF. Switch

Requirement	Description
SWI.1	The TOE shall be able to manage interfaces, enabling or disabling them, as well as assigning priorities to them through STP.
SWI.2	The TOE shall forward network traffic through its ports at the data link layer (layer 2) of the open systems interconnection model (ISO/IEC 7498-1) according to Ethernet physical addressing or Media Access Control (MAC).
SWI.3	The TOE shall have virtual network segmentation (VLAN) capability.

6 Acronyms

The following table shows the acronyms used in this document.

Acronym	Meaning
CCN	Centro Criptológico Nacional (National Cryptologic Centre).
LINCE	Certificación Nacional Esencial de Seguridad
ST	Security Target – Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y la Comunicación (Security of Information and Communication Technologies).
TOE	Target Of Evaluation - Objeto a evaluar.
OSI	Open Systems Interconnection
MAC	Media Access Control
IP	Internet Protocol
SSH	Secure Socket Shell
SNMP	Simple Network Management Protocol
SHA	Secure Hashing Algorithm
HMAC	Hash-based Message Authentication Code
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
USB	Universal Serial Bus
ID	Identification
CLI	Command-Line Interface
HTTPS	HyperText Transfer Protocol Secure
NTP	Network Time Protocol
RSA	Rivest-Shamir-Adleman
IEC	International Electrotechnical Commission

Table 1 *Abbreviations*

7 Document references

The following table shows the documents referenced in this document.

Reference	Document
CCN-STIC-2001	Definición de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (National Essential Security Certification Definition, march 2022 version 2.0).
CCN-STIC-2002	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Evaluation Methodology for National Essential Security Certification, march 2022 version 2.0).
CCN-STIC-2003	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE), marzo 2022 version 2.0 (Security Target template for National Essential Security Certification, march 2022 version 2.0).
CCN-STIC-807	Criptología de empleo en el Esquema Nacional de Seguridad, mayo 2022 (National Security Scheme employment cryptology, May 2022).

Table 2 List of document references

8 Annex

8.1 Third Party Libraries Used by the TOE

Library Name	Version	Vendor
ca_certificates	v20210119	Debian
curl	v8.0.1	Curl
fipscheck	v10.0.0.170	LairdCP
haproxy	v1.8.30	Haproxy
jitterentropy-library	v3.4.1	smuellerDD
mozilla-ssl-config	v5.6	Mozilla
openldap	v2.6.0	OpenLDAP
openssl	v3.1.1	OpenSSL
sshfs	v3.7.1	libfuse