Security Target Description Junos OS 23.4R2-S2.3-EVO for QFX5700 Switches

Version 1.4

January 13, 2025

Prepared for:
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089
www.juniper.net

Document History

Date	Version	Description	Author
01/09/2024	1.0	First version of the Security Target	Juniper Networks
10/10/2024	1.1	Small fixes	Juniper Networks
15/10/2024	1.2	Reference of secure configuration guide added	Juniper Networks
08/01/2025	1.3	Small fixes	Juniper Networks
13/01/2025	1.4	Small fixes	Juniper Networks

Table of contents

Index of tables

Index of Figures

1. Introduction

1.1 Sponsor, TOE and evaluation information

Sponsor information	Juniper Networks, Inc., 1133 Innovation Way, Sunnyvale, CA 94089
Developer information	Juniper Networks, Inc., 1133 Innovation Way, Sunnyvale, CA 94089
Contact of the developer	Diego Arranz de la Pena, Sales Engineer, darranzde@juniper.net + 34 646 572 392
TOE name	QFX5700
TOE version	Junos OS 23.4R2-S2.3-EVO
Evaluation type	LINCE
User guidance and version	Junos® OS Evolved Getting Started with Junos OS Evolved, 2024-06-23 QFX5700 Switch Hardware Guide, 2024-07-31
Taxonomy according to CCNSTIC-140	D.1-M Enrutadores D.2-M Switches

Table 1 Sponsor, TOE and evaluation information

***Note:** The "TOE name" belongs to the name of the HW appliance (**QFX5700**) and the "TOE version" belongs to the OS that is running in the QFX5700 (**Junos OS 23.4R2-S2.3-EVO**).

1.2 Methodology and evaluation criteria

[CCN-STIC-2001]	Definición de la Certificación Nacioal Esencial de Seguridad (LINCE). Marzo 2022. Versión 2.0.
[CCN-STIC-2002]	Metodología de Evaluación para la Certificación Nacional Esencial de Seguridad (LINCE). Marzo 2022. Versión 2.0.
[CCN-STIC-2003]	Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE). Marzo 2022. Versión 2.0.
[CCN-STIC-2004]	Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE). Marzo 2022. Versión 2.0.
[ANNEXD1M]	Guía de Seguridad de las TIC CCN-STIC 140 (Taxonomía de productos STIC - Anexo D.1-M: Enrutadores) Septiembre 2023.
[ANNEXD2M]	Guía de Seguridad de las TIC CCN-STIC 140 (Taxonomía de productos STIC - Anexo D.2-M: Switches) Septiembre 2023.

Table 2 Methodology and evaluation criteria

2. TOE description

2.1 TOE Functional description

The **QFX5700** is a high-capacity aggregation switch by Juniper Networks, offering a 12.8 Tbps throughput in a 5-U form factor. It supports various high-speed Ethernet interfaces (10/40/100/400GE) and is designed for high performance, scalability, and flexibility, suitable for service providers, web, and enterprise networks. The switch utilizes the Broadcom Trident 4 chipset and supports advanced Layer 2, Layer 3, and EVPN-VXLAN features, along with in-line MACsec support, making it an optimal choice for dense 400GbE IP fabrics in data centers.

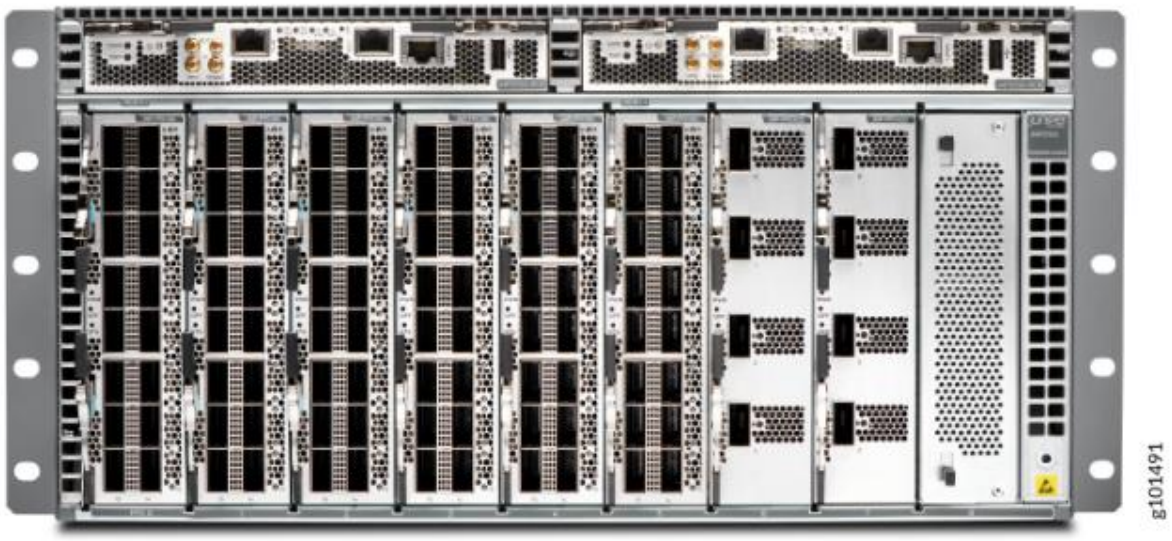


Figure 1 QFX5700 hardware

The **QFX5700** runs the Operative System **Junos OS 23.4R2-S2.3-EVO**. Junos OS Evolved Release 23.4R2-S2.3-EVO introduces several enhancements and features aimed at improving the functionality and performance of Juniper's network devices.

The TOE provides the following security functions:

- **Trusted Administration**: The TOE provides the administration role and the ability to associate users with roles. The *administrator* role is the only one that is able to perform the following actions: product management (both locally and remotely), configuration of the termination times or blocking in case of detected inactivity, updating the TOE software, modifying the TOE configuration, configuring audit behaviour and configuring the access banner.
- **Identification and Authentication**: All users must be identified and authenticated before access is granted. To prevent brute force authentication attacks, the TOE employs a blacklist. Passwords must be set to a minimum length of 12 characters and include a combination of lowercase letters, uppercase letters, numbers, and special characters ["!", "@", "#", "$","%", "^", "&", "*", "(", "]. Additionally, the TOE allows the configuration of an inactivity timer, automatically logging out users after a specified period of inactivity. If a user attempts to access the TOE using default credentials or with no credentials after the initial setting of the credentials, the access is refused.
- **Trusted Channels:** The TOE protects information in transit by establishing secure channels when exchanging sensitive data with any authorized entity. These channels can be initiated either by

the TOE itself or by authorized entities. When exchanging information with the remote administrator, the TOE will establish secure channels using SSHv2.

- **Cryptography:** The TOE only allows the use of the cryptographic mechanisms SSHv2 authorized in accordance with the provisions of guide CCN-STIC-807. Furthermore, digital signatures will be used to authenticate firmware/software updates.
- **Trusted updates:** The TOE provides the option to check the current firmware/software version and allows manual initiation of updates, no other initiation method is supported. The TOE utilizes digital signatures authorized in CCN-STIC-807 to authenticate firmware/software updates before installation. Only users with administration role are permitted to initiate these updates.
- **Audit:** The TOE generates audit records when certain defined events occur. These audit logs contain at least: the date and time of the event, the identified event type, the result of the event, and the user that has produced the event. The TOE includes an access policy that determines permissible actions related to the audit record for each user. Audit records can be saved internally and transmitted to an external entity. When the dedicated audit storage is full, the TOE overwrites previous audit entries.
- **Protection of credentials and sensitive data:** The TOE stores the credentials encrypted. These credentials can be saved using hmac-sha2-512 for password accounts and AES-GCM-256 for private keys.
- **Failure protection:** The TOE has the ability to perform a test during both power up of the product and at the request of an authorized user to verify the integrity of the software/firmware.
- **Router:** The TOE is capable of managing ports by enabling or disabling them and assigning priority. It forwards network traffic through its ports at the network layer level of the Open Systems Interconnection model, following a routing table.
- **Switches**: The TOE must manage ports, including enabling, disabling, and prioritizing them, and must forward network traffic at the data link layer using physical or MAC addressing. Additionally, it must support VLAN segmentation.

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

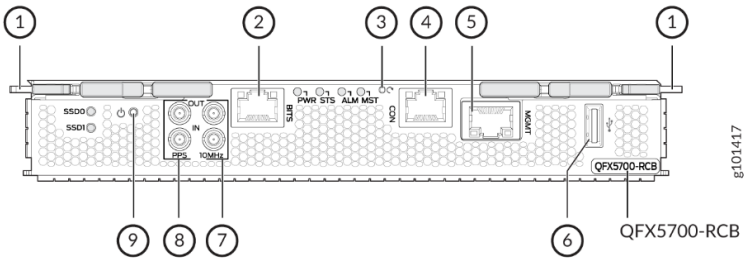
The following table lists the documents and user's guide necessary to carry out the configuration of the TOE properly:

Document	Version	Date	Description
Junos® OS Evolved Getting Started with Junos OS Evolved	N/A	2024-06-23	Guide to configure common system management features on Juniper Networks devices using Junos OS Evolved.
QFX5700 Switch Hardware Guide	N/A	2024-07-31	Guide to plan, install, perform initial software configuration, perform routine maintenance, and to troubleshoot QFX5700 Switches.
Guía de Instalación y Configuración segura	1.0	09-10-24	Guide to perform the secure configuration of QFX5700 Juniper Switches with Junos OS 23.4R2-S2.3-EVO.

Table 3 Identification of the TOE secure use, installation and configuration guides

2.3 TOE usage description

This type of product is presented in the form of an appliance composed of a hardware (**QFX5700**) with dedicated firmware (**Junos OS 23.4R2-S2.3-EVO**).



1– RCB	6– USB port (USB 2.0 standard)
2– RJ-45 BITS port	7– 10 MHz IN/OUT Timing port
3– Reset switch	8– PPS IN/OUT Timing port
4– RJ-45 console port	9– Online/Offline button
5– RJ-45 management port	

Figure 2. QFX5700 Routing and Control (RCB) Board Faceplate

- In the hardware part (**QFX5700**) of the TOE, there are two different physical interfaces:
  - The RCB interface ports with the indicated labels function as follows:
    - **CON**: Connects the RCB to a system console through a serial cable with an RJ-45 connector. (Port number 4 in **Figure *2***)
    - **MGMT**: Connects the RCB through an Ethernet connection to a management LAN (or any other device that plugs into an Ethernet connection) for out-of-band management. The port uses an autosensing RJ-45 connector to support 10-Mbps, 100-Mbps, or 1000-

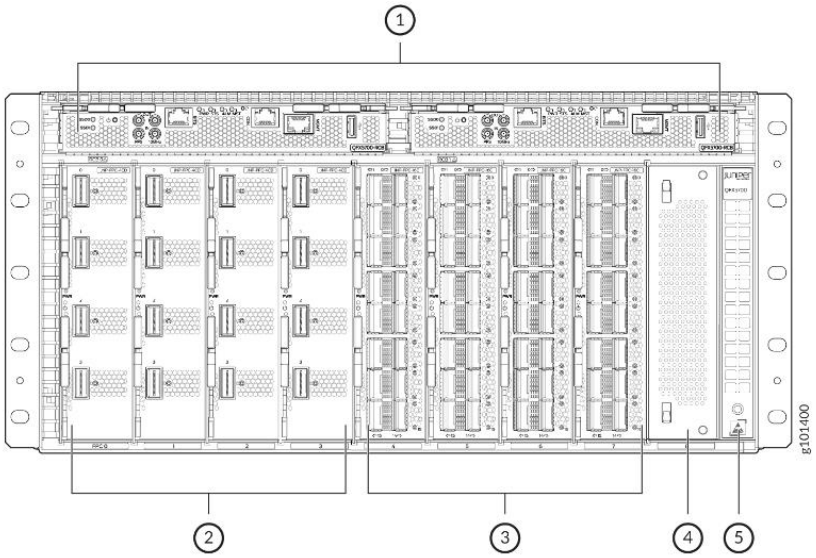
Mbps connections. Two small LEDs (an activity LED and a link LED) on the port indicate that the connection is in use. (Port number 5 in **Figure *2***)

The link LED is:

- Green (steady) when the 1000-Mbps link is up.
- Orange (steady) when the 10/100-Mbps link is up.
- Off when the link is down.

The activity LED is:

- Green (blinking) when traffic is passing through the port.
- Off when traffic is not passing through the port



1– RCB	4– Unsupported slot
2– FPC 0-3	5– ESD Point
3– FPC 4-7	

Figure 3. Front View of QFX5700

The QFX5700 comes with two RCB slots. The RCBs are accessible from the front side. The RCBs are kept upside down. The configuration of the RCS includes a 30mm pitch, 200mm width Hewitt Lake 6 Core (D1637), 2.9GHz, 55W CPU, and DRAM: 32GB (2x16GB DIMM) Memory which is expandable up to 64 (4x 16GB). The storage support includes 2x 100G M.2 SATA/NVME SSD.

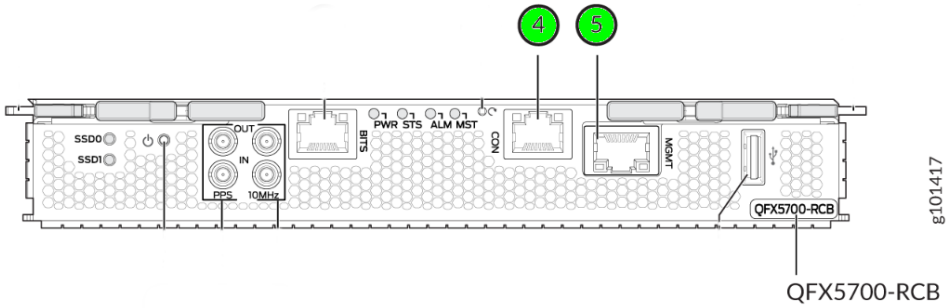


Figure 4 Boundaries of the TOE

- The firmware part of the TOE (Junos OS 23.4R2-S2.3-EVO):
  - It is designed to be **remotely** accessible through the logical interface that implements the secure communications protocols (SSH) and **locally** accessible through a console port to perform the initial configuration which allows the TOE to be managed remotely. Furthermore, the TOE is accessible via console port, LAN (Local Area Network) and WAN (Wide Area Network).
    - **Console Port:** A user can manage the TOE locally via console port by using an RJ-45 cable.
    - **Wired method:** A user can manage the TOE through an ethernet connection using SSH.

2.4 Third party libraries and external binaries.

The TOE includes the following security related third-party libraries:

Library Name	Version
arptables	0.0.4+gitAUTOINC+f4ab8f63f1
at	3.1.23
audit	2.8.5
binutils	2.32.0
cracklib	2.9.5
glibc	2.30
grub	2.04
grub-verify	0.1.7
iptables	1.8.3
jitterentropy-rngd	1.2.6
keyutils	1.6
libgcrypt	1.8.4
libpam	1.3.1
libxcrypt	4.4.8
sbsigntool	git+8e97a41

3. Operational environment

3.1 Operational environment description

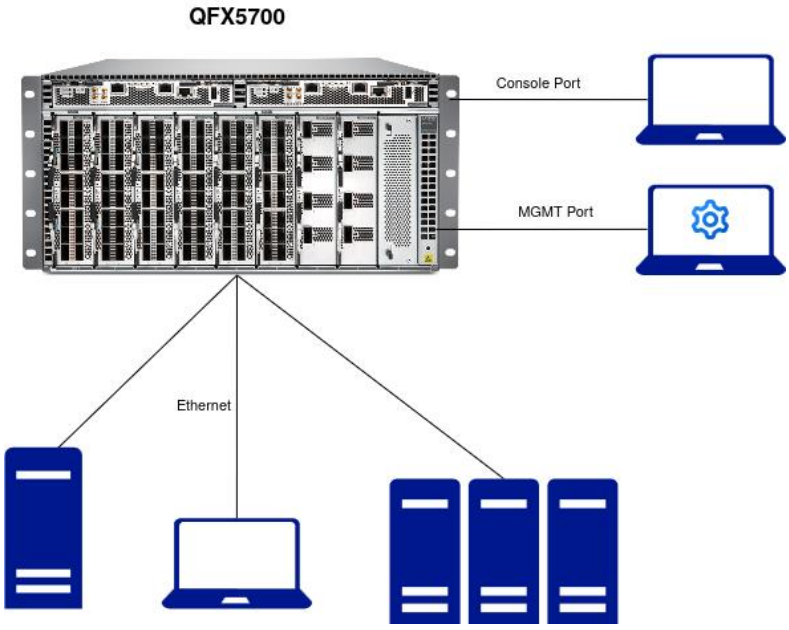


Figure 5 TOE operational environment

The regular users will connect to the TOE through the Ethernet ports located in the appliance. The TOE will create a VXLAN that allows for scalable network segmentation and overlays, enabling efficient and flexible connectivity across different physical and virtualized environments within the data center.

The management of the TOE can be performed by administrator users through the following methods through local access:

- **Console port:** The administrator can connect to the TOE through the Console Port located in the appliance.
- **Management port:** The administrator can connect to the TOE through the Console Port located in the appliance to a management LAN (or any other device that plugs into an Ethernet connection) for out-of-band management

In order to do so, a workstation with at least the following minimum requirements is required by the administrator:

- x86-64 compatible processor
- Minimum 2GB RAM
- Variable amount of persistent storage
- Serial Port (RS-232) is available

3.2 NON-TOE hardware description

This section provides a detailed overview of the hardware components that are integral to the product but are not included within the boundaries of the TOE. These non-TOE hardware components, although outside the scope of the security evaluation, are essential for the product's overall operation and performance.

- **BITS**: Building-integrated timing system (BITS) is the external clocking interface for connecting to external clocking devices. (Port number 2 in **Figure *2***)
- **10MHZ** (one input and one output)—The 10-MHz timing connectors on the front panel of the router connect to external clock signal sources. The clocking ports provide the synchronized output clocks from any one of the reference clock inputs, based on the clock's priority (Port number 7 in **Figure *2***)
- **PPS** (one input and one output)—1-pulse-per-second (PPS) connector on the front panel of the router connects to external clock signal sources. The clocking ports provide the synchronized output clocks from any one of the reference clock inputs, based on the clock's priority. (Port number 8 in **Figure *2***)
- **USB**—Provides a removable media interface through which you can install Junos OS Evolved manually. Junos OS Evolved supports USB version 2.0 and later. (Port number 6 in **Figure *2***)

The following buttons are located on the RCB:

• RESET button—When pressed, reboots the RCB as follows (number 3 in **Figure *2***):

  • Short press reboots the RCB and the reset-reason logs the button press event. The press event is logged in the RCB FPGA register.

  • When pressed for more than 10 seconds, the RCB reboots with an option for BIOS recovery.

• Online/Offline button—When the RCB is offline and if the button is pressed (short press), the RCB starts booting. When the RCB is online and if the button is pressed for four seconds or more (long press), the RCB shuts down (number 9 in **Figure *2***).

4. Security Problem Definition

4.1 Operational Environment Assumptions

This section includes assumptions about the environment where the product operates established by [ANNEXD1M] and [ANNEXD2M].

Assumption	Description
Physical protection	The product must be physically protected by its operational environment and not subject to physical attack, that could compromise its security or interfere with its proper operation.
Limited functionality	The product shall only provide the routing and network filtering functionality as its primary function, and shall not provide any other functionality or service that can be considered general purpose.
Trusted administration	Administrators are fully trusted members and look after the best security interests of the organization. They must be properly trained and free of malicious intent or conflict of interest in administering the product.
Periodic Updates	The product's firmware/software is updated as updates are released to correct known vulnerabilities.
Credentials protection	All credentials, especially the administrator's credentials, shall be properly protected by the organization using the product.

Table 4 Operational Environment Assumptions

4.2 Assets to protect

This section describes the assets that the TOE's security features protect established by [ANNEXD1M] and [ANNEXD2M].

Asset	Description
AC. Administration	Product and information management interfaces transmitted through them, in both directions, which must be protected in Confidentiality, Traceability, Authenticity and Integrity.
AC.PSS	Configuration data and audit logs must be protected in Integrity.
AC.PSC	Credentials and keys that must be protected in confidentiality and Integrity.
AC.Updates	Product updates likely to affect your configuration and functionality, which must be protected in integrity and Authenticity.
AC.Communications	Product communications, established between your own components and management systems that must be protected in Confidentiality, Integrity and Authenticity.

Table 5 Assets to protect

4.3 Threats description

This section describes the threats mitigated by the security features of the TOE established by [ANNEXD1M] and [ANNEXD2M].

Threats	Description
A.NOAUT	Unauthorized administrator access: An attacker can gain unauthorized administration access by posing as an administrator to the product, posing as the product to an administrator, replaying an administration session, or performing man-in-the-middle attacks
A.CRYPTO	Weak cryptographic mechanisms: Use in the product of cryptographic mechanisms or weak key lengths that allow an attacker compromising you, primarily through force attacks gross.
A.COM	Unauthorized communication protocols: Use of unauthorized protocols that allow an attacker to compromise the integrity and confidentiality of critical product communications.
A.ACT	Malicious update: an attacker can perform a malicious update / malicious code that compromises the functionality of the product.
A.AUD	Undetected Activities: An attacker may attempt to gain access, change or modify the security features of the product without the administrator knowledge.
A.PSC	Compromise of critical security parameters: an attacker can compromise critical security parameters and gain unauthorized access monitoring of the product and its critical data.
A.FUN	Failure of security functionalities: An external attacker can take advantage of flaws in the declared security functionalities of the product and could access, change or modify information, functionalities of security or network traffic on the product.
A.NOAUTUSR	unauthorized user access: An attacker can obtain unauthorized access by posing as a user to the product, impersonating the product to a user, replaying a session user, or performing man-in-the-middle attacks.
A.CRE	Credential Compromise: An attacker can take advantage of using of weak or unprotected credentials, to gain privileged access to the product.
A.RED	Network attack: An attacker gains access to the network, being able to perform mappings of the machines that reside in it and obtain data from IP address, services or any other information that allows you to launch attacks on those machines and services.

Table 6 Threats description

5. Security Functions

The security functions specified in this section are based on the requirements established by [ANNEXD1M] and [ANNEXD2M].

5.1 TOE Administration

Requirement	Description	Threat mitigated
ADM.1	The product must define at least the *administrator* role and be able to associate users to roles.	A.NOAUT
ADM.2	The product must be capable of managing the following functionalities: • Product management locally and remotely. • Configuration of the session termination time or blocking when detecting inactivity. • Update the TOE software • Update the TOE configuration • Configure audit behaviour • Configure the access banner	A.NOAUT
ADM.3	The TOE must ensure that only an user with administration rights will be able to perform the activities described in **ADM.2**.	A.NOAUT

Table 7 TOE Administration Security Functional Requirements

5.2 Identification and Authentication

Requirement	Description	Threat mitigated
IAU.1	The product must identify and authenticate each user before granting access.	A.NOAUT A.NOAUTUSR
IAU.2	The product must implement mechanisms that prevent brute force authentication attacks.	A.CRE
IAU.3	The TOE must have password management capabilities: • Password must be set to a minimum length of 12 characters. • Password must be composed of lower case letters, upper case letters, numbers and special characters [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “].	A.CRE
IAU.4	The TOE must log out a user after a configurable inactivity time.	A.NOAUT

IAU.5	When access is made using default credentials or a user has no assigned credentials yet, the TOE shall force the change of credentials on the next access.	A.CRE

Table 8 Identification and Authentication Security Functional Requirements

5.3 Trusted Channels

Requirement	Description	Threat mitigated
COM.1	Protection of information in transit. The TOE shall establish secure channels when exchanging sensitive information with any authorized entity: audit server or between different parts of the product, using SSHv2 or higher with the following cryptographic mechanisms: - SSH: see **Table 10**.	A.CRYPTO A.COM
COM.2	The product must allow communications through secure channels initiated by itself or by authorized entities.	A.COM
COM.3	The TOE will use digital certificates for authentication when using any of the protocols defined in **COM.1**.	A.COM
COM.4	Protection of the administration channel information. The TOE shall establish secure channels when exchanging information with the remote administrator, using SSHv2 or higher; with the following cryptographic mechanisms listed: - SSH: see **Table 10**.	A.CRYPTO A.COM

Table 9 Supported algorithms on the TOE

	Cryptography
Encryption algorithms	aes256-ctr
Hash algorithms	hmac-sha2-256, hmac-sha2-512
Key Exchange	ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521

Table 10 Ciphersuites used by SSH protocol

5.4 Cryptography

Requirement	Description	Threat mitigated
CIF.1	The TOE shall only allow the use of cryptographic mechanisms: SSH and encrypted data authorized in accordance with the provisions of guide CCN-STIC-807 (See **Table 12**). The key strength used shall be the indicated in that guide for ENS (Esquema Nacional de Seguridad) Credentials for accounts are stored in the TOE encrypted with hmac-sha2-512. Private keys where the original value is needed to use them are stored with AES-GCM-256 encryption.	A.CRYPTO A.COM

Table 11 Cryptography Security Functional Requirements

Cryptography	
SSH	
Encryption algorithms	aes256-ctr
Hash algorithms	hmac-sha2-256, hmac-sha2-512
Key Exchange	ecdh-sha2-nistp256,ecdh-sha2-nistp384, ecdh-sha2-nistp521
Encryption for sensitive data	
Hash algorithms	hmac-sha2-512 for account passwords.
Symmetric encryption	AES-GCM-256 (PBKDF2) for private keys
Firmware digital signature	
Digital Signature	RSA 3072

Table 12 CIF.1 Compliant crypto algorithm on the TOE

5.5 Trusted updates

Requirement	Description	Threat mitigated
ACT.1	The TOE shall offer the possibility to check the current firmware/software version and may initiate updates manually and no other.	A.ACT

ACT.2	The TOE shall use a digital signature that are authorized in CCN-STIC-807 to authenticate firmware/software updates before installing them. Note: The firmware is signed by using **RSA 3072.**	A.ACT
ACT.3	Firmware/software update will only be allowed for users with *administrator* role.	A.ACT

Table 13 Trusted Updates Security Functional Requirements

5.6 Audit

Requirement	Description	Threat mitigated
AUD.1	The product shall generate audit records when any occur of the following events: a) At the beginning and end of the audit functions b) Login and logout of registered users. c) Changes in user credentials. d) Changes in product configuration: - Initiation of a manual update, and the result of the update attempt - Resetting passwords e) Events related to the functionality of the product: - Initiation, termination or failure of the trusted channel - Failure to establish an SSH session f) Generation, import or elimination of cryptographic keys.	A.AUD
AUD.2	Audit logs shall contain at least the following information: date and time of the event, type of event identified, result of the event, the user producing the event.	A.AUD
AUD.3	The following access policy shall be applied to the audit records: • Reading: authorized users. • Modification: not allowed. • Deletion: only administrators.	A.AUD
AUD.4	The generated audit information must be able to be stored in the TOE itself and transmit the generated audit information to an external entity using a secure **COM.1** channel.	A.AUD
AUD.5	The product shall be able to overwrite previous audit following the rule: *oldest log is overwritten* when the storage space is full	A.AUD

Table 14 Audit Security Functional Requirements

5.7 Protection of credentials and sensitive data

Requirement	Description	Threat mitigated
PSC.1	In the case where the TOE stores credentials, private keys these shall not be stored in the clear text. Cryptologic protection mechanisms compliant with CIF.1 shall be used.	A.PSC

Table 15 Protection of credentials and sensitive data Security Functional Requirements

5.8 Protection of the product and its services

Requirement	Description	Threat mitigated
PRO.1	The TOE shall be able to perform a test during boot or power up of the product to verify the integrity of the software/firmware.	A.FUN

Table 16 Failure protection Security Functional Requirements

5.9 Router

Requirement	Description	Threat mitigated
ROU.1	The product shall be able to manage ports, enabling or disabling them for use, as well as assigning priorities to them.	A.RED
ROU.2	The product shall forward network traffic through its ports at network layer (layer 3) level of the Open Systems Interconnection model (ISO / IEC 7498-1) according to a routing table	A.RED

Table 17 Router Security Functional Requirements

5.10 Switch

Requirement	Description	Threat mitigated
SWI.1	The product must be able to manage ports, enabling or disabling them for use, as well as assigning priorities to them.	A.RED
SWI.2	The product must forward network traffic through its ports at the data link layer (layer 2) of the Open Systems Interconnection (OSI) model (ISO/IEC 7498-1), using physical addressing or Ethernet Media Access Control (MAC).	A.RED
SWI.3	The product must have the capability for Virtual LAN (VLAN) segmentation.	A.RED

Table 18 Switch Security Functional Requirements

6. References

[ANNEXD1M]	Guía de Seguridad de las TIC CCN-STIC 140 (Taxonomía de productos STIC - Anexo D.1-M: Enrutadores) September 2023.
[ANNEXD2M]	Guía de Seguridad de las TIC CCN-STIC 140 (Taxonomía de productos STIC - Anexo D.2-M: Enrutadores) September 2023.
[CCN-STIC-2001]	CCN-STIC-2001 Definición LINCE
[CCN-STIC-2002]	CCN-STIC-2002 Metodología de Evaluación para la Certificación Nacional
[CCN-STIC-2003]	CCN-STIC-2003 Plantilla para la Declaración de Seguridad de la Certificación Nacional Esencial de Seguridad (LINCE)
[CCN-STIC-2004]	CCN-STIC-2004 Plantilla del Informe Técnico de Evaluación de la Certificación Nacional Esencial de Seguridad (LINCE)

7. Terms and Acronyms

The following table shows the acronyms used in this document.

ACL	Access Control List
BGP	Border Gateway Protocol
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de Información y las Comunicaciones
ENS	Esquema Nacional de Seguridad
CLI	Command Line Interface
VLAN	Virtual local area network
VXLAN	Virtual Extended Local Area Network
IP	Internet Protocol
MAC	Media Access Control
RFS	Requisito Fundamentales de Seguridad
TOE	Target of evaluation
ISP	Internet Service Provider