Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Juniper Networks Junos OS Evolved 23.4R1 for PTX10001-36MR

Version 1.0, 19 May 2025

Document reference: AISEP-CC-CR-2025-EFT-T045-CR-V1.0
(Certification expires five years from certification report date)

Table of contents

Executive Summary

This report describes the findings of the IT security evaluation of Juniper Networks Junos OS Evolved 23.4R1 for PTX10001-36MR appliances against Common Criteria approved Protection Profiles (PPs).

The Target of Evaluation (TOE) is a fixed configuration packet transport router that is non-virtual and non-distributed network device. It is a purpose built platform that does not provide any general-purpose computing capabilities.

This report concludes that the Target of Evaluation (TOE) has complied with the following PPs [4]:

- Collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23 March 2020. (CPP_ND_V2.2E)
- PP-Module for MACsec Ethernet Encryption, Version 1.0, 02 March 2023 (MOD_MACSEC_V1.0)

Additionally, the above PPs are grouped together using certified PP-Configurations. This evaluation used the following PP-Configuration [4]:

- PP-Configuration for Network Devices and MACsec Ethernet Encryption Version: 1.0, 2023-03-29 (CFG_NDcPP-MACsec_V1.0)

The evaluation was conducted in accordance with the Common Criteria and the requirements of the Australian Information Security Evaluation Program (AISEP). The evaluation was performed by Teron Labs with the final Evaluation Technical Report (ETR) submitted on 02 May 2025.

With regard to the secure operation of the TOE, the Australian Certification Authority (ACA) recommends that administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are understood
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings
- verify the hash of any downloaded software, as present on the Juniper website
- the system auditor should review the audit trail generated and exported by the TOE periodically
- the administrator should update the device firmware and software in timely manners in response to the release of product updates due to known vulnerabilities.

Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Introduction

Overview

This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

Purpose

The purpose of this Certification Report is to:

- report the certification of results of the IT security evaluation of the TOE against the requirements of the Common Criteria [1,2,3] and Protection Profiles [4]
- provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target [8] which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

Identification

The TOE is Junos OS Evolved 23.4R1 for PTX10001-36MR.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Junos OS Evolved 23.4R1 for PTX10001-36MR
Software version	Junos OS Evolved 23.4R1
Hardware platforms	PTX10001-36MR
Security Target	Security Target Juniper Junos OS Evolved 23.4R1 for PTX10001-36MR, Juniper Networks, Version 1.0, 23 March, 2025
Evaluation Technical Report	Evaluation Technical Report 1.1, dated 24 April 2051 Document reference EFT-T045-ETR 1.1
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant, April 2017, Version 3.1 Rev 5
Methodology	Common Methodology for Information Technology Security, April 2017 Version 3.1 Rev 5
Conformance	Collaborative Protection Profile for Network Devices (NDcPP), Version 2.2e, 23 March 2020. (CPP_ND_V2.2E)

	PP-Module for MACsec Ethernet Encryption Version: 1.0, 02 March 2023 (MOD_MACSEC_V1.0) PP-Configuration for Network Devices and MACsec Ethernet Encryption Version: 1.0, 2023-03-29 (CFG_NDcPP-MACsec_V1.0)
Developer	Juniper Networks, Inc. 1133 Innovation Way, Sunnyvale California 94089 United States of America
Evaluation facility	Teron Labs Level 2, 14 Moore St, Canberra ACT 2601 Australia

Target of Evaluation

Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, its security policies and its secure usage.

Description of the TOE

The Target of Evaluation (TOE) is the Juniper Networks Junos OS Evolved 23.4R1 for PTX10001-36RM, a non-virtual and non-distributed network device that meets the security requirements of the Base-PP and PP-Module in accordance with the PP-Configuration. The TOE is a part of Juniper Networks' software-defined networking (SDN)-enabled routing platforms, designed to support a scale-out core backbone architecture for consistent user experiences across various geographies.

The PTX10001-36RM is a fixed configuration packet transport router, ideal for cloud and communication provider networks requiring transit-focused IP/MPLS applications. It features a compact 1U chassis, making it suitable for space and power constrained environments, and offers significant power efficiency at 0.14 watts/Gbps. The router supports up to 4 million IPv4 Forward Information Base (FIB), deep buffers, and integrated 100GbE and 400GbE MACsec capabilities, operating at 9.6 Tbps with 36 multi-rate ports. The Juniper Express 4 Silicon line card enhances performance with low latency, MACsec encryption, and dynamic table memory allocation, ensuring high packet performance and power efficiency.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.3 of the Security Target [8].

TOE Physical Boundary

The TOE is the complete appliance consisting of the Junos OS Evolved 23.4R1 firmware running on the PTX10001-36MR. The TOE is contained within the physical boundary of the PTX10001-36MR. The PTX10001-36MR fitted with Express 4 Silicon linecard. The line card is powered by Juniper Express 4 Silicon, the industry's first inline MACsec-enabled chip for 400GbE networks

The install image provided for the TOE is:

- junos-evo-install-ptx-fixed-x86-64-23.4R1.10-EVO.iso

The firmware version reflects the detail reported for the components of the Junos OS when the “show version” command is executed on the device.

The TOE parts included in the physical boundary are described below:

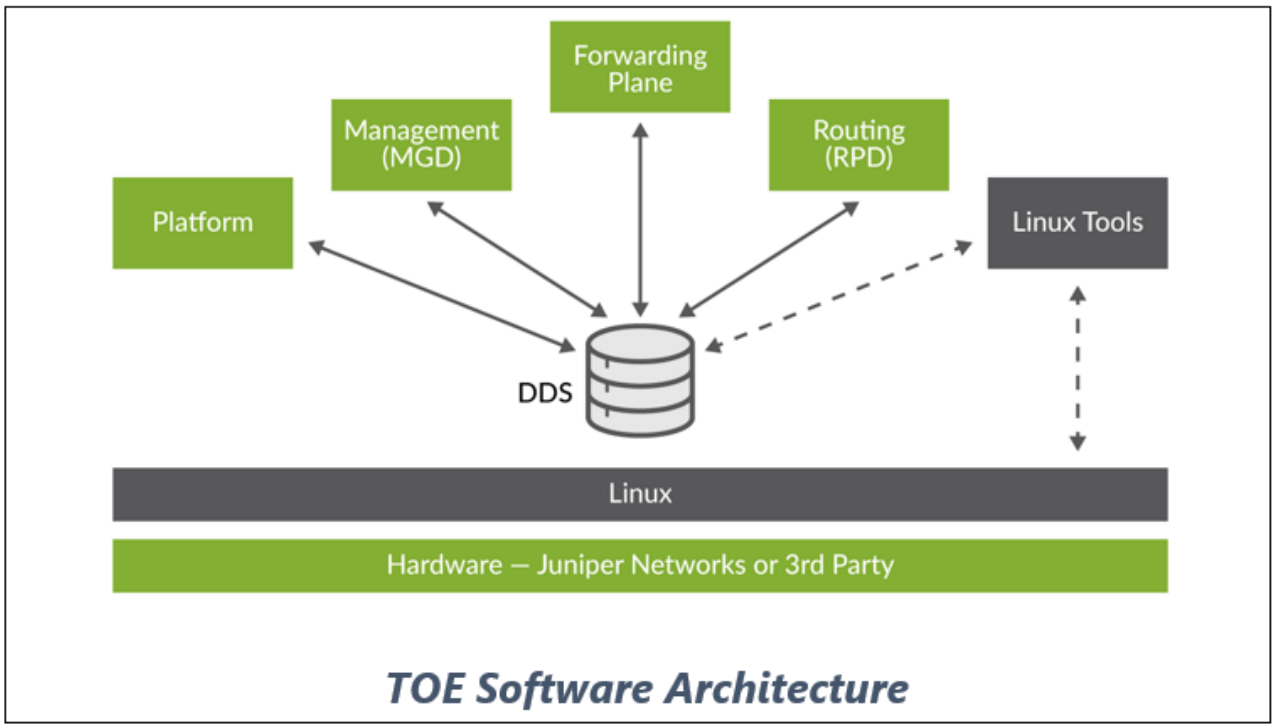
Part of the TOE	Identification	Description
Chassis	PTX10001-36MR	The hardware platform and the casing of the TOE, including all physical connectivity to the other networks and power sources.
Line Card	Express 4 Silicon	Highly scalable, next generation ASIC in the Express silicon family, an inline MACsec for 400GbE chips that supports universal multirate QSFP56-DD.
TOE Software	Junos OS Evolved 23.4R1	The software included in the TOE is Junos OS Evolved 23.4R1. The software is distributed as the specific Junos installation package: - junos-evo-install-ptx-fixed-x86-64-23.4R1.10-EVO.iso
Security Guidance	Juniper Junos OS Evolved 23.4R1 for PTX10001-36MR Common Criteria Guidance Supplement v1.0	The Common Criteria Guidance supplement for the TOE. Security Guidance is distributed in Portable Document Format (PDF) through the Juniper web site.

Architecture

The TOE architecture consists of a hardware chassis, integrated line cards, and the Junos OS Evolved operating system, forming a complete network appliance. The chassis, PTX10001-36MR, is a compact 1U platform designed for deployment in constrained environments such as Internet exchange points, remote central offices, and cloud-hosted services. It supports high-performance networking with 36 multi-rate ports, including 24 400GbE and 12 100GbE ports, enabling seamless migration between 100GbE and 400GbE deployments. With a power-efficient design consuming only 0.14 watts per Gbps, it provides deep buffering, up to 4 million IPv4 FIB entries, and full MACsec encryption across all ports for secure data transmission.

The line card within the TOE is powered by Juniper Express 4 Silicon, an advanced networking chip that delivers low-latency processing, high-speed encryption, and dynamic memory allocation. Supporting multi-rate QSFP56-DD ports, it ensures high-performance packet processing without compromising power efficiency. The TOE's software component, Junos OS Evolved, is a Linux-based operating system designed for software-defined networking (SDN). It decouples application processes from the hardware, creating a flexible and scalable infrastructure where protocols and services communicate efficiently. This architecture allows the TOE to handle demanding networking environments while maintaining optimal performance, security, and adaptability.

The graphical description of the TOE software Architecture is shown in the below figure.



Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies.

The scope of the evaluation was limited to those claims made in the Security Target [8].

Evaluated Functionality

Functional tests performed during the evaluation were taken from the Protection Profiles [4] and Supporting Documents [12] and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

Non-TOE Hardware/Software/Firmware

The TOE is the entire network appliance. Yet, it does require external IT devices to be properly operated. Specifically, the TOE requires the following items in the network environment:

- Syslog server supporting SSHv2 connections to send audit logs
- SSHv2 client for remote administration
- serial connection client for local administration

Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

Australian Government users should refer to the *Australian Government Information Security Manual* [5] for policy relating to using an evaluated product in an unevaluated configuration.

The following components are considered outside of the scope of the TOE:

- use of telnet, since it violates the Trusted Path requirement set
- use of File Transfer Protocol, since it violates the Trusted Path requirement set
- use of Simple Network Management Protocol, since it violates the Trusted Path requirement set
- use of SSL and TLS, including management via JUNOScript, since it violates the Trusted Path requirement set
- The TOE only includes the PTX10001-36MR chassis. No other hardware platforms must be used
- 3rd party applications and tools allowed by the Junos OS Evolved architecture must not be used
- No user should be granted super-user or Linux root account privileges. All administrative tasks for the TOE must be performed exclusively through the Command Line Interface (CLI).

TOE Security Policy

The TOE Security Policy is a set of rules that defines the required security behaviour of the TOE; how information within the TOE is managed and protected. The Security Target [8] contains a summary of the functionality that is evaluated.

Secure Delivery

There are several mechanisms provided in the delivery process to ensure that a customer receives a product that has not been tampered with. The customer should perform the following checks upon receipt of a device to verify the integrity of the platform:

- shipping label - Ensure that the shipping label correctly identifies the correct customer name and address as well as the device
- outside packaging - Inspect the outside shipping box and tape. Ensure that the shipping tape has not been cut or otherwise compromised. Ensure that the box has not been cut or damaged to allow access to the device
- inside packaging - Inspect the plastic bag and seal. Ensure that the bag is not cut or removed. Ensure that the seal remains intact.

If the customer identifies a problem during the inspection, they should immediately contact the supplier providing the order number, tracking number and a description of the identified problem to the supplier.

Additionally, there are several checks that can be performed to ensure that the customer has received a box sent by Juniper Networks and not a different company masquerading as Juniper Networks. The customer should perform the following checks upon receipt of a device to verify the authenticity of the device:

- verify that the device was ordered using a purchase order. Juniper Networks devices are never shipped without a purchase order
- when a device is shipped, a shipment notification is sent to the e-mail address provided by the customer when the order is taken. Verify that this e-mail notification was received and contains the following information:
    - purchase order number
    - Juniper Networks order number used to track the shipment
    - carrier tracking number used to track the shipment
    - list of items shipped including serial numbers

- address and contacts of both the supplier and the customer

- verify that the shipment was initiated by Juniper Networks, by performing the following tasks:
  - compare the carrier tracking number of the Juniper Networks order number listed in the Juniper Networks shipping notification with the tracking number on the package received
  - log on to the Juniper Networks online customer support portal at https://www.juniper.net/customers/csc/management to view the order status
  - compare the carrier tracking number or the Juniper Networks order number listed in the Juniper Networks shipment notification with the tracking number on the package received.

Installation of the TOE

The Configuration Guide [6] contains all relevant information for the secure configuration of the TOE.

Version Verification

The verification of the TOE is largely automatic, including the verification using hashes. The TOE cannot load a modified image. Valid software images can be downloaded from https://www.juniper.net. In addition to the automated verification, the site includes individual hashes for each image. The administrator should verify the hash of the software before installing it into the hardware platform.

Security Administrators are able to query the current version of the TOE firmware using the CLI command 'show version'.

Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. The evaluated configuration guide (System Admin Guide) document for the Juniper Junos OS Evolved 23.4R1 for PTX10001-36MR is available for download at https://www.juniper.net/documentation. The title is:

- *Junos OS Evolved Common Criteria Evaluated Configuration Guide for PTX10001-36MR Published 2025-03-25 Release 23.4R1* [6]

All Common Criteria guidance material is available at https://www.commoncriteriaportal.org.

The *Australian Government Information Security Manual* is available at https://www.cyber.gov.au/ism [5].

Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

The network device is assumed to be physically secured within its operational environment, protected from physical attacks that could compromise its security or interfere with its physical connections and correct operation. This level of protection is expected to be sufficient to safeguard the device and the sensitive data it handles.

The TOE is expected to provide networking functionality as its primary purpose and should not offer any general-purpose computing capabilities, such as running compilers or user applications unrelated to its networking functions. This ensures that the device remains focused solely on its intended security and networking roles.

The network device's administrator(s) are assumed to be trustworthy, acting in the best interests of the organisation's security. This includes being well-trained, adhering to established policies, and following all guidance documentation. Administrators are responsible for ensuring that passwords and credentials used within the TOE are strong and secure. The TOE is not expected to protect against a malicious administrator who deliberately seeks to bypass or compromise its security features.

The TOE's firmware and software are assumed to be regularly updated by an administrator, particularly in response to newly discovered vulnerabilities. This ensures that the TOE remains protected against emerging threats.

The credentials (such as private keys) used by administrators to access the TOE must be securely protected on any platform where they are stored. Administrators must also ensure that sensitive residual information, including cryptographic keys, keying material, PINs, and passwords, is not accessible to unauthorised individuals when networking equipment is discarded or removed from service.

The TOE is assumed to be connected to distinct networks in a way that ensures its security policies are enforced on all relevant network traffic flowing between these networks.

Evaluation

Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the relevant Protection Profiles [4] and Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 5, Parts 2 and 3 [1, 2].

Testing methodology was drawn from Common Methodology for Information Technology Security, April 2017 Version 3.1 Revision 5 [3] and relevant Supporting Documents [12].

The evaluation was carried out in accordance with the operational procedures of the Australian Information Security Evaluation Program [10].

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security [9] and the document *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs* [13] were also upheld.

Functional Testing

All functional tests performed by the evaluators were taken from the Protection Profiles [4] and Supporting Documents [12]. The tests were designed to provide the required testing coverage for the security functions claimed by the TOE.

Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report [11]. CAVP certificate references, organised by the applicable Security Functional Component, are given in the Security Target [8].

Penetration Testing

The evaluators performed the evaluation activities for vulnerability assessment specified by the NDcPP Supporting Document [12] that follow a flaw hypothesis methodology. Accordingly, four types of flaw hypotheses have been considered:

- Type 1 - public vulnerabilities
- Type 2 - ND-iTC (Network international Technical Community) sourced
- Type 3 - evaluation team generated
- Type 4 - tool generated.

The evaluators conducted a review of public vulnerability databases and technical community sources to determine potential flaw hypotheses using searches that include TOE device name and components, protocols supported by the

TOE and terms relating to the device type of the TOE. These searches were conducted up to the **03 December 2024** coinciding with the conclusion of the evaluation. There were no identifiable Type 2 hypotheses for this evaluation.

The evaluation team devised one test to check a potential vulnerability within the TOE's boot process. The evaluation team also conducted tool-generated vulnerability testing of the TOE as per the Supporting Document [12]

Based on the results of this testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

Certification

Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

Assurance

This certification is focused on the evaluation of product compliance with Protection Profiles that cover the technology area of network devices. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profiles cover the necessary security functionality expected of the evaluated product and known threats will have been addressed.

The analysis is supported by testing as outlined in the PP Supporting Document and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the Protection Profiles (PP). PP provides assurance by providing a full Security Target, and an analysis of the Security Functional Requirements in that Security Target, guidance documentation, and a basic description of the architecture of the TOE.

Certification Result

Teron Labs **has determined** that the TOE upholds the claims made in the Security Target [8] and **has met** the requirements of the Protection Profiles CPP_ND_V2.2E [4.a], MOD_MACSEC_V1.0 [4.b] and PP configuration for NDcPP and MACsec [4.c].

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [7], the Australian Certification Authority **certifies** the evaluation of the Juniper Junos OS Evolved 23.4R1 for PTX10001-36MR performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the Security Target [8] have met the requirements of all relevant Protection Profiles [4].

Certification is not a guarantee of freedom from security vulnerabilities.

Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian Government users. For further guidance, Australian Government users should refer to the Australian Government Information Security Manual [5].

In addition to ensuring that the assumptions concerning the operational environment are fulfilled, and the guidance document is followed, the Australian Certification Authority also recommends that users and administrators:

- ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
- configure and operate the TOE according to the vendor's product administrator guidance and pay attention to all security warnings

- maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
- verify the hash of any downloaded software, as present on the https://www.juniper.net website
- the system auditor should review the audit trail generated and exported by the TOE periodically

Annex – References and Abbreviations

References

1. *Common Criteria for Information Technology Security Evaluation Part 2: Security functional components April 2017, Version 3.1 Revision 5*

2. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components April 2017, Version 3.1 Revision 5*

3. *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, April 2017, Version 3.1 Revision 5*

4. Protection Profiles:

    a) *collaborative Protection Profile for Network Devices, Version 2.2e, 23 March 2020 (CPP_ND_V2.2E)*

    b) *PP-Module for MACsec Ethernet Encryption Version: 1.0, 02 March 2023 (MOD_MACSEC_V1.0)*

    c) *PP-Configuration for Network Devices and MACsec Ethernet Encryption Version: 1.0, 2023-03-29 (CFG_NDcPP-MACsec_V1.0)*

5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism

6. Junos OS Evolved Common Criteria Evaluated Configuration Guide for PTX10001-36MR Published 2025-03-25 Release 23.4R1

7. *Evaluation Technical Report Junos OS Evolved 23.4R1 for PTX10001-36MR Version 1.1, dated 24 April 2025* (Document reference EFT-T045-ETR 1.1)

8. *Security Target Juniper Junos OS Evolved 23.4R1 for PTX10001-36MR, Juniper Networks, Version 1.0, 23 March, 2025*

9. *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 July 2014*

10. *AISEP Policy Manual (APM):* https://www.cyber.gov.au/sites/default/files/2019-03/AISEP_Policy_Manual.pdf

11. Entropy Documentation:

    a) *Junos OS Physical Entropy Source – Intel Xeon D-2100 Series (Skylake) 18 Core Die with FCBGA2518 Package, Version 1.0, 27 November 2023*

12. Protection Profile Supporting Documents

    a) *Supporting Document, Evaluation Activities for Network Device cPP, Version 2.2, December-2019*

    b) *Supporting Document, Mandatory Technical Document, PP-Module for MACsec Ethernet Encryption, Version 1.0, 23-Mar-2023*

13. *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0*

Abbreviations

AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
ASE	Advanced Encryption Standard
ASIC	Application Specific Integrated Circuit
CAVP	Cryptographic Algorithm Validation Program
CCRA	Common Criteria Recognition Arrangement
CEM	Common Criteria Evaluation Methodology
CLI	Command Line Interface
cPP	Collaborative Protection Profile
Gbps	Gigabits per second
IP	Internet Protocol
IPv4	Internet Protocol version 4
MACsec	Media Access Control Security
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
RE	Routing Engine
SDN	Software-defined networking
SSH	Secure Shell
ST	Security target
TOE	Target of Evaluation

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate