Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Juniper SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11

Version 1.0, 30 March 2026

Document reference: AISEP-CC-CR-2026-EFT-T048-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, Juniper SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11 appliances against Common Criteria approved *Protection Profiles (PPs).*

The Target of Evaluation (TOE) is the Juniper SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11, which are Session Smart Routing (SSR) appliances, allowing the development of agile, secure, and resilient applications and solutions with Wide Area Network (WAN) connections.

This report concludes that the TOE has complied with the following *PPs [4]:*

- *collaborative Protection Profile for Network Devices, Version: 2.2e, 23 March 2020 (CPP_ND_V2.2E).*
- *PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (MOD_CPP_FW_V1.4E).*

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

- *PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.4 +Errata20200625, 25 June 2020 (CFG_NDcPP-FW_V1.4E).*

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 12 March 2026.

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

- Review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.
- 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
- The ProLiant DL345 Gen11 platform was tested running on an AMD EPYC 9575F. If using other ProLiant DL345 Gen11 configurations, the algorithm assurance only covers CPUs from the same CPU family.

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 [8]* 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 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 Juniper SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Juniper SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11
Software version	7.0.1
Hardware platforms	SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500 and HPE ProLiant DL345 Gen 11
Security Target	Security Target Juniper SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11, Version 1.0, 04 March 2026
Evaluation Technical Report	Evaluation Technical Report 1.0, dated 12 March 2026 Document reference EFT-T048-ETR 1.0

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, Version: 2.2e, 23 March 2020 (CPP_ND_V2.2E). ▪ PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (MOD_CPP_FW_V1.4E). ▪ PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.4 +Errata20200625, 25 June 2020 (CFG_NDcPP-FW_V1.4E).
Developer	Juniper Networks, Inc.
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 TOE is the Juniper SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11, which are Session Smart Routing (SSR) appliances, allowing the development of agile, secure, and resilient applications and solutions with Wide Area Network (WAN) connections.

Each TOE variant includes the same software and may be provisioned and configured by the user to be a Session Smart Router (in short: Router) or a Session Smart Conductor (in short: Conductor). The TOE configured as a Router implements the data plane and control plane functions of the TOE and performs most functions. The TOE configured as a Conductor implements a centralized management and policy engine allowing provisioning and management of several Routers. A Conductor also acts as an information aggregation repository.

The TOE implements all security functions of a network device. It also implements a stateful traffic filtering firewall to guard access to the protected network. Instances of the TOE configured as Routers are deployed in various data centres, branches, and other facilities to protect the network connection. The Routers are associated to one or more instances of TOE configured as Conductors for information aggregation, life-cycle management, and configuration management. The Conductor may additionally be connected to other services to utilize the collected information.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.4 of the *Security Target [8].*

TOE Physical Boundary

The physical boundary of the TOE includes all hardware and software parts and the security guidance of the TOE. The parts of the TOE included in the physical boundary are detailed in *Table 1*.

Part of the TOE	Identification	Description
TOE Hardware	SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500 and HPE ProLiant DL345 Gen 11	The hardware platform and the casing of the TOE. Includes the processor, the memories, and the persistent storage.
TOE Software	Juniper SSR Software v7.0.1	The SSR-OS included in the TOE is Juniper SSR Software v7.0.1. TOE software is distributed as the following installation package: ▪ SSR-7.0.1-1.r1.el9.x86_64.ibu-v1.iso

Security Guidance	SSR v7.0.1 Common Criteria Install and Configuration v1.0	The Common Criteria Guidance supplement for the TOE. The security guidance is distributed as a document in PDF format.

Table 1 -Parts Included in the physical boundary of the TOE

TOE Hardware is the platform on which the TOE Software is executed. Only the platforms identified in *Table 1* are included in the evaluation. The technical characteristics of the hardware platforms are summarized in *Table 2.*

Platform	CPU	Microprocessor	Networking
Juniper SSR120	4-Core Intel Atom C3558	Denverton	1 x RJ45 Console Port 4 x 1 GbE Ethernet Ports 2 x 1 GbE RJ-45/SFP Combo Ports
Juniper SSR130	8-Core Intel Atom C3758	Denverton	1 x RJ45 Console Port 6 x 1 GbE Ethernet Ports 2 x 1 GbE RJ-45/SFP Combo Ports
Juniper SSR1200	8-Core AMD EPYC 3251	Snowy Owl	1 x RJ45 Console Port 1 x 1 GbE Management port 4 x 1/10 GbE SFP+ ports 7 x 1 GbE Ethernet ports
Juniper SSR1300	16-Core Intel Xeon Gold 6208U	Cascade Lake	1 x RJ45 Console Port 1 x 1 GbE Management port 4 x 10 GbE SFP+ ports 4 x 1/10 GbE SFP+ ports 4 x 1 GbE Ethernet ports
Juniper SSR1400	24-Core Intel Xeon Gold 6212U	Cascade Lake	1 x RJ45 Console Port 1 x 1 GbE Management port 4 x 10 GbE SFP+ ports

			4 x 1/10/25 GbE SFP28 ports 4 x 1 GbE Ethernet ports
Juniper SSR1500	64-Core AMD EPYC 7713P	Milan	1 x RJ45 Console Port 1 x 1 GbE Management port 12 x 1/10/25 GbE SFP28 ports 4 x 1 GbE Ethernet ports
HPE ProLiant DL345 Gen11	AMD EPYC 9575F	EPYC	None. Choice of OCP or stand-up card, supporting NIC adapters BTO models pre-selected with a primary networking card.

Table 2 - TOE Hardware Variants

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 relies on the following external components to operate securely and as evaluated. These items are outside the TOE boundary and must be present and correctly configured in the operational environment.

- Syslog server supporting SSHv2 connections to send audit logs
- SSHv2 client for remote administration
- Local administration or the remote management workstation is required but not part of the TOE
- NTP Server is not part of the TOE
- Audit server is mandatory but not part of TOE
- Hardware platforms not explicitly included in the physical scope of the TOE, even if Juniper or HPE branded

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 Simple Network Management Protocol, since it violates the Trusted Path requirement set
- REST API must only be used over HTTPS, not over HTTP
- VPN Gateway and IPsec are not included in the TOE
- Intrusion Prevention System (IPS) functions are not included
- TLS uses X.509 certificates which are verified and validated by the TOE but is not part of the TOE
- The Juniper MIST for the management of the TOE is not included.

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 Network, 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 Guides [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/documentation/us/en/software/session-smart-router/docs/intro_downloading_iso/. 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 SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11is available for download at https://www.juniper.net/documentation. The title is:

- *SSR v7.0.1 Common Criteria Install and Configuration, Version 1.0, 03 March 2026 [6].*

All Common Criteria guidance material is available at https://www.commoncriteriaportal.org [1, 2, 3, 9, and 13].

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 organization'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.

For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).

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 unauthorized 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 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].*

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 **09 December 2025** coinciding with the conclusion of the evaluation. There was 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 with added security functionality including stateful traffic filter firewall functions. Organisations can have confidence that the scope of an evaluation against an ASD-approved Protection Profile covers 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 Documents and Protection Profile Module activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the *Protection Profiles (PPs) [4].* PPs provide 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_CPP_FW_V1.4E [4.b] and PP configuration for Network Device and Stateful Traffic Filter Firewalls [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 SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11 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 the *Network Device 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:

- Review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

- 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
- The ProLiant DL345 Gen11 platform was tested running on an AMD EPYC 9575F. If using other ProLiant DL345 Gen11 configurations, the algorithm assurance only covers CPUs from the same CPU family.

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 Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (MOD_CPP_FW_V1.4E).*

    c) *PP-Configuration for Network Device and Stateful Traffic Filter Firewalls, Version 1.4 +Errata20200625, 25 June 2020 (CFG_NDcPP-FW_V1.4E).*

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

6. *SSR v7.0.1 Common Criteria Install and Configuration, Version 1.0, 03 March 2026.*

7. *Evaluation Technical Report Juniper SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11* (Document reference EFT-T048-ETR 1.0)

8. *Security Target for Juniper SSR Software v7.0.1 on Juniper SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen 11, Version 1.0, 04 March 2026.*

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/2023-03/2022_AUG_REL_AISEP_Policy_Manual_6.3.pdf*

11. Entropy Documentation:

    a) *Entropy Assessment Report, Juniper SSR Software v7.0.1 on SSR120, SSR130, SSR1200, SSR1300, SSR1400, SSR1500, and HPE ProLiant DL345 Gen11, Version 1.0, dated 02 December 2025.*

12. Protection Profile Supporting Documents

    a) *Supporting Document, Evaluation Activities for Network Device cPP, December 2019, version 2.2 (CPP_ND_V2.2E_SD)*

    b) *Supporting Document, Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, Version 1.4 + Errata 20200625, June 2020 (MOD_CPP_FW _v1.4e_SD)*

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
API	Application programming interface
ASD	Australian Signals Directorate
ASIC	Application Specific Integrated Circuit
CA	Certificate Authority
CCRA	Common Criteria Recognition Arrangement
CLI	Command Line Interface
GbE	Gigabit Ethernet
HTTPS	Hypertext Transfer Protocol Secure
HPE	Hewlett Packard Enterprise
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
NTP	Network Time Protocol
PIN	Personal Identification Number
PP	Protection Profile
RJ-45	8-pin copper connection
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSR	Session Smart Router
SFP	Small Form factor Pluggable
SFP+	enhanced Small Form factor Pluggable
TOE	Target of Evaluation
VPN	Virtual Private Network

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