Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Juniper Junos OS 22.2R1 for SRX380

Version 1.0, 26 June 2023

Document reference: AISEP-CC-CR-2023-EFT-T034-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 22.2R1 for the SRX380 appliance against approved Protection Profiles (PPs).

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

- collaborative Protection Profile for Network Devices, version 2.2e, 23 March 2020 (CPP_ND)
- PP-Module for Intrusion Protection Systems (IPS), Version 1.0, 11 May 2021 (MOD_IPS)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (MOD_CPP_FW)
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1, 18 June 2020 (MOD_VPNGW)
- Network Device collaborative Protection Profile Extended Package (EP) MACsec Ethernet Encryption, Version 1.2, 10 May 2016.

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 21 June 2023.

With regard to the secure operation of the TOE, the Australian Certification Authority 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
- 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 Juniper website
- have a system auditor review the audit trail generated and exported by the TOE periodically.

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 and Protection Profiles [4.a – 4.e]
- 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 [7] 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 22.2R1 for SRX380.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Junos OS 22.2R1 for SRX380
Software version	22.2R1
Hardware platform	SRX380
Security Target	Security Target Junos OS 22.2R1 for SRX380, Version 1.0, June 13 2023
Evaluation Technical Report	Evaluation Technical Report 1.1, dated 21 June 2023 Document reference EFT-T034-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 Version 2.2e dated 23 March 2020 PP-Module for Intrusion Protection Systems (IPS), Version 1.0 dated 11 May 2021 PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 dated 25 June 2020 PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1 dated 18 June 2020 Extended Package MACsec Ethernet Encryption, Version 1.2, 10 May 2016
Developer	Juniper Networks, Inc. 1133 Innovation Way, Sunnyvale California 94089 United States of America
Evaluation facility	Teron Labs Unit 3, 10 Geils Court Deakin ACT 2600 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 Juniper Networks, Inc. Junos OS 22.2R1 for SRX380 services gateway appliance.

The Services Gateway appliance primarily supports the definition and enforcement of information flow policies among network nodes. The Services Gateway appliance provides for stateful inspection of every packet that traverses the network and provides central management to manage the network security policy. All information flow from one network node to another passes through an instance of the TOE. Information flow is controlled on the basis of network node addresses, protocol, type of access requested, and services requested. In support of the information flow security functions, the TOE ensures that security-relevant activity is audited, that its own functions are protected from potential attacks, and provides the security tools to manage all of the security functions. The TOE provides multi-site virtual private network (VPN) gateway functionality. The TOE also implements Intrusion Prevention System (IPS) functionality, capable of monitoring information flows to detect potential attacks based on pre-defined attack signature and anomaly characteristics in the traffic.

The appliance has been evaluated in the typical standalone mode and in cluster mode. In cluster mode a pair of devices are connected together and configured to operate like a single device to provide high availability. When configured as a cluster, the two nodes back up each other, with one node acting as the primary device and the other as the secondary device, ensuring stateful failover of processes and services in the event of system or hardware failure. If the primary device fails, the secondary device takes over processing of traffic.

The SRX Services Gateway appliance runs the Juniper Networks Junos operating system (Junos OS), Junos OS 22.2R1.

The appliance is physically self-contained, housing the software, firmware and hardware necessary to perform all router functions. The hardware consists of the Services Gateway appliance itself and various generic network media adaptors which allow the appliance to communicate with the different types of networks that may be required.

TOE Functionality

The TOE functionality that was evaluated is described in section 1.6 of the Security Target [7].

TOE physical boundary

The TOE is the Junos OS 22.2R1 firmware running on the SRX380 as listed in the table below. The TOE is contained within the physical boundary of the SRX380.

Chassis Model	Networking Ports
SRX380	• Four Mini PIM slots

- Sixteen 1Gb Ethernet RJ45 ports
- Four 10Gb SFP+ ports
- One console (RJ45 serial + mini-USB) port
- One Management RJ45 port

In the SRX380 the sixteen 1Gb RJ45 and four 10Gb SFP+ ports support MACsec.

Abbreviations:

IOC	Input / Output Card
Mini-PIM	Mini Physical Interface Module
mini-USB	mini Universal Serial Bus
RJ45	8-pin copper connection
SFP+	enhanced Small Form factor Pluggable

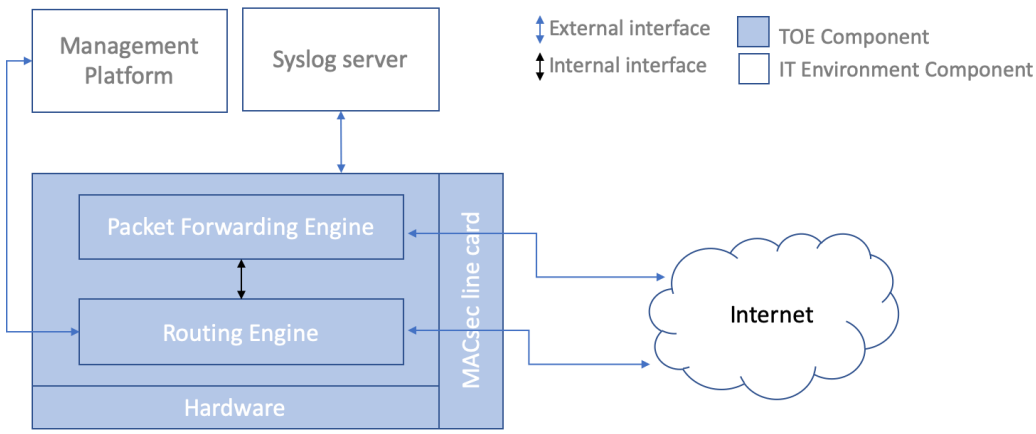
More information on the mini-PIM slots for the Juniper SRX380 is available in the Security Target [7] and the Juniper web site.

The jinstall image provided for the TOE is:

- junos-srxsme-22.2R1.9.tgz

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 physical boundary for the SRX380 model is shown in the figure below.



The TOE interfaces comprise the following:

- network interfaces which pass traffic
- management interface which handles administrative actions.

Architecture

The TOE consists of the following two major architectural components.

The Routing Engine (RE) runs the Junos firmware and provides Layer 3 routing services and network management for all operations necessary for the configuration and operation of the TOE. The RE also controls the flow of information through the TOE, including Network Address Translation (NAT) and all operations necessary for the encryption/decryption of packets for secure communication via the IPSec protocol.

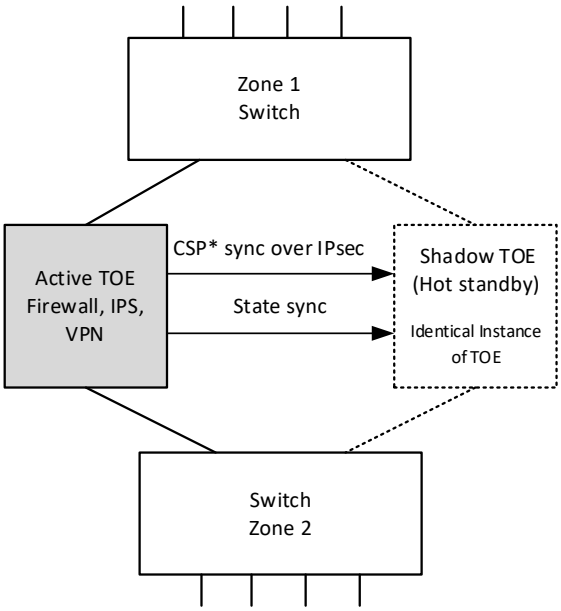
The Packet Forwarding Engine (PFE) provides all operations necessary for transit packet forwarding.

The Routing Engine and Packet Forwarding Engine perform their primary tasks independently, while constantly communicating through a high-speed internal link. This arrangement provides streamlined forwarding and routing control and the capability to run Internet-scale networks at high speeds.

The functions of the TOE can all be managed through the Junos firmware, either from a connected terminal console or via a network connection. All management, whether from a user connecting to a terminal or from the network, requires successful authentication. In the evaluated deployment the TOE is managed and configured via Command Line Interface, either via a directly connected console or over the network secured using the SSH protocol.

The MACsec line cards support MACsec between adjacent devices, all traffic communicated between the devices including frames for LLDP, DHCP, ARP, STP, Ethernet Control frames, etc. In the evaluated configuration MACsec must be configured individually on each point-to-point Ethernet link, such that a pair of MACsec devices (connected by a physical medium) protect Ethernet frames switched or routed from one device to the other.

To operate in high availability cluster mode the TOE must be paired with another identically configured TOE instance as shown in the diagram below. The secondary (shadow) TOE is invisible to the Zone 1 and Zone 2 networks until it is required to replace the previously active primary TOE and become the new active TOE. The state sync activities of the primary TOE required to maintain cluster mode place a strain on the primary TOE that makes this mode different to standalone mode. This is noticeable during TOE management activities as some commands take longer to complete.



* CSP – Critical Security Parameters

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 [7].

Evaluated functionality

Functional tests performed during the evaluation were taken from the Protection Profiles and Supporting Documents 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 provision of 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
- MACsec enabled peers
- IPsec enabled peers.

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 Secure Sockets Layer, including management via J-Web, JUNOScript and JUNOScope, since it violates the Trusted Path requirement set
- use of Command Line Interface account super-user and Junos root account.

Security

The TOE Security Policy is a set of rules that defines how information within the TOE is managed and protected. The Security Target [7] contains a summary of the functionality that is evaluated.

Usage

Evaluated configuration

The evaluated configuration is based on the default installation of the TOE with additional configuration implemented from specific guidance instructions. The Common Criteria document for this evaluation is *Junos OS, Common Criteria Guide for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC and SRX380 Devices, Release 22.2R1, 2022-11-21* [6].

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 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 the https://www.juniper.net support pages. 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 SRX380 running Junos OS 22.2R1 is available for download at https://www.juniper.net/documentation. The document is: *Junos OS, Common Criteria Guide for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC and SRX380 Devices, Release 22.2R1, 2022-11-21*.

Common Criteria 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 protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.

The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).

The administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organisation. This includes being appropriately trained, following policy and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy. The network device is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the device.

The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known security vulnerabilities.

The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.

The administrator must ensure that there is no unauthorised access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached 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.a – 4.e] 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], the relevant Supporting Documents [12.a – 12.d] and Extended Package [4.e].

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 draft 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 collaborative Protection Profile for Network Devices Supporting Document [12.a] which follow a flaw hypothesis methodology. In addition, the PP-Module for VPN Gateways Supporting Document [12.d] provides extra search term information for generating public vulnerability based flaw hypotheses. Accordingly, four types of flaw hypotheses have been considered:

- public vulnerabilities
- ND iTC (Network Device international Technical Community) sourced
- evaluation team generated
- tool generated.

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 firewall functions, VPN gateway functions, intrusion prevention functions and MACsec encryption. 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 Protection Profile Supporting Documents 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). 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 [7] and **has met** the requirements of the Protection Profiles CPP_ND [4.a], MOD_IPS [4.b], MOD_CPP_FW [4.c], MOD_VPNGW [4.d] and MACsecEP [4.e].

After due consideration of the conduct of the evaluation as reported to the certifiers, and of the Evaluation Technical Report [8], the Australian Certification Authority **certifies** the evaluation of Juniper Junos OS 22.2R1 for SRX380 performed by the Australian Information Security Evaluation Facility, Teron Labs.

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 understood
- 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
- have a system auditor review the audit trail generated and exported by the TOE periodically.

Annex A – 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 (CPP_ND), Version 2.2e, 23-March-2020*
    b) PP-Module for Intrusion Protection Systems (IPS), Version 1.0, 11 May 2021 (MOD_IPS)
    c) PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625, 25 June 2020 (MOD_CPP_FW)
    d) PP-Module for Virtual Private Network (VPN) Gateways, Version 1.1, 18 June 2020 (MOD_VPNGW)
    e) *Extended Package MACsec Ethernet Encryption (MACsecEP), Version 1.2, 10 May 2016.*
5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
6. *Junos OS, Common Criteria Guide for SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC and SRX380 Devices, Release 22.2R1, Published 2022-11-21*
7. *Security Target Junos OS 22.2R1 for SRX380, Version 1.0, 13 June 2023*
8. *Evaluation Technical Report - Junos OS 22.2R1 for SRX380, dated 21 June 2023* (Document reference EFT-T034-ETR 1.1)
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) *Seeding of the Kernel RBG in Junos OS 22.2R1, SRX300, SRX320, SRX340, SRX345, SRX345-DUAL-AC and SRX380, Version 1.0, 08/11/2022*
12. *Supporting Documents:*
    a) *Supporting Document, Evaluation Activities for Network Device cPP, Version 2.2, December-2019 (CPP_ND_SD)*

b) *Supporting Document, Mandatory Technical Document, PP-Module for Intrusion Prevention Systems (IPS), Version: 1.0, 2021-05-11 (MOD_IPS_SD)*

c) *Evaluation Activities for Stateful Traffic Filter Firewalls PP-Module, Version 1.4 +Errata 20200625, June-2020 (MOD_FW_SD)*

d) *Supporting Document, Mandatory Technical Document, PP-Module for Virtual Private Network (VPN) Gateways, version 1.1, dated 2020-06-18 (MOD_VPNGW_SD)*

13. *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs May 2017, Version 0.5 CCDB-2017-05-xx*

Abbreviations

AISEP	Australian Information Security Evaluation Program
ARP	Address Resolution Protocol
ASD	Australian Signals Directorate
ASIC	Application Specific Integrated Circuit
CCRA	Common Criteria Recognition Arrangement
DHCP	Dynamic Host Configuration Protocol
LLDP	Link Layer Discovery Protocol
MACsec	Media Access Control Security (IEEE 802.1AE)
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
ND iTC	Network Device international Technical Community
PFE	Packet Forwarding Engine
PP	Protection Profile
RE	Routing Engine
SSH	Secure Shell
STP	Spanning Tree Protocol
TOE	Target of Evaluation