Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Information Security Evaluation Program

Certification Report

Juniper Networks Junos OS 22.3R1 for QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y

Version 1.0, 17 October 2024

Document reference: AISEP-CC-CR-2024-EFT-T033-CR-V1.0
(Certification expires five years from certification report date)

cyber.gov.au

Table of contents

Executive summary

This report describes the findings of the IT security evaluation of Juniper Networks Junos OS 22.3R1 for QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y appliances against Common Criteria approved Protection Profile (PP).

The variants of the TOE are secure network devices which protect themselves largely by offering only a minimal logical interface to the network and the attached nodes. It is a purpose built platform that does not provide any general-purpose computing capabilities. The TOE implements both management and control functions as well as all IP routing.

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

- collaborative Protection Profile for Network Devices, version 2.2E, 23 March 2020 (NDcPP)

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 04 October 2024.

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 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

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 [7] 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 Profile [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 [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 22.3R1 for QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y.

Description	Version
Evaluation scheme	Australian Information Security Evaluation Program
TOE	Junos OS 22.3R1 for QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y
Software version	v22.3R1
Hardware platforms	QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y
Security Target	Security Target Junos OS 22.3R1 for QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y , Version 1.0, 05 August 2024
Evaluation Technical Report	Evaluation Technical Report 1.1, dated 4 October 2024 Document reference EFT-T033-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	Network Device collaborative Protection Profile version 2.2e, 23 March 2020 (NDcPP)
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 Target of Evaluation (TOE) are the Juniper Networks, Inc. QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y Ethernet Switches executing the Junos OS 22.3R1 software as a complete appliance of hardware and software.

The variants of the TOE are grouped by equivalency, share a common architecture and feature set. They implement a variety of high-speed interfaces (only Ethernet is in the scope of the evaluation) for enterprise branch, campus, and data center networks. They also share common Junos firmware, features, and technology for compatibility across platforms.

The appliance variations constituting the TOE are secure network devices that protect themselves largely by offering only a minimal logical interface to the network and attached nodes. They include the Junos OS firmware Junos OS 22.3R1, which is a special purpose OS offering no general-purpose computing capabilities. Junos OS implements both management and control functions as well as all IP routing.

The TOE allows multiple interconnected switches to operate as a single, logical unit, enabling users to manage all platforms as one virtual device. The functions of the appliances are managed through the Junos firmware, either from a connected terminal console or via a network connection. Network management is secured using the SSH protocol. 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 TOE supports the definition and enforcement of information flow policies among network nodes. Each information flow from one network node to another passes through an instance of the TOE. Information flows are controlled based on network node addresses and protocols. The TOE also ensures that security-relevant activity is audited and provides the necessary tools to manage all the security functions.

The variants of the TOE are appliances that are physically self-contained, housing the software and hardware necessary to perform all routing and switching functions. The architecture components of the TOE are the Routing Engine implementing routing and switching services while also providing a network management interface for the configuration and operation of the TOE. The Packet Forwarding Engine implement transit packet forwarding operations. The power supply connects to the midplane of the TOE, distributing different voltage outputs to the appliance components, depending on the voltage requirements needed. The switch fabric boards provide a scalable, non-blocking central matrix for all network data passing through the TOE.

TOE Functionality

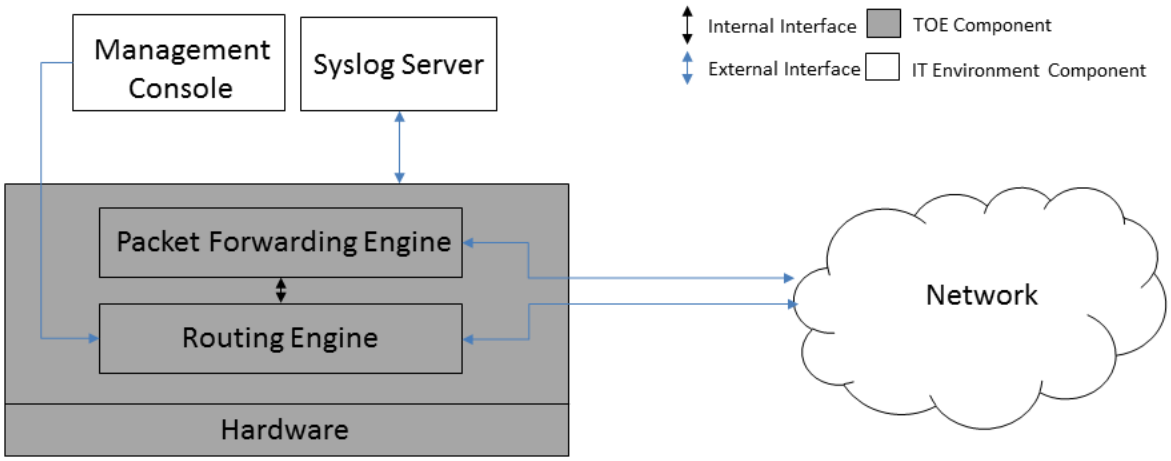
The TOE functionality that was evaluated is described in section 1.5 of the Security Target [7].

TOE physical boundary

The TOE is the Junos OS 22.3R1 firmware running on the appliance chassis listed in the table below. The TOE is contained within the physical boundary of the specified appliance chassis.

The physical boundary of the TOE is the entire chassis of the appliance platform, and includes both the hardware and software of the network device. The TOE is the Junos OS 22.3R1 software running on the appliance chassis listed in the table above. This includes the firmware implementing the Routing Engine and the ASICs implementing the Packet Forwarding Engine. Hence the TOE is contained within the physical boundary of the specified appliance chassis. The install package for the QFX models is jinstall-host-qfx-5e-x86-64-22.3R1.11.tgz. The install package for the EX4650-48Y is jinstall-host-ex-4e-x86-64-22.3R1.11.tgz.

The physical boundary for QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y is shown in the figure below.



The TOE interfaces comprise the following:

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

Architecture

Each instance of the TOE consists of the following major architectural components:

- Switch fabric – the switch fabric boards provide a highly scalable, non-blocking, centralized switch fabric matrix through which all network data passes.
- Routing Engine (Control Board) – the Routine Engine (RE) runs the Junos firmware and implements Layer 3 routing services and Layer 2 switching services. The RE also implements the management functions for configuration and operation of the TOE and controls the flow of information through the TOE, including support for appliance interface control and control plane functions such as chassis component, system management and user access to the appliance.
- Layer 2 switching services, Layer 3 switching/routing services and network management for all operations necessary for the configuration and operation of the TOE and controls the flow of information through the TOE.
- Packet Forwarding Engine (PFE) – The PFE implements all operations necessary for transit packet forwarding. The line cards implement an extensive set of Layer 2 and Layer 3 services that can be deployed in any combination of L2- L3 applications.

- Power –The power supplies connect to the midplane, which distributes the different output voltages produced by the power supplies to the appliance components, depending on their voltage requirements.

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

The functions of the TOE can be managed using a Command Line Interface (CLI) implemented by the Junos OS. The CLI may be accessed from a connected terminal console or via a network connection secured by the SSH Protocol. All management accesses require successful authentication. The TOE implements measures to prevent access by the parties not successfully authenticated and to make it difficult for unauthorized parties to gain access to the CLI.

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 Profile [4] and Supporting Document [13] 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

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 Linux root account.

- MACsec is not included in the scope of the evaluation.

Security

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 [7] contains the functionality that is to be 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. 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 QFX model devices and EX4650-48Y running Junos OS 22.3R1 are available for download at https://www.juniper.net/documentation. The title is:

- *Junos® OS Common Criteria Evaluated Configuration Guide for EX4650-48Y, QFX5110-32Q, QFX5110-48S, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX5200-32C, QFX5200-48Y, and QFX5210-64C Devices, Release 22.3R1, Date 2024-09-10 [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 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 Profile [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 the relevant Supporting Document [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 Profile [4] and Supporting Document [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] which 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 **16 April 2024** 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 Profile that cover the technology area of network devices. 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 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. 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 Profile (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 [7] and **has met** the requirements of the Protection Profiles NDcPP V2.2E [4].

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 the Juniper Junos OS 22.3R1 for QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y performed by the Australian Information Security Evaluation Facility, Teron Labs.

The Australian Certification Authority certifies that the Security Target [7] have met the requirements of the Network Device Protection Profile.

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 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 Profile:
    a) *collaborative Protection Profile for Network Devices (NDcPP), Version 2.2E, 23 March 2020*
5. *Australian Government Information Security Manual:* https://www.cyber.gov.au/ism
6. Guidance documentation: *Junos® OS Common Criteria Evaluated Configuration Guide for EX4650-48Y, QFX5110-32Q, QFX5110-48S, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5120-48YM, QFX5200-32C, QFX5200-48Y, and QFX5210-64C Devices, Release 22.3R1, 10 September 2024*
7. *Security Target for Junos OS 22.3R1 for QFX5200-32C, QFX5110-48S, QFX5110-32Q, QFX5120-48T, QFX5120-48Y, QFX5120-32C, QFX5210-64C, QFX5200-48Y and EX4650-48Y, Version 1.0, 05 August 2024*
8. *Evaluation Technical Report - Junos OS 22.3R1 for EX4650-48Y, QFX5110-32Q, QFX5110-48S, QFX5120-32C, QFX5120-48T, QFX5120-48Y, QFX5200-32C, QFX5200-48Y, and QFX5210-64C, dated 4 October 2024* (Document reference EFT-T033-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) *Junos OS Entropy Source version 22.3, Entropy Assessment and SP 800-90B Compliance Report, Junos OS 22.3R1, Version 1.5, 30 August 2023*
12. Protection Profile Supporting Document:
    a) *Supporting Document, Evaluation Activities for Network Device cPP, December 2019, version 2.2 (NDcPP-SD)*
13. *CC and CEM addenda, Exact Conformance, Selection-Based SFRs, Optional SFRs 30 September 2021, Version 2.0, CCDB-013-v2.0*

Abbreviations

ACA	Australian Certification Authority
AISEP	Australian Information Security Evaluation Program
ASD	Australian Signals Directorate
ASIC	Application Specific Integrated Circuit
CCRA	Common Criteria Recognition Arrangement
ETR	Evaluation Technical Report
MACsec	Media Access Control security
NDcPP	CCRA-approved collaborative Protection Profile for Network Devices
ND-iTC	Network International Technical Community
OS	Operating System
PFE	Packet Forwarding Engine
PP	Protection Profile
RE	Routing Engine
SSH	Secure Shell
TOE	Target of Evaluation