Certification Report

Juniper Networks M,T, MX and PTX Routers and EX9200 Switches running Junos OS 13.3R1.8 and Juniper QFX and EX Switches Running Junos OS 13.2X50-D19 and 13.2X51-D20

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

© Government of Canada, Communications Security Establishment, 2014

Document number: 383-4-297-CR
Version: 1.0
Date: 3 September 2014
Pagination: i to iii, 1 to 9

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provide a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 3 September 2014, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks or registered trademarks:

- Juniper Networks is a registered trademark of Juniper Networks, Inc; and
- Junos is a registered trademark of Juniper Networks, Inc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

Juniper Networks M,T, MX and PTX Routers and EX9200 Switches running Junos OS 13.3R1.8 and Juniper QFX and EX Switches Running Junos OS 13.2X50-D19 and 13.2X51-D20 (hereafter referred to as Junos OS 13), from Juniper Networks, is the Target of Evaluation. The results of this evaluation demonstrate that Junos OS 13 is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

Junos OS 13 is a complete routing system that supports a variety of high speed interfaces (only Ethernet is within scope of this evaluation) for medium to large networks and network applications.

The hardware has two components: the router itself and the PICs/DPC (Interface Cards) that have been installed in the router. The various PICs/DPC that have been installed in the router allow it to communicate with the different types of networks that may be required within the environment where the router will be used.

The router architecture of each platform separates routing and control functions from packet forwarding operations, thereby reducing bottlenecks and permitting the router to maintain a higher level of performance.

Each router consists of two major architectural components:

- The Routing Engine, which provides Layer 3 routing services and network management and control; and
- The Packet Forwarding Engine, which 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.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 15 July 2014 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Junos OS 13, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the Junos OS 13 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

Juniper Networks M,T, MX and PTX Routers and EX9200 Switches running Junos OS 13.3R1.8 and Juniper QFX and EX Switches Running Junos OS 13.2X50-D19 and 13.2X51-D20 (hereafter referred to as Junos OS 13), from Juniper Networks, is the Target of Evaluation. The Junos OS 13 is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

2 TOE Description

Junos OS 13 is a complete routing system that supports a variety of high speed interfaces (only Ethernet is within scope of this evaluation) for medium to large networks and network applications.

The hardware has two components: the router itself and the PICs/DPC (Interface Cards) that have been installed in the router. The various PICs/DPC that have been installed in the router allow it to communicate with the different types of networks that may be required within the environment where the router will be used.

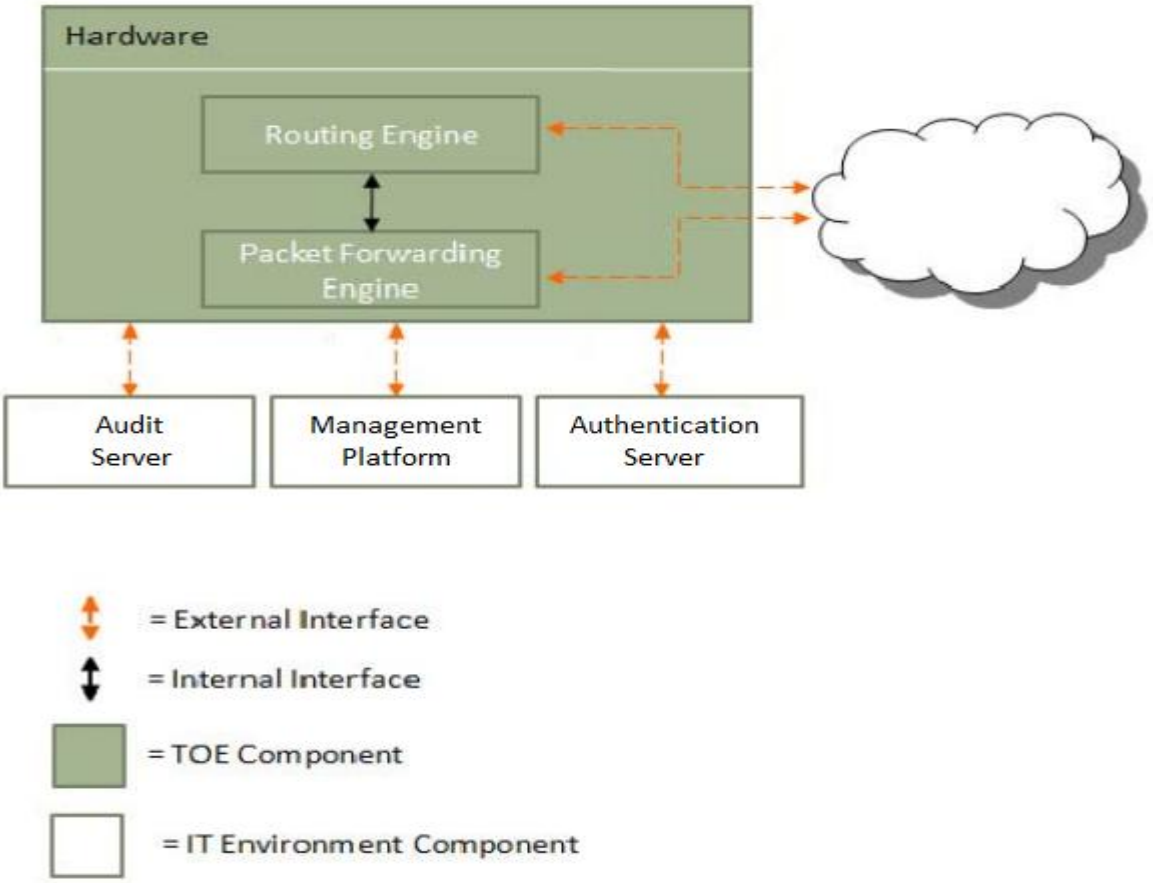
The router architecture of each platform separates routing and control functions from packet forwarding operations, thereby reducing bottlenecks and permitting the router to maintain a higher level of performance.

Each router consists of two major architectural components:

- The Routing Engine, which provides Layer 3 routing services and network management and control; and
- The Packet Forwarding Engine, which 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.

A diagram of the Junos OS 13 architecture is as follows;



3 Security Policy

Junos OS 13 implements a role-based access control policy to control administrative access to the system. In addition, Junos OS 13 implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access
- Trusted Path/Channels

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in Junos OS 13:

Cryptographic Algorithm	**Standard**	**Certificate #**
Eliptical Curve Digital Signature Algorithm (ECDSA)	FIPS 186-3	501, 520, 521
Advanced Encryption Standard (AES)	FIPS 197	2845, 2889, 2890
Rivest Shamir Adleman (RSA)	FIPS 186-2	1486, 1520, 1521
Secure Hash Algorithm (SHA-1)	FIPS 180-2	2386, 2387, 2430, 2431, 2432, 2433
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	1784, 1785, 1823, 1824, 1825, 1826
Deterministic Random Bit Generator – Hash Method Authentication Code	FIPS 180	499, 524, 525

4 Security Target

The ST associated with this Certification Report is identified below:

Security Target: Juniper Networks M, T, MX and PTX Routers and EX9200 Switches running Junos OS 13.3R1.8 and Juniper QFX and EX Switches Running Junos OS 13.2X50-D19 and Junos OS 13.2X51-D20 v 1.1, 26 August 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Junos OS 13 is:

a. Conformant to the Protection Profile for Network Devices, v1.1, June 8, 2012,
b. *Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:*

- FAU_STG_EXT.1 - External audit trail storage
- FCS_CKM_EXT.4 - Cryptographic key zeroization
- FCS_RBG_EXT.1 - Cryptographic operation: random bit generation
- FCS_SSH_EXT.1 - SSH
- FIA_PMG_EXT.1 - Password management
- FIA_UIA_EXT.1 - User identification and authentication
- FIA_UAU_EXT.2 - Password-based authentication mechanism
- FPT_SKP_EXT.1 - Protection of TSF data
- FPT_APW_EXT.1 - Protection of administrator passwords
- FPT_TUD_EXT.1 - Trusted update
- FPT_TST_EXT.1 - TSF testing

- FTA_SSL_EXT.1 - TSF-initiated session locking

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of Junos OS 13 should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE; and
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

6.3 Clarification of Scope

Junos OS 13 incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

7 Evaluated Configuration

The evaluated configuration for Junos OS 13 comprises:

the following secure network devices running Junos OS 13.3R1.8:

- M-Series Multiservice Edge Routers: M7i, M10i, M120 and M320;
- MX-Series 3D Universal Edge Routers: MX5, MX10, MX40, MX80, MX104, MX240, MX480, MX960, MX2010 and MX20202;
- T-Series Core Routers: T640, T1600 and T4000;
- PTX-Series Packet Transport Switches: PTX3000 and PTX5000; and
- EX-Series Ethernet Switches: EX9200 (EX9204, EX9208 and EX9214).

the following secure network devices running Junos OS 13.2X51-D20:

- EX-Series Ethernet Switches: EX2200, EX4300, EX4500 and EX4550; and
- QFX-Series Ethernet Switches: QFX5100.

the following secure network devices running Junos OS 13.2X50-D19:

- EX3200, EX3300, EX4200, EX621,0 EX8208 and EX8216.

The publications entitled

- Junos OS Common Criteria Evaluation Configuration Guide for Devices Running Junos OS 13.2;
- Junos OS Common Criteria Evaluation Configuration Guide for Devices Running Junos OS 13.3R1.8;

describe the procedures necessary to install and operate Junos OS 13 in its evaluated configuration.

8 Documentation

The Juniper Networks documents provided to the consumer are as follows:

- Junos OS for EX Series Ethernet Switches System Basics on EX9200 Switches;
- Junos OS Common Criteria Evaluation Configuration Guide for Devices Running Junos OS 13.2;
- Junos OS Common Criteria Evaluation Configuration Guide for Devices Running Junos OS 13.3R1.8;
- Junos OS System Log Messages Reference; and
- Junos OS System Services Administration Guide for Routing Devices.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Junos OS 13, including the following areas:

Development: The evaluators analyzed the Junos OS 13 functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the Junos OS 13 functional specification is an accurate and complete instantiation of the SFRs.

Guidance Documents: The evaluators examined the Junos OS 13 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the Junos OS 13 configuration management system and associated documentation was performed. The evaluators found that the Junos OS 13 configuration items were clearly marked.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. NDPP required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the NDPP to which the TOE is claiming conformance.

10.2 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. NDPP required assurance activities. The evaluator performed the assurance activities mandated by the protection profile to which the TOE is claiming conformance; and
b. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

10.3 Conduct of Testing

Junos OS 13 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the information Technology Security Evalaution and Test Facility. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.4 Testing Results

The independent tests yielded the expected results, providing assurance that Junos OS 13 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a NDPP conformance claim as claimed in Section 5. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

The end user is reminded that guidance given in the Common Criteria Configuration Guide must be strictly followed in order to meet the security level attested to in this evaluation. For example, the root account will remain available during continued operation but, as per the configuration guidance, that account must not be used beyond the installation phase of device deployment.

End users must also recognize that only the Security Functional Requirements listed in the Security Target have been assessed during this evaluation. Any functionality of the TOE which is beyond this scope has not been evaluated. This includes packet filtering, routing protocols, and items listed in the "Summary of Out-of-Scope Items" section of the Security Target.

The evaluator recommends that administrators of the TOE regularly review the Junos Security Advisories to stay aware of security issues that might arise subsequent to the date this evaluation is concluded.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report

Acronym/Abbreviation/ Initialization	Description
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

14 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Protection Profile for Network Devices, v1.1, June 8, 2012.

e. Security Target: Juniper Networks M, T, MX and PTX Routers and EX9200 Switches running Junos OS 13.3R1.8 and Juniper QFX and EX Switches Running Junos OS 13.2X50-D19 and Junos OS 13.2X51-D20 v 1.1, 26 August 2014

f. Evaluation Technical Report Juniper Networks Junos OS 13.3R1.8, Junos OS 13.2X50-D19 and Junos OS 13.2X51-D20 Common Criteria NDPP Evaluation v3.2, 15 July 2014.