Certification Report

EAL 3+ Evaluation of Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running JUNOS 11.4R2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-227-CR
Version: 1.0
Date: 22 October 2012
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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply 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 Canada, 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 Canada, 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) provides 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 Canada.

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 located in Ottawa, Canada.

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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 22 October 2012, 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 registered trademarks:

- Juniper Networks, JUNOS and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

TABLE OF CONTENTS

Disclaimer ..... **i**

Foreword ..... **ii**

Executive Summary **1**

1 Identification of Target of Evaluation **2**

2 TOE Description **2**

3 Evaluated Security Functionality **2**

4 Security Target **2**

5 Common Criteria Conformance **2**

6 Security Policy **3**

7 Assumptions and Clarification of Scope **3**

7.1 SECURE USAGE ASSUMPTIONS 3
7.2 ENVIRONMENTAL ASSUMPTIONS 3
7.3 CLARIFICATION OF SCOPE 4

8 Evaluated Configuration **4**

9 Documentation **4**

10 Evaluation Analysis Activities **4**

11 ITS Product Testing **6**

11.1 ASSESSMENT OF DEVELOPER TESTS 6
11.2 INDEPENDENT FUNCTIONAL TESTING 6
11.3 INDEPENDENT PENETRATION TESTING 7
11.4 CONDUCT OF TESTING 7
11.5 TESTING RESULTS 8

12 Results of the Evaluation **8**

13 Evaluator Comments, Observations and Recommendations **8**

14 Acronyms, Abbreviations and Initializations **8**

15 References **8**

Executive Summary

Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running JUNOS 11.4R2 (hereafter referred to as JUNOS® 11.4R2), from Juniper Networks, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 augmented evaluation.

JUNOS® 11.4R2 is a combined hardware/software TOE designed to forward network packets from source network entities to destination network entities based on available routing information.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 11 October 2012 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® 11.4R2 , the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security 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.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 3 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. The following augmentation is claimed: ALC_FLR.3 – Systematic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the JUNOS® 11.4R2 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running JUNOS 11.4R2 (hereafter referred to as JUNOS® 11.4R2), from Juniper Networks, Inc.

2 TOE Description

JUNOS® 11.4R2 is a combined hardware/software TOE which routes IP traffic between source and destination network entities. IP traffic on the monitored network is scanned and then compared against a set of rules to determine where the traffic should be routed, and is then passed to the appropriate destination. The routing decision is based on the presumed source and destination IP address of the packet, the network layer protocol, service and the interface on which the packet arrives and is to depart on.

A detailed description of the JUNOS® 11.4R2 architecture is found in Section 1.5 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for JUNOS® 11.4R2 is identified in Section 6 of the ST.

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running JUNOS 11.4R2
Version: 1.0
Date: 01 October 2012

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

JUNOS® 11.4R2 is:

a. *Common Criteria Part 2 conformant*, with security functional requirements based only upon functional components in Part 2;

b. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3; and
c. *Common Criteria EAL 3 augmented*, containing all security assurance requirements in the EAL 3 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation.

6 Security Policy

JUNOS® 11.4R2 implements an unauthenticated flow control policy which controls the flow of information passing through the TOE.

In addition, JUNOS® 11.4R2 implement policies pertaining to security audit, user data protection, identification and authentication, security management, protection of the TOE Security Functionality (TSF), and TOE Access. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of JUNOS® 11.4R2 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- The authorized users will be competent, and not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access;
- External authentication services will be available via either RADIUS or TACACS+, or both;
- External NTP services will be available;
- Management traffic will be protected using SSH; and

- The IT environment network components that have access to the management interface of the TOE are protected.

7.3 Clarification of Scope

JUNOS® 11.4R2 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing basic attack potential. JUNOS® 11.4R2 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for JUNOS® 11.4R2 comprises Juniper Networks JUNOS® 11.4R2 running on the following hardware appliances: M7i, M10i, M120, M320, T320, T640, T1600, MX5, MX10, MX40, MX80, MX240, MX480, MX960, EX2200, EX3200, EX3300, EX4200, EX4500, EX6210 and EX8200.

The publication entitled *Junos OS Secure Configuration Guide for Common Criteria for EX Series Ethernet Switches, M Series Multiservice Edge Routers, MX Series 3D Universal Edge Routers, and T Series Core Routers* describes the procedures necessary to install and operate JUNOS® 11.4R2 in its evaluated configuration.

9 Documentation

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

a. Junos OS, System Basics Configuration Guide , Release 11.4, November 08, 2011;

b. Junos OS, CLI User Guide , Release 11.4, November 08, 2011; and

c. Junos OS Secure Configuration Guide for Common Criteria for EX Series Ethernet Switches, M Series Multiservice Edge Routers, MX Series 3D Universal Edge Routers, and T Series Core Routers , Release 11.4, August 31, 2012.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of JUNOS® 11.4R2, including the following areas:

Development: The evaluators analyzed the JUNOS® 11.4R2 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the JUNOS® 11.4R2 security architectural description and determined that the initialization

process is secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the JUNOS® 11.4R2 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® 11.4R2 configuration management system and associated documentation was performed. The evaluators found that the JUNOS® 11.4R2 configuration items were clearly marked and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was also observed during the site visit, and it was found to be mature and well-developed.

During the site visit the evaluators examined the development security procedures and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the JUNOS® 11.4R2 design and implementation. The evaluators confirmed that the developer used a documented model of the TOE life-cycle and that the life-cycle model provides for the necessary control over the development and maintenance of the TOE.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of JUNOS® 11.4R2 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Juniper Networks, Inc. for JUNOS® 11.4R2 . During a site visit, the evaluators examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of JUNOS® 11.4R2. Additionally, the evaluators conducted a review of public domain vulnerability databases, and a search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to JUNOS® 11.4R2 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification and TOE design was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

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 CGI IT Security Evaluation & Test Facility test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Restrictive Defaults at TOE Initialization: The objective of this test goal is to verify that the TOE will not forward packets until it has been configured in accordance with the JUNOS Secure Configuration Guide;

c. TOE Filtering Using In-band Management Port: The objective of this test goal is to demonstrate packets sent to the TOE are processed properly by traffic filters and access from non-authorized IP addresses is refused. This test also verifies that valid login credentials are accepted, while invalid credentials are rejected and all failed connection attempts are properly logged;

d. Only Privileged Users Can Modify Audit Logs: The objective of this test goal is to demonstrate that logs generated by syslog can only be modified by users with 'root' and 'super-user' class; and

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

e. User Identification: The objective of this test case is to verify authentication by the RADIUS server is properly managed by the TOE.

11.3 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. Port Scanning: The objective of this test is to scan the TOE using a port scanner to determine what ports are open and what services are running. In addition a firewall filter was implemented to verify whether the SSH login port is properly filtered;

b. Privilege Escalation: The objective of this test is to determine whether the TOE is susceptible to a known vulnerability (PSN-2012-07-646) by having the TOE reload a default configuration while another user is editing the current configuration. The second portion of this test was to determine whether the workaround solution provided by the vendor mitigates this vulnerability;

c. Exponential Delay for Failed Logins: The objective of this test is to determine whether the exponential delay for failed logins can be bypassed by using multiple simultaneous connections;

d. Exhaust Audit Log: The objective of this test is to send a large amount of network traffic attempting to exhaust the audit log and cause possible adverse effects; and

e. Reboot: The objective of this test is to reboot the TOE unexpectedly (simulate a system crash) to determine if any potential vulnerabilities are found.

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

11.4 Conduct of Testing

JUNOS® 11.4R2 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at CGI IT Security Evaluation & 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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that JUNOS® 11.4R2 behaves as specified in its ST and functional specification and TOE design.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 3+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Evaluator Comments, Observations and Recommendations

The evaluator recommends that administrators of the TOE regularly review the Juniper Knowledge Base, JTAC Technical Bulletins (security advisories) and adhere to the Juniper Networks Junos® OS Secure Configuration Guide for Common Criteria.

14 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
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

15 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 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running JUNOS 11.4R2, version 1.0, 01 October 2012.

e. Juniper Networks M-Series Multiservice Edge Routers, MX-Series 3D Universal Edge Routers, T-Series Core Routers and EX-Series Ethernet Switches running JUNOS 11.4R2, version 1.1, 11 October 2012.