Certification Report

EAL 4+ Evaluation of JUNOS-FIPS for SRX Series version 10.4R4

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-180-CR
Version: 1.0
Date: 9 January 2012
Pagination: i to iii, 1 to 12

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 9 January 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 trademarks or registered trademarks:

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

TABLE OF CONTENTS

Executive Summary

The JUNOS-FIPS for SRX Series version 10.4R4 (hereafter referred to as JUNOS-FIPS 10.4R4 SRX), from Juniper Networks, Inc, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

JUNOS-FIPS 10.4R4 SRX is a combined hardware/software TOE deployed at branch and remote locations in the network to provide all-in-one secure WAN connectivity, IP telephony, and connection to local PCs and servers via integrated Ethernet switching.

JUNOS-FIPS 10.4R4 SRX provide the following services:

- VPN routing - securely forwarding data packets along networks in accordance with one or more routing protocols;
- Firewall - applying access rules to control connectivity between two or more network environments; and
- Intrusion detection and prevention - monitoring and analyzing a set of IT system resources for potential vulnerabilities or misuse and taking action upon detection of potential vulnerabilities.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 23 December 2011 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-FIPS 10.4R4 SRX , the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the 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 4 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.2 – Flaw Reporting Procedures.

[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.

JUNOS-FIPS 10.4R4 SRX is conformant with the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments Version 1.1, dated July 25, 2007 (FWPP) and the U.S. Government Protection Profile Intrusion Detection System - System for Basic Robustness Environments, Version 1.7, dated July 25, 2007 (IDSPP).

Communications Security Establishment Canada, as the CCS Certification Body, declares that JUNOS-FIPS 10.4R4 SRX 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

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is JUNOS-FIPS for SRX Series version 10.4R4 (hereafter referred to as JUNOS-FIPS 10.4R4 SRX), from Juniper Networks, Inc.

2 TOE Description

JUNOS-FIPS 10.4R4 SRX is a combined hardware/software TOE deployed at branch and remote locations in the network to provide all-in-one secure WAN connectivity, IP telephony, and connection to local PCs and servers via integrated Ethernet switching. JUNOS-FIPS 10.4R4 SRX provides the following services:

- VPN routing - securely forwarding data packets along networks in accordance with one or more routing protocols
- Firewall - applying access rules to control connectivity between two or more network environments
- Intrusion detection and prevention - monitoring and analyzing a set of IT system resources for potential vulnerabilities or misuse and taking action upon detection of potential vulnerabilities.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for JUNOS-FIPS 10.4R4 SRX is identified in Section 7 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
Juniper Networks SRX100, SRX210, SRX220, SRX240 and SRX650 Series Gateways	1613
Juniper Networks SRX3400 and SRX3600 Series Gateways	1611
Juniper Networks SRX5600 and SRX5800 Series Gateways	1602

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in JUNOS-FIPS 10.4R4 SRX :

Cryptographic Algorithm for SRX 100, 210, 220, 240, 650	**Certificate #**
Triple-DES (3DES)	1064
Advanced Encryption Standard (AES)	1624
Digital Signature Algorithm(DSA)	510

Secure Hash Standard (SHS)	1433
Random Number Generators (RNG)	871
Rivest Shamir Adleman (RSA)	802
Keyed-Hash Message Authentication Code (HMAC)	955

Cryptographic Algorithm for SRX 3400, 3600	**Certificate #**
Triple-DES (3DES)	1032,1033
Advanced Encryption Standard (AES)	1575, 1577
Digital Signature Algorithm(DSA)	486
Secure Hash Standard (SHS)	1395, 1396
Random Number Generators (RNG)	849
Rivest Shamir Adleman (RSA)	768
Keyed-Hash Message Authentication Code (HMAC)	922, 923

Cryptographic Algorithm for SRX 5600, 5800	**Certificate #**
Triple-DES (3DES)	1030, 1034
Advanced Encryption Standard (AES)	1573, 1578
Digital Signature Algorithm(DSA)	484
Secure Hash Standard (SHS)	1393, 1397
Random Number Generators (RNG)	847
Rivest Shamir Adleman (RSA)	766
Keyed-Hash Message Authentication Code (HMAC)	920, 924

4 Security Target

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

Title: Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series
Version: 1.5, Rev A
Date: 22 December 2011

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-FIPS 10.4R4 SRX is:

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

components in Part 2, except for the following explicitly stated requirements defined in the ST:

- IDS_SDC.1 – System Data Collection;
- IDS_ANL.1 – Analyzer Analysis;
- IDS_RDR.1 – Restricted Data Review;
- IDS_RCT.1 – Analyzer React;
- IDS_STG.1 – Guarantee of System Data Availability;
- IDS_STG.2 – Prevention of System Data Loss; and
- FAU_STG_EXT.1 – External Audit Trail Storage;

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

c. *Common Criteria EAL 4 augmented, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.*

d. JUNOS-FIPS 10.4R4 SRX is conformant with the U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments Version 1.1, dated July 25, 2007 (FWPP) and the U.S. Government Protection Profile Intrusion Detection System - System for Basic Robustness Environments, Version 1.7, dated July 25, 2007 (IDSPP).

6 Security Policy

JUNOS-FIPS 10.4R4 SRX implements two information flow control policies. The Secure Information Flow and Unauthenticated Information Flow security polices enforce rules for traffic in terms of what traffic can pass through the TOE and the actions required to take place on the traffic as it passes through the TOE. Details of these security policies can be found in Section 6 and Section 7.3 of the ST.

In addition JUNOS-FIPS 10.4R4 SRX implements polices pertaining to security audit, cryptographic support, identification and authentication, security management, protection of the TOE Security Functionality (TSF) and traffic analysis. Further details on these security policies may be found in Section 6 and Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of JUNOS-FIPS 10.4R4 SRX 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 Assumptions are listed in the ST:

- The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors;

- There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains;
- The TOE can only be accessed by authorized users;
- The TOE does not host public data;
- The Authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation;
- Human users within the physically secure boundary protecting the TOE may attempt to access the TOE from some direct connection if the connection is part of the TOE;
- Human users who are not authorized administrators cannot access the TOE remotely from the internal or external networks; and
- Authorized administrators may access the TOE remotely from the internal and external networks.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE has access to all the IT System data it needs to perform its functions;
- The TOE is appropriately scalable to the IT System the TOE monitors;
- The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical access;
- The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access; and
- Information cannot flow among the internal and external networks unless it passes through the TOE.

7.3 Clarification of Scope

JUNOS-FIPS 10.4R4 SRX is suitable for use in a well-protected environment accessible by authorized administrators only.

8 Evaluated Configuration

The evaluated configuration for JUNOS-FIPS 10.4R4 SRX comprises Juniper Networks JUNOS-FIPS Version 10.4R4.5 running on the SRX100, SRX210, SRX220, SRX240, SRX650, SRX3400, SRX3600, SRX5600, and SRX5800 hardware appliances. The evaluated configuration also includes a FIPS 140-2 validated cryptographic module.

The publication entitled Operational User Guidance and Preparative Procedures Supplement: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series Version 1.4 Rev A describes the procedures necessary to install and operate JUNOS-FIPS 10.4R4 SRX in its evaluated configuration.

9 Documentation

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

a. Operational User Guidance and Preparative Procedures Supplement: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series Version 1.4 Rev A;

b. JUNOS 10.4 Administration Guide for Security Devices;

c. JUNOS 10.4 Access Privilege Configuration Guide;

d. JUNOS 10.4 System Log Messages Reference;

e. JUNOS 10.4 CLI User Guide;

f. JUNOS 10.4 MPLS Applications Configuration Guide;

g. JUNOS 10.4 Network Interfaces Configuration Guide;

h. JUNOS 10.4 Policy Framework Configuration Guide;

i. JUNOS 10.4 Routing Protocols Configuration Guide;

j. JUNOS 10.4 Services Interfaces Configuration Guide;

k. JUNOS 10.4 System Basics Configuration Guide;

l. JUNOS 10.4 VPNs Configuration Guide;

m. JUNOS 10.4 Routing Protocols and Policies Command Reference; and

n. JUNOS 10.4 System Basics and Services Command Reference

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of JUNOS-FIPS 10.4R4 SRX , including the following areas:

Development: The evaluators analyzed the JUNOS-FIPS 10.4R4 SRX functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the JUNOS-FIPS 10.4R4 SRX security architectural description and determined that the initialization process is secure and that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the JUNOS-FIPS 10.4R4 SRX 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-FIPS 10.4R4 SRX configuration management system and associated documentation was performed. The evaluators found that the JUNOS-FIPS 10.4R4 SRX configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of JUNOS-FIPS 10.4R4 SRX during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the JUNOS-FIPS 10.4R4 SRX design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Juniper Networks, Inc for JUNOS-FIPS 10.4R4 SRX . During a site visit, the evaluators also 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-FIPS 10.4R4 SRX . Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the JUNOS-FIPS 10.4R4 SRX in its operational environment.

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

11 ITS Product Testing

Testing at EAL 4 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, TOE design and security architecture description 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;

[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.

b. Security Audit: The objective of this test goal is to ensure that audit events for authentication activities, configuration changes, shutdown and start-up of system, and traffic flow of the Unauthenticated Information Flow SFP are logged as specified and that audit log data is not deleted when the storage capacity has been reached;

c. User Data Protection: The objective of this test goal is to ensure that the TOE enforces the Unauthenticated Information Flow SFP during normal operation and when the TOE is abruptly shut down and restarted;

d. Identification and Authentication: The objective of this test goal is to ensure that the TOE's identification and authentication requirements operate as specified; and

e. Security Management: The objective of this test goal is to ensure that the TSF enforces the correct security behaviour based on the attributes assigned to roles and users.

11.3 Independent Penetration Testing

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

a. Use of commercial vulnerability tools to scan the TOE for open ports and platform vulnerabilities;

b. Exploiting a Denial of Service vulnerability by sending fragmented ICMP packets to TOE; and

c. Determining if it is possible for a threat agent to exhaust the entire log storage area to crash the TOE or prevent further logging.

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

11.4 Conduct of Testing

JUNOS-FIPS 10.4R4 SRX 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-FIPS 10.4R4 SRX behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ 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

JUNOS-FIPS 10.4R4 SRX are versatile network devices providing reliable basic services. It is highly recommended the appliances are securely configured by an experienced Juniper administrator.

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
IP	Internet Protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
ST	Security Target
TOE	Target of Evaluation
VPN	Virtual Private Network
WAN	Wide Area Network

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. U.S. Government Protection Profile for Traffic Filter Firewall in Basic Robustness Environments Version 1.1, dated July 25, 2007 (FWPP) and the U.S. Government Protection Profile Intrusion Detection System - System for Basic Robustness Environments, Version 1.7, dated July 25, 2007 (IDSPP).

e. Security Target: Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series, 1.5, Rev A, 22 December 2011.

f. Juniper Networks JUNOS-FIPS 10.4R4 for SRX Series EAL4+ ETR, Version 1.2, December 23 2011.