Certification Report

EAL 3 Evaluation of Juniper Networks Circuit to Packet Series Version 5.4R2

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-142-CR
Version:	1.0
Date:	4 March 2011
Pagination:	i to iii, 1 to 8

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 4 March 2011, 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 and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries.

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

TABLE OF CONTENTS

Executive Summary

Juniper Networks Circuit to Packet Series Version 5.4R2 (hereafter referred to as Juniper CTP 5.4R2), from Juniper Networks, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 3 evaluation.

Juniper CTP 5.4R2 is a software/hardware product that connects Time Division Multiplexing (TDM), Private Branch Exchange (PBX), serial encryption, and analog and digital radio systems across an IP network. Juniper CTP 5.4R2 comprises CTPOS Version 5.4R2 running on the hardware appliances CTP1004, CTP1012, CTP2008, CTP2024 and CTP2056, and the appliance management tool CTPView Version 3.4R2 that runs on a CentOS 5.3 platform in the IT Environment.

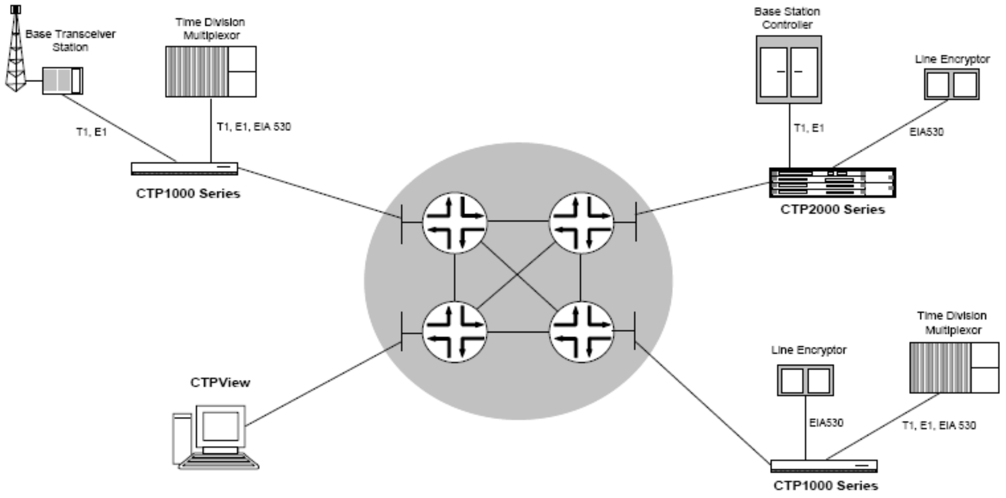

Figure 1- Juniper CTP 5.4R2 deployment

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 22 February 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 Juniper CTP 5.4R2, 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 3 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*.

Communications Security Establishment Canada, as the CCS Certification Body, declares that Juniper CTP 5.4R2 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 evaluation is Juniper Networks Circuit to Packet Series Version 5.4R2 (hereafter referred to as Juniper CTP 5.4R2), from Juniper Networks.

2 TOE Description

Juniper CTP 5.4R2 comprises CTPOS Version 5.4R2 running on the hardware appliances CTP1004, CTP1012, CTP2008, CTP2024 and CTP2056, and the appliance management tool CTPView Version 3.4R2 that runs on a CentOS 5.3 platform in the IT Environment. Deployment is shown in Figure 1, below.

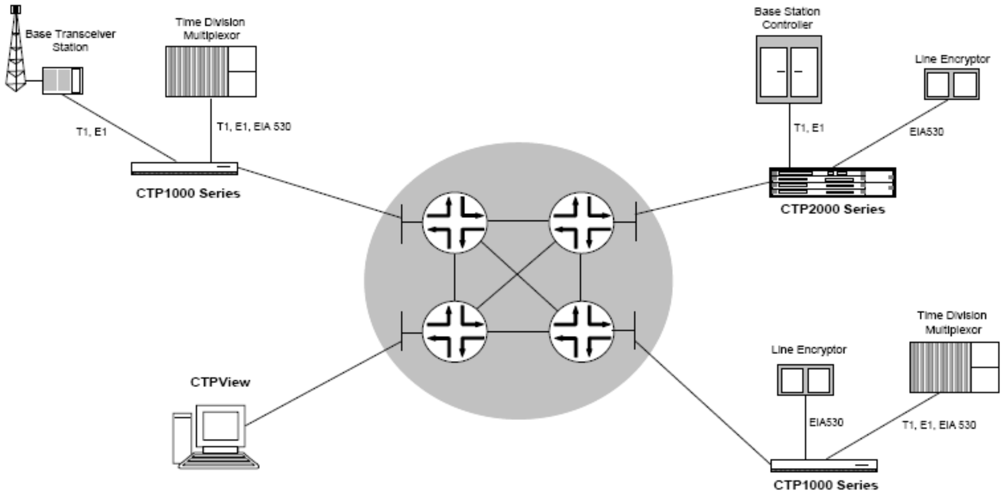

Figure 1- Juniper CTP 5.4R2 deployment

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Juniper CTP 5.4R2 is identified in Section 7 of the Security Target (ST).

4 Security Target

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

Title: Security Target: Juniper Networks Circuit to Packet Series Version 5.4R2
Version: 1.3
Date: 17 February 2011

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

Juniper CTP 5.4R2 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 conformant*, with all security the assurance requirements in the EAL 3 package.

6 Security Policy

Juniper CTP 5.4R2 implements the Virtual Circuit Flow Control Security Policy. This policy enforces rules in terms of what traffic can pass through Juniper CTP 5.4R2. Details of this security policy are found in Section 6 and Section 7.3 of the ST.

In addition, Juniper CTP 5.4R2 implements policies pertaining to Security Audit, User Data Protection, Identification and Authentication and Security Management. Further details on these security policies are found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Juniper CTP 5.4R2 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 Assumptions are 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; and

- Components accessing the management interfaces of the TOE will be located within controlled facilities, and the authorized users of these components 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; and
- The connection between physically separate TOE components is protected from unauthorized tamper, modification, or eavesdropping.

7.3 Clarification of Scope

Juniper CTP 5.4R2 is suitable for use in well-protected environments. It is not intended for environments in which attackers use sophisticated attacks.

8 Evaluated Configuration

The evaluated configuration for Juniper CTP 5.4R2 comprises CTPOS Version 5.4R2 running on the hardware appliances CTP1004, CTP1012, CTP2008, CTP2024 and CTP2056, and the appliance management tool CTPView Version 3.4R2 that runs on a CentOS 5.3 platform in the IT Environment.

The publication entitled Operational User Guidance and Preparative Procedures Supplement: Juniper Networks Circuit to Packet Series Version 5.4R2 describes the procedures necessary to install and operate Juniper CTP 5.4R2 in its evaluated configuration.

9 Documentation

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

- Operational User Guidance and Preparative Procedures Supplement: Juniper Networks Circuit to Packet Series Version 5.4R2;
- CTP Software Configuration Guide *CTP Release 5.2, CTPView Release 3.2*;
- CTPView Server Release Notes *Release 3.4*;
- CTPOS Release Notes *Release 5.4*;
- CTP Hardware Guide, Release 5.4.x; and
- CTPView Security Implementation Guide, Release 3.4R2-p1-rc3.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Juniper CTP 5.4R2, including the following areas:

Development: The evaluators analyzed the Juniper CTP 5.4R2 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 Juniper CTP 5.4R2 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 Juniper CTP 5.4R2 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 Juniper CTP 5.4R2 configuration management system and associated documentation was performed. The evaluators found that the Juniper CTP 5.4R2 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 Juniper CTP 5.4R2 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 Juniper CTP 5.4R2 during distribution to the consumer.

Vulnerability assessment: The evaluators conducted an independent vulnerability analysis of Juniper CTP 5.4R2. 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 the Juniper CTP 5.4R2 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. Security Audit: The objective of this test goal is to ensure that audit events for authentication activity, configuration changes and processing errors of the Virtual Circuit Flow Control SFP are logged as specified;

c. Information Flow Control: The objective of this test goal is to determine the TOE's ability to send and receive network packets that are sent through the TOE from one subject to another;

[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.

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

e. Security Management: The objective of this test goal is to ensure that the TSF can control its data and can perform its management functions as specified.

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. Penetration testing included testing of the CTPView GUI, the CTPView server, and the CTP appliances. The penetration tests focussed on:

- Exploiting default passwords;
- Privilege verification and privilege escalation;
- Password strength;
- Web and network scans for vulnerabilities using commercial vulnerability tools; and
- Cross-site scripting.

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

11.4 Conduct of Testing

Juniper CTP 5.4R2 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 Juniper CTP 5.4R2 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

Juniper CTP 5.4R2 appliances come purpose-built and include comprehensive and clear documentation for configuration and use.

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
PBX	Private Branch Exchange
SFR	Security Functional Requirement
ST	Security Target
TDM	Time Division Multiplexing
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 for TOE Evaluation, 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. Security Target: Juniper Networks Circuit to Packet Series Version 5.4R2, Version 1.3, 17 February 2011; and

e. EAL3 Common Criteria Evaluation of Juniper Networks Circuit to Packet Series Version 5.4R2 Evaluation Technical Report version 1.1, 22 February 2011.