Certification Report

Juniper Networks vGW Series Version 5.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

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, 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 EWA-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 10 June 2013, 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).

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

TABLE OF CONTENTS

Executive Summary

Juniper Networks vGW Series Version 5.5 (hereafter referred to as Juniper vGW), from Juniper Networks, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

The Juniper vGW is a comprehensive security solution for virtualized data centers and clouds capable of monitoring and protecting virtualized environments while maintaining VM host capacity and performance. The Juniper vGW includes a high-performance hypervisor-based stateful firewall, integrated intrusion detection , and virtualization-specific antivirus protection.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 30 April 2013 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 vGW, 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 2 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.* The following augmentation is claimed: ALC_FLR.2 – Flaw Reporting Procedures.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Juniper vGW 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) 2 augmented evaluation is Juniper Networks vGW Series Version 5.5 (hereafter referred to as Juniper vGW), from Juniper Networks, Inc.

2   TOE Description

The Juniper vGW is a comprehensive security solution for virtualized data centers and clouds capable of monitoring and protecting virtualized environments while maintaining VM host capacity and performance. vGW includes a high-performance hypervisor-based stateful firewall, integrated intrusion detection (IDS), and virtualization-specific antivirus (AV) protection.

A detailed description of the Juniper vGW architecture is found in Section 1 of the Security Target (ST).

3   Evaluated Security Functionality

The complete list of evaluated security functionality for Juniper vGW is identified in Section 1.7 of the ST.

4   Security Target

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

Title: Security Target: Juniper Networks vGW Series Version 5.5
Version: 0.5
Date: 25 March 2013

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.*

Juniper vGW is:

a. *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:

- FAV_ACT.1 - Anti-Virus Actions;
- FAV_SCN.1 - Anti-Virus Scanning; and
- IDS_ANL.1 - Analyzer Analysis.

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

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

6   Security Policy

Juniper vGW implements a role-based access control policy to control user access to the system, as well as an information flow control policy to control information entering the system; details of these security policies can be found in Section 7.4 of the ST.

In addition, Juniper vGW implements insert other policies pertaining to security audit, information flow control, identification and authentication, security management, traffic analysis, and virus scanning. Further details on these security policies may be found in Section 7 of the ST.

7   Assumptions

Consumers of Juniper vGW 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:

- There are no general-purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE;

- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error; and

- The TOE does not host public data.

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;

- Information cannot flow among the internal and external networks unless it passes through the TOE.

8   Evaluated Configuration

The evaluated configuration for Juniper vGW comprises:

- vSphere ESX/ESXi 4 or 5.0 hosts;

- VMware Virtual Center (vCenter) server, version 2.5; and

- Microsoft Internet Explorer 7/8 or Mozilla Firefox 3.

The publication entitled *Operational User Guidance and Preparative Procedures Supplement Juniper Networks vGW Series Version 6.0, Version 1.0, April 3, 2012* describes the procedures necessary to install and operate Juniper vGW in its evaluated configuration.

9   Documentation

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

a. Juniper Networks vGW Series Installation and Administration Guide, Release 5.0 r2, version 2, 2012-03-27;

b. Operational User Guidance and Preparative Procedures Supplement Juniper Networks vGW Series Version 6.0, Version 1.0, April 3, 2012; and

c. Juniper vGW Series Event and Alert Messages Reference Guide, 5.0r2, January 25, 2012

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Juniper vGW, including the following areas:

Development: The evaluators analyzed the Juniper vGW 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 vGW security architectural description and determined that the initialization process is secure, 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 Juniper vGW 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 vGW configuration management system and associated documentation was performed. The evaluators found that the Juniper vGW configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Juniper vGW during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the Juniper vGW. 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 Juniper vGW. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Juniper vGW potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to Juniper vGW in its operational environment.

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

11 ITS Product Testing

Testing 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 analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

---

[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.

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 EWA-Canada 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. Concurrent Logins: The objective of this test goal is to confirm that there is no privilege escalation with concurrent logins

c. User Deletion: The objective of this test goal is confirm that deleted users cannot login; and

d. IDS functionality: The objective of this test goal is to confirm that the IDS functionality of the TOE works as intended.

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 Scan: The objective of this test goal is to scan the TOE using a port scanner to identify open ports for potential issues;

b. Vulnerability Identification: Tool Scanning: The objective of this test goal is to scan the TOE for vulnerabilities using automated tools; and

c. Information Leakage Verification: The objective of this test goal is to monitor the TOE for leakage during start-up, shutdown, login, and other scenarios using a packet sniffer.

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

11.4 Conduct of Testing

Juniper vGW 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 EWA-Canada. 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 vGW behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ 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

In order to install the TOE, correct placement within the network is important. It is recommended that the administrator consult with their IT architect to ensure proper support for the appliance in the environment as incorrect placement within the network could lead to traffic not being detected.

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

Acronym/Abbreviation/ Initialization	Description
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation

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 4, July 2009.

c.   Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, July 2009.

d.   Security Target: Juniper Networks vGW Series Version 5.5, 0.5, 25 March 2013.

e.   Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of Juniper Networks, Inc. Juniper Networks vGW Series Version 5.5, v0.5, 30 April 2013.