Certification Report

Trustwave Secure Web Gateway Version 11.0

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-250-CR
Version:	1.0
Date:	17 December 2013
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, 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 17 December 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).

TABLE OF CONTENTS

Executive Summary

Trustwave Secure Web Gateway Version 11.0 (hereafter referred to as SWG), from Trustwave Holdings, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

SWG is a web gateway that protects against next-generation threats from web site access in real time. By detecting new and targeted attacks, it enables users to access the Internet safely. SWG protects against dynamic, cross-component malware threats using real-time code analysis, analyzing the whole composition of a web page.

SWG Real-Time Code Analysis technology provides functionality to detect and block dynamic malware. As inbound and outbound web communication occurs it is dynamically analyzed and viewed by multiple malware engines to determine intent. These engines run in parallel providing the following abilities:

- Detection and blocking of dynamic malware from cross-component attacks
- Detection of malicious code on web pages
- Web page analysis of both single and multiple component attacks

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 7 November 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 SWG, 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.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the SWG 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

[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.

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) augmented evaluation is Trustwave Secure Web Gateway Version 11.0 (hereafter referred to as SWG), from Trustwave Holdings, Inc.

2 TOE Description

SWG is a web gateway that protects against next-generation threats from web site access in real time. By detecting new and targeted attacks, it enables users to access the Internet safely. SWG protects against dynamic, cross-component malware threats using real-time code analysis, analyzing the whole composition of a web page.

SWG Real-Time Code Analysis technology provides functionality to detect and block dynamic malware. As inbound and outbound web communication occurs it is dynamically analyzed and viewed by multiple malware engines to determine intent. These engines run in parallel providing the following abilities:

- Detection and blocking of dynamic malware from cross-component attacks
- Detection of malicious code on web pages
- Web page analysis of both single and multiple component attacks

A detailed description of the SWG architecture is found in 1.6 of the Security Target (ST).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for SWG is identified in 1.6.2 of the ST.

4 Security Target

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

Title: Trustwave Secure Web Gateway Security Target
Version: 1.5
Date: 18 September 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.*

SWG 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:
    - IDS_SDC - System Data Collection
    - IDS_ANL - Analyser Analysis
    - IDS_RCT - Analyser React
    - IDS_RDR - Restricted Data Review; and
    - IDS_STG - System Data Storage.

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

6 Security Policy

SWG implements a role-based access control policy to control administrator 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 of the ST.

In addition, SWG implements policies pertaining to security audit, user, identification and authentication, and security management. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of SWG 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 authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation;
- The TOE can only be accessed by authorized users; and
- The TOE is appropriately scalable to the IT System the TOE monitors.

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 processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access;
- The TOE components will be interconnected by a segregated management network that protects the intra-TOE traffic from disclosure to or modification by untrusted systems or users; and
- The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical modification.

8 Evaluated Configuration

The TOE consists of one instance of the SWG software executing on either a dedicated physical appliance or virtual appliance (two distinct configurations). For the physical appliance, the hardware is part of the TOE. For the virtual appliance, the hardware and hypervisor software are provided by the operational environment.

The evaluated configuration for SWG comprises:

- The TOE software running on one of the following SWG appliances;
  - SWG3000;
  - SWG5000; or
  - SWG7000.

Or;

- The TOE deployed as a virtual appliance running on a hardware platform with the following minimum requirements;
  - VMWare ESXi version 4.1;
  - IBM X3550 M3 2xQuad-Core Intel E5506 2.1 GHz CPU; and
  - 4GB of RAM.

The publication entitled *Trustwave Secure Web Gateway Common Criteria Supplement* describes the procedures necessary to install and operate SWG in its evaluated configuration.

9 Documentation

The Trustwave Holdings, Inc. documents provided to the consumer are as follows:

a. Trustwave Secure Web Gateway Common Criteria Supplement-April 29, 2013;

b. Secure Web Gateway Version 11.0 Quick Start Guide - v2.0, December 2012;

c. Secure Web Gateway Version 11.0 Setup Guide - v2.0, October 2012; and

d. Secure Web Gateway Management Console Reference Guide Version 11.0, 1.0 December 2012.

10 Evaluation Analysis Activities

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

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

The evaluators reviewed the flaw remediation procedures used by developer for the SWG. 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.

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.

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 login: The objective of this test goal is to confirm the use of concurrent logins and that they don't interfere with each other;

c. Creating and deleting of user groups: The objective of this test goal is confirm the ability of an admin to create and delete user groups;

d. Creating and deleting of user accounts: The objective of this test goal is to confirm the ability of an admin to create and delete user accounts; and

e. IP address based Management Console access control: The objective of this test goal is to confirm that the TOE will only accept management connection from a specific IP range.

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 reveal a potential avenue of attack;

[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. Automated vulnerability 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

SWG 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, providing assurance that SWG 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

'The evaluator found some intermittent display issues when using Internet Explorer to access the TOE Management Console. Firefox was found to perform without any issues for the display of the TOE Management Console.

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
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, September 2012.

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

d. Trustwave Secure Web Gateway Security Target,v1.5, 18 September 2013.

e. Evaluation Technical Report for EAL 2+ Common Criteria Evaluation of Trustwave Holdings, Inc. Trustwave Secure Web Gateway Version 11.0, v1.1, 7 November 2013.