Certification Report

EAL 2+ Evaluation of Websense V10000 G2 Web Gateway Appliance v7.6

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-179-CR
Version:	1.0
Date:	18 January 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 18 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:

- Websense is a registered trademark of Websense, 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

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 5

10 Evaluation Analysis Activities 5

11 ITS Product Testing 6

11.1 Assessment of Developer Tests 6
11.2 Independent Functional Testing 7
11.3 Independent Penetration Testing 7
11.4 Conduct of Testing 8
11.5 Testing Results 8

12 Results of the Evaluation 8

13 Evaluator Comments, Observations and Recommendations 8

14 Acronyms, Abbreviations and Initializations 9

15 References 9

Executive Summary

Websense V10000 G2 Web Gateway Appliance v7.6 (hereafter referred to as Websense V10000 G2 7.6), from Websense, Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

Websense V10000 G2 7.6 is a protocol filtering appliance that provides web proxy and traffic filtering.

Web proxy allows the TOE to inspect web content accessed by users and determine if it is malicious or otherwise undesirable. Traffic filtering allows the TOE to inspect non-web traffic in order to determine whether the traffic should be allowed or not, based on the protocol. Web proxy and traffic filtering work together to prevent security breaches.

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 Websense V10000 G2 7.6, 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 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 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.

Communications Security Establishment Canada, as the CCS Certification Body, declares that Websense V10000 G2 7.6 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 Websense V10000 G2 Web Gateway Appliance v7.6 (hereafter referred to as Websense V10000 G2 7.6), from Websense, Inc..

2 TOE Description

Websense V10000 G2 7.6 is a protocol filtering appliance that provides web proxy and traffic filtering.

Web proxy allows the TOE to inspect web content accessed by users and determine if it is malicious or undesirable. Traffic filtering allows the TOE to inspect non-web traffic in order to determine whether the traffic should be allowed or not, based on the protocol. Web proxy and traffic filtering work together to prevent security breaches.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Websense V10000 G2 7.6 is identified in Section 7 of the ST.

4 Security Target

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

Title: Websense, Inc. V10000 G2 Web Gateway Appliance v7.6 Security Target
Version: 1.0
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.*

Websense V10000 G2 7.6 is:

a. *Common Criteria Part 2 extended*, with security functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST:
   - EXT_FDP_ROL – Rollback of TOE configurations

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

Websense V10000 G2 7.6 implements the Proxy Filtering Policy, a role-based access control policy to control user access to the system; details of this security policy can be found in Section 6.2.2 and 7.1.2 of the ST.

In addition, Websense V10000 G2 7.6 implements policies pertaining to security audit, user data protection, identification and authentication, security management and resource utilization. Further details on these security policies may be found in Section 7 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Websense V10000 G2 7.6 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 has been installed and configured according to the appropriate installation guides;
- Administrators who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained and follow all guidance;
- There are one or more competent individuals assigned to manage the TOE and the security of the information it contains; and
- All administrative interfaces are not accessible to non-administrators and only administrators have access to the administrative interfaces to ensure the network is secure.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- All Proxy Filtering Policy-controlled traffic between the internal and external networks traverses the TOE; and
- The TOE is located within a controlled access facility and is physically available to authorized administrators only.

7.3 Clarification of Scope

This section highlights functionality of the TOE which did not reside in the evaluated configuration. The following were not tested or evaluated as part of the Common Criteria Evaluation, which may be included or configured in the purchased product:

- Use of Active Directory or other Directory Server;
- Use of an email server for password resets;
- Use of SNMP;
- Use of Email or Data Security Components; and
- Use of SSH for remote CLI connectivity.

Additionally due to the assumption that the GUI interfaces for administration are protected by the IT environment, they were not inspected for vulnerabilities.

As such the Security Target makes no claim against any of this functionality, and the reader should carefully take this into account.

8 Evaluated Configuration

The evaluated configuration for Websense V10000 G2 7.6 is comprised of Websense Version 7.6 running on the G2 version of the V10000 appliance. The evaluated configuration also includes the following web-based GUI management tools:

- The Appliance Manager GUI;
- The Content Gateway Manager GUI; and
- The Triton GUI.

Additionally the TOE requires a Management Server which hosts the Triton GUI. This server in the evaluated configuration includes the logging components and is to be installed off-appliance in the operational environment for the purposes of managing the TOE. Additionally in the evaluated configuration this management system also includes an SQL Database in order to support the management station.

The publication entitled Websense, Inc. V10000 G2 Web Gateway Appliance v7.6 Guidance Documentation Supplement v0.7 describes the procedures necessary to install Websense V10000 G2 7.6 in its evaluated configuration.

The publication entitled Websense TRITON Unified Security Center Help v7.6 describes the procedures necessary to operate Websense V10000 G2 7.6 in its evaluated configuration.

9 Documentation

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

a. Websense, Inc. V10000 G2 Web Gateway Appliance v7.6 Guidance Documentation Supplement v0.7;

b. Websense TRITON Unified Security Center Help v7.6;

c. Websense Content Manager Help v7.6;

d. Websense TRITON – Web Security Help v7.6;

e. Websense Appliance Manager Help v7.6

f. Websense Release Notes for TRITON Unified Security Center v7.6;

g. Websense Quick Start Guide V10000 G2;

h. Deployment and Installation Center Websense TRITON Enterprise v7.6;

i. Websense Domain Agent Interfaces Reference, Version 0.3; and

j. Websense V10000 v7.6 CLI and Appliance Manager Error Messages, Version 0.1.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Websense V10000 G2 7.6, including the following areas:

Development: The evaluators analyzed the Websense V10000 G2 7.6 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 Websense V10000 G2 7.6 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 Websense V10000 G2 7.6 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 Websense V10000 G2 7.6 configuration management system and associated documentation was performed. The evaluators found that the Websense V10000 G2 7.6 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 Websense V10000 G2 7.6 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Websense, Inc. for Websense V10000 G2 7.6. 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 Websense V10000 G2 7.6. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify Websense V10000 G2 7.6 potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the Websense V10000 G2 7.6 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 2 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 CGI IT Security Evaluation & Test Facility test goals:

a. Repeat of Developer's Tests: The evaluator repeated all the developer tests to gain a deeper understanding of the TOE and the TOE interfaces. All security functions and interfaces were exercised;

b. Security Audit: The objective of this test goal is to determine the TOE’s ability to audit the activity of users;

c. Identification and Authentication: The objective of these tests is to ensure that access to the TOE is restricted to authorized administrators only;

d. Security Management: The objective of this test goal is to ensure that role based access control requirements have been met and that functionality pertaining to the creation, access, review and approval of administrator defined CCS policies operate as specified; and

e. User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data.

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. Use of automated vulnerability scanning tools (NESSUS and NMAP) to discover potential network, platform and application layer vulnerabilities;

b. Use of weak passwords to try and gain access to the TOE’s GUI Management tools;

c. Use of a third party proxy server in an attempt to bypass defined content restrictions;

d. Use of known malicious content files to test the TOE’s capabilities of detecting malicious content that is compressed or obscured; and
e. Changing of session cookie to determine if user is able to gain higher privileges.

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

11.4 Conduct of Testing

Websense V10000 G2 7.6 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 and at the Websense Quality Assurance Laboratories. 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 Websense V10000 G2 7.6 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 noted throughout the testing and vulnerability assessment portion of the evaluation that there are a great deal of configuration options available on the Websense V10000 G2 v7.6.

As the product is shipped with a default permissive stance, the evaluator strongly recommends professional training for any potential administrator on the product and appliance from a qualified training facility in order to support the ST's stated assumption that administrators who manage the TOE are not careless, negligent, or willfully hostile and are appropriately trained and will follow all guidance. An unintentional misconfiguration due to a poorly trained administrator can easily lead to security threats not being countered as expected.

Additionally it is noted that in order to install the Websense V10000 G2 v7.6, 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 on the "N" port for non-http traffic enforcement.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CLI	Command Line Interface
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirements
SNMP	Simple Network Management Protocol
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. Websense, Inc. V10000 G2 Web Gateway Appliance v7.6 Security Target, 1.0, 22 December 2011.

e. Websense V10000 EAL2 ETR 1.0, 23 December 2011