Certification Report

EAL 2 Evaluation of

Symantec Brightmail™ Gateway 9.0.1

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Evaluation number: 383-4-162-CR
Version: 1.0
Date: 26 January 2011
Pagination: I to iii, 1 to 10

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 3.1R3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1R3*. 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, 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 located in Ottawa, Ontario.

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 26 January 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 trademarked or registered trademarks:

- Symantec is a registered trademark of Symantec Corporation

TABLE OF CONTENTS

Executive Summary

Symantec Brightmail™ Gateway 9.0.1 (hereafter referred to as Symantec Brightmail Gateway), from Symantec, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

Symantec Brightmail Gateway offers enterprises a comprehensive gateway-based message-security solution which provides inbound and outbound email security capabilities in one appliance. This appliance can be deployed as a physical or virtual appliance. Symantec Brightmail Gateway does the following to protect the customer environment:

- Detects spam, denial-of-service attacks, and other inbound email threats.
- Leverages a global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections.
- Secures and protects public instant messaging communications with the same management console that it uses to secure and protect email.
- Obtains visibility into messaging trends and events.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 29 December 2010 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 the Symantec Brightmail Gateway, 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 assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1R3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, version 3.1R3*.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Symantec Brightmail Gateway evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will

[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.

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) 2 evaluation is Symantec Brightmail™ Gateway 9.0.1 (hereafter referred to as Symantec Brightmail Gateway), from Symantec.

2 TOE Description

Symantec Brightmail Gateway offers enterprises a comprehensive gateway-based message-security solution which provides inbound and outbound email security capabilities in one appliance. This appliance can be deployed as a physical or virtual appliance. Symantec Brightmail Gateway does the following to protect the customer environment:

- Detects spam, denial-of-service attacks, and other inbound email threats.
- Leverages a global sender reputation and local sender reputation analysis to reduce email infrastructure costs by restricting unwanted connections.
- Secures and protects public instant messaging communications with the same management console that it uses to secure and protect email.
- Obtains visibility into messaging trends and events.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Symantec Brightmail Gateway is identified in Section 6 of the Security Target (ST).

4 Security Target

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

Title: Security Target Symantec Brightmail Gateway 9.0.1
Version: 1.4
Date: 23 December 2010

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1R3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1R3*.

Symantec Brightmail Gateway is:

a. Common Criteria Part 2 conformant, with security functional requirements based on functional components in Part 2;

b. Common Criteria Part 3 conformant, with security assurance requirements based on assurance components in Part 3; and
c. Common Criteria EAL 2 conformant, with all the security assurance requirements from EAL 2 package.

6 Security Policy

Symantec Brightmail Gateway implements an incoming security policy that controls all incoming network traffic via SMTP or Instant Messaging (IM) protocols. Details on this security policy may be found in Section 3.2 of the ST.

In addition, Symantec Brightmail Gateway implements other policies pertaining to Security Audit, User Data protection, Identification and Authentication, and Security Management. Further details on these security policies may be found in the ST.

7 Assumptions and Clarification of Scope

Consumers of the Symantec Brightmail Gateway product 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 Assumption is listed in the ST:

- Personnel authorized to install, configure, and operate Symantec Brightmail Gateway possess appropriate training, are not hostile, and will adhere to the procedures for secure usage of the product.

7.2 Environmental Assumptions

The following Environmental Assumption is listed in the ST:

- Symantec Brightmail Gateway resides within controlled access facilities, which will prevent unauthorized physical access.

7.3 Clarification of Scope

Symantec Brightmail Gateway relies on the environment to provide it physical and logical protection. Symantec Brightmail Gateway provides a level of protection that is appropriate for low robustness environments processing unclassified information. It offers protection against inadvertent or casual attempts to breach system security. It is not intended for situations in which hostile and well funded attackers use sophisticated attacks from within the physical zone.

8 Architectural Information

Symantec Brightmail Gateway is comprised of the following main components:

- Control Center – enables Web-based configuration and administration of the TOE; and
- Scanner – performs email filtering.

The Control Center enables Web-based configuration and administration of the TOE. With a single Control Center, the end user can centrally configure, monitor, and manage all the Scanners in the network. The Control Center also contains *Quarantine*, which is an optional storage area for caught spam.

Each TOE installation has exactly one Control Center. The Control Center communicates with the Agent on each Scanner. From the Control Center's Web-based graphical user interface, a TOE Administrator can:
• Configure, start and stop each Scanner;
• Specify email filtering options for groups of users or for all users at once;
• Monitor consolidated reports and logs for all Scanners;
• See summary information;
• Administer Quarantine; and
• View online help for Control Center screens.

The Scanner component performs email filtering, and a TOE installation can have one or more Scanners. Each Scanner can reside on the same appliance or virtual machine as the Control Center component or on a separate appliance or virtual machine.

9 Evaluated Configuration

The evaluated configuration for Symantec Brightmail Gateway Security comprises:

- Control Center – Brightmail Gateway v9.0.1-10 running on a VMware ESX Server Version 4.0; and
- Scanner - Brightmail Gateway v9.0.1-10 running on a VMware ESX Server Version 4.0.

10 Documentation

The Symantec documents provided to the consumer are as follows:

- Operational User Guidance and Preparative Procedures Supplement Symantec Brightmail Gateway Version 9.0.1;
- Symantec Brightmail™ Gateway 9.0.1 Getting Started;
- Symantec Brightmail™ Gateway 9.0 Installation Guide;
- Symantec Brightmail™ Gateway 9.0 Administration Guide; and
- Symantec Brightmail™ Gateway 9.0.1 Release Notes.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the Symantec Brightmail Gateway, including the following areas:

Development: The evaluators analyzed the Symantec Brightmail Gateway 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 Symantec Brightmail Gateway security architectural description and determined that the initialization process was 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 Symantec Brightmail Gateway preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 were complete and sufficiently detailed to result in a secure configuration.

Life-Cycle Support: An analysis of the Symantec Brightmail Gateway configuration management system and associated documentation was performed. The evaluators found that the Symantec Brightmail Gateway 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 Symantec Brightmail Gateway during distribution to the consumer.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of Symantec Brightmail Gateway. Additionally, the evaluators conducted a review of public domain vulnerability databases. The evaluators identified potential vulnerabilities for testing applicable to the Symantec Brightmail Gateway in its operational environment.

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

12 ITS Product Testing

Testing at EAL 2 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 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 and TOE design was complete.

12.2 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 was the following list of EWA-Canada test goals:

- Initialization: The objective of this test goal is to confirm that the TOE can be installed and configured into the evaluated configuration, as identified in the TOE Description of the Security Target, by following all instructions in the developer's Installation and Administrative guidance;
- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests on the evaluator's TOE installation; and
- Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met;
- Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed;
- Users and Roles: The objective of this test goal is to ensure the users and roles functionality is correct; and
- User Data Protection: The objective of this test goal is to determine the TOE's ability to protect user data.

12.3 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:

[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.

- Port Scanning: The objective of this test goal is to determine if the Scanner or Control Centre opens any ports that could be exploited from the network;
- Internet Search: The objective of this test to search public domain information sources for vulnerabilities for the TOE and its underlying software, and specific hardware or design components used in the TOE;
- Scan for Weaknesses: The objective of this test case is to a scan for known and unknown weaknesses relevant to the TOE type; and
- Leakage Verification: The objective of this test goal is to monitor the TOE for leakage during start up and shut down.

The evaluator conducted a port scan of the Symantec Brightmail Gateway. The only ports found to be open were ones that would be expected to be. The evaluator used a publicly available tool to scan the Symantec Brightmail Gateway for weaknesses, and none were found. The evaluator also used a publicly available packet capture tool to examine output from the Symantec Brightmail Gateway during startup, shutdown and normal operations. The evaluator searched the captured results in an attempt to extract information which might be useful to a potential attacker; no useful information was uncovered.

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

12.4 Conduct of Testing

Symantec Brightmail Gateway 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 Testing (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.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the Symantec Brightmail Gateway behaves as specified in its ST, functional specification, TOE design, and security architecture description.

13 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.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for Symantec Brightmail Gateway includes a comprehensive Installation and Security Guide and an Administrator's Guide.

Symantec Brightmail Gateway is straightforward to configure, use and integrate into a corporate network.

Symantec is strongly committed to secure practices, the CC effort and effective configuration management and delivery processes as evidenced by the high-quality of the CC evaluation evidence and its practical application for Symantec Brightmail Gateway.

15 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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IM	Instant Messaging
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories Canada
SFR	Security Functional requirements
SMTP	Simple Mail Transfer Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 References

This section lists all documentation used as source material for this report:

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1R3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1R3, July 2009.

d. Security Target Symantec Brightmail Gateway 9.0.1, Revision No. 1.4, 23 December 2010.

e. Evaluation Technical Report for EAL 2 Common Criteria of Symantec Corporation Symantec Brightmail Gateway 9.0.1, Document No. 1665-000-D002, Version 1.2, 29 December 2010, Common Criteria Evaluation Number: 383-4-162.