Certification Report

EAL 2+ Evaluation of Proofpoint Protection Server®

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-97
Version: 1.0
Date: 29 September 2008
Pagination: i to iv, 1 to 10

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have 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 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. This certification report, and its associated certificate, applies 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 Standard 17025, General requirements for the accreditation of calibration and testing 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 September 29, 2008, 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 at:
http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and
http://www.commoncriteria.es

This certification report makes reference to the following trademarked names:

- Proofpoint, Proofpoint Protection Server, Proofpoint Messaging Security Gateway, and PLINX are trademarks of Proofpoint Inc;
- Microsoft and Windows are trademarks of Microsoft Corporation;
- Mozilla and Firefox are trademarks of Mozilla Foundation;
- MySQL is a trademark of MySQL AB; and
- Linux is a trademark of Linus Torvalds.

TABLE OF CONTENTS

Executive Summary

The Proofpoint Protection Server® (hereafter referred to as the PPS), from Proofpoint, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

PPS is perimeter email gateway software that integrates virus protection, spam detection, regulatory compliance, and digital asset protection into a comprehensive message management solution. PPS is designed to defend an Information Technology (IT) environment from internal and external email-based threats by scanning all inbound and outbound emails for spam, viruses, connection-level attacks, prohibited text, and other user-definable data. Customers who deploy PPS are typically concerned with one or more of the following:

- Preventing the receipt of spam;
- Preventing the sending or receipt of offensive emails;
- Ensuring email compliance with various regulations, such as HIPAA;
- Protecting the privacy and security of customer, company, and employee data, such as Social Security Numbers; and
- Preventing the loss of intellectual property and trade secrets.

The evaluated version of PPS is delivered to the customer installed on a stand-alone appliance called the Proofpoint Messaging Security Gateway. The appliance hardware and proprietary Linux Operating System (PLINX) are part of the IT environment and are outside the TOE boundary.

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 15 September 2008 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 PPS, 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 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 2.3* (with applicable

[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.

final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed: ALC_FLR.1 – Basic flaw remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the PPS 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 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented evaluation is the Proofpoint Protection Server® (hereafter referred to as PPS), from Proofpoint.

2 TOE Description

PPS is perimeter email gateway software that integrates virus protection, spam detection, regulatory compliance, and digital asset protection into a comprehensive message management solution. PPS is designed to defend an Information Technology (IT) environment from internal and external email-based threats by scanning all inbound and outbound emails for spam, viruses, connection-level attacks, prohibited text, and other user-definable data. Customers who deploy PPS are typically concerned with one or more of the following:

- Preventing the receipt of spam;
- Preventing the sending or receipt of offensive emails;
- Ensuring email compliance with various regulations, such as HIPAA;
- Protecting the privacy and security of customer, company, and employee data, such as Social Security Numbers; and
- Preventing the loss of intellectual property and trade secrets.

The evaluated version of PPS is delivered to the customer installed on a stand-alone appliance (called the Proofpoint Messaging Security Gateway). The appliance hardware and proprietary Linux Operating System (PLINX) are part of the IT environment outside the TOE boundary.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the PPS is identified in Section 5 of the Security Target (ST).

4 Security Target

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

Title: Proofpoint Protection Server® v5.0.4 Security Target
Version: 0.7
Date: 8 September 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

The PPS 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 2 augmented, containing all the security assurance requirements in the EAL 2 package, as well as ALC_FLR.1 - Basic Flaw Remediation.

6 Security Policy

The PPS implements a role-based access control policy to control administrator and user access to the system, as well as an information flow control policy to control information passing through the system; details of these security policies can be found in Section 5 of the ST.

In addition, the PPS implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the PPS 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

Personnel authorized to install, configure, and operate the PPS possess appropriate training and will adhere to the procedures for secure usage of the product described in the ST and guidance documentation.

7.2 Environmental Assumptions

It is assumed that the PPS appliance resides in a physically secure location and only authorized individuals are granted physical access to the host.

For more information about the TOE security environment, refer to Section 3 of the ST (Security Environment).

7.3 Clarification of Scope

The PPS level of protection is appropriate for low robustness environments. It offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing a low attack potential. It is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques

8 Architectural Information

In the evaluated configuration PPS software version 5.0.4.176 runs on the Proofpoint Messaging Server Gateway model 840.

PPS scans all incoming email messages for threats against End Users' workstations or the trusted network itself. All email messages are filtered by modules configured by the Super-user to compare each message against specific policies and rules. Once an email message violates a rule and is assigned to the quarantine, a copy of the email message is sent to the quarantine while the original message is discarded, re-routed, or rejected. This allows for Limited Administrators and End Users to review those quarantined email messages and take action against those emails as the End User sees fit in accordance to company policy.

PPS offers a web-based management interface for reporting, configuration, and management tasks. Authorized Limited Administrators can access the management functionality remotely over Secure Hypertext Transfer Protocol (HTTPS). Limited Administrators are given permission by the Super-user to access specific components within the TOE, such as Digital Assets or Email Alerts. These Limited Administrators can perform all configuration and management tasks for the specified components.

The functionality, databases, files, external interfaces, and other components that compose the PPS software include the following:

- Filtering Agent;
- Reinject Queue;
- Quarantine Consolidation functionality;
- Log Consolidation and Summary functionality;
- Update Utilities;
- Web Servers (e.g., End-user Web Server, Admin Web Server, and API Service Web Server);
- Log Files; and
- MySQL databases (e.g., Message Queue Database, Quarantine Database, Log Database, User Database, etc.).

PPS offers a web-based management interface for reporting, configuration, and management tasks. Administrators can access the management functionality remotely over HTTPS. End users can manage their own email messages over HTTPS. In addition, PPS can automatically retrieve signature updates from Proofpoint-administered servers over HTTPS.

The majority of PPS's main functionality is performed by the Filtering Agent. This component includes the following functionality:

- Spam detection: checks for matches with known Spam signatures;
- Regulatory compliance: provides policy-based filtering for violations of privacy-based or financial transaction regulations
- Digital asset protection: protects confidential information from accidental or deliberate disclosure via email;
- Email firewall: provides policy-based allow/deny functionality for email traffic; and
- Virus Protection: interacts with third-party Anti-Virus engines to scan emails for viruses.

9 Evaluated Configuration

The evaluated configuration comprises PPS v5.0.4.176 running on Proofpoint Messaging Security Gateway model 840. Administrator browsers include Internet Explorer 6, Internet Explorer 7, and Firefox 2.0.

10 Documentation

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

a. Proofpoint Administration Guide - Release 5.0.4, Rev A, June 2008;

b. Installation Guide - Release 5.0.4, Revision A, June 2008;

c. Pre-Installation Requirements, Revision A, June 2008;

d. Quick Start Guide - Messaging Security Gateway P-Series and X-Series, Revision A, June 2008;

e. Proofpoint Protection Server™ Reference Guide - Release 5.0.4, Rev A, June 2008;

f. Proofpoint Release Notes- Release 5.0.4, Rev A, July 30 2008; and

g. Proofpoint Protection Server v5.0.4 Guidance Supplement, 0.3, September 8 2008.

11 Evaluation Analysis Activities

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

Configuration management: An analysis of the PPS development environment and associated documentation was performed. The evaluators found that the PPS configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the PPS during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the PPS functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the PPS user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators reviewed the flaw remediation procedures used by Proofpoint for PPS. 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 PPS ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for PPS and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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 Assessing 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].

Proofpoint employs a rigorous testing process that tests the changes and fixes in each release of the PPS. Comprehensive regression testing is conducted for all releases.

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate.

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:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met;

c. Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed;

d. Users and Roles: The objective of this test goal is to ensure the users and roles functionality (including security management functions) is correct;

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

f. Basic Product Functionality: The objective of this test goal is to exercise the TOE's functionality to ensure that the security claims may not be inadvertently compromised.

[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.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks.

Due to the intended operating environment the penetration testing focussed on attempting to bypass authentication and attempting to enter out of erroneous values within the administrator interface. The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

PPS was subjected to a comprehensive suite of formally documented, independent functional 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.

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that PPS behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL augmented 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 PPS includes comprehensive installation and administration guides as well as a guidance supplement which provides information specific to the evaluated configuration. The PPS is straightforward to configure, use and integrate into a corporate network.

EWA-Canada performed a site visit to review developer processes (ACM, ADO, and ALC). Proofpoint, Inc. Configuration Management (CM) and Quality Assurance (QA) provide the

requisite controls for managing all CM/QA activities. Though development security was not part of the evaluation, the evaluators observed that the developer was exceptionally conscious of security. The physical, procedural, and personnel security measures meet or exceed the assurance requirements of higher-level CC evaluations. This is reported on in the CC Evaluation Site Visit Report. This document contains proprietary and confidential Proofpoint information.

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
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
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

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 1.0.

b. Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.

d. Proofpoint Protection Server® v5.0.4 Security Target, Revision No. 0.7, 8 September 2008.

e. Evaluation Technical Report (ETR) Proofpoint Protection Server®, EAL 2+ Evaluation, Common Criteria Evaluation Number: 383-4-97, Document No. 1584-000-D002, Version 1.4, 3 September 2008.