Certification Report

EAL 2+ Evaluation of

Blue Coat ProxySG Operating System

Version 4.2.5.1

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-74-CR
Version:	1.0
Date:	14 November 2007
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 (CSE), 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 CSE, 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.

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 DOMUS IT Security Laboratory, a division of NUVO Network Management, 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) to which the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 14 November 2007, 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.commoncriteriaportal.org.

This certification report makes reference to the following trademarked or registered trademarks:

- ProxySG is a registered trademark of Blue Coat Systems, Inc.

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

TABLE OF CONTENTS

Executive Summary

The Blue Coat ProxySG Operating System v4.2.5.1 (hereafter referred to as the ProxySG OS v4.2.5.1), from Blue Coat Systems, Inc. is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 augmented.

The ProxySG OS v4.2.5.1 is a proprietary operating system that runs on appliances manufactured by Blue Coat Systems. The ProxySG OS v4.2.5.1 provides a layer of security between an internal network and an external network (typically an office network and the Internet) by enforcing information flow rules on selected traffic protocols.

DOMUS IT Security Laboratory, a division of NUVO Network Management, is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 30 October 2007, 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 ProxySG OS v4.2.5.1, 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[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 IT Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for IT Security Evaluation, version 2.3*. The following augmentation is claimed: ALC_FLR.1 – Basic flaw remediation

CSE, as the CCS Certification Body, declares that the ProxySG OS v4.2.5.1 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 evaluation technical report 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 the ProxySG Operating System, Version 4.2.5.1 (hereafter referred to as the ProxySG OS v4.2.5.1), from Blue Coat Systems, Incorporated.

2 TOE Description

The ProxySG OS v4.2.5.1 is a proprietary operating system that runs on appliances manufactured by Blue Coat Systems. The ProxySG OS v4.2.5.1 provides a layer of security between an internal network and an external network (typically an office network and the Internet) by acting as a proxy, and enforcing information flow rules on selected protocol traffic.

In order to act as a proxy and enforce information flow rules on protocol traffic, all of the targeted traffic must flow through the appliance. Arranging for controlled protocol traffic to flow through the appliance requires configuration of the organization's network environment.

There are two kinds of network deployments: explicit and transparent. In an explicit deployment, the users' client software (e.g. web browser) is configured to access the external network via the ProxySG OS v4.2.5.1. The client software presents the traffic to the internal network port of the ProxySG OS v4.2.5.1 for service. In a transparent deployment, the network and ProxySG OS v4.2.5.1 are configured so that the ProxySG OS v4.2.5.1 intercepts controlled protocol traffic intended for the external network. In this configuration, the users' software is not changed and the user is unaware that controlled protocol traffic is passing through the ProxySG OS v4.2.5.1.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the ProxySG OS v4.2.5.1 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: Blue Coat Systems, Inc. ProxySG Operating System v4.2.5.1 Security Target
Version: Version 0.94
Date: 19 October 2007

5 Common Criteria Conformance

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

The ProxySG OS v4.2.5.1 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 security assurance requirements in the EAL 2 package, as well as the following: ALC_FLR.1 – Basic flaw remediation

6 Security Policy

The ProxySG OS v4.2.5.1 implements a Proxy SFP (Security Functional Policy) and an Administrative Access SFP.

After initial installation and configuration, the ProxySG OS v4.2.5.1 is operational and behaves as a proxy that, by default, denies all traffic. To enable controlled protocol traffic flow, the authorized administrator must define the Proxy SFP information flow policy rules.

The information flow policy rules can include the requirement for end user authentication. The authorized administrator defines the end users to be authenticated by using the ProxySG OS v4.2.5.1 management interface to create unique user accounts in a local user list.

The policy rules that define the Proxy SFP and Administrative Access SFP are expressed using the syntax and rules described in the Blue Coat Systems, Inc. ProxySG Content Policy Language Guide, 4.2.5 (Document Number 231-02780).

The ProxySG OS v4.2.5.1 security policy detail can be found in Section 2.2.1 and Section 5.1 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the ProxySG OS v4.2.5.1 should consider assumptions about usage and environmental settings as requirements for the product’s installation and its operating environment. This will help to ensure the proper and secure operation of the ProxySG OS v4.2.5.1.

7.1 Secure Usage Assumptions

Administrators are non-hostile and follow all administrator guidance. Administration is competent and ongoing.

The ProxySG OS v4.2.5.1 is installed and configured according to the installation guide.

Administrator and end user passwords are at least eight characters in length and comprise at least one letter (from a set of 26 upper-case letters and 26 lower-case letters), one special character or symbol (from a set of 32), and one number (from a set of 10).

7.2 Environmental Assumptions

The ProxySG OS v4.2.5.1 is located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware.

Physical access to the appliance running the ProxySG OS v4.2.5.1 is restricted to authorized persons.

All plaintext-controlled protocol traffic between the internal and external networks traverses the ProxySG OS v4.2.5.1 appliance; there is no other connection between the internal and external networks for plaintext-controlled protocol traffic.

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

7.3 Clarification of Scope

The ProxySG OS v4.2.5.1 was designed and intended for use in a structured corporate environment. In this type of environment, users will not typically be allowed to install programs on their machines or change system settings. Administrators will set policy that controls what users are, and are not allowed, to do.

The ProxySG OS v4.2.5.1 is designed to control only specific protocols on specific ports. It is not intended to protect user data or sessions flowing through the ProxySG OS v4.2.5.1, but rather to prevent users from accessing specific protocol and port combinations, and web content.

Protection against attacks such as Session Hijacking [2] and Traffic Interception fall outside the ProxySG OS v4.2.5.1 intended use, and should be addressed by other security mechanisms such as firewalls and Intrusion Detection Systems.

8 Architectural Information

The ProxySG OS v4.2.5.1 is a proprietary operating system that runs on custom, purpose-built hardware. The ProxySG OS v4.2.5.1 comprises a kernel, that provides the basic operating system functions, and the following four subsystem groups: Proxy, Administration, Policy, and Support. The Support subsystem is further decomposed into the four modules: Authentication Subsystem, Content Filtering Subsystem, Logging Subsystem, and Registry Subsystem. Further details about the system architecture are proprietary to the vendor, and are not provided in this report.

9 Evaluated Configuration

The ProxySG OS v4.2.5.1 evaluated configuration comprises the ProxySG OS v4.2.5.1 running on the following Blue Coat Systems appliances: SG200, SG510, SG810, and SG8100. All appliances run the same ProxySG OS v4.2.5.1 binary image.

Protocols controlled by the ProxySG OS v4.2.5.1 that are included in the evaluated configuration are: Hypertext Transfer Protocol (HTTP); File Transfer Protocol (FTP); SOCKS (abbreviation for SOCKetS) and Instant Messaging (AOL, Microsoft Network, and Yahoo!)

10 Documentation

The ProxySG Operating System v4.2.5.1 documents provided to the consumer are as follows:

- Blue Coat Systems SG200, SG510, SG810, and SG8100 Series Installation Guide;
- Blue Coat Systems, Inc. ProxySG Operating System v4.2.5.1 Readme: Installation, Generation, Startup, and Administrative Guidance;
- Blue Coat Systems ProxySG Command Line Interface Reference;
- Blue Coat Systems ProxySG Configuration and Management Guide;
- Blue Coat SGOS 4.2.x Release Notes;
- Blue Coat Systems ProxySGTM Content Policy Language Guide;
- Blue Coat Systems ProxySG SGOS 4.x Upgrade Guide; and
- Blue Coat Systems Deployment Guide.

[2] Session Hijacking refers to the exploitation of a valid computer session to gain unauthorised access to information or services in a computer system.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the ProxySG OS v4.2.5.1, including the following areas:

Configuration management: An analysis of the ProxySG OS v4.2.5.1 CM system and associated documentation was performed. The evaluators found that the ProxySG OS v4.2.5.1 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 ProxySG OS v4.2.5.1 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 ProxySG OS v4.2.5.1 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 ProxySG OS v4.2.5.1 administrator and user guidance documentation and determined that it sufficiently and unambiguously described how to securely administer and use 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 Blue Coat Systems, Inc. for the ProxySG OS v4.2.5.1. 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 ProxySG OS v4.2.5.1 ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the ProxySG OS v4.2.5.1 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 EAL2 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 [3].

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.

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 all 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 DOMUS IT Security Laboratory test goals:

The tests focused on the following areas, based upon the security functional requirements in the ST and the security functions defined in the functional specification:

- Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;
- Audit: The objective of this test goal is to ensure that the System Event Logging and Access Logging requirements have been met;
- Identification and Authentication: The objective of this test goal is to ensure that access to the management capability was restricted to authorized administrators;
- User Data Protection: The objective of this test goal is to ensure that the security policy rules are enforced; and

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

- Security Management: The objective of this test goal is to ensure that authorized administrators are able to manage and configure the ProxySG OS v4.2.5.1.

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:

- Reconnaissance;
- Port Scanning;
- Bypassing;
- Monitoring the network traffic; and
- Denial-of-service attack

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

12.4 Conduct of Testing

The ProxySG OS v4.2.5.1 was subjected to a comprehensive suite of formally-documented, independent, functional and penetration tests. The testing took place at the developer’s facility in Sunnyvale, California, USA*,* and at the ITSET facility at DOMUS IT Security Laboratory located in Ottawa, Ontario, 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 separate Test Results document.

12.5 Testing Results

The developer’s tests and independent functional tests yielded the expected results, giving assurance that the ProxySG OS v4.2.5.1 behaves as specified in its ST and functional specification.

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

Consumers should review the security aspects of the intended environment defined in Section 3 of the ST when deploying the ProxySG OS v4.2.5.1.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/Initialization	Description
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CPL	Certified Products List
CR	Certification Report
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
SOCKS	Abbreviation for SOCKetS
SFP	Security Functional Policy
ST	Security Target
TOE	Target of Evaluation

16 References

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

a) Canadian Common Criteria Evaluation and Certification Scheme (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) Blue Coat Systems, Inc. ProxySG Operating System v4.2.5.1 Security Target, Version 0.94, 19 October 2007.

e) Evaluation Technical Report for EAL2+ Evaluation of ProxySG Operating System v4.2.5.1, Version 0.7, 30 October 2007.