Certification Report

EAL 2+ Evaluation of the Blue Coat ProxySG® v5.3.1.9 Appliance Build Number 36410 running on SG510, SG810, and SG8100

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-93-CR
Version: 1.0
Date: 6 March 2009
Pagination: 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 2, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2. 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 the DOMUS IT Security Laboratory 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 6 March 2009, 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/its-sti/services/cc/cp-pc-eng.html and http://www.commoncriteriaportal.org/products.html.

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

- ProxySG is a registered trademark of Blue Coat Systems, Incorporated;
- SGOS is a registered trademark of Blue Coat Systems, Incorporated;
- Broadcom is trademark of Broadcom Corp; and
- Cavium is a trademark of Cavium Networks.

TABLE OF CONTENTS

Executive Summary

Blue Coat ProxySG® v5.3.1.9 Appliance Build Number 36410 running on the SG510, SG810, and SG8100 (hereafter referred to as ProxySG), from Blue Coat Systems, Incorporated, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 2 augmented evaluation.

ProxySG is a product family that provides traffic acceleration and 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.

The DOMUS IT Security Laboratory is the CCEF that conducted the evaluation. This evaluation was completed on 17 February 2009 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 ProxySG, 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 2 (with applicable final interpretations), for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2. The following augmentation is claimed: ALC_FLR.1 – Basic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the ProxySG 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 Blue Coat ProxySG v5.3.1.9 running on the SG510, SG810, and SG8100 (hereafter referred to as ProxySG), from Blue Coat Systems, Incorporated.

2 TOE Description

ProxySG is a product family that provides traffic acceleration and 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.

3 Evaluated Security Functionality

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

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
ProxySG 510 and ProxySG 810	*Pending* [2]
ProxySG 8100	*Pending*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in ProxySG:

Cryptographic Algorithm	**Standard**	**Certificate #**
Triple-DES (3DES)	FIPS 46-3	706
Advanced Encryption Standard (AES)	FIPS 197	859
Rivest Shamir Adleman (RSA)	ANSI x9.31	413
Secure Hash Algorithm (SHA-1)	FIPS 180-2	854
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	476
Digital Signature Algorithm (DSA)	FIPS 186-2	310
ANSI x9.31 RNG	ANSI x9.31	491

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

4 Security Target

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

Title: Blue Coat Systems, Inc. ProxySG® v5.3.1.9 running on SG510, SG810, and SG8100 Security Target
Version: 0.6
Date: 21 October 2008

5 Common Criteria Conformance

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 2 (with applicable final interpretations), for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2.

ProxySG 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:
   - FIA_ADM_PCR.1(a) - Password controlled role;
   - FIA_ADM_PCR.1(b) - Password controlled role; and
   - EXT_FRU_ARP.1 – Health check alarms.

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 Policies

ProxySG implements an Administrative Access Policy that defines the rules for access to administrative functions; a Proxy Policy that defines the rules for traffic flow; and a WAN Optimization Policy that defines the rules for traffic optimization and acceleration.

In addition, ProxySG implements policies pertaining to security audit, cryptographic support, identification and authentication, security management, protection of the TSF, resource utilization, and TOE access.

Further details on these security policies may be found in Section 1.4.2 of the ST.

7 Assumptions and Clarification of Scope

Consumers of ProxySG 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 ProxySG.

7.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The ProxySG device has been installed and configured according to the appropriate installation guides;
- Administrators are non-hostile and follow all administrator guidance when using the TOE. Administration is competent and on-going; and
- Passwords for administrative access to the TOE and for End User accounts are at least five characters in length, and are not dictionary words.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The TOE is located in an environment that provides physical security, uninterruptible power, air conditioning, and all other conditions required for reliable operation of the hardware; and
- All Proxy SFP-controlled protocol traffic between the Internal and External Networks traverses the ProxySG device; there is no other connection between the Internal and External Networks for Proxy SFP-controlled protocol traffic.

7.3 Clarification of Scope

The ProxySG was designed and intended for use in a structured corporate environment where users will not typically be allowed to install programs on their machines, or change system settings.

Protection against attacks such as Session Hijacking[3] and Traffic Interception fall outside the ProxySG intended use, and should be addressed by other security mechanisms such as firewalls and Intrusion Detection Systems.

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

8 Architectural Information

ProxySG comprises ProxySG® v5.3.1.9 which is a proprietary operating system which is installed on an SG510, SG810, or SG8100 which are purpose built hardware appliances.

ProxySG® v5.3.1.9 comprises the kernel, that provides the basic operating system functions, and the subsystems: Management; Proxy; Authentication; Policy; Registry; Logging; Crypto; Alerts; and Content Filtering. Further details about the ProxySG® v5.3.1.9 and appliance architectures are proprietary to the vendor, and are not provided in this report.

9 Evaluated Configuration

The ProxySG evaluated configuration comprises ProxySG® v5.3.1.9 Appliance Build Number 36410 installed on an SG510, SG810, or SG8100 appliance with FIPS accelerator card options: no accelerator card, Broadcom 5825 SSL accelerator card, or Cavium CN1010 SSL accelerator card.

10 Documentation

The ProxySG documents provided to the consumer are as follows:

a) Blue Coat Systems, Inc. ProxySG® v5.3.1.9 running on SG510, SG810, and SG8100 Guidance Supplement v0.4;
b) Blue Coat Systems, Inc. ProxySG® v5.3.1.9 running on SG510, SG810, and SG8100 Administrative Guidance;
c) Blue Coat Systems SG Appliance Document Suite (SGOS version 5.3);
d) Blue Coat SGOS 5.3.x Release Notes (Version: SGOX 5.3.x)
e) Blue Coat Systems SG510 Series Installation Guide (Version: SGOS 5.3.x);
f) Blue Coat Systems SG810 Series Installation Guide (Version: SGOS 5.3.x); and
g) Blue Coat Systems SG8100 Series Installation Guide (Version: SGOS 5.3.x).

11 Evaluation Analysis Activities

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

Development: The evaluators analyzed the ProxySG functional specification and design documentation and determined that the design completely and accurately instantiated the security functional requirements. The evaluators analyzed the ProxySG security architectural description and determined that the initialization process was secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

Guidance Documents: The evaluators examined the ProxySG 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 ProxySG configuration management system and associated documentation was performed. The evaluators found that the ProxySG 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 ProxySG during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by Blue Coat Systems, Inc. for ProxySG. 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 ProxySG. Additionally, the evaluators conducted a search of public domain vulnerability databases to identify ProxySG potential vulnerabilities. The evaluators identified potential vulnerabilities for testing applicable to the ProxySG 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[4].

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

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

12.2 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 DOMUS IT Security Laboratory test goals:

- Repeat of Developer's Tests. The objective of this test goal is to repeat 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.
- Cryptographic Support. The objective of this test goal is to ensure that all cryptographic functionality was properly exercised.
- Identification and Authentication. The objective of this test goal is to ensure that access to the management capability was restricted to authorized administrators.
- SFP implementation. The objective of this test goal is to ensure that the security policy rules are enforced.
- Security Management. The objective of this test goal is to ensure that authorized administrators are able to manage and configure the ProxySG.
- TOE Access. The objective of this test goal is to ensure that the TOE terminates a user session after a period of 15 minutes of inactivity.

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:

- Reconnaissance. Wireshark was run to view available plaintext network traffic.
- Port Scanning. Nmap was used to scan for unnecessary open ports.
- Denial-of-service attack. A SynFlood attack was run against the ProxySG.

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

12.4 Conduct of Testing

The ProxySG 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 DOMUS IT Security Laboratory. 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 ProxySG 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.

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
SFP	Security Functional Policy

16 References

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

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 2, September 2007.

d. Blue Coat Systems, Inc. ProxySG® v5.3.1.9 running on SG510, SG810, and SG8100 Security Target v0.6, 21 October 2008.

e. Evaluation Technical Report v1.7, Blue Coat Systems, Inc. ProxySG Version 5.3.1.9 running on the SG510, SG810, and SG8100 EAL 2 + February 17, 2009.