Certification Report

EAL 4+ Evaluation of Blue Coat ProxySG SG510, SG810, and SG9000 running SGOS v5.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-169-CR
Version: 1.0
Date: 9 March 2012
Pagination: i to iii, 1 to 11

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 9 March 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 registered trademarks:

- Blue Coat, ProxySG, SGOS, Blue Touch Online and the Blue Coat logo are registered trademarks of Blue Coat Systems, Inc. in the United States and other countries.

TABLE OF CONTENTS

Executive Summary

Blue Coat ProxySG SG510, SG810, and SG9000 running SGOS v5.5 (hereafter referred to as ProxySG 5.5), from Blue Coat Systems, Inc, is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

ProxySG 5.5 consists of appliances manufactured by Blue Coat Systems running a proprietary operating system. The ProxySG OS v5.5 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. In addition, the system also provides the ability to optimize Wide-Area-Network (WAN) traffic.

ProxySG 5.5 is deployed as a purpose-built hardware/software appliance installed at each site and can be configured to provide transparent forward proxy services to all internal users.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 02 March 2012 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 5.5, 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 4 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 the ProxySG 5.5 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) 4 augmented evaluation is Blue Coat ProxySG SG510, SG810, and SG9000 running SGOS v5.5 (hereafter referred to as ProxySG 5.5), from Blue Coat Systems, Inc.

2 TOE Description

ProxySG 5.5 consists of appliances manufactured by Blue Coat Systems running a proprietary operating system. ProxySG 5.5 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. In addition, ProxySG 5.5 provides the ability to optimize Wide Area Network (WAN) traffic.

ProxySG 5.5 is deployed as a purpose-built hardware/software appliance installed at each site and can be configured to provide transparent forward proxy services to all internal users.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for ProxySG 5.5 is identified in Section 6 of the ST.

ProxySG 5.5 provides encryption and decryption of all data transmitted between the TOE using a FIPS 140-2-validated cryptographic module. The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
ProxySG 510-5, 510-10, 510-20, 510-25, 810-5, 810-10, 810-20, 810-25	*Pending* [2]
ProxySG 9000-10, 9000-20, 9000-20B	*Pending*

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in ProxySG 5.5:

Cryptographic Algorithm	**Certificate #**
Triple-DES (3DES)	1224

[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.

Advanced Encryption Standard (AES)	1885
Secure Hash Standard (SHS)	1656
Deterministic Random Bit Generators (DRBG) - Random Number Generator (RNG) based on NIST SP 800-90	987
Rivest Shamir Adleman (RSA)	962
Keyed-Hash Message Authentication Code (HMAC)	1127

4 Security Target

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

Title: Blue Coat Systems, Inc. ProxySG SG510, SG810, and SG9000 running SGOS v5.5 Security Target
Version: v1.3
Date: 23 February 2012

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.*

ProxySG 5.5 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_PCR_EXT.1 – Password controlled role; and
    - FRU_ARP_EXT.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 4 augmented*, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.2 – Flaw Reporting Procedures.

6 Security Policy

ProxySG 5.5 implements an Administrative Access Security Functional Policy (SFP) which ensures administrative interfaces are available only under specific rules using attributes such as authenticated identity, group membership and time of day.

ProxySG 5.5 also implements two information flow control policies, the Proxy SFP and the WAN Optimization SFP. Both policies enforce rules for the transit traffic, in terms of what

traffic can pass through the TOE, and the actions that need to take place on the traffic as it passes through the TOE.

Details of these security policies can be found in Section 1.4.2.3 of the ST.

In addition, ProxySG 5.5 implements policies pertaining to security audit, cryptographic support, identification and authentication, security management, protection of TOE security functionality, resource utilization and TOE access. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of ProxySG 5.5 should consider assumptions about usage, policies in place 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:

- Administrators are non-hostile and follow all administrator guidance when using the TOE. Administration is competent and on-going;
- The TOE has been installed and configured according to the appropriate installation guides; 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. Physical access to the appliance is restricted to authorized persons; 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

ProxySG 5.5 offers protection against inadvertent or casual attempts to breach system security by unsophisticated attackers possessing enhanced-basic attack potential. ProxySG

5.5 is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Evaluated Configuration

The evaluated configuration for ProxySG 5.5 comprises the software SGOS v5.5 running on one of the following appliances:

- ProxySG 510/810-5
- ProxySG 510/810-10, 510/810-20, 510/810-25 with a Cavium CN1010 PCI Extended (PCI-X) card, or a BCM5825 PCI-Extended (PCI-X) card
- ProxySG 9000-10, 9000-20, 9000-20B with a Cavium CN1620 PCI-Express (PCIe) card

For all the above appliance models, the appliance type can be either Mach5 edition (For example, ProxySG 510-5-M5) for WAN optimization, or Proxy edition (For example, ProxySG 510-5-PR) for Proxy and WAN optimization features. No additional hardware or environmental components are required for the TOE to function in the evaluated configuration.

The publication entitled *Blue Coat Systems, Inc. ProxySG SG510, SG810, and SG9000 running SGOS v5.5 Guidance Supplement v0.5* describes the procedures necessary to install and operate ProxySG 5.5 in its evaluated configuration.

9 Documentation

The Blue Coat Systems, Inc documents provided to the consumer are as follows:

a. Blue Coat Systems, Inc. ProxySG SG510, SG810, and SG9000 running SGOS v5.5 Guidance Supplement v0.5;

b. Blue Coat Systems SGOS Administration Guide, Version 5.5.x, 231-03082,SGOS 5.5.4-01/2011;

c. Blue Coat SGOS 5.5.x. Release Notes, SGOS 5.5.7.1, 2.21, 11/20/2011;

d. Blue Coat Systems ProxySG Appliance Command Line Interface Reference, version SGOS 5.5.x, 231-03035, SGOS 5.5.4-08/2011;

e. Blue Coat Systems ProxySG Appliance Content Policy Language Reference, version SGOS 5.5.x, 231-03019, SGOS 5.5.4-07/2011;

f. Blue Coat Systems ProxySG Appliance SGOS 5.5.x Upgrade/Downgrade Feature Change Reference, Version SGOS 5.5.x, 231-03034, SGOS 5.5.2-03/2010;

g. Blue Coat Systems ProxySG Appliance Visual Policy Manager Reference and Advanced Policy Tasks, SGOS Version 5.5.x, 231-03015, SGOS 5.5.2-03/2010;

h. Blue Coat ProxySG Quick Start Guide ProxySG 210 ProxySG 510 ProxySG 810 ProxySG 9000 Series, 231-03122, Rev B.3;

i. Blue Coat Systems SG510 Series Installation Guide, Version: SGOS 5.2.x, 231-02942, B.0;

j. Blue Coat Systems SG810 Series Installation Guide, Version: SGOS 5.2.x, 231-02941, B.0;

k. Blue Coat 510/810 Series FIPS Compliant Tamper Evident Faceplate and Label Installation Guide, 231-02995, A-0;

l. Blue Coat SG9000 Series FIPS Compliant Tamper Evident Shutter and Label Installation Guide, 231-03063, A.1;

m. Blue Coat Using FIPS Mode on the ProxySG, 231-03154, March 2011; and

n. Blue Coat Systems ProxySG Appliance, SGOS 5.5.x Upgrade/Downgrade Guide, SGOS Version 5.5.x, N/A, Version 1.3 (03/2010).

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of ProxySG 5.5, including the following areas:

Development: The evaluators analyzed the ProxySG 5.5 functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the ProxySG 5.5 security architectural description and determined that the initialization process is 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 ProxySG 5.5 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 ProxySG 5.5 configuration management system and associated documentation was performed. The evaluators found that the ProxySG 5.5 configuration items were clearly marked and could be modified and controlled by automated tools. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorised access to the configuration items.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of ProxySG 5.5 during distribution to the consumer.

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the ProxySG 5.5 design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Blue Coat Systems, Inc for ProxySG 5.5. 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 5.5. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the ProxySG 5.5 in its operational environment.

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

11 ITS Product Testing

Testing at EAL 4 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[3].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

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 objective of this test goal is to repeat a subset of the developer's tests;

b. Altering Signed Configuration Files: This test case demonstrates that altered signed configuration files will not be applied to the appliance;

c. Administrator Session Timeout: This test case demonstrates the timeout mechanism for the Command Line Interface (CLI) and the Java Management Console (JMC) interface; and

d. Use of Advanced Uniform Resource Locator (URL) command: This test case demonstrates the Advanced-URL command and how it can be used by privileged and non-privileged users of the system.

11.3 Independent Penetration Testing

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

a. Port Scan: The purpose of this test case is to identify all open ports on the TOE;

[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.

b. Monitor for Information Leakage: The purpose of this test is to determine if the TOE is leaking any information that might be useful to an attacker;

c. Locking out the Administrative Console User: The purpose of this test is to attempt to lock out the administrative console user and cause a denial of service;

d. Delivering Active Content: The purpose of this test is to attempt to deliver active content to the end-user's browser while the appliance is actively engaged in removing it;

e. Cross-Site Scripting within Authentication and Exception Pages: The objective of this test is to determine if there are any obvious Cross-Site Scripting (XSS) vulnerabilities when using Uniform Resource Locator (URL) based substitution variables within authentication and exception pages; and

f. Reverse Proxy Server Cache Poisoning: The objective of this test is to determine if the TOE is vulnerable to cache poisoning attacks.

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

11.4 Conduct of Testing

ProxySG 5.5 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. 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 ProxySG 5.5 behaves as specified in its ST, functional specification, TOE design and security architecture description.

12 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ 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 numerous configuration options available on the ProxySG 5.5. As such the evaluator strongly recommends professional training for ProxySG 5.5 administrators from a qualified training facility. It is recommended that ongoing administration activities involve periodic reviews of the Blue Coat Knowledge Base (KB) as well as the Security Advisories.

14 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CAC	Common Access Card
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
JMC	Java Management Console
KB	Knowledge Base
PALCAN	Program for the Accreditation of Laboratories - Canada
SFP	Security Functional Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
URL	Uniform Resource Locator
WAN	Wide Area Network
XSS	Cross-Site Scripting

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. Blue Coat Systems, Inc. ProxySG SG510, SG810, and SG9000 running SGOS v5.5 Security Target, v1.3, 23 February 2012.

e. Blue Coat Systems, Inc. ProxySG SG510, SG810 and SG9000 running SGOS ProxySG SG510, SG810 and SG9000 running SGOS v5.5 Common Criteria EAL4+ ETR, Version 0.5, March 2, 2012.