Certification Report

Blue Coat ProxySG SG600, SG900, SG9000 running SGOS v6.5

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-268-CR
Version:	1.0
Date:	8 September 2014
Pagination:	i to iii, 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 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. 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, 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, 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) provide 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/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.

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, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 8 September 2014, 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 trademarks or registered trademarks:

- Blue Coat, SGOS and ProxySG are registered trademarks of Blue Coat Systems, Inc.

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

TABLE OF CONTENTS

Executive Summary

Blue Coat ProxySG SG600, SG900, SG9000 running SGOS v6.5 (hereafter referred to as Blue Coat ProxySG), from Blue Coat Systems, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that Blue Coat ProxySG is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

Blue Coat ProxySG is a proprietary OS and hardware appliance that together serve as an Internet proxy. The purpose of the appliance is to provide a layer of security between an Internal and External Network (typically an office network and the Internet), and to provide WAN optimization for traffic passing between networks.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 30 July 2014 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 Blue Coat ProxySG, and the security functional/assurance 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.

Communications Security Establishment, as the CCS Certification Body, declares that the Blue Coat 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).

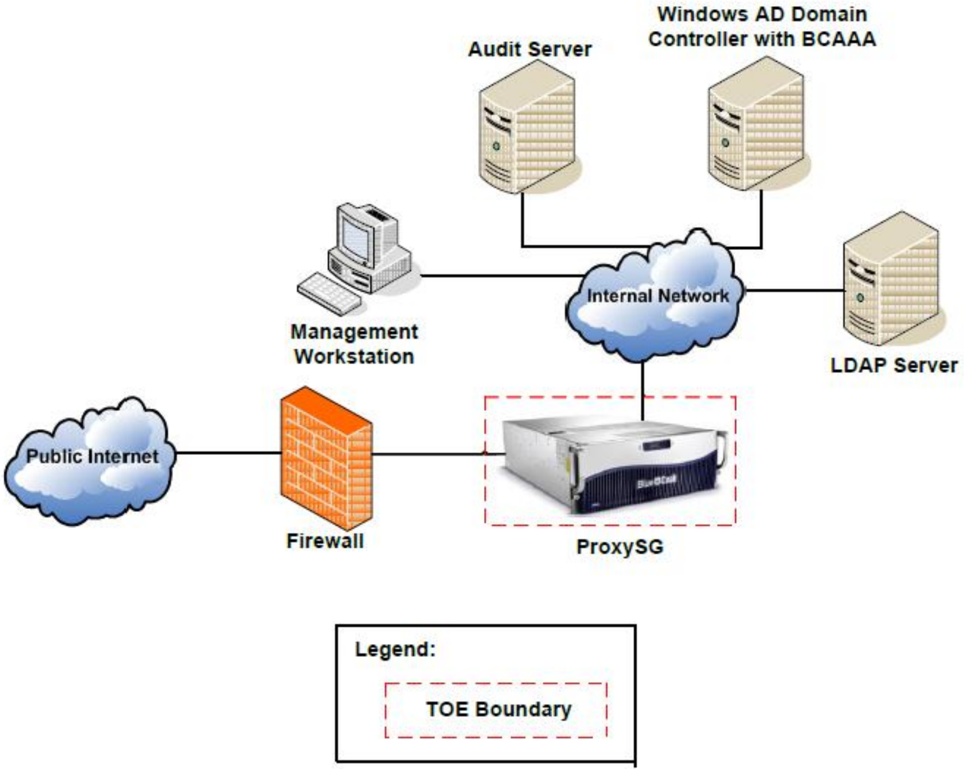
1 Identification of Target of Evaluation

Blue Coat ProxySG SG600, SG900, SG9000 running SGOS v6.5 (hereafter referred to as Blue Coat ProxySG), from Blue Coat Systems, Inc., is the Target of Evaluation. The Blue Coat ProxySG is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

2 TOE Description

Blue Coat ProxySG is a proprietary OS and hardware appliance that together serve as an Internet proxy. The purpose of the appliance is to provide a layer of security between an Internal and External Network (typically an office network and the Internet), and to provide WAN optimization for traffic passing between networks.

A diagram of the Blue Coat ProxySG architecture is as follows;



3 Security Policy

Blue Coat ProxySG implements a role-based access control policy to control administrative access to the system. In addition, Blue Coat ProxySG implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access
- Trusted Path/Channels

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

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS 197	105, 1265, 2925
Rivest Shamir Adleman (RSA)	FIPS 186-2	1534
Secure Hash Algorithm (SHA-1)	FIPS 180-2	2461
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	1852
Deterministic Random Bit Generator (DRBG)	ANSI x9.31 FIPS 186-2	539

4 Security Target

The ST associated with this Certification Report is identified below:

Blue Coat ProxySG SG600, SG900, SG9000 running SGOS v6.5 Security Target, v1.3, 18 September 2014

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

Blue Coat ProxySG is:

a. Conformant to the Protection Profile for Network Devices, v1.1, June 8, 2012,
b. *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:*

- FAU_STG_EXT.1 – External audit trail storage
- FCS_CKM_EXT.4 – Cryptographic key zeroization
- FCS_RBG_EXT.1 – Cryptographic operation: random bit generation
- FCS_HTTPS_EXT.1 – Explicit HTTPS
- FCS_TLS_EXT.1 – Explicit TLS
- FCS_SSH_EXT.l – Explicit SSH
- FIA_PMG_EXT.1 – Password management
- FIA_UIA_EXT.1 – User identification and authentication
- FIA_UAU_EXT.2 – Password-based authentication mechanism
- FPT_SKP_EXT.1 – Protection of TSF data
- FPT_APW_EXT.1 – Protection of administrator passwords
- FPT_TUD_EXT.1 – Trusted update
- FPT_TST_EXT.1 – TSF testing
- FTA_SSL_EXT.1 – TSF-initiated session locking

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of Blue Coat 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 the TOE.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE; and
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.

6.3 Clarification of Scope

Blue Coat ProxySG incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

7 Evaluated Configuration

The evaluated configuration for Blue Coat ProxySG comprises:

The software SGOS v6.5.1.5 build 143753 installed on on one of the following hardware appliances:

- ProxySG SG600-10, SG600-20, SG600-35 with a Cavium CN501 Hardware Accelerator Card (HAC);
- ProxySG SG900-10, SG900-20, 900-30, SG900-45, SG900-55 with a Cavium CN1610 HAC; and
- ProxySG SG9000-20, SG9000-30, SG9000-40 with a Cavium CN1620 PCI-e18 HAC.

The publications entitled :

- Blue Coat Systems, Inc. Blue Coat ProxySG SG600, SG900, and SG9000 running SGOS v6.5 Guidance Supplement v1.0;
- Blue Coat Systems SGOS Administration Guide, Version SGOS 6.5.x, 231-03113, SGOS 6.5.x, 06/2014;
- Blue Coat Systems ProxySG Appliance Command Line Interface Reference, version SGOS 6.5.x, 231-03035, SGOS 6.5.x, 04/2014;
- Blue Coat Systems Common Access Card (CAC) Solutions Guide, SGOS 6.1.2 and later, 231-03155, SGOS 6.5.x, 06/2014;
- Blue Coat Systems ProxySG Appliance Visual Policy Manager Reference and Advanced Policy Tasks, SGOS Version 6.5.x, 231-03015, SGOS 6.5.x, 01/2014;
- Blue Coat Systems ProxySG Appliance Content Policy Language Reference, version SGOS 6.5.x, 231-03019, SGOS 6.5.3, 07/2014;
- Blue Coat SGOS Upgrade/Downgrade Guide, 04/2014;
- Blue Coat Notice and Consent Banner Configuration Webguide, SGOS 6.5.x, Webguide version 01-2014.03.14 (https://bto.bluecoat.com/sgos/NCB/Notice_Consent_Banner.htm);
- ProxySG Quick Start Guide SG600 Series, 231-03048, Rev A.0;
- ProxySG Quick Start Guide: SG900 Series, 231-03109, Rev C.0; and
- ProxySG Quick Start Guide: SG9000 Series, 231-03159, Rev A.2.

describe the procedures necessary to install and operate Blue Coat ProxySG in its evaluated configuration.

8 Documentation

In addition to the documents identified in section 7, the following Blue Coat Systems, Inc. documents are provided to the consumer:

- Blue Coat Systems SGOS Administration Guide, Version SGOS 6.5.x, 231-03113, SGOS 6.5.x, 06/2014;
- Blue Coat Systems SCPS19 Deployment Guide SGOS Version 6.3.x and later, 231-03156, SGOS 6.3, 08/2013;
- Blue Coat ProxySG 600 Series FIPS20 Compliance Guide: Tamper Evident Panel and Label Installation, 231-03160, C.0;
- Blue Coat ProxySG 900 Series FIPS Compliance Guide: Tamper Evident Panel and Label Installation, 231-03161, B.0;
- Blue Coat ProxySG 9000 Series FIPS Compliant Tamper Evident Faceplate and Label Installation Guide, 231-03063, B.0;
- Blue Coat ProxySG Maintenance and Upgrade Guide, ProxySG 600 Series, 231-03051, A.2;
- Blue Coat ProxySG Maintenance and Upgrade Guide, ProxySG 900 Series, 231-03166, B.1;
- Blue Coat 9000 Series Maintenance & Upgrade Guide, 231-03038, E.4; and
- Blue Coat Systems, Inc. Blue Coat ProxySG SG600, SG900, and SG9000 running SGOS v6.5 Guidance Supplement v1.0.

9 Evaluation Analysis Activities

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

Development: The evaluators analyzed the Blue Coat ProxySG functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the Blue Coat ProxySG functional specification is an accurate and complete instantiation of the SFRs.

Guidance Documents: The evaluators examined the Blue Coat ProxySG 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 Blue Coat ProxySG configuration management system and associated documentation was performed. The evaluators found that the Blue Coat ProxySG configuration items were clearly marked.

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

10 ITS Product Testing

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

10.1 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

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 test goals:

a. NDPP required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the NDPP to which the TOE is claiming conformance.

10.2 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:

a. NDPP required assurance activities. The evaluator performed the assurance activities mandated by the protection profile to which the TOE is claiming conformance; and
b. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities.

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

10.3 Conduct of Testing

Blue Coat 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 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.

10.4 Testing Results

The independent tests yielded the expected results, providing assurance that Blue Coat ProxySG behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a NDPP conformance claim as claimed in Section 5. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

During the course of the evaluation, the evaluator determined some security functions of the TOE are enforced by the installed policy which are written in CPL (Content Policy Language). Each web request is also evaluated and actioned based on the installed policy. Since misconfiguration of the policy may have detrimental effect; the evaluator recommends an administrator who is competent with Visual Policy Manager (VPM) or the CPL syntax in order to define or compose the security policy. Such knowledge is also critical for troubleshooting and to maintain normal operation of the TOE.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CMVP	Cryptographic Module Validation Program
CPL	Certified Products list
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMAC	Keyed – Hash Message Authentication Code
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NDPP	Netwok Device Protection Profile
PALCAN	Program for the Accreditation of Laboratories - Canada
RSA	Rivest Shamir Adleman
SFR	Security Functional Requirement
SHA	Secure hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VPM	Visual Policy Manager
WAN	Wide Area Network

14 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 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. Protection Profile for Network Devices, v1.1, June 8, 2012.

e. Blue Coat ProxySG SG600, SG900, SG9000 running SGOS v6.5 Security Target, v1.3, 18 September 2014

f. Evaluation Technical Report for Blue Coat ProxySG SG600, SG900, SG9000 running SGOS v6.5, v 1.2, 30 July 2014.