Swedish Certification Body for IT Security

Certification Report - Blue Coat ProxySG S400 and S500 running SGOS v6.5

Issue: 1.0, 2015-mar-05

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Executive Summary

The Blue Coat ProxySG S400 and S500 running SGOS v6.5 appliances (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.

The TOE claims exact Conformance to Security Requirements for Network Devices v1.1: [NDPP] as well as the Security Requirements for Network Devices Errata #2: [NDPP-ERRATA].

The evaluation has been performed by atsec information security AB and was completed on the 22nd of january 2015.

The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1, release 4, and the Common Methodology for IT Security Evaluation, version 3.1, release 4. The evaluation was also performed to meet the Security Requirements for Network Devices v1.1: [NDPP] as well as the Security Requirements for Network Devices Errata #2: [NDPP-ERRATA].

atsec information security AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. atsec information security AB is is also accredited by the Swedish accreditation body SWEDAC according to ISO/IEC 17025 for Common Criteria evaluation.

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports. The certifier determined that the evaluation results confirm the security claims in the Security Target [ST], and have been reached in agreement with the requirements of the Common Criteria and the Common Methodology and exact Conformance to Security Requirements for Network Devices v1.1 (NDPP) plus the Security Requirements for Network Devices Errata #2.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met.

This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2014004
Name and version of the certified IT product	Blue Coat ProxySG S400 and S500 running SGOS v6.5
Security Target Identification	Blue Coat ProxySG S400 and S500 running SGOS v6.5 Security Target, Version 1.4, Date 2015-02-06
EAL	PP compliant
Sponsor	Blue Coat Systems, Inc.
Developer	Blue Coat Systems, Inc.
ITSEF	atsec information security AB
Common Criteria version	3.1 release 4
CEM version	3.1 release 4
Certification date	2015-03-06

3 Security Policy

3.1 Security Audit

The Security Audit function provides the TOE with the functionality of generating audit records. As administrators manage and configure the TOE, their activities are tracked and recorded as audit records and are stored in the TOE's file system. The resulting audit records can be examined to determine which security relevant activities took place and who (i.e., which user) is responsible for those activities.

The Audit Log entries contain at a minimum the following fields:

- Date and time of the event
- Type of event
- Identity of the subject
- Outcome of the event

Additional fields will be found in addition to these fields for those events that explicitly require additional information as defined in the "Additional Audit Record Contents" column of Table 12 in [ST].

The TOE supports the SSH, TLS, and HTTPS protocols and will record administrator session establishment failures, successful session establishment, and session termination events to the audit log. Session establishment failure can occur if invalid or incorrect authentication credentials are submitted.

3.2 Cryptographic Support

Cryptographic operations necessary to support SSH, TLS, HTTPS, encryption, decryption, and key generation are provided by the TOE's Blue Coat proprietary cryptographic module (Blue Coat SGOS Crypto Library version 3.1.5). The TOE uses SSH, TLS, and HTTPS (via TLS) to protect communications.

SSH provides a trusted path for remote administrators accessing the TOE's CLI. TLS is used to provide a trusted channel for ProxySG requests to a Lightweight Directory Access Protocol (LDAP) server and to BCAAA. TLS is also used to provide a trusted channel during audit log transmissions from the TOE. HTTPS (via TLS) is used to provide a trusted path for administrator management connections to the TOE's Management Console.

3.3 User Data Protection

The TOE enforces the User Data Protection TSF on user data by ensuring that the buffer area used by previous network packets is made unavailable during allocation of the buffer.

3.4 Identification and Authentication

The TOE provides mechanisms for authenticating administrators connecting to the TOE through the CLI and Management Console.

A login is considered successful if the credentials submitted by the administrator can be validated by the TOE. If authentication using username and password credentials is used, and the credentials match a locally stored username and password or the IWA realm, login is considered successful. If the RSA public key authentication is in use, the TOE must first verify the submitted RSA public key matches an RSA public key present on the TOE and then makes further verifications. For certificate authentication, if the TOE verifies that the certificate was signed by a Certificate Authority (including certificates extracted from CACs) that the TOE trusts, login is considered successful. Administrators are notified by the CLI and Management Console when there is a failure in authentication and they will be prompted to try again.

Unauthenticated users only have access to read the displayed warning banner before authenticating successfully with the TOE and establish a secure SSH or TLS session with the TOE.

3.5 Security Management

The TOE provides authorized administrators with the Management Console to easily manage the security functions and TSF data of the TOE. The Management Console can be used to configure the cryptographic functionality available on the TOE, update the TOE, and verify the updates via digital signatures. The same functionality is available to administrators over the CLI as well.

The TOE defines two Authorized Administrator roles:

- Standard or Unprivileged mode Administrator – has not been granted access to the "enabled" mode in the CLI and has been given "read-only" privileges when using the Management Console.
- Enabled, or Privileged mode Administrator – has been granted "enabled" mode access while using the CLI and "read/write" access while using the Management Console.

3.6 Protection of the TSF

The TOE provides SSH, TLS, and HTTPS/TLS to protect TSF data from disclosure and to detect modification of TSF data while in transit between different parts of the TOE.

The TOE does not allow any Administrator to read plaintext passwords stored on the TOE, since all passwords are stored in encrypted form using an AES-256-bit key. The TOE also prevents symmetric and private keys from being read by storing keys in encrypted form using an AES-256-bit key. The encrypting AES-256-bit key is stored in internally-allocated data structure. The TOE's SGOS safeguards memory and process space from unauthorized access.

The TOE generates its own time stamps that originate from a system hardware clock. The timestamp is used by the audit logs to record an accurate time for each auditable event and must be set to the current Coordinated Universal Time (UTC). The clock can be changed through the CLI and Management Console.

Administrators can find the current version of TOE software by going to the home page of the Management Console or using the show version command through the CLI.

At power up, the TOE runs a suite of self-tests that check for the correct operation of the cryptographic functionality provided by the TOE. All TOE appliances run these tests on startup.

3.7 TOE Access

The TOE terminates local and remote management sessions after an Administrator configurable time period of inactivity has elapsed. Local sessions must be initiated by accessing the CLI via the serial port. Remote sessions may be initiated by accessing the CLI using SSH or accessing the Management Console using HTTPS via TLS. Administrators may also terminate their sessions voluntarily. Users must log in again to regain access to TOE management capabilities. At the login screen Administrators are shown an advisory notice and consent warning message regarding unauthorized use of the TOE. The message is shown to users of both the Management Console and the CLI.

3.8 Trusted path/channels

The TOE provides a trusted path between the TOE management interfaces and remote TOE administrators. These interfaces are the CLI over SSH and the Management Console over HTTPS. The protocols and the cryptography implemented by the TOE provide adequate defense against unauthorized disclosure and provide for the detection of modification of TSF data while it is being communicated.

Additionally, the TOE provides a trusted channel between the TOE and the trusted IT entities used for the audit and authentication servers. The TOE protects audit log traffic by encrypting it with a secure TLS/HTTPS tunnel. For authentication mechanisms that require the use of LDAP or the BCAAA, the communication between the TOE and the authentication server is also protected with TLS.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes one assumptions on the usage of the TOE.

A.TRUSTED_ADMIN TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.2 Environmental Assumptions

Two assumption on the environment is made in the Security Target [ST]:

A.NO_GENERAL_PURPOSE It is assumed that 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.

A.PHYSICAL Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.

4.3 Organisational Security Policies

One Organisational Security Policies has been defined:

P.ACCESS_BANNER The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4.4 Clarification of Scope

The following threats are identified:

T.ADMIN_ERROR An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.

T.TSF_FAILURE Security mechanisms of the TOE may fail, leading to a compromise of the TSF.

T.UNDETECTED_ACTIONS Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

T.UNAUTHORIZED_ACCESS A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.

T.UNAUTHORIZED_UPDATE A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.

T.USER_DATA_REUSE User data may be inadvertently sent to a destination not intended by the original sender.

5 Architectural Information

5.1 Architectural Overview

The Blue Coat ProxySG S400 and S500 running SGOS v6.5 appliances (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.

5.2 Cryptographic Functions

Cryptographic operations necessary to support SSH, TLS, HTTPS, encryption, decryption, and key generation are provided by the TOE's Blue Coat proprietary cryptographic module (Blue Coat SGOS Crypto Library version 3.1.5). The TOE uses SSH, TLS, and HTTPS (via TLS) to protect communications. SSH provides a trusted path for remote administrators accessing the TOE's CLI. TLS is used to provide a trusted channel for ProxySG requests to a Lightweight Directory Access Protocol (LDAP) server and to BCAAA. TLS is also used to provide a trusted channel during audit log transmissions from the TOE. HTTPS (via TLS) is used to provide a trusted path for administrator management connections to the TOE's Management Console. The TOE uses symmetric AES keys to encrypt and decrypt data. The TOE also provides HMAC-SHA and SHS to support TOE cryptographic functionality.

The TOE supports the following mandatory TLS ciphersuite:

- TLS_RSA_WITH_AES_128_CBC_SHA

The TOE also supports the following optional TLS ciphersuites:

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

The TOE's cryptographic module supports the following algorithms:

- AES key sizes of 128 bits and 256 bits
- AES modes of CBC, ECB, OFB, and CFB-128
- rDSA with key sizes of 2048 and greater
- SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512
- HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512

The TOE uses the open source OpenSSH implementation of the SSHv2 protocol which conforms to RFCs 4251, 4252, 4253, and 4254 as shown here: http://www.openssh.org/specs.html. The TOE supports the use of the RSA public key algorithm (SSH_RSA) and password-based mechanisms for authentication over SSH. The TOE detects large SSH packets by examining the header information for incoming packets. If the packet is an SSH packet, and the packet size is greater than 256 kilobytes, then the packet is dropped. SSH traffic can be encrypted with AES-CBC-128 and AES-CBC-256. For data integrity during SSH sessions, HMAC-SHA1 and HMAC-SHA1-96 are available. Diffie-Hellman-group14-SHA1 is the only allowed key exchange method used for the SSH protocol.

6 Documentation

The following guides are part of the TOE:

- Blue Coat Systems SGOS Administration Guide, Version SGOS 6.5.2.10, 231-03113, SGOS 6.5.2.10, 11/2014
- Blue Coat Systems Common Access Card Solutions Guide, For SGOS 6.1.2 and later, 231-03155, SGOS 6.5.x, 11/2014
- Blue Coat Systems ProxySG Appliance Command Line Interface Reference, Version SGOS 6.5.2.10, 231-03035, SGOS 6.5.2.10, 09/2014
- Blue Coat Systems ProxySG Appliance Content Policy Language Reference, SGOS 6.5.2.10, 231- 03019, SGOS 6.5.2.10, 10/2014
- Blue Coat SGOS Upgrade/Downgrade Guide, 04/2014
- Blue Coat Systems, Inc. Blue Coat ProxySG S400 and S500 running SGOS v6.5.2.10
- Guidance Documentation Supplement v1.0

The TOE claims exact Conformance to Security Requirements for Network Devices v1.1: [NDPP] as well as the Security Requirements for Network Devices Errata #2: [NDPP-ERRATA].

7 IT Product Testing

The evaluator used the guidance documentation listed in [ST] for the installation, configuration and management of the TOE.

7.1 Developer Tests

Not applicable.

7.2 Independent Evaluator Tests

7.2.1 Testing approach

The TOE was set up at the atsec office in Austin, Texas, USA and the initial testing was performed onsite by Rasma Araby and King Ables in September, 2014. Due to issues found during the testing, the TOE software had to be updated. The evaluators then repeated their testing in November and December, 2014 on a updated version of the TOE. Michael Almér and Rasma Araby then performed most of the tests using remote access tools from the critical location in Danderyd, Stockholm, Sweden. Some of the test were performed by King Ables who was in the Austin office to physically access the TOE.

The evaluator notes that the [ST] lists two different TOE appliances. However, the evaluators chose to only test Blue Coat ProxySG S400-20 running SGOS v6.5.2.10 and the evaluators have provided the following testing rationale:

All platforms of the TOE runs the same version of firmware code (SGOS v6.5.2.10) and use the same family of processor (Intel Sandy Bridge-E). The only substantive difference between the two architectures is the model of Sandy Bridge-E processor and the hard disk devices and network interfaces and corresponding device drivers. There is no unique code path in the TOE that is specific to a particular architecture other than at the device driver level. The evaluator came to conclusion that it is sufficient to only use one model for the independent testing. The TOE model used during the independent testing is Blue Coat ProxySG S400-20 running SGOS v6.5.2.10.

The algorithm testing has been performed on cryptographic module version 3.1.5 included in SGOS v.6.5.2.10 on the following version of the TOE:

- E5-2430 – the processor and motherboard for the S400-30 and S400-40 are the same. Only S400-30 was tested.
- E5-2658 – the processor and motherboard for the S500-10 and S500-20 are the same. Only S500-20 was tested
- E5-2418L – corresponds to the processor and motherboard for the S400-20. S400-20 was tested

The evaluator configured the TOE and set up the test environment. The evaluator verified that the configured TOE and environment is consistent with the requirements of the [ST]. The evaluator used the following documentation during the installation and configuration of the TOE:

- SGOS Administration Guide: [ADMGD]
- ProxySG Appliance Command Line Interface Reference: [CMD]
- Guidance Documentation Supplement: [ECG]
- Blue Coat Systems Common Access Card Solutions Guide: [CACS]

7.2.2 Depth

The evaluator has devised a test subset to ensure that the TOE behaves as specified in the ST and the guidance documentation as well as to perform tests described in [NDPP] and [NDPP-ERRATA].

7.2.3 Results

All evaluator test cases were completed successfully.

7.3 Penetration Tests

7.3.1 Testing effort

Vulnerability testing was performed against the TOE interfaces that are accessible to a potential attacker. I.e., the IPv4 TCP and UDP ports of the TOE.

7.3.2 Testing approach

Since an attack requires an attack surface, the evaluator decided to start by examining if the TOE exposes such interfaces, i.e., open ports.

7.3.3 Testing configuration

The TOE and environment was configured according to [ST].

7.3.4 Testing depth

The evaluator examined all potential interfaces, i.e., all IPv4 UDP and TCP ports.

7.3.5 Testing results

The evaluator determined that only the following ports are available:

- Port 22 - used for SSH
- Port 444 - used for HTTPS connection to access the “Notice and Consent – Management Console” banner. Please see [ECG] section 3.1.1 for more information (during installation the evaluator configured the TOE to use port 444 for showing the banner to the user accessing the TOE)
- Port 8082 - used for HTTPS connection to the administrative interface

This is the expected result.

The evaluator also determined that the TOE use OpenSSH version 6.3 as SSH application. With this knowledge, the evaluator include it in the public vulnerability search and found no applicable vulnerabilities to OpenSSH version 6.3.

8 Evaluated Configuration

The TOE environment must include the following components as stated in [ST]:

- cables, connectors, and switching and routing devices that allow all of the TOE and environmental components to communicate with each other
- an audit server that will contain a script to continuously pull audit logs off the TOE
- a management workstation with a standards-compliant client program to access the Management Console over HTTPS and the CLI using SSH
- a server installed with the BCAAA or an LDAP server for remote authentication.
- a firewall between the TOE and the External Network

9 Results of the Evaluation

The TOE

1. is conformant to the following PPs:
   a) Protection Profile for Network Devices. Version 1.1 as of 2012-07-08; strict conformance;
   b) Network Devices Errata #2.
2. is CC part 2 extended;
3. is CC part 3 conformant.
4. meets all security objectives for the TOE stated in the Security Target;
5. meets all security functional requirements for the TOE stated in the Security Target;
6. resists an attack potential of Basic.

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Security Target Evaluation	ASE	Pass
ST Introduction	ASE_INT.1	Pass
Conformance claims	ASE_CCL.1	Pass
Security objectives for the operational environment	ASE_OBJ.1	Pass
Extended components definition	ASE_ECD.1	Pass
Stated security requirements	ASE_REQ.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Assurance activities for NDPP	ASE_NDPP.1	Pass
Life-cycle support	ALC	Pass
Labelling of the TOE	ALC_CMC.1	Pass
TOE CM coverage	ALC_CMS.1	Pass
Assurance activities for NDPP	ALC_NDPP.1	Pass
Development	ADV	Pass
Basic functional specification	ADV_FSP.1	Pass
Guidance documents	AGD	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Assurance activities for NDPP	AGD_NDPP.1	Pass
Tests	ATE	Pass
Independent testing - Conformance	ATE_IND.1	Pass
Assurance activities for NDPP	ATE_NDPP.1	Pass
Vulnerability assessment	AVA	Pass
Vulnerability survey	AVA_VAN.1	Pass
Assurance activities for NDPP	AVA_NDPP.1	Pass

10 Evaluator Comments and Recommendations

The evaluators have no remaining comments, observations, or recommendations.

11 Glossary

Augmentation	The addition of one or more requirement(s) to a package.
Authentication data	Information used to verify the claimed identity of a user.
Authorised user	A user who may, in accordance with the SFRs, perform an operation.
Class	A grouping of CC families that share a common focus.
Component	The smallest selectable set of elements on which requirements may be based.
Connectivity	The property of the TOE which allows interaction with IT entities external to the TOE. This includes exchange of data by wire or by wireless means, over any distance in any environment or configuration.
Dependency	A relationship between components such that if a requirement based on the depending component is included in a PP, ST or package, a requirement based on the component that is depended upon must normally also be included in the PP, ST or package.
Deterministic RNG (DRNG)	An RNG that produces random numbers by applying a deterministic algorithm to a randomly selected seed and, possibly, on additional external inputs.
Element	An indivisible statement of security need.
Entropy	The entropy of a random variable X is a mathematical measure of the amount of information gained by an observation of X.
Evaluation	Assessment of a PP, an ST or a TOE, against defined criteria.
Evaluation Assurance Level (EAL)	An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale.
Evaluation authority	A body that implements the CC for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
Evaluation scheme	The administrative and regulatory framework under which the CC is applied by an evaluation authority within a specific community.
Extension	The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in Part 3 of the CC.
External entity	Any entity (human or IT) outside the TOE that interacts (or may interact) with the TOE.
Family	A grouping of components that share a similar goal but may differ in emphasis or rigour.
Formal	Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.
Guidance doc-	Documentation that describes the delivery, preparation, operation,

umentation	management and/or use of the TOE.
Identity	A representation (e.g. a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.
Informal	Expressed in natural language.
Object	A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.
Operation (on a component of the CC)	Modifying or repeating that component. Allowed operations on components are assignment, iteration, refinement and selection.
Operation (on an object)	A specific type of action performed by a subject on an object.
Operational environment	The environment in which the TOE is operated.
Organisational Security Policy (OSP)	A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment.
Package	A named set of either functional or assurance requirements (e.g. EAL 3).
PP evaluation	Assessment of a PP against defined criteria.
Protection Profile (PP)	An implementation-independent statement of security needs for a TOE type.
Random number generator (RNG)	A group of components or an algorithm that outputs sequences of discrete values (usually represented as bit strings).
Refinement	The addition of details to a component.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
Secret	Information that must be known only to authorised users and/or the TSF in order to enforce a specific SFP.
Secure state	A state in which the TSF data are consistent and the TSF continues correct enforcement of the SFRs.
Security attribute	A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs.
Security Function Policy (SFP)	A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs.
Security objective	A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions.
Security Target (ST)	An implementation-dependent statement of security needs for a specific identified TOE.
Seed	Value used to initialize the internal state of an RNG.

Selection	The specification of one or more items from a list in a component.
Semiformal	Expressed in a restricted syntax language with defined semantics.
ST evaluation	Assessment of an ST against defined criteria.
Subject	An active entity in the TOE that performs operations on objects.
Target of Evaluation (TOE)	A set of software, firmware and/or hardware possibly accompanied by guidance.
TOE evaluation	Assessment of a TOE against defined criteria.
TOE resource	Anything useable or consumable in the TOE.
TOE Security Functionality (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs.
Transfers outside of the TOE	TSF mediated communication of data to entities not under control of the TSF.
True RNG (TRNG)	A device or mechanism for which the output values depend on some unpredictable source (noise source, entropy source) that produces entropy.
Trusted channel	A means by which a TSF and a remote trusted IT product can communicate with necessary confidence.
Trusted path	A means by which a user and a TSF can communicate with necessary confidence.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE.
TSF Interface (TSFI)	A means by which external entities (or subjects in the TOE but outside of the TSF) supply data to the TSF, receive data from the TSF and invoke services from the TSF.
User	See external entity
User data	Data created by and for the user, that does not affect the operation of the TSF.

12 Bibliography

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 4, September 2012, CCMB-2012-09-001

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 4, September 2012, CCMB-2012-09-002

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 4, September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, revision 4, September 2012, CCMB-2012-09-004

[SP-002] Evaluation and Certification, SP-002, Issue: 22.0, 2014-12-12, 14FMV9859-38:1, FMV/CSEC

[ADMGD] SGOS Administration Guide, Version SGOS 6.5.2.10-11/2014, Date 11/2014

[CACS] Blue Coat Systems Common Access Card Solutions Guide, Author(s) Blue Coat Systems, Inc. Version SGOS 6.5.x-11/2014, Date 2014-11

[CMD] Blue Coat Systems ProxySG Appliance Command Line Interface, Reference, Version SGOS 6.5.2.10-09/2014, Date 06/2014

[ECG] Guidance Documentation Supplement, Author(s) atsec information security, Version 1.0, Date 2014-12-08

[NDPP] Protection Profile for Network Devices, Version 1.1, Date 2012-06-08

[NDPP-ERRATA] Security Requirements for Network Devices, Errata #2, Date 2013-01-13

[ST] Blue Coat ProxySG S400 and S500 running SGOS v6.5 Security Target, Author(s) atsec information security, Version 1.3, Date 2014-12-08

Appendix A - QMS Consistency

During the certification project, the following versions of the quality management system (QMS) have been applicable since the certification application was received 20134-04-30:

QMS 1.16.1 valid from 2014-03-27

QMS 1.16.2 valid from 2014-07-07

QMS 1.17 valid from 2014-11-20

QMS 1.17.1 valid from 2014-12-02

QMS 1.17.2 valid from 2015-01-13

QMS 1.17.3 valid from 2015-01-29

In order to ensure consistency in the outcome of the certification, the certifier has examined the changes introduced in each update of the quality management system.

The changes between consecutive versions are outlined in “Ändringslista QMS 1.17.3”.

The certifier concluded that, from QMS 1.16.1 to the current QMS 1.17.3, there are no changes with impact on the result of the certification.