Certification Report

Blue Coat Systems, Inc. SSL Visibility Appliance, 3.8.4FC

Sponsor and developer: ***Blue Coat Systems, Inc***
384 Santa Trinita Ave
Sunnyvale, CA 94085
USA

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Reportnumber: **NSCIB-CC-15-66461-CR**

Report version: **1**

Projectnumber: **NSCIB-CC-15-66461**

Authors(s): **Denise Cater**

Date: **04 August 2016**

Number of pages: **14**

Number of appendices: **0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 AV Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard	Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)
Certificate number	**CC-16-66461**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Blue Coat Systems, Inc** **384 Santa Trinita Avenue, 94085 Sunnyvale CA, USA**
Product and assurance level	**Blue Coat Systems, Inc. SSL Visibility Appliance, 3.8.4FC,** Assurance Package: ▪ EAL3 augmented with ALC_FLR.3
Project number	**NSCIB-CC-15-66461**
Evaluation facility	**Brightsight BV located in Delft, the Netherlands** Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (ISO/IEC 18045)

Common Criteria Recognition Arrangement for components up to EAL2

SOGIS IT SECURITY CERTIFIED

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 3.1 Revision 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report. The evaluation has been conducted in accordance with the provisions of the Netherlands scheme for certification in the area of IT security [NSCIB] and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity	Date of issue : **22-08-2016** Certificate expiry : **22-08-2021**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 2200
6802 CE Arnhem
The Netherlands

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

CONTENTS:

Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products, as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025 “General requirements for the accreditation of calibration and testing laboratories”.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, 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 stated in the security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate would indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nation

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 8 September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

European recognition

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products related to specific technical domains. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations, approved certification schemes and the list of technical domains for which the higher recognition applies can be found on: http://www.sogisportal.eu.

1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Blue Coat Systems, Inc. SSL Visibility Appliance, 3.8.4FC. The developer of the Blue Coat Systems, Inc. SSL Visibility Appliance is Blue Coat Systems, Inc located in Sunnyvale, USA and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The TOE is the Blue Coat SSL Visibility Appliance, consisting of hardware appliances and software. The Blue Coat SSL Visibility Appliance is an integral component to any encrypted management strategy, and offers visibility into encrypted traffic without requiring the re-architecting of the network infrastructure.

The SSL Visibility Appliance provides a complete solution to the problem of dealing with threats contained within encrypted SSL traffic. A single SSL Visibility Appliance can be deployed to detect and inspect all SSL traffic that may pose a threat, and can pass the decrypted content to one or more network security appliances which can record or block any threats. The SSL Visibility Appliance is designed to work alongside existing security devices such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Data Loss Prevention (DLP) systems, Network Forensic appliances. It provides a non-encrypted version of SSL traffic to the associated appliance while maintaining an end to end SSL connection between the client and server involved in the session.

The SSL Visibility Appliance does not rely on the TCP destination port number being used by a session to determine if it is using SSL or not. The SSL Visibility Appliance uses deep packet inspection (DPI) to identify SSL flows. This ensures that it can find and inspect SSL traffic in the network, even if the traffic is using non-standard port numbers. The SSL Visibility Appliance incorporates flow processing hardware and cryptographic acceleration hardware, enabling it to forward non SSL traffic at multi-Gigabit/s rates, while offering transparent proxy performance (that is, decrypting and re-encrypting) for SSL traffic.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. Brightsight performed this evaluation in conjunction with a NIAP accredited CC lab (Acumen, located in Montgomery Village, MD, USA). Brightsight was the main point of contact and retained full responsibility for the end result. The evaluation was completed on 12 July 2016 with the approval of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Blue Coat Systems, Inc. SSL Visibility Appliance, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Blue Coat Systems, Inc. SSL Visibility Appliance are advised to verify that their own environment is consistent with 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 EAL3 augmented (EAL3(+)) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_FLR.3 (Systematic flaw remediation).

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

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Blue Coat Systems, Inc. SSL Visibility Appliance, 3.8.4FC evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Blue Coat Systems, Inc. SSL Visibility Appliance, 3.8.4FC from Blue Coat Systems, Inc located in Sunnyvale, USA.

The TOE is comprised of the following main components:

Delivery item type	Identifier	Version
Hardware	SV1800-C appliance	090-03061
	SV1800-F appliance	090-03062
	SV2800 appliance	090-03063
	SV3800 appliance	090-03064
Software	SSL Visibility Appliance and Software	3.8.4FC

To ensure secure usage a set of guidance documents is provided together with the Blue Coat Systems, Inc. SSL Visibility Appliance. Details can be found in section 2.5 of this report.

2.2 Security Policy

The TOE is a transparent network proxy appliance providing SSL inspection capabilities. The TOE can be deployed to detect and inspect all SSL traffic, and can pass the decrypted content to one or more network security appliances (e.g. IDS, IPS, DLP, Network Forensic). The TOE can be deployed in one of three network connectivity modes:

- Active-Inline
- Passive-Inline
- Passive-Tap

The modes of deployment are further explained in section 1.4.1 of the *[ST]*.

The TOE offers the following security features:

- Security Audit – Generates audit records for security relevant actions of the administrator.
- Cryptographic Support – Provides cryptographic functions to WebUI and CLD sessions between an administrator's management workstation and the TOE (TLS and SSH).
- User Data Protection – Decrypt and mediate SSL/TLS traffic into and out of a network. Clears of memory buffers mapped to network packet data upon deallocation.
- Identification and Authentication – Requires administrative users to be authenticated prior to allowing access to any TOE administrative functionality.
- Security Management – Provides a WebUI and CLD for administrators to manage the security functions, configuration, and other features of the TOE.
- Protection of the TSF – Invokes a set of self tests each time the TOE is powered on to ensure that the TSF operates correctly.
- TOE Access – Terminates local and remote management sessions after an administrator-configurable time period of inactivity.
- Trusted Path/Channels – Uses Cryptographic Support functionality to create trusted paths and trusted channels between the TOE and a remote server, between administrators and the CLD via SSH, and between administrators and the WebUI via TLS/HTTPS.

2.3 Assumptions and Clarification of Scope

2.3.1 Assumptions

Detailed information on the assumption and threats can be found in the *[ST]* sections 3.3 and 3.1 respectively. Detailed information on the security objectives that must be fulfilled by the TOE environment can be found in section 4.2 of the *[ST]*.

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
- Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- The IT environment provides trusted NTP server (providing reliable time stamps), Management Workstations, and Syslog servers. These servers shall reside in a separated management network.
- The IT environment provides a non-TOE Security Appliance. Decrypted SSL/TLS traffic is passed from the TOE to the Security Appliance for inspection. The Security Appliance will provide the TOE with network traffic inspection allow/disallow decisions for TOE enforcement when the TOE is configured in active inline mode.
- A physically secure environment is provided for all equipment directly connecting to the TOE, including, serial port/cable/keyboard/monitor, associated cabling/equipment, and the security appliance.

2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

2.4 Architectural Information

This chapter provides a high-level description of the IT product and its major components based on the evaluation evidence described in the Common Criteria assurance family entitled “TOE design (ADV_TDS)”. The intent of this chapter is to characterise the degree of architectural separation of the major components.

The TOE security Functionality is implemented in a combination of hardware and software. These are depicted in the figure below:

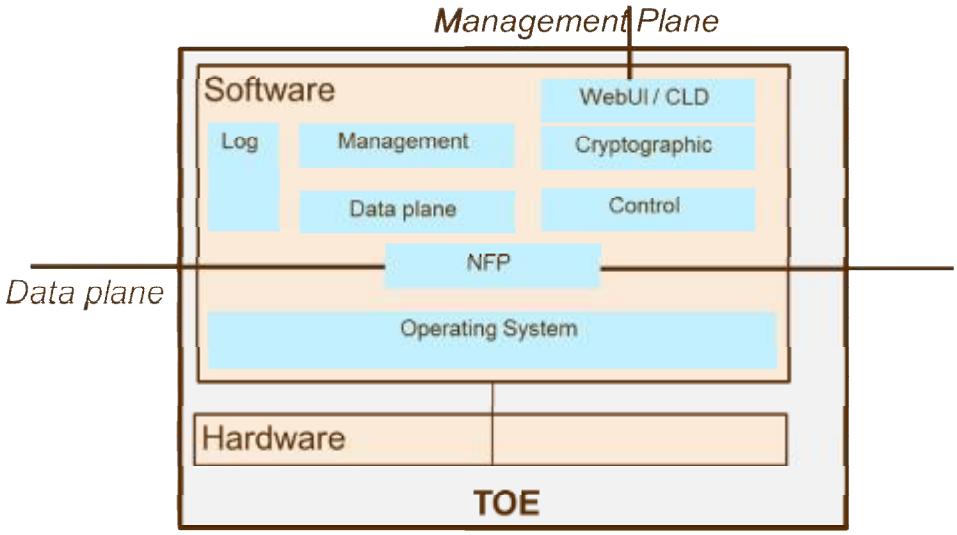

Figure 1 TOE Architecture

The major flow of a data packets is consulted by the SSLV policy to decide whether to intercept and decrypt the session. Then the actions of the policy are applied.

The hardware makes up the TOE including all of the external interfaces including TSFIs and cryptographic functionality. All communication into and out of the TOE is via physical network functionality. The software includes:

- Management: Enforces initial appliance configuration during the bootstrap phase. Manages the appliance's Policy and PKI store and authenticates administrative users. Stores the user authentication data as part of its user store and stores keys as part of its secure store.
- Dataplane: Initializes the NFP, configures it based on the SSLV policy, and communicates with the NFP subsystem to send and receive packets on SSL sessions. Examines SSL sessions that pass through the TOE. Consults the SSLV policy to determine whether to intercept them.
- Control: Configures and monitors the platform's Dataplane network interfaces. Allows administrators to manage platform configuration, install software updates/export diagnostics information. Manages the internal timestamp and logging capabilities.
- Logging: Parses the SSLV appliance system log files and presents the log messages to users.
- Cryptographic: Executes cryptographic algorithms, including secure storage. Uses the NFP for acceleration. Performs cryptographic self-tests.
- NFP: Logical interface to the HW functionality for the Dataplane and Cryptographic components.
- WebUI / Command Line Diagnostic: Interface for the administrator. Establishes TLS connections with management clients. Provides a limited set of approved cipher suites. The CLD functionality is a subset of the WebUI.
- Operating System Subsystem: A Linux based Operating System providing general OS functions.

2.5 Documentation

The following documentation is provided with the product by the developer to the customer:

Identifier	Version
Blue Coat Systems SSL Visibility Appliance Guidance Document, 3.8.4FC	1.0

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer's testing activities documentation and verified that the developer has met their testing responsibilities.

2.6.1 Testing approach and depth

The developer has 36 separate tests organized by SFR. Each test case focuses on the functionality provided by the SFR and may test multiple TSFI and subsystems. All SFR are covered and all hardware platforms are covered.

The evaluator repeated 14 of 36 developer tests. In this sample every TSFI is exercised, every subsystem is exercised and each SFR Class is exercised. In addition the evaluator devised 10 independent test cases, covering areas including FDP_RIP.2, negative tests for of SSH KEX and accepted encryption algorithms, zeroising CSPs and precedence of manual vs NTP time changes.

2.6.2 Independent Penetration Testing

The evaluators performed twenty-four (24) penetration tests. These were derived from a vulnerability analysis comprised of three parts:

- Public domain vulnerability analysis of TOE specific vulnerabilities related to the Management Plane and the Data Plane;

- Public domain vulnerability analysis of TOE-type vulnerabilities (vulnerabilities that are generic for network devices);
- Analysis of TOE deliverables (Functional Specification, TOE Design, etc.).

2.6.3 Test Configuration

The network diagram in Figure 2 describes the overall setup of the lab and the IP addresses used for developer and evaluator testing. The majority of the tests were performed remotely. Those test cases that required physical access to the TOE (e.g. to access network cables and or to avoid interference by intermediate network equipment) were performed locally at the premises where the equipment was installed.

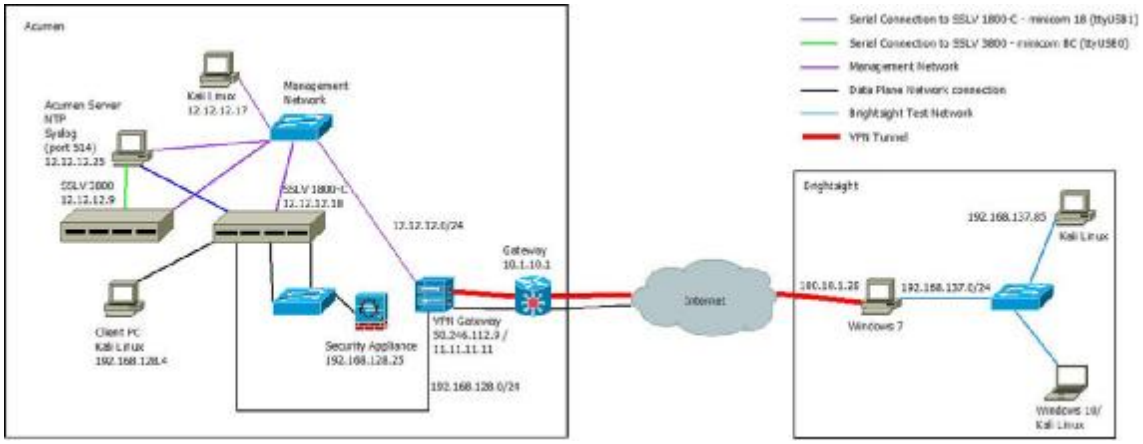

Figure 2 Test Configuration

The following tools were used during testing:

- Bitvise SSH client v6.45
- CAVS version 17.6
- Hydra 8.1
- ISIC, version 0.07
- Large Putty v1.0
- Nessus 6.5.6 professional
- OSWALD (TLS Modification tool) v1.0
- OWASP ZAP 2.4.1
- Putty v0.62
- Skipfish 2.10.b

2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

2.7 Evaluated Configuration

The TOE is defined uniquely by its name and version number Blue Coat Systems, Inc. SSL Visibility Appliance, 3.8.4FC.

2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references the ASE Intermediate Report and other NSP#6-compliant evaluator documents.

The verdict of each claimed assurance requirement is "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Blue Coat Systems, Inc. SSL Visibility Appliance, 3.8.4FC, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 3 augmented with ALC_FLR.3**. This implies that the product satisfies the security technical requirements specified in Security Target Blue Coat Systems, Inc. SSL Visibility Appliance Security Target EAL3, version 0.26.

2.9 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE.

In addition all aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The strength of the implemented cryptographic algorithms was not rated in the course of this evaluation. To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

3 Security Target

The Security Target Blue Coat Systems, Inc. SSL Visibility Appliance Security Target EAL3, version 0.26 *[ST]* is included here by reference.

4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

CLD	Command Line Diagnostics
DLP	Data Loss Prevention
DPI	Deep Packet Inspection
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
IT	Information Technology
ITSEF	IT Security Evaluation Facility
MITM	Man-in-the-Middle
NFP	Netronome chip
NSCIB	Netherlands scheme for certification in the area of IT security
PKI	Public Key Infrastructure
PP	Protection Profile
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TOE	Target of Evaluation
WebUI	Web User Interface

5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[CC]	Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1,revision 4, September 2012.
[CEM]	Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4, September 2012.
[ETR]	Evaluation Technical Report Blue Coat Systems, Inc. SSL Visibility Appliance 3.8.4FC EAL 3+, 16-RPT-170, v4.0, 6 July 2016.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.
[ST]	Blue Coat Systems, Inc. SSL Visibility Appliance Security Target EAL3, version 0.26.

(This is the end of this report).