Certification Report

Symantec SSL Visibility Appliance, 3.10.2.1-21-FIPS140

Sponsor and developer: ***Symantec Corporation***
350 Ellis Street
Mountain View, CA 94043
USA

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

Reportnumber: **NSCIB-CC-66433-CR2**

Report version: **2**

Projectnumber: **NSCIB-CC-66433**

Authors(s): **Denise Cater**

Date: **06 March 2017**

Number of pages: **15**

Number of appendices: **0**

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE 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 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch 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-17-66433**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**Symantec Corporation** **350 Ellis Street, Mountain View, CA, USA**
Product and assurance level	**Symantec SSL Visibility Appliance, 3.10.2.1-21-FIPS140,** Protection Profile Conformance: ▪ Information Assurance Directorate: Protection Profile for Network Devices, version 1.1, 08 June 2012
Project number	**NSCIB-CC-66433**
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 Mutual Recognition Agreement for components up to EAL4

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 1st issue : **22-08-2016**

Date of 2nd issue : **09-03-2017**

Certificate expiry : **22-08-2021**

PRODUCTS
RvA C078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 2200
NL-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 (site) 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 or site satisfies the security requirements stated in the (site) security target.

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates 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 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 Symantec SSL Visibility Appliance, 3.10.2.1-21-FIPS140. The developer of the Symantec SSL Visibility Appliance is Symantec Corporation located in Mountain View, 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.

This second issue of the Certification Report is a result of a "recertification with major changes" with respect to the initial certification of the "SSL Visibility Appliance" (NSCIB-CC-15-66433). The major changes are the change of the developers name and the addition of new hardware models. Small changes to the firmware including security fixes are also included.

A full, up to date vulnerability analysis has been made, as well as renewed testing, renewing the certificate's reusability date to the date of the ETR.

The TOE is the Symantec SSL Visibility Appliance, consisting of hardware appliances and software. The 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 TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 09 February 2017 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 Symantec 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 Symantec 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 assurance requirements for the evaluated security functionality as defined in *[NDPP]*.

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 Symantec SSL Visibility Appliance, 3.10.2.1-21-FIPS140 evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list. It should be noted that the certification results only apply to the specific version of the product as evaluated.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Symantec SSL Visibility Appliance, 3.10.2.1-21-FIPS140 from Symantec Corporation 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
	SV1800B-C appliance	090-03547
	SV1800B-F appliance	090-03548
	SV2800 appliance	090-03063
	SV2800B appliance	090-03549
	SV3800 appliance	090-03064
	SV3800B appliance	090-03550
	SV3800B-20 appliance	090-03551
Software	Symantec SSL Visibility Appliance and Software	3.10.2.1-21-FIPS140

To ensure secure usage a set of guidance documents is provided together with the Symantec 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 security policy of the TOE is consistent with that specified in *[NDPP]*, and does not include the SSL inspection functionality of the appliance.

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 sessions between an administrator's management workstation and the TOE (TLS).
- User Data Protection –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 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 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.

2.3.2 Clarification of scope

The TOE provides a SSH interface for remote user to access its CLD interface, however the security of this interface is not claimed, and this interface cannot be closed by the TOE leaving this interface accessible to the attacker. Therefore, this interface remains a TSFI and the evaluator performed penetration tests to confirm the SSH interface was not vulnerable to attack.

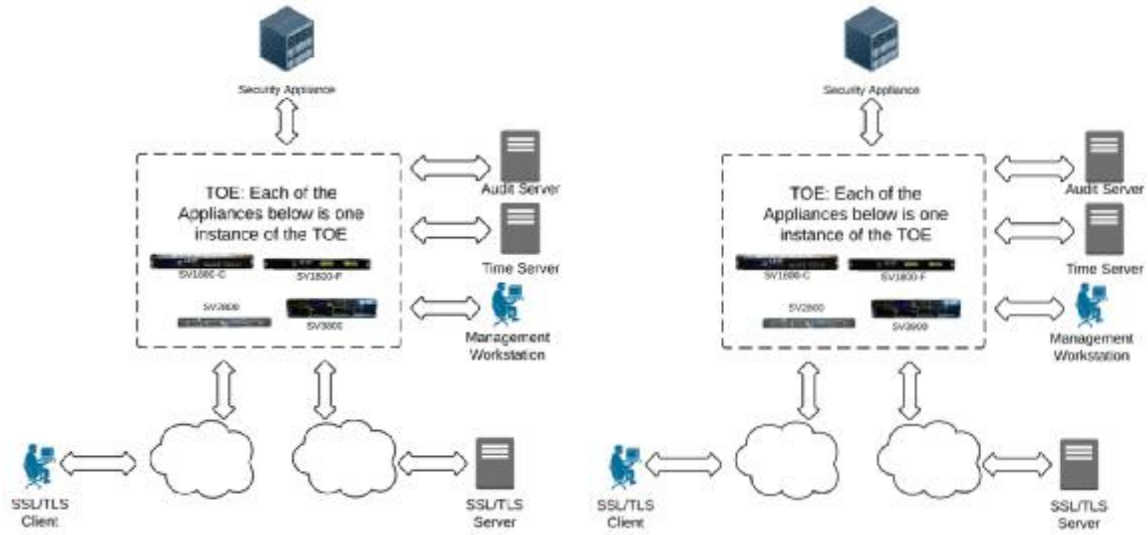
The evaluated deployment of the TOE assumes:

- 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 non-IT environment provides 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.

2.4 Architectural Information

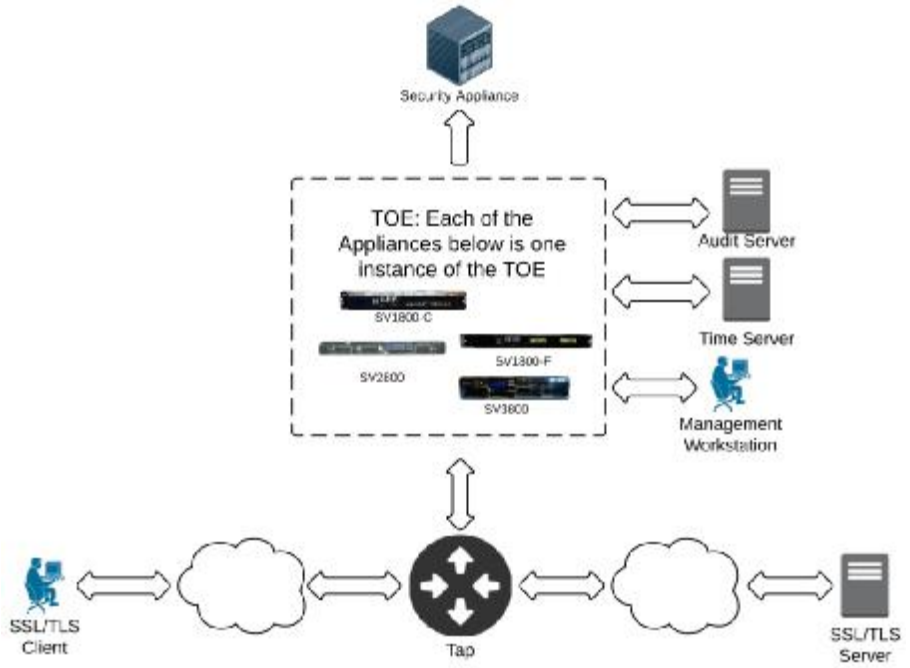
As *[NDPP]* does not include any Development assurance requirements taken from the Common Criteria assurance families entitled “TOE design (ADV_TDS)” and “Security Architecture (ADV_ARC)” the only design information available to the evaluators is the description of the TSFI as required by the “Functional specification (ADV_FSP)” family.

In the *[ST]* the deployment modes of operation possibilities are defined. These are represented in Figure 1. The Active/Passive designation refers to the associated IT environment security appliance and how it behaves. The Inline/Tap designation refers to how the TOE is connected to the network. An “Active” associated IT environment security appliance processes traffic from the TOE and then returns the traffic to the TOE, while a “Passive” appliance simply consumes traffic from the TOE.



Passive inline mode

Active inline mode



Passive tap mode

Figure 1 TOE Deployment modes

The Functional Specification defines the TSFI for the TOE. Below this is summarised.

- TSFI #1: Management GUI (WebUI): Used to configure all security functionality and is accessible over a secure HTTPS connection.
- TSFI #2: Management CLI: Used to configure all security functionality and is accessible either over a SSH connection or via a directly connected console. Note that SSH is not claimed in the NDPP evaluation scope.
- TSFI #3: TLS protocol: Protocol level interface used to facilitate secure communications with remote IT environment devices and for remote administration with the TOE. This interface provides cryptographic protection of network traffic. This interface supports secure remote administration, secure communications with IT environment devices, and the information flow policy control.

- TSFI #4: SSH protocol: Protocol level interface used to facilitate remote administration with the TOE. Note that SSH is not claimed in the NDPP evaluation scope.
- TSFI #5: NTP protocol interface: Interface on which the TOE communicated with an external trusted 3rd party Time server (reliable time source).
- TSFI #6: Audit log server interface: Interface over which the TOE has a one way connection with the audit (Syslog) server (RFC 5424, through a TLS 1.1 or 1.2 connection). This interface is NOT invoked unless the TLS connection is first established.
- TSFI #7: Security appliance interface: Interface in which the TOE communicates with the IT environment provided Security Appliance.
- TSFI #8: Data plane network connection: Network interface over which the TOE monitors (and at times enforces flow decisions) network SSL traffic between two separate networks.

2.5 Documentation

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

Identifier	Version
Symantec Corporation SSL Visibility Appliance Guidance Document, Software version: 3.10.2.1-21-FIPS140	1.6

2.6 IT Product Testing

Testing (depth, coverage, functional tests, independent testing): There are no requirements for developer testing in *[NDPP]*.

2.6.1 Testing approach and depth

The test approach followed the testing assurance activities of each SFR in the *[NDPP]* specified in chapter 4.2 and annex C (where applicable) of the *[NDPP]*.

There were twenty-nine (29) NDPP tests for the claimed SFR testing assurance activities which were fully performed in the previous full evaluation (as reported in *[CR]*) using multiple hardware platforms (SSLV-1800-C and SSLV 3800). For the re-certification, the evaluator sampled twenty-one (21) tests out of the 29 tests to be repeated. Two hardware platforms were sampled to perform these tests: the SSLV 1800B-F (newly added hardware) and the SSLV1800-C (existing hardware). Out of the 21 tests, 11 were tested on the SSLV 1800B-F, 15 were tested on SSLV 1800B-C, and 5 were performed on both platforms. For cipher suite tests, they were performed on a special build (3.2.10-23-debug) which enables the root access to the underlying Linux kernel for feeding the CAVS testing vectors, while for other tests they were tested on the target build (3.2.10-21-FIPS140). All tests results were identical to the previous evaluation (*[CR]*).

2.6.2 Independent Penetration Testing

The evaluators performed nineteen (19) penetration tests in the previous full evaluation (as reported in *[CR]*). 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, Operational User Guidance etc.).

In addition, the evaluator performed penetration tests to confirm the SSH interface did not present any potential vulnerabilities for an attacker to exploit.

For this re-certification, the evaluators repeated their vulnerability analysis, including an updated public domain search. In light of the changes to the TOE since the previous certification, as reported in *[CR]*, the evaluators concluded the relevant public domain vulnerabilities are either patched or not relevant. Consequently it was considered unnecessary to repeat any penetration tests.

2.6.3 Test Configuration

The network diagram in Figure 2 describes the overall setup of the lab and the IP addresses used for evaluator testing during the original evaluation. 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.

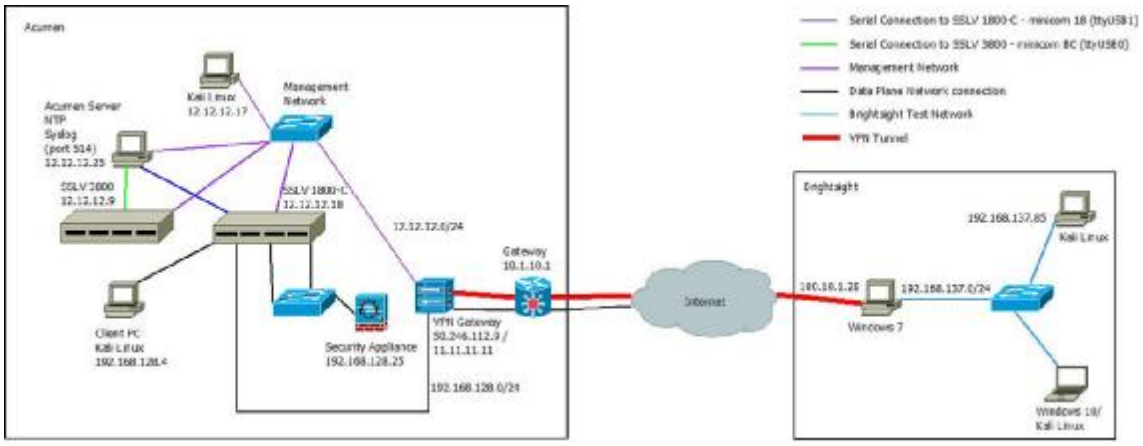


Figure 2 Original Test Configuration

For this re-certification, the evaluators used two test beds (one for each appliance tested) to perform independent testing. These are show in Figure 3 and Figure 4. The tests were performed remotely, as none of the test cases required physical access to the TOE.

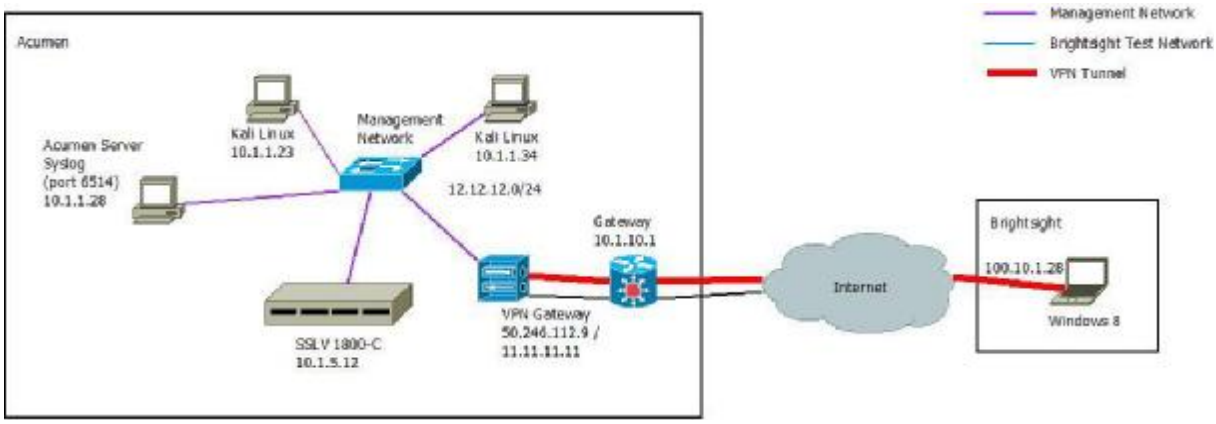


Figure 3 Testbed #1 Configuration

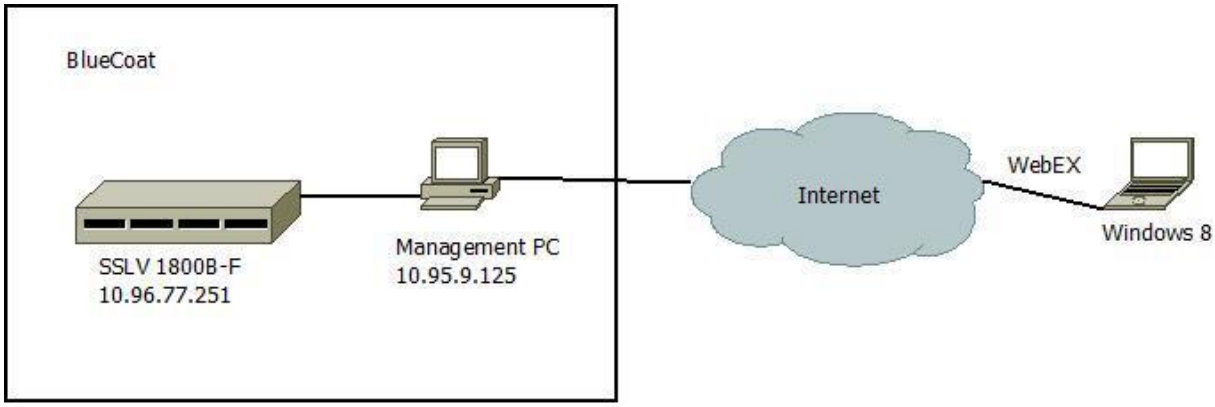


Figure 4 Testbed #2 Configuration

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
- ACUMENSEC Test Suite (TLS Modification tool) version 1.0

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 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.

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 Re-used evaluation results

This is a re-certification: the developer provided an Impact Analysis Report *[IAR]* and the evaluator assessed that in combination with direct re-use of previous evaluation results on the older hardware platforms. Additional verification of the similarity of the newer hardware platforms with the older hardware platforms has been performed including a repetition of a sample of the tests on both a new platform and an old platform. The evaluators also repeated their vulnerability analysis, including an updated public domain search.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Symantec SSL Visibility Appliance, 3.10.2.1-21-FIPS140.

2.9 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 Symantec SSL Visibility Appliance, 3.10.2.1-21-FIPS140, to be **CC Part 2 extended, CC Part 3 refined**, and to meet the assurance requirements specified in *[NDPP]*. This implies that the product satisfies the security technical requirements specified in Security Target Symantec SSL Visibility Appliance NDPP Security Target, version 1.3, 8 February 2017.

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

The Security Target claims 'exact' conformance to the 'Information Assurance Directorate: Protection Profile for Network Devices' Protection Profile, version 1.1, 08 June 2012.

2.10 Comments/Recommendations

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

It should be noted that the use of the SSH interface to the CLD is not claimed in this *[NDPP]* conformant evaluation.

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).

3 Security Target

The Symantec SSL Visibility Appliance NDPP Security Target, version 1.3, 8 February 2017 *[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
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
IT	Information Technology
ITSEF	IT Security Evaluation Facility
NSCIB	Netherlands scheme for certification in the area of IT security
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, 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.
[CR]	Certification Report Blue Coat Systems, Inc. SSL Visibility Appliance 3.8.4FC, version 1.0, 4 August 2016.
[ETR]	Evaluation Technical Report Symantec Corporation SSL Visibility Appliance 3.10.2.1 NDPP, 16-RPT-171, v8.0, 9 February 2017.
[NDPP]	Information Assurance Directorate: Protection Profile for Network Devices, version 1.1, 08 June 2012.
[NSCIB]	Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.
[ST]	Symantec SSL Visibility Appliance NDPP Security Target, version 1.3, 8 February 2017.

(This is the end of this report).