Certification Report

Lancope StealthWatch v6.3.5

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-254-CR
Version: 1.2
Date: 05 May 2014
Pagination: i to iii, 1 to 10

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 evaluation laboratory.

This certification report is associated with the certificate of product evaluation dated 05 May 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 registered trademarks:

- Lancope and StealthWatch are registered trademarks of Lancope, Inc.

TABLE OF CONTENTS

Executive Summary

Lancope StealthWatch v6.3.5 (hereafter referred to as StealthWatch v6.3.5), from Lancope, Inc., is the Target of Evaluation. The StealthWatch v6.3.5 is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

StealthWatch v6.3.5 is a network monitoring system which continuously monitors network traffic for health, performance, and security anomalies. The TOE functionality included within the scope of the evaluation is limited to the secure management features described in the NDPP.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 16 April 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 StealthWatch v6.3.5, and the security requirements to which it is asserted that the product satisfies. 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 StealthWatch v6.3.5 evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

1 Identification of Target of Evaluation

Lancope StealthWatch v6.3.5 (hereafter referred to as StealthWatch v6.3.5), from Lancope, Inc., is the Target of Evaluation. The StealthWatch v6.3.5 is conformant with the Protection Profile for Network Devices, v1.1, June 8, 2012 (hereafter referred to as the NDPP).

2 TOE Description

StealthWatch v6.3.5 monitors network traffic for health, performance, and security anomalies and is comprised of the following components:

- *FlowCollector appliance* which serves as the network flow collection and analysis point;
- *FlowSensor appliance* which gathers packet-level details of network flows in order to provide deep packet inspection of network data flows; and
- *StealthWatch Management Console (SMC)* which manages the other components and provides the user interfaces that allows Administrators to control the configuration for each StealthWatch component.

The FlowSensor(s) forward flow data to the FlowCollector which aggregates all gathered data and forwards it to the Management Console for analysis and reporting. Administrators can review gathered data from the SMC web interface.

The TOE functionality included within the scope of the evaluation is limited to the secure management features described in the NDPP.

A diagram of the StealthWatch v6.3.5 architecture is depicted below. The red dotted line depicts the TOE boundary.

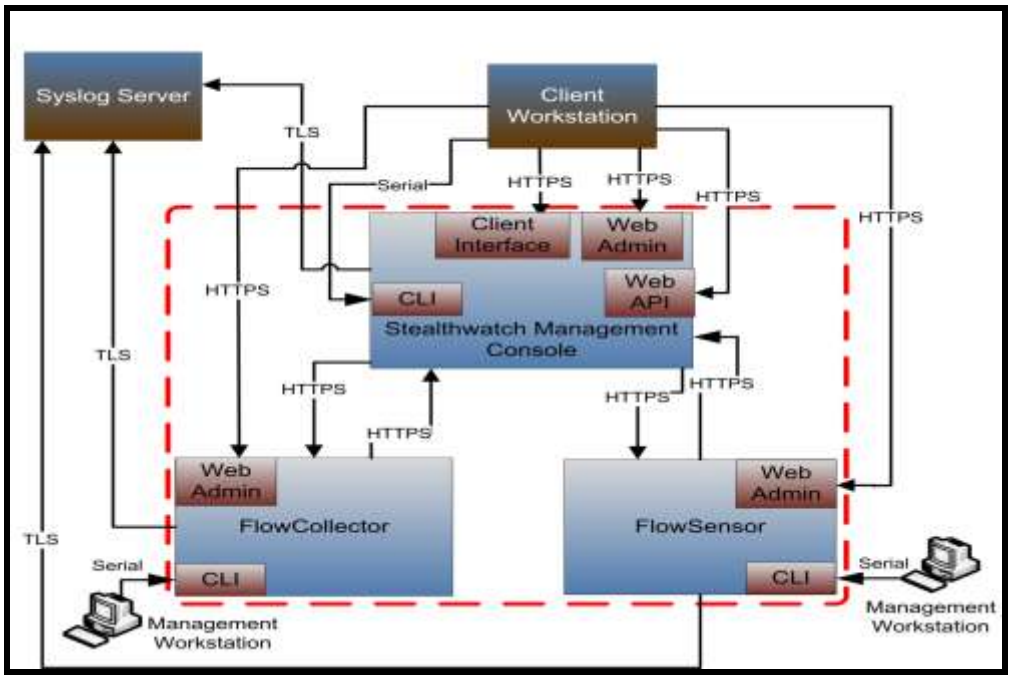

Figure 1: TOE Architecture

3 Security Policy

StealthWatch v6.3.5 implements a role-based access control policy to control administrative access to the system. In addition, StealthWatch v6.3.5 implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support[1]
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Functionality (TSF)
- TOE Access
- Trusted Path/Channels

Specific details concerning the above mentioned security policies can be found in Section 6 of the Security Target (ST).

[1] The TOE implements the RSA BSAFE Crypto-J Software Module. FIPS 140-2 certificate 1291.

4 Security Target

The ST associated with this Certification Report is identified below:

Lancope, Inc. StealthWatch v6.3.5 Security Target, version 1.3, April 3, 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.*

StealthWatch v6.3.5 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 - HTTPS
    - FCS_TLS_EXT.1 - TLS
    - 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 StealthWatch v6.3.5 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 Assumption is 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

The StealthWatch v6.3.5 network monitoring functionality was not included within the scope of this evaluation.

The FIPS validation is vendor affirmed and has been ported according to Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program (FIPS IG G.5).

7 Evaluated Configuration

The evaluated configuration for StealthWatch v6.3.5 comprises StealthWatch v6.3.5 running on the following hardware appliances:

- FlowCollector 1000, 2000, 4000
- FlowSensor 1000, 2000, 3000; and
- StealthWatch Management Console 1000, 2000.

The publication entitled Lancope, Inc. StealthWatch v6.3.5 Guidance Documentation Supplement, Version 1.2 describes the procedures necessary to install and operate StealthWatch v6.3.5 in its evaluated configuration.

8 Documentation

The Lancope, Inc. documents provided to the consumer are as follows:

a. StealthWatch Management Console User Guide for StealthWatch v6.3;
b. Lancope, Inc. StealthWatch v6.3.5 Guidance Documentation Supplement;
c. StealthWatch System v6.3.4 Update Guide;
d. StealthWatch System Hardware Configuration Guide (for StealthWatch System v6.3);
e. SMC Web Services Programming Guide For SMC Version 6.3;
f. StealthWatch System Hardware Installation Guide (for StealthWatch System v6.3);
g. StealthWatch Management Console Admin Interface Online Help for Version 6.3;
h. StealthWatch Management Console Web Interface Online Help for Version 6.3;
i. StealthWatch Management Console Client Interface Online Help for Version 6.3; and
j. StealthWatch FlowSensor Admin Interface Online Help for Version 6.3.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of StealthWatch v6.3.5, including the following areas:

Development: The evaluators analyzed the StealthWatch v6.3.5 functional specification and determined that the functional specification describes the purpose and method of use for each TSF interface and that the StealthWatch v6.3.5 functional specification is an accurate and complete instantiation of the SFRs.

Guidance Documents: The evaluators examined the StealthWatch v6.3.5 preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the StealthWatch v6.3.5 configuration management documentation was performed. The evaluators found that the StealthWatch v6.3.5 configuration items were clearly marked.

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

10 ITS Product Testing

Testing consists of the following two steps: 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 CGI IT Security Evaluation & Test Facility test goal:

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

StealthWatch v6.3.5 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test 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 StealthWatch v6.3.5 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 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NDPP	Protection Profile for Network Devices
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SMC	StealthWatch Management Console
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

13 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. Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, April 25, 2014.

e. Lancope, Inc. StealthWatch v6.3.5 Security Target, version 1.3, April 3, 2014.

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

g. Lancope StealthWatch v6.3.5 Common Criteria NDPP v1.1 Evaluation Technical Report, version 0.5, April 16, 2014.