Certification Report

Forum Sentry v8.1.641

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-271-CR
Version: 1.2
Date: 29 July 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 Canada, 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 Canada, 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 Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 22 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).

TABLE OF CONTENTS

Executive Summary

Forum Sentry v8.1.641 (hereafter referred to as Sentry 8.1.641), from Forum Systems, Inc., is the Target of Evaluation. Sentry 8.1.641 is conformant with the Protection Profile for Network Devices Version 1.1, 08 June 2012, hereafter referred to as PP_ND_v1.1 .

Sentry 8.1.641 is a hardware TOE that provides application gateway functionality for a variety of web-based (such as HTTP and XML) and non-web-based (such as SFTP and LDAP) protocols. This functionality is implemented by an engine that examines application-layer traffic elements to apply policy to traffic. Policy takes the form of application-firewall rules, an antivirus engine, and pattern recognition rules. This allows the product to protect against attacks and to enforce access control rules based on the information within XML requests. The TOE functionality included within the scope of the evaluation is limited to the secure management features described in the PP_ND_v1.1 .

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 30 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 Sentry 8.1.641, 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 Sentry 8.1.641 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).

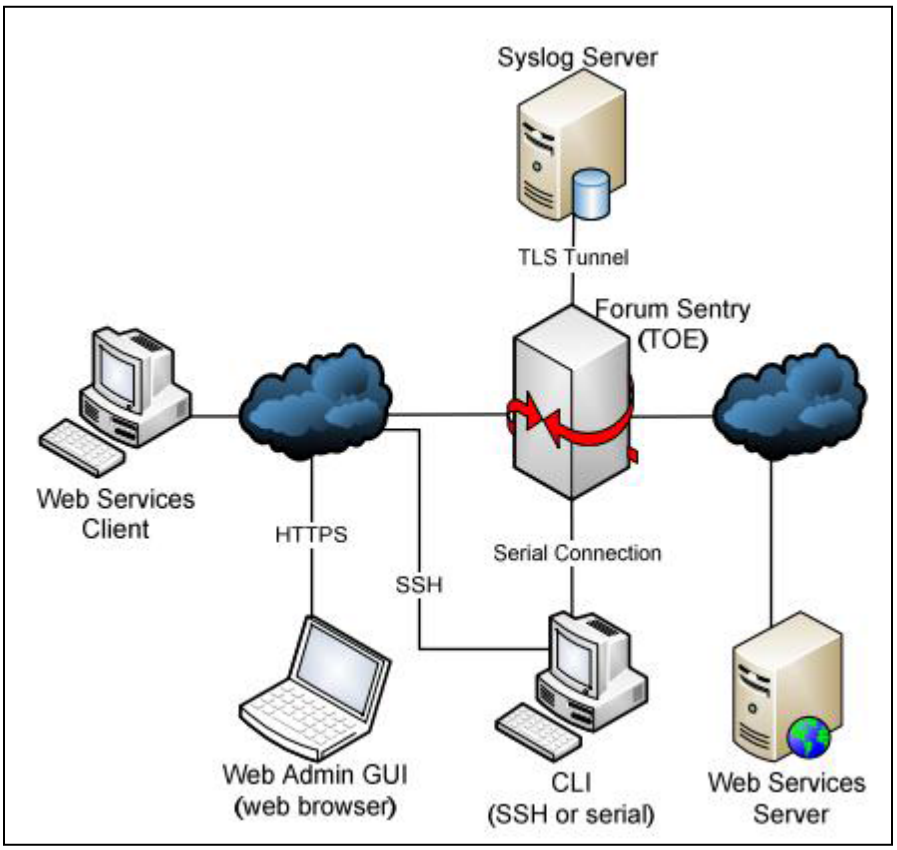
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Protection Profile (PP) conformant evaluation is Forum Sentry v8.1.641 (hereafter referred to as Sentry 8.1.641), from Forum Systems, Inc.

2 TOE Description

Sentry 8.1.641 is a hardware TOE that provides application gateway functionality for a variety of web-based (such as HTTP and XML) and non-web-based (such as SFTP and LDAP) protocols. This functionality is implemented by an engine that examines application-layer traffic elements to apply policy to traffic. Policy takes the form of application-firewall rules, an antivirus engine, and pattern recognition rules. This allows the product to protect against attacks and to enforce access control rules based on the information within XML requests. The TOE functionality included within the scope of the evaluation is limited to the secure management features described in the PP_ND_v1.1 .

A diagram of the Sentry 8.1.641 architecture is as follows;



3 Security Policy

Sentry 8.1.641 implements a role-based access control policy to control administrative access to the system. In addition, Sentry 8.1.641 implements policies pertaining to the following security functional classes:

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

The following cryptographic module was evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
nShield F2 6000e [1], nShield F2 1500e [2], nShield F2 500e [3] and nShield F2 10e [4]	*1743*

4 Security Target

The ST associated with this Certification Report is identified below:

Forum Systems, Inc. Sentry v8.1.641 Security Target, v1.2, 2014-06-02

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.*

Sentry 8.1.641 is:

a. *Protection Profile for Network Devices Version 1.1, 08 June* 2012 *conformant.;*

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 Sentry 8.1.641 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

Sentry 8.1.641 application gateway functionality was not included within the scope of this evaluation, only the functionality listed in the PP_ND_v1.1 is included.

When accessing the TOE via SSH, users of the TOE are required to configure the SSH client to only use AES-CBC-128 and AES-CBC-256 for encryption. Use of any other encryption algorithm for SSH is prohibited when the TOE is in its evaluated configuration. This was not the intent of the SSH requirements in the NDPP, the TOE and not the client is supposed enforce the use of AES-CBC-128 or AES-CBC-256 for encryption.

7 Evaluated Configuration

The evaluated configuration for Sentry 8.1.641 comprises:

- Sentry v8.1.641 software running on a Forum Sentry 4564 appliance with a Thales nShield 6000e F3 HSM.

The publication entitled *Forum Systems, Inc. Sentry v8.1.641 Guidance Documentation Supplement v0.7, April 23, 2014* describes the procedures necessary to install and operate Sentry 8.1.641 in its evaluated configuration.

8 Documentation

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

a. Forum Systems Sentry v8.1 CLI Reference Guide, January 2012;

b. Forum Systems Sentry 456X Rev. B Hardware Installation Guide, January 2013;

c. Forum Systems Sentry Guide to Security Worlds, January 2013;

d. Forum Systems Sentry Logging Guide, January 2013;

e. Forum Systems, Inc. Sentry v8.1.641 Guidance Documentation Supplement v0.7, April 23, 2014;

f. Forum Systems Sentry System Management Guide, January 2013; and

g. *Forum Systems Sentry Web-based Administration Guide, January 2013.*

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Sentry 8.1.641, including the following areas:

Development: The development documentation was not reviewed, as the requirements on the content of the development documentation is implicitly assessed by virtue of the other assurance activities listed in the PP being performed.

Guidance Documents: The evaluators examined the Sentry 8.1.641 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 Sentry 8.1.641 configuration management system and associated documentation was performed. The evaluators found that the Sentry 8.1.641 configuration items were clearly marked.

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

10 ITS Product Testing

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

10.1 Independent Functional Testing

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

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following CGI IT Security Evaluation & Test Facility test goal:

a. PP_ND_v1.1 required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the PP_ND_v1.1

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. PP_ND_v1.1 required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the PP_ND_v1.1 ; and

b. Vulnerability scans: The objective of this test goal is the 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

Sentry 8.1.641 was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. 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 functional tests yielded the expected results, providing assurance that Sentry 8.1.641 behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for a protection profile conformance claim as stated 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
HTTP	Hypertext Transfer Protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LDAP	Lightweight Directory Access Protocol
NDPP	Network Device Protection Profile
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
XML	Extensible Markup Language

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. Protection Profile for Network Devices Version 1.1, 08 June 2012

e. Forum Systems, Inc. Sentry v8.1.641 Security Target, v1.2, 2014-06-02

f. Evaluation Technical Report NDPP v1.1 Common Criteria Evaluation of Sentry 8.1.641, v1.1, June 2, 2014.