Certification Report

SonicWALL SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-224-CR
Version: 1.0
Date: 5 February 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 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3*. This certification report, and its associated certificate, apply 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) provides 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 EWA-Canada.

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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 5 February 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

SonicWALL SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances (hereafter referred to as SonicOS 5.9.0), from Dell SonicWALL, Inc., is the Target of Evaluation. SonicOS 5.9.0 is conformant with the *Protection Profile for Network Devices version 1.1, 8 June 2012 (NDPP v1.1).*

SonicOS 5.9.0 is custom software running on purpose built hardware platforms that combine to form a UTM (Unified Threat Management) device. UTMs are network firewalls that provide additional features, such as anti-virus capabilities and IPS (Intrusion Prevention System). The product is managed using a web-based GUI, accessed through a permitted device running a supported web browser connected directly to the appliance over a network cable and communicating via hypertext transfer protocol – secure (HTTPS). For the purpose of this evaluation, only the functionality covered by the NDPP (Network Device Protection Profile) has been evaluated; as a result, the UTM functionality has not been evaluated.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 28 November 2013 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 SonicOS 5.9.0, the security requirements, and the level of confidence (evaluation assurance level) to which it is asserted that the product satisfies its security requirements. 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.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the requirements of the claimed protection profile. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

Communications Security Establishment Canada, as the CCS Certification Body, declares that the SonicOS 5.9.0 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

SonicWALL SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances (hereafter referred to as SonicOS 5.9.0), from Dell SonicWALL, Inc. is the Target of Evaluation. The SonicOS 5.9.0 is conformant with the *Protection Profile for Network Devices version 1.1, 8 June 2011 (NDPP v1.1).*

2 TOE Description

SonicOS 5.9.0 is custom software running on purpose built hardware platforms that combine to form a UTM (Unified Threat Management) device. UTMs are network firewalls that provide additional features, such as anti-virus capabilities and IPS (Intrusion Prevention System). The product is managed using a web-based GUI, accessed through a permitted device running a supported web browser connected directly to the appliance over a network cable and communicating via hypertext transfer protocol – secure (HTTPS).

3 Evaluated Security Functionality

The complete list of evaluated security functionality for SonicOS 5.9.0 is identified in Section 6 of the ST.

The following cryptographic modules were evaluated to the FIPS 140-2 standard:

Cryptographic Module	**Certificate #**
NSA 4500 and NSA E5500	*Pending* [2]
NSA E8500 and NSA E8510	*Pending*
NSA E7500	*Pending*
NSA E10000 Series	*Pending*
NSA 3500	*Pending*
NSA 250M and NSA 250MW	*Pending*
NSA 2400 and NSA 2400MX	*Pending*
NSA 220, NSA 220W and NSA 240	*Pending*
NSA E6500	*Pending*
TZ 105, TZ 105W, TZ 205, TZ 205W, TZ 210, TZ 210W, TZ	*Pending*

[2] The cryptographic module is in the process of FIPS 140-2 validation under the Cryptographic Module Validation Program (CMVP). Information regarding the status of the module validation can be found on the NIST website.

215 and TZ 215W	

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in SonicOS 5.9.0:

Cryptographic Algorithm	**Standard**	**Certificate #**
Advanced Encryption Standard (AES)	FIPS 197	2015
Rivest Shamir Adleman (RSA)	FIPS 186-3	640
Secure Hash Algorithm (SHA-1)	FIPS 180-3	1765
Keyed-Hash Message Authentication (HMAC)	FIPS 198	1219

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: SonicWall SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances Security Target
Version: 2.4
Date: 29 November 2013

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3.*

SonicOS 5.9.0 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 Destruction;
   - FCS_HTTPS_EXT.1 – Extended: HTTPS;
   - FCS_IPSEC_EXT.1 – Extended: IPSEC;
   - FCS_RBG_EXT.1 – Extended: Cryptographic Operation (random bit generator);
   - FCS_TLS_EXT.1 – Extended: TLS;
   - FIA_PMG_EXT.1 – Password Management;
   - FIA_UAU_EXT.2 – Extended: Password-based authentication mechanism;
   - FIA_UIA_EXT.1 – User Identification and Authentication;
   - FPT_APW_EXT.1 – Extended: Protection of Administrator Passwords;

- FPT_SKP_EXT.1 – Extended: Management of TSF Data (for reading symmetric keys);
- FPT_TST_EXT.1 – TSF Self Test;
- FPT_TUD_EXT.1 – Extended: Trusted Update; and
- FTA_SSL_EXT.1 – TSF-Initiated Locking.

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Security Policy

SonicOS 5.9.0 implements a role-based access control policy to control user access to the system; details of this security policy can be found in Section 6 of the ST.

In addition, SonicOS 5.9.0 implements polices pertaining to security audit, user data protection, identification and authentication, cryptographic support, security management, protection of the TOE Security Function (TSF), TOE access and trusted path. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of SonicOS 5.9.0 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.

7.1 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;

- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner;

7.2 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.

8 Evaluated Configuration

The evaluated configuration for SonicOS 5.9.0 comprises:

SonicOS Enhanced v5.9.0 running on one of the following hardware appliances:

- TZ 105;

- TZ 105W;
- TZ 205;
- TZ 205W;
- TZ 215;
- TZ 215W;
- NSA 220;
- NSA 220W;
- NSA 240;
- NSA 250M;
- NSA 250MW;
- NSA 2400;
- NSA 2400MX;
- NSA 3500;
- NSA 4500;
- NSA E5500;
- NSA E6500;
- NSA E7500;
- NSA E8500;
- NSA E8510;
- NSA E1040;
- NSA E10800; and
- NSA E10200.

The following publications describe the procedures necessary to install and operate SonicOS 5.9.0 in its evaluated configuration:

- Dell SonicWALL, Inc. SonicOS Enhanced 5.9 Administrator's Guide Rev A
- Dell SonicWALL, Inc. SonicOS 5.5.1.2 FIPS/Common Criteria Release Notes 232-001907-00 Rev A 07/10
- Dell SonicWALL, Inc. SonicOS 5.9.0.0 Release Notes 232-000925-00 Rev D 08/13
- Dell SonicWALL, Inc. SonicOS 5.9.0.0 SuperMassive 10000 Series Release Notes 232-002305-00 Rev A

9 Documentation

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

- Dell SonicWALL, Inc. NSA 220 Series Quick Start Poster P/N 232-002003-50 Rev A 09/11;
- Dell SonicWALL, Inc. NSA 240 Getting Started Guide P/N 232-001580-00 Rev A 2/2010;
- Dell SonicWALL, Inc. NSA 250M or 250MW Quick Start Poster P/N 232-001924-51 Rev A 01/12;
- Dell SonicWALL, Inc. NSA 2400 Getting Started Guide P/N 232-001276-52 Rev A 04/10;
- Dell SonicWALL, Inc. NSA 2400MX Getting Started Guide P/N 232-001475-51 Rev A 3/10;
- Dell SonicWALL, Inc. NSA 5000/4500/3500 Getting Started Guide P/N 232-001265-52 Rev A 01/11;
- Dell SonicWALL, Inc. NSA E5500 Getting Started Guide P/N 232-001052-55 Rev A 3/13;
- Dell SonicWALL, Inc. NSA E6500 Getting Started Guide P/N 232-001051-54 Rev A 03/13;
- Dell SonicWALL, Inc. NSA E7500 Getting Started Guide P/N 232-001050-55 Rev A 04/13;
- Dell SonicWALL, Inc. NSA E8500 Getting Started Guide P/N 232-001891-53 Rev A 04/13;
- Dell SonicWALL, Inc. NSA E8510 Getting Started Guide P/N 232-001858-51 Rev A 04/13;
- Dell SonicWALL, Inc. TZ 105 Series Quick Start Poster P/N 232-002038-50 Rev A 03/12;
- Dell SonicWALL, Inc. TZ 205 Series Quick Start Poster P/N 232-002114-51 Rev A 04/12;
- Dell SonicWALL, Inc. TZ 215 Series Quick Start Poster P/N 232-002037-51 Rev A 11/11;
- Dell SonicWALL, Inc. SuperMassive Series Datasheet;
- Dell SonicWALL, Inc. SonicOS Enhanced 5.9 Administrator's Guide Rev A;
- Dell SonicWALL, Inc. SonicOS 5.5.1.2 FIPS/Common Criteria Release Notes 232-001907-00 Rev A 07/10;
- Dell SonicWALL, Inc. SonicOS 5.9.0.0 Release Notes 232-000925-00 Rev D 08/13; and
- Dell SonicWALL, Inc. SonicOS 5.9.0.0 SuperMassive 10000 Series Release Notes 232-002305-00 Rev A.

10 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of SonicOS 5.9.0, including the following areas:

Development: The evaluators analyzed the SonicOS 5.9.0 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the SonicOS 5.9.0 security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the SonicOS 5.9.0 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 SonicOS 5.9.0 configuration management system and associated documentation was performed. The evaluators found that the SonicOS 5.9.0 configuration items were clearly marked. The developer's configuration management system was observed during a site visit, and it was found to be mature and well-developed.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of SonicOS 5.9.0 during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the SonicOS 5.9.0. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

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

11 ITS Product Testing

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

11.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[3].

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

11.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

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 list of EWA-Canada test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Protection Profile required assurance activities: The objective of this test goal is to perform the assurance activities mandated by the protection profile to which the TOE is claiming conformance.

11.3 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. Protection Profile 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.

[3] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

11.4 Conduct of Testing

SonicOS 5.9.0 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 (ITSET) Facility at EWA-Canada. 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.

11.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, providing assurance that SonicOS 5.9.0 behaves as specified in its ST and functional specification.

12 Results of the Evaluation

This evaluation has provided the basis for an NDPP v1.1 conformance claim. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
AES	Advanced Encryption Standard
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User interface
HMAC	Keyed-Hash Message Authentication
HTTPS	Hypertext transfer protocol
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
UTM	Unified Threat Management

14 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 3, July 2009.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 3, July 2009.

d. SonicWall SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances Security Target, 2.4, Security Target, 29 November 2013.

e. Evaluation Technical Report for SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Applances,version 1.0 28 November 2013.