



# COMMON CRITERIA CERTIFICATION REPORT

SonicWall SonicOS Enhanced V6.2.5 with IPS on NSA, SM, and TZ  
Appliances

383-4-422P

12 January 2018

v1.0





# FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

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 Scheme – 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 Canadian CC Scheme, 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.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services

Telephone: (613) 991-7654

E-mail: [itsclientservices@cse-cst.gc.ca](mailto:itsclientservices@cse-cst.gc.ca)



## OVERVIEW

The Canadian Common Criteria Scheme 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 Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the 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 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.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme and to the Common Criteria portal (the official website of the International Common Criteria Project).



# TABLE OF CONTENTS

<b>Executive Summary</b> .....	<b>1</b>
<b>1 Identification of Target of Evaluation</b> .....	<b>2</b>
1.1 Common Criteria Conformance.....	2
1.2 TOE description .....	2
1.3 TOE architecture.....	2
<b>2 Security policy</b> .....	<b>3</b>
2.1 Cryptographic functionality.....	3
<b>3 Assumptions and Clarifications of Scope</b> .....	<b>4</b>
3.1 Usage and Environmental assumptions .....	4
3.2 Clarification of Scope.....	5
<b>4 Evaluated Configuration</b> .....	<b>6</b>
4.1 Documentation.....	6
<b>5 Evaluation Analysis Activities</b> .....	<b>8</b>
5.1 Development.....	8
5.2 Guidance Documents .....	8
5.3 Life-cycle Support .....	8
<b>6 Testing Activities</b> .....	<b>9</b>
6.1 Assessment of Developer Tests.....	9
6.2 Conduct of Testing.....	9
6.3 Independent Functional Testing.....	9
6.4 Independent Penetration Testing .....	10
<b>7 Results of the Evaluation</b> .....	<b>11</b>
7.1 Recommendations/Comments.....	11
<b>8 Supporting Content</b> .....	<b>12</b>
8.1 List of Abbreviations.....	12
8.2 References .....	13



## LIST OF FIGURES

Figure 1 TOE Architecture .....2

## LIST OF TABLES

Table 1 TOE Identification .....2  
Table 2 Cryptographic Algorithm(s) .....3



## EXECUTIVE SUMMARY

SonicWall SonicOS Enhanced V6.2.5 with IPS on NSA, SM, and TZ Appliances (hereafter referred to as the Target of Evaluation, or TOE), from SonicWall, Inc., was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 12 January 2018 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance 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.

Communications Security Establishment, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Canadian Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).

# 1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

**Table 1 TOE Identification**

<b>TOE Name and Version</b>	SonicWall SonicOS Enhanced V6.2.5 with IPS on NSA, SM, and TZ Appliances
<b>Developer</b>	SonicWall, Inc.
<b>Conformance Claim</b>	collaborative Protection Profile for Network Devices (v1.0, 27-Feb-2015)

## 1.1 COMMON CRITERIA CONFORMANCE

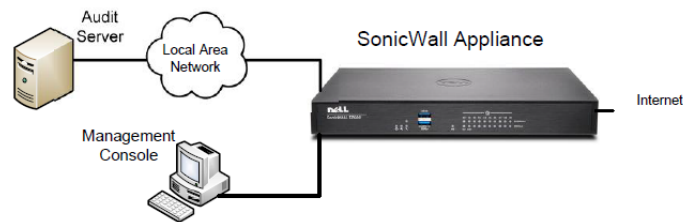
The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

## 1.2 TOE DESCRIPTION

The TOE is comprised of the SonicWALL SonicOS Enhanced v6.2.5 software running on purpose built NSA, SM, and TZ model hardware platforms. The TOE supports Virtual Private Network (VPN) functionality, which provides a secure connection between the TOE and the audit server. The TOE supports authentication, and protects data from disclosure or modification during transfer.

## 1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:



**Figure 1 TOE Architecture**



## 2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

### 2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following Government of Canada approved cryptographic algorithms were evaluated by the CAVP and used by the TOE:

**Table 2 Cryptographic Algorithm(s)**

Cryptographic Algorithm	Standard	Certificate Number
Advanced Encryption Standard (AES)	FIPS 197	5070
Rivest Shamir Adleman (RSA)	FIPS 186-4	2750
Secure Hash Algorithm (SHS)	FIPS 180-3	4130
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	3384
Deterministic Random Bit Generation (DRBG)	SP 800-90A	1887
Key Agreement Scheme	SP 800-56A	1631
Component Validation List	SP 800-56A	1631,1632
Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-4	1315





## 3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE 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.

### 3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The network device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.
- The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the device should not provide computing platform for general purpose applications (unrelated to networking functionality).
- A standard/generic network device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the network device to protect data that originates on or is destined to the device itself, to include administrative data and audit data.
- The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device.
- The network device firmware and software is assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.



## 3.2 CLARIFICATION OF SCOPE

---

The scope of the evaluation is limited to secure management of the TOE. The following features/functionality are excluded from this evaluation:

- Remote Authentication Dial-In User Service (RADIUS)
- Lightweight Directory Access Protocol (LDAP)
- Active Directory (AD)
- eDirectory authentication
- Command Line Interface (CLI) (Secure Shell (SSH))
- Application Firewall
- Web Content Filtering
- Hardware Failover
- Real-time Blacklist (Simple Mail Transfer Protocol (SMTP))
- Global Security Client (including Group VPN)
- Global Management System
- SonicPoint
- Voice over IP (VoIP)
- Network Time Protocol (NTP)
- Antivirus
- Intrusion Prevention

A separate evaluation of the TOE determined that this product satisfies the requirements of the collaborative Protection Profile for Network Devices version 1.0 and the extended package for Intrusion Prevention Systems version 2.1. Results for this evaluation can be found on the Canadian Certified Products list.



## 4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises the TOE firmware (SonicOS Enhanced V6.2.5.0-50n) installed on the following hardware platforms:

### SonicWall NSA Series

- NSA 2600
- NSA 3600
- NSA 4600
- NSA 5600
- NSA 6600

### SonicWall SM Series

- SM 9200
- SM 9400
- SM 9600

### SonicWall TZ Series

- TZ 300/W
- TZ 400/W
- TZ 500/W
- TZ 600

An audit server that supports syslog and IPSEC VPNs is required in the operating environment.

### 4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

- a. SonicWall™ TZ300 / TZ300 Wireless Quick Start Guide 232-003785-50 Rev A Updated - January 2017
- b. SonicWall™ TZ400 / TZ400 Wireless Quick Start Guide 232-003783-50 Rev B Updated - February 2017
- c. SonicWall™ TZ500 / TZ500 Wireless Quick Start Guide 232-003781-50 Rev A Updated - January 2017
- d. SonicWall™ TZ600 Quick Start Guide 232-003779-50 Rev A Updated - January 2017
- e. SonicWall™ NSA 2600/3600/4600/5600/6600 Getting Started Guide 232-003419-51 Rev A Updated - March 2017
- f. SonicWall™ SuperMassive™ 9200/9400/9600 Getting Started Guide 232-000344-50 Rev A Updated - February 2017
- g. SonicWall™ SonicOS 6.2 Administration Guide 232-002365-02 Rev B Updated - April 2017



- h. SonicWall™ SonicOS 6.2.5/6.2.7/6.2.9 Log Events Reference Guide 232-004020-00 Rev A Updated - July 2017
- i. SonicWALL SonicOS Enhanced V6.2 with IPS on NSA, SM, and TZ Appliances Common Criteria Guidance Supplement Version 1.2, 10 May 2017



## 5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

### 5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; 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 determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

### 5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE 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.

Section 4.1 provides details on the guidance documents.

### 5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

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



## 6 TESTING ACTIVITIES

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

### 6.1 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. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

### 6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

### 6.3 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. The following testing activities were performed:

- a. PP Assurance Activities: The evaluator performed the assurance activities listed in the claimed PP.

#### 6.3.1 FUNCTIONAL TEST RESULTS

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



## 6.4 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. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and
- b. Fuzz Testing: The evaluator conducted fuzz testing using unexpected inputs and malformed packets on the TOE interfaces.

### 6.4.1 PENETRATION TEST RESULTS

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.



## 7 RESULTS OF THE EVALUATION

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

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme 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. These evaluation results apply 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 Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

### 7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.





## 8 SUPPORTING CONTENT

### 8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VPN	Virtual Private Network



## 8.2 REFERENCES

---

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
SonicWall SonicOS Enhanced V6.2 with IPS on NSA, SM, and TZ Appliances Security Target v1.21P, 12 January 2018.
Evaluation Technical Report for SonicOS Enhanced v6.2.5 with IPS on NSA, SM, and TZ Appliances v1.1, 12 January 2018.