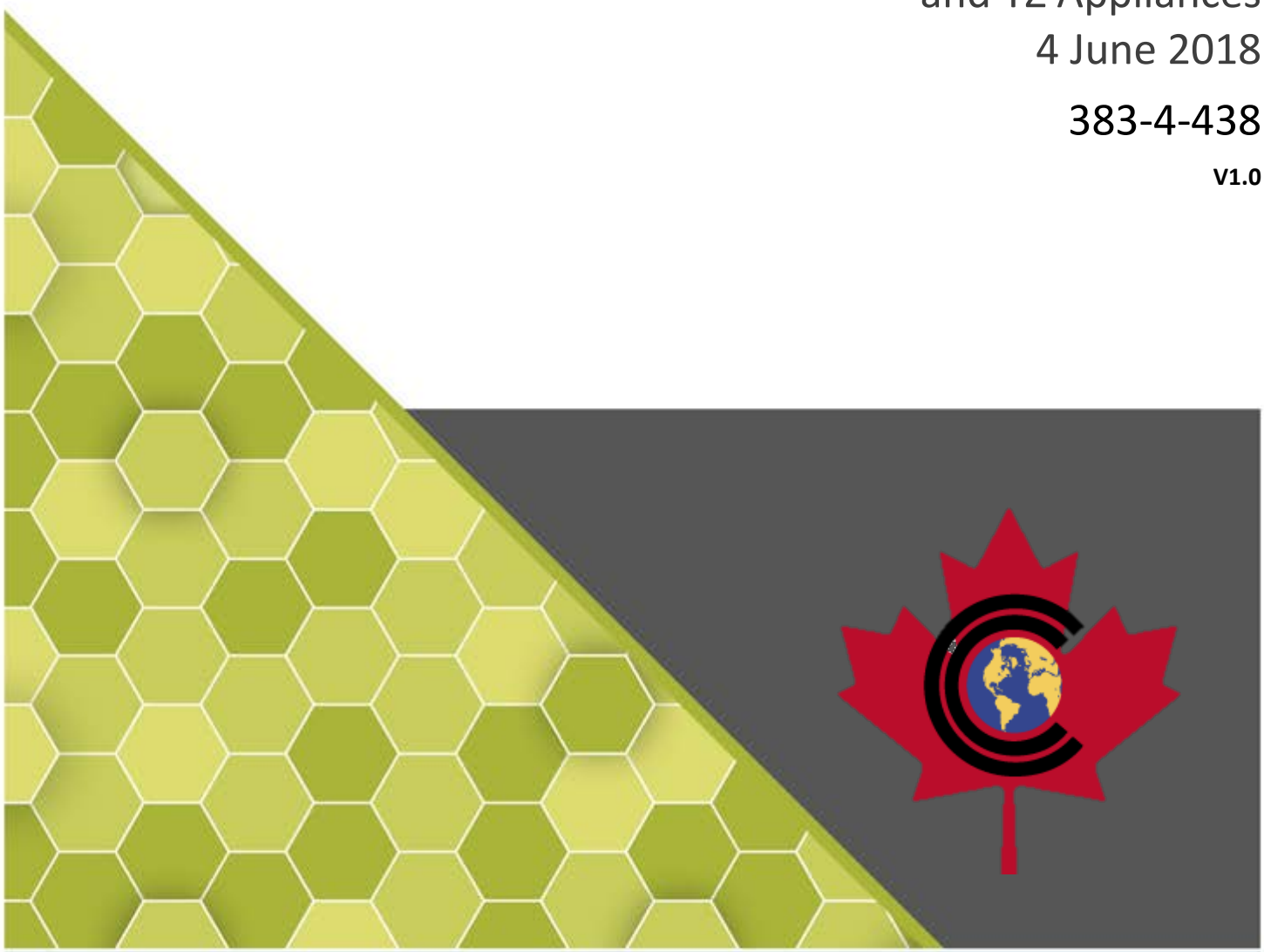
COMMON CRITERIA CERTIFICATION REPORT

SonicWall SonicOS Enhanced V6.2.5 VPN Gateway on NSA, SM, and TZ Appliances

4 June 2018

383-4-438

V1.0



Canada

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 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. 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

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.

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

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

SonicWall SonicOS Enhanced V6.2.5 VPN Gateway 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 4 June 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

TOE Name and Version	SonicWall SonicOS Enhanced V6.2.5 VPN Gateway on NSA, SM, and TZ Appliances
Developer	SonicWall, Inc.
Conformance Claim	collaborative Protection Profile for Stateful Traffic Filter Firewalls (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 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

1.2 TOE DESCRIPTION

The TOE is a network appliance that acts as network gateway device that terminate Virtual Private Network (VPN) tunnels. It can be used to provide an authenticated and encrypted path to another site. The TOE supports authentication, and protects data from disclosure or modification during transfer. The VPN functionality is also used to provide a secure connection between the device and the audit server.

The firewall capabilities of the TOE include stateful packet inspection. Stateful packet inspection maintains the state of network connections, such as Transmission Control Protocol (TCP) streams and User Datagram Protocol (UDP) communication, traveling across the firewall. The firewall distinguishes between legitimate packets and illegitimate packets for the given network deployment. Only packets adhering to the administrator-configured access rules are permitted to pass through the firewall; all others are rejected.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

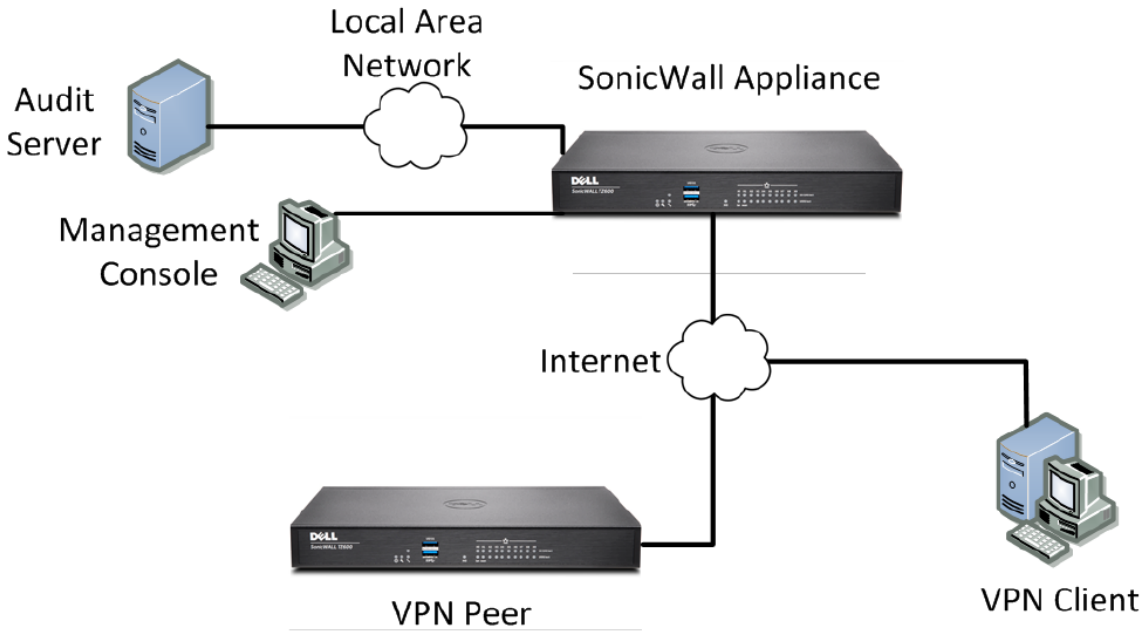


Figure 1 TOE Architecture

2 SECURITY POLICY

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

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels
- Stateful Traffic Filtering

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
Component Validation List	SP 800-56A	#1631, #1632
Elliptic Curve Digital Signature Algorithm (ECDSA)	FIPS 186-4	#951, #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 firewall 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 firewall's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the firewall and the data it contains. As a result, the cPP will not include any requirements on physical tamper protection or other physical attack mitigations. The cPP will not expect the product to defend against physical access to the firewall that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the firewall.
- The firewall is assumed to provide networking and filtering functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example the firewall should not provide computing platform for general purpose applications (unrelated to networking/filtering functionality).
- The authorized administrator(s) for the firewall 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 firewall. The firewall is not expected to be capable of defending against a malicious administrator that actively works to bypass or compromise the security of the firewall.
- The firewall 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 firewall are protected by the host platform on which they reside.
- It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE security policies will be enforced on all applicable network traffic flowing among the attached networks.

3.2 CLARIFICATION OF SCOPE

The scope of the evaluation is limited to secure management of the TOE and Stateful Traffic filtering functions. The TOE incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

The following features/functionality is excluded from this evaluation:

- Although SonicWall SonicOS Enhanced v6.2 supports several authentication mechanisms, the following mechanisms are excluded from the evaluated configuration:
    - 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

A separate evaluation of the TOE determined that this product satisfies the requirements of the collaborative Protection Profile for Stateful Traffic Filter Firewalls version 1.0 and the extended package for Virtual Private Gateway 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 V6.2.5.0-51n) executing on the following supported hardware platform(s);

NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
SM 9200	SM 9400	SM 9600	TZ 300/W	TZ 400/W
TZ 500/W	TZ 600	[redacted]		

With support from the operating environment for;

- Audit Server (rsyslog 8.24.0) with StrongSwan v4.3.2-1.1ubuntu1 IPsec VPN client

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. SonicOS 6.2 Administration Guide 232-002365-02 Rev D Updated - November 2017

h. SonicOS 6.2.5/6.2.7/6.2.9 Log Events Reference Guide P/N 232-004020-00 Rev A

i. Dell SonicWall SonicOS Enhanced V6.2 VPN Gateway on NSA, SM, and TZ Appliances Common Criteria Guidance Supplement Version: 1.2, 7 March 2018

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 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;

b. Cryptographic module/library verification: The evaluator verified the cryptographic certificates claimed are valid and present in the TOE.

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 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. 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
AD	Active Directory
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
DPD	Dead Peer Detection
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
LDAP	Lightweight Directory Access Protocol
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
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 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Security Target for SonicWall SonicOS Enhanced V6.2 VPN Gateway on NSA, SM, and TZ Appliances, v1.9P, 4 June 2018
Evaluation Technical Report for SonicWall SonicOS Enhanced V6.2 VPN Gateway on NSA, SM, and TZ Appliances, v0.9, 16 May 2018
Assurance Activity Report for SonicWall SonicOS Enhanced V6.2 VPN Gateway on NSA, SM, and TZ Appliances, v1.2, 17 May 2018