Certification Report

EAL 4+ Evaluation of SonicOS v5.0.1 on NSA Series and TZ Series Appliances

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number: 383-4-85-CR
Version: 1.0
Date: 16 May 2008
Pagination: i to iv, 1 to 12

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 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. 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 Standard 17025, General requirements for the accreditation of calibration and testing 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 located in Ottawa, Ontario.

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 16 May 2008, and the security target identified in Section 0 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at:
http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and
http://www.commoncriteriaportal.org/

TABLE OF CONTENTS

Disclaimer i

Foreword ii

Executive Summary 1

1 Identification of Target of Evaluation 2

2 TOE Description 2

3 Evaluated Security Functionality 3

4 Security Target 3

5 Common Criteria Conformance 4

6 Security Policy 4

7 Assumptions and Clarification of Scope 4

7.1 SECURE USAGE ASSUMPTIONS 4
7.2 ENVIRONMENTAL ASSUMPTIONS 5
7.3 CLARIFICATION OF SCOPE 5

8 Architectural Information 5

9 Evaluated Configuration 6

10 Documentation 6

11 Evaluation Analysis Activities 6

12 ITS Product Testing 7

12.1 ASSESSMENT OF DEVELOPER TESTS 8
12.2 INDEPENDENT FUNCTIONAL TESTING 8
12.3 INDEPENDENT PENETRATION TESTING 9
12.4 CONDUCT OF TESTING 9
12.5 TESTING RESULTS 9

13 Results of the Evaluation 9

14 Evaluator Comments, Observations and Recommendations 10

15 Acronyms, Abbreviations and Initializations 11

16 References 12

Executive Summary

The SonicOS v5.0.1 on NSA Series and TZ Series Appliances (hereafter referred to as the SonicOS v5.0.1), from SonicWALL, Inc., is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) EAL 4 Augmented evaluation.

The SonicOS v5.0.1 combines Unified Threat Management (UTM) protection, enterprise-class networking, and IPSec Virtual Private Networking, within a single management interface. These solutions include gateway anti-virus, anti-spyware, intrusion prevention, and when combined provide real-time, granular protection against a multitude of network and data attacks. By combining multiple technologies into one appliance, the SonicWALL solutions reduce deployment time, automate ongoing operation and increase the reliability of the client's network.

EWA-Canada is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 25 April 2008 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 the SonicOS v5.0.1, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the 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 EAL 4 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed: ALC_FLR.1 – Basic flaw remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the SonicOS v5.0.1 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

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is the SonicOS v5.0.1 on NSA Series and TZ Series Appliances (hereafter referred to as SonicOS v5.0.1), from SonicWALL, Inc.

2 TOE Description

The SonicOS v5.0.1 is custom software running on purpose built hardware appliances that combine to form a Unified Threat Management (UTM) device. UTMs are network firewalls that provide additional features such as anti-virus capabilities, anti-spyware, and intrusion prevention systems (IPS). The appliances provide firewall, UTM, Virtual Private Network (VPN), and traffic management capabilities that can be managed using an intuitive web-based Graphical User Interface (GUI) which facilitates deployment and management.

SonicOS v5.0.1's firewall capabilities include stateful packet inspection. Stateful packet inspection keeps track of 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 allowed to pass through the firewall; all others are rejected.

SonicOS's UTM capabilities include IPS, Gateway Anti Virus (GAV), and Gateway Anti-Spyware (SPY) and Application Firewall (AppFW). All UTM services employ stream-based analysis wherein traffic traversing the product is parsed and interpreted so that its content might be matched against sets of signatures to determine the acceptability of the traffic. The parsing and interpretation engines allow for the reliable handling of various protocols (such as Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), Post Office Protocol (POP), Internet Access Protocol (IMAP), as well as Generic TCP), encodings (Multipurpose Internet Mail Extensions (MIME), Base64, Unix-to-Unix Encode (UUEncode)), and types of compression (Compressed File (ZIP), Gnu Compressed File (GZIP), Lempel-Ziv Coding 1977 (LZ77)). In the event a certain flow of traffic is found to match an IPS/GAV/SPY signature meeting or exceeding the configured threshold, the event is logged, and the offending flow is terminated.

SonicOS supports VPN functionality, which provides a secure connection between two or more computers or protected networks over the public internet. It provides authentication to ensure that the information is going to and from the correct parties, and protects the information from viewing or tampering en route. SonicOS supports the creation and management of Internet Protocol Security (IPSec) VPNs. IPSec is a suite of protocols that operate on network traffic to secure Internet Protocol (IP) communications by authenticating and encrypting packets. Cryptographic key establishment is also possible through IPSec. For this, SonicOS supports Internet Key Exchange (IKE), which is the protocol used to set up a

security association (SA) in the IPSec protocol suite. SonicOS enables VPN policy creation to provide the configuration of multiple VPN tunnels. VPN policy definitions include the IP address of the remote gateway appliance with which the product will communicate, the IP address of the destination network, the type of encryption used for the policy, and other configuration information.

(Note: SonicOS 5.0.1 supports IKEv2, the next version of the Internet Key Exchange protocol)

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the SonicOS v5.0.1 is identified in Section 5 of the Security Target (ST).

The following Government of Canada approved algorithms were evaluated for correct implementation in the SonicOS v5.0.1:

Algorithm	**Standard**	**Certificate #**
Cryptographic module	FIPS 140-2	*Pending*
Random Number Generator (RNG)	FIPS 186-2	413, 414, 415, 416
Digital Signature Algorithm (DSA)	FIPS 186-2	266, 267, 268, 269, 270
Rivest Shamir Adleman (RSA)	FIPS 186-2	327, 327, 329, 330, 331
Advanced Encryption Standard (AES)	FIPS 197	701, 702, 703, 704, 705
Triple-DES (3DES)	FIPS 46-3	632, 633, 634, 635, 636
Secure Hash Algorithm (SHA-1)	FIPS 180-2	729, 730, 731, 732, 733
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	379, 380, 381, 382, 383

4 Security Target

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

Title: SonicWALL, Inc. SonicOS v5.0.1 on NSA Series and TZ Series Appliances
Version: 0.7
Date: 28 April 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*.

The SonicOS v5.0.1 is:

a. Common Criteria Part 2 extended, with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST;
   - FCS_FIPS.1,

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c. Common Criteria EAL 4 Augmented, containing all the security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.1 – Basic Flaw Remediation.

6 Security Policy

The SonicOS v5.0.1 implements a Traffic Information Flow Control Policy which controls the flow of data through the TOE from external entities, as well as a Diffie-Hellman Information Flow Control Policy to control the Diffie-Hellman public parameter for key exchange; details of these security policies can be found in Section 5 of the ST.

In addition, the SonicOS v5.0.1 implements other policies pertaining to security audit, user data protection, identification and authentication, TSF protection, TOE access, and security management. Further details on these security policies may be found in Sections 2 and 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the SonicOS v5.0.1 product 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 are the assumptions about the environment of use of the TOE:

a. Personnel authorized to install, configure, and operate the SonicOS v5.0.1 possess appropriate training and will adhere to the procedures for secure usage of the product described in the ST.

b. Personnel authorized to install, configure, and operate SonicOS v5.0.1 will adhere to all organizational policies including standards regarding secure usage of computer resources including physical, network, and password complexity policies.

c. The TOE Administrator will operate the TOE in *FIPS Enabled* mode and only on SonicWALL appliances that have been Federal Information Processing Standard (FIPS) 140-2 validated.

d. Authorized administrators will only access the TOE with a management console that is directly connected via crossover cable.

7.2 Environmental Assumptions

The following assumptions are made about the operating environment of the TOE:

a. The host machine upon which SonicOS v5.0.1 is installed resides in a physically secure location and only authorized individuals are granted physical access to the host.

b. Prior to audit storage exhaustion on the TOE, the audit records will be exported to an external server for persistent storage.

For more information about the TOE security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

While the TOE may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment.

The TOE is intended for use by non-hostile and well trained network administrators that have followed the installation and configuration guidance provided in;

- SonicOS Enhanced 5.0 Administrator's Guide
- SonicOS v5.0.1 on NSA Series and TZ Series Appliances Installation and Administrative Guidance Supplement.

8 Architectural Information

The SonicOS v5.0.1 is composed of firmware running on purpose built hardware that combine to form a UTM device which provide consolidated threat-management services such as network firewall, spam filtering, anti-virus, intrusion prevention systems, traffic management, and virtual private networking capabilities.

The TOE architecture comprises the following subsystems: Command and Configuration, Access Control, Network Traffic, Cryptography, Audit, and Hardware. Further details about the system architecture are proprietary to the vendor, and are not provided in this report.

9 Evaluated Configuration

The TOE is a software-only TOE consisting of SonicOS firmware version 5.0.1.0-11e for the TZ platforms and 5.0.1.0-6o for the NSA platforms. The purpose built FIPS 140-2 validated hardware appliance models are as follows: TZ180, TZ180W, TZ190, TZ190W, NSA 3500, NSA 4500, NSA 5000, NSA E5500, NSA E6500, and NSA E7500.

The SonicWALL appliance must be running in FIPS enable mode. This is specified in the SonicOS v5.0.1 on NSA and TZ Series Appliances Installation and Administrative Guidance Supplement.

10 Documentation

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

a. SonicWALL Getting Started Guide;

b. SonicOS Enhanced 5.0 Administrator's Guide; and

c. SonicOS v5.0.1 on NSA and TZ Series Appliances Installation and Administrative Guidance Supplement.

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of the SonicOS v5.0.1, including the following areas:

Configuration management: An analysis of the SonicOS v5.0.1 configuration management system and associated documentation was performed. The evaluators found that the SonicOS v5.0.1 configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the SonicOS v5.0.1 during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the SonicOS v5.0.1 functional specification, high-level design, low-level design, and a subset of the implementation representation; they determined that the documents were internally consistent, and

completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the SonicOS v5.0.1 user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the SonicOS v5.0.1 design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by SonicWALL, Inc. for the SonicOS v5.0.1. 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.

Vulnerability assessment: The SonicOS v5.0.1 STs strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the SonicOS v5.0.1 and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

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

12 ITS Product Testing

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

12.1 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[2].

SonicWALL, Inc. employs a rigorous testing process that tests the changes and fixes in each release of the SonicOS v5.0.1, a portion of this is fully automated. Comprehensive regression testing is conducted for a General Availability (GA) targeted release.

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

12.2 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 was the following list of EWA-Canada test goals:

a. Initialization: The objective of this test goal is to provide procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

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

c. Firewall: The objective of this test goal is to ensure that the network segregation, flow control, and protection requirements have been met with the firewall functionality;

d. Data Protection: The objective of this test goal is to determine the TOE's VPN capability for protecting its data;

e. Basic Product Functionality: The objective of this test goal is to exercise the TOE's functionality to ensure that the security claims may not be inadvertently compromised; and

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

f. Vulnerability Testing: The objective of this test goal is to perform penetration tests on the TOE, and to determine that the guidance is not misleading and facilitates the prevention and detection of insecure TOE states.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis, independent vulnerability analysis, and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

.

- Generic vulnerabilities;
- Bypassing;
- Tampering; and
- Direct attacks

The evaluator conducted a leakage verification test and found that no valuable information was disclosed during start-up and shutdown procedures. The evaluator used publicly available tools to scan the SonicOS v5.0.1 for generic vulnerabilities, and none were found. In addition, the evaluator performed direct attacks on the SonicOS v5.0.1, attempting to disrupt the services offered by the TOE. The independent penetration testing, and subsequent ad-hoc testing, did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

The SonicOS v5.0.1 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.

12.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that the SonicOS v5.0.1 behaves as specified in its ST and functional specification.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

The complete documentation for the SonicOS v5.0.1 includes a comprehensive Installation, Configuration and Security Guide.

The SonicWALL UTM Appliance is straightforward to configure, use and integrate into a corporate network. The Web GUI is intuitive and provides the administrator with a one stop tool for management.

SonicWALL Inc. Configuration Management (CM) and Quality Assurance (QA) provide the requisite controls for managing all CM/QA activities.

EWA-Canada performed a site visit to review the developer's processes, product life-cycle and site security, and to repeat a sample of the developer's tests. The evaluator found the company was well established and practising sound and documented processes in order to develop their products. SonicWALL, Inc. demonstrated a strong commitment to the Common Criteria evaluation and its completion.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
ACLs	Access Control Lists
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIAC	Computer Incident Advisory Capability
CPL	Certified Products list
CM	Configuration Management
CVE	Common Vulnerabilities and Exposures
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GA	General Availability
GAV	Gateway Anti-virus
IPS	Intrusion Prevention System
IKE	Internet Key Exchange
ITSET	Information Technology Security Evaluation and Testing
MIME	Multipurpose Internet Mail Extension
NIST	National Institute of Standards and Technology
OS	Operating System
PALCAN	Program for the Accreditation of Laboratories Canada
QA	Quality Assurance
SANS	SysAdmin, Audit, Network, Security
SFP	Security Function Policy
SNMP	Simple Network Management Protocol
SPY	Gateway Anti-Spyware

Acronym/Abbreviation/ Initialization	Description
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TSF	TOE Security Function
UDP	User Datagram Protocol
UTM	Unified Threat Management
VPN	Virtual Private Network

16 References

This section lists all documentation used as source material for this report:

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.

d. SonicWALL, Inc. SonicOS v5.0.1 on NSA Series and TZ Series Appliances, Security Target Revision No. 0.7, 28 April 2008.

e. Evaluation Technical Report (ETR) SonicOS v5.0.1 on NSA Series and TZ Series Appliances, EAL 4+ Evaluation, Common Criteria Evaluation Number: 383-4-85, Document No. 1564-000-D002, Version 1.3, 29 April 2008.