Swedish Certification Body for IT Security

Certification Report SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances

Issue: 1.0, 2014-jun-16

Authorisation: Dag Ströman, Head of CSEC , CSEC

Table of Contents

1 Executive Summary

The TOE is a unified threat management (UTM) device. UTMs are consolidated threat management devices that provide multiple security services, such as network firewall, spam filtering, anti-virus capabilities, intrusion prevention systems (IPS), and World Wide Web content filtering at the network level. SonicWALL appliances also provide Virtual Private Networking (VPN), and traffic management capabilities. Note that not all parts of a UTMs security services are part of the evaluation. For more details, see section 4.3 Clarification of Scope.

The TOE is the SonicOS Enhanced v5.9.0 build 118 on NSA Series and TZ Series Appliances. The TOE is delivered as one software part. Guidance documentation is also a part of the TOE as listed in chapter 6 Documentation.

No claims to Protection Profile conformance were made.

The TOE will protect its assets against two types of attackers:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess an enhanced basic skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network.

No Organisational Security Policies were defined. Ten assumptions on the operational environment were defined.

The evaluation has been performed by Combitech AB and EWA-Canada. The evaluation was completed on 2014-04-16. The evaluation was conducted in accordance with the requirements of Common Criteria, version 3.1R4, and the Common Methodology for IT Security Evaluation, version 3.1R4. The evaluation was performed at the evaluation assurance level EAL4, augmented by Flaw Remediation ALC_FLR.2.

Combitech AB is a licensed IT Security Evaluation Facility, ITSEF, within the scope of the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is accredited against ISO/IEC 17025 by the Swedish accreditation body, SWEDAC.

EWA-Canada operates as a Foreign location for Combitech AB within the scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifier audited the activities of the evaluator by reviewing all evaluation reports and by overseeing the evaluators performing site visit and testing. The certifier determined that the evaluation results showed that the product satisfied all functional and assurance requirements stated in the Security Target [ST]. The evaluator concluded that the common criteria requirements for evaluation assurance level EAL4 augmented by ALC_FLR.2 have been met.

The technical information included in this report has been compiled from the Security Target [ST] and from the final evaluation report produced by Combitech AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2013004
Name and version of the certified IT product	SonicWALL SonicOS Enhanced v5.9.0 build 118 on NSA Series and TZ Series Appliances.
Security Target Identification	Dell SonicWALL, Inc., SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances Security Target, document version 1.1
EAL	EAL4+, augmented with Flaw Remediation ALC_FLR.2
Sponsor	Dell SonicWALL, Inc.
Developer	Dell SonicWALL, Inc.
ITSEF	Combitech AB
Common Criteria version	Common Criteria version 3.1R4 [CCp1], [CCp2], [CCp3]
CEM version	Common Methodology for Information Technology Security Evaluation, version 3.1R4, [CEM],
National and international interpretations	-
Scheme version	QMS 1.16.1 QMS 1.16 2014-02-13 QMS 1.15 2013-10-23 The changes have had no impact on the certification.
Applicable Scheme Notes	-
Certification completion date	2014-06-16

3 Security Policy

The TOE provides the following security services:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TOE Security Function (TSF)
- TOE Access

3.1 Security Audit

The TOE generates audit records for startup and shutdown of the audit functions, blocked traffic, blocked websites, administrator account activity, VPN activity, firewall activity, firewall rule modification, network access, IPS/GAV/SPY activity, and login attempts. Administrators can view, search, sort and order the audit records based on priority, category, source IP or Interface, and destination IP or interface.

3.2 Cryptographic Support

The TOE provides IPSec VPN functionality for secure communications over the public internet. IKE protocol is used for exchanging authentication information and establishing the VPN tunnel. The TOE supports both version 1 and version 2 of IKE. The TOE is only installed and run on SonicWALL appliances that are validated to FIPS 140-2, all cryptographic operations are performed in accordance with FIPS 140-2, and all keys, algorithms, and key destruction meet the FIPS 140-2 standard. The cryptographic internals are not included in the evaluation and are part of the TOE's operational environment. The TOE uses the SonicOS Cryptography module's interface to request and receive cryptographic services.

3.3 User Data Protection

The TOE controls network traffic via the Traffic Information Flow Control Security Functional Policy (SFP). The Traffic Information Flow SFP relies on source and destination IP addresses, protocol type, port numbers, port types or subtypes, and rules defined in the Traffic Information Flow Control Lists to determine how to treat the network traffic. The rules define external IT entities that send traffic through the TOE as subjects and the traffic sent by these subjects as the information. These rules determine whether traffic should be passed through the TOE to its destination, be denied passage through the network, or be discarded. Keys and key parameters destined for the TOE are allowed and imported without security attributes associated.

VPN traffic follows the VPN Information Flow Control SFP. As traffic enters the TOE, the packet headers are checked to determine protocol type. If the packet header includes an IPsec header the traffic is allowed and decrypted. If the header does not include an IPsec header the Traffic Information Flow Control Policy SFP is enforced. The VPN Flow Control SFP defines subjects as users of the VPN tunnel and the information as the traffic these subjects send through the tunnel in encrypted form.

3.4 Identification and Authentication

Administrators are required to successfully identify and authenticate with the TOE prior to any actions on the TOE. Username, password, and role are stored in the TOE and are compared against the username and password entered by an administrator before assigning a role and allowing access.

3.5 Security Management

The TOE supports the roles of Full Administrator, Limited Administrator, and Read-Only Administrator. The Full and Limited Administrators have different permission based on if they are in configuration mode or not. When these administrators are in configuration mode they are called Config Mode Full Administrators and Config Mode Limited Administrators. The Config Mode Full Administrator role has the ability to modify and delete the restrictive default security attributes for the Traffic and Information Flow Control SFP. The TOE ensures that only secure values of the security attributes are accepted. The VPN Flow Control SFP security attributes have restrictive default values that cannot be changed.

3.6 Protection of the TSF

The TSF provides a reliable timestamp for operations in the TOE.

3.7 TOE Access

An administrator can configure the TOE to terminate management sessions after five to 60 minutes of inactivity. The default time for termination is 15 minutes.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security target [ST] makes two assumptions on the environment

- A.NOEVIL -Authorized administrators are non-hostile and follow all administrator guidance.
- A.REMACC -Authorized administrators may only access the TOE locally.

4.2 Environmental Assumptions

The Security target [ST] makes eight assumptions on the environment

- A.GENPUR -The TOE only stores and executes security-relevant applications and only stores data required for its secure operation.
- A.DIRECT -The TOE is available to authorized administrators only.
- A.PHYSEC -The TOE is physically secure.
- A.MODEXP -The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered moderate.
- A.PUBLIC -The TOE does not host public data.
- A.SINGEN -Information cannot flow among the internal and external networks unless it passes through the TOE.
- A.UPS -The TOE will be supported by an Uninterruptible Power Supply.
- A.FIPS -The TOE will only be installed and run on SonicWALL appliances that have been evaluated under FIPS 140-2 with the same version of the TOE.

4.3 Clarification of Scope

Features/Functionality that are not part of the evaluated configuration of the TOE are:

- Command Line Interface (CLI) (Secure Shell, or SSH)
- Remote management and login (Remote Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), Active Directory, eDirectory authentication)
- NTP Server
- Application Firewall
- Web Content Filtering
- Hardware Failover
- Real-time Blacklist (Simple Mail Transfer Protocol (SMTP))
- Global Security Client (including GroupVPN)
- Global Management System (GMS)
- SonicPoint
- VoIP

The Security Target [ST] contains nine threats, which have been considered during the evaluation:

- T.ASPOOF An unauthorized entity may carry out spoofing in which information flows through the TOE into a connected network by using a spoofed source address.
- T.AUDACC Persons may not be accountable for the actions that they conduct, thus allowing an attacker to escape detection.
- T.NOAUTH An unauthorized user may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE.
- T.SELPRO An unauthorized user may read, modify, or destroy security critical TOE configuration data stored on the TOE.
- T.REPEAT An unauthorized person may repeatedly try to guess authentication data used for performing I&A functionality in order to use this information to launch attacks on the TOE.
- T.MEDIAT An unauthorized person may send impermissible information through the TOE which results in the exploitation of resources on the internal network.
- T.AUDFUL An unauthorized user may cause audit records to be lost or prevent future records from being recorded by taking actions to exhaust audit storage capacity, thus masking an attacker's actions.
- T.NACCESS An unauthorized person or external IT entity may be able to view data that is transmitted between the TOE and a remote authorized external IT entity.
- T.NMODIFY An unauthorized person or external IT entity may modify data that is transmitted between the TOE and a remote authorized external entity.

5 Architectural Information

5.1 TOE Design

The TOE consists of software only and is divided in the following subsystems, TSFIs, and modules.

Subsystem	TSFI	Modules
Command and Configuration	Management Traffic Interface	User Interface Module
		Parameter Table Module
Access Control	-	IP Table Module
Network Traffic	Network Traffic In Network Traffic Out	Protocol Interpreting Module
		Traffic Inspection Module
		Connection Cache Module
		NAT module
Cryptographic	Cryptographic Module Interface	Cryptographic Engine Module
Audit	-	Audit Buffer Module
Hardware	Hardware API	Hardware Module

Table 1, TOE design

The TOE is a UTM which runs on the SonicWALL NSA series and TZ series hardware appliances listed in chapter 8 *Evaluated Configuration*. The TOE is installed on a network wherever firewall/UTM/VPN services are required, as depicted in the figure below. The essential physical component for the proper operation of the TOE in the evaluated configuration is

- SonicOS Enhanced

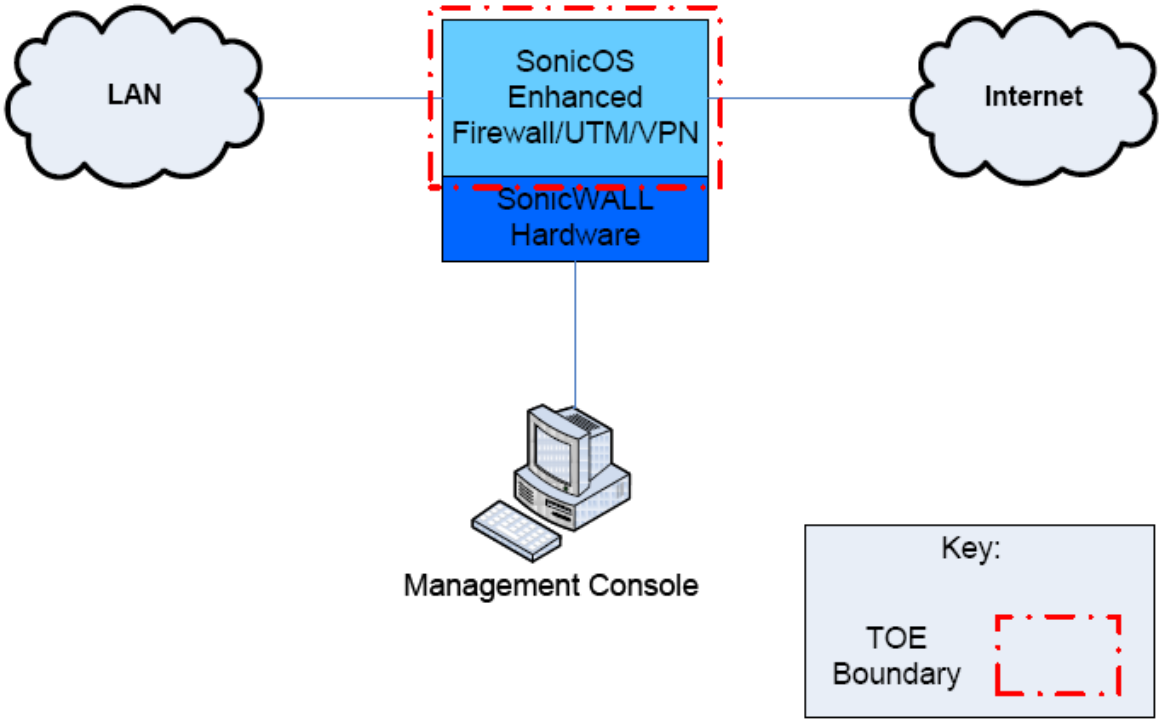

Figure 1, Physical TOE Boundary

6 Documentation

The following guides are required reading and part of the TOE:

- Dell SonicWALL SonicOS 5.9 Administrator's Guide, Rev E, 232-002229-00
- Dell SonicWALL SonicOS 5.9.0.4 Release Notes, Rev B, 232-002328-00
- Dell SonicWALL SonicOS 5.9 Log Event Reference Guide, Rev A, 232-002230-00
- Dell SonicWALL SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances Guidance Documentation Supplement, Version 0.2, March 27, 2014
- One of the following, based on the appliance used:
  - Dell SonicWALL NSA 220 Quick Start Poster, Rev A, 232-002003-50
  - Dell SonicWALL NSA 240 Getting Started Guide, Rev A, 232-001580
  - Dell SonicWALL NSA 250M or 250 MW Quick Start Poster, Rev A, 232-001924-51
  - Dell SonicWALL NSA 2400 Getting Started Guide, Rev A, 232-001276-50
  - Dell SonicWALL NSA 2400MX Getting Started Guide, Rev A, 232-001475-51
  - Dell SonicWALL NSA 5000/4500/3500 Getting Started Guide, Rev A, 232-001265-50
  - Dell SonicWALL NSA E5500 Getting Started Guide, Rev A, 232-001052-55
  - Dell SonicWALL NSA E6500 Getting Started Guide, Rev A, 232-001051-52
  - Dell SonicWALL NSA E7500 Getting Started Guide, Rev A, 232-001050-55
  - Dell SonicWALL NSA E8500 Getting Started Guide, Rev A, 232-001891-53
  - Dell SonicWALL NSA E8510 Getting Started Guide, Rev A, 232-001858-50
  - Dell SonicWALL TZ 105 Quick Start Poster, Rev A, 232-002038-50
  - Dell SonicWALL TZ 205 Quick Start Poster, Rev A, 232-002114-51
  - Dell SonicWALL TZ 215 Quick Start Poster, Rev A, 232-002037-51
  - Dell SonicWALL SuperMassive Series Datasheet, DS 0465L, 05/13

The NSA E10200, E10400, and E10800 are installed by SonicWALL professional services and therefore do not have an associated Getting Started Guide or Poster.

7 IT Product Testing

7.1 Developer Tests

The developer's testing covered all TSFIs and the security functional behaviour. The interaction between subsystems and the interfaces of the SFR-enforcing modules have been tested.

7.2 Independent Evaluator Tests

The evaluator repeated approximately 20% of the Developer's tests representing tests of different TSFIs and security functionality.

The evaluator conducted and executed 14 additional test cases to cover the TOE security functionality behaviour both in a firewall and a VPN deployment. The TSFIs were excited by consoles used for management and user traffic and the TOE behavior was observed at the consoles or at tools such as a packet sniffer (Wireshark).

One test case was run on a NSA 220 appliance; all other tests were run on NSA E8500 appliances.

The TOE was configured for L2 Bridge Mode in one test case. All other test cases were performed in Central-site Gateway Mode.

The evaluator tests were mainly performed at the developer site and under oversight by the certifier. Complementary testing took also place at Combitech's site in Sundbyberg.

7.3 Penetration Tests

Three types of penetration tests were executed:

- Port scanning
- Fuzzing
- Vulnerability scanning

The firewall WAN interface, facing an unprotected network, was scanned for open ports and available services after initial installation and configuration. The tool Nmap (www.nmap.org) was used configured for TCP Connect, TCP SYN, UDP, and IP scanning.

To verify the stability of the LAN interface, the HTTPS identification and authentication methods were fuzzed using various different inputs. The tool WebScarab (www.owasp.org) was used.

To reveal possible vulnerabilities both WAN and LAN interfaces listening to HTTP/HTTPS traffic were scanned using the Nessus (www.tenable.com) vulnerability scanner.

For the penetration test cases the NSA E8500 appliances were used and configured in Central-site Gateway Mode.

None of the penetration tests revealed any vulnerabilities.

8 Evaluated Configuration

The TOE is dependent on a cryptographic module that is outside the TOE scope, and therefore its internals are not covered by this evaluation. The cryptographic module is under FIPS 140-2 validation by NIST and CSE.

The TOE is also dependent on a hardware appliance for its operation.The following models of hardware appliances are supported: 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 E10400, NSA E10800, and NSA E10200.

A general purpose computer is required as Management Console. The Management Console should be equipped with a Web browser for HTTPS management sessions:

- Chrome 4.0 or higher (recommended browser);
- Mozilla Firefox 3.0 or higher; or
- Internet Explorer 8.0 or higher.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potenitial of Enhanced-Basic.

The certifier reviewed the work of the evaluator to determine that the evaluation was conducted in accordance with the requirements of the Common Criteria [CC].

The evaluators overall verdict of the evaluation is: PASS

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Security Target Evaluation	ASE	Pass
ST Introduction	ASE_INT.1	Pass
Conformance claims	ASE_CCL.1	Pass
Security problem definition	ASE_SPD.1	Pass
Security objectives	ASE_OBJ.2	Pass
Extended components definition	ASE_ECD.1	Pass
Derived security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Life-cycle support	ALC	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Flaw remediation	ALC_FLR.2	Pass
Development	ADV	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	AGD	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Tests	ATE	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	AVA	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

10 Evaluator Comments and Recommendations

The evaluators have no remaining comments, observations, or recommendations.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within an evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications, used as the basis of a TOE evaluation
TOE	Target of Evaluation
CC	Common Criteria
CSE	Communications Security Establishment Canada
FIPS	Federal Information Processing Standard
IKE	Internet Key Exchange
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
SFP	Security Function Policy
SFR	Security Functional Requirements
TSF	TOE Security Functionality

12 Bibliography

[ST] Dell SonicWALL, Inc., SonicOS Enhanced v5.9.0 on NSA Series and TZ Series Appliances Security Target, document version 1.1, February 28, 2014

[CCp1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version 3.1, revision 4, September 2012, CCMB-2012-09-001

[CCp2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version 3.1, revision 4, September 2012, CCMB-2012-09-002

[CCp3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, version 3.1, revision 4, September 2012, CCMB-2012-09-003

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, version 3.1, revision 4, September 2012, CCMB-2012-09-004

[SP-002] Evaluation and Certification, SP-002, Issue: 20.0, 2013-09-30, 13FMV7990-2:1, FMV/CSEC