National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances

Report Number:	**CCEVS-VR-11028-2020-FW**
Dated:	**April 16, 2020**
Version:	**1.0**

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Validation Team

James Donndelinger

Marybeth Panock

Harry Beddo

Lian Bloch

George Odom

Common Criteria Testing Laboratory

Natasha Mathias

Varsha Shetye

Kenji Yoshino

Acumen Security, LLC

Table of Contents

1 Executive Summary 4

2 Identification 5

3 Architectural Information 6

4 Security Policy 7

5 Assumptions, Threats & Clarification of Scope 10

5.1 Assumptions 10

5.2 Threats 11

5.3 Clarification of Scope 12

6 Documentation 14

7 TOE Evaluated Configuration 15

7.1 Evaluated Configuration 15

8 IT Product Testing 16

8.1 Developer Testing 16

8.2 Evaluation Team Independent Testing 16

9 Results of the Evaluation 17

9.1 Evaluation of Security Target 17

9.2 Evaluation of Development Documentation 17

9.3 Evaluation of Guidance Documents 17

9.4 Evaluation of Life Cycle Support Activities 18

9.5 Evaluation of Test Documentation and the Test Activity 18

9.6 Vulnerability Assessment Activity 18

9.7 Summary of Evaluation Results 19

10 Validator Comments & Recommendations 20

11 Annexes 20

12 Security Target 22

13 Glossary 23

14 Bibliography 24

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Target of Evaluation (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in March 2020. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018.

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (CEM), Version 3.1, Rev. 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1, Rev. 4, as interpreted by the Assurance Activities contained in the collaborative Protection Profile for Stateful Traffic Filter Firewalls, Version 2.0+Errata 20180314, dated 14 March 2018. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliance List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances
Protection Profile	• Collaborative Protection Profile for Stateful Traffic Filter Firewalls (v2.0+Errata 20180314, 14-March-2018) [FWcPP]
Security Target	SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Security Target
Evaluation Technical Report	Evaluation Technical Report for SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO
CC Version	Version 3.1, Revision 4
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	SonicWALL, Inc.
Developer	SonicWALL, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security, LLC
CCEVS Validators	James Donndelinger, Marybeth Panock, Harry Beddo, Lian Bloch, George Odom

3 Architectural Information

The TOE is comprised of the SonicWall SonicOS Enhanced v6.5.4 software running either on purpose built TZ and SOHO hardware appliance platforms.

The appliance firewall capabilities 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.

The appliance capabilities include deep-packet inspection (DPI) used for intrusion prevention and detection. These services employ stream-based analysis wherein traffic traversing the product is parsed and interpreted so that its content might be matched against a set of signatures to determine the acceptability of the traffic. Only traffic adhering to the administrator-configured policies is permitted to pass through the TOE.

The appliances support Virtual Private Network (VPN) functionality, which provides a secure connection between the device and the audit server. The appliances support authentication and protect data from disclosure or modification during transfer.

The appliances are managed through a web based Graphical User Interface (GUI). All management activities may be performed through the web management GUI via a hierarchy of menu buttons. Administrators may configure policies and manage network traffic, users, and system logs. The appliances also have local console access where limited administrative functionality to configure the network, perform system updates, and view logs.

4 Security Policy

The TOE implements the following security functional requirements:

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

Each of these security functionalities are listed in more detail below.

Security Audit

The TOE generates audit records for administrative activity, security related configuration changes, cryptographic key changes and startup and shutdown of the audit functions. The audit events are associated with the administrator who performs them, if applicable. The audit records are transmitted over an IPsec VPN tunnel to an external audit server in the IT environment for storage.

Cryptographic Support

The TOE provides cryptographic functions (key generation, key establishment, key destruction, cryptographic operation) to secure remote administrative sessions over Hypertext Transfer Protocol Secure (HTTPS)/Transport Layer Security (TLS), and to support Internet Protocol Security (IPsec) to provide VPN functionality and to protect the connection to the audit server.

Algorithm	Description	Mode Supported	CAVP Cert. #
AES	Used for symmetric encryption/decryption FCS_TLSS_EXT.1 FCS_IPSEC_EXT.1 FCS_COP.1/DataEncryption	CBC (128, 256) GCM (128, 256)	C743
SHS	Cryptographic hashing services FCS_TLSS_EXT.1 FCS_IPSEC_EXT.1 FCS_RBG_EXT.1 FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash	SHA (1, 256, 384, 512)	C743
DRBG	Deterministic random bit generation FCS_TLSS_EXT.1 FCS_IPSEC_EXT.1 FCS_RBG_EXT.1 FCS_CKM.1	Hash (SHA-256)	C743

Algorithm	Description	Mode Supported	CAVP Cert. #
ECDSA (186)	Key Generation, SigGen, SigVer FCS_IPSEC_EXT.1 FCS_CKM.1 FCS_COP.1/SigGen FPT_TUD_EXT.1	P-256, P-384	C743
RSA (186)	Key Generation FCS_TLSS_EXT.1 FCS_IPSEC_EXT.1 FCS_CKM.1	n (2048)	C743
	SigGen (PKCS1_V1.5) FCS_TLSS_EXT.1 FCS_IPSEC_EXT.1 FCS_COP.1/SigGen	n = 2048 SHA(256, 384, 512)	C743
	SigVer (PKCS1_v1.5) FCS_TLSS_EXT.1 FCS_IPSEC_EXT.1 FCS_COP.1/SigGen	n = 2048 SHA(1, 256, 384, 512)	C743
HMAC	Keyed hashing services FCS_TLSS_EXT.1 FCS_IPSEC_EXT.1 FCS_COP.1/KeyedHash	SHA (1, 256, 384, 512)	C743
KAS ECC	SP 800-56A FCS_IPSEC_EXT.1 FCS_CKM.2	Key Agreement (Initiator, Responder) EC: P-256, SHA-512 ED: P-384, SHA-512	C743
RSA	PKCS1_v1.5 FCS_TLSS_EXT.1 FCS_CKM.2	RSA Key Establishment	Vendor Affirmed

Table 2 CAVP Certificate References

Identification and Authentication

The TOE provides a password-based logon mechanism. This mechanism enforces minimum strength requirements and ensures that passwords are obscured when entered. The TOE also validates and authenticates X.509 certificates for all certificate use.

Security Management

The TOE provides management capabilities via a Web-based GUI, accessed over HTTPS. Management functions allow the administrators to configure and update the system, manage users and configure the Virtual Private Network (VPN).

Protection of the TSF

The TOE prevents the reading of plaintext passwords and keys. The TOE provides a reliable timestamp for its own use. To protect the integrity of its security functions, the TOE implements a suite of self-tests at startup and shuts down if a critical failure occurs. The TOE verifies the software image when it is loaded. The TOE ensures that updates to the TOE software can be verified using a digital signature.

TOE Access

The TOE monitors local and remote administrative sessions for inactivity and either locks or terminates the session when a threshold time period is reached. An advisory notice is displayed at the start of each session.

Trusted Path/Channels

The TSF provides IPsec VPN tunnels for trusted communication between itself and an audit server. The TOE implements HTTPS for protection of communications between itself and the Management Console.

Stateful Traffic Filtering

The TOE restricts the flow of network traffic between protected networks and other attached networks based on addresses and ports of the network nodes originating (source) and/or receiving (destination) applicable network traffic, as well as on established connection information.

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

ID	Assumption
A.PHYSICAL_PROTECTION	The firewall 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 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.
A.LIMITED_FUNCTIONALITY	The firewall 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 firewall device should not provide a computing platform for general purpose applications (unrelated to networking/filtering functionality).
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the firewall 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 firewall. The firewall device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The firewall 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.
A.ADMIN_CREDENTIALS_SECURE	The Administrator's credentials (private key) used to access the firewall device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on firewall equipment when the equipment is discarded or removed from its operational environment.

Table 1 Assumptions

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

ID	Threat
T.UNAUTHORIZED_ ADMINISTRATOR_ACCESS	Threat agents may attempt to gain administrator access to the firewall by nefarious means such as masquerading as an administrator to the firewall, masquerading as the firewall to an administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between the firewall and a network device. Successfully gaining administrator access allows malicious actions that compromise the security functionality of the firewall and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_ COMMUNICATION_CHANNELS	Threat agents may attempt to target firewalls that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the firewall itself.
T.WEAK_AUTHENTICATION _ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints – e.g. a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the firewall itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the firewall without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.

ID	Threat
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and firewall data enabling continued access to the firewall and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or firewall credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the firewall. Having privileged access to the firewall provides the attacker unfettered access to the network traffic, and may allow them to take advantage of any trust relationships with other network devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.
T.NETWORK_DISCLOSURE	An attacker may attempt to "map" a subnet to determine the machines that reside on the network, and obtaining the IP addresses of machines, as well as the services (ports) those machines are offering. This information could be used to mount attacks to those machines via the services that are exported.
T. NETWORK_ACCESS	With knowledge of the services that are exported by machines on a subnet, an attacker may attempt to exploit those services by mounting attacks against those services.
T.NETWORK_MISUSE	An attacker may attempt to use services that are exported by machines in a way that is unintended by a site's security policies. For example, an attacker might be able to use a service to "anonymize" the attacker's machine as they mount attacks against others.
T.MALICIOUS_TRAFFIC	An attacker may attempt to send malformed packets to a machine in hopes of causing the network stack or services listening on UDP/TCP ports of the target machine to crash.

Table 2 Threats

5.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the (FWcPP).
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not "obvious" or vulnerabilities to objectives not claimed in the ST. The CEM defines an "obvious" vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PP. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality listed in Section 7.2 of this document is not covered.

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

- SonicWall® SonicOS 6.5 Common Criteria Addendum, Version 1.4

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The TOE is a software and hardware TOE. It is a combination of a particular SOHO or TZ hardware appliance and the SonicOS v6.5.4.4-44n--federal-12n software that is configured in accordance with the Common Criteria Addendum described in Section 6. The following table lists all the instances of the TOE that operate in the evaluated configuration. All listed TOE instances offer the same core functionality but vary in number of processors, physical size, and supported connections.

Appliance Series	Hardware Model	Operational Environment
TZ	TZ 300P	Cavium Octeon III CN7020-800
	TZ 350W	Cavium Octeon III CN7020-800
	TZ 600P	Cavium Octeon III CN7130-1400
SOHO	SOHO 250	Cavium Octeon III CN7020-800
	SOHO 250W	Cavium Octeon III CN7020-800

Table 5 TOE Appliance Series and Models

The underlying platform that comprises the TOE has common hardware characteristics. These differing characteristics effect only non-TSF relevant functionality, such as throughput, processing speed, number and type of connections, and amount of internal storage.

In the evaluated configuration, the devices are placed in “Network Device Protection Profile (NDPP)” mode. “NDPP mode” is a configuration setting.

The SonicWall appliances are designed to filter traffic based on a set of rules created by a system administrator. The audit server provides a platform for sorting and viewing the log files that are produced by the appliance.

7.2 Excluded Functionality

The following features/functionality are excluded from this evaluation:

- Although SonicWall SonicOS Enhanced 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))
- 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
- Application Firewall

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances, which is not publicly available. The Assurance Activities Report provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the (FWcPP). The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here. A description of the test configurations and the test tools may be found in Section 4 of that report.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances TOE to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the (FWcPP).

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the (FWcPP).

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the (FWcPP) related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the (FWcPP) related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team ran the set of tests specified by the Assurance Activities in the (FWcPP) and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the (FWcPP), and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team performed a public search for vulnerabilities between February 20 and 25, 2020, and again on April 14, 2020 and did not discover any issues with the TOE. The evaluators searched for publicly available information at nvd.nist.gov and www.cvedetails.com. The following search terms were used:

- SonicWall SonicOS Enhanced v6.5.4
- SonicWall
- TZ 300P
- TZ 350W
- TZ 600P
- SOHO 250
- SOHO 250W
- SOHO
- TZ
- TLS 1.1
- TLS 1.2
- IPSEC
- HTTPS
- Firewall
- TCP
- UDP
- IPv4
- IPv6
- ICMPv4
- ICMPv6

- VPNGW
- VPN
- IPS
- Cavium Octeon III CN7020-800
- Cavium Octeon III CN7130-1400
- Cavium Octeon

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the (FWcPP), and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the (FWcPP), and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

Administrators are cautioned to pay attention to the configurable options as there are services, protocols and capabilities that are not to be enabled in the evaluated configuration. See the list in section 7.2 in this document. For example, RADIUS, LDAP, Active Directory, NTP are not to be used in the evaluated configuration.

The only approved software for use in the evaluated configuration is: SonicOS v6.5.4.4-44n--federal-12n software; no versions, either earlier or later, were evaluated.

Note that while the overview sections in this VR and in the ST discuss VPN and IPS capabilities, no VPN or IPS capabilities are being claimed.

All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable.

12 Security Target

SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Security Target, v1.9

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 4.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 4.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 4.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4.
5. Collaborative Protection Profile for Stateful Traffic Filter Firewalls (v2.0+Errata 20180314, 14-March-2018) [FWcPP]
6. Assurance Activity Report for SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Version 1.4 April 14, 2020
7. SonicWall® SonicOS 6.5 Common Criteria Addendum version 1.4 April 2020
8. Vulnerability Assessment for SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Version 1.4 April 14, 2020
9. Evaluation Technical Report for SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Version 1.4, April 14, 2020
10. SonicWall SonicOS Enhanced V6.5.4 with VPN and IPS on TZ and SOHO Appliances Security Target (FW-VPNGW-IPS) Version 1.9 April 2020