

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

for the

**Sonicwall SonicOS/X v7.0.1 with VPN and IPS on TZ, NSa,
NSsp, and NSv Appliances**

Report Number: CCEVS-VR-VID11473-2025

Dated: 01/08/2025

Version: 1.0

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

**Department of Defense
ATTN: NIAP, SUITE: 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982**

ACKNOWLEDGEMENTS

Validation Team

Jerome Myers

Swapna Katikaneni

DeRon Graves

The Aerospace Corporation.

Common Criteria Testing Laboratory

Shehan Dissanayake

Rupal Gupta

Reema Nagwekar

Yogita Kore

Halil Tosunoglu

Acumen Security, LLC

Table of Contents

1	Executive Summary	4
2	Identification	5
3	Architectural Information	7
4	Security Policy	8
5	Assumptions, Threats & Clarification of Scope	10
5.1	Assumptions	10
5.2	Threats	12
5.3	Clarification of Scope	17
6	Documentation	19
7	TOE Evaluated Configuration	20
7.1	Evaluated Configuration	20
7.1.1	Physical Boundaries and IT Testing Environment Components	20
7.1.2	Security Functions Provided by the TOE.....	20
7.2	Excluded Functionality	20
8	IT Product Testing	22
8.1	Developer Testing	22
8.2	Evaluation Team Independent Testing	22
9	Results of the Evaluation	23
9.1	Evaluation of Security Target	23
9.2	Evaluation of Development Documentation	23
9.3	Evaluation of Guidance Documents	23
9.4	Evaluation of Life Cycle Support Activities	24
9.5	Evaluation of Test Documentation and the Test Activity	24
9.6	Vulnerability Assessment Activity	24
9.7	Summary of Evaluation Results	24
10	Validator Comments & Recommendations	25
11	Annexes	26
12	Security Target	27
13	Glossary	28
14	Bibliography	29

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/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances** Series 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 January 2025. 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 of the list of PP-Configuration/PP/PP-Modules below:

(NDcPP + IPS MOD + FW +VPNGW) PP-Configuration for Network Device, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.2

This PP-Configuration includes the following:

- Collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
- PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E)
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_1.3)

The TOE identified in this VR has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the Protection Profile (PP). This VR 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 ETR 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 of the functional requirements and assurance requirements stated in the 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 ETR are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) 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 PPs containing Assurance Activities, which are interpretations of Common Evaluation Methodology (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 IT products are 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 Compliant 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/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances
Protection Profile	<p>(NDcPP + IPS MOD + FW +VPNGW) PP-Configuration for Network Device, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.2</p> <p>This PP-Configuration includes the following:</p> <ul style="list-style-type: none"> ○ Collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E) ○ PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0) ○ PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E) ○ PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_1.3)
Security Target	Sonicwall SonicOS/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances Security Target, version 1.2
Evaluation Technical Report	Evaluation Technical Report for Sonicwall SonicOS/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances, version 1.1
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Sonicwall, Inc.

Item	Identifier
Developer	Sonicwall, Inc.
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Jerome Myers Swapna Katikaneni DeRon Graves

3 Architectural Information

The TOE is comprised of the SonicWall SonicOS/X v7.0.1 software running either on purpose built TZ, NSa, NSsp, series hardware appliance platforms and NSv virtual appliances running on purpose built ESXi hardware appliances.

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 provides the security functions required by the Collaborative Protection Profile for Network Devices, hereafter referred to as NDcPP v2.2e or NDcPP, collaborative Protection Profile Module for Stateful Traffic Filter Firewall, hereafter referred to as MOD_FW v1.4e or MOD_FW, PP-Module for VPN Gateways Version 1.3 hereafter referred to as MOD_VPNGW v1.3 or MOD_VPNGW, PP-Module for Intrusion Protection Systems (IPS) Version 1.0, hereafter referred to as MOD_IPS v1.0 or MOD_IPS.

4.1.1.1 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.

4.1.1.2 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.

4.1.1.3 Residual Data Protection

The TOE ensures that data cannot be recovered once deallocated.

4.1.1.4 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.

4.1.1.5 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) and Intrusion Prevention System (IPS) functionality.

4.1.1.6 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.

4.1.1.7 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.

4.1.1.8 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.

4.1.1.9 Intrusion Prevention

The TOE performs analysis of IP-based network traffic and detects violations of administratively defined IPS policies. The TOE inspects each packet header and payload for anomalies and known signature-based attacks and determines whether to allow traffic to traverse the TOE.

4.1.1.10 Stateful Traffic Filtering and Packet 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.

The TOE performs packet filtering on network packets.

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.

Assumptions (CPP_ND)

ID	Assumption
A.PHYSICAL_PROTECTION	<p>The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device’s physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.</p>
A.LIMITED_FUNCTIONALITY	<p>The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).</p> <p>If a virtual TOE evaluated as a pND, following Case 2 vNDs as specified in Section 1.2, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of a distributed TOE run inside more than one virtual machine (VM) on a single VS. In Case 2 vND, no non-TOE guest VMs are allowed on the platform.</p>
A.NO_THRU_TRAFFIC_PROTECTION	<p>A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).</p>

ID	Assumption
A.TRUSTED_ADMINISTRATOR	<p>The Security Administrator(s) for the Network Device are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The Network Device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.</p> <p>(The paragraph that follows is for x509v3 cert-based authentication. If not relevant, remove)</p> <p>For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', 'trusted CA Key Store', or similar) as a trust anchor prior to use (e.g. offline verification).</p>
A.REGULAR_UPDATES	<p>The Network Device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.</p>
A.ADMIN_CREDENTIALS_SECURE	<p>The Administrator's credentials (private key) used to access the Network Device are protected by the platform on which they reside.</p>
A.RESIDUAL_INFORMATION	<p>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 networking equipment when the equipment is discarded or removed from its operational environment.</p>
A.VS_TRUSTED_ADMINISTRATOR (applies to vNDs only)	<p>The Security Administrators for the VS are assumed to be trusted and to act in the best interest of security for the organization. This includes not interfering with the correct operation of the device. The Network Device is not expected to be capable of defending against a malicious VS Administrator that actively works to bypass or compromise the security of the device.</p>
A.VS_REGULAR_UPDATES (applies to vNDs only)	<p>The VS software is assumed to be updated by the VS Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.</p>

ID	Assumption
A.VS_ISOLATION (applies to vNDs only)	For vNDs, it is assumed that the VS provides, and is configured to provide sufficient isolation between software running in VMs on the same physical platform. Furthermore, it is assumed that the VS adequately protects itself from software running inside VMs on the same physical platform.
A.VS_CORRECT_CONFIGURATION (applies to vNDs only)	For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

Assumptions (MOD_VPNGW)

ID	Assumption
A.CONNECTIONS	This assumption defines the TOE’s placement in a network such that it is able to perform its required security functionality. The Base-PP does not define any assumptions about the TOE’s architectural deployment so there is no conflict here.

Assumptions (MOD_IPS)

ID	Assumption
A.CONNECTIONS	It is assumed that the TOE is connected to distinct networks in a manner that ensures that the TOE's security policies will be enforced on all applicable network traffic flowing among the attached networks.

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.

Threats (CPP_ND)

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the Network Device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device 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 Network Devices. Successfully gaining Administrator access allows malicious

ID	Threat
	actions that compromise the security functionality of the device 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 Network Devices that do not use standardized secure tunnelling 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 Network Device 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 Network Device 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 Network Device 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.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the Network Device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining

ID	Threat
	the Administrator or device 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 device. Having privileged access to the device 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.

Threats (MOD_CPP_FW)

ID	Threat
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.

Threats (MOD_VPNGW)

ID	Threat
T.DATA_INTEGRITY	Devices on a protected network may be exposed to threats presented by devices located outside the protected network that may attempt to modify the data without authorization. If known malicious external

ID	Threat
	<p>devices are able to communicate with devices on the protected network or if devices on the protected network can communicate with those external devices then the data contained in the communications may be susceptible to a loss of integrity.</p>
T.NETWORK_ACCESS	<p>Devices located outside the protected network may seek to exercise services located on the protected network that are intended to only be accessed from inside the protected network or only accessed by entities using an authenticated path into the protected network. Devices located outside the protected network may, likewise, offer services that are inappropriate for access from within the protected network.</p> <p>From an ingress perspective, VPN gateways can be configured so that only those network servers intended for external consumption by entities operating on a trusted network (e.g., machines operating on a network where the peer VPN gateways are supporting the connection) are accessible and only via the intended ports. This serves to mitigate the potential for network entities outside a protected network to access network servers or services intended only for consumption or access inside a protected network.</p> <p>From an egress perspective, VPN gateways can be configured so that only specific external services (e.g., based on destination port) can be accessed from within a protected network, or moreover are accessed via an encrypted channel. For example, access to external mail services can be blocked to enforce corporate policies against accessing uncontrolled email servers, or, that access to the mail server must be done over an encrypted link.</p>
T.NETWORK_DISCLOSURE	<p>Devices on a protected network may be exposed to threats presented by devices located outside the protected network, which may attempt to conduct unauthorized activities. If known malicious external devices are able to communicate with devices on the protected network, or if devices on the protected network can establish communications with those external devices (e.g., as a result of a phishing episode or by inadvertent responses to email messages), then those internal devices may be susceptible to the unauthorized disclosure of information.</p> <p>From an infiltration perspective, VPN gateways serve not only to limit access to only specific destination network addresses and ports within a protected network, but whether network traffic will be encrypted or transmitted in plaintext. With these limits, general network port scanning can be prevented from reaching protected networks or machines, and access to information on a protected network can be limited to that obtainable from specifically</p>

ID	Threat
	<p>configured ports on identified network nodes (e.g., web pages from a designated corporate web server). Additionally, access can be limited to only specific source addresses and ports so that specific networks or network nodes can be blocked from accessing a protected network thereby further limiting the potential disclosure of information.</p> <p>From an exfiltration perspective, VPN gateways serve to limit how network nodes operating on a protected network can connect to and communicate with other networks limiting how and where they can disseminate information. Specific external networks can be blocked altogether or egress could be limited to specific addresses or ports. Alternately, egress options available to network nodes on a protected network can be carefully managed in order to, for example, ensure that outgoing connections are encrypted to further mitigate inappropriate disclosure of data through packet sniffing.</p>
T.NETWORK_MISUSE	<p>Devices located outside the protected network, while permitted to access particular public services offered inside the protected network, may attempt to conduct inappropriate activities while communicating with those allowed public services. Certain services offered from within a protected network may also represent a risk when accessed from outside the protected network.</p> <p>From an ingress perspective, it is generally assumed that entities operating on external networks are not bound by the use policies for a given protected network. Nonetheless, VPN gateways can log policy violations that might indicate violation of publicized usage statements for publicly available services. From an egress perspective, VPN gateways can be configured to help enforce and monitor protected network use policies. As explained in the other threats, a VPN gateway can serve to limit dissemination of data, access to external servers, and even disruption of services – all of these could be related to the use policies of a protected network and as such are subject in some regards to enforcement. Additionally, VPN gateways can be configured to log network usages that cross between protected and external networks and as a result can serve to identify potential usage policy violations.</p>
T.REPLAY_ATTACK	<p>If an unauthorized individual successfully gains access to the system, the adversary may have the opportunity to conduct a “replay” attack. This method of attack allows the individual to capture packets traversing throughout the network and send the packets at a later time, possibly</p>

ID	Threat
	<p>unknown by the intended receiver. Traffic is subject to replay if it meets the following conditions:</p> <ul style="list-style-type: none"> • Cleartext: an attacker with the ability to view unencrypted traffic can identify an appropriate segment of the communications to replay as well in order to cause the desired outcome • No integrity: alongside cleartext traffic, an attacker can make arbitrary modifications to captured traffic and replay it to cause the desired outcome if the recipient has no means to detect these

Threats (MOD_IPS)

ID	Threat
T.NETWORK_ACCESS	Unauthorized access may be achieved to services on a protected network from outside that network, or alternately services outside a protected network from inside the protected network. If malicious external devices are able to communicate with devices on the protected network via a backdoor then those devices may be susceptible to the unauthorized disclosure of information.
T.NETWORK_DISCLOSURE	Sensitive information on a protected network might be disclosed resulting from ingress- or egress-based actions.
T.NETWORK_DOS	Attacks against services inside a protected network, or indirectly by virtue of access to malicious agents from within a protected network, might lead to denial of services otherwise available within a protected network.
T.NETWORK_MISUSE	Access to services made available by a protected network might be used counter to operational environment policies. Devices located outside the protected network may attempt to conduct inappropriate activities while communicating with allowed public services. (e.g. manipulation of resident tools, SQL injection, phishing, forced resets, malicious zip files, disguised executables, privilege escalation tools and botnets).

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 claimed PP-Configuration/PP/PP-Modules below:
 - **(NDcPP + IPS MOD + FW +VPNGW)** PP-Configuration for Network Device, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.2
 - Collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
 - PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0)
 - PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E)
 - PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_1.3)
- Consistent with the expectations of the PP and PP-Modules, 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 PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation. In particular, the functionality mentioned in Section 7.2 of this report was excluded from the scope of the evaluation.

6 Documentation

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

- Sonicwall SonicOS 7.0.1 Common Criteria Administration Guide for NDPP, December 2024

Note: The above documents are the only documents that should be trusted for the configuration, administration, and use of the TOE in its evaluated configuration

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The Section 1.2 and 1.3 of the ST provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references.

7.1.1 Physical Boundaries and IT Testing Environment Components

The physical boundaries of the TOE are outlined in Section 1.3 of the ST. All physical boundaries are required in the TOE Environment. The IT Testing Environment components used to test the TOE are shown in section 1.4 of the ST.

7.1.2 Security Functions Provided by the TOE

The TOE provides the security functions required by the following claimed PP-Configuration:

- **(NDcPP + IPS MOD + FW +VPNGW)** PP-Configuration for Network Device, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.2

This PP-Configuration includes the following:

- collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
- PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0)
- PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E)
- PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_1.3)

7.2 Excluded Functionality

The following product functionality is not included in the CC 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 ETR for **Sonicwall SonicOS/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances**, which is not publicly available. The AAR 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 to the vendor-provided guidance documentation and ran the tests specified in the claimed PP-Configuration, PP/PP-Modules below:

- **(NDcPP + IPS MOD + FW +VPNGW)** PP-Configuration for Network Device, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.2
 - collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
 - PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0)
 - PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E)
 - PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_1.3)

The Independent Testing activity is documented in the AAR. A description of the test configurations may be found in Section 4.3 of the AAR and a list of the test tools may be found in the same section.

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 ETR. The reader of this document can assume that all 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. 5 and CEM version 3.1 Rev. 5. The evaluation determined the TOE Name to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP-Configuration/PP/PP-Modules.

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/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv 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 claimed PP-Configuration.

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 applied each EAL 1 ADV CEM work unit. 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 ST's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the claimed PP-Configuration 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 applied each EAL 1 AGD CEM work unit. 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 claimed PP-Configuration/PP/PP-Modules 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 applied each EAL 1 ALC CEM work unit. 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 applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the claimed PP-Configuration/PP/PP-Modules and recorded the results in a Test Report, summarized in the ETR and AAR.

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 claimed PP-Configuration/PP/PP-Modules, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

A list of the search terms used, the databases searched, and the date when the search was performed may be found in Section 6.3.1.2 of the AAR

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 claimed PP-Configuration/PP/PP-Modules, 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 claimed PP-Configuration, and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the guidance documents listed in Section 6. No versions of the TOE and software, either earlier or later were evaluated. Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other concerns and issues are adequately addressed in other parts of this document.

11 Annexes

Not applicable.

12 Security Target

Sonicwall SonicOS/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances Security Target, version 1.2

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 or not 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. Assurance Activity Report for Sonicwall SonicOS/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances, version 1.1
2. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
4. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
5. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.
6. Evaluation Technical Report for Sonicwall SonicOS/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances, version 1.1
7. Sonicwall SonicOS 7.0.1 Common Criteria Administration Guide for NDPP, December 2024
8. PP-Configuration: **(NDcPP + IPS MOD + FW +VPNGW)** PP-Configuration for Network Device, Intrusion Prevention Systems, Stateful Traffic Filter Firewalls, and Virtual Private Network Gateways, Version 1.2
9. PP/PP-Modules:
 - Collaborative Protection Profile for Network Devices, Version 2.2e (CPP_ND_V2.2E)
 - PP-Module for Intrusion Protection Systems (IPS), Version 1.0 (MOD_IPS_V1.0)
 - PP-Module for Stateful Traffic Filter Firewalls, Version 1.4 + Errata 20200625 (MOD_FW_1.4E)
 - PP-Module for Virtual Private Network (VPN) Gateways, Version 1.3 (MOD_VPNGW_1.3)
10. Sonicwall SonicOS/X v7.0.1 with VPN and IPS on TZ, NSa, NSsp, and NSv Appliances Security Target, version 1.2