National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

SonicWALL Secure Mobile Access (SMA) v12.4.1

Report Number: **CCEVS-VR-VID11218**
Dated: **Sep 28, 2021**
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 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jim Donndelinger

Ken Stutterheim

Swapna Katikaneni
Aerospace Corporation

Common Criteria Testing Laboratory

Fathi Nasraoui

Nithya Rachamadugu

Cygnacom Solutions

McLean, Virginia

Much of the material in this report was extracted from evaluation material prepared by the CCTL. The CCTL team deserves credit for their hard work in developing that material. Many of the product descriptions in this report were extracted from the SonicWALL SMA v12.4 Security Target.

Table of Contents

List of Figures and Tables

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 Secure Mobile Access (SMA) v12.4.1 as defined in the SonicWall SMA v12.4 Security Target v0.5. 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 SonicWALL Secure Mobile Access (SMA) v12.4 appliance functions as a remote access gateway operating as an intermediary device between end users on client devices and network resources residing on internal network. The appliance provides multiple access methods for end users or client devices to remotely access internal network resources from untrusted external networks. The SMA administrator configures policies comprised of security rules operating on users and targeting resources that must be satisfied to establish remote access. The TOE, SonicWALL SMA v12.4.1, is offered as SMA 6210 and SMA 7210 hardware appliances. The TOE consists of both hardware and software components. The SMA 6210 and SMA 7210 are identical except for CPU, RAM, and network ports. The SMA 8200v is a virtual appliance designed to operate in virtualization environment.

The TOE is a Network Device as defined by the collaborative Protection Profile for Network Devices v2.2e [NDcPP]: “A network device in the context of this cPP is a device composed of both hardware and software that is connected to the network and has an infrastructure role within the network”.

The evaluation was performed by the Cygnacom Common Criteria Testing Laboratory (CCTL) and was completed in September 2021. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the Cygnacom CCTL. The evaluation team determined that the product is:

- Common Criteria version 3.1 R5 Part 2 and Part 3 conformant,
- Demonstrates exact conformance to collaborative Protection Profile for Network Devices, Version 2.2e, March 23, 2020 as clarified by all applicable Technical Decisions.

The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org.

The Validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associate test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the Security Target (ST). The validation team, therefore, concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct.

2. Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology 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.
Information below 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.

Target of Evaluation: SonicWALL Secure Mobile Access (SMA) v12.4.1

Series	Platforms	Build
SonicWall Secure Mobile Access SMA1000 Series	SMA 6210	12.4.1-02451 [1]
	SMA 7210	
	SMA 8200v	

Security Target	SonicWall SMA v12.4 Security Target v0.5
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, March 2020.
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Developer:	SonicWALL 1033 McCarthy Boulevard, San Jose, CA, 95054

[1] Core build SMA 12.4.1-02451 with pform-hotfix-12.4.1-02559 and Connect Tunnel 12.4.1.939 was used in testing.

CCTL:	Cygnacom Solutions 7925 Jones Branch Dr, Suite 5400 McLean, VA 22102-3321
Evaluators:	Fathi Nasraoui
Validation Scheme:	National Information Assurance Partnership CCEVS
Validators:	Jim Donndelinger, Swapna Katikaneni, Ken Stutterheim.
CC Identification:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017
CEM Identification:	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017

3. TOE Architectural Information

The architecture of each hardware appliance consists of generic hardware that supports physical network connections, memory, storage, and computing resources. In case of virtual appliance, the hardware abstracted by the virtualization environment. The software includes operating system and SMA application software. The application software implements End User and Control & Configuration planes. Control & Configuration functionality includes all Security Functionality claimed in this document including administration, while End User is the gateway functionality that implements access to the internal network resource. While hardware varies between the appliance models, the software and End User and Control & Configuration is consistent across all evaluated appliances.

The physical boundary of the TOE includes:

- The appliance hardware
  - RJ-45 to serial local management port (Console port)
  - USB port
  - Ethernet management port (X0 Ethernet port)

The Operational Environment of the TOE includes:

- The management workstation with a web browser
- VPN client (Connect Tunnel for Windows 10 v12.4.1)
- External IT servers:
  - Audit server for external storage of audit records
  - Certificate Authority and OCSP servers to support X.509 (optional)

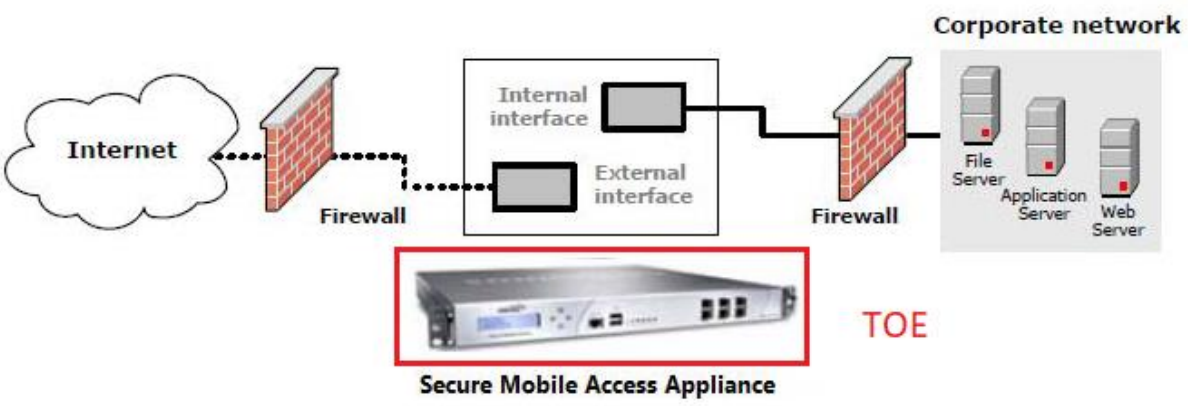


Figure 1: TOE Boundary

4. Security Policy

The TOE enforces the following security policies as described in the Security Target (ST):

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted path/Channel

4.1. Security Audit

The TOE generates audit records for all security-relevant events. For each event, the TOE records the date and time, the type of event, the subject identity, and the outcome of the event logged. The resulting records can be stored locally or securely sent to a designated audit server for archiving. Security Administrators using the appropriate AMC menu can also view audit records locally. The TOE also implements timestamps based on a local system clock to ensure reliable audit information produced.

4.2. Cryptographic Support

The TOE performs the following cryptographic functionality:

- Encryption, decryption, hashing, keyed-hash message authentication, random number generation, signature generation and verification utilizing dedicated cryptographic library
- Cryptographic functionality is utilized to implement secure channels
    - TLSv1.2
- Entropy is collected from multiple software entropy sources and used to support PRNG seeding with full entropy
- Critical Security Parameters (CSPs) internally stored and cleared when no longer in use
- X.509v3 certificate-based authentication integrated with TLS protocol

The TOE is certified as a FIPS 140-2 level 2 cryptographic module, it internally manages CSPs and implements deletion procedures to mitigate the possibility of disclosure or modification of CSPs. Additionally, the TOE provides functionality to manually clear

CSPs (e.g., host RSA keys), that can be invoked by a Security Administrator with appropriate permissions.

4.3. Identification and Authentication

Before any other action, each user is identified with a login name and authenticated with a password. Each authorized user is associated with assigned role and specific permissions that determine access to TOE features.

4.4. Security Management

The TOE allows remote administration using a TLS session over an internal management Ethernet port and local administration using a console adapter via a separate RJ-45 running RS-232 signaling. Remote administration is conducted over web-based interface (AMC) and local administration conducted over CLI.

All the management functionality is restricted to the Security Administrators of the TOE. Security Administrators are authorized perform configuration and management of the TOE. The term “Security Administrator” is used to refer to any user with administrative role and sufficient permissions.

4.5. Protection of the TSF

The TOE implements a number of measures to protect the integrity of its security features. The TOE protects CSPs, including stored passwords and cryptographic keys, so they are not directly viewable in plaintext. The TOE also ensures that reliable time information is available for both log accountability and synchronization with the operating environment.

The TOE employs both dedicated communication channels as well as cryptographic means to protect communication between itself and other components in the operational environment.

The TOE performs self-tests to detect internal failures and protect itself from malicious updates.

4.6. TOE Access

The TOE will display a customizable banner when an administrator initiates an interactive local or remote session. The TOE also enforces an administrator-defined inactivity timeout after which the inactive session is automatically terminated. Once a

session (local or remote) has been terminated, the TOE requires the user to re-authenticate.

4.7. Trusted Path/Channels

The TOE protects remote sessions by establishing a trusted path secured with TLS between itself and the administrator. The TOE prevents disclosure or modification of audit records by establishing a trusted channel secured with TLS between itself and the audit server.

5. Assumptions and Clarifications of Scope

5.1. Usage and Environmental Assumptions

The following assumptions are made regarding the use and deployment of the TOE:

- The network 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 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 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 device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device.
- 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 computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
- 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 for particular types of network devices (e.g., firewall).
- 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 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 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.

  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);

- The network device firmware and software are assumed to be updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

  The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside; and

- 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.
- 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.
- 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.
- For vNDs, it is assumed that VS provides, and is configured to provide sufficient isolation between software running in VMs one the same physical platform. Furthermore, it is assumed that the VS adequately protects itself form software running inside VMs on the same physical platform.
- For vNDs, it is assumed that the VS and VMs are correctly configured to support ND functionality implemented in VMs.

5.2. 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 Protection Profile for Network Devices, version 2.2e
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process
- 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 PPs. Any additional security-related

functional capabilities included in the product were not covered by this evaluation.

- Consumers employing the TOE must follow the configuration instructions provided in the CC Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.
- Consumers need to pay specific attention to all the functionality and features that are explicitly excluded from the scope of the evaluation and are identified below.

The TOE supports several features that are not part of the evaluated functionality. These features are not tested and excluded from the scope of the evaluation:

- Integration with a domain controller was not evaluated
- Any integration and/or communication with a single sign-on (SSO) provider is excluded from the evaluated configuration.
- Use of the SNMP management functionality is excluded, and it is disabled by default. The use of SNMPv3 for monitoring is not restricted; however, it is not evaluated.
- The use of SMTP is not evaluated and should not be configured in the evaluated configuration.
- Remote access to CLI over SSH is not evaluated and not enabled in the evaluated configuration.
- Remote access to CLI via hypervisor console emulation is not evaluated, this configuration and mode of access is controlled by hypervisor software.
- Synchronization with an NTP server is not evaluated.
- ExtraWeb and WorkPlace interfaces and all relevant end-user functionality is not evaluated.
    - ✓ Interoperability with additional VPN clients, other than Connect Tunnel on Windows, is not evaluated
    - ✓ Access Policy setting and enforcement is not evaluated
    - ✓ File Shares is not evaluated
    - ✓ OnDemand Tunnel Agent is not evaluated
    - ✓ Mobile Connect App integration is not evaluated
    - ✓ Web Proxy Agent is not evaluated
- Limited controls via physical buttons on hardware appliance were not evaluated.
- The separation of security domains within SMA appliance was not evaluated, single-domain mode was configured and utilized throughout testing.
- The TOE was tested in a single-homed configuration, dual-homed configuration was not evaluated.
- Support for TLS 1.3 was not evaluated as corresponding SF and AAs are still being developed by NDcPP iTC and are not available in the current version of the cPP.
- Support for hypervisors other than ESXi was not evaluated.

6. Documentation

The following documents were available for the evaluation. These documents are developed and maintained by SonicWALL and delivered to the end user of the TOE:

6.1. Security Target

SonicWall SMA v12.4 Security Target, Version 0.5, Sep 22, 2021

6.2. User Documentation

Reference Title	**ID**
SonicWALL Secure Mobile Access 12.4 Administration Guide	[ADMIN]
SonicWall SMA v12.4, Common Criteria Configuration Guide, Version 1.1 July 2021	[CC Addendum]

These are the only documents that should be trusted for the configuration, administration, and use of the TOE in the evaluated configuration. If other documents are referenced in CC Configuration Guide, only the sections of other documents referenced should be trusted and used to configure and operate the TOE.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website

7. Evaluated Configuration

The TOE, SonicWall SMA v12.4.1, is offered as physical appliances, which consists of SMA 6210 and SMA 7210 appliances and the SMA 8200v virtual appliance. The TOE consists of both hardware and software components. The SMA 6210 and SMA 7210 are identical except for CPU and 2 additional SFP+ network ports. The SMA 8200v is a virtual appliance designed to operate in the VMware Hypervisor version 6.7 virtualization environment.

All the physical TOE appliances are shipped ready for immediate access through a Command Line Interface (CLI) and after basic network configuration through a web-based Appliance Management Console (AMC). Virtual appliance requires installation into hypervisor environment and supports configuration through AMC. To ensure secure use the TOE must be configured prior to being put into production environment as specified in the user guidance.

7.1. Hardware

Table 1: SMA hardware appliances

Platform	Model	OS	CPU	RAM	Form	Specs
SMA v12.4.1	SMA 6210	SMA1000	Intel Core i5-7500 (Kaby Lake)	8GB (DDR4)	1U	6 1GB Ports
	SMA 7210	SMA1000	Intel Xeon E3-1275 v6 (Kaby Lake)	16GB (DDR4)	1U	6 1GB, 2 10GB SFP+ Ports

7.2. Software

The TOE, SonicWall SMA v12.4.1, is offered as SMA 6210 and SMA 7210 hardware appliances and SMA 8200v virtual appliance. The TOE's firmware is consistent across all appliances and consists of multiple components, including SonicWall Operating System (SMA1000). SonicWall Operating System, SMA1000, is based on Linux 5.4 kernel. The firmware assigned a uniquely identifiable build number and is the same for each appliance. Note that the Core build SMA 12.4.1-02451 with pform-hotfix-12.4.1-02559 and Connect Tunnel 12.4.1.939 was used in testing

7.3. Virtualization

The TOE, SonicWall SMA v12.4.1, includes SMA 8200v virtual appliance. While SMA 8200v can be installed on a variety of hypervisors, it was only evaluated using the VMware ESXi 6.7 hypervisor running on a Dell PowerEdge R640, with the following virtual system specification:

Table 2: SMA virtual appliances

Platform	Model	Hypervisor	OS	CPU	RAM	Hard disk space	Virtual NIC
SMA v12.4.1	SMA 8200v	ESXi 6.7	SMA1000	4 vCPUs (Xeon Silver 4208 2.1GHz)	8GB ECC DDR-4 2400	160 GB, thick provisioned	2 vNIC of 1000BaseT

8. IT Product Testing

This section describes the testing efforts of the Evaluation Team. The information is derived from the *Test Report for SonicWALL SMA v12.4* document. The purpose of this activity was to confirm that the TOE behaves in accordance with security functional requirements specified in the ST.

8.1. Developer Testing

NDcPPv2.2e evaluations do not require developer testing evidence for assurance activities.

8.2. Evaluator Independent Testing

A test plan was developed in accordance with the Testing Assurance Activities specified in the NDcPPv2.2e.

Testing was conducted remotely from May 2021 to June 2021 at the laboratory at McLean 7925 Jones Branch Dr. #5200, McLean, VA 22102.

The Evaluator successfully performed the following activities during independent testing:

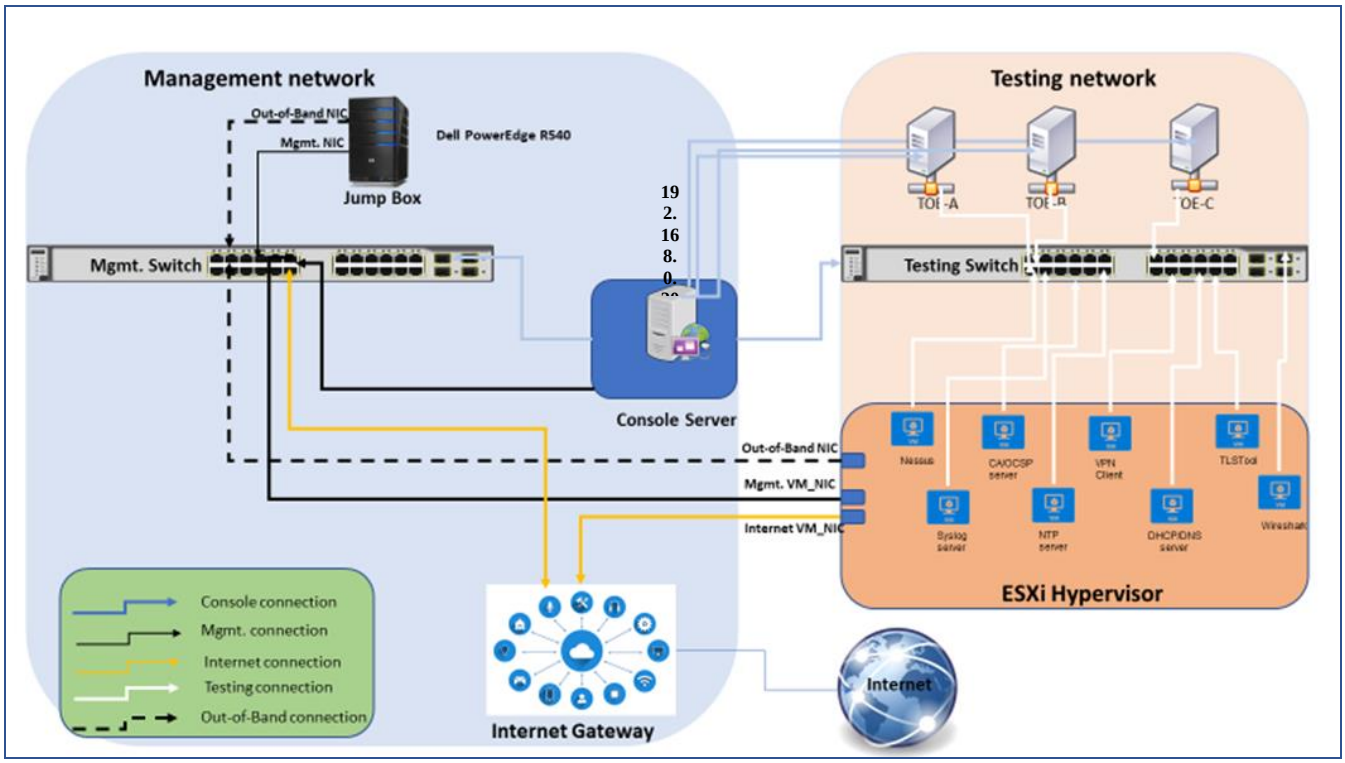
- Placed TOE into evaluated configuration by following the preparative procedures
- Successfully executed the NDcPP Assurance-defined tests including the selection-based TLS, and X509 tests
- Planned and executed a series of vulnerability/penetration tests

It was determined after examining the Test Report and full set of test results provided by the evaluators the testing requirements for NDcPPv2.2e are fulfilled.

8.3. Testing Topology

As shown below, the test topology is configured for a dedicated and fully isolated ‘Test’ LAN. This setup prevents general access while still granting evaluators direct access to the TOE. The setup consists of a ‘Test’ LAN for IPv4. The server is local to the ‘Test’ LAN and packet capture is done by a laptop connected to a mirrored port on the switch. All devices in the testing setup are synchronized through an NTP server virtual machine

Note: The diagram shows the components involved in the testing.



Physical Lab Test Setup – SonicWALL Test Environment

Device	Purpose
TOE-A	TOE, connected to S1 port 1
TOE-B	TOE, connected to S1 port 2
TOE-C	TOE, connected to S1 port 3
Console Server	***TOE's Console access***
Console server with USB and RJ45 interfaces	Provide local console access to TOEs through USB or RJ45 interfaces
S1	Switch with port mirroring capability
Virtualized servers	
Syslog Server	OS : CentOS 7 Syslog-ng-3.19.1-1.e17.x86_64 Function : audit server

Device	Purpose
VPN connect tunnel Client	OS : Windows 10 Entreprise Software version connect tunnel v12.4.1
OpenSSL CA OpenSSL OCSP Responder	OS: CentOS 7 Openssl version: OpenSSL 1.0.2k Function: CA and OCSP server
DNS and DHCP server	OS: Windows Server 2016 Function: AD, DNS and DHCP servers
NTP Server	OS: CentOS NTP version: 4.2.6p5 Function: ntp server
TLS tool	TLS tool version 1.3.27 used to send modified TLS handshake traffic or modified certificates OS: windows 10 Enterprise Protocols: TLS 1.2
Wireshark Laptop	OS: Windows 7 Professional Tools/version: Wireshark 3.0.2 (64 bits) Function: Network Traffic Monitor
Management Host (TOE-A)	Windows 10 Enterprise Bitvise 6.47 and 8.35, putty 0.74, nmap 7.80, Nessus 8.13.1, Winscp v5.15.2
Management Host (TOE-B)	Windows 10 Enterprise Bitvise 6.47 and 8.35, putty 0.74, nmap 7.80, Nessus 8.13.1, Winscp v5.15.2
Management Host (TOE-C)	Windows 10 Enterprise Bitvise 6.47 and 8.35, putty 0.74, nmap 7.80, Winscp v5.15.2
Nessus Scanner	OS: Windows 10 Entreprise Tools version: Nessus Pro version 8.13.1

Table 1: Testing Topology Identifiers

8.4. Test Hardware

Formal testing in the lab was conducted using the following hardware:

- Cisco Switch SG550X-48P running Cisco IOS v6.5 with port-mirroring capabilities
- Cisco Switch SG550X-48P running Cisco IOS v6.5
- Dell PowerEdge R540 running ESXi v6.7
- Dell PowerEdge R340 running Windows 10 Enterprise
- BlackBox LES1608A console server

8.5. Test Software

All testing was conducted using the following software:

- VMware ESXi 6.7 bare metal hypervisor
- Wireshark v3.4.5 (64-bit)
- Nessus v8.13.1 with a full set of plugins
- Nmap v7.80
- Syslog-ng version 3.28.1
- PuTTY Release 0.74
- WinSCP v5.17.9
- VM CentOS Linux 7
- VM Windows 10 Enterprise
- TLS tool v1.3.27

9. Results of 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 5 and CEM version 3.1 rev 5. Additionally, the evaluators performed the assurance activities specified in the Protection Profile collaborative Protection Profile for Network Devices Version 2.2e. The evaluation determined the TOE meets the SARs contained the NDcPPv2.2e.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by Cygnacom CCTL (proprietary).

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 TOE, SonicWALL Secure Mobile Access (SMA) v12.4.1, 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 Protection Profile for Network Devices, version 2.2e.

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 Security Target's TOE Summary Specification.

Additionally, the evaluator performed the Assurance Activities specified in the Protection Profile for Network Devices, version 2.2e.

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 Protection Profile for Network Devices, version 2.2e 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 Protection Profile for Network Devices, version 2.2e. 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 Protection Profile for Network Devices, version 2.2e., 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.

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 Protection Profile for Network Devices, version 2.2e., 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 Protection Profile for Network Devices, version 2.2e., and correctly verified that the product meets the claims in the ST.

10. Validators Comments/Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Configuration for Common Criteria Guide. The evaluated version consists of core build SMA 12.4.1-02451 with pform-hotfix-12.4.1-02559 and VPN connect Tunnel version 12.4.1.939. No other versions of the TOE and software, either earlier or later were evaluated.

Note that The TOE doesn't support log synchronization, which means the logs that were created during a network disconnect will not be transferred to the Syslog server. The newly created logs after the reconnection will start to transfer from TOE to the syslog server.

Please note that the functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target. Other product functionality included, such as TLS v1.3 functionality, was not assessed as part of this evaluation. Additional functionality provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

The excluded functionality is specified in section 5.2 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11. 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.

11.1. Acronyms

The following are product specific and CC specific acronyms. Not all these acronyms are used in this document.

BGP	Border Gateway Protocol
CEM	Common Evaluation Methodology
CLI	Command Line Interface
DNS	Domain Name System
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTP	HyperText Transmission Protocol
HTTPS	HyperText Transmission Protocol, Secure

IP	Internet Protocol
IPS	Intrusion Protection System
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OSPFv2	Open Shortest Path First
PDF	Portable Document Format
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell Network Protocol
SSL	Secure Sockets Layer,
ST	Security Target
TACACS	Terminal Access Controller Access-Control System
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security,
UDP	User Datagram Protocol
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

12. Bibliography

URLs

[1] Common Criteria Evaluation and Validation Scheme (CCEVS): (http://www.niap-ccevs.org/cc-scheme).

[2] Cygnacom Solutions CCTL (http://www.Cygnacom.com).

CCEVS Documents

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, July 2009 Version 3.1 Revision 5, CCMB-2017-04-001.

[2] Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components, April 2017 Version 3.1 Revision 5, CCMB-2017-04-002.

[3] Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003.

[4] Common Methodology for Information Technology Security Evaluation - Evaluation methodology, April 2017, Version 3.1 Revision 5, CCMB-2017-04-004.

[5] SonicWall SMA v12.4 Security Target Version 0.5, Sep 22, 2021

[6] Evaluation Technical Report for a Target of Evaluation Volume 1: Evaluation of the ST SonicWall SMA v12.4 Version 0.3 ETR Volume 1 Sep 22, 2021

[7] Evaluation Technical Report for a Target of Evaluation Volume 2: Evaluation of the TOE SonicWall SMA v12.4 Version 0.4 ETR Volume 2, Sep 13,2021

[8] Test Report SonicWall SMA v12.4 Document Version 0.5 Sep 13,2021

[9] Assurance Activity Report for SonicWALL SMA v12.4 Version 0.7, Sep 22,2021

[10] SonicWall SMA v12.4, Common Criteria Configuration Guide, Version 1.1 July 2021

[11] SonicWALL Secure Mobile Access 12.4 Administration Guide