National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme Validation Report

SonicWall Secure Mobile Access (SMA) v12.1

Report Number: **CCEVS-VR-VID11023**
Dated: **July 13, 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

Jerome Myers, PhD

Kenneth Stutterheim

Marybeth Panock

Harry Beddo

James Donndelinger

The Aerospace Corporation

Common Criteria Testing Laboratory

Fathi Nasraoui

Sridevi Kumar

Cygnacom Solutions

McLean, Virginia

Table of Contents

List of Figures and Tables

1. Executive Summary

This report documents the National Information Assurance Partnership (NIAP) validation team's assessment of the evaluation of the SonicWall, Inc. Secure Mobile Access (SMA) v12.1 network device. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation by any agency of the U.S. government, and no warranty is either expressed or implied.

The evaluation was performed by the Cygnacom Solutions Common Criteria Testing Laboratory (CCTL) and was completed in July 2020. The information in this report is derived from the Evaluation Technical Report (ETR) and associated test reports, all written by the Cygnacom Solutions CCTL. The evaluation determined that the product is:

- Common Criteria version 3.1 R5 Part 2 and Part 3 conformant,
- and demonstrates exact conformance to *collaborative Protection Profile for Network Devices, Version 2.1, September 2018* as clarified by all applicable Technical Decisions.

The Target of Evaluation (TOE) is the SonicWall, Inc. Secure Mobile Access (SMA) v12.1 network device.

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 (Version 3.1, Rev 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 5). 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 monitored the activities of the evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, 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.

The Cygnacom Solutions evaluation team concluded that the product meets the Common Criteria requirements of the collaborative Protection Profile for Network Devices Version 2.1 24 September-2018 (NDcPP21).

The technical information included in this report was obtained from the SonicWall SMA v12.1 Security Target Version 0.8, June 30, 2020 and analysis performed by the Validation Team.

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) using the Common Methodology for Information Technology Security Evaluation (CEM) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

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 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 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, Inc. Secure Mobile Access (SMA) v12.1
Protection Profile	collaborative Protection Profile for Network Devices Version 2.1 24 September-2018 (NDcPP21)
ST	SonicWall SMA v12.1 Security Target, Version 0.8, June 30, 2020
Evaluation Technical Report	Evaluation Technical Report for a Target of Evaluation Volume 1: Evaluation of the ST SonicWall SMA v12.1 Version 0.9 ETR Volume 1 June 30, 2020
	Evaluation Technical Report for a Target of Evaluation Volume 2: Evaluation of the TOE SonicWall SMA v12.1 Version 0.7 ETR Volume 2 July 8, 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, rev 5
Conformance Result	CC Part 2 extended, CC Part 3 conformant
Sponsor	SonicWall, Inc.
Developer	SonicWall, Inc.

Item	Identifier
Common Criteria Testing Lab (CCTL)	Cygnacom Solutions
CCEVS Validators	Kenneth Stutterheim, Marybeth Panock, Harry Beddo, James Donndelinger

3. TOE Architecture

Note: The following architectural description is based on the description presented in the Security Target.

The SonicWall Secure Mobile Access (SMA) v12.1 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 in order to establish remote access.

3.1. Evaluated Platforms

The TOE, SonicWall SMA v12.1, is offered as SMA 6210 and SMA 7210 appliances. The TOE consists of both hardware and software components. The SMA 6210 and SMA 7210 are identical except for CPU, RAM, and SFP+ ports.

3.2. TOE Architecture

The underlying architecture of each TOE appliance consists of hardware that supports physical network connections, memory, processor and software that implements End User and Control and Configuration. While hardware slightly varies between the two appliance models, the software is consistent across all evaluated appliances.

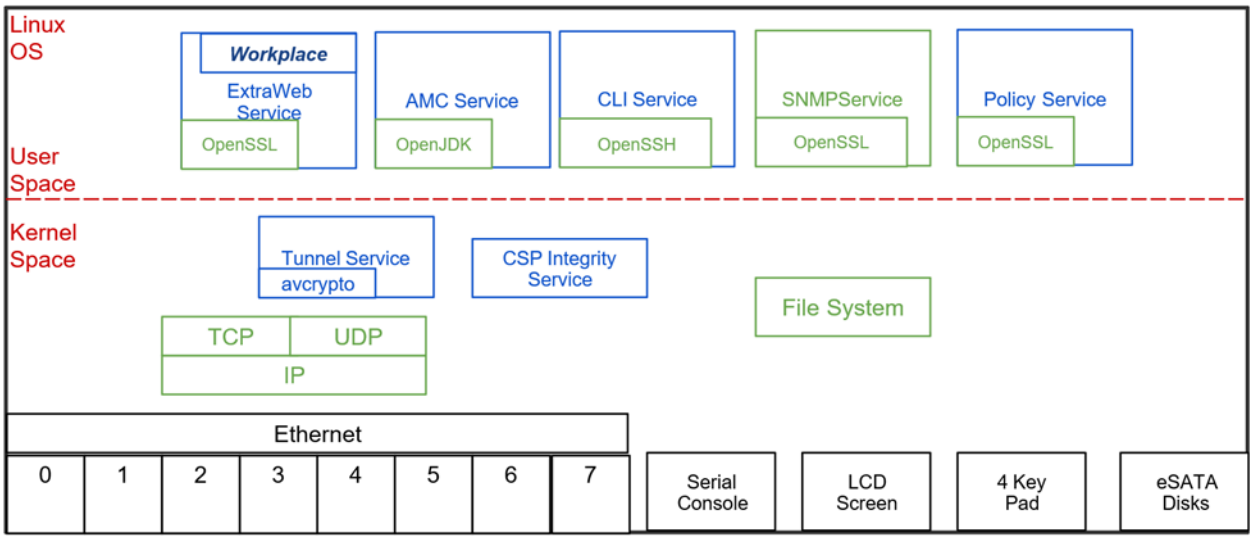

Figure 1: TOE Architecture

There are numerous open source and proprietary components packaged in the software, but only those relevant to the TOE's SF are presented in this reference architecture (**Error! Reference source not found.**) for simplicity.

3.3. Physical Boundary

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
- External IT servers:
  - Audit server for external storage of audit records
  - Certificate Authority and OCSP servers to support X.509 (optional)

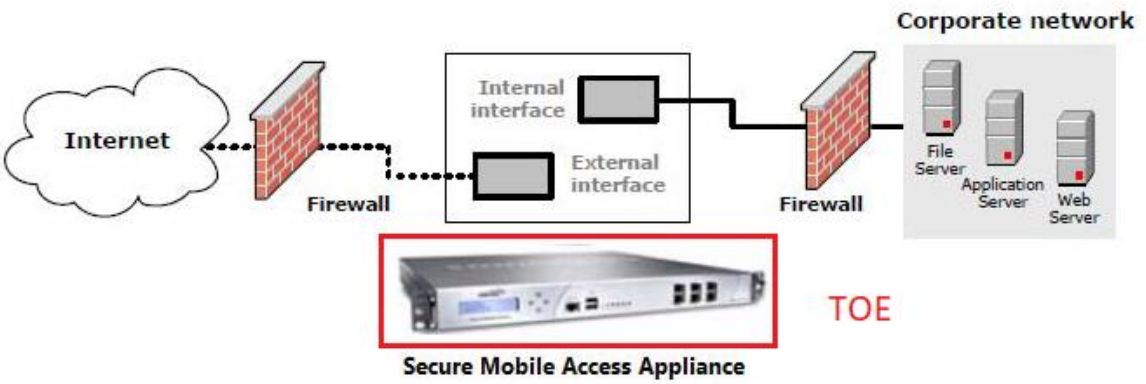

Figure 2: TOE Boundary

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
    - TLSv1.1 and 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

The TOE supports Role-Based Access Control (RBAC) managed by an AAA module that stores and manages permissions of all users and their roles. 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 of 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

5.1. General Assumptions

The scope of this evaluation was limited to the functionality and assurances covered in the NDcPP21 as described for this TOE in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

5.2. 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);
- 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.

6. Clarification of Scope

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

- 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 (NDcPP21), this evaluation did not specifically search for, nor attempt to exploit, 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 that may be included in the product were not covered by this evaluation. In particular, the functionality listed in Section 9.2 of this document is not covered.

7. Documentation

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

- SonicWall Secure Mobile Access 12.1 Administration Guide
- Configuration for Common Criteria SonicWall SMA v12.1 version 0.5

The documentation listed above is the only documentation that should be trusted to install, administer, or use the TOE in its evaluated configuration. 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 device as evaluated. To use the product in the evaluated configuration, the product must be configured as specified in the guidance documentation listed above.

Consumers are encouraged to download the configuration guides from the NIAP website to ensure the device is configured as evaluated.

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 v12.1* 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

NDcPPv2.1 evaluations do not require developer testing evidence for assurance activities.

8.2. Evaluator Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the (NDcPPv2.1). 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 may be found in Section 1.5 of that report.

A test plan was developed in accordance with the Testing Assurance Activities specified in the NDcPPv2.1.

Testing was conducted from January 2020 to July 2020 at the laboratory's sister facility in Ottawa with the testing being performed by, and completely under the control of, evaluators who are part of the U.S. CCTL staff.

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 NDcPPv2.1 are fulfilled.

9. Evaluated Configuration

9.1. Evaluated Models

The evaluated configuration consists of the following models:

- SMA 6210 with an Intel Core i5-7500 (Kaby Lake) processor, 1U form, and 6 1GB Ports
- SMA 7210 with an Intel Xeon E3-1275 v6 (Kaby Lake) processor, 1U form, and 6 1GB, 2 10GB SFP+ Ports

The SMA 6210 and SMA 7210 are identical except for CPU and 2 additional SFP+ network ports. The evaluated version consists of core build SMA 12.1.0-05477 with pform-hotfix-12.1.0-06384 and pform-hotfix-12.1.0-06427.

To use the product in the evaluated configuration, the product must be configured as specified in the following documents:

- Configuration for Common Criteria SonicWall SMA v12.1 version 0.5
- SonicWall Secure Mobile Access 12.1 Administration Guide
- SonicWall SMA v12.1 Security Target, Version 0.8, June 30, 2020

9.2. Excluded Functionality

The TOE supports a number of features that are not part of the core functionality. These features are not included in 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.
- Remote access to CLI over SSH is not evaluated and not enabled in the evaluated configuration.
- Synchronization with an NTP server is not evaluated.
- ExtraWeb and WorkPlace interfaces and all relevant end-user functionality is not evaluated.
    - SSL-based VPN 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
    - LCD controls functionality is not evaluated
- The separation of security domains was not evaluated, but multiple domains were concurrently utilized throughout testing

- The TOE was tested in a single-homed configuration, dual-homed configuration was not evaluated

10. Results of Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. The TOE was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 5. The evaluation methodology used by the Evaluation Team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 5.

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 version 3.1 R5 of the CC and the CEM. Additionally, the evaluators performed the assurance activities specified in the Protection Profile *collaborative Protection Profile for Network Devices Version 2.1.* and its Supporting Document: Mandatory Technical Document Evaluation Activities for Network Device cPP, September-2018.

The evaluation determined the TOE meets the security assurance requirements (SARs) contained the NDcPPv2.1.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by Cygnacom Solutions CCTL (proprietary). They are also summarized in the Assurance Activity Report (AAR), which is publicly available on the NIAP website for this evaluation.

The security assurance requirements the TOE was required to be evaluated conforming to from the NDcPP are listed below. All assurance activities and work units received a passing verdict.

- ADV_FSP.1 Basic functional specification
- AGD_OPE.1 Operational user guidance
- AGD_PRE.1 Preparative procedures
- ALC_CMC.1 Labelling of the TOE
- ALC_CMS.1 TOE CM coverage
- ASE_CCL.1 Conformance claims
- ASE_ECD.1 Extended components definition
- ASE_INT.1 ST Introduction
- ASE_OBJ.1 Security objectives
- ASE_REQ.1 Derived security requirements
- ASE_TSS.1 TOE summary specification
- ATE_IND.1 Independent testing – conformance
- AVA_VAN.1 Vulnerability survey

- The databases searched and the search terms are listed in section 3.6.1 of the Assurance Activity Report. The most recent search was conducted on July 6, 2020.

The evaluators concluded that the overall evaluation result for the target of evaluation is PASS. The validators reviewed the findings of the evaluation team and have concurred that the evidence and documentation of the work performed support the assigned rating.

11. Validators Comments/Recommendations

SonicWall, Inc. SMA devices provide capabilities that are in addition to those evaluated. The validators suggest that the consumer pay attention to the evaluated configuration of the devices as the functionality that was evaluated was scoped exclusively to the security functional requirements specified in the Security Target. Only the functionality implemented by the SFR's within the Security Target was 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.

All other functionality provided, to include software, firmware, or hardware that was not part of the evaluated configuration needs to be assessed separately and no further conclusions can be drawn about their effectiveness. The excluded functionality is specified in section 9.2 of this report.

All other items and scope issues have been sufficiently addressed elsewhere in this document.

12. Annexes

Not applicable.

13. Security Target

SonicWall SMA v12.1 Security Target, Version 0.8, June 30, 2020.

14. Glossary

14.1. 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.

14.2. Acronyms

The following are product specific and CC specific acronyms. Not all of 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

15. Bibliography

[1] Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and General Model, Version 3.1 Revision 5, April 2017.

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

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

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

[5] collaborative Protection Profile for Network Devices, Version 2.1, September 2018 (NDcPP21)

[6] SonicWall SMA v12.1 Security Target Version 0.8, June 30, 2020

[7] Evaluation Technical Report for a Target of Evaluation Volume 1: Evaluation of the ST SonicWall SMA v12.1 Version 0.9 ETR Volume 1 June 30, 2020

[8] Evaluation Technical Report for a Target of Evaluation Volume 2: Evaluation of the TOE SonicWall SMA v12.1 Version 0.7 ETR Volume 8, July 8, 2020

[9] Test Report SonicWall SMA v12.1 Document Version 1.4 June 30, 2020

[10] Assurance Activity Report for SonicWALL SMA v12.1 Version 0.9, July 8, 2020

[11] SonicWall SMA v12.1 Configuration for Common Criteria Version 0.5 June 24, 2020

[12] SonicWall Secure Mobile Access 12.1 Administration Guide