# FIPS 140-3 Non-Proprietary Security Policy

## SonicWall, Inc.

### SonicWall NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700

### Firmware Version: SonicOS/X 7.0.1

### Date: March 18th, 2025

**Prepared for:**

SONICWALL™

**Prepared by:**

intertek acumen security


**SonicWall, Inc.**

1033 McCarthy Boulevard

Milpitas, CA 95035
United States of America

Phone:
www.sonicwall.com

**Acumen Security, LLC.**

2400 Research Blvd.
Suite 395
Rockville, MD 20850
United States of America

Phone: +1 703 375 9820
www.acumensecurity.net

## Introduction

Federal Information Processing Standards Publication 140-3 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) Cryptographic Module Validation Program (CMVP) run the FIPS 140-3 program. The NVLAP accredits independent testing labs to perform FIPS 140-3 testing; the CMVP validates modules meeting FIPS 140-3 validation. Validated is the term given to a module that is documented and tested against the FIPS 140-3 criteria.

More information is available on the CMVP website at:
https://csrc.nist.gov/projects/cryptographic-module-validation-program

## About this Document

This FIPS 140-3 non-proprietary Cryptographic Module Security Policy for the SonicWall, Inc. SonicWALL NSa 4700, Nsa 5700, NSa 6700, NSsp 10700, NSsp 11700 and NSsp 13700 models provides an overview of the product and a high-level description of how it meets the overall Level 2 security requirements of FIPS 140-3.

## Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. SonicWall, Inc. shall have no liability for any error or damages of any kind resulting from the use of this document.

## Notices

# Table of Contents


Introduction ..... 2
Disclaimer ..... 2
Notices ..... 2
1. General ..... 5
2. Cryptographic Module Specification ..... 6
Module Description and Cryptographic Boundary ..... 6
Cryptographic Algorithms ..... 9
Modes of Operation ..... 14
Approved Mode of Operation ..... 14
Non-Approved Mode of Operation ..... 16
Security Rules and Guidance ..... 16
Applicable Implementation Guidance ..... 17
Self-Initiated Cryptographic Output ..... 17
3. Cryptographic Module Interfaces ..... 18
4. Roles, Services, and Authentication ..... 18
Assumption of Roles ..... 18
Authentication Methods ..... 21
Services ..... 22
Crypto Officer Services ..... 22
5. Software/Firmware Security ..... 34
6. Operational Environment ..... 34
7. Physical Security ..... 34
8. Non-Invasive Security ..... 36
9. Sensitive Security Parameter Management ..... 37
10. Self-Tests ..... 45
Pre-Operational Self-Tests ..... 45
Conditional Self-Tests ..... 45
11. Life-Cycle Assurance ..... 46
Crypto Officer Guidance ..... 46
Configuration Management ..... 47
12. Mitigation of Other Attacks ..... 48
References and Definitions ..... 50


# List of Tables


Table 1 - Security Levels ..... 5
Table 2 - Cryptographic Module Tested Configuration ..... 8
Table 3 – Approved Algorithms ..... 12
Table 4 – Non-Approved Algorithms Allowed in the Approved Mode of Operation ..... 13
Table 5 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed ..... 13
Table 5a – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation ..... 13
Table 6 - Security Relevant Protocols Used in Approved Mode ..... 14

Table 7 – Ports and Interfaces ..... 18
Table 8 – Roles, Service Commands, Input and Output ..... 20
Table 9 – Roles and Authentication ..... 21
Table 10 – Approved Services ..... 29
Table 11 – non-Approved Services ..... 33
Table 12 – Physical Security Inspection Guidelines ..... 34
Table 13 – Number of Tamper-Evident Seals ..... 34
Table 14 – SSPs ..... 43
Table 15 – Non-Deterministic Random Number Generator Specification ..... 44
Table 16 – References ..... 51
Table 17 – Acronyms and Definitions ..... 52

## List of Figures

Figure 1. Front view of the NSa 4700 ..... 6
Figure 2. Front view of the NSa 5700 ..... 6
Figure 3. Rear view of the NSa 4700/NSa 5700 ..... 6
Figure 4. Front view of the NSa 6700 ..... 6
Figure 5. Rear view of the NSa 6700 ..... 7
Figure 6. Front view of the NSsp 10700 ..... 7
Figure 7. Front View of the NSsp 11700 ..... 7
Figure 8. Front View of the NSsp 13700 ..... 7
Figure 9. Rear View of the NSsp 10700/NSsp 11700/NSsp 13700 ..... 7
Figure 10. Tamper-evident seal placements for NSa 4700/5700/6700 and NSsp 10700/11700/13700 ... 35

# 1. General

This document describes the cryptographic module security policy for the SonicWall, Inc. SonicWALL NSa 4700, Nsa 5700, NSa 6700, NSsp 10700, NSsp 11700 and NSsp 13700 models (FW version: SonicOS/X 7.0.1) cryptographic module (also referred to as the "module" hereafter). It contains the specification of the security rules, under which the cryptographic module operates, including the security rules derived from the requirements of the FIPS 140-3 standard.

The Module, a hardware cryptographic module, meets the overall security level 2 requirements. The following table lists the level of validation for each area in FIPS 140-3:

| ISO/IEC 24759 Section 6. [Number Below] | FIPS 140-3 Section Title | Security Level |
|---|---|---|
| 1 | General | 2 |
| 2 | Cryptographic module specification | 2 |
| 3 | Cryptographic module interfaces | 2 |
| 4 | Roles, services, and authentication | 3 |
| 5 | Software/Firmware security | 2 |
| 6 | Operational environment | N/A |
| 7 | Physical security | 2 |
| 8 | Non-invasive security | N/A |
| 9 | Sensitive security parameter management | 2 |
| 10 | Self-tests | 2 |
| 11 | Life-cycle assurance | 2 |
| 12 | Mitigation of other attacks | 2 |

*Table 1 - Security Levels*

# 2. Cryptographic Module Specification

The module is an Internet security appliance, which provides stateful packet filtering firewall, deep packet inspection, virtual private network (VPN), and traffic shaping services.

The module is intended for use by US Federal agencies and other markets that require FIPS 140-3 validated cryptographic modules. The appliance Encryption technology uses Suite B algorithms. Suite B algorithms are approved by the U.S. government for protecting both Unclassified and Classified data.

## Module Description and Cryptographic Boundary

The cryptographic module is defined as a multi-chip standalone hardware module. The cryptographic boundary of the module is the surfaces and edges of the device enclosure, inclusive of the physical ports. The physical form of the Module is depicted below.


Figure 1. Front view of the NSa 4700


Figure 2. Front view of the NSa 5700


Figure 3. Rear view of the NSa 4700/NSa 5700


Figure 4. Front view of the NSa 6700


Figure 5. Rear view of the NSa 6700


Figure 6. Front view of the NSsp 10700


Figure 7. Front View of the NSsp 11700


Figure 8. Front View of the NSsp 13700


Figure 9. Rear View of the NSsp 10700/NSsp 11700/NSsp 13700

The cryptographic module tested configurations can be found in the table below:

| Model | Hardware [Part Number and Version] | Firmware Version | Distinguishing Features |
|---|---|---|---|
| NSa 4700 | 101-500668-55 (Rev A) | SonicOS/X 7.0.1 | Optional add in 1TB storage and redundant power supply, field replacement power supply and fan modules |
| Nsa 5700 | 101-500667-52 (Rev A) | SonicOS/X 7.0.1 | Optional add in 1TB storage and redundant power supply, field replacement power supply and fan modules |
| NSa 6700 | 101-500685-55 (Rev A) | SonicOS/X 7.0.1 | Optional add in 1TB storage and redundant power supply, field replacement power supply and fan modules |
| NSsp 10700 | 101-500684-51 (Rev B) | SonicOS/X 7.0.1 | Field replacement power supply and fan modules |
| NSsp 11700 | 101-500683-51 (Rev B) | SonicOS/X 7.0.1 | Field replacement power supply and fan modules |
| NSsp 13700 | 101-500647-54 (Rev B) | SonicOS/X 7.0.1 | Field replacement power supply and fan modules |

Table 2 - Cryptographic Module Tested Configuration

## Cryptographic Algorithms

The Module implements the Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

| CAVP Cert | Algorithm and Standard | Mode/Method | Description / Key Size(s) / Key Strength(s) | Use / Function |
|---|---|---|---|---|
| A6598 | AES<br>FIPS 197<br>SP800-38A | CBC | Key Sizes: 128, 192, 256 | Encrypt, Decrypt |
| A6598 | AES<br>FIPS 197<br>SP800-38D | GCM [38D][1] | Key Sizes: 128, 192, 256<br>Tag Len: 128 | Authenticated Encrypt, Authenticated Decrypt, Message Authentication |
| A2138 | AES<br>FIPS 197<br>SP800-90B | Conditioning Component CBC-MAC | Key Size: 128<br>Payload Length: 128 | Conditioning component used in Entropy Source |

[1] The module's AES-GCM implementation conforms to IG C.H scenario #1 following RFC 5288 for TLS. The module is compatible with TLSv1.2 (RFC 7627) and provides support for the acceptable GCM cipher suites from Section 3.3.1 of SP 800-52 Rev1 or SP 800-52 Rev2. The counter portion of the IV is set by the module within its cryptographic boundary. The construction of the 64-bit nonce_explicit part of the IV is deterministic via a monotonically increasing counter. When the IV exhausts the maximum number of possible values for a given session key, the first party, client or server, to encounter this condition will trigger a handshake to establish a new encryption key. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established. The module's AES GCM implementation also conforms to IG C.H Scenario #5 following RFC 8446 for TLS 1.3 and provides support for the acceptable GCM cipher suites from Section B.4 of RFC 8446 and confirms that the IV is generated and used within the protocol's implementation.

| CAVP Cert | Algorithm and Standard | Mode/Method | Description / Key Size(s) / Key Strength(s) | Use / Function |
|---|---|---|---|---|
| Vendor Affirmed | CKG<br>NIST SP 800-133rev2 | Section 4 | N/A | Key Generation |
| A6598 | CVL<br>RFC 8446 | KDF TLS v1.3<br>(as per Section 7.1 of RFC 8446) | SHA2-256, SHA2-384 | Key Derivation |
| A6598 | CVL<br>NIST SP 800-135rev1 | IKEv1<br>Digital Signature and PSK | SHA2-256, SHA2-384, SHA2-512 | Key Derivation |
| A6598 | CVL<br>NIST SP 800-135rev1 | IKEv2<br>DH 224-521 bits | SHA2-256, SHA2-384, SHA2-512 | Key Derivation |
| A6598 | CVL<br>NIST SP 800-135rev1 | TLS v1.2 (RFC 7627) | SHA2-256, SHA2-384, SHA2-512 | Key Derivation |
| A6598 | ECDSA (FIPS186-5) | SigGen | P-224, P-256, P-384, P-521 | Signature Generation |
| A6598 | ECDSA (FIPS186-5) | SigVer | P-256, P-384, P-521 | Signature Verification |
| A6598 | DRBG<br>SP800-90Arev1 | Hash DRBG | Mode: SHA2-256<br>Entropy Input: 256<br>Nonce: 128 | Deterministic Random Bit Generation |

| CAVP Cert | Algorithm and Standard | Mode/Method | Description / Key Size(s) / Key Strength(s) | Use / Function |
|---|---|---|---|---|
| A6598 | ECDSA<br>FIPS PUB 186-5 | KeyGen | P-224, P-256, P-384, P-521 | Key Pair Generation |
| A6598 | ECDSA<br>FIPS PUB 186-5 | KeyVer | P-224, P-256, P-384, P-521 | Key Pair Validation |
| A6598 | HMAC<br>FIPS PUB 198-1 | HMAC-SHA-1 | MAC: 32-160 Increment 8<br>Key Length: 8-524288 Increment 8 | Message Authentication, KDF Primitive |
| A6598 | HMAC<br>FIPS PUB 198-1 | HMAC-SHA-256 | MAC: 32-256 Increment 8<br>Key Length: 8-524288 Increment 8 | |
| A6598 | HMAC<br>FIPS PUB 198-1 | HMAC-SHA-384 | MAC: 32-384 Increment 8<br>Key Length: 8-524288 Increment 8 | |
| A6598 | HMAC<br>FIPS PUB 198-1 | HMAC-SHA-512 | MAC: 32-512 Increment 8<br>Key Length: 8-524288 Increment 8 | |
| A6598 | KAS-1<br>[IG D.F] | KAS-FFC-SSC (SP 800-56Arev3 Shared Secret Computation, Per Scenario 2 of IG D.F) | Domain Parameter Generation Methods: FB, FC, ffdhe2048, MODP-2048; provides 112 bits of encryption strength | Key Agreement |
| A6598 | KAS-2<br>[IG D.F] | KAS-ECC-SSC (SP 800-56Arev3 Shared Secret Computation, Per Scenario 2 of IG D.F) | Domain Parameter Generation Methods: P-256, P-384, P-521; provides between 128 and 256 bits of encryption strength | Key Agreement |

| CAVP Cert | Algorithm and Standard | Mode/Method | Description / Key Size(s) / Key Strength(s) | Use / Function |
|---|---|---|---|---|
| A6598 | KTS-1<br>[IG D.G] | AES-CBC with HMAC-SHA-1 | AES-CBC (Key Sizes: 128, 256); HMAC-SHA-1; provides 128 or 256 bits of encryption strength | Key Transport/ Authentication (TLS 1.2) |
| A6598 | KTS-2<br>[IG D.G] | AES-CBC with HMAC-SHA2-256 | AES-CBC (Key Sizes: 128, 256); HMAC-SHA2-256; provides 128 or 256 bits of encryption strength | Key Transport/ Authentication (TLS 1.2) |
| A6598 | KTS-3<br>[IG D.G] | AES-GCM | AES-GCM (Key Sizes: 128, 256); provides 128 or 256 bits of encryption strength | Key Transport (TLS 1.3) |
| A6598 | RSA<br>(FIPS 186-5) | KeyGen | Mod: 2048, 3072, 4096 | Key Generation |
| A6598 | RSA<br>(FIPS 186-5) | SigGen: PKCS 1.5 | Mod: 2048, 3072, 4096 | Signature Generation |
| A6598 | RSA<br>(FIPS 186-5) | SigVer: PKCS 1.5 | Mod: 2048, 3072, 4096 | Signature Verification |
| A6598 | Safe Primes | NIST SP 800-56A, Rev3 | Safe Prime Groups: ffdhe2048, MODP-2048 | Key Generation |
| A6598 | Safe Primes | NIST SP 800-56A, Rev3 | Safe Prime Groups: ffdhe2048, MODP-2048 | Key Verification |
| A6598 | SHS<br>FIPS PUB 180-4 | SHA-1<br>SHA-256<br>SHA-384<br>SHA-512 | Message Length: 0-65536 Increment 8 | Message Digest Generation |
| N/A | SP 800-90B | N/A | Intel entropy source is used and meets SP800-90B and IG D.K compliance | For seeding DRBG |

Table 3 – Approved Algorithms

Note: There are some algorithms, modes, moduli and key sizes that have been CAVP tested but are not implemented/used by the module. Only the algorithms, modes, and key sizes shown in this table are implemented by the module.

| Algorithm | Caveat | Use / Function |
|---|---|---|
| DSA | Allowed per I.G. C.K resolution #3. (PQGGen and KeyGen tests performed) | Used as part of SP 800-56Ar3 key agreement |

Table 4 – Non-Approved Algorithms Allowed in the Approved Mode of Operation

The module supports the following non-Approved but allowed algorithms with no security claimed:

| Algorithm | Caveat | Use / Function |
|---|---|---|
| Triple-DES | No security claimed | Associated with the configuration setting. Used to encrypt/decrypt Gateway Anti-Virus (GAV) signature files (internal to the module only)<br><br>(This function is considered obfuscation and cannot be used to store or transmit sensitive information) |
| MD5 | No security claimed | Used to obfuscate RADIUS and TACACS+ (always encapsulated using IPsec) |
| PBKDF (non-compliant) | No security claimed | Associated with RADIUS (always encapsulated using IPsec) |

Table 5 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

The module supports the following Non-Approved Algorithms Not Allowed in the Approved Mode of Operation:

| Algorithm/Function | Use / Function |
|---|---|
| KDF-SSH | Used for SSH operations in the non-approved mode |
| KDF-SNMP | Used for SNMP operations in the non-approved mode |

Table 5a – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

| Protocol[2] | Key Exchange | Auth | Cipher | Integrity |
|---|---|---|---|---|
| IKEv1 | DH Group 14, 19, 20, 21 | RSA and ECDSA digital signature | AES CBC 128/192/256 | HMAC-SHA-256-128<br>HMAC-SHA-384-192<br>HMAC-SHA-512-256 |
| IKEv2 | DH Group 14, 19, 20, 21 | RSA and ECDSA Digital Signature<br>Shared Key Message Integrity Code | AES CBC 128/192/256 | HMAC-SHA-256-128<br>HMAC-SHA-384-192<br>HMAC-SHA-512-256 |
| IPsec ESP | IKEv1 or IKEv2 with optional:<br>Diffie-Hellman (L=2048, N=224, 256)<br>EC Diffie-Hellman P-256, P-384 and P-521 | IKEv1,<br>IKEv2 | AES CBC 128/192/256 | HMAC-SHA-256-128<br>HMAC-SHA-384-192<br>HMAC-SHA-512-256 |
| TLS 1.2 | TLS_RSA_WITH_AES_128_CBC_SHA<br>TLS_RSA_WITH_AES_256_CBC_SHA<br>TLS_RSA_WITH_AES_128_CBC_SHA256<br>TLS_RSA_WITH_AES_256_CBC_SHA256<br>TLS_RSA_WITH_AES_128_GCM_SHA256<br>TLS_RSA_WITH_AES_256_GCM_SHA384 | | | |
| TLS 1.3 | TLS_AES_128_GCM_SHA256<br>TLS_AES_256_GCM_SHA384 | | | |

Table 6 - Security Relevant Protocols Used in Approved Mode

## Modes of Operation

### Approved Mode of Operation

The Approved mode configuration can be determined by the operator, by checking the state of the "Approved Mode" checkbox on the System/Settings page over the web interface or issuing "show fips" command over the console. When the "Approved mode" checkbox is selected, the module executes a compliance checking procedure, examining all settings related to the security rules described below. The operator is responsible for appropriately updating these settings during setup and will be prompted by the compliance tool if a setting has been modified taking the module out of compliance. The "Approved mode" checkbox and corresponding system flag ("fips"), which can be queried over the console, will not be set unless all settings are compliant. The "Approved mode" checkbox and fips system flag are indicators that the module is running in the Approved mode of operation.

[2] No parts of the TLS or IKE protocols, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

The module is not configured to operate in Approved mode by default. The following steps shall be taken during set-up of the module to enable Approved mode of operation:

1. The default Administrator and User passwords shall be immediately changed and be at least eight (8) characters.
2. The RADIUS/TACACS+ shared secrets shall be at least eight (8) characters.
3. Traffic between the module and the RADIUS/TACACS+ server shall be secured via an IPsec tunnel. *Note: This step only needs to be performed if RADIUS or TACACS+ is supported.
    - LDAP cannot be enabled in Approved mode without being protected by TLS
    - LDAP cannot be enabled in Approved mode without selecting 'Require valid certificate from server'
    - LDAP cannot be enabled in Approved mode without valid local certificate for TLS
4. IKE shall be configured with 3rd Party Certificates or Preshared key for IPsec Keying Mode when creating VPN tunnels.
    - RSA Certificates lengths shall be 2048-bit or greater in size.
    - ECDSA Certificates curves shall be P-256, P-384 or P-521 only.
      or
    - Preshared key lengths shall be no less than 8 characters.
5. When creating VPN tunnels, ESP shall be enabled for IPSec.
6. Approved algorithms shall be used for encryption and authentication when creating VPN tunnels.
7. Group 14, 19, 20 or 21 shall be used for IKE Phase 1 DH Group. SHA-256 and higher shall be used for Authentication
8. “Advanced Routing Services” shall not be enabled.
9. “Group VPN management” shall not be enabled.
10. SNMP or SSH shall not be enabled.
11. The “SonicWALL Read-Only Admins,” group, satisfies neither the Cryptographic Officer nor the User Role and shall not be used in the Approved mode operation.

Note: Once the Approved mode of operation is enabled, SonicOSX enforces all of the above items. (Operators will not be allowed to change these features while in Approved mode of operation.)

Additionally:

The operator shall not enable the following :

- USB interface(s)
- Wireless interface
- 802.11i wireless security

## Non-Approved Mode of Operation

The Cryptographic Module provides the same set of services in the non-Approved mode as in the Approved mode but allows the following additional administration options and non-approved services which are not used in the Approved mode of operation. The following services shall be disabled before placing the module in Approved mode. The module does not transition to Approved mode until the following services are disabled.

- AAA server authentication (the Approved mode requires operation of RADIUS or TACACS+ only within a secure VPN tunnel)
- SSH
- SNMP

## Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-3.

1. The module provides two distinct operator roles: User and Crypto Officer.
2. The module provides identity-based authentication for the Crypto Officer and for the User.
3. The module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The module allows the operator to initiate the pre-operational or conditional self-tests on demand for periodic testing of the module by power cycling or resetting the module.
6. Self-tests do not require any operator action.
7. Data output is inhibited during, pre-operational self-tests, zeroization, and error states.
8. Status information does not contain SSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The module does not support a maintenance interface or role.
11. The module does not support manual key entry.
12. The module does not have any proprietary external input/output devices used for entry/output of data.
13. The module does not enter or output plaintext SSPs.
14. The module does not output intermediate key values.
15. The module does not support a bypass capability.
16. Firmware upgraded in the non-approved mode cannot be used in the approved mode. (The module enforces the deletion of any firmware upgrade before the approved mode can be entered.)

## Applicable Implementation Guidance

**2.4.B Tracking the Component Validation List**

The key derivation functions for IKEv1, IKEv2, TLS v1.2 RFC7627, and TLS v1.3 are only used in the context of their respective protocols.

**C.B Validation Testing of Hash Algorithms and Higher Cryptographic Algorithm Using Hash Algorithms**

Every approved hash algorithm implementation has been CAVP tested as shown in Table 3.

**C.F RSA Approved Parameter Sizes in FIPS 186-5**

The RSA modulus lengths supported by the module for RSA signature generation are 2048, 3072, and 4096 bits. CAVP testing was performed for the implemented RSA signature algorithm implementation. For FIPS 186-5 signature verification, the module supports the allowed mod sizes of 2048, 3072, 4096. The Miller-Rabin testing rounds are consistent with Table B.1 of FIPS 186-5.

**C.H Key/IV Pair Uniqueness Requirements from SP 800-38D**

Please see Footnote #1.

**D.C References to the Support of Industry Protocols**

The KDFs implemented are those described in SP 800-135rev1. (IKEv1, IKEv2, TLS v1.2 RFC7627, and TLS v1.3). All implemented KDFs have been CAVP tested under Cert. #A6598. No parts of the protocols, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

**D.H Requirements for Vendor Affirmation to SP 800-133r2**

The relevant sections of SP 800-133r2 are Section 4.

## Self-Initiated Cryptographic Output

The module implements a self-initiated cryptographic output capability for IPSec VPN. As part of enabling the service, the Crypto Officer shall configure the IPSec VPN client policy and enable it. Following this, the Crypto Officer shall turn on the "Enable Keep Alive" switch under the "Advanced" tab in the VPN Policy settings.

# 3. Cryptographic Module Interfaces

The module's ports and associated FIPS 140-3 defined logical interface categories are listed in the tables in this section:

| Physical Port | Logical Interface[3] | Data that passes over port/interface |
|---|---|---|
| MGMT Port | Data Input,<br>Data Output,<br>Status Output and<br>Control Input | Unit administration data |
| Status LEDs | Status Output | Status |
| Serial Console Port | Status Output and<br>Control Input | Unit administration data |
| Ethernet Ports | Data Input,<br>Data Output, Status Output<br>and Control Input (via the external GUI Administration interface) | Network connection data |
| Safe Mode (bootloader)/Reset Button | Control Input | Used to manually reset the appliance |
| Power Interface | N/A | N/A |

Table 7 – Ports and Interfaces

# 4. Roles, Services, and Authentication

## Assumption of Roles

The cryptographic module provides the roles of Crypto Officer and User. The cryptographic module does not provide a Maintenance role. The built-in "Administrator" is a member of "SonicWALL Administrators" group on the module, and the name used to login may be configured by the Cryptographic Officer role; the default username for the "Administrator" is "admin". The User role is authenticated using the credentials of a member of the "Limited Administrators" group. The configuration settings required to enable the Approved mode of operation is specified in Section 2.

The built-in administrator for which the default username is "admin" which is a member of "SonicWALL Administrators" group has full control privilege to query status and configure all firewall configurations including configure other user privilege. Other members of "SonicWALL Administrators" group have the same full control privilege as built-in administrator (part of "SonicWALL Administrators" group). There is another group called "Limited Administrators". Members of "Limited Administrators" group can query

[3] Control Output Interface is omitted as it is Not Applicable.

status and non-critical configuration. An operator is granted privilege by the membership of a particular group after login.

| Role | Service | Input | Output |
|---|---|---|---|
| CO (referred to as "SonicWALL Administrators" group) | Show Status | Command | Command Response |
| | Show Non-critical Configuration | Command | Command Response |
| | Monitor Network Status | Command | Command Response |
| | Log On | Username and Password or public key | Successful completion of service |
| | Log Off | Command | Command Response |
| | Clear Log | Command | Command Response |
| | Export Log | Command | Command Response |
| | Import/Export Certificates | Commands and Public Key | Public Key |
| | Filter Log | Command | Command Response |
| | Setup DHCP Server | Command | Command Response |
| | Generate Log Reports | Command | Command Response |
| | Configure VPN Settings | Commands, Preshared Key | Command Response |
| | IPsec VPN | SSPs and Encrypted Data | SSPs and Encrypted Data |
| | TLS | SSPs and Encrypted Data | SSPs and Encrypted Data |
| | Set Content Filter | Command | Command Response |
| | Configure DNS Settings | Command | Command Response |
| | Configure Access | Command | Command Response |
| | Zeroize | Command | Status Output indicating the completion of service. |
| | Perform Self-tests on-demand | Command | Output display on each algorithm running self-test and pass or fail |
| | Self-Initiate Cryptographic Output | SSPs and Encrypted Data | SSPs and Encrypted Data |
| User (referred to as "Limited Administrators" group) | Show Status | Command | Command Response |
| | Show Non-critical Configuration | Command | Command Response |
| | Monitor Network Status | Command | Command Response |
| | Log On | Username and Password or public key | Successful completion of service |
| | Log Off | Command | Command Response |
| | Export Log | Command | Command Response |
| | Filter Log | Command | Command Response |
| | Generate Log Reports | Command | Command Response |

| Role | Service | Input | Output |
|---|---|---|---|
| | TLS | SSPs and Encrypted Data | SSPs and Encrypted Data |
| | Configure DNS Settings | Command | Command Response |
| Unauthenticated | Module Reset | Command | Command Response |
| | No Auth Function | Command | Command Response |
| | Show Status (LED/Console) | N/A | N/A |
| | Perform Self-tests on-demand | Power Cycle | Output display on each algorithm running self-test and pass or fail |

Table 8 – Roles, Service Commands, Input and Output

The Module supports concurrent operators. Separation of roles is enforced by requiring operators to authenticate using either a username and password, or digital signature verification. The User role requires the use of a username and password or possession of the private key of a user entity belonging to the "Limited Administrators" group. The Crypto Officer role requires a username and password for authentication.

Multiple users may be logged in simultaneously, but only a single user-session can have full configuration privileges at any time, based upon the prioritized preemption model described below:

1. The Admin user (SonicWALL Administrators) has the highest priority and can preempt any users.
2. The additional operators who are members of the "SonicWALL Administrators" group can preempt any users except for the Admin user.
3. An operator that is a member of the "Limited Administrators" group can only preempt other members of the "Limited Administrators" group.

Session preemption may be handled in one of two ways, configurable from the System > Administration page, under the "On admin preemption" setting:

1. "Drop to non-config mode" – the preempting operator will have three choices:
    a. "Continue" – this action will drop the existing administrative session to a "non-config mode" and will impart full administrative privileges to the preempting user.
    b. "Non-Config Mode" – this action will keep the existing administrative session intact and will login the preempting user in a "non-config mode".
    c. "Cancel" – this action will cancel the login and will keep the existing administrative session intact.

2. "Log-out" – the preempting user will have three choices:
    a. "Continue" – this action will log out the existing administrative session and will impart full administrative privileges to the preempting user.
    b. "Non-Config Mode" – this action will keep the existing administrative session intact and will login the preempting user in a "non-config mode".
    c. "Cancel" – this action will cancel the login and will keep the existing administrative session intact.

"Non-config mode" administrative sessions will have no privileges to cryptographic functions making them functionally equivalent to User role sessions. The ability to enter "Non-config mode" may be disabled altogether from the System > Administration page, under the "On admin preemption" setting by selecting "Log out" as the desired action.

## Authentication Methods

The cryptographic module provides authentication relying upon username/passwords or an RSA 2048-bit (at a minimum) digital signature verification.

| Role | Authentication Method | Authentication Strength |
|---|---|---|
| CO and User password<br>(Identity-based) | Username and Password<br><br>(Passwords shall be at least eight (8) characters long, and the password character set is ASCII characters 32-127, which is 96 ASCII characters, hence, the probability is 1 in 96^8) | The probability is 1 in 96^8, which is less than one in 1,000,000 that a random attempt will succeed, or a false acceptance will occur for each attempt (This is also valid for RADIUS shared secret keys). After three (3) successive unsuccessful password verification tries, the cryptographic module pauses for one second before additional password entry attempts can be reinitiated<br><br>This makes the probability approximately 180/96^8 = 2.5E-14, which is less than one in 100,000 that a random attempt will succeed, or a false acceptance will occur in a one-minute period |
| User RSA 2048-bit (minimum) digital signature<br>(Identity-based) | Digital Signature<br><br>(A 2048-bit RSA digital signature has a strength of 112-bits; hence the probability is 1/2^112) | The probability that a random attempt will succeed, or a false acceptance will occur is 1/2^112, which is less than 1 in 1,000,000. Due to processing and network limitations, the module can verify at most 300 signatures in a one-minute period. Thus, the probability that a random attempt will succeed, or a false acceptance will occur in a one-minute period is 300/2^112 = 5.8E-32, which is less than 1 in 100,000 |
| Unauthenticated | N/A | N/A |

Table 9 – Roles and Authentication

## Services

### Crypto Officer Services

The Crypto Officer role is authenticated using the credentials of the "Administrator" user, which is the member of "SonicWALL Administrators" group (also referred to as "Admin"), or the credentials of other members (users) of the "SonicWALL Administrators" group. The use of "SonicWALL Administrators" provides identification of specific users (i.e., by username) upon whom is imparted full administrative privileges. The Cryptographic Officer role can show all status and configure cryptographic algorithms, cryptographic keys, certificates, and servers used for VPN tunnels. The Crypto Officer sets the rules by which the module encrypts, and decrypts data passed through the VPN tunnels. The authentication mechanisms are discussed in Table 9.

The modes of access shown in the table is defined as:

- G = Generate: The module generates or derives the SSP.
- R = Read: The SSP is read from the module (e.g. the SSP is output).
- W = Write: The SSP is updated, imported, or written to the module.
- E = Execute: The module uses the SSP in performing a cryptographic operation.
- Z = Zeroise: The module zeroises the SSP

| Service[4] | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| Show Status | Monitoring, pinging, traceroute, viewing logs | N/A | N/A | Crypto Officer, User, Unauthenticated (LED activity/Console) | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Show Non-critical Configuration | "Show" commands that enable the operator to view VPN tunnel status and network configuration parameters | N/A | N/A | Crypto Officer, User | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |

[4] The same services are available in the non-Approved mode of operation. In the non-Approved mode of operation, the non-Approved functions listed in Tables 4 and 5 can be utilized.

| Service[4] | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| Monitor Network Status | Monitor the network status | N/A | N/A | Crypto Officer, User | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = “FIPS” |
| Crypto Officer Log On | Logs the CO into the module | N/A | Password | Crypto Officer | E | Approved Mode Checkbox Checked in WebUI |
| User Log On | Logs the User into the module | RSA | Authentication Public Key | User | E | Approved Mode Checkbox Checked in WebUI, Show Status = “FIPS” |
| Crypto Officer Log Off | Logs the CO off the module | N/A | N/A | Crypto Officer | E | Approved Mode Checkbox Checked in WebUI, Show Status = “FIPS” |
| User Log Off | Logs the User off the module | N/A | N/A | User | E | Approved Mode Checkbox Checked in WebUI, Show Status = “FIPS” |

| Service[4] | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| Clear Log | Clears session log | N/A | N/A | Crypto Officer | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Export Log | Export session log | N/A | N/A | Crypto Officer, User | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Import/Export Certificates | Session key management | RSA, ECDSA | Root CA Public Key | Crypto Officer | E, R | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Filter Log | Session log management | N/A | N/A | Crypto Officer, User | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Setup DHCP Server[5] | Setup and configure a DHCP Server | N/A | N/A | Crypto Officer | N/A | Approved Mode Checkbox Checked |

| Service[4] | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| | | | | | | in WebUI, Show Status = "FIPS" |
| Generate Log Reports | Generate Log Reports | N/A | N/A | Crypto Officer, User | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Configure VPN Settings | System configuration, network configuration, Security services including initiating encryption, key management, and VPN tunnels | Shared Secret, RSA or ECDSA | Preshared Key, IKE Private Key, Root CA Public Key, IKE Public Key | Crypto Officer | G, W | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| IPsec VPN | Network traffic over an IPsec VPN | Shared Secret, AES, HMAC, RSA or ECDSA, KAS-FFC-SSC, KAS-ECC-SSC, DRBG | IKE Shared Secret, SKEYID, SKEYID_d, SKEYID_a, SKEYID_e, Preshared Key, IKE Session Encryption Key, IKE Session Authentication Key, IKE Private Key, | Crypto Officer, User | G, W, E | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |

| Service[4] | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| | | | IPsec Session Encryption Key, Ipsec Session Authentication Key, DH/ECDH Private Key, DRBG V and C values, DRBG seed, Entropy Input, RADIUS Shared Secret, Storage Key | | | |
| TLS | TLS used for the https configuration tool or network traffic over a TLS VPN | DRBG, RSA or ECDSA, AES, HMAC, KAS-FFC-SSC, KAS-ECC-SSC | TLS Master Secret, TLS Premaster Secret, TLS Extended Master Secret (TLS 1.2), TLS Private Key, TLS Session Key, TLS Integrity Key, ECDH Private Key, DRBG V and C values, DRBG seed, Entropy Input, TLS Public Key, ECDH Public Key | Crypto Officer, User | G, W, E | Approved Mode Checkbox Checked in WebUI, Show Status = “FIPS” |
| Set Content Filter | Network configuration settings | N/A | N/A | Crypto Officer | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = “FIPS” |

| Service[4] | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| Configure DNS Settings | Configure DNS Settings | N/A | N/A | Crypto Officer, User | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Configure Access | Configure User and Crypto Officer access | Password | Password | Crypto Officer | W | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Zeroize | Zeroize SSPs | N/A | All SSPs | Crypto Officer | Z | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Perform Self tests on-demand | Perform Self tests on-demand | N/A | N/A | Crypto Officer, Unauthenticated (power-cycle) | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |
| Self-Initiated Cryptographic Output | This service is enabled for IPSec VPN. As part of enabling this | Shared Secret, HMAC, AES, RSA or ECDSA, | IKE Shared Secret, SKEYID, SKEYID_d, SKEYID_a, | Crypto Officer | G, E | Approved Mode Checkbox Checked in |

| Service[4] | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| | service, the CO must configure and enable the IPSec VPN client policy, and then turn on the "Enable Keep Alive" switch under the "Advanced" tab in the VPN Policy settings. | KAS-FFC-SSC, KAS-ECC-SSC, DRBG | SKEYID_e, Preshared Key, IKE Session Encryption Key, IKE Session Authentication Key, IKE Private Key, IPsec Session Encryption Key, Ipsec Session Authentication Key, DH/ECDH Private Key, DRBG V and C values, DRBG seed, Entropy Input, Root CA Public Key, IKE Public Key, Peer IKE Public Key, DH/ECDH Public Key | | | WebUI, Show Status = “FIPS” |
| Module Reset | Firmware removal with configuration returned to factory state | N/A | N/A | Unauthenticated | Z | Approved Mode Checkbox Checked in WebUI, Show Status = “FIPS” |

| Service[4] | Description | Approved Security Functions | Keys and/or SSPs | Roles | Access rights to Keys and/or SSPs | Indicator |
|---|---|---|---|---|---|---|
| No Auth Function | Power Cycle, Cable Plugin, View LEDs | N/A | N/A | Unauthenticated | N/A | Approved Mode Checkbox Checked in WebUI, Show Status = "FIPS" |

Table 10 – Approved Services

| Service | Description | Algorithms Accessed | Role | Indicator |
|---|---|---|---|---|
| Show Status | Monitoring, pinging, traceroute, viewing logs | | Crypto Officer, User, Unauthenticated (LED activity/Console) | Approved Mode Checkbox Unchecked in WebUI, Show Status = "NO FIPS" |
| Show Non-critical Configuration | "Show" commands that enable the operator to view VPN tunnel status and network configuration parameters | | Crypto Officer, User | Approved Mode Checkbox Unchecked in WebUI, Show Status = "NO FIPS" |
| Monitor Network Status | Monitor the network status | | Crypto Officer, User | Approved Mode Checkbox Unchecked in WebUI, Show Status = "NO FIPS" |
| Crypto Officer Log On | Logs the CO into the module | | Crypto Officer | Approved Mode Checkbox Unchecked in |

| Service | Description | Algorithms Accessed | Role | Indicator |
|---|---|---|---|---|
| | | | | WebUI, Show Status = “NO FIPS” |
| Crypto Officer Log Off | Logs the CO off the module | | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Clear Log | Clears session log | | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Export Log | Export session Log | | Crypto Officer, User | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Import/Export Certificates | Session key management | RSA or DSA | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Filter Log | Session log management | | Crypto Officer, User | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Setup DHCP Server | Setup and configure a DHCP Server | | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |

| Service | Description | Algorithms Accessed | Role | Indicator |
|---|---|---|---|---|
| Generate Log Reports | Generate Log Reports | | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Configure VPN Settings | System configuration, network configuration, Security services including initiating encryption, key management, and VPN tunnels. | RSA or ECDSA | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| IPsec VPN | Network traffic over an IPsec VPN | AES, HMAC, RSA or ECDSA, KAS-FFC-SSC, KAS-ECC-SSC, DRBG | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| TLS | TLS used for the https configuration tool or network traffic over a TLS VPN | DRBG, RSA or ECDSA, AES, HMAC, KAS-FFC-SSC, KAS-ECC-SSC | Crypto Officer, User | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Set Content Filter | Network configuration settings | | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Configure DNS Settings | Configure DNS Settings | | Crypto Officer, User | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |

| Service | Description | Algorithms Accessed | Role | Indicator |
|---|---|---|---|---|
| Configure Access | Configure User and CO access | | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Zeroize | Zeroize SSPs | | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Perform Self tests on-demand | Perform Self tests on-demand | | Crypto Officer, Unauthenticated | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Self-Initiated Cryptographic Output | This service is enabled for IPSec VPN. As part of enabling this service, the CO must configure and enable the IPSec VPN client policy, and then turn on the Enable Keep Alive switch under the Advanced tab in the VPN Policy settings | HMAC, AES, RSA or ECDSA, KAS-FFC-SSC, KAS-ECC-SSC, DRBG | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| User Log On | Logs the User into the module | RSA | User | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |

| Service | Description | Algorithms Accessed | Role | Indicator |
|---|---|---|---|---|
| User Log Off | Logs the User off the module | | User | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Module Reset | Firmware removal with configuration returned to factory state | | Unauthenticated | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| No Auth Function | Power Cycle, Cable Plugin, View LEDs | | Unauthenticated | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| Firmware Update | Upgrade Module Firmware | | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| SSH | SSH Service | SSH-KDF, SHA2-256, SHA2-512, Hash_DRBG, KAS-ECC-SSC, AES-GCM, RSA SigGen | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |
| SNMP | SNMP Service | SNMP-KDF | Crypto Officer | Approved Mode Checkbox Unchecked in WebUI, Show Status = “NO FIPS” |

Table 11 – non-Approved Services

# 5. Software/Firmware Security

The module is a hardware module with firmware (SonicOS/X 7.0.1) running on it. The Module uses SHA2-256 (Cert. #A6598) performed over all module firmware as the integrity technique/EDC. The operator can initiate the integrity test on demand by power cycling the module. The temporary values generated during the integrity test are cleared automatically by the module from the memory after the test is completed.

The module does not support the external loading of firmware in the Approved mode of operation.

# 6. Operational Environment

The module operates in a non-modifiable operational environment per FIPS 140-3 specifications, as the module does not support external firmware loading.

# 7. Physical Security

The chassis of the multi-chip standalone cryptographic modules are opaque within the visible spectrum, and direct observation of the modules' internal components is not possible. The chassis are sealed with either 1 or 2 tamper-evident seals (depending on model), applied during manufacturing. The physical security of the module is intact if there is no evidence of tampering with the tamper-evident seal(s).

| Physical Security Mechanism | Recommended Frequency of Inspection | Inspection Guidance Details |
|---|---|---|
| Tamper-evident seals | Periodic inspection of tamper-evident seals once every 6 months | If evidence of tamper is found, the Cryptographic Officer is requested to follow their internal IT policies, which may include contacting SonicWALL for replacing the unit |

Table 12 – Physical Security Inspection Guidelines

Table 13 below lists the number of tamper-evident seals applied per model:

| # | Model | Number of tamper-evident seals(s)/module |
|---|---|---|
| 1 | NSa 4700 | 341-000041-51 (1pcs) and 341-000029-51 (1pcs) |
| 2 | NSa 5700 | 341-000041-51 (1pcs) and 341-000029-51 (1pcs) |
| 3 | NSa 6700 | 341-000041-51 (1pcs) and 341-000029-51 (1pcs) |
| 4 | NSsp 10700 | 341-000041-51 (1pcs) and 341-000029-51 (2pcs) |
| 5 | NSsp 11700 | 341-000041-51 (1pcs) and 341-000029-51 (2pcs) |
| 6 | NSsp 13700 | 341-000041-51 (1pcs) and 341-000029-51 (2pcs) |

Table 13 – Number of Tamper-Evident Seals

The locations of the tamper-evident seals (highlighted by red rectangles) are indicated in Figure 10 (below):

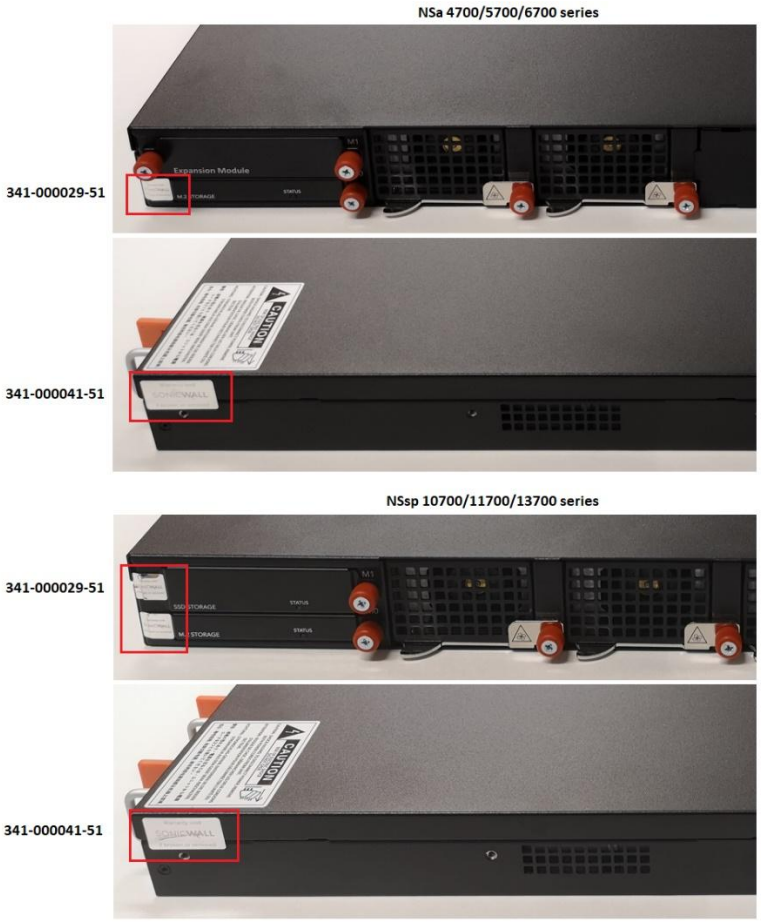


Figure 10. Tamper-evident seal placements for NSa 4700/5700/6700 and NSsp 10700/11700/13700

# 8. Non-Invasive Security

Not Applicable. The module does not implement non-invasive security measures.

# 9. Sensitive Security Parameter Management

All SSPs used by the Module are described in this section.

| Key/SSP Name/Type | Strength | Security Function and Cert. Number | Generation | Import/ Export | Establishment | Storage | Zeroisation | Use & related keys |
|---|---|---|---|---|---|---|---|---|
| IKE Shared Secret | String: 32 - 256 bytes | Shared Secret A6598 | Generated Internally | Neither Input nor Output | Established as a part of IKE exchange process | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or IKE session termination | Shared secret used during IKE Phase 1 |
| SKEYID | 256, 384 or 512-bits | IKE KDF HMAC A6598 | Generated Internally | Neither Input nor Output | Established as a part of IKE exchange process | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or IKE session termination | Secret value used to derive other IKE secrets |
| SKEYID_d | 256, 384 or 512-bits | IKE KDF HMAC A6598 | Generated Internally | Neither Input nor Output | Established as a part of IKE exchange process | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or IKE session termination | Secret value used to derive keys for security associations |
| SKEYID_a | 256, 384 or 512-bits | IKE KDF HMAC A6598 | Generated Internally | Neither Input nor Output | Established as a part of IKE exchange process | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or IKE session termination | Secret value used to derive keys to authenticate IKE messages |

| Key/SSP Name/Type | Strength | Security Function and Cert. Number | Generation | Import/ Export | Establishment | Storage | Zeroisation | Use & related keys |
|---|---|---|---|---|---|---|---|---|
| SKEYID_e | 256, 384 or 512-bits | IKE KDF HMAC A6598 | Generated Internally | Neither Input nor Output | Established as a part of IKE exchange process | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or IKE session termination | Secret value used to derive keys to encrypt IKE messages |
| Preshared Key | A minimum of 8 characters | IKE KDF A6598 | Not Applicable | Input electronically | Not Applicable | Flash (Encrypted by AES CBC 256-bit) | Zeroize Service | Used to authenticate the module to a peer during IKE |
| IKE Session Encryption Key | 128, 192 or 256-bit | IKE KDF AES (CBC) A6598 | Generated Internally during SSP establishment | Neither Input nor Output | Established as a part of IKE exchange process (SP800-56a rev3 and SP800-135 KDF) | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or IKE session termination | Used to establish phase 2 tunnel |
| IKE Session Authentication Key | 256, 384 or 512-bits | IKE KDF HMAC A6598 | Generated Internally during SSP establishment | Neither Input nor Output | Established as a part of IKE exchange process (SP800-56a rev3 and SP800-135 KDF) | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or IKE session termination | Used to establish phase 2 tunnel |
| IKE Private Key | 2048-bit or P-256, P-384 or P-521 | RSA or ECDSA CKG A6598 | Generated as per SP800-90A DRBG and FIPS 186-5 compliant RSA or ECDSA key generation | Neither Input nor Output | Not Applicable | Flash (Plaintext) | Zeroize Service | Used as a part of IKE process |

| Key/SSP Name/Type | Strength | Security Function and Cert. Number | Generation | Import/ Export | Establishment | Storage | Zeroisation | Use & related keys |
|---|---|---|---|---|---|---|---|---|
| IPsec Session Encryption Key | 128, 192 or 256-bit | AES (CBC) A6598 | Generated Internally during SSP establishment | Neither Input nor Output - | Established as a part of IKE exchange process (SP800-56a rev3 and SP800-135 KDF) | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or IPsec session termination | Used to encrypt data |
| IPsec Session Authentication Key | 256, 384 or 512-bits | HMAC A6598 | Generated Internally during SSP establishment | Neither Input nor Output | Established as a part of IKE exchange process (SP800-56a rev3 and SP800-135 KDF) | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or IPsec session termination | Used for data authentication for IPsec traffic |
| TLS Master Secret | 384-bits | TLS A6598 | Generated Internally during TLS handshake process | Neither Input nor Output | Established as a part of TLS handshake process | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or the TLS session termination | Used for the generation of TLS Session Keys and TLS Integrity Key |
| TLS Extended Master Secret | 384-bits | TLS 1.2 A6598 | Generated Internally during TLS handshake process | Neither Input nor Output | Established as a part of TLS handshake process | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or the TLS session termination | Binds the master secret to the full handshake context |
| TLS Premaster Secret | 384-bits | TLS A6598 | Generated Internally during TLS handshake process | Neither Input nor Output | Established as a part of TLS handshake process | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or the TLS | Used for the generation of Master Secret |

| Key/SSP Name/Type | Strength | Security Function and Cert. Number | Generation | Import/ Export | Establishment | Storage | Zeroisation | Use & related keys |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | session termination | |
| TLS Session Key | TLS 1.2: 128 or 256-bit and 128 or 256-bit<br><br>TLS 1.3: 128 or 256-bit | TLS 1.2: AES CBC<br><br>AES GCM<br><br>TLS 1.3: AES-GCM<br><br>A6598 | Generated Internally during SSP establishment | Neither Input nor Output | Established as a part of TLS exchange process (SP800-56a rev3 and SP800-135 KDF/TLS 1.3 KDF) | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or the TLS session termination | Used to protect TLS 1.2 connection<br><br>Used to protect TLS 1.3 connection |
| TLS Integrity Key | TLS 1.2: 160/256/384-bit<br><br>TLS 1.3: 256/384-bit | TLS 1.2/ TLS 1.3 HMAC A6598 | Generated Internally during SSP establishment | Neither Input nor Output | Established as a part of TLS exchange process (SP800-56a rev3 and SP800-135 KDF/TLS 1.3 KDF) | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or the TLS session termination | Used to check the integrity of TLS 1.2 connection<br><br>Used to check the integrity of TLS 1.3 connection |
| TLS Private Key | 2048-bit or P-256, P-384 or P-521 | RSA or ECDSA CKG A6598 | Generated as per SP800-90A DRBG and FIPS 186-5 compliant RSA or ECDSA key generation | Neither Input nor Output | Not Applicable | Flash (Plaintext) | Zeroize Service | Used in the TLS 1.2/TLS 1.3 signature algorithm |
| Diffie-Hellman/EC | IKE: Diffie-Hellman Private Key | KAS-SSC CKG A6598 | Generated as per SP800-90A DRBG and FIPS 186-4 compliant | Neither Input nor Output | Not Applicable | Temporarily in RAM | Zeroize Service, Power | Used within IKE key agreement |

| Key/SSP Name/Type | Strength | Security Function and Cert. Number | Generation | Import/ Export | Establishment | Storage | Zeroisation | Use & related keys |
|---|---|---|---|---|---|---|---|---|
| Diffie-Hellman Private Key | (N = 224, 256) or EC DH P-256/P-384/P-521<br><br>TLS: EC DH P-256/P-384/P-521 | | DSA or 186-5 compliant ECDSA key generation | | | (Plaintext) | Cycle or the TLS/IKE session termination | Used within TLS key agreement |
| DRBG Internal State | 256-bits | Hash_DRBG A6598 | Generated Internally | Neither Input nor Output | Not Applicable | Temporarily in RAM (Plaintext) | Zeroize Service or Power Cycle | The values of V and C are the “secret values” of the internal state |
| DRBG Seed | 256-bits | Hash_DRBG A6598 | Intel® Digital Random Number Generator SP800-90B | Neither Input nor Output | Not Applicable | Temporarily in RAM (Plaintext) | Zeroize Service or Power Cycle | Used to seed the Approved DRBG |
| Entropy Input | 256-bits security strength | Hash_DRBG A6598 | Intel® Digital Random Number Generator SP800-90B | Neither Input nor Output | Not Applicable | Temporarily in RAM (Plaintext) | Zeroize Service or Power Cycle | Entropy (min) input used to instantiate the DRBG |
| RADIUS Shared Secret | A minimum of 8 characters for RADIUS authentication | Shared Secret A6598 | Not Applicable | Input electronically and output via IPsec | Not Applicable | Flash (Encrypted by AES CBC 256-bit) | Zeroize Service | Used for authenticating the RADIUS server to the module and vice versa via IPSec |

| Key/SSP Name/Type | Strength | Security Function and Cert. Number | Generation | Import/ Export | Establishment | Storage | Zeroisation | Use & related keys |
|---|---|---|---|---|---|---|---|---|
| Passwords (hashed) | A minimum of 8 ASCII characters. | Not Applicable | Not Applicable | Entered electronically | Not Applicable | Flash (Encrypted by AES CBC 256-bit) | Zeroize Service | Authentication data |
| Storage Key | 256-bit Key | AES CBC CKG A6598 | Generated as per SP800-90A DRBG | Neither Input nor Output | Not Applicable | Flash (Plaintext) | Zeroize Service | For encrypting RADIUS Shared Secret, Passwords and Preshared Key |
| **Public Keys** | | | | | | | | |
| Root CA Public Key | 2048-bit or P-256, P-384 or P-521 | RSA or ECDSA A6598 | Not Applicable | Input electronically via IPsec. Not output | Not Applicable | Flash (Plaintext) | Zeroize Service | Used for verifying a chain of trust for receiving certificates |
| Peer IKE Public Key | 2048-bit or P-256, P-384 or P-521 | RSA or ECDSA A6598 | Not Applicable | Input electronically Not output | During IKE negotiation | RAM (Plaintext) | Zeroize Service, Power Cycle or IKE session termination | Used for verifying digital signatures from a peer device |
| IKE Public Key | 2048-bit or P-256, P-384 or P-521 | RSA or ECDSA A6598 | Generated as per SP800-90A DRBG and FIPS 186-5 compliant RSA or ECDSA key generation | Not Input. Output electronically during IKE negotiation | During IKE negotiation | Flash (Plaintext) | Zeroize Service | Used for verifying digital signatures from a peer device |

| Key/SSP Name/Type | Strength | Security Function and Cert. Number | Generation | Import/ Export | Establishment | Storage | Zeroisation | Use & related keys |
|---|---|---|---|---|---|---|---|---|
| Diffie-Hellman/EC Diffie-Hellman Public Key | IKE: Diffie-Hellman Public Key (N = 224, 256) or EC DH P-256/P-384/P-521<br><br>TLS: EC DH P-256/P-384/P-521 | KAS-SSC A6598 | Generated as per SP800-90A DRBG and FIPS 186-4 compliant DSA or 186-5 compliant ECDSA key generation | Not Input. Electronic output during IKE negotiation | During IKE negotiation | Temporarily in RAM (Plaintext) | Zeroize Service, Power Cycle or the TLS/IKE session termination | Used within IKE key agreement<br><br>Used within TLS key agreement |
| Authentication Public Key | 2048-bit | RSA A6598 | Not Applicable | Input electronically over CLI. No output | Not Applicable | Temporarily in RAM (Plaintext) | Zeroize Service | Used to authenticate the User |
| TLS Public Key | 2048-bit or P-256, P-384 or P-521 | RSA or ECDSA A6598 | Generated as per SP800-90A DRBG and FIPS 186-5 compliant RSA or ECDSA key generation | Electronically Output during TLS handshake | During TLS Handshake | Flash (Plaintext) | Zeroize Service | Used in the TLS handshake |

Table 14 – SSPs

**Note:** The keys are explicitly zeroized by the module when the zeroize service is executed and are implicitly zeroized when power cycling or the termination of the IPsec, IKE, and/or TLS sessions.

| Entropy sources | Minimum number of bits of entropy | Details |
|---|---|---|
| Intel® Digital Random Number Generator SP800-90B<br><br>ESV Certificate: E164 | 0.6 | The module supports the Intel® Digital Random Number Generator SP800-90B as the module's noise source, outputting full entropy. (The entropy source supports a vetted conditioning component consistent with NIST SP 800-90B, Section 3.1.5.1.1.) The noise source is the root of security for the entropy source and for the DRBG as a whole<br><br>The noise source (internal to the Intel CPUs) is a circuit that employs a feedback-stabilized metastable latch to generate entropic binary data by measuring the resolution state of the latch after exiting metastability. The feedback is used to keep the metastable latch balanced so that thermal noise will drive the resolution process |

Table 15 – Non-Deterministic Random Number Generator Specification

# 10. Self-Tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests. The pre-operational self-tests are performed and shall pass successfully prior to the module providing any data output via the data output interface. CASTs are performed on the condition that the pre-operational self-test complete successfully. Other conditional self-tests are performed when an applicable security function or process is invoked. If the module fails a self-test, the module enters the error state and outputs the error message. The module does not perform any cryptographic operations, and data output is inhibited while in the error state.

Self–tests (CASTs) are available on demand by power cycling the module.

## Pre-Operational Self-Tests

- Firmware Integrity Test: SHA2-256 (256-bit EDC)

## Conditional Self-Tests

Cryptographic Algorithm Self Tests

- AES-CBC Decrypt CAST
- AES GCM Encrypt CAST
- AES GCM Decrypt CAST
- CVL: IKEv1 KDF CAST
- CVL: IKEv2 KDF CAST
- CVL: TLS 1.2 KDF CAST
- CVL: TLS 1.3 KDF CAST
- DRBG: SP 800-90A Section 11.3 Health Tests (Instantiate, Generate, Reseed)
- DSA CAST (Pairwise Consistency Test)
- ECDSA Signature Generation CAST
- ECDSA Signature Verification CAST
- HMAC-SHA-1 CAST
- HMAC-SHA2-256 CAST
- HMAC-SHA2-384 CAST
- HMAC-SHA2-512 CAST
- KAS-FFC-SSC Primitive “Z” CAST (SP 800-56Arev3)
- KAS-ECC-SSC Primitive “Z” CAST (SP 800-56Arev3)
- RSA Signature Generation CAST (Key size: 2048)
- RSA Signature Verification CAST (Key size: 2048)
- SHA-1 CAST
- SHA2-256 CAST
- SHA2-384 CAST
- SHA2-512 CAST
- NIST SP 800-90B Start-Up Health Tests
- NIST SP 800-90B Continuous Health Tests

Conditional Pairwise Consistency Tests

- ECDSA Pairwise Consistency Test
- DSA Pairwise Consistency Test
- RSA Pairwise Consistency Test

If any of the tests described above fail, the cryptographic module enters the error state. No security services are provided in the error state. No cryptographic output is started until all tests are successfully completed. This effectively inhibits the data output interface. When all tests are completed successfully, the Test LED is turned off.

# 11. Life-Cycle Assurance

## Crypto Officer Guidance

The following steps shall be performed by the Crypto Officer (CO) to configure the required roles and place the module in the Approved mode of operation:

1. Apply power to the module. On a GPC, connect to the module's console using the serial port. The network interface drivers/login prompt will only be available once all power-up self-tests have completed successfully.

2. Login using the vendor provided default login and password. The default password and login shall be changed/updated.

3. Configure management IP address and Gateway.

4. Over the web interface, proceed to system settings and update the settings to be consistent with Section 2 of this document with the assistance of compliance checking procedure and then enabling Approved mode using the checkbox. The FIPS checkbox does not place the module in Approved mode until the settings in the Modes of Operation Section are met. Then click OK. The system automatically restarts.

5. Observe that the module self-tests execute automatically before a log in is possible. Observe that the "FIPS enabled checkbox" is checked/enabled to indicate that the module is in the Approved mode of operation. This can be verified in the system/settings page. In addition, on the dashboard, the operator can verify the version of the module.

6. Proceed to create the roles specified in Section 4 of this document. Passwords and Digital signatures required for authentication to each role should be configured or installed as appropriate.

*Note 1: When the "Approved mode" checkbox is selected, the module executes a compliance checking procedure, examining all settings related to the security rules described previously in this document. The operator is responsible for updating these settings appropriately during setup and will be prompted by the compliance tool if a setting has been modified, taking the module out of compliance. The "Approved mode" checkbox and corresponding system flag ("fips") which can be queried over the console will not be

set unless all settings are compliant. The "Approved mode" checkbox and “fips” system flag are indicators that the module is running in the Approved mode of operation.

*Note 2: The keys and SSPs generated in the cryptographic module during Approved mode of operation shall not be used when the module transitions to non-Approved mode and vice versa. While the module transitions from Approved to non-Approved mode or from non-Approved to Approved mode, all SSPs shall be zeroized by the Crypto Officer using the “Zeroize” service. If transitioning from the non-Approved to Approved mode, the CO shall zeroize all plaintext keys and SSPs by issuing “Zeroize” service and then the CO shall follow the CO Guidance (above) in this section to place the module in Approved mode of operation.

## Configuration Management

SonicWall uses Perforce software for the management of source code artifacts and for hardware and documentation version control.

KlocWork is used for static code analysis.

The module is developed using high level programming languages C++ and C. Assembly code is only used for select performance enhancements.

The module is securely delivered from Sonicwall to customers via the mechanism specified by the customer. FedEx, UPS, or any other freight forwarder of their choice can be utilized. Tracking numbers are used to track and confirm delivery to the authorized operator. The Crypto Officer should check the package for any irregular tears or openings. If the Crypto Officer suspects tampering has occurred, they should immediately contact Sonicwall, Inc.

The end of life for the module meets the FIPS 140-3 requirements. The sanitization requirements are met by zeroising the module.

# 12. Mitigation of Other Attacks

The SonicWall NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, and NSsp 13700 are capable of mitigating other attacks using the following features (dependent on licensing).

**Capture ATP**

The Capture ATP Service revolutionizes advanced threat detection and sandboxing with a cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway. Capture ATP blocks zero-day attacks before they enter your network. It lets you establish advanced protection against the changing threat landscape and analyze a broad range of file types.

**Gateway Anti-Virus**

ICSA-certified Gateway Anti-Virus protection combines network-based anti-malware with a dynamically updated cloud database of tens of millions of malware signatures. Dynamic spyware protection blocks the installation of malicious spyware and disrupts existing spyware communications.

**IPS**

Cutting-edge IPS technology protects against worms, trojans, software vulnerabilities and other intrusions by scanning all network traffic for malicious or anomalous patterns, thereby increasing network reliability and performance.

**Comprehensive Anti-Spam Service**

SonicWall Comprehensive Anti-Spam Service offers small-to medium sized businesses >99% effectiveness against spam, dropping >80% of spam at the gateway, while utilizing advanced anti-spam techniques like Adversarial Bayesian™ and machine-learning filtering.

**DNS Filtering**

DNS filtering blocks malicious websites or applications at the DNS layer to filter out harmful or inappropriate content without enabling TLS decryption and adversely affecting performance.

**Network Access Control**

Network access control integration provides network access control for SonicWall customers by integrating with Aruba ClearPass, giving you comprehensive and precise profiling, authentication, and authorization for systems and devices trying to access your IT resources. SonicOS provides a RESTful API that will support Aruba ClearPass as NAC to integrate with SonicWall NGFW. This architecture will turn static security into contextual security to provide more flexible and advanced security protection.

**Content Filtering Service**

Content Filtering Services (CFS) lets you enforce Internet use policies and control internal access to inappropriate, unproductive and potentially illegal web content with comprehensive content filtering. Reputation-based CFS 5.0 provides a reputation score that forecasts the security risk of a URL across 93 web categories.

**Other**

The modules also include basic DNS security, deep packet inspection for SSL, and a botnet service.

## References and Definitions

The following standards are referred to in this Security Policy.

| Abbreviation | Full Specification Name |
|---|---|
| [FIPS140-3] | *Security Requirements for Cryptographic Modules*, March 22, 2019 |
| [IG] | *Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program* |
| [108] | *NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised)*, *October 2009* |
| [131Arev2] | *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, *March 2019* |
| [132] | *NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications*, *December 2010* |
| [133rev2] | *NIST Special Publication 800-133rev2, Recommendation for Cryptographic Key Generation*, *June 2020* |
| [135rev1] | *National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1*, *December 2011.* |
| [186-4] | *National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4*, *July, 2013.* |
| [186-5] | *National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5*, February 2023 |
| [186-2] | *National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2*, *January 2000.* |
| [197] | *National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197*, *November 26, 2001* |
| [198] | *National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1*, *July, 2008* |
| [180-4] | *National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4*, *August, 2015* |
| [202] | *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202*, *August 2015* |
| [38A] | *National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A*, *December 2001* |

| Abbreviation | Full Specification Name |
|---|---|
| [38B] | *National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005 (Updated 10/6/2016)* |
| [38C] | *National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004 (Updated 7/20/2007)* |
| [38D] | *National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007* |
| [56Arev3] | *NIST Special Publication 800-56A (rev3), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018* |
| [56Br2] | *NIST Special Publication 800-56B Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, March 2019* |
| [67rev2] | *National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, November 2017* |
| [90Arev1] | *National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.* |
| [90B] | *Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018* |

Table 16 – References

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| CBC | Cipher Block Chaining |
| DH | Diffie-Hellman |
| DRBG | Deterministic Random Bit Generator |
| FIPS | Federal Information Processing Standard |
| GUI | Graphical User Interface |
| HMAC | Hashed Message Authentication Code |
| IKE | Internet Key Exchange |
| IPSec | Internet Protocol Security |
| RADIUS | Remote Authentication Dial-In User Service |
| RSA | Rivest, Shamir, Adleman asymmetric algorithm |
| SHA | Secure Hash Algorithm |

| Acronym | Definition |
|---|---|
| SSP | Sensitive Security Parameter |
| TACACS+ | Terminal Access Controller Access-Control System Plus |
| Triple-DES | Triple Data Encryption Standard |
| VPN | Virtual Private Network |

Table 17 – Acronyms and Definitions