SonicWall, Inc.
SonicWALL Network Security Virtual Appliances

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.0

Date: February 2, 2022

Level 1

Copyright Notice

Table of Contents

List of Tables

List of Figures

1. Introduction

This document defines the Security Policy for the SonicWALL Network Security Virtual Appliances Firewall Series, hereafter denoted the module. 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 140-2 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.

The Module (NSv 270, NSv 470 and NSv 870) runs on many different UCS Servers with various hypervisors. The firmware modules included in this validation are comprised of an OVA package file "SonicWALL_NSV_270.ova" for the NSv 270, "SonicWALL_NSV_470.ova" for the NSv 470 and "SonicWALL_NSV_870.ova" for the NSv 870. The module firmware version for all tested models is SonicOSX 7.0 or SonicOSX referred in this document as NSv.

For the purpose of this validation, the module was tested on the following servers:

Table 1 – Cryptographic Module List

	OS/Model	Tested Platforms	Hypervisor	Processor
1	SonicOSX 7.0 (NSv 270, NSv 470 and NSv 870)	Dell PowerEdge R740	VMWare ESXi 6.7	Intel Xeon Platinum 8260 (Cascade Lake)
2	SonicOSX 7.0 (NSv 270, NSv 470 and NSv 870)	Dell PowerEdge R740	VMWare ESXi 7.0	Intel Xeon Platinum 8260 (Cascade Lake)

The following platforms have not been tested as part of the FIPS 140-2 level 1 certification, however SonicWALL "vendor affirms" that these platforms are equivalent to the tested and validated platform. Additionally, SonicWALL affirms that the module will function the same way and provide the same security services on the following Hypervisors/Cloud listed below:

- ESXi 5.0
- ESXi 5.5
- ESXi 6.0
- AWS
- HYPERV
- AZURE
- KVM

The above vendor affirmed platforms were not tested for this FIPS 140-2 validation. As per FIPS 140-2 Implementation Guidance G.5, compliance is maintained for other versions of the respective operational environments where the module binary is unchanged. Please note that the above porting is only permitted when the operating system of the module is unchanged and in the case of this module

validation, the operating system is defined as a part of the logical boundary and is unchanged when it is run on the above-mentioned vendor affirmed platforms.

CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when so ported if the specific operational environment is not listed on the validation certificate.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall Level	1

The overall FIPS 140-2 validation level for the module is Security Level 1.

1.1 Module Description and Cryptographic Boundary

The cryptographic module is defined as a multi-chip standalone firmware module. As a firmware module, the module has no physical characteristics; however, the physical boundary of the cryptographic module is defined by the hard enclosure around the tested host platform (Dell PowerEdge R740) on which it runs. The module's physical cryptographic boundary is illustrated by the green dashed line in Figure 1.

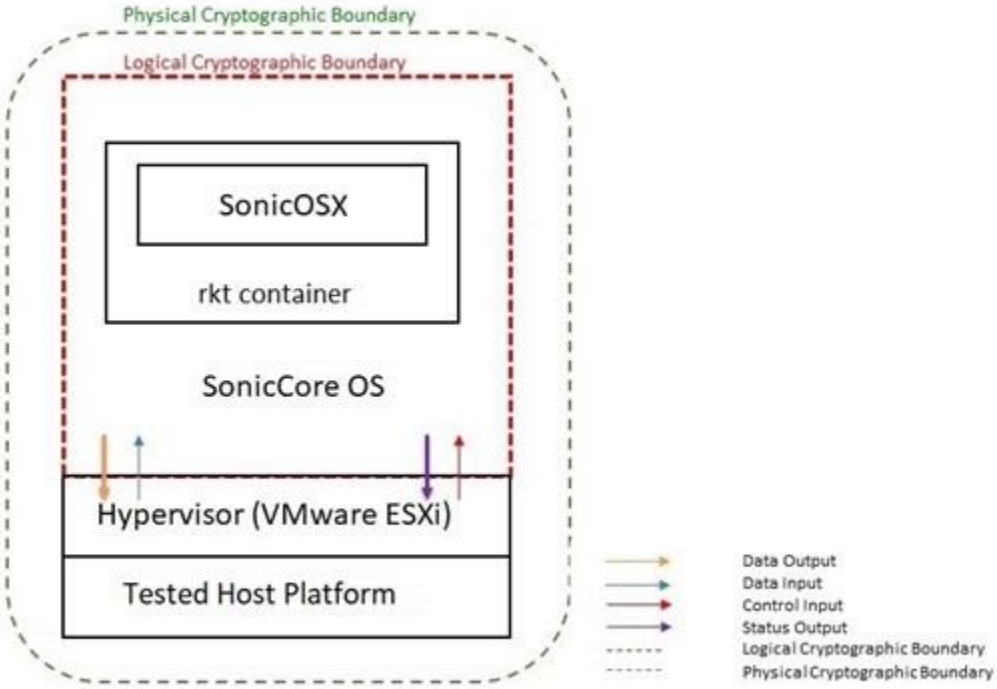

Figure 1 – Block Diagram

The module makes use of the physical interfaces of the tested platform hosting the virtual environment upon which the module is installed. The hypervisor controls and directs all interactions between the module and the operator, and is responsible for mapping the module's virtual interfaces to the tested platform's physical interfaces.

Figure 1 also shows the logical cryptographic boundary of the module executing in memory and it's interactions with the hypervisor. The logical cryptographic boundary of the module (shown by the red dashed line in Figure 1) is the SonicCore OS. The SonicCore module launches the rkt container with SonicOSX module running inside. The module interacts directly with the hypervisor, which runs directly on the tested host platform.

1.2 Ports and Interfaces

The module's ports and associated FIPS 140-2 defined logical interface categories are listed in the following table:

Table 3 – Module Interfaces

Physical Port/Interface	NSv Logical Port/Interface	FIPS 140-2 Interface
Host Platform Ethernet (10/100/1000) ports	Virtual Ethernet Ports	Data Input
Host Platform Ethernet (10/100/1000) ports	Virtual Ethernet Ports	Data Output
Host Platform Ethernet (10/100/1000) ports; Serial port	Virtual Ethernet Ports, Virtual Serial Ports	Control Input
Host Platform Ethernet (10/100/1000) ports; Serial port	Virtual Ethernet Ports, Virtual Serial Ports	Status Output

1.3 Modes of Operation

1.3.1 FIPS 140-2 Approved mode of Operation

The FIPS mode configuration can be determined by the operator, by checking the state of the "FIPS Mode" checkbox on the System/Settings page over the web interface or issuing "show fips" over the console. When the "FIPS 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 "FIPS Mode" checkbox and corresponding system flag ("fips"), which can be queried over the console, will not be set unless all settings are compliant. The "FIPS Mode" checkbox and fips system flag are indicators that the module is running in the FIPS Approved mode of operation.

The module is not configured to operate in FIPS-mode by default. The following steps must be taken during set-up of the module to enable FIPS-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 must be at least eight (8) characters.
3. Traffic between the module and the RADIUS/TACACS+ server must be secured via an IPSec tunnel.

   Note: This step need only be performed if RADIUS or TACACS+ is supported.
   - LDAP cannot be enabled in FIPS mode without being protected by TLS
   - LDAP cannot be enabled in FIPS mode without selecting 'Require valid certificate from server'
   - LDAP cannot be enabled in FIPS mode without valid local certificate for TLS

4. IKE must be configured with 3rd Party Certificates for IPsec Keying Mode when creating VPN tunnels.
   - RSA Certificates lengths must be 2048-bit or greater in size

5. When creating VPN tunnels, ESP must be enabled for IPSec.
6. FIPS-approved algorithms must be used for encryption and authentication when creating VPN tunnels.
7. Group 14, 19, 20 or 21 must be used for IKE Phase 1 DH Group. SHA-256 and higher must be used for Authentication
8. “Advanced Routing Services” must not be enabled.
9. “Group VPN management” must not be enabled.
10. SNMP or SSH must not be enabled.

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

The module does not enforce but as a policy, a user should not enable the below features while in FIPS mode of operation:

- Do not use USB interface
- Do not use TLS 1.3 KDF
- In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption must be established.

1.3.2 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 FIPS-approved algorithms which are not used in the FIPS mode of operation. The following services must be disabled before placing the module in FIPS mode. The module does not transition to FIPS 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[1]
- SNMP[2]

1.3.3 Non-Approved Algorithms with No Security Claimed

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

- Triple-DES (non-compliant)
- MD5 (non-compliant)
- PBKDF (non-complaint)

The operator must also follow the rules outlined in Section 1.3.1 and consult FIPS 140-2 IG 1.23 for further understanding the use of functions where no security is claimed. Section 3.3 indicates the module services associated with these functions.

[1] Keys derived using the SSH KDF are not allowed for use in the Approved mode.

[2] Keys derived using the SNMP KDF are not allowed for use in the Approved mode.

2. Cryptographic Functionality

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

Table 4 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
C2143	AES [197]	CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 128, 192, 256	Encrypt
		GMAC [38D]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		GCM [38D][3]	Key Sizes: 128, 192, 256 Tag Len: 128	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
Vendor Affirmed	CKG [IG D.12]	[133 rev2] Section 5.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation
		[133 rev2] Section 5.2 Asymmetric key establishment key generation using unmodified DRBG output		
		[133 rev2] Section 6.1 Direct symmetric key generation using unmodified DRBG output		
		[133 rev2] Section 6.2.1 Derivation of symmetric keys from a key agreement shared secret.		
		[133 rev2] Section 6.2.2 Derivation of symmetric keys from a pre-shared key		
		[133 rev2] Section 6.3 Combining multiple keys and other data		

[3] The module's AES-GCM implementations conforms to IG A.5 Scenario#1 following RFC 5288 for TLS. The module is compatible with TLSv1.2 and provides support for the acceptable GCM cipher suites from SP 800-52 Rev1, Section 3.3.1. Method ii) was used by the tester to demonstrate the module's compliance with the TLS provision for the AES GCM IV generation in IG A.5. The counter portion of the IV is set by the module within its cryptographic boundary. The restoration of the IV is in accordance with scenario 3 in IG A.5 in that a new AES GCM key is established. The construction of the 64-bit nonce_explicit part of the IV is deterministic via a monotonically increasing counter. The module ensures that that when the deterministic part of the IV uses the maximum number of possible values and new session key is established. The module generates new AES-GCM keys if the module loses power. This is consistent with RFC 5288. 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.

Cert	Algorithm	Mode	Description	Functions/Caveats
Vendor Affirmed	DH	KAS-SSC (SP 800-56Arev3 Shared Secret Calculation per Scenario X1 of IG D.8 and IG D.1rev3. Key Derivation per SP 800-135 (CVL Cert. #C2143) and RFC 8446)	DH group 14 (dhEphem scheme per section 6.1.2.1 of SP800-56Arev3)	Key Agreement
	ECDH		ECDH P-256, P-384 and P-521 (Ephemeral Unified scheme per section 6.1.2.2 of SP800-56Arev3)	
C2143	CVL: IKEv1 [135]	DSA, PSK[135]	SHA (256, 384, 512)	Key Derivation
	CVL: IKEv2 [135]	DH 224-521 bits	SHA (256, 384, 512)	
	CVL: TLS [135][4]	v1.0, v1.1, v1.2	SHA (256, 384, 512)	
	CVL: SSH [135]	v2	SHA-1	
	CVL:SNMP [135]		SHA-1	
C2143	DRBG [90Arev1]	Hash	SHA-256	Deterministic Random Bit Generation
C2143	DSA [186-4][5]		(L = 2048, N = 224) (L = 2048, N = 256) (L = 3072, N= 256)	KeyGen
			(L = 2048, N = 224) SHA(256, 384, 512) (L = 2048, N = 256) SHA(256, 384, 512) (L = 3072, N = 256) SHA(256, 384, 512)	PQG Gen
			(L = 1024, N = 160) SHA(1, 256, 384, 512) (L = 2048, N = 224) SHA(256, 384, 512) (L = 2048, N = 256) SHA(256, 384, 512) (L = 3072, N = 256) SHA(256, 384, 512)	PQG Ver

[4] SSH, SNMP, TLS 1.0 and 1.1 KDFs were CAVP tested but are not supported in the Approved mode of operation.

[5] DSA was CAVP tested but is only used as a pre-requisite for DH.

Cert	Algorithm	Mode	Description	Functions/Caveats
			(L = 1024, N = 160) SHA(1, 256, 384, 512) (L = 2048, N = 224) SHA(1, 256, 384, 512) (L = 2048, N = 256) SHA(1, 256, 384, 512) (L = 3072, N = 256) SHA(1, 256, 384, 512)	SigVer
C2143	ECDSA[186-4][6]		P-224, P-256, P-384, P-521	KeyGen
			P-192, P-224, P-256, P-384, P-521	PKV
			P-224 [6]SHA(256, 384, 512) P-256 SHA(256, 384, 512) P-384 SHA(256, 384, 512) P-521 SHA(256, 384, 512)	SigGen
			P-192 SHA(1, 256, 384, 512) P-224 SHA(1, 256, 384, 512) P-256 SHA(1, 256, 384, 512) P-384 SHA(1, 256, 384, 512) P-521 SHA(1, 256, 384, 512)	SigVer
C2143	HMAC [198]	SHA-1	Key Sizes: KS < BS λ = *12*	Message Authentication, KDF Primitive, Password Obfuscation
		SHA-256	Key Sizes: KS = BS λ = *32*	
		SHA-384	Key Sizes: KS = BS λ = *48*	
		SHA-512	Key Sizes: KS = BS λ = *64*	
C2143	KTS [IG D.9 and G.13]	AES (Cert. # C2143); HMAC (Cert. # C2143)	AES (Key Sizes: 128, 192, 256); HMAC SHA (1, 256, 384, 512)	Encryption, Key Transport, Authentication using within TLS.
C2143	RSA [186-4]	X9.31	n = 2048 n = 3072	KeyGen
		PKCS1_v1.5	n = 2048 SHA(256, 384, 512) n = 3072 SHA(256, 384, 512)	SigGen
		PKCS1_v1.5 [186-2 Legacy]	n = 1024 SHA-1 n = 1536 SHA-1 n = 2048 SHA-1	SigVer

[6] ECDSA P-224 was been CAVP tested but is not supported in the Approved mode of operation.

Cert	Algorithm	Mode	Description	Functions/Caveats
		PKCS1_v1.5 [186-4]	n = 1024 SHA(1, 256, 384, 512) n = 2048 SHA(1, 256, 384, 512) n = 3072 SHA(256, 384, 512)	SigVer
C2143	SHS [180-4]	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, Password Obfuscation
C2143	Triple-DES [67][7]	TCBC [38A]	Key Size: 192	Encrypt, Decrypt

Note 1: There are few algorithms, modes, moduli and key sizes that have been CAVP tested but are not implemented/used by the module.

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
RSA	RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
NDRNG (used only to seed the Approved DRBG)	NDRNG (internal entropy source) for seeding the Hash_DRBG. The module generates a minimum of 256 bits of entropy for key generation.

The following service/security function is non-approved and not allowed to be used in FIPS mode of operation.

- TLS 1.3 KDF

By policy, the operators in FIPS mode of operation shall not use TLS 1.3. Usage of the above algorithm/function results in non-conformance as the TLS 1.3 KDF is not CAVP tested, and module does not implement self-test for the algorithm/function specified above.

[7] Triple-DES was CAVP tested but is not available in the Approved mode of operation.

The following table provides the security relevant protocols used in Approved mode of operation.

Table 6 – Security Relevant Protocols Used in FIPS Mode

Protocol	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 HMAC-SHA-384-192 HMAC-SHA-512-256
IKEv2	DH Group 14, 19, 20, 21	RSA and ECDSA Digital Signature Shared Key Message Integrity Code	AES CBC 128/192/256	HMAC-SHA-256-128 HMAC-SHA-384-192 HMAC-SHA-512-256
IPsec ESP	IKEv1 or IKEv2 with optional: Diffie-Hellman (L=2048, N=224, 256) EC Diffie-Hellman P-256, P-384	IKEv1, IKEv2	AES CBC 128/192/256	HMAC-SHA-256-128 HMAC-SHA-384-192 HMAC-SHA-512-256
TLS 1.2	TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384			

Note: no parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) are described in the services detailed in Section 3.3.

The following Critical Security Parameters (CSP) are contained in the cryptographic module:

- IKE Shared Secret – Shared secret used during IKE Phase 1 (length 4 ~ 128 bytes).
- SKEYID – Secret value used to derive other IKE secrets.
- SKEYID_d – Secret value used to derive keys for security associations.
- SKEYID_a – Secret value used to derive keys to authenticate IKE messages.
- SKEYID_e – Secret value used to derive keys to encrypt IKE messages.
- IKE Session Encryption Key – AES (CBC) 128, 192, 256 key used to encrypt data.
- IKE Session Authentication Key – HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512 bit key used for data authentication.
- IKE Private Key – RSA 2048 bit and ECDSA P-256, P-384 and P-521 key used to authenticate the module to a peer during IKE.
- IPsec Session Encryption Key – AES (CBC) 128, 192, 256 key used to encrypt data.
- IPsec Session Authentication Key – HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512 bit key used for data authentication for IPsec traffic.
- TLS 1.2 Master Secret– used for the generation of TLS Session Keys and TLS Integrity Key (384-bits).
- TLS 1.2 Premaster Secret – used for the generation of Master Secret (384 bits).
- TLS 1.2 Private Key– used in the TLS 1.2 signature algorithm (RSA 2048 bit).
- TLS 1.2 Session Key – AES CBC 128/256 bit and AES GCM 128/256 bit key used to protect TLS 1.2 connection.
- TLS 1.2 Integrity Key – HMAC-SHA-1/256/384-bit key used to check the integrity of TLS 1.2 connection.

- Diffie-Hellman/EC Diffie-Hellman – Diffie-Hellman Private Key (N = 224, 256) or EC DH P-256/P-384/P-521 used within IKE key agreement and EC DH P-256/P-384 used within TLS key agreement.
- DRBG V and C values – Used to seed the Approved DRBG.
- Entropy Input: 880-bits seed used to instantiate the DRBG.
- RADIUS Shared Secret – Used for authenticating the RADIUS server to the module and vice versa
- Passwords – Authentication data..

2.2 Public Keys

The following Public Keys are contained in the cryptographic module:

- Root CA Public Key – Used for verifying a chain of trust for receiving certificates.
- Peer IKE Public Key – RSA 2048 bit and ECDSA P-256, P-384 and P-521 key for verifying digital signatures from a peer device.
- IKE Public Key – RSA 2048 bit and ECDSA P-256, P-384 and P-521 key for verifying digital signatures from a peer device.
- Firmware Verification Key – 2048-bit RSA key used for verifying firmware during firmware load.
- Diffie-Hellman/EC Diffie-Hellman Public Key – ECDH P-256/P-384 is used within TLS key agreement.
- Diffie-Hellman/EC Diffie-Hellman Public Key – Diffie-Hellman 2048-bit key, EC DH P-256/P-384/P-521[8] used within IKE key agreement.
- Authentication Public Key – 2048-bit RSA public key used to authenticate the User.
- TLS 1.2 Public Key – RSA 2048-bit public key used in the TLS handshake.

[8] P-521 curve only available for IKEv1 and IKEv2

3. Roles, Authentication and Services

3.1 Assumption of Roles

The cryptographic module provides the roles described in Table 7. The cryptographic module does not provide a Maintenance role. The built-in "Administrator" is a member of "SonicWALL Administrators" group on the SonicWALL appliance, and the name used to login may be configured by the Cryptographic Officer role; the default username for the "Administrator" user is "admin". The User role is authenticated using the credentials of a member of the "Limited Administrators" user group. The User role can query status and non-critical configuration. The user group, "SonicWALL Read-Only Admins," satisfies neither the Cryptographic Officer nor the User Role and should not be used in FIPS mode operations. The configuration settings required to enable FIPS mode are specified in Section 1.3.1 of this document.

The built-in administrator for which the default username is "admin" which is a member of "SonicWALL Administrators" group has the full control privilege to query status and configure all firewall configurations including configure other user privilege. Other members (users) 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" user group can query status and non-critical configuration. A User is authenticated by username and password. User is granted privilege by the membership of user group after login.

Table 7 – Role Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Referred to as "SonicWALL Administrators" group (Administrator and as well as other members (users)) in the vendor documentation	Identity-based	Username and Password
User	Referred to as "Limited Administrators" (user group) in the vendor documentation	Identity-based	Username and Password or Digital Signature

The Module supports concurrent operators. Separation of roles is enforced by requiring users 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 Cryptographic Officer role requires the use of the "Administrator" username and password, or the username and password of a user entity belonging to the "SonicWALL Administrators" group.

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 users who are members of the "SonicWALL Administrators" group can preempt any users except for the Admin user.
3. A user that is a member of the "Limited Administrators" user 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 user 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.

3.2 Authentication Methods

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

Table 8 – Authentication Description

Authentication Method	Probability	Justification
CO and User password	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. 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.	Passwords must be at least eight (8) characters long each, and the password character set is ASCII characters 32-127, which is 96 ASCII characters, hence, the probability is 1 in 96^8.

Authentication Method	Probability	Justification
User RSA 2048-bit (minimum) digital signature	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.	A 2048-bit RSA digital signature has a strength of 112-bits, hence the probability is 1/2^112.

3.3 Services

3.3.1 User Role Services

- Show Status – Monitoring, pinging, traceroute, viewing logs.
- Show Non-Critical Configuration – "Show" commands that enable the User to view VPN tunnel status and network configuration parameters
- Session Management – Limited commands that allow the User to perform minimal VPN session management, such as clearing logs, and enabling some debugging events. This includes the following services:
    1. Log On
    2. Monitor Network Status
    3. Log Off (themselves and users)
    4. Clear Log
    5. Export Log
    6. Filter Log
    7. Generate Log Reports
    8. Configure DNS Settings
- TLS 1.2 – TLS used for the https configuration tool or network traffic over a TLS VPN
- IPsec VPN – Network traffic over an IPsec VPN

3.3.2 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 Section 3.1 and 3.2.

- Show Status - Monitoring, pinging, traceroute, viewing logs.
- Configuration Settings – System configuration[9], network configuration, User settings, Hardware settings, Log settings, and Security services including initiating encryption, decryption, random number generation, key management, and VPN tunnels. This includes the following services:
    1. Configure VPN Settings
    2. Set Content Filter
    3. Import/Export Certificates
    4. Upload Firmware[10]
    5. Configure DNS Settings
    6. Configure Access
- Session Management – Management access for VPN session management, such as setting and clearing logs, and enabling debugging events and traffic management. This includes the following services:
    1. Log On
    2. Import/Export Certificates
    3. Clear Log
    4. Filter Log
    5. Export Log
    6. Setup DHCP Server
    7. Generate Log Reports
- Zeroize – Zeroizing cryptographic keys
- TLS 1.2 – TLS used for the https configuration tool or network traffic over a TLS VPN
- IPsec VPN [11]– Network traffic over an IPsec VPN

The cryptographic module also supports unauthenticated services, which do not disclose, modify, or substitute CSP, use approved security functions, or otherwise affect the security of the cryptographic module.

3.3.3 Unauthenticated services

- No Auth Function - Authenticates the operator and establishes secure channel.
- Show Status – Console message display
- Self-test Initiation – power cycle

Note: 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 Section 1.3.2 can be utilized.

[9] Non-compliant Triple-DES implementation associated with the configuration setting is used to encrypt/decrypt signature files (internal to the module only). This function is considered obfuscation and cannot be used to compromise the module or store/transmit sensitive information.

[10] Note: Only validated firmware versions shall be loaded using the firmware upload service.

[11] MD5 (no security claimed) and keys derived from the non-conformant PBKDF are always encapsulated by the IPsec VPN service.

The cryptographic module provides several security services including VPN and IPsec. The cryptographic module provides the Cryptographic Officer role the ability to configure VPN tunnels and network settings. All services implemented by the Module are listed in the table(s) below.

Table 9 – Authenticated Services

Service	Description	CO	User
Status Information	Viewing Logs, viewing network interface settings	X	X
Configuration management	Setting up VPN, setup filters, upload firmware, Auth directory configuration, creating user accounts	X	
Session Management	Certificate management, DHCP setup	X	X[12]
Zeroize	Destroys all CSPs. Upon system reboot, all CSP in transient memory are erased	X	
TLS 1.2	TLS used for HTTPS management of the module/ network traffic over TLS	X	X
IPsec VPN	Module can configure/run traffic over IPsec VPN using certificates	X	X

Table 10 – Unauthenticated Services

Service	Description
No Auth Function	Authenticates the operator and establishes secure channel.
Show Status	Console message display
Self-test Initiation	Power Cycle

Note: 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 Section 1.3.2 can be utilized.

Table 11 defines the relationship between access to Security Parameters and the different module services. Table 12 defines the relationship between access to Public Keys and the different module services.

The modes of access shown in the tables are defined as:

- G = Generate: The module generates the CSP.
- I = Import: The CSP is entered into the module from an external source.
- R = Read: The module reads the CSP for output.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP to persistent storage.
- Z = Zeroize: The module zeroizes the CSP.

[12] Certificate Management and DHCP Setup services not available to a Limited Administrator(s) User role.

In the tables below, TLS and IPsec listings are inclusive of functions that can be operated with IPsec or TLS communications active.

Table 11 – Security Parameters Access Rights within Services and CSPs

Service	CSPs																			
	IKE Shared Secret	SKEYID	SKEYID_d	SKEYID_a	SKEYID_e	IKE Session Encryption Key	IKE Session Authentication Key	IKE Private Key	IPsec Session Encryption Key	IPsec Session Authentication Key	TLS 1.2 Master Secret	TLS 1.2 Premaster Secret	TLS 1.2 Private Key	TLS 1.2 Session Key	TLS 1.2 Integrity Key	DH/ECDH Private Key	DRBG V and C values	RADIUS Shared Secret	Entropy Input	Passwords
Show Status	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Show Non-critical Configuration	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Monitor Network Status	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	--	-
Log On	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		E
Log Off	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Clear Log	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Export Log	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Import/Export Certificates	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Filter Log	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Setup DHCP Server[13]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Generate Log Reports	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Configure VPN Settings	-	-	-	-	-	IE	-	-	IG	-	-	-	-	-	-	-	IG	-	-	-
IPsec VPN	GERW	GE	GE	GE	GE	-	GE	GE	GERW	GE	-	-	-	-	-	-	GE	GE	GE	-

[13] DHCP setup does not use CSPs, but DHCP server setup is performed with IPsec active. See below for IPsec VPN CSP usage.

Service	CSPs																			
	IKE Shared Secret	SKEYID	SKEYID_d	SKEYID_a	SKEYID_e	IKE Session Encryption Key	IKE Session Authentication Key	IKE Private Key	IPsec Session Encryption Key	IPsec Session Authentication Key	TLS 1.2 Master Secret	TLS 1.2 Premaster Secret	TLS 1.2 Private Key	TLS 1.2 Session Key	TLS 1.2 Integrity Key	DH/ECDH Private Key	DRBG V and C values	RADIUS Shared Secret	Entropy Input	Passwords
TLS	-	-	-	-	-	-	-	-	-	-	GE	GE	GE	GE	GE	GE	GE	GE	-	-
Set Content Filter	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Upload Firmware	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Configure DNS Settings	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Configure Access	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	IEW
Zeroize	Z	Z	Z	Z	Z	z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

Table 12 – Security Parameters Access Rights within Services and Public Keys

Service	Public Keys								
	Root CA Public Key	IKE Public Key	TLS 1.2 Public Key	Peer IKE Public Key	TLS 1.2 Peer Public Key	Authentication Public Key	Firmware Verification Key	DH/ECDH Public Key	DH/ECDH Peer Public Key
Show Status	-	-	-	-	-	-	-	-	-
Show Non-critical Configuration	-	-	-	-	-	-	-	-	-
Monitor Network Status	-	-	-	-	-	-	-	-	-
Log On	-	-	-	-	-	-	-	-	-
Log Off	-	-	-	-	-	-	-	-	-

Service	Public Keys								
	Root CA Public Key	IKE Public Key	TLS 1.2 Public Key	Peer IKE Public Key	TLS 1.2 Peer Public Key	Authentication Public Key	Firmware Verification Key	DH/ECDH Public Key	DH/ECDH Peer Public Key
Clear Log	-	-	-	-	-	-	-	-	-
Export Log	-	-	-	-	-	-	-	-	-
Import/Export Certificates	-	-	-	-	-	-	-	-	-
Filter Log	-	-	-	-	-	-	-	-	-
Setup DHCP Server[14]	-	-	-	-	-	-	-	-	-
Generate Log Reports	-	-	-	-	-	-	-	-	-
Configure VPN Settings	I	IG	IG	-	-	-	-	-	-
IPsec VPN	E	E	E	IE	IE	IE	-	-	E
TLS	-	-	E	-	IE	IE	-	E	-
Set Content Filter	-	-	-	-	-	-	-	-	-
Upload Firmware	-	-	-	-	-	-	E	-	-
Configure DNS Settings	-	-	-	-	-	-	-	-	-
Configure Access	-	-	-	-	-	-	-	-	-
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z

[14] DHCP setup does not use CSPs, but DHCP server setup is performed with IPsec active. See below for IPsec VPN CSP usage.

4. Self-tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand by power cycling the module.

The module performs the following algorithm KATs on power-up:

- Firmware Integrity Test: 512-bit EDC
- AES: KATs: Encryption, Decryption; Modes: CBC and GCM; Key sizes: 128 bits
- DRBG: KATs: HASH DRBG; Security Strengths: 256 bits
- ECDSA: PCT: Signature Generation, Signature Verification; Curves/Key sizes: P-256
- HMAC: KATs: Generation, Verification; SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512
- RSA: KATs: Signature Generation, Signature Verification; Key sizes: 2048 and 3072 bits
- SHA: KATs: SHA-1, SHA-256, SHA-384, SHA-512
- TDES: KATs: Encryption, Decryption; Modes: CBC; Key sizes: 2-key, 3-key[15]
- DSA: KATs: Signature Generation, Signature Verification; Key sizes: 1024, 2048, 3072 bits
- KDFs: IKEv1, IKEv2, TLS, SSH, SNMP[16]

The module performs the following conditional self-tests as indicated.

- DRBG and NDRNG Continuous Random Number Generator Tests per IG 9.8
- RSA Pairwise Consistency Test on RSA key pair generation
- ECDSA Pairwise Consistency Test on ECDSA key pair generation
- Firmware Load Test: 2048-bit RSA signature verification

When a new firmware image is loaded, the cryptographic module verifies the 2048-bit RSA signed SHA-256 hash of the image. If this verification fails, the firmware image loading is aborted, and module should be reloaded to clear the error.

If any of the tests described above fail, the cryptographic module enters the error state. No security services are provided in the error state. Upon successful completion of the Diagnostic Phase, the cryptographic module enters the Command and Traffic Processing State. Security services are only provided in the Command and Traffic Processing State. No VPN tunnels are started until all tests are successfully completed. This effectively inhibits the data output interface.

[15] Triple-DES KATs are performed even if they are not supported in the Approved mode of operation

[16] The SSH and SNMP KDF KATs are performed if they are not supported in the Approved mode of operation

The module performs the following critical self-tests. These critical function tests are performed for the SP 800-90A DRBG:

- SP 800-90A Instantiation Test
- SP 800-90A Generate Test
- SP 800-90A Reseed Test
- SP 800-90A Uninstantiate Test

5. Physical Security Policy

The firmware module relies on the physical embodiment of the referenced host platforms as listed in Table 1 of the document, which store the module within their enclosure. The referenced host platforms meet Level 1 physical security requirements and are made of production grade material.

6. Operational Environment

The module operates in a limited operational environment per FIPS 140-2 level 1 specifications. Hence the operational environment requirements do not apply.

The module's firmware version is SonicOSX 7.0

7. Mitigation of Other Attacks Policy

Area 11 of the FIPS 140-2 requirements do not apply to this module as it has not been designed to mitigate any specific attacks outside the scope of FIPS 140-2 requirements.

8. Security Rules and Guidance's

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-2.

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 power-up self-tests by power cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output are inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs 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 CSPs.
14. The module does not output intermediate key values.
15. The operators should not use TLS 1.3 as the TLS 1.3KDF is not CAVP tested and hence considered as non-approved security function in FIPS mode of operation.

8.1 Crypto Officer Guidance

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

1. The tester shall connect an Ethernet cable from a GPC to the ethernet port on the module's host platform. On the GPC, the tester should connect to the console interface using virtual serial port.
2. The tester should then boot up the virtual appliance and wait for the boot process to complete and login prompt will be available only upon initial boot up of all power-up self-tests and successful completion of these self-tests.
3. As the CO, the tester should login using the vendor provided default login and password. The default password and login should be changed/updated.
4. As the CO, management IP address and Gateway should be configured for the module.
5. Over the web interface, the tester should then proceed to system settings and update the settings to be consistent with Section 1.3.1 of this document with the assistance of compliance checking procedure and then enabling FIPS mode using a checkbox. The FIPS checkbox does not place the module in FIPS

mode until the settings of Section 1.3.1 of this document are met. Then click OK. The system automatically restarts.
6. The tester shall observe that the module self-tests executed automatically before a log in was possible. The tester will observe that the “FIPS enabled checkbox” is enabled to indicate that the module is in the Approved mode of operation. The tester can verify that in the system/settings page that FIPS mode is enabled.
7. As the CO, the tester shall proceed to create the roles specified in Section 3.1 of this document. Passwords and Digital signatures required for authentication to each should be configured or installed as appropriate.

Note: When the "FIPS 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 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 "FIPS Mode" checkbox and corresponding system flag ("fips") which can be queried over the console will not be set unless all settings are compliant. The "FIPS Mode" checkbox and fips system flag are indicators that the module is running in the FIPS Approved mode of operation.

9. References and Definitions

The following standards are referred to in this Security Policy.

Table 13 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, *January 2011*
[132]	*NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010*
[133]	*NIST Special Publication 800-133rev2, Recommendation for Cryptographic Key Generation, June 2020*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[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]	*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*
[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*
[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*
[56Br1]	*NIST Special Publication 800-56B Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, September 2014*
[67]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*

Table 14 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
FIPS	Federal Information Processing Standard
CSP	Critical Security Parameter
VPN	Virtual Private Network
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
Triple-DES	Triple Data Encryption Standard
DES	Data Encryption Standard
CBC	Cipher Block Chaining
DSA	Digital Signature Algorithm
DRBG	Deterministic Random Bit Generator
RSA	Rivest, Shamir, Adleman asymmetric algorithm
IKE	Internet Key Exchange
RADIUS	Remote Authentication Dial-In User Service

Acronym	Definition
IPSec	Internet Protocol Security
LAN	Local Area Network
DH	Diffie-Hellman
GUI	Graphical User Interface
SHA	Secure Hash Algorithm
HMAC	Hashed Message Authentication Code