SonicWall, Inc.

SonicWall Network Security Virtual Appliances

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.1

Date: February 24th , 2021

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, 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 runs on many different UCS Servers with various hypervisors. The firmware module is comprised of an OVA package file "SonicWALL_NSV_300.ova" for the NSv 300. For the purpose of this validation, the module was tested on the following servers:

Table 1 – Cryptographic Module List

	Model	Tested Platforms	Hypervisor	Processor
1	NSv 300	Dell PowerEdge M630	VMWare ESXi 6.5	Intel Xeon E5
2	NSv 300	Dell PowerEdge R630	VMWare ESXi 6.7	Intel Xeon E5

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

- NSv 10
- NSv 25
- NSv 50
- NSv 100
- NSv 200
- NSv 400
- NSv 800
- NSv 1600

The following Hypervisors/Cloud are vendor affirmed on the additional platforms listed above:

ESXi 5.0, ESXi 5.5, ESXi 6.0, NFVIS, AWS, HYPERV, AZURE and KVM.

The above vendor affirmed modules and 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.

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 module firmware version for all tested models is SonicOS v6.5.4 or SonicOSv referred in this document as NSv.

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	2
Finite State Model	1
Physical Security	N/A
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall	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 M630/ Dell PowerEdge R630 Server) on which it runs. The module's physical cryptographic boundary is illustrated by the green dashed line in Figure 1.

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.

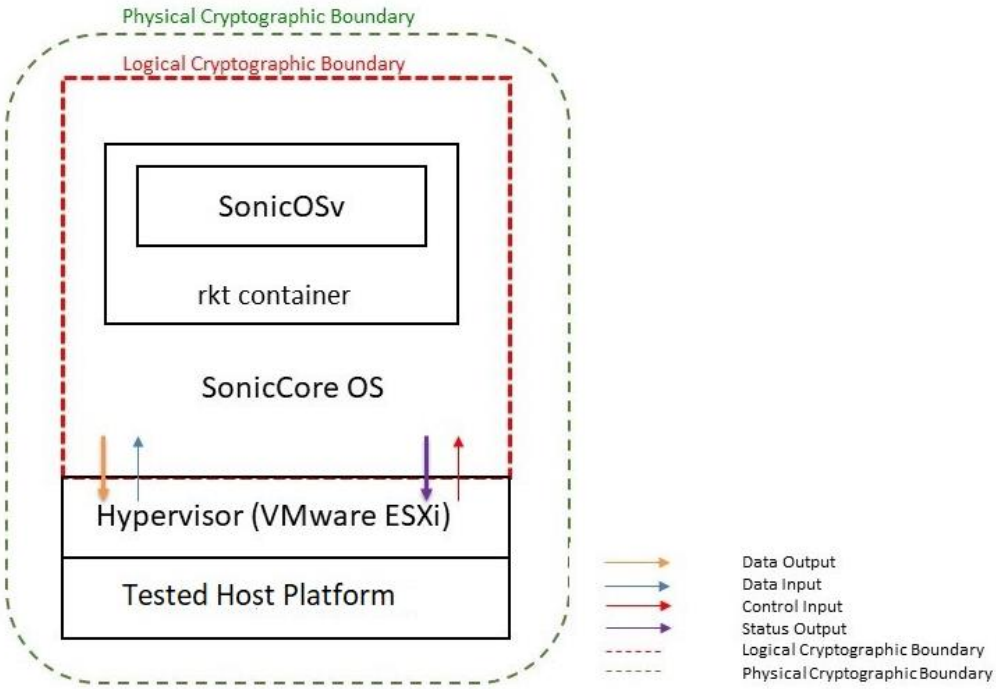

Figure 1 – Block Diagram

Figure 1 also shows the logical cryptographic boundary of the module executing in memory and its interactions with the hypervisor. The logical cryptographic boundary of the module (shown by the red dashed line in Figure 1) is the SonicCore OS. SonicCore Module launches the rkt container with SonicOSv 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 an 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 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.

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. Bandwidth management must be set to “ON”.
9. “Advanced Routing Services” must not be enabled.
10. “Group VPN management” must not be enabled.
11. SNMP or SSH must not be enabled.

Note: Once FIPS mode of operation is enabled SonicOS 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
- In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption muse 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. These services are not enabled by default, if operator selects to enable these services the system will transition to non-approved mode of operation. The crypto-officer must zeroize the module prior to switching between the approved and the non-approved modes of operation.

- 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 of 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
#C965	AES [197] [3]	CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 128, 192, 256	Encrypt
		ECB [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		GCM [38D][4]	Key Sizes: 128, 192, 256 Tag Len: 128	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
Vendor Affirmed	AES [IG A.3]	AES-CBC Ciphertext Stealing (CBC-CS1)	Key Sizes: 128, 192, 256	Encrypt, Decrypt
Vendor Affirmed	CKG [IG D.12]	[133] Section 6.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation
		[133] Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output		
		[133] Section 7.1 Direct symmetric key generation using unmodified DRBG output		
		[133] Section 7.3 Derivation of symmetric keys from a key agreement shared secret.		
		[133] Section 7.4 Derivation of symmetric keys from a pre-shared key		
		[133] Section 7.6 Combining multiple keys and other data		
#C965	CVL: All of SP800-56A except KDF [56A]	FFC (Initiator, Responder)(Hybrid1, Ephem, Hybrid1Flow, OneFlow, Static)	FB: Hash Algorithm: SHA2-512 FC: Hash Algorithm: SHA2-512	Key Agreement
		ECC (Initiator, Responder)(FullUnifi	P-224, P-256, P-384, P-521	

[3] AES-GMAC has been CAVP tested but is not used in the Approved mode of operation.

[4] The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS. Per RFC 5246, if the module is the party that encounters this condition it will trigger a handshake to establish a new encryption key.

Cert	Algorithm	Mode	Description	Functions/Caveats
		ed, EphemUnified, OnePassUnified, OnePassDH, StaticUnified)		
#C965	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][5]	v1.0, v1.1, v1.2	SHA (256, 384, 512)	
	CVL: SSH [135]		SHA-1	
	CVL:SNMP [135]		SHA-1	
#C965	DRBG [90Arev1]	Hash	SHA-256	Deterministic Random Bit Generation
#C965	DSA [186-4][6]		(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

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

[6] DSA was CAVP tested but is only used as a pre-requisite for CVL Cert. # C965.

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
#C965	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 [7]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
#C965	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*	
#C965	KTS [IG G.8]	AES (Cert. #C965); HMAC (Cert. #C965)	AES (Key Sizes: 128, 192, 256); HMAC SHA(1, 256, 384, 512)	Encryption, Key Transport, Authentication using within TLS 1.2
#C965	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 has 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
#C965	SHS [180-4]	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, Password Obfuscation
#C965	Triple-DES [67][8]	TCBC [38A]	Key Size: 192	Encrypt, Decrypt

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

Table 5 - Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
DH	Diffie-Hellman (CVL Certs. #C965 with #C965, key agreement; key establishment methodology provides 112 bits of encryption strength)
EC DH	EC Diffie-Hellman (CVL Certs. #C965 with #C965, key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)
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.

Table 6 - Security Relevant Protocols Used in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv1	DH Group 14, 19, 20, 21	RSA 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 Digital Signature Shared Key Message Integrity Code	AES CBC 128/192/256	HMAC-SHA-256-128 HMAC-SHA-384-192 HMAC-SHA-512-256

[8] Triple-DES was CAVP tested but is not used by any service implemented in the Approved mode of operation.

Protocol	Key Exchange	Auth	Cipher	Integrity
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 or SSL 3.1	RSA_WITH_AES_128_CBC_SHA RSA_WITH_AES_256_CBC_SHA RSA_WITH_AES_128_CBC_SHA256 RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_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) is 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 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 Master Secret– used for the generation of TLS Session Keys and TLS Integrity Key (384-bits).
- TLS Premaster Secret – used for the generation of Master Secret (384 bits).
- TLS Private Key– used in the TLS handshake (ECDSA P-256, P-384, P-521 and RSA 2048 bit).
- TLS Session Key – AES 128 and 256 bit key used to protect TLS connection.
- TLS Integrity Key – HMAC-SHA-1/256/384 bit key used to check the integrity of TLS connection.
- Diffie-Hellman/EC Diffie-Hellman – Diffie-Hellman Private Key (N = 224, 256) or EC DH P-256/P-384 used within IKE or TLS key agreement.
- DRBG V and C values – Used to seed the Approved DRBG.
- Entropy Input: 256 bits entropy (min) input used to instantiate the DRBG.
- DRBG Seed: Seed material used to seed or reseed the DRBG .

- RADIUS Shared Secret – Used for authenticating the RADIUS server to the module and vice versa. Type: A minimum of 8 characters for RADIUS authentication.
- Passwords – Authentication data. Type: A minimum 8 ASCII characters.

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 key for verifying digital signatures from a peer device
- IKE Public Key –RSA 2048 bit key for verifying digital signatures created by the module
- Firmware Verification Key – P-256 ECDSA key used for verifying firmware during firmware load
- Diffie-Hellman/EC Diffie-Hellman Public Key – Diffie-Hellman 2048-bit key, EC Diffie-Hellman P-256/P-384 used within TLS key agreement
- Diffie-Hellman/EC Diffie-Hellman Peer Public Key – Diffie-Hellman 2048-bit key, EC DH P-256/P-384/P-521 [9]used within IKE key agreement
- Authentication Public Key – 2048-bit RSA public key used to authenticate the User
- TLS Public Key – RSA – 2048-bit public key used in the TLS handshake

[9] 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 "Administrator" user is a local account on the SonicWALL appliance, and the name used to login as this account may be configured by the Cryptographic Officer role; the default name for the "Administrator" account 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.

A built-in administrator with the default username "admin" has the control privilege to query status and configure all firewall configurations including configuration of other users' privilege. There are two user groups that have control privilege besides the built-in administrator, the "SonicWALL Administrators" and the "Limited Administrators" groups. Members of "SonicWALL Administrators" user group have the same control privilege as the built-in administrator. Members of "Limited Administrators" user group can query status and non-critical configuration. A user is authenticated using a username and password and is granted privilege based on membership of a user group after login.

Table 7 – Role Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Referred to as "Administrator" (individual user) and "SonicWALL Administrators" (user group) in the vendor documentation	Role-based and 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 a 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 has the highest priority and can preempt any users.
2. A user that is a member of the "SonicWALL Administrators" user group can preempt any users except for the Admin.
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 two choices:
    a. "Continue" – this action will log out the existing administrative session and will impart full administrative privileges to the preempting user.
    b. "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 guest users)
    4. Clear Log
    5. Export Log
    6. Filter Log
    7. Generate Log Reports
    8. Configure DNS Settings
- TLS – 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 Cryptographic Officer role is authenticated using the credentials of the "Administrator" user account (also referred to as "Admin"), or the credentials of a member of the "SonicWALL Administrators" user group. The use of the latter allows for identification of specific users (i.e., by username) upon whom is imparted full administrative privileges through their assigned membership to the "SonicWALL Administrators" group by the Admin user, or other user with 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[10], 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[11]
    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 – TLS used for the https configuration tool or network traffic over a TLS VPN
- IPsec VPN [12]– 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

- Module Reset - Firmware removal with configuration return to factory state
- NoAuth Function - Authenticates the operator and establishes secure channel.
- Show Status – LED activity and console message display

[10] 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.

[11] Note: Only validated firmware versions shall be loaded using the firmware upload service. Any other firmware version that is not listed in the module certificate is considered out of scope and requires separate FIPS 140-2 certificate.

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

- Self-test Initiation – power cycle

Note 1: 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.

Note 2: The module does not support a bypass capability.

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, viewing system flag to check whether the module is running in the FIPS Approved mode of operation ("Show fips") and viewing status of the module (i.e module configuration)	X	X
Configuration management	Setting up VPN, setup filters, upload firmware, Auth directory configuration, creating user accounts	X	
Session Management	Audit configuration, Certificate management, DHCP setup	X	X[13]
Zeroize	Destroys all CSPs. Upon system all CSP in transient memory are erased	X	
TLS	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
Module Reset	Reset the Module by activating the reset switch
NoAuth Function	Authenticates the operator and establishes secure channel.
Show Status	LCD Display available on only SM Series
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.

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

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.

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 Master Secret	TLS Premaster Secret	TLS Private Key	TLS Session Key	TLS 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	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

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 Master Secret	TLS Premaster Secret	TLS Private Key	TLS Session Key	TLS Integrity Key	DH/ECDH Private Key	DRBG V and C values	RADIUS Shared Secret	Entropy Input	Passwords
Setup DHCP Server[14]	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Generate Log Reports	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Configure VPN Settings	-	-	-	-	-	IE	-	-	IG	-	-	-	-	-	-	-	IG	-	-	-
IPsec VPN	GERW	GE	GE	GE	GE	-	GE	GE	GERW	GE	-	-	-	-	-	-	GE	GE	GE	-
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

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

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

Service	Public Keys								
	Root CA Public Key	IKE Public Key	TLS Public Key	Peer IKE Public Key	TLS 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	-	-	-	-	-	-	-	-	-
Clear Log	-	-	-	-	-	-	-	-	-
Export Log	-	-	-	-	-	-	-	-	-
Import/Export Certificates	-	-	-	-	-	-	-	-	-
Filter Log	-	-	-	-	-	-	-	-	-
Setup DHCP Server[15]	-	-	-	-	-	-	-	-	-
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

[15] 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: 256-bit EDC
- AES: KATs: Encryption, Decryption; Modes: ECB 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: 1024, 2048, 3072 bits
- SHA: KATs: SHA-1, SHA-256, SHA-384, SHA-512
- TDES: KATs: Encryption, Decryption; Modes: CBC; Key sizes: 2-key, 3-key[16]
- AES-CBC Ciphertext Stealing (CS): KATs: Encryption, Decryption; Modes: CBC-CS1; Key sizes: 128, 192, 256 bits
- DSA: KATs: Signature Generation, Signature Verification; Key sizes: 1024, 2048, 3072 bits
- KDFs: IKEv1, IKEv2, TLS, SSH, SNMP[17]
- Diffie-Hellman Primitive "Z" Computation KAT
- EC Diffie-Hellman Primitive "Z" Computation KAT

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

- DRBG and NDRNG Continuous Random Number Generator Tests per IG 9.8
- SP 800-90A DRBG Section 11.3 Health Checks
- 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.

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

[16] Triple-DES KATs are performed even though they are not implemented in any of the services available in the Approved mode of operation.

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

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.

When all tests are completed successfully, the Test LED is turned off.

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

Physical security requirements do not apply to the module because it is a FIPS 140-2 Level 1 firmware module and the physical security is provided by the host platform.

6. Operational Environment

The module operates in a non-modifiable operational environment per FIPS 140-2 level 1 specifications and as such the operational environment requirements do not apply.

The module firmware version is SonicOS v6.5.4.

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

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 Cryptographic Officer.
2. The module provides role-based and identity-based authentication for the crypto-officer, and identity-based authentication 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.

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. Apply power to the module's host platform and observe that upon initial boot all power-up self-tests are executed automatically and successfully completed before a login prompt is available.
2. As the CO, log in using the vendor provided default login and password.
3. As the CO, configure the management IP address and Gateway for the module.
4. Over the web interface, proceed to system settings and enable FIPS mode using the corresponding checkbox. Then click OK. The system restarts automatically.
5. The module executes the self-tests automatically before a log in is possible. Verify in the system/settings page that FIPS mode was enabled. Update the settings to be consistent with Section 1.3.1 with the assistance of the compliance checking procedure.
6. As the CO (Administrator), create the roles specified in Section 3.1. Configure/install passwords and digital signatures required for authentication to each role as appropriate. Change the password for the default account and reboot the module.
7. Upon reboot the self-tests run automatically. Upon completion of the self-tests' execution, log in using the newly created CO role.

8. Verify that the FIPS enabled checkbox is checked indicating that the module is in the Approved mode of operation.

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 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[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*
[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*

Abbreviation	Full Specification Name
[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*
[56A]	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007*
[56Ar2]	*NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013*
[56Br1]	*NIST Special Publication 800-56A 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