SonicWall, Inc.
SonicWall Network Security Manager Appliance

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.0

Date: July 18, 2023

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 Manager Appliance, hereafter denoted the "module". The module is an Internet security appliance, which manages all firewalls, connected switches and access points, all in one (1) easy-to-use interface.

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 the platform as listed below in Table 1. The firmware module included in this validation is comprised of an OVA package file "SonicWall_NSM_On-Prem_2.3.0.ova". The module's firmware version for the tested platform is "2.3".

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

Table 1 – Cryptographic module List

	OS/Model	Tested Platforms	Hypervisor	Processor
1	SonicCore OS v6.5.0	Dell PowerEdge R640	VMWare ESXi 6.7	Intel Xeon Silver 4208 (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 7.0
- ESXi 6.5
- 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.

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	2
Finite State Model	1

Security Requirement	Security Level
Physical Security	1
Operational Environment	1
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 R640) on which it runs. The module's physical cryptographic boundary is illustrated by the green dashed line in Figure 1.

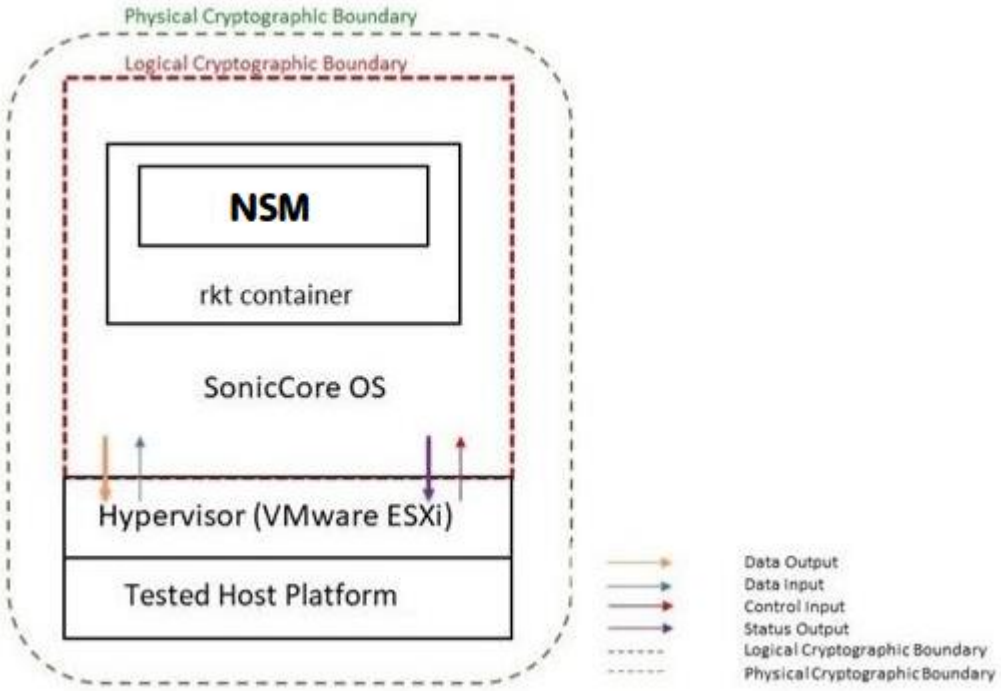

Figure 1 – Block Diagram

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 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. The SonicCore OS launches the rkt container with the NSM 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	NSM 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" toggle button on the System > Settings > Firmware and Settings page over the web interface. When the "FIPS Mode" toggle button is enabled, the module executes a compliance checking procedure, examining all settings related to the security rules described below. The operator is responsible for updating the Step 1 setting, otherwise the module will not allow the operator to set the "FIPS Mode" toggle button.

Except for Step 1 in the following settings, once the "FIPS Mode" toggle button is enabled, irrespective of whether or not the operator has updated the following settings, the module will reload and automatically update the following settings. In addition, as soon as the "FIPS Mode" toggle button is set, the module will automatically reload to enable the FIPS mode. The "FIPS Mode" toggle button is an indication 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 the FIPS-mode of operation:

1. The default Administrator and User passwords shall be immediately changed and be at least eight (8) characters.
2. SMTP traffic must be configured to enable TLS 1.2.
3. External authentication sever must not be configured.
4. RSA Certificates used during authentication must have a minimum modulus size of 2048 bits or greater in size.
5. Control communication for High Availability shall always be encrypted using AES GCM 256.
6. Zero touch must be disabled.

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

Note: 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 non-FIPS approved services which are not available in the FIPS mode of operation.

- External server authentication
- CSR generation with key size 1024 and 1536 for RSA
- Zero touch support for firewall
- Control communication for High Availability without encryption
- SMTP server communication without TLS 1.2.

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
A1960	AES [197]	ECB CBC GCM[1]	ECB - Key Sizes: 128 and 256 CBC - Key Sizes: 128 and 256 GCM - Key Sizes: 128 and 256; Tag Len: 128	Encrypt, Decrypt, Authenticated Encrypt, Authenticated Decrypt, Message Authentication

[1] The module's AES-GCM implementations conforms to IG A.5 Scenario#1 Method ii) 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. 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.

Cert	Algorithm	Mode	Description	Functions/Caveats
Vendor Affirmed	CKG [IG D.12]	In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation as per Scenario 1 of Section 4 in SP800-133 rev2. The resulting generated symmetric key and the seed used in the asymmetric key generation are the unmodified output from SP800-90A DRBG.		Key Generation
N/A	ENT (P)	Intel DRNG is used as an entropy source and meets SP800-90B, IG 7.14 Scenario 1B, IG 7.18 and 7.19.		For seeding firmware DRBG
N/A	KAS	KAS-SSC (Cert. #A1960) with CVL (Cert. #A1960, SP 800-135 TLS KDF or RFC 8446 TLS 1.3 KDF)		Key Agreement

Cert	Algorithm	Mode	Description	Functions/Caveats
A1960	KAS-SSC[2] (ECDH: SP800-56a rev3)	Domain Parameter Generation Methods: P-256, P-384 Scheme(s): Ephemeral Unified	ECDH P-256 and P-384 (Ephemeral Unified scheme per section 6.1.2.2 of SP800-56Arev3)	Key Agreement
A1960	CVL: TLS v1.3 KDF	TLS 1.3 KDF (as per Section 7.1 of RFC 8446)	HMAC SHA (256, 384) KDF Modes: DHE	Key Derivation
A1960	CVL: TLS [135]	v1.2	SHA (256, 384, 512)	Key Derivation
A1960	DRBG [90Arev1]	AES	CTR-256	Deterministic Random Bit Generation
A1960	ECDSA[186-4]		P-256 and P-384	KeyGen
			P-256 and P-384	PKV
			P-256 SHA(256, 384) P-384 SHA(256, 384)	SigGen
			P-256 SHA(1, 256, 384) P-384 SHA(1, 256, 384)	SigVer
A1960	HMAC [198]	SHA-1	Key Sizes: KS = BS λ = *20*	Message Authentication, KDF Primitive.
		SHA-256	Key Sizes: KS = BS λ = *32*	
		SHA-384	Key Sizes: KS = BS λ = *48*	
		SHA-512	Key Sizes: KS = BS λ = *64*	
A1960	KTS [IG D.9 and G.13]	AES (Cert. #A1960); HMAC (Cert. #A1960)	AES (Key Sizes: 128, 256); HMAC SHA (1, 256, 384)	Encryption, Key Transport, Authentication using within TLS.
A1960	RSA [186-4]	B.3.3 Key Gen Mode	n = 2048 n = 3072	KeyGen
		PKCS1_v1.5 [186-4]	n = 2048 SHA(256, 384)	SigGen

[2] The module meets IG D.8 Scenario X1 path (2) where CAVP testing is performed, in which it is split into (i) testing the computation of the shared secret, (ii) testing the key derivation function used in deriving the keying material.

Cert	Algorithm	Mode	Description	Functions/Caveats
			n = 3072SHA(256, 384)	
		PKCS1_v1.5 [186-4]	n = 2048 SHA(256, 384) n = 3072SHA(256, 384)	SigVer
A1960	SHS [180-4]	SHA-1[3] SHA-256 SHA-384 SHA-512		Message Digest Generation

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
RSA[4]	RSA (key wrapping; key establishment methodology provides 112 or 128 bits of encryption strength)

Table 6 – Security Relevant Protocols Used in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
TLS 1.2	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) are described in the services detailed in Section 3.3.

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

- 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 1.2 signature algorithm (RSA 2048/3072-bits, ECDSA P-256 and P-384).
- TLS Session Key – AES CBC 128/256 and AES GCM 128/256-bits used to protect TLS 1.2 connection.
- TLS Integrity Key – HMAC SHA-1/256/384 key used to check the integrity of TLS 1.2 connection.
- EC Diffie-Hellman – EC DH P-256/P-384 used within TLS key agreement.
- DRBG V and C values – Used to seed the Approved DRBG.

[3] SHA-1 is only used in non-digital signature applications and digital signature verification purposes only.

[4] As per IG D.9, this RSA-based key wrapping algorithm uses RSA (modulus 2048 or 3072 bits long) of PKCS#1-v1.5 scheme and is not compliant with any revision of SP800-56B.

- Entropy Input – 880-bits seed used to instantiate the DRBG.
- Passwords – Authentication data.

2.2. Public Keys

The following Public Keys are contained in the cryptographic module:

- Firmware Verification Key – 2048-bit RSA key used for verifying firmware during firmware load.
- EC Diffie-Hellman Public Key – ECDH P-256/P-384 is used within TLS key agreement.
- Authentication Public Key – 2048/3072-bit RSA public key used to authenticate the User.
- TLS Public Key – RSA 2048/3072-bits, ECDSA P-256 and P-384 public key used in the TLS handshake.

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 operator is the "SuperAdmin" role on the SonicWall appliance, and the default username for the "SuperAdmin" role is "admin". There are other operators classified as a CO role under the "Administrator" group using the credentials of the member of that group. The User role is classified as the "Operator" group, "Read Only" group, "Guest" group and "Support" group and the users are authenticated using the credentials of a member of that assigned group. The User role has very limited capability and the services performed by that role are provided in detail in Section 3.3. of the document. The configuration settings required to enable FIPS mode are specified in Section 1.3.1 of this document.

The built-in operator has the default username as "admin" and has the full control privilege to query status and configure all tenants and device configurations including configuration of other user privileges. The members (operators) of the "Administrator" group have the same full control privilege as the built-in "SuperAdmin" role except that they cannot create tenants and have control over their own tenants assigned by the "SuperAdmin". The services available for the "Administrator" group are described in Section 3.3 of this document. The members of the "Administrator" group can be authenticated either by username and password or by digital signature.

The members of the "Operator" group are classified as the user role and can maintain firewall-related configuration that is assigned by the "SuperAdmin" user. Members of the "Guest", "Support" and "ReadOnly" groups have only read-only permissions. Please note that the member of user role can be either authenticated using username and password or by digital signature.

Table 7 – Role Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Referred to as "SuperAdmin" (individual user) and "Administrators" (user group) in the vendor documentation	Role-based and Identity-based	Username and Password or Digital Signature (Applicable for Administrator group)

Role ID	Role Description	Authentication Type	Authentication Data
User	Referred to as “Operator” (user group), “Guest” (user group), “Support” (user group) and “Read-Only” (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. The User role requires the use of a username and password or possession of the private key of a user entity belonging to the “Operator” (user group), “Guest” (user group), “Support” (user group) and “Read-Only” (user group). The Cryptographic Officer role requires the use of the “SuperAdmin” username and password, or the username and password or possession of the private key of a user entity belonging to the “Administrators” group.

3.2. Authentication Methods

The cryptographic module provides authentication relying upon username/password 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 94^8, which is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur for each attempt. By default, after three (3) successive unsuccessful password verification tries, the cryptographic module automatically locks for 5 minutes before additional password entry attempts can be reinitiated. Duration of the lockout will grow incrementally from the last lockout duration. For example: Three successive failed attempts result in a lockout of the module for 5 minutes, fourth failed attempt will result in lockout of 10 minutes and on. Hence, only three attempts or less than that can be made in a minute which makes the probability approximately 3/94^8 = 4.9E-16, 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 94 (alphabets, numbers and special characters). Hence, the probability is 1 in 94^8.
CO and 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 (Applicable to Operator, Guest, Read Only and Support users) – Monitoring, pinging, traceroute, viewing logs.
- Show Non-Critical Configuration (Applicable to Operator, Guest, Read Only and Support users) – "Show" commands that enable the User to view VPN tunnel status and network configuration parameters.
- Firewall Management (Applicable only to Operator users) - Manage SonicWall Firewall devices. This includes the following service:
    - Device Management – Firewall life cycle such as add/edit/delete and its operation.
    - Configuration Management – Creating a set of changes that needs to be pushed to firewall.
    - Certificate Management – Certificate related tasks such as add/edit/delete certificate and push those certificates to firewall from the module.
    - Group Management – Creating a group of firewall devices and managing the group of firewall devices. The firewall configuration is pushed at once to the group of firewall devices.
    - SD-WAN Topology – Creating SD-WAN configuration among the firewall devices managed by the module.
    - VPN Topology – Creating VPN among the firewall devices managed by the module.
- Session Management (Applicable to Operator, Guest, Read Only and Support users) – Limited commands that allow the User to perform session management, such as clearing logs, and enabling some debugging events. This includes the following services:
    1. Log On
    2. Log Off (themselves and users)
    3. Export Logs
    4. Filter Log
- TLS (Applicable to Operator, Guest, Read Only and Support users) – TLS used for the https configuration tool or network traffic over a TLS VPN

3.3.2. Crypto Officer Services

- Show Status (Applicable to both SuperAdmin and Administrator users) - Monitoring, pinging, traceroute, viewing logs.
- Configuration Management – System configuration, Network configuration, User settings, Hardware settings, Log settings, and Security services including initiating encryption, decryption, random number generation and key management. This includes the following services:

1. Import/Export Certificates (Applicable to Super Admin user).
2. Upload Firmware[5] (Applicable to Super Admin user).
3. Configure DNS Settings (Applicable to Super Admin user).
4. Installation, Secure Initialization and placing the module in FIPS mode (Applicable to Super Admin user).
5. Setup SMTP server (Applicable to Super Admin user).
6. Setup two factor authentication (Applicable to both Super Admin and Administrator users).

- Session Management – Management access such as setting and clearing logs, and enabling debugging events and traffic management. This includes the following services:
    1. Export logs (Applicable to both Super Admin and Administrator users).
    2. Filter Log (Applicable to both Super Admin and Administrator users).
    3. Setup Twilio (Applicable to Super Admin user) – Used to send Alerts and notifications that are not security relevant and the communication uses TLS v1.2.
    4. Log on and Off (Applicable to both Super Admin and Administrator users).
- Firewall Management (Applicable to both Super Admin and Administrator users) - Manage SonicWall Firewall devices. This includes the following service:
    - Device Management – Firewall life cycle such as add/edit/delete and its operation.
    - Configuration Management – Creating a set of changes that needs to be pushed to firewall.
    - Certificate Management – Certificate related tasks such as add/edit/delete certificate and push those certificates to firewall from the module.
    - Group Management – Creating a group of firewall devices and managing the group of firewall devices. The firewall configuration is pushed at once to the group of firewall devices.
    - SD-WAN Topology – Creating SD-WAN configuration among the firewall devices managed by the module.
    - VPN Topology – Creating VPN among the firewall devices managed by the module.
- User Management (Applicable to both Super Admin and Administrator users)- Manage Users, User lockout settings, and Roles.
- High Availability (Applicable only to the Super Admin user) - Monitoring and configuring the Secondary Device for HA configuration. Uses AES 256 for HA communication channel encryption. This includes the following services:
    - Show Status
    - Diagnostics

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

- Virtual IP Configuration for HA configuration

- Zeroize – Zeroizing all cryptographic keys and CSPs
- TLS (Applicable to both Super Admin and Administrator users) – TLS used for the https configuration tool or network traffic over a TLS VPN

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

3.3.3. Unauthenticated services

- No Auth Function - Authenticates the users and establishes secure channel
- Show Status – Console message display
- Self-test Initiation – power cycle
- Viewing logs, viewing system info, Ping and configuration of IP address

All services implemented by the module are listed in the table(s) below.

Table 9 – Authenticated Services

Service	Description	CO	User
Status Information	Monitoring, pinging, traceroute, viewing logs.	X	X
Configuration management	System configuration, network configuration, User settings, Hardware settings, Log settings, and Security services including initiating encryption, decryption, random number generation and key management.	X	
Session Management	Management access such as setting and clearing logs, and enabling debugging events and traffic management.	X	
Firewall Management	Manage SonicWall Firewall devices.	X	X
User Management	Manage Users, User lockout settings, and Roles.	X	
High Availability	Monitoring and configuring the Secondary Device for HA.	X	
Zeroize	Destroys all CSPs. Upon system reboot, all CSP in transient memory are erased	X	
TLS	TLS used for HTTPS management of the module/ network traffic over TLS	X	X

Table 10 – Unauthenticated Services

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

Service	Description
Viewing logs, viewing system info, Ping and configuration of IP address	Viewing logs and system info on console. The operator can also ping and configure the IP address

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								
	TLS Master Secret	TLS Premaster Secret	TLS Private Key	TLS Session Key	TLS Integrity Key	ECDH Private Key	DRBG V and C values	Entropy Input	Passwords
Show Status	-	-	-	-	-	-	-	-	-
Show Non-critical Configuration	-	-	-	-	-	-	-	-	-
Device Management	-	-	-	-	-	-	-	--	-
Template Management	-	-	-	-	-	-	-	--	-

Service	CSPs								
	TLS Master Secret	TLS Premaster Secret	TLS Private Key	TLS Session Key	TLS Integrity Key	ECDH Private Key	DRBG V and C values	Entropy Input	Passwords
Certificate Management	-	-	-	-	-	-	-	--	-
Group Management	-	-	-	-	-	-	-	--	-
SD-WAN Topology	-	-	-	-	-	-	-	--	-
Log On	-	-	-	-	-	-	-		E
Log Off	-	-	-	-	-	-	-	-	-
Export Log	-	-	-	-	-	-	-	-	-
Filter Log	-	-	-	-	-	-	-	-	-
Generate Log Reports	-	-	-	-	-	-	-	-	-
TLS	GE	GE	GE	GE	GE	GE	GE	-	-
Import/Export Certificates	-	-	-	-	-	-	-	-	-
Upload Firmware	-	-	-	-	-	-	-	-	-
Configure DNS Settings	-	-	-	-	-	-	-	-	-
Installation, Secure Initialization and placing the module in FIPS mode	-	-	-	-	-	-	-	-	E
Setup SMTP server	GE	GE	GE	GE	GE	GE	GE	-	-
Setup two factor authentication	-	-	-	-	-	-	-	-	-

Service	CSPs								
	TLS Master Secret	TLS Premaster Secret	TLS Private Key	TLS Session Key	TLS Integrity Key	ECDH Private Key	DRBG V and C values	Entropy Input	Passwords
Setup Twilio	GE	GE	GE	GE	GE	GE	GE	-	-
User Management	-	-	-	-	-	-	-	-	-
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z

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

Services	Public Keys					
	TLS Public Key	TLS Peer Public Key	Authentication Public Key	Firmware Verification Key	ECDH Public Key	ECDH Peer Public Key
Show Status	-	-	-	-	-	-
Show Non-critical Configuration	-	-	-	-	-	-
Device Management	-	-	-	-	-	-
Template Management	-	-	-	-	-	-
Certificate Management	-	-	-	-	-	-
Group Management	-	-	-	-	-	-
SD-WAN Topology	-	-	-	-	-	-
VPN Topology	-	-	-	-	-	-
Log On	-	-	-	-	-	-

Services	Public Keys					
	TLS Public Key	TLS Peer Public Key	Authentication Public Key	Firmware Verification Key	ECDH Public Key	ECDH Peer Public Key
Log Off	-	-	-	-	-	-
Export Log	-	-	-	-	-	-
Filter Log	-	-	-	-	-	-
Generate Log Reports	-	-	-	-	-	-
TLS	E	IE	IE	-	E	-
Import/Export Certificates	-	-	-	-	-	-
Upload Firmware	-	-	-	E	-	-
Configure DNS Settings	-	-	-	-	-	-
Installation, Secure Initialization and placing the module in FIPS mode	-	-	-	-	-	-
Setup SMTP server	E	IE	IE	-	E	-
Setup two factor authentication	-	-	-	-	-	-
Setup Twilio	E	IE	IE	-	E	-
User Management	-	-	-	-	-	-
Zeroize	Z	Z	Z	Z	Z	Z

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 GCM KAT: Encryption, Decryption; Key size(s): 128 bits
- AES ECB KAT: Encryption, Decryption; Key size(s): 128, 192, 256 bits
- DRBG KAT: AES CTR DRBG; Security Strength(s): 256 bits
- ECDSA PCT: Signature Generation, Signature Verification; Curves/Key sizes: P-256 with SHA-256 and P-384 with SHA-384
- HMAC KAT: SHA sizes – SHA-1, SHA-256, SHA-384, SHA-512
- RSA KAT: Signature Generation, Signature Verification; Key sizes: 2048 with SHA-256, SHA-384 and 3072 bits with SHA-1, SHA-256 and SHA-384
- SHA KAT: SHA-256, SHA-384, SHA-512
- KDFs KAT: TLS 1.2
- TLS 1.3 KAT[6]: HKDF
- ECDH KAT (P-256 and P-384): EC Diffie-Hellman “Z” shared secret computation (SP800-56a rev3)
- SP800-90B Section 4.5 Vendor defined Health tests - the startup test runs over 65,536 samples which exceeds the requirement for 1024 samples.

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

- 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
- SP800-90B Section 4.5 Vendor defined Health tests

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 the 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.

[6] TLS 1.3 KDF is ACVTS tested and self-tested but not used in any of the services in 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 platform as listed in Table 1 of the document, which store the module within the enclosure. The referenced host platform meet Level 1 physical security requirements and is made of production grade material.

6. Operational Environment

The module operates in a limited operational environment per FIPS 140-2 Level 1 specifications. The module firmware version is 2.3.

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 FIPS 140-2 roles: User and Crypto 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. A user 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 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. 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 management IP address and Gateway should be configured for the module.
4. As the CO, the tester should login using the vendor-provided default login and password. The default password should be changed/updated.
5. Over the web interface, the tester should proceed to the System Settings page and update the settings to be consistent with Section 1.3.1 of this document, and then enabling FIPS mode by selecting the toggle button. Once the FIPS mode toggle button is enabled, the module must be reloaded for the FIPS mode of operation to take effect.

6. The tester shall observe that the module self-tests executed automatically before a login was possible. The tester will observe that the “FIPS Mode” toggle button is enabled to indicate that the module is in the Approved mode of operation. The tester can verify 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” toggle button is enabled, the module executes a compliance checking procedure, examining all settings related to the security rules. The user is responsible for updating the passwords described in Section 1.3.1 of the document, otherwise the module will not allow the user to set the “FIPS Mode” toggle button. Except for Step 1 setting of Section 1.3.1 of the document, once the “FIPS Mode” toggle button is enabled, irrespective of whether or not the operator has updated the other settings of Section 1.3.1 of the document, the module will reload and automatically update the settings of Section 1.3.1. In addition, as soon as the “FIPS Mode” toggle button is set, the module will automatically reload to enable the FIPS mode. The “FIPS Mode” toggle button is an indication that the module is running in the FIPS Approved mode of operation.

8.2 Transition of module to and from Approved mode of operation

The keys and CSPs generated in the cryptographic module during FIPS mode of operation cannot be used when the module transitions to non-FIPS mode and vice versa. While the module transitions from FIPS to non-FIPS mode or from non-FIPS to FIPS mode, all the keys and CSPs shall be zeroized by the Crypto Officer using the “Zeroize” service.

While transition from non-FIPS to FIPS mode, the CO has to zeroize all plaintext key and CSPs by issuing “Zeroize” service and then the CO has to follow Section 8.1 of the Security Policy to place the module in 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.*
[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*
[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*

Abbreviation	Full Specification Name
[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 800-56A 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
CO	Crypto Officer
CSP	Critical Security Parameter
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
LAN	Local Area Network
DH	Diffie-Hellman
GUI	Graphical User Interface
GCM	Galois/Counter Mode
SP	Security Policy

Acronym	Definition
SHA	Secure Hash Algorithm
HMAC	Hashed Message Authentication Code
TDEA	Triple Data Encryption Algorithm