SMA 6200 and SMA 7200
Non-Proprietary Security Policy

Document Version 1.3

SonicWall, Inc.

June 7, 2017

TABLE OF CONTENTS

1. Module Overview

The SonicWALL SMA 6200 (HW P/N 101-500399-57 Rev A, FW Version SRA 10.7.2-619) and SMA 7200 (HW P/N 101-500398-57 Rev A, FW Version SRA 10.7.2-619) are a multi-chip standalone cryptographic modules enclosed in hard, black, commercial grade metal cases. The primary purpose of these modules is to provide secure remote access to internal resources via the Internet Protocol (IP). The modules provide network interfaces for data input and output. The appliance encryption technology uses FIPS approved algorithms. FIPS approved algorithms are approved by the U.S. government for protecting unclassified data. Figure 1 depicts the module's cryptographic boundary which is defined as the outer perimeter of the chassis.

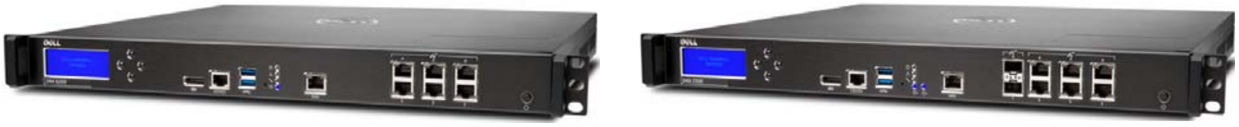

Figure 1 – SMA 6200 (Left) and SMA 7200 (Right)

2. Security Level

The cryptographic modules meet the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

The cryptographic modules support both an Approved and Non-Approved mode of operation.

3. Approved Mode of Operation

The cryptographic modules support the following FIPS Approved algorithms and security functions:

- CTR_DRBG SP 800-90A AES-128 (No prediction resistance; block_cipher_df instantiation)
  - avcrypto (Cert. #954)
- AES 128 and 256 bit in ECB and CBC mode encrypt and decrypt
  - avcrypto (Cert. #3626), libcrypto (Cert. #3627), ojdk (Cert. #3628)
- RSA 2048 bit key gen, signing and verification
  - libcrypto (Cert. #1869), ojdk (Cert. #1870)
- Triple-DES CBC 3-key
  - avcrypto (Cert. #2021), libcrypto (Cert. #2022), ojdk (Cert. #2023)
- SHA-1, SHA-256, SHA-384
  - avcrypto (Cert. #3044), libcrypto (Cert. #3045), ojdk (Cert. #3046)
- HMAC-SHA-1, HMAC-SHA-256
  - avcrypto (Cert. #2378), libcrypto (Cert. #2379), ojdk (Cert. #2380)
- SP 800-135 TLS 1.0, 1.1 and 1.2 KDFs
  - OpenSSL (Cert. #649) (CAVP Component validation list)
  - ojdk (Cert. #648) (CAVP Component validation list)
- SP 800-135 SSH KDF
  - OpenSSH (Cert. #647) (CAVP Component validation list)
- SP 800-135 SNMP KDF
  - Net-SNMP (Cert. #646) (CAVP Component validation list)

Note: The TLS, SSH, and SNMP protocols has not been reviewed or tested by the CAVP and CMVP

The cryptographic modules support the following allowed algorithms in the Approved mode:

- MD5 (Limited use within TLS) and Password Hash.
- RSA key wrapping (key establishment methodology 112 bits of strength)
- RSA 1024 bit verification of legacy firmware.
- RNG HAVEGE algorithm used to seed the CTR_DRBG.

Requirements for FIPS 140-2

The following items are required to properly configure the Approved mode for full compliance:

- An SMA 6200 or SMA 7200 appliance.

  CAUTION: For a SonicWALL SMA appliances with 140-2 Level 2 FIPS validation, the tamper evident seals affixed to it must remain in place.

- A license to run FIPS Approved mode. FIPS mode is not automatically enabled after a license is imported.
- A secure connection to the authentication server
- A strong administrator password, (8 to 14 characters), containing punctuation characters, numbers, and a combination of uppercase and lowercase letters. In addition, an authentication server must be specified when a realm is configured; "null auth" is not allowed.

Enabling FIPS Approved Mode

Before enabling FIPS Approved mode, a strong password, secure connection to the authentication server, and valid license are required.

To be FIPS-compliant, the password must be at least 8 characters long, but it is recommended that it be at least 14 characters. Although this recommendation is not enforced by the software, having a weak administrator password is a potential vulnerability. A strong password includes a mix of letters, numbers and symbols. Think of this as a phrase, not just a password. For instance, “I never saw a purple cow, I never hope 2C1.” has a combination of all three types of characters.

Only administrators with System rights can change the mode of operation. When in FIPS Approved mode, you will not be able to select non-compliant algorithms for session security.

To Enable the FIPS Approved mode:

1. In the main navigation menu, click **General Settings**, then click **FIPS Security**.
2. Click **Edit**.
3. If the license is imported, select the **Enable FIPS mode** check box.

   Note: Existing certificates will be removed from the system in the next step. To preserve the FIPS-compliant certificates, ensure that they have been exported.

4. Click **Save** and then apply the Pending changes.

! The appliance will be rebooted to apply these changes. Any connections will be terminated.

! Once in FIPS Approved mode, hand editing via the shell of any configuration files is not allowed and if done will cause the appliance to immediately reboot and be placed into single user mode for remediation by the primary administrator.

If the appliance configuration is known to not be FIPS compliant, FIPS compliance warning will be provided. Click on the link for more information on how to bring the appliance configuration into FIPS compliance.

Caution: The lack of this alert does not mean the environment is FIPS compliant. It is the operator's responsibility to ensure all of the FIPS prerequisites are met in order to be FIPS compliant.

Managing FIPS Compliant Certificates

Any keys generated on SMA 6200 or SMA 7200 appliances running in FIPS Approved mode will be FIPS compliant. If certificates are imported (and their associated public and private keys) to the appliance, it is the Crypto-Officer's or User's responsibility to make sure that they are also FIPS compliant. Certificates must be exported and then re-imported when switching FIPS mode on or off. For the export and import procedure, see "Exporting and Importing Certificates".

The best way to ensure that the certificates used are FIPS compliant is to generate all CSRs (certificate signing requests) on a FIPS-enabled appliance.

Exporting and Importing Certificates

If existing Certificate keys were generated on a FIPS-compliant system and are to be used after FIPS is enabled, they must be exported from the FIPS-compliant system and then imported after FIPS is enabled.

To export Certificates before the FIPS-mode transition:

1. In AMC, navigate to **SSL Setting > SSL Certificates > Click Edit**.
2. For each certificate to export, do the following:
    a. On the **Certificates** table, select a certificate and click the **Export** button.
    b. Enter a password for the exported **.p12** file.
    c. Click the **Save** button

To import certificates after the FIPS-mode transition:

1. In AMC, navigate to **SSL Settings > SSL Certificates> Click Edit**.
2. For each certificate to import, do the following:
    a. On the **Certificates** table, select **New > Import certificate...**.
    b. Select the certificate file to import.
    c. Enter the password for the **.p12** file.
    d. Click the **Import** button

Zeroization

Zeroization is the practice of permanently destroying all critical security parameters. This is accomplished by overwriting the entire disk with zeros. Zeroization makes it very hard to retrieve sensitive data from the appliance. It is used before recycling hardware, or in other cases where data security is more important than retaining the data. Once this operation is completed, the appliance can no longer be used at the site and must be returned to SonicWALL for replacement hardware to restore service.

To Zeroize the appliance:

1. Connect to the appliance using a serial connection, and log in as the Crypto Officer.
2. Type **factory_reset_tool --zeroize**.
3. Stay physically present with the appliance until the appliance halts.

! The appliance can take up to an hour to complete the zeroization process.

4. Non-Approved Mode of Operation

The cryptographic modules provide non-FIPS Approved algorithms as follows:

- MD5 with TLS and ESP
- RC4 with TLS

These algorithms are not usable in the Approved mode of operation and are available only when the system is not configured in FIPS mode.

Disabling FIPS Approved Mode

Turning off FIPS disables the FIPS feature and removes all of the constraints imposed by the FIPS mode prerequisites.

To disable FIPS:

1. From the main navigation menu, click **General Settings**, then click **FIPS Security**.
2. Click **Edit**.
3. Clear the box next to **Enable FIPS mode**.

   Note: Existing certificates will be deleted from the system in the next step. To preserve the existing certificates, ensure that they have been exported.
4. Click **Save** and then apply the Pending changes.

! The appliance will be rebooted to apply these changes. Any connections will be terminated.

! **Warning**: To be fully FIPS compliant, no FIPS critical security parameters shall be used outside of the FIPS Approved mode of operation. Zeroization must be performed prior to transitioning out of the Approved mode of Operation.

5. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

Ports	Type
Ethernet The cryptographic modules provide Ethernet interfaces. Ethernet interface 0 thru 5 are [10/100/1000] auto-sensing with an RJ- 45 connector. Ethernet interfaces 6-7 on the SMA 7200 only are 10000 SFP+ cavities and support a variety of transceivers including but not limited to SC, LC and 10GBase-CX-4 physical mediums. Each Ethernet interface includes LINK and ACT LEDs.	The 0 Ethernet interface provides Data In, Data Out, Status Out and Control In. It is not enabled when the 6 is enabled. The 1 Ethernet interface provides Data In and Data Out. It is not enabled when 7 is enabled. The 2 Ethernet interface provides Data In and Data Out. It is not supported in the Approved mode of operation. The 3 Ethernet interface, when enabled provides Status Out and Control In. The 4-5 Ethernet interfaces are not enabled and are reserved for future use. The 6 Ethernet 10G interface provide Data In, Data Out, Status Out and Control In. It is not enabled when the 0 interface is enabled. The 7 Ethernet 10G interface provides Data In and Data Out. It is not enabled when the 1 interface is enabled.
DIAG **The cryptographic module provides a diagnostic interface. This interface is a Ethernet [10/100/1000] RJ45 and includes LINK and ACT LEDs.**	The DIAG interface is used during the manufacturing process and is disabled.
USB The cryptographic module provides USB interfaces. Neither is supported in the Approved mode of operation.	Each USB interface shall not be used in the Approved mode of operation. The hardware platform is a common design with other models outside the scope of this validation which use this port.
Console The cryptographic module provides a single console interface. The console interface is a DB-9/RJ-45 serial connector. The serial port provides a serial console. The serial console can be used for basic administration functions.	The console interface provides Data In, Data Out, Status Out and Control In.
LED The cryptographic modules provide Status LEDs. The Power LED indicates the module is receiving power. The Test LED indicates the module is initializing and performing self-tests. The Alarm LED indicates an alarm condition.	The LED interface provides Status Out.

Ports	Type
LCD Screen The cryptographic module provides a single LCD screen interface. The LCD screen is used to display basic setup information.	The LCD interface provides Status Out.
eSATA The cryptographic module provides a eSATA interface. Neither is supported in the Approved mode of operation.	The eSATA interface shall not be used in the Approved mode of operation. The hardware platform is a common design with other configurations which use this port.
4-Button Panel The cryptographic module provides a single 4-button panel interface. The 4-button panel is used to control the LCD screen display. Inputting of setup information is not supported in the Approved mode of operation.	The 4-button panel interface provides Control In.
Power The cryptographic module provides power interfaces.	The power port provides Power In. The power is activated by a front panel power switch.

6. Identification and Authentication Policy

Assumption of roles

The cryptographic modules support administrator roles (User and Cryptographic Officer) and the VPN End User role.

Cryptographic Officer and User must authenticate with the AMC GUI console via the GUI Administration Interface and a HTML forms-based username and password method. The username and password are validated with an internal database. Once validated, the username is mapped into either the User or Cryptographic Officer role.

Cryptographic Officers may also utilize a command line shell for basic administration purpose by authenticating using the password over either the SSH Administration Interface or the Console Interface.

The VPN End User accesses the routing and data handling of the VPN device. Authentication is provided by username and password or by an authenticated external AAA server.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Username and Password
Cryptographic-Officer	Identity-based and Role-based operator authentication	Username or Role and Password
VPN End User	Identity-based authentication.	Username and Password or Transitive trust with authentication of the external AAA server utilizing either X.509 certificates or shared secrets.

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	The Cryptographic Officer and User passwords must be at least eight characters long each, and the password character set is ASCII characters 32-127, which is 96 ASCII characters. This makes the probability, 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. After three 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, 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.
Transitive AAA with shared secret	When shared secrets are employed with external AAA servers, strong passwords must be used. These strong passwords have the same strength properties as the Username and Password previously described.
Transitive AAA with X.509	When X.509 certificates are employed with external AAA servers, the AAA server is authenticated via its TLS presented certificate with key sizes of 2048 bits The probability is between 1 in 2^80, 1 and 1 in 2^112 which is less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur for each attempt. Based on processing limitations, at most 600 digital signatures can be verified in a one minute period. The probability is between 1 in 600/2^80 and 1 in 600/2^112, 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.

7. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
Cryptographic-Officer	**Module Initialization** – Initial configuration of module in the non-approved mode. **Security Administration** – Administrator access to pages for access control rules, resources, users and groups, web portal services and client end point control. **System Configuration** – Administrator access to pages for network settings, general appliance settings, SSL settings, access and network services, and authentication. **System Maintenance** – Administrator permission to shut down or restart the appliance, update or roll back the system software, and import or export configuration data. **System Monitoring** – Read access permits the administrator to view system logs and graphs, view active users and run troubleshooting tools. Write access permits termination of VPN End Users and to change logging levels. **Remote Assistance** – Read access permits viewing of the service configuration and the trouble ticket queue. Write access permits modify the service configuration and reorder the trouble ticket queue. **Update Firmware**– Write access permits installing updates to the firmware. **Verify Image Signature** –Read access permits access to filesystem integrity check status in the management console. **Initiate FIPS mode** – Write access permits entering the approved mode of operation. **Initiate non-FIPS mode** – Write access permits leaving the approved mode of operation. **Establish SSH connection** – Execute access permits access to the module over a secure network connection. **System Zeroize** – Zeroizes the hard disk and firmware portion of flash by writing zeros to these areas.
User	**Security Administration** – Rights are delegated by the Crypto-Officer and can be none, read only or read/write. **System Configuration** – Rights are delegated by the Crypto-Officer and can be none, read only or read/write. **System Maintenance** – Rights are delegated by the Crypto-Officer and can be none, read only or read/write. **System Monitoring** – Rights are delegated by the Crypto-Officer and can be none, read only or read/write. **Remote Assistance** – Rights are delegated by the Crypto-Officer and can be

Role	Authorized Services
	none, read only or read/write. **Update Firmware** – Rights are delegated by the Crypto-Officer and can be none or write. **Verify Image Signature** – Rights are delegated by the Crypto-Officer and can be none or read. **System Zeroize** – Rights are delegated by the Crypto-Officer and can be none or allowed to zeroize the hard disk and firmware portion of flash by writing zeros to these areas.
VPN End User	**Send and receive network traffic** – route traffic via the VPN TLS and VPN ESP interfaces. Cryptographic Encryption, Decryption and all CSP state management are outside the control of the VPN End User and are maintained by the cryptographic module according to the security policies of the Cryptographic Officer.

Note: the same set of services are available when the module is operating in the Non-Approved mode of operation.

Unauthenticated Services:

The cryptographic modules support the following unauthenticated services, none of which disclose, modify or substitute CSP, use approved security functions, or otherwise affect the security of the cryptographic modules:

- Show Status: This service provides the current status of the cryptographic module on the LED and LCD interfaces.
- Self-tests: This service executes the suite of self-tests required by FIPS 140-2. Performed by power-cycling or rebooting the module.

Table 5 - Definition of Critical Security Parameters (CSPs)

Key / CSP	Description/Usage	Generated / Derived	Storage	Entry/Output	Destruction
AMC TLS private key	RSA 2048 bit private key used in the TLS negotiation for web administration GUI.	Externally or Internally	Plaintext	Encrypted via TLS session	System Zeroization
WorkPlace Site TLS private key(s)	RSA 2048 bit key used in TLS handshakes for VPN sessions. There is one key for each WorkPlace site VPN TLS interface.	Externally or Internally	Plaintext	Encrypted via TLS session	System Zeroization
SSH private key	RSA private key is used in Administration shell SSH negotiation. Key length is 2048.	Internally	Plaintext	Not Applicable	System Zeroization
SAML private key	RSA private key (certs) are used for digital signing of AAA SAML requests. Key length is 2048.	Generated internally using CTR_DRBG	Plaintext	Imported / Exported in PKCS12 format Or Passphrase entered via web Administration GUI	Deleted from key store when the Self-Signed or 3rd Party Certificate is removed, or when disk is wiped.
SNMPv3 Shared Secret	Symmetric HMAC-SHA-256 160bit shared secret is used to verify the authenticity of SNMP messages being sent and received.	Generated internally using CTR_DRBG	Plaintext	Passphrase entered via web Administration GUI	Deleted when the keys are removed from key store or when disk is wiped
Firmware Integrity shared secret	Symmetric HMAC-SHA-1 160 bit shared secret is used to verify firmware integrity.	Externally	Plaintext	Loaded during manufacturing	System Zeroization
Keystore Password Encryption shared secret	Symmetric Triple-DES 192 bit secret key is used to encrypt passwords.	Externally	Plaintext	Loaded during manufacturing	System Zeroization
ESP Session Authentication Keys	Symmetric HMAC-SHA-256 160 bit shared secret for ESP session. Used to authenticate an ESP session.	Generated internally using CTR_DRBG	Plaintext	Not Applicable	ESP session ends and System Zeroization.

Key / CSP	Description/Usage	Generated / Derived	Storage	Entry/Output	Destruction
ESP Session Encryption Keys	Symmetric AES 128, 256 bit shared secret for ESP session. Used to encrypt an ESP session.	Generated internally using CTR_DRBG	Plaintext	Not Applicable	ESP session ends and System Zeroization.
TLS Session Authentication Keys	Symmetric HMAC-SHA-256 160 bit shared secret for TLS session. Used to authenticate a TLS session.	Generated internally using CTR_DRBG	Plaintext	Not Applicable	TLS session ends and System Zeroization.
TLS Session Encryption Keys	Symmetric AES 128, 256 bit or Triple-DES 192 bit shared secret for TLS session. Used to encrypt a TLS session.	Generated internally using CTR_DRBG	Plaintext	Not Applicable	TLS session ends and System Zeroization
TLS Shared Secret	Shared secret for TLS session. Used to establish a TLS session.	Externally or Internally	Plaintext	Encrypted via TLS handshake	Process completion and System Zeroization
Passwords	Authentication Passwords	N/A	Hashed	Hashed, except via console	System Zeroization
DRBG seeding material	Seeding the Approved DRBG	Internally	Plaintext	Not Applicable	System Zeroization
DRBG State	SP 800-90A CTR_DRBG V and K values (AES 128)	Internally	Plaintext	Not Applicable	System Zeroization

Note: The module generates cryptographic keys whose strengths are modified by DRBG security strength.

Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Generate: This operation generates keys using the FIPS Approved DRBG
- Read: Export the CSP
- Write: Enter/establish and store a CSP
- Destroy: Overwrite the CSP
- Execute: Employ the CSP

Table 6 - CSP Access Rights within Roles & Services

Roles			Services	Cryptographic Keys and CSPs Access Operation
CO	**User**	**VPN User**		
X			Module initialization	None
X	X[1]		System Maintenance	Firmware Integrity Shared Secret (Execute) Passwords (Read/Write) AMC Private Key (Read/Write) Work Place Site Private Keys (Read/Write) SAML Private Key (Read/Write) SNMPv3 (Read/Write)
X	X[1]		Security Administration	Passwords (Read/Write)
X	X[1]		System Monitoring	Password (Read) SSH Private Key (Read, Execute) AMC Private Key (Read, Execute)
X	X[1]		System Configuration	Passwords (Read/Write) AMC Private Key (Generate/Read/Write/Execute) Work Place Site Private Keys (Generate/Read/Write) SSH Private Key (Generate/Execute) SAML Private Key (Generate/Read/Write) SNMPv3 Shared Secret (Generate/Read/Write)
X	X[1]		Remote Assistance	Work Place Site Private Keys (Execute)
X			System Zeroize	Passwords(Destroy) AMC Private Key (Destroy) Work Place Site Private Keys (Destroy) SSH Private Key (Destroy) SAML Private Key (Destroy) SNMPv3 Shared Secret (Destroy) Firmware Integrity Shared Secret (Destroy) Keystore Password Encryption Shared Secret (Destroy) TLS Shared Secret (Destroy) TLS Session Encryption Keys (Destroy) TLS Session Authentication Keys (Destroy) ESP Session Encryption Keys (Destroy) ESP Session Authentication Keys (Destroy) DRBG Seed Material (Destroy)
		X	Send and receive	Passwords (Read/Write)

Roles			Services	Cryptographic Keys and CSPs Access Operation
			network traffic	AMC Private Key (Execute) Work Place Site Private Keys (Execute) SSH Private Key (Execute) TLS Shared Secret (Write/Execute) TLS Session Encryption Keys (Write/Execute) TLS Session Authentication Keys (Write/Execute) ESP Session Encryption Keys (Write/Execute) ESP Session Authentication Keys (Write/Execute)
X	X[1]		Update firmware	Firmware Integrity Shared Secret (Read)
X	X[1]		Verify image signature	Firmware Integrity Shared Secret (Read)
X			Initiate FIPS mode	Passwords(Destroy) AMC Private Key (Destroy) Work Place Site Private Keys (Destroy) SSH Private Key (Destroy) SAML Private Key (Destroy) SNMPv3 Shared Secret (Destroy) Firmware Integrity Shared Secret (Destroy) Keystore Password Encryption Shared Secret (Destroy) TLS Shared Secret (Destroy) TLS Session Encryption Keys (Destroy) TLS Session Authentication Keys (Destroy) ESP Session Encryption Keys (Destroy) ESP Session Authentication Keys (Destroy) DRBG Seed Material (Destroy)
X			Initiate non-FIPS mode	Passwords(Destroy) AMC Private Key (Destroy) Work Place Site Private Keys (Destroy) SSH Private Key (Destroy) SAML Private Key (Destroy) SNMPv3 Shared Secret (Destroy) Firmware Integrity Shared Secret (Destroy) Keystore Password Encryption Shared Secret (Destroy) TLS Shared Secret (Destroy) TLS Session Encryption Keys (Destroy) TLS Session Authentication Keys (Destroy) ESP Session Encryption Keys (Destroy)

Roles			Services	Cryptographic Keys and CSPs Access Operation
				ESP Session Authentication Keys (Destroy) DRBG Seed Material (Destroy)
X			Establish SSH connection	Passwords (Read) SSH Private Key (Read, Execute)

[1] Rights must be explicitly delegated by the Crypto-Officer to the User. These rights may be restricted to read only or full rights at the discretion of the Crypto-Officer.
[2] User cannot generate their own password nor can they generate the Crypto-Officer password.

Table 7 - Definition of Public Keys

Public Keys	Description/Usage	Storage
License Verification public key	RSA public key used to verify product license and authenticity. Key length 2048 for 10.7.1 and newer.	Stored in fixed disk as plaintext
AMC TLS public key	RSA public key is used for Administration GUI TLS negotiation. Key length is 2048.	Stored in fixed disk as plaintext
WorkPlace Site TLS public key(s)	RSA public keys are used for VPN TLS negotiation. Key length is 2048.	Stored in fixed disk as plaintext
SSH public key	RSA public key is used in Administration shell SSH negotiation. Key length is 2048.	Stored in fixed disk as plaintext
Destination Web Server public keys	RSA public keys are used by cryptographic module VPN web proxy service to establish VPN TLS sessions with HTTPS web server resources. Key length is 2048.	Stored in fixed disk as plaintext
AAA Server public keys	RSA public keys are used by cryptographic module policy service to establish VPN TLS sessions with LDAPS AAA servers, and for verifying digital signatures from SAML and OCSP AAA servers. Key length is 2048.	Stored in fixed disk as plaintext
Trusted CA public keys	RSA public keys are used by cryptographic module to validate X.509 certificate chains from VPN client devices. Key length is 2048.	Stored in fixed disk as plaintext

8. Operational Environment

The FIPS 140-2 Operational Environment requirements are not applicable because the module only allows the loading of firmware through the firmware load test, which ensures the image is appropriately HMAC authenticated by SonicWALL.

9. Security Rules

The cryptographic modules' design corresponds to the cryptographic modules' security rules. This section documents the security rules enforced by the cryptographic modules to implement the security requirements of these FIPS 140-2 Level 2 modules.

1. The cryptographic module provides distinct operator roles. These are the User role and the Cryptographic Officer role. Additionally, the module supports a VPN End User role.
2. The cryptographic module provides identity-based and role-based authentication.
3. When the module is not placed in a valid role, the operator does not have access to any cryptographic services.
4. The cryptographic module encrypts message traffic using the AES or Triple-DES algorithms.
5. The cryptographic module performs the following tests automatically without operator intervention:

   A. Power up Self-Tests:

Test Target	**Description**
DRBG	KATs: SP 800-90A CTR_DRBG Instantiate, Generate, Reseed. Modules: avcrypto (DRBG Cert. #954)
AES	KATs: Encryption and Decryption Mode: CBC Key sizes: 128 bits, 256 bits Modules: avcrypto, libcrypto, ojdk (AES Certs. #3626, #3627 and #3628) Mode: ECB Key sizes: 128 bits, 256 bits Modules: avcrypto (AES Cert. #3626)
RSA	KATs: Signature Generation, Signature Verification, Key Generation Key sizes: 2048 bits Modules: libcrypto, ojdk (RSA Certs. #1869, #1870)
Triple-DES	KATs: Encryption, Decryption Modes: TECB, Key sizes: 3-key Modules: avcrypto, libcrypto, ojdk (Triple-DES Certs. #2021, #2022 and #2023)
SHA	KATs: SHA-1, SHA-256, SHA-384 Modules: avcrypto, libcrypto, ojdk (SHA Certs. #3044, #3045 and #3046)
HMAC	KATs: Generation, Verification SHA sizes: SHA-1, SHA-256 Modules: avcrypto, libcrypto, ojdk (HMAC Certs. #2378, #2379 and #2380)

B. Firmware Integrity Test

- Firmware integrity test of CSPs and CSP processing components using 160 bit HMAC-SHA-1 and 16 bit CRC are performed on each power up cycle.

C. Critical Functions Tests

- CSP integrity is performed at each system configuration invocation and configuration update

D. Conditional Self-Tests:

- Continuous Random Number Generator (RNG) test – performed on Non-Approved RNG and Approved DRBG
- RSA pairwise consistency test for generation of asymmetric keys
    a. For signature generation and verification
    b. For key encryption and decryption
- Firmware Load Test: When a new firmware image or patch is loaded, the cryptographic module verifies the 160 bit HMAC-SHA-1 of the image. If this verification fails, the firmware image loading is aborted and the module reboots. Note that updating the module's firmware will take the module out of the FIPS Approved mode of operation.

6. Power-up self-test is performed on demand by rebooting or power-cycling the module the appliance.
7. The module inhibits data output during power up self-tests 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. The module supports concurrent use by VPN End Users and the system's Crypto-Officer or User.
10. If any of the self-tests fail, the cryptographic module enters an error state. No VPN services are provided in the error state.
11. Certificates are entered and output from the module in PKCS #12 format, which obfuscates the embedded keys but does not protect them. All import and export of key values shall be performed over VPN tunnels.
12. Zeroization overwrites all CSPs. Performance of the zeroization process will prevent the module from successfully booting, effectively disabling the module. The operator is required to be physically present while the module completes this process. The process may take up to one hour to complete.
13. The module does not share CSPs between the Approved mode of operation and the non-Approved mode of operation.

14. The following are required configuration and steps must be performed to operate in the Approved mode:

    A. Do not used unsecured connections with authentication servers.

    B. Do not use RADIUS authentication servers

    C. Do use LDAP authentications servers without using LDAP connections employing only FIPS Approved ciphers.

    D. Do not use Active Directory single domain authentication servers without using TLS connections employing only FIPS Approved ciphers.

    E. Do use RSA Authentication Manager authentication servers without using TLS connections employing only FIPS Approved ciphers.

    F. Do not use RSA Authentication Manager servers without strong passwords as shared secrets.

    G. Do not use USB devices for any purpose.

    H. Do not use eSATA devices for any purpose.

    I. Do not use clustering (High Availability). Clustering (HA) is not supported in FIPS mode.

    J. Do not use with SonicWALL GMS or Viewpoint servers.

    K. Do not Load or unload any kernel modules via the shell command line.

    L. Do not Install third party software via the shell command line.

    M. Do not attempt Firmware upgrades via the shell command line.

    N. Do not use Debug 1, Debug 2, Debug 3 or plaintext logs.

    O. Do not use certificates with private/public key-pairs generated by non_FIPS validated systems.

    P. The FIPS Approved mode must be enabled as described in "Enabling FIPS Approved Mode".

This section summarizes the security rules imposed by the vendor:

1. Before enabling FIPS mode, a strong password, secure connection to the authentication server, and valid license are required.
2. If any of the Power up Self-Test, CSP Firmware Integrity Tests or Conditional Self-Tests fail, the cryptographic module enters an error state. No VPN services are provided in the error state.
3. When all power-up self-tests are completed successfully, an LED indicator is provided and status is available via logs and/or console access.

10. Physical Security Policy

Physical Security Mechanisms

The cryptographic modules each include the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Tamper-evident material and two seals
- Protected vents

Operator Required Actions

The operator is required to periodically inspect tamper-evident seals.

Table 8 - Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	**Recommended Frequency of Inspection/Test**	**Inspection/Test Guidance Details**
Tamper-Evident Seals	Inspect tamper-evident seals monthly.	*See the SonicWALL Aventail Secure Remote Access Installation and Administration Guide Version 10.7 for procedure.*

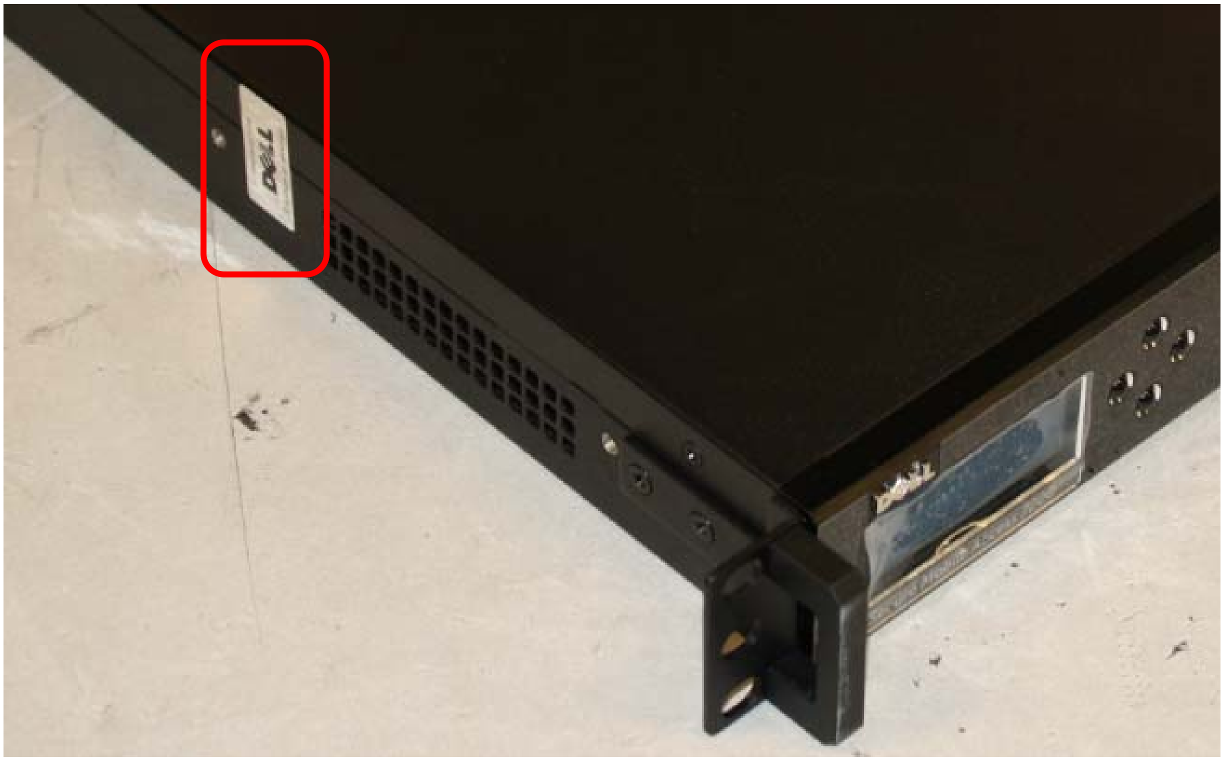

Figure 2 - Tamper Seal #1 –Chassis Seam

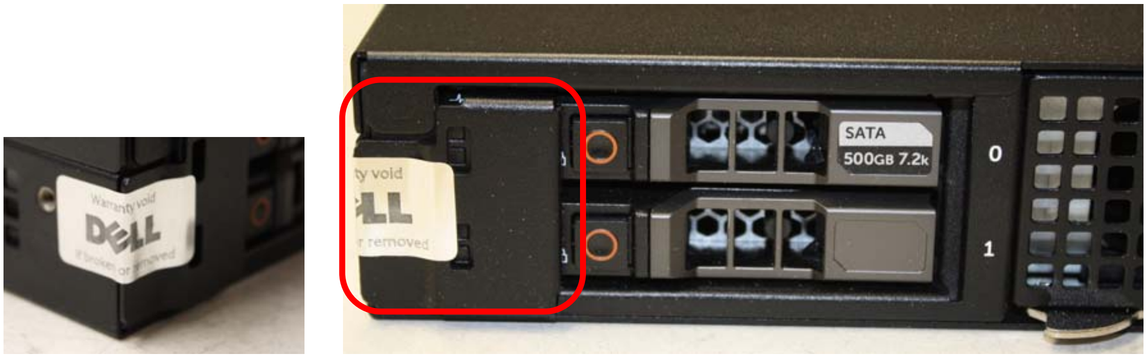

Figure 3 - Tamper Seal #2 – Tamper seal over drive bay protective plate

11. Mitigation of Other Attacks Policy

The modules have not been designed to mitigate attacks outside the scope of FIPS 140-2.

12. References

[ESP] Kent, S., “IP Encapsulating Security Payload (ESP)”, RFC 4303, Internet Engineering Task Force, December 2005.

[LDAP] Semersheim, J., Ed., “Lightweight Directory Access Protocol (LDAP): The Protocol”, RFC 4511, Internet Engineering Task Force, June 2006.

[RADIUS] Rigney, C., Rubens, A., Simpson, W. and S. Willens, “Remote Authentication Dial In User Service (RADIUS), RFC 2865, Internet Engineering Task Force, June 2000.

[SSH] Ylonen, T. and C. Lonvick, “The Secure Shell (SSH) Connection Protocol”, RFC 4254, Internet Engineering Task Force, January 2006.

[TLS] Dierks, T., and E. Rescoria, “The Transport Layer Security (TLS) Protocol Version 1.2”. RFC 5246, Internet Engineering Task Force, August 2008.

13. Definitions and Acronyms

AES	Advanced Encryption Standard
AMC	Administration Management Console
CA	Certificate Authority
CBC	Cipher Block Chaining
CSP	Critical Security Parameter
DES	Data Encryption Standard
RNG	Random Number Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ESP	Encapsulated Security Payload
FIPS	Federal Information Processing Standard
GMS	Global Management System
GUI	Graphical User Interface
HAVEGE	Hardware Volatile Entropy Gathering and Expansion
HMAC	Hashed Message Authentication Code
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PKCS #12	Public-Key Cryptography Standards
RADIUS	Remote Authentication Dial-In Service
RSA	Rivest, Shamir, Adleman asymmetric algorithm
SAML	Security Assertion Markup Language
SNMP	Simple Network Management Protocol
SHA	Secure Hash Algorithm
SSH	Secure Shell
Triple-DES	Triple Data Encryption Standard
VPN	Virtual Private Network