# SonicWALL SMA Series v11.4
# EX6000, EX7000, EX9000, SMA 6200, SMA 7200

## FIPS 140-2 Non-Proprietary Security Policy

## Document Version: 1.4
## Date: May 4, 2017

# Contents



# Tables

# Figures

# 1 Introduction

The SonicWALL SMA Series v11.4, also referred to as "the Module", are multi-chip standalone cryptographic modules enclosed in hard, commercial grade metal cases. The cryptographic boundary for these modules is the enclosure. 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.

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

| | Module | HW P/N and Version | FW Version |
|---|---|---|---|
| 1 | SRA EX6000 | 101-500210-78 Rev A | 11.4.0-512 |
| 2 | SRA EX7000 | 101-500188-79 Rev A | 11.4.0-512 |
| 3 | SRA EX9000 | 101-500352-62 Rev A | 11.4.0-512 |
| 4 | SMA 6200 | 101-500399-61 Rev B | 11.4.0-512 |
| 5 | SMA 7200 | 101-500398-61 Rev B | 11.4.0-512 |

***Table 1 – Cryptographic Module Configurations***

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

| Security Requirement | Security Level |
|---|---|
| Cryptographic Module Specification | 2 |
| Cryptographic 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 |

***Table 2 – Security Level of Security Requirements***

## 1.1 Hardware

The physical forms of each configuration of the module are depicted in Figure 1.

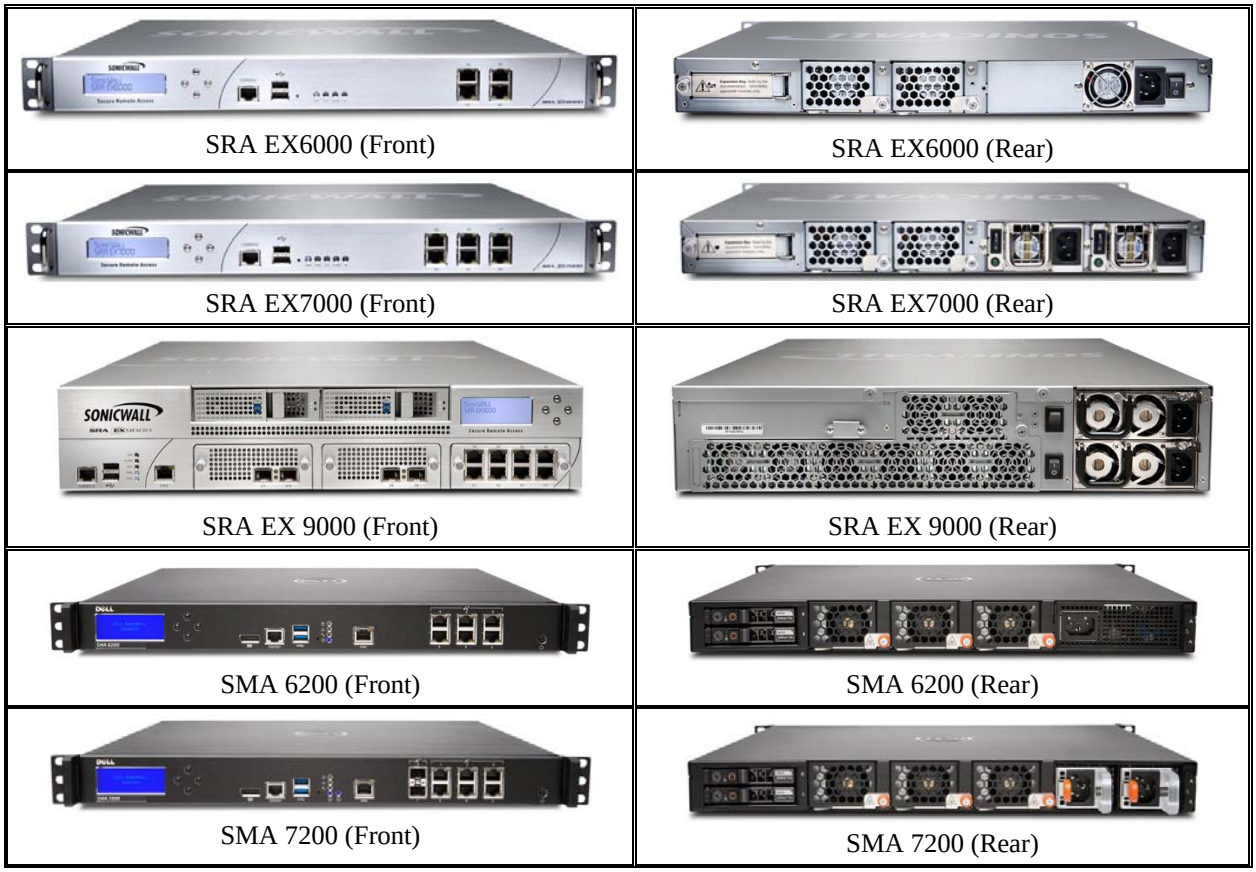


***Figure 1 – Physical form of all Module configurations***

| Port | Description | Logical Interface Type |
|---|---|---|
| Console | Serial (all configurations) and DisplayPort (SMA 6200/7200 only) command line interface | Control in, Status out |
| DIAG | Ethernet port for manufacturing: EX9000, SMA 6200 and SMA 7200 only. | N/A: Used only during manufacturing process; disabled prior to product delivery. |
| eSATA | Disk interface. | N/A: Not used in approved mode. The hardware platform design is common with other configurations that use this port. |
| Ethernet | Network traffic connections.<br>EX6000: 4 ports SMA 6200: 6 ports<br>EX7000: 6 ports SMA 7200: 8 ports<br>EX9000: 12 ports | Control in, Data in, Data out, Status out |
| Display buttons | Four (4) buttons used to navigate LCD displays. | Control in |
| Display | LCD display for basic status information. | Status out |
| LEDs | Unit level: Disk Activity, Test, Alarm and Power (1 or 2 LEDs). Ethernet: Link and Activity LEDs. | Status out |
| Power | AC power, inclusive of switch. EX9000, EX7000 and SMA 7200 have dual (redundant) power supplies. | Power |
| USB | Two (2) USB ports, used for disaster recovery only. | N/A: Not for use in approved mode |

***Table 3 – Ports and Interfaces***

## 1.2 Modes of Operation

The module's Management Console provides the mechanism to configure the module for the Approved mode of operation, found in *General Settings* > *Configure FIPS Security*. Attempts to check the *Enable FIPS mode* checkbox execute a FIPS Approved mode compliance checking tool, which enforces the use of only the FIPS Approved mode ciphers listed in Table 4 below, and provides clearly visible warnings if any of the the following configuration conditions are not met:

- The following authentication servers may be used, if connected using only FIPS approved ciphers:
  - LDAP
  - Active Directory single domain
  - RSA Authentication Manager
- Use of RADIUS authentication servers is not permitted in the Approved mode.
- Clustering (High Availability) is not supported in FIPS mode.
- Configured connections with SonicWALL GMS or Viewpoint servers are not permitted in the Approved mode.

In the non-Approved mode, the additional ciphersuites shown in Table 5 are available for use by the AMC Interface and VPN Network Traffic services, and the features cited in the bullets above are available for use. See Section 8, *Security Rules and Guidance* for additional Approved mode operation guidance.

# 2 Cryptographic Functionality

The cryptographic protocols and primitves implemented and used by the modules are listed in this section. Table 4 and 5 list the TLS ciphersuites available in the Approved and non-Approved modes, respectively. Table 6 lists the SSH security methods; unlike TLS ciphersuites, SSH methods are independently selectable and may be used in any combination.

| Cipher Suite String (IETF enumeration) | TLS | Key Exchange | Cipher | Auth |
|---|---|---|---|---|
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 | 1.2 | ECDH_P384 | AES-128 | GCM |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 | 1.2 | ECDH_P384 | AES-256 | GCM |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | 1.2, 1.1, 1.0 | RSA | Triple-DES | SHA-1 |
| TLS_RSA_WITH_AES_128_CBC_SHA | 1.2, 1.1, 1.0 | RSA | AES-128 | SHA-1 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 | 1.2 | RSA | AES-128 | SHA-256 |
| TLS_RSA_WITH_AES_256_CBC_SHA | 1.2, 1.1, 1.0 | RSA | AES-256 | SHA-1 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 | 1.2 | RSA | AES-256 | SHA-256 |

***Table 4 – Management Console and VPN session TLS Ciphersuites used in the Approved mode***

| Cipher Suite String (IETF enumeration) | TLS | Key Exchange | Cipher | Auth |
|---|---|---|---|---|
| SSL_RSA_WITH_RC4_128_SHA | 1.2, 1.1, 1.0 | RSA | RC4 | SHA-1 |
| TLS_RSA_WITH_AES_128_CBC_SHA | 1.2, 1.1, 1.0 | RSA | AES-128 | SHA-1 |
| TLS_RSA_WITH_AES_256_CBC_SHA | 1.2, 1.1, 1.0 | RSA | AES-256 | SHA-1 |
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256[1] | 1.2 | ECDHE_P384 | AES-128 | GCM |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384[1] | 1.2 | ECDHE_P384 | AES-256 | GCM |

***Table 5 – TLS Ciphersuites used in the non-Approved mode***

| Key Exchange |
|---|
| ecdh-sha2-nistp256 |
| ecdh-sha2-nistp384 |
| Server Host Key (Authentication) |
| ecdsa-sha2-nistp384 |
| ssh-rsa |
| Digest |
| hmac-sha2-256 |
| hmac-sha1 |
| Encryption |
| aes256-gcm |
| aes256-cbc |
| aes128-cbc |

***Table 6 – SSH Security Methods Available (Approved and non-Approved modes)***

The module uses IPsec ESP mode only over UDP for data transport, using AES-128 and AES-256 in CBC or GCM mode. IKE is not used; rather, the keys and IVs are generated by the module and provided to the peer over an out-of-band TLS tunnel.

| Cipher Suite String (IETF enumeration) | Cipher | Auth |
|---|---|---|
| AES128-CBC-SHA | AES-128 | SHA-1 |
| AES128-CBC-SHA256 | AES-128 | SHA256 |
| AES128-GCM | AES-128 | GCM |
| AES256-CBC-SHA | AES-256 | SHA-1 |
| AES256-CBC-SHA256 | AES-256 | SHA256 |
| AES256-GCM | AES-256 | GCM |

***Table 7 – IPsec ESP Cipher and Digest Methods Available***

[1] Uses the secp160k1 Koblitz curve defined by secg.org, with strength below the minimum required by FIPS 140-2

| CAVP | Algorithm | Mode/Method | Strength[2] | Useage |
|---|---|---|---|---|
| 4044 | AES [197],[38A], [38D] | CBC, ECB, GCM | 128, 256 | Data Encryption/ Decryption [A]. |
| 4045 | AES [197],[38A], [38D] | CBC, ECB, GCM | 128, 256 | Data Encryption/ Decryption [O]. |
| 4046 | AES [197],[38A], [38D] | CBC, ECB, GCM | 128, 256 | Data Encryption/ Decryption [L]. |
| 869 | CVL-SNMP[3] KDF [135] | SHA-1 | | SNMP AES key KDF. |
| 870 | CVL-TLS[3] KDF [135] | TLS 1.0/1.1/1.2 (SHA-256) | | TLS session keys KDF [L] |
| 871 | CVL-SSH[3] KDF [135] | SHA-1, SHA-256 | | SSH v2 session key KDF |
| 872 | CVL-TLS[3] KDF [135] | TLS 1.0/1.1/1.2 (SHA-256) | | TLS session keys KDF. [O] |
| 1211 | DRBG[4] [90A] | CTR_DRBG | {128}, 256 | Random Bit Generation [A]. |
| 906 | ECDSA [186] | P-256 (SHA-256)<br>P-384 (SHA-384) | | ECC Key Generation; Digital Signature Generation, Verification [O]. |
| 907 | ECDSA [186] | P-256 (SHA-256)<br>P-384 (SHA-384) | | ECC Key Generation; Public Key Validation; Digital Signature Generation, Verification [L]. |
| 2639 | HMAC [198] | HMAC-SHA-1<br>HMAC-SHA-256 | 128<br>256 | Message Authentication [A]. |
| 2640 | HMAC [198] | HMAC-SHA-1<br>HMAC-SHA-256 | 128<br>256 | Message Authentication. [O] |
| 2641 | HMAC [198] | HMAC-SHA-1<br>HMAC-SHA-256 | 128<br>256 | Message Authentication. [L] |
| 2076 | RSA [186] | n=1024<br>n=2048 (SHA-256, SHA-384)<br>n=3072 (SHA-256, SHA-384) | | RSA Key generation; Digital Signature Generation and Verification [O]. 1024 bit keys are used for firmware signature verification only, in a fallback scenario. |
| 2077 | RSA [186] | {n=1024}<br>n=2048 (SHA-256, SHA-384)<br>n=3072 (SHA-256, SHA-384) | | RSA Key generation; Digital Signature Generation and Verification. [L] |
| 3333 | SHS [180] | SHA-1, SHA-256, SHA-384 | | Message Digest generation. [A] |
| 3334 | SHS [180] | SHA-1, SHA-256, SHA-384 | | Message Digest generation. [O] |
| 3335 | SHS [180] | SHA-1, SHA-256, SHA-384 | | Message Digest generation. [L] |
| 2211 | Triple-DES [67] | TCBC | 3-Key (112) | Data Encryption/ Decryption [A] |
| 2212 | Triple-DES [67] | TCBC | 3-Key (112) | Data Encryption/ Decryption [O] |
| 2213 | Triple-DES [67] | TCBC | 3-Key (112) | Data Encryption/ Decryption [L] |

***Table 8 – Approved algorithms (Implementations: [ A]=avcrypto; [L]= libcrypto; [O] = ojdk)***

References to standards are given in square bracket [ ]; see the References table.
Items enclosed in curly brackets { } are CAVP tested but not used by the module in the Approved mode.
The module uses only the RSA functions shown above in the Approved mode under 186-4.

[2] Strength indicates DRBG Strength, Key Lengths, Curves or Moduli
[3] The TLS, SSH, and SNMP protocols have not been reviewed or tested by the CAVP and CMVP
[4] No prediction resistance; block_cipher_df used for instantiation.

| Algorithm | (Establishment) Strength | Use |
|---|---|---|
| Elliptic Curve Diffie-Hellman | Provides 128 or 192 bits of encryption strength. | Key establishment |
| HMAC-SHA-1-96 | The underlying HMAC-SHA-1 uses a 160 bit key; per SP 800-157, this corresponds to 128 bits of strength. | SNMP message authenticity. |
| MD5 | | TLS 1.0/1.1, password obfuscation. |
| NDRNG | Internal entropy source with rationale to support the claimed DRBG security strength. | Entropy input to Cert. #1211 DRBG. |
| RSA | Signature verification using legacy (n=1024) key. | Legacy firmware signature verification, fallback use only. |
| RSA Key Wrapping | Provides 112 or 128 bits of encryption strength. | Key establishment |

***Table 9 - Allowed Algorithms***

| Algorithm | Use |
|---|---|
| RC4 | Element of TLS ciphersuite allowed only in non-approved mode. |
| Elliptic Curve Diffie-Hellman And ECDSA using P-160 | Element of TLS ciphersuite allowed only in non-approved mode. |

***Table 10 - Non-Approved Algorithms (Used only in the non-Approved Mode)***

## 2.1 Critical Security Parameters

All CSPs used by the module are described in this section.

| Name | Description and usage |
|---|---|
| AUTH-PW | Authentication Passwords, minimum of 8 characters, printable character set (96 unique values). |
| DRBG-EI | Entropy input (256 bits) to the block_cipher_df used to instantiate the Approved CTR_DRBG. |
| DRBG-STATE | SP 800-90A CTR_DRBG V and K values (AES-256 Key, 128-bit V, per IG 14.5). |
| ESP-SENC | ESP Session Encryption key. AES-128 or AES-256 key for IPsec ESP tunnel message encrypt/decrypt. |
| ESP-SMAC | ESP Session Authentication Keys. HMAC-SHA-1 160-bit / HMAC-SHA-256 256-bit session key for IPsec ESP message authentication. |
| OS-FWK | FirmWare authenticity key. HMAC-SHA-256 256-bit key used to verify firmware authenticity; HMAC-SHA-1 160 bit key may be used for fallback scenarios only. |
| OS-KEK | Key(store) encryption key. Triple-DES 192 bit key is used to encrypt CSPs in certificate storage. |
| SAML-Priv | SAML private key. RSA (n=2048, n=3072) or ECDSA (P-256, P-384) private key used to digitally sign AAA SAML requests. |
| SNMP-MS | SNMP (RFC 3414/3826) Master Secret. Secret used to derive (SP 800-135 SNMP KDF) SNMP-SMAC and SNMP-SENC. |
| SNMP-SENC | SNMP (RFC 3414/3826) session encryption key. AES-128 key used to encrypt/decrypt SNMP messages. |
| SNMP-SMAC | SNMP (RFC 3414/3826) session authentication key. HMAC-SHA-1-96 160-bit key used to verify SNMP message authenticity. |
| SSH-Priv | SSH private key. RSA (n=3072) or ECC (P-256, P-384) private key used to establish SSH sessions. |
| SSH-SENC | SSH Session Encryption Key. AES-128 or AES-256 key for SSH message encrypt/decrypt. |
| SSH-SMAC | SSH Sesssion Authentication Key. HMAC-SHA 160-bit session key for SSH message authentication. |
| TLS-AMC-Priv | AMC TLS private key. RSA (n=2048, n=3072) or ECC (P-256, P-384) private key used to establish AMC TLS sessions. |
| TLS-SENC | TLS Session Encryption Keys. AES-128, AES-256 or 3-Key Triple-DES key for TLS message encrypt/decrypt. |
| TLS-SMAC | TLS Session Authentication Keys. HMAC-SHA-1 160-bit / HMAC-SHA-256 256-bit session key for TLS message authentication. |
| TLS-WP-Priv | WorkPlace TLS private keys. RSA (n=2048, n=3072) or ECC (P-256, P-384) private key used to establish AMC TLS sessions. |

***Table 11 – Critical Security Parameters (CSPs)***

## 2.2 Public Keys

| | |
|---|---|
| AAA-TLS-Pub | AAA Server public keys. RSA (n=2048, n=3072) or ECC (P-256, P-384) public key used by the policy service to establish VPN TLS sessions with LDAP AAA servers; and for verifying digital signatures from SAML and OCSP AAA servers . |
| CA-Pub | Trusted CA public keys. RSA (n=2048, n=3072) or ECC (P-256, P-384) public key used for VPN client devices path validation. |
| DWS-TLS-Pub | Destination Web Server public key. RSA (n=2048, n=3072) or ECC (P-256, P-384) public key used by the module's VPN web proxy service to establish VPN TLS sessions with HTTPS web server resources. |
| LV-Pub | License Verification public key. RSA (n=2048) public key used to verify product licenses. |
| SSH-Pub | SSH public key. RSA (n=3072) or ECDSA (P-256, P-384) public key used for SSH session establishment. |
| TLS-AMC-Pub | AMC TLS public key. RSA (n=2048, n=3072) or ECC (P-256, P-384) public key used for AMC TLS session establishment. |
| TLS-WP-Pub | Workplace site TLS public key. RSA (n=2048, n=3072) or ECC (P-256, P-384) public key used for VPN TLS session establishment. |

***Table 12 – Public Keys***

# 3 Roles, Authentication and Services

## 3.1 Assumption of Roles

The module supports the operator roles and associated authentication methods listed in Table 13.

The Module does not support a maintenance role or bypass capability. The Module supports concurrent users, enforcing separation of roles by the partitioning of major subsystems (such as VPN traffic vs. shell or AMC administrative functions), and by partitioning of the administrative interfaces (e.g.,. by organization of the AMC web GUI pages). Authentication status does not persist across module power cycles. The module does not permit multiple concurrent operators in the same role: to change roles, an operator must first log out, then log in using another role. Table 13 lists the available roles.

| Role | | Authentication | |
|---|---|---|---|
| **ID** | **Description** | **Type** | **Data** |
| CO | Cryptographic Officer – Has full access to administer and configure the module as well as delegate admin access control rights to Admin users. | Identity-based (using *Local password verification*) or role-based (using *Transitive trust with authentication*) dependent on configured policy. | Username and PIN or X.509 certificate |
| User | Admin User – Configure and administer the module per the delegated access rights assigned by the CO. | | |
| VPN | Typical end user accessing the virtual private network resources via an encrypted connection. | | |
| SNMP | SNMP agent and trap – provides module status via SNMP messages | Identity-based (using *SNMP authentication*) | SNMP-SMAC |

***Table 13 – Roles Description***

## 3.2 Authentication Methods

The *Local password verification* method requires an 8 character minimum password using characters in the printable character set. The maximum rate for local password authentication is conservatively estimated to be approximately one (1) attempt per microsecond.

Hence the probability of false authentication is: 1/(8^96) = **2.0E-87**

And the probability of false authentication in a one minute period is (60*10^6)/(8^96) = **1.2E-79**

The *Transitive trust with authentication* method first establishes a secure connection to an external authentication server, which authenticates to the module using X.509 certificates. Subsequent interaction with the authentication server determines the applicable access rights; as such, this method is a role-based authentication method.

Based on the minimum strength SAML key (RSA 2048) security strength of 112 bits, the probability of false authentication is: 1/(2^112) = **1.9E-34**

And the probability of false authentication in a one minute period is: (60*10^6)/(2^112) = **1.2E-26**

*SNMP authentication* method: communications established with an SNMP client include verification of a initial message, confirming a 96-bit truncated HMAC-SHA-1 value calculated using the SNMP-SMAC key and a designated message , with maximum processing rate measured on the fastest configuration as requiring at minimum one microsecond:

Hence the probability of false authentication is: 1/(2^96) = **1.3E-29**

And the probability of false authentication in a one minute period is (60*10^6)/(2^96) = **7.6E-22**

## 3.3 Services

All services implemented by the module are listed in the tables below.

| Service | Description | CO | SNMP | User | VPN |
|---|---|---|---|---|---|
| Shell Interface | Shell interface via the console serial port using SSH to perform limited module configuration and administration. Uses the following cryptographic security functionality (unless otherwise noted, using Libcrypto certs marked "[L]" in Table 6):<br>- SSH handshake (see Table 6 "Key Exchange", "Host Key Authentication")<br>- Generate session keys (Cert. #871 SSH KDF; Cert. #1211 DRBG)<br>- Secure channel operation (See Table 6 "Encryption" and "Digest") | X | | | |
| AMC Interface | Use of the Administration Management Console (Web GUI) using TLS (via https). Uses the following cryptographic security functionality (unless otherwise noted, using Libcrypto certs marked "[O]" in Table 6):<br>- TLS handshake (see Table 4 "TLS" and "Key Exchange" Columns)<br>- Generate session keys (Cert. #872 ojdk TLS KDF; Cert. #1211 DRBG)<br>- Secure channel operation (See Table 4 "Cipher" and "Digest") | X | | X | |
| Admin User Access Rights Administration | The creation of new Administrative users, Administrative user access rights and authentication sources through the AMC. | X | | X | |
| Security Administration | Administrator access to pages for VPN end user access control rules, resources, users and groups, web portal services and client end point control. | X | | X | |
| System Configuration | Administrator access to pages for network settings, Licensing, SSL settings, access and network services, authentication servers and realms, and the switching in and out of FIPS mode of operation. | X | | X | |
| System Maintenance ***(includes Zeroization)*** | Administrator permission to shut down or restart the appliance, update or roll back the system software, and import or export configuration data, and ***zeroize all CSPs*** . | X | | X | |
| 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. | X | | X | |
| 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. | X | | X | |
| SNMP | Read access permits external SNMP monitoring system to query on MIBS. Uses the following cryptographic security functionality (unless otherwise noted, using Libcrypto certs marked "[L]" in Table 6):<br>- Generate session keys (Cert. #869 SNMP KDF; Cert. #1211 DRBG)<br>- Secure channel operation (Cert. #4046 AES) | | X | | |
| VPN network traffic | Establish an encrypted connection via the VPN TLS and VPN ESP interfaces. Uses the following cryptographic security functionality (unless otherwise noted, using Libcrypto certs marked "[A]" in Table 6):<br>- TLS handshake (see Table 4 "TLS" and "Key Exchange" Columns)<br>- Generate session keys (Cert. #870 OpenSSL TLS KDF; Cert. #1211 DRBG)<br>- Secure channel operation (See Table 4 "Cipher" and "Digest") | X | | X | X |

***Table 14 – Authenticated Services***

| Unauthenticated Services | |
|---|---|
| **Service** | **Description** |
| Module Reset (Self-test) | Reset the Module by the AMC interface, physical power removal, or shell interface. This service executes the suite of self-tests required by FIPS 140-2. Performed by power-cycling or rebooting the module. |
| Show Status | This service provides the current status of the cryptographic module on the LED and LCD interfaces as well as low level response from the network interfaces. |

***Table 15 – Unauthenticated Services***

Table 16 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP. The read access is typically performed before the module uses the CSP.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP. The write access is typically performed after a CSP is imported into the module, when the module generates a CSP, or when the module overwrites an existing CSP.
- Z = Zeroize: The module zeroizes the CSP.

| Service | CSPs | | | | | | | | | | | | | | | | | | Public keys | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | AUTH-PW | DRBG-EI | DRBG-STATE | ESP-SENC | ESP-SMAC | OS-FWK | OS-KEK | SAML-Priv | SNMP-MS | SNMP-SENC | SNMP-SMAC | SSH-Priv | SSH-SENC | SSH-SMAC | TLS-AMC-Priv | TLS-SENC | TLS-SMAC | TLS-WP-Priv | AAA-TLS-Pub | CA-Pub | DWS-TLS-Pub | LV-Pub | SSH-Pub | TLS-AMC-Pub | TLS-WP-Pub |
| Module Reset (Self-test) | -- | GEZ | GZ | Z | Z | -- | -- | -- | -- | Z | Z | -- | Z | Z | -- | Z | Z | -- | -- | -- | -- | -- | -- | -- | -- |
| Show Status | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Shell Interface | E | -- | EW | -- | -- | -- | -- | -- | -- | -- | -- | E | GEZ | GEZ | -- | -- | -- | -- | -- | -- | -- | -- | R | -- | -- |
| AMC Interface | E | -- | EW | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | E | GEZ | GEZ | -- | -- | -- | -- | -- | -- | R | -- |
| Admin User Access Rights Administration | EW | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Security Administration | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| System Configuration | -- | -- | EW | -- | -- | -- | -- | GR | W | -- | --- | GR | -- | -- | GR | -- | -- | GR | ER | ER | ER | ER | G | GR | GR |
| System Maintenance (includes Zeroization) | Z | -- | -- | -- | -- | EZ | EZ | Z | Z | -- | -- | Z | -- | -- | Z | -- | -- | Z | -- | -- | -- | -- | -- | -- | -- |
| System Monitoring | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| Remote Assistance | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| SNMP | -- | -- | EW | -- | -- | -- | -- | E | E | GEZ | GEZ | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- | -- |
| VPN network traffic | E | -- | EW | GEZ | GEZ | -- | -- | E | -- | -- | -- | -- | -- | -- | -- | GEZ | GEZ | E | E | E | E | -- | -- | -- | R |

***Table 16 – CSP Access Rights within Services***

# 4 Self-tests

Each time the module is powered up it tests that the cryptographic algorithms still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the module.

On power up or reset, the module performs the self -tests described in below. All KATs must be completed successfully prior to any other use of cryptography by the module. The Test LED is lit only during power-self-test. If any power-up self-test fails, the module remains in the *FIPS Error* state, indicated by the Test and Alarm LEDs remaining lit, until it is reset. Self-test status is also shown on the console and captured into system logs.

| Test Target (Cert. #) | Description |
|---|---|
| Firmware Integrity | HMAC-SHA-256 performed over all code in EEPROM. |
| AES (#4046) | Separate KATs for each permutation of: encrypt, decrypt functions; 128, 256 bit keys; CBC, GCM modes. ECB encrypt/decrypt tested with 256 bit key only. |
| AES (#4044) | Separate KATs for each permutation of: encrypt, decrypt functions; 128, 256 bit keys; CBC, ECB and GCM modes. |
| AES (#4045) | Separate KATs for each permutation of: encrypt, decrypt functions; 128, 256 bit keys; CBC, ECB and GCM modes. |
| DRBG (#1211) | AES-256 CTR DRBG test. Performed conditionally (where initial use at power-up is the condition) per SP 800-90 Section 11.3. |
| ECDSA (#907) | Separate signature generation and signature verification KAT's as well as a PCT are performed using a P-256 key. |
| ECDSA (#906) | Separate signature generation and signature verification KAT's as well as a PCT are performed using a P-256 key. |
| HMAC (#2641) | Separate HMAC generation and HMAC verification KATs, using SHA-1 and SHA-256. [5] |
| HMAC (#2640) | Separate HMAC generation and HMAC verification KATs, using SHA-1 and SHA-256. [5] |
| HMAC (#2639) | Separate HMAC generation and HMAC verification KATs, using SHA-1 and SHA-256.[5] |
| RSA (#2077) | Separate KATs of n=2048 bit signature generation and signature verification. |
| RSA (#2076) | Separate KATs of n=2048 bit signature generation and signature verification. |
| SHS (#3335) | Separate KATs of SHA-1, SHA-256, SHA-384[5] |
| SHS (#3334) | Separate KATs of SHA-1, SHA-256, SHA-384[5] |
| SHS (#3333) | Separate KATs of SHA-1, SHA-256, SHA-384[5] |
| Triple-DES (# 2213) | Separate KATs of Encryption, Decryption using 3-key TECB. |
| Triple-DES (# 2212) | Separate KATs of Encryption, Decryption using 3-key TECB. |
| Triple-DES (# 2211) | Separate KATs of Encryption, Decryption using 3-key TECB. |
| CSP Integrity | (Critical function) A CSP integrity test is performed at power-on and at each system configuration invocation and configuration update. |

***Table 17 – Power Up Self-tests***

[5] IG 9.4 requires separate self-tests of each of the SHA-1, SHA-256 and SHA-384 methods. IG 9.4 requires an HMAC KAT for at least one of the implemented underlying SHS methods.

| Test Target | Description |
|---|---|
| CSP Integrity | (Critical function) A CSP integrity test is performed at power-on and at each system configuration invocation and configuration update. |
| DRBG | AS09.42 Continuous RNG Test performed when a random value is requested from the DRBG. |
| ECDSA | ECDSA Pairwise Consistency Test performed on every ECDSA key pair generation. |
| Firmware Load | HMAC-SHA-256 verification performed when firmware is loaded. HMAC-SHA-1 is possible to use only for fallback scenarios. |
| NDRNG | AS09.42 Continuous RNG Test performed when a random value is requested from the NDRNG. |
| RSA | RSA Pairwise Consistency Test performed on every RSA key pair generation. |

***Table 18 – Conditional Self-tests***

# 5 Physical Security Policy

The cryptographic modules each include the following physical security mechanisms:

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

Some module components (e.g., hard drives) are field replaceable. If a replacement component is installed in the field, new tamper seals are sent with the replacement component, along with specific instructions on how to properly prepare the module surface and apply the new seals. Tamper seals may not be ordered separately. The location and placement of tamper seals for each configuration are shown in the figures below. The tamper-evident seals shall be installed for the module to operate in a FIPS mode of operation. EX6000 and EX7000 configurations require three (3) tamper seals placed as shown in Section 5.1. EX9000 requires seven (7) seals placed as shown in Section 5.2. SMA 6200 and SMA 7200 require two (2) seals as shown in Section 5.3.

An operator in the CO role is responsible for the following:

- Directly controlling and monitoring module reconfigurations where the tamper- evident seals are removed and re-installed, to ensure that the security of the module is maintained during component replacement and that the module is returned to a FIPS Approved state.
- Securing and controlling any unused tamper seals.

| Physical Security Mechanism | 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 11.4 for procedure. |

***Table 19 – Physical Security Inspection Guidelines***

## 5.1 SRA EX6000 and SRA EX7000 Tamper Seal Placement

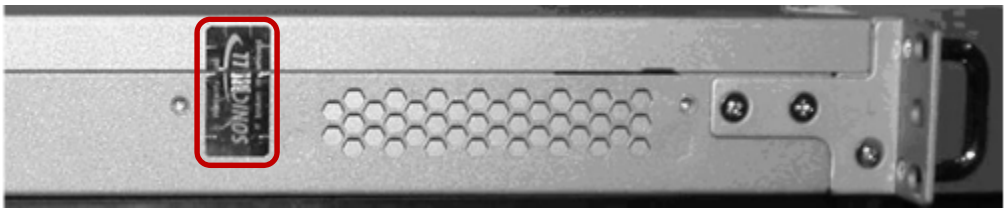

***Figure 2 - Tamper Seal #1 – Left Side***

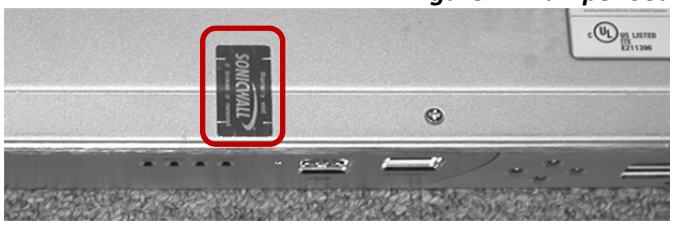

***Figure 3 - Tamper Seal #2 - Bottom Cover***

***Figure 4 – Tamper Seal #3 – Expansion Bay***

## 5.2 SRA EX9000 Tamper Seal Placement

***Figure 5 – SRA EX9000 Tamper Seal #1 - Right Side***

***Figure 6 –SRA EX9000 Underside Tamper Seals #2, #3 and #4***

***Figure 7 – SRA EX9000 Tamper Seal #5 - Rear Fans***

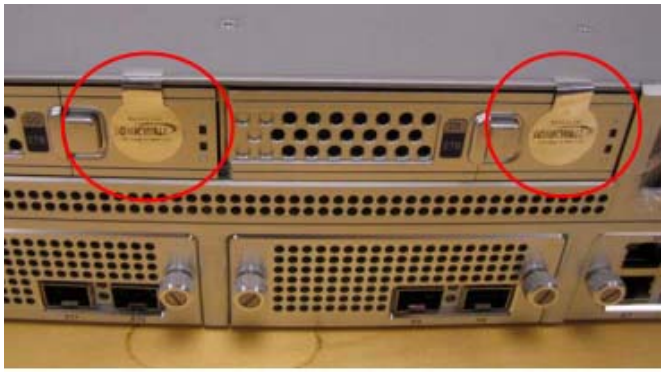

***Figure 8 –SRA CBCCSPs and EX9000 Tamper Seals #6 and #7 - Front Drive Bays***

## 5.3 SMA 6200 and SMA 7200 Tamper Seal Placement

***Figure 9 - SMA 6200 / SMA 7200 Tamper Seal #1 - Chassis Seam***

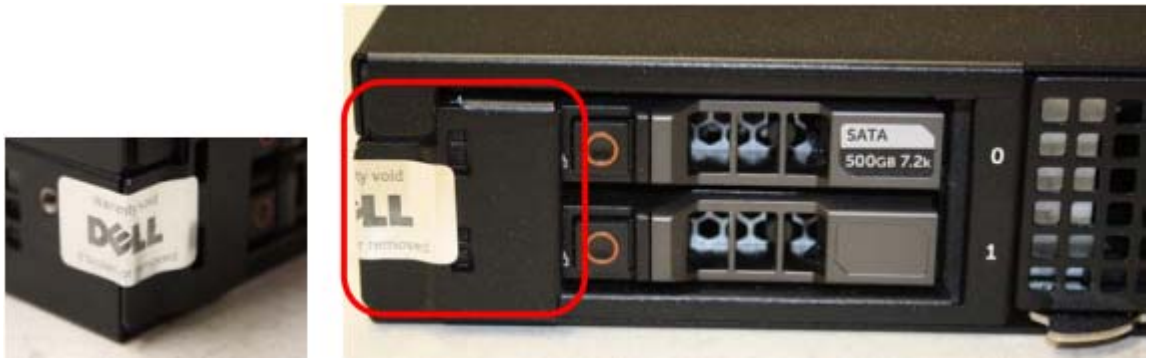


***Figure 10 - SMA 6200 / SMA 7200 Tamper Seal #2 (over drive bay protected plate)***

# 6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions; see the statement in §1 *Introduction* ¶2.

# 7 Mitigation of Other Attacks Policy

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

# 8 Security Rules and Guidance

The Module design corresponds to the module security rules. The module implements and enforces the following security rules:

1. An unauthenticated operator does not have access to any CSPs or cryptographic services.
2. The module inhibits data output during power up self-tests and error states.
3. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
4. 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.
5. 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 (1) hour to complete.
6. The module does not share CSPs between the Approved mode of operation and the non-Approved mode of operation.

The following security rules must be adhered to for operation in the FIPS 140-2 Approved mode:

1. Before enabling the FIPS Approved mode, a strong password, secure connection to the authentication server, and valid license are required.
2. The module must be configured for FIPS Security as detailed in §1.2, with no warnings present.
3. Passwords must be at least 8 characters; 14 characters or more with a mix of numbers , letters and symbols is recommended.
4. Do not use RSA Authentication Manager servers without strong passwords as shared secrets.
5. USB ports may be used for disaster recovery system restoration only.
6. Do not use eSATA devices for any purpose.
7. Do not Load or unload any kernel modules via the shell command line.
8. Do not Install third party software via the shell command line.
9. Do not attempt Firmware upgrades via the shell command line.
10. Do not use Debug 1, Debug 2, Debug 3 or plaintext logs. Plaintext logs do not contain CSPs, but may contain information sensistive to users.
11. Do not use certificates with private/public key-pairs generated by non-FIPS validated systems.
12. Confirm physical security protections in accordance with Section 5, *Physical Security Policy.*
13. In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption is established.

## References and Definitions

| Ref | Full Specification Name |
|---|---|
| [135] | SP 800-135, NIST, Recommendation for Existing Application-Specific Key Derivation Functions, December 2011. |
| [180] | FIPS 180-4, NIST, Secure Hash Standard (SHS), August 2015. |
| [186] | FIPS 186-4, NIST, Digital Signature Standard (DSS), July 2013. |
| [197] | FIPS 197, NIST, Advanced Encryption Standard (AES), November 26, 2001. |
| [198] | FIPS 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008. |
| [2865] | Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service RFC 2865, (RADIUS), RFC 2865, Internet Engineering Task Force, June 2000. |
| [38A] | SP 800-38A, NIST, Recommendation for Block Cipher Modes of Operation - Methods and Techniques, December 2001. |
| [38D] | SP 800-38D, NIST, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007. |
| [4254] | RFC 4254, Ylonen, T. and C. Lonvick, "The Secure Shell (SSH) Connection Protocol", Internet Engineering Task Force, January 2006. |
| [4303] | RFC 4303, Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, Internet Engineering Task Force, December 2005. |
| [4511] | RFC 4511, Semersheim, J., Ed., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, Internet Engineering Task Force, June 2006. |
| [5246] | RFC 5246, Dierks, T., and E. Rescoria, "The Transport Layer Security (TLS) Protocol Version 1.2",. RFC 5246, Internet Engineering Task Force, August 2008. |
| [6239] | RFCTBD, K. Igoe, "Suite B Cryptography in Suites for Secure Shell (SSH)", Internet Engineering Task Force, May 2011. |
| [6379] | RFC 6379, Law, L. and J. Solinas, "Suite B Cryptography Suites for IPsec", RFC 6379, Internet Engineering Task Force, October 2011. |
| [6460] | RFCTBD, Salter, M and R. Housely, "Suite B Profile for Transport Layer Security (TLS)", Internet Engineering Task Force, January 2012. |
| [67] | SP 800-67, NIST, Recommendation for the Triple Data Encryption Algorithm (Triple-DES) Block Cipher, January 2012. |
| [90A] | SP 800-90A, NIST, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015. |

***Table 20 – References***

| Term | Definition |
|---|---|
| AAA | Authentication, Authorization and Accounting - access control, policy enforcement and auditing framework for computing systems, e.g. LDAP |
| AMC | Administration Management Console |
| ESP | Encapsulated Security Payload (a subset of IPsec, Internet Protocol Security) |
| IKE | Internet Key Agreement, a key agreement scheme associated with IPsec (but not used by the module) |
| GMS | Global Management System |
| GUI | Graphical User Interface |
| LDAP | Lightweight Directory Access Protocol |
| PKCS #12 | Public-Key Cryptography Standards #12, regarding certificate formats. |
| RADIUS | Remote Authentication Dial-In Service |
| SAML | Security Assertion Markup Language |
| SNMP | Simple Network Management Protocol |
| SSH | Secure Shell |
| VPN | Virtual Private Network |
| TLS | Transport Layer Security |

***Table 21 – Acronyms and Definitions (for terms not defined in FIPS 140-2 and associated documents)***