SonicWall, Inc.

SonicWALL NSA Series SM 9600, SM 9400, SM 9200, NSA 6600

FIPS 140-2 Non-Proprietary Security Policy

Level 2

Version 1.6
June 7, 2017

Copyright Notice

Table of Contents

Introduction

The SonicWALL NSA Series SM 9600, SM 9400, SM 9200, NSA 6600 (hereafter referred to as "the cryptographic module") is a multiple-chip standalone cryptographic module, with hardware part numbers and versions as follows:

Module	Hardware Version	Firmware Version
SM 9600	P/N 101-500380-71, Rev. A	SonicOS v6.2.5
SM 9400	P/N 101-500361-70, Rev. A	SonicOS v6.2.5
SM 9200	P/N 101-500363-70, Rev. A	SonicOS v6.2.5
NSA 6600	P/N 101-500364-66, Rev. A	SonicOS v6.2.5

Note that the different SM HW versions vary only in form factor, CPU and memory. The overall FIPS validation level for the module is Security Level 2. The cryptographic module is an Internet security appliance, which provides stateful packet filtering firewall, deep packet inspection, virtual private network (VPN), and traffic shaping services. 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.

Table 1 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports Interfaces	2
Roles, Services, and Authentication	2
Finite State Machine	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

Cryptographic Boundary

The cryptographic boundary the surfaces and edges of the device enclosure, inclusive of the physical ports.

The chassis of all the modules are sealed with two (2) tamper-evident seals, which are applied during manufacturing. The physical security of the module is intact if there is no evidence of tampering with the seals. The locations of the tamper-evident seals are indicated by the red arrows in the figures below. The Cryptographic Officer shall inspect the tamper seals for signs of tamper evidence once every six months. If evidence of tamper is found, the Cryptographic Officer is requested to follow their internal IT policies which may include either replacing the unit or resetting the unit to factory defaults. For further instructions on resetting to factory defaults, please review Sonicwall guidance documentation.

Figure 1 - NSA 6600 Front

Figure 2 - NSA 6600 Tamper Seal Location on Underside, Front

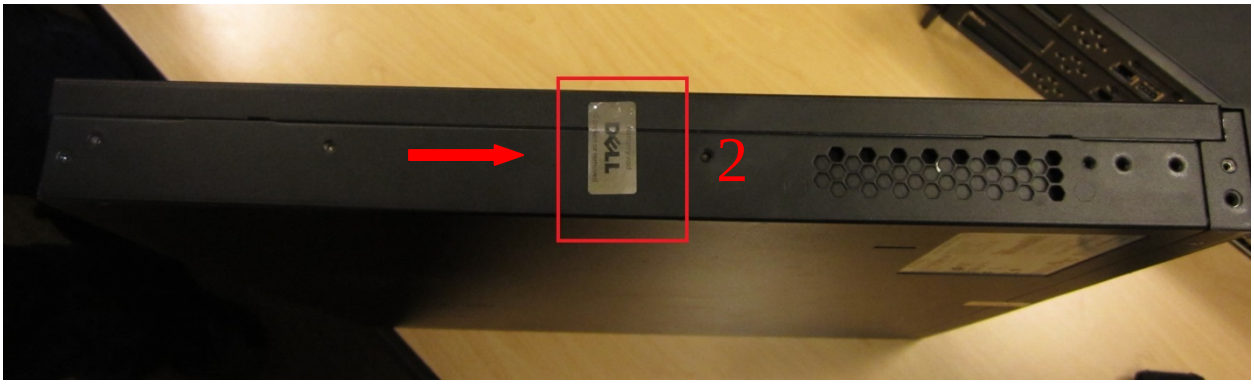

Figure 3 - NSA 6600 Tamper-Evident Seal Location on Left Side

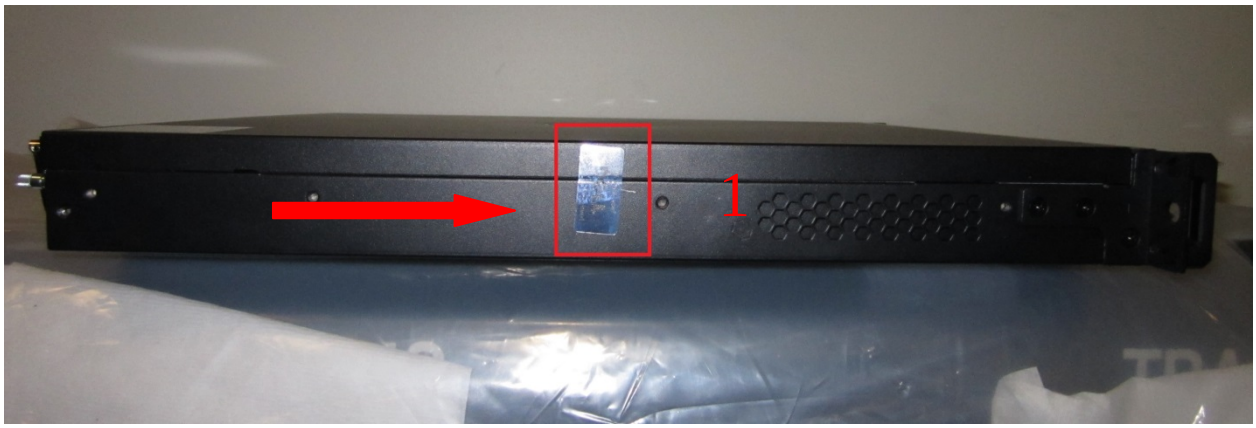

Figure 4 – SM Chassis with Tamper-Evident Seal Location on Left Side

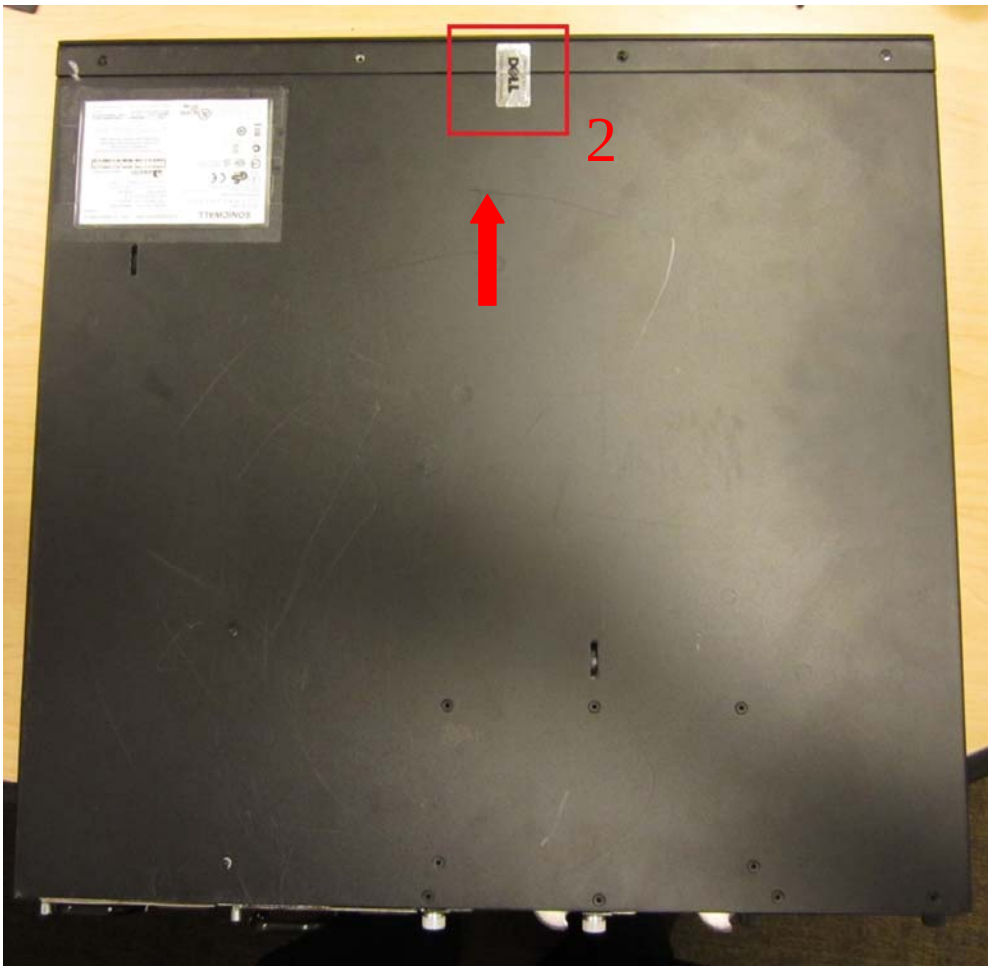

Figure 5 - SM Chassis with Tamper Seal Location on Underside, Front

Roles and Services

The cryptographic module provides a User role and a Cryptographic Officer role via role-based authentication. The cryptographic module does not provide a Maintenance role. The User role is referred to as "Limited Administrator" (individual user) or "Limited Administrators" (user group) in the vendor documentation. The Cryptographic Officer role is referred to as "Administrator" (individual user) or "SonicWALL Administrators" (user group) in the vendor documentation. The "Administrator" user is a local account on the SonicWALL appliance, and the name used to login as this account may be configured by the Cryptographic Officer role; the default name for the "Administrator" account is "admin". The user group, "SonicWALL Read-Only Admins," satisfies neither the Cryptographic Officer nor the User Role, and should not be used in FIPS mode operations.

The configuration settings required to enable FIPS mode are specified on page 15 of this document.

The User role is authenticated using the credentials of a member of the "Limited Administrators" user group. The User role can query status and non-critical configuration. The authentication mechanisms are discussed in the Security Rules Section.

User Role Services

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

The Cryptographic Officer role is authenticated using the credentials of the "Administrator" user account (also referred to as "Admin"), or the credentials of a member of the "SonicWALL Administrators" user group. The use of the latter allows for identification of specific users (i.e., by username) upon whom is imparted full administrative privileges through their assigned membership to the "SonicWALL Administrators" group by the Admin user, or other user with full administrative privileges. The Cryptographic Officer role can show all status and configure cryptographic algorithms, cryptographic keys, certificates, and servers used for VPN tunnels. The Crypto Officer sets the rules by which the module encrypts and decrypts data passed through the VPN tunnels. The authentication mechanisms are discussed in the Security Rules Section.

Crypto Officer Services

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

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

Unauthenticated services

- Self-test Initiation – power cycle
- Firmware removal with configuration return to factory state – reset switch.
- Status – LED activity and console message display

Note: The same services are available in the non-Approved mode of operation. In the non-Approved mode of operation, the non-Approved algorithms listed on page 16 can be utilized.

Separation of roles is enforced by requiring users to authenticate using either a username and password, or digital signature verification. The User role requires the use of a username and password or possession of a private key of a user entity belonging to the “Limited Administrators” group. The Cryptographic Officer role requires the use of the “Administrator” username and password, or the username and password of a user entity belonging to the “SonicWALL Administrators” group.

Multiple users may be logged in simultaneously, but only a single user-session can have full configuration privileges at any time, based upon the prioritized preemption model described below:

1. The Admin user has the highest priority and can preempt any users.
2. A user that is a member of the “SonicWALL Administrators” user group can preempt any users except for the Admin.
3. A user that is a member of the “Limited Administrators” user group can only preempt other members of the “Limited Administrators" group.

Session preemption may be handled in one of two ways, configurable from the System > Administration page, under the “On admin preemption” setting:

1. “Drop to non-config mode” – the preempting user will have three choices:
    a. “Continue” – this action will drop the existing administrative session to a “non-config mode”, and will impart full administrative privileges to the preempting user.
    b. “Non-Config Mode” – this action will keep the existing administrative session intact, and will login the preempting user in a “non-config mode”
    c. “Cancel” – this action will cancel the login, and will keep the existing administrative session intact.
2. “Log-out” – the preempting user will have two choices:
    a. “Continue” – this action will log out the existing administrative session, and will impart full administrative privileges to the preempting user.
    b. “Cancel” – this action will cancel the login, and will keep the existing administrative session intact.

“Non-config mode” administrative sessions will have no privileges to cryptographic functions making them functionally equivalent to User role sessions. The ability to enter “Non-config mode” may be disabled altogether from the System > Administration page, under the “On admin preemption” setting by selecting “Log out” as the desired action.

The cryptographic module provides several security services including VPN and IPsec. The cryptographic module provides the Cryptographic Officer role the ability to configure VPN tunnels and network settings.

When configured to operate in FIPS mode, the cryptographic module provides only FIPS 140-2 compliant services. Whether or not the device is in FIPS mode is indicated on the System/Settings page; checking the FIPS mode enable check box causes the module to execute a compliance check; the module sets the flag only when all conditions are met, and automatically resets the module to enter the FIPS 140-2 Approved mode.

The module supports the following FIPS-approved cryptographic algorithms:

Table 2 – FIPS 140-2 Approved Cryptographic Algorithms

Description	Cert. #
AES (128, 192, and 256-bit) in CBC mode	3901
SHA-1, SHA-256, -384, -512	3214
FIPS 186-4 RSA Key Generation, Signature Generation and Signature Verification using 2048 and 3072-bit key sizes with SHA-256, -384, and -512	1986
FIPS 186-4 DSA Signature Verification using 2048-bit key size with SHA-256, -384 and -512.	1061
HMAC-SHA-1, -256, -384, -512	2531
SP 800-90A Hash_DRBG (SHA-256)	1117
SP 800-135 KDF's for IKE v1, IKE v2, TLS *	756

* The corresponding protocols were not reviewed or tested by the CAVP or CMVP.

The CAVP certificates associated with this module include other algorithms, modes, and key sizes that have been CAVP validated but are not available in the Approved mode of the module. Only the algorithms, modes, and key sizes shown in Table 2 are available in the Approved mode of the module.

The Cryptographic Module also provides the following non FIPS-approved but allowed algorithms:

- Diffie-Hellman within IKE using 2048-bit keys (key agreement; key establishment methodology provides 112 bits of encryption strength)
- NDRNG (used only to seed the Approved DRBG). The NDRNG provides an effective 768 bits of entropy input to the SP 800-90A Hash_DRBG for use in key generation.
- MD5 within TLS and internal password storage

Ports and Interfaces

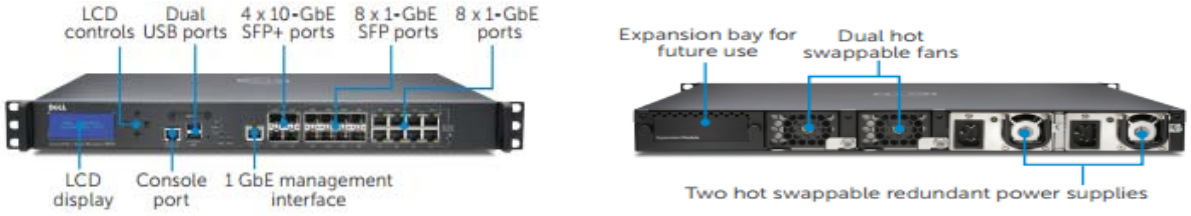

Figure 6 – SM Series Front Panel (Top) and Rear Panel (Bottom)

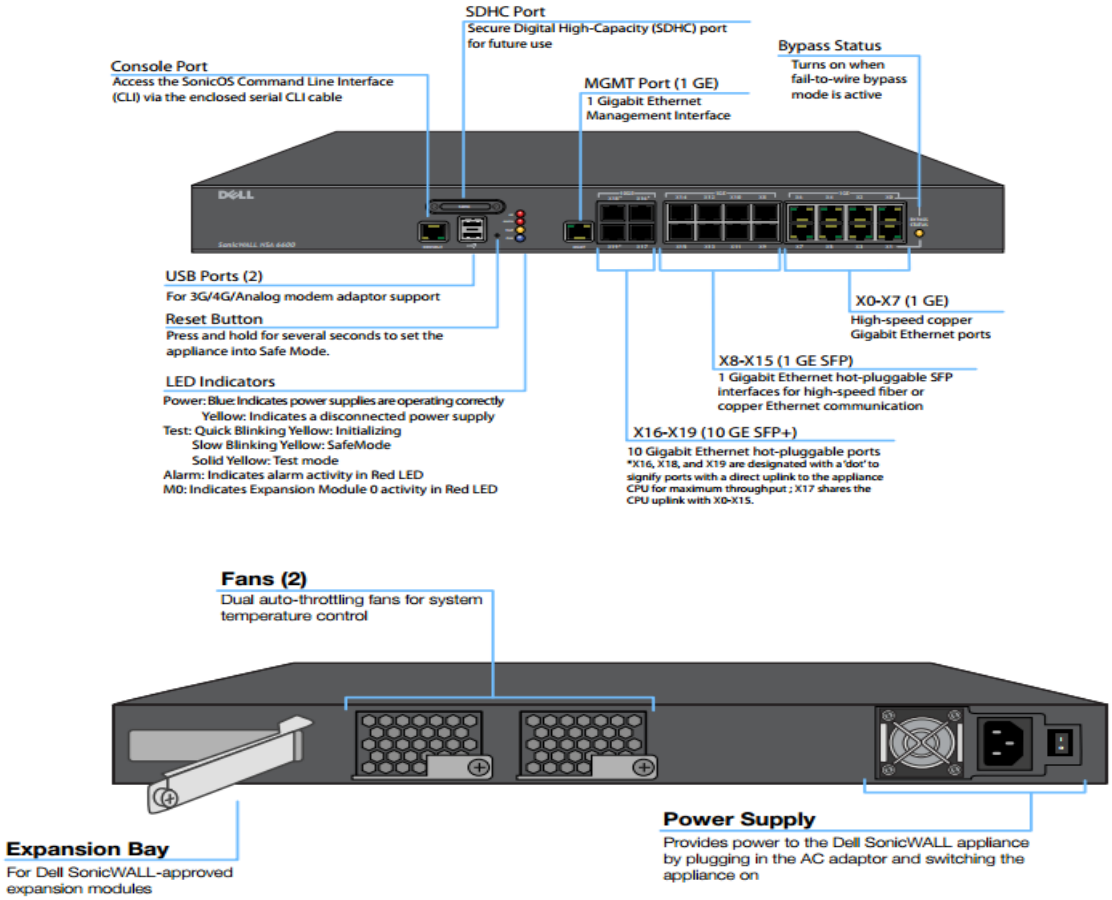

Figure 7 – NSA 6600 Front Panel (Top) and Rear Panel (Bottom)

Table 3 describes the physical ports and corresponding logical interfaces.

Table 3 – Ports and Interfaces

Physical Ports	Qty.	Description	Logical Interfaces
LCD display	1	LCD status display	Status output
LCD controls	4	Controls for scrolling thru the LCD display options	Control input, status output
Console	1	DB-9/RJ-45 serial connector. Provides a serial console which can be used for basic administration functions.	Data input, control input, status output
USB	2	*Non-functional, not currently supported*	N/A
Reset Button	1	Used to manually reset the appliance to Safe Mode.	Control input
Status LEDs	6	Power LEDs: Indicate module is receiving power. Test LED: Indicates module is initializing and performing self-tests. Alarm LED: Indicates alarm condition. HD and Bypass Status LEDs:	Status output
Expansion	1	*Expansion connector, unused, disconnected internally.*	N/A
SDHC [NSA]	1	*Secure Digital High-Capacity port. Non-functional, not currently supported.*	N/A
MGMT	1	1Gbps RJ45 isolated out-of-band management (MGMT) port, with integral LINK and ACT LEDs	Control input, Status output
Ethernet	8	10/100/1000 auto-sensing with an RJ-45/SX/SC multimode fiber connector. Labeled X#..., LAN/WAN/…. Each Ethernet interface includes LINK and ACT LEDs.	Data input, data output, status output, control input
1GE SFP	8	1GE Ethernet hot-pluggable SFP interfaces supporting RJ-45/SX/SC multimode fiber connector with LINK and ACT LEDs.	Data input, data output, status output, control input
10GE SFP	4	10GbE Ethernet hot-pluggable SFP+ interfaces with LINK and ACT LEDs	Data input, data output, status output, control input
Power [SM]	2	AC power inputs	Power
Power [NSA]	1	AC power input and switch	Power

Security Rules

The cryptographic module has the following security rules:

- The cryptographic module provides two distinct operator roles: User role and Cryptographic Officer role.
- The cryptographic module provides authentication relying upon username/passwords or an RSA 2048-bit digital signature verification.
    - The CO and User passwords must be at least eight (8) characters long each, and the password character set is ASCII characters 32-127, which is 96 ASCII characters. 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 (This is also valid for RADIUS shared secret keys). After three (3) successive unsuccessful password verification tries, the cryptographic module pauses for one second before additional password entry attempts can be reinitiated. This makes the probability approximately 180/96^8 = 1.5E-14, which is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur in a one-minute period.
    - For User authentication based on RSA digital signature verification, 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, which is less than 1 in 100,000.
- The following cryptographic algorithm self-tests are performed by the cryptographic module at power-up:
    - Firmware integrity test (using 16-bit CRC EDC)
    - AES-CBC Encrypt and Decrypt Known Answer Tests
    - SHA-1, -256, -384, -512 Known Answer Tests
    - HMAC-SHA-1, -256, -512 Known Answer Tests
    - DSA Signature Verification Pairwise Consistency Test
    - RSA Sign and Verify Known Answer Tests
    - DH Pairwise Consistency Test
    - DRBG KAT

    The module supports the following conditional self-tests:
    - DRBG and NDRNG Continuous Random Number Generator Tests
    - RSA Pairwise Consistency Test
    - Firmware Load Test

- When a new firmware image is loaded, the cryptographic module verifies the 2048-bit DSA signed SHA-2 hash of the image. If this verification fails, the firmware image loading is aborted.

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

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

Operational Environment

Area 6 of the FIPS 140-2 requirements does not apply to this module as the module only allows the loading of firmware through the firmware load test, which ensures the image is appropriately DSA signed by SonicWall, Inc.

FIPS 140-2 Approved mode of Operation

The module is not configured to operate in FIPS-mode by default. The following steps must be taken to enable FIPS-mode operation.

- Set Administrator and User passwords, as well as the RADIUS shared secret, to at least eight (8) characters.
- Traffic between the module and the RADIUS server must be secured via an IPsec tunnel. Note: this step need only be performed if RADIUS is supported.
- Use IKE with 3rd Party Certificates for IPsec Keying Mode when creating VPN tunnels.
- When creating VPN tunnels, ensure ESP is enabled for IPsec.
- Use FIPS-approved encryption and authentication algorithms when creating VPN tunnels.
- Use Group 2 or Group 5 for IKE Phase 1 DH Group and Use SHA-256 for Authentication
- Do not enable Advanced Routing Services.
- Do not enable Group VPN management.
- Do not enable SNMP or SSH.
- Enable FIPS mode from the System/Settings page by checking “FIPS Mode” checkbox.

The FIPS mode configuration can be determined by an operator, by checking the state of the “FIPS Mode” checkbox on the System/Settings page and verification of the preceding steps. When the “FIPS Mode” checkbox is selected, the module executes a compliance checking procedure, examining all settings related to the security rules described above and in this Security Policy, and reporting any non-compliant settings. The operator, prompted by the compliance tool, is responsible for updating these settings appropriately. The “FIPS Mode” checkbox and corresponding system flag will not be set unless all settings are compliant, and as such is a reliable indicator that the module is running in the FIPS Approved mode of operation.

Non-Approved mode of Operation

The Cryptographic Module provides the same set of services as listed above, but allows the following additional administration options and non FIPS-approved algorithms not used in the FIPS mode of operation:

- MD5 within MSCHAP
- ARCFOUR and ARCFOUR128 within L2TP, TLS and SSH
- AES GCM (non-compliant) within SSL
- DES within SSL, SSH and SNMP
- Triple-DES (non-compliant) within SSL and SSH
- FIPS 186-2 RSA Signature Generation using 1024, 1536, and 2048-bit key sizes with SHA-1
- Diffie-Hellman within IKE using 1024-bit keys (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant)
- http management GUI
- AAA server authentication (the Approved mode requires operation of RADIUS only, within a secure VPN tunnel)
- SSH[*]
- SNMP[*]

Definition of Critical Security Parameters

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

- IKE Shared Secret – Shared secret used during IKE Phase 1
- SKEYID – Secret value used to derive other IKE secrets
- SKEYID_d – Secret value used to derive keys for security associations
- SKEYID_a – Secret value used to derive keys to authenticate IKE messages
- SKEYID_e – Secret value used to derive keys to encrypt IKE messages
- IKE Session Encryption Key – AES 128, 192, 256 key used to encrypt data
- IKE Session Authentication Key - HMAC 160 bit key used for data authentication
- IKE RSA Private Key – RSA 2048 bit RSA key used to authenticate the module to a peer during IKE
- IPsec Session Encryption Key – AES 128, 192, 256 key used to encrypt data
- IPsec Session Authentication Key – HMAC 160 bit key used for data authentication for IPsec traffic
- TLS Master Secret: used for the generation of TLS Session Keys and TLS Integrity Key
- TLS Premaster Secret: used for the generation of Master Secret
- TLS Session Key: AES key used to protect TLS connection
- TLS Integrity Key: HMAC 160 bit key used to check the integrity of TLS connection
- Diffie-Hellman Private Key – Used within IKE key agreement
- DRBG V and C values – Used to seed the Approved DRBG

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

- RADIUS Shared Secret – Used for authenticating the RADIUS server to the module and vice versa
- Passwords – Authentication data

Public Keys

- Root CA Public Key – Used for verifying a chain of trust for receiving certificates
- Peer IKE RSA Public Key – RSA 2048 bit key for verifying digital signatures from a peer device
- IKE RSA Public Key – RSA 2048 bit key for verifying digital signatures created by the module
- DSA Firmware Verification Key – 2048 bit DSA key used for verifying firmware during firmware load
- Diffie-Hellman Public Key – Used within IKE key agreement
- Diffie-Hellman Peer Public Key – Used within IKE key agreement
- Authentication Public Key – RSA public key used to authenticate the User
- TLS Public Key – RSA public key used in the TLS handshake

Definition of CSP Modes of Access

Table 4 describes the methods of accessing the individual CSPs.

Import: The CSP is entered into the module from an external source.

Generate: The CSP is internally generated using the Hash_DRBG and approved asymmetric key generation methods, as applicable.

Execute: The module uses the CSP.

Removal/Deletion: The CSP is actively destroyed.

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

Table 4 - Roles, Services, CSP Access Matrix

Service	Cryptographic Keys and CSPs Access Operation
Show Status	N/A
Show Non-critical Configuration	N/A
Monitor Network Status	N/A
Log On	Execute - Passwords
Log Off	N/A
Clear Log	N/A
Export Log	N/A
Import/Export Certificates	N/A
Filter Log	N/A
Setup DHCP Server	N/A (Note: DHCP setup does not use CSPs, but DHCP server setup is performed with IPsec active. See below for IPsec VPN CSP usage.)

Service	Cryptographic Keys and CSPs Access Operation
Generate Log Reports	N/A
Configure VPN Settings	Import - Root CA Public Key Import/Generate - IKE RSA Private and Public Keys Import/Generate - Diffie-Hellman Private and Public Keys
IPsec VPN	Generate/Execute – IKE Shared Secret Generate/Execute – SKEYID Generate/Execute – SKEYID_d Generate/Execute – SKEYID_a Generate/Execute – SKEYID_e Generate/Execute – IKE RSA Private Key Generate/Execute – DH Private Key Generate/Execute – IKE Session Authentication Key Generate/Execute – IPsec Session Authentication Key Generate/Execute – IKE Session Encryption Key Generate/Execute – IPsec Session Encryption Key Generate/Execute – DRBG V and C values Generate/Execute – RADIUS Shared Secret Execute – Root CA Public Key Import/Execute – Peer IKE RSA Public Key Execute – IKE RSA Public Key Execute – Diffie-Hellman Public Key Import/Execute – Diffie-Hellman Peer Public Key Import/Execute – Authentication Public Key
TLS	Generate/Execute - TLS Master Secret Generate/Execute - TLS Premaster Secret Generate/Execute - TLS Session Key Generate/Execute - TLS Integrity Key Execute - TLS Public Key Execute - Diffie-Hellman Public Key Import/Execute - Diffie-Hellman Peer Public Key Import/Execute - Authentication Public Key
Set Content Filter	N/A
Upload Firmware	Execute - DSA Firmware Verification Key
Configure DNS Settings	N/A
Configure Access	Import/Execute - Passwords
Key Zeroization	Remove – IKE Shared Secret Remove – SKEYID Remove – SKEYID_d Remove – SKEYID_a Remove – SKEYID_e Remove – IKE Session Encryption Key

Service	Cryptographic Keys and CSPs Access Operation
	Remove – IKE Session Authentication Key Remove – IKE RSA Private Key Remove – IPsec Session Encryption Key Remove – IPsec Session Authentication Key Remove – TLS Master Secret Remove – TLS Premaster Secret Remove – TLS Session Key Remove – TLS Integrity Key Remove – DH Private Key Remove – DRBG V and C values Remove – RADIUS Shared Secret Remove – Passwords

Mitigation of Attacks

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.

Definitions and Glossary

AES	Advanced Encryption Standard
FIPS	Federal Information Processing Standard
CSP	Critical Security Parameter
VPN	Virtual Private Network
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
Triple-DES	Triple Data Encryption Standard
DES	Data Encryption Standard
CBC	Cipher Block Chaining
DSA	Digital Signature Algorithm
DRBG	Deterministic Random Bit Generator
RSA	Rivest, Shamir, Adleman asymmetric algorithm
IKE	Internet Key Exchange
RADIUS	Remote Authentication Dial-In User Service
IPSec	Internet Protocol Security
LAN	Local Area Network
DH	Diffie-Hellman
GUI	Graphical User Interface
SHA	Secure Hash Algorithm
HMAC	Hashed Message Authentication Code
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
NSA	Network Security Appliance (SonicWALL product name)
SFP	Small Form-factor Pluggable (a high speed LAN connection type)
SM	Super Massive (SonicWALL product name)