Dell SonicWALL

NSA 3500 FIPS 140-2 Non-Proprietary Security Policy

Level 2

Version 2.1
April 28, 2014

Copyright Notice

Table of Contents

Introduction

The SonicWALL NSA Series 3500 (hereafter referred to as "the cryptographic module") is a multiple-chip standalone cryptographic module, HW P/N 101-500248-63, Rev. B; FW Version SonicOS v5.9.0. 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

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 11 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. Monitor Network Status
    2. Log Off (themselves and guest users)
    3. Clear Log
    4. Export Log

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 Encryption
    3. Set Content Filter
    4. Import/Export Certificates
    5. Upload Firmware
    6. Configure DNS Settings
    7. (Related to wireless activity) Configure Access Rules
- 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. Import/Export Certificates
    2. Clear Log
    3. Filter Log
    4. Export Log
    5. Setup DHCP Server
    6. Generate Log Reports
- Key Zeroization – Zeroizing cryptographic keys

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 – reset switch
- Status – console and LED

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 8 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.

The module supports the following FIPS-approved cryptographic algorithms:

- AES (128, 192, and 256-bit) in CBC mode (Cert. #2015)
- Triple-DES in CBC mode; 2-key[1] and 3-key (Cert. #1300)
- SHA-1, -256, -384, -512 (Cert. #1765)
- FIPS 186-2 DSA Signature Verification using 1024-bit key size with SHA-1 (Cert. #640)
- FIPS 186-2 RSA Signature Verification using 1024, 1536, and 2048-bit key sizes with SHA-1 (Cert. #1044)
- FIPS 186-2 RNG (Cert. #1156)
- HMAC-SHA-1, -256, -384, -512 (Cert. #1219)
- Hashed based DRBG (Cert. #189
- SP 800-135 KDF's for IKEv1, IKEv2, TLS, SSH, SNMP (CVL Cert. #86) - the corresponding protocols have not been reviewed or tested by the CAVP and CMVP

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 to seed the DRBG and RNG)

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

- MD5 within MSCHAP
- RC4 within L2TP (not used in the FIPS mode of operation)

The module supports the following algorithms which are Disallowed as of January 1, 2014 per the NIST SP 800-131A algorithm transitions:

- FIPS 186-2 RSA Signature Generation using 1024, 1536, and 2048-bit key sizes with SHA-1 (Cert. #1044)
- Diffie-Hellman within IKE using 1024-bit keys (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant)

Algorithms providing less than 112 bits of security strength (Disallowed per NIST SP 800-131A) are not allowed in the FIPS Approved mode of operation for use by Federal agencies.

[1] Per NIST SP 800-131A: Through December 31, 2015, the use of 2-key Triple DES for encryption is restricted: the total number of blocks of data encrypted with the same cryptographic key shall not be greater than 2^{20}. After December 31, 2015, 2-key Triple DES shall not be used for encryption. Decryption using 2-key Triple DES is allowed for legacy-use.

Ports and Interfaces

Figure 1 shows the locations of the physical ports on the front of the module.

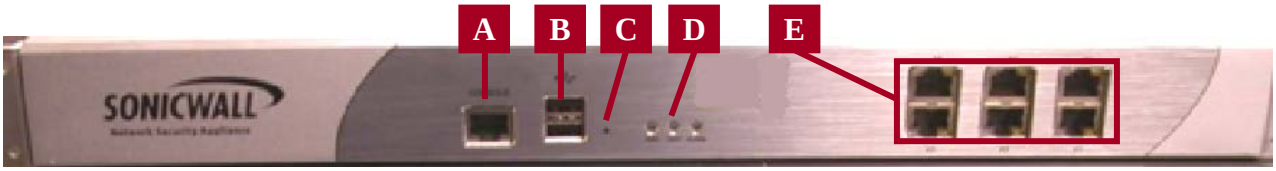

Figure 1 – NSA 3500 Front Panel

Table 2 describes the physical ports (mapped to Figure 1) and corresponding logical interfaces.

Table 2 – Front Panel Ports and Interfaces

Physical Ports	Qty.	Description	Logical Interfaces
Serial Console Interface [A]	1	DB-9/RJ-45 serial connector. Provides a serial console which can be used for basic administration functions.	Data input, control input and status output
USB Interfaces [B]	2	*Not currently supported*	N/A
Reset (Safe Mode) Button Interface [C]	1	Used to manually reset the appliance to Safe Mode.	Control input
Status LED Interface [D]	3	Power LED: Indicates module is receiving power. Test LED: Indicates module is initializing and performing self-tests. Alarm LED: Indicates alarm condition.	Status output
Ethernet Interfaces [E]	6	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, and control input (via the external GUI Administration interface)

Figure 2 shows the locations of the physical ports on the back of the module.

Figure 2 – NSA 3500 Back Panel

Table 3 describes the physical ports (mapped to Figure 2) and corresponding logical interfaces.

Table 3 – Back Panel Ports and Interfaces

Physical Ports	Qty.	Description	Logical Interfaces
Fan Interface [A]	2	Dual removable fan components	N/A
Power Interface [B]	1	AC power interface	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 role-based authentication relying upon username/passwords or an RSA 2048-bit digital signature verification.
    - The CO 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 (this is also valid for RADIUS shared secret keys). 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.
    - 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)

— Triple-DES-CBC Encrypt and Decrypt Known Answer Tests
— AES-CBC Encrypt and Decrypt Known Answer Tests
— SHA-1,-256, -384, -512 Known Answer Tests
— HMAC-SHA-1, -256 Known Answer Tests
— DSA Signature Verification Pairwise Consistency Test
— RSA Sign and Verify Known Answer Tests
— DH Pairwise Consistency Test
— DRBG KAT
— FIPS 186-2 RNG KAT

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

- When a new firmware image is loaded, the cryptographic module verifies the 1024-bit DSA signed SHA-1 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.

FIPS-mode 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 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-1 or SHA-256 for Authentication
- Do not enable Advanced Routing Services.
- Do not enable Group VPN management
- 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. If the “FIPS Mode” checkbox is checked, the module is running in the FIPS Approved mode of operation.

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, or Triple-DES key used to encrypt data
- IKE Session Authentication Key - HMAC key used for data authentication
- IKE RSA Private Key – RSA 1024, 1536 or 2048 bit RSA key used to authenticate the module to a peer during IKE
- IPsec Shared Secret – Used to derive IPsec encryption and authentication keys
- IPsec Session Encryption Key – AES 128, 192, 256, or Triple-DES key used to encrypt data
- IPsec Session Authentication Key – HMAC key used for data authentication for IPsec traffic
- TLS Master Secret: used for the generation of TLS Session Key and TLS MAC Secret
- TLS Premaster Secret: used for the generation of Master Secret
- TLS Session Key: AES or Triple-DES key used to protect TLS connection
- TLS Integrity Key: HMAC key used to check the integrity of TLS connection
- SSH Session Key: AES or Triple-DES key used to protect SSH sessions
- SSH Authentication Key: HMAC key used for data authentication for SSH sessions
- DH Private Key – Used within IKE key agreement
- DRBG V and C values – Used to seed the Approved DRBG
- RNG Seed Key – Used to seed the Approved RNG
- RADIUS Shared Secret Keys – 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 1024, 1536 or 2048 bit key for verifying digital signatures from a peer device
- IKE RSA Public Key – RSA 1024, 1536 or 2048 bit key for verifying digital signatures created by the module
- DSA Firmware Verification Key – 1024 bit DSA key used for verifying firmware during firmware load
- DH Public Key – Used within IKE key agreement
- DH Peer Public Key – Used within IKE key agreement
- Authentication Public Key – Used to authenticate the User
- TLS Public Key – Facilitates TLS sessions
- SSH Public Key – Facilitates SSH sessions

Definition of CSP Modes of Access

Table 4 describes the methods of accessing the individual CSPs.

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

Generate/Execute: The CSP is internally generated using the Hash based DRBG and the module uses the CSP.

Removal/Deletion: The CSP is actively destroyed.

Table 4 – Roles, Services, CSP Access Matrix

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	**User**		
X	X	Show Status	N/A
	X	Show Non-critical Configuration	N/A
	X	Monitor Network Status	N/A
	X	Log Off	N/A
X	X	Clear Log	N/A
X	X	Export Log	N/A
X		Import/Export Certificates	N/A
X		Filter Log	N/A
X		Setup DHCP Server	Generate/Execute – DRBG V and C values Generate/Execute – RNG Seed Key Generate/Execute – DH Private Key Generate/Execute – SKEYID Generate/Execute – SKEYID_d Generate/Execute – SKEYID_a Generate/Execute – SKEYID_e Generate/Execute – IKE RSA Private Key
X		Generate Log Reports	N/A
X		Configure VPN Settings	Generate/Execute – DRBG V and C values Generate/Execute – RNG Seed Key Generate/Execute – DH Private Key Generate/Execute – SKEYID

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	**User**		
			Generate/Execute – SKEYID_d Generate/Execute – SKEYID_a Generate/Execute – SKEYID_e Generate/Execute – IKE RSA Private Key Generate/Execute – IKE Shared Secret Generate/Execute – IKE Session Authentication Key Generate/Execute – IPsec Shared Secret Generate/Execute – IPsec Session Authentication Key Generate/Execute – RADIUS Shared Secret Keys
X		Set Encryption	Generate/Execute – IKE Session Encryption Key Generate/Execute – IPsec Session Encryption Key
X		Set Content Filter	N/A
X		Upload Firmware	N/A
X		Configure DNS Settings	N/A
X		Configure Access Rules	N/A
X		Key Zeroization	Remove – DRBG V and C values Remove – RNG Seed Key Remove – Passwords Remove – IKE Shared Secret Remove – SKEYID Remove – SKEYID_d Remove – SKEYID_a Remove – SKEYID_e Remove – IKE Session Encryption Key Remove – IKE Session Authentication Key Remove – IKE RSA Private Key

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
			Remove – TLS Master Secret Remove – TLS Premaster Secret Remove – TLS Session Key Remove – TLS Integrity Key Remove – SSH Session Key Remove – SSH Authentication Key Remove – RADIUS Shared Secret Remove – IPsec Shared Secret Remove – IPsec Session Encryption Key Remove – IPsec Session Authentication Key Remove – DH Private Key

Cryptographic Boundary

The cryptographic boundary includes the entire device.

Figure 3: NSA 3500 Front

Figure 4: NSA 3500 Rear

The chassis is sealed with two 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 Figure 3 below:

Figure 5: Tamper Evident Seal Locations (Bottom)

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