SonicWALL PRO 3060/4060 FIPS 140-2 Security Policy

Level 2

Version 1.16
May 16, 2006

Copyright Notice

Table of Contents

Introduction

The SonicWALL PRO 3060/4060 (hereafter referred to as "the cryptographic module") is a multiple-chip standalone cryptographic module, hardware version 3060 101-500078-00 rev. A/4060 101-500067-00 rev. A, SonicOS Enhanced 2.0, 2.5, and 3.1. The overall FIPS validation level for the module is Security Level 2. The cryptographic module is an Internet security appliance, which provides firewall, virtual private network (VPN), and traffic shaping services.

Table 1 – Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
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	3
Self-Tests	2
Design Assurance	2
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 in the vendor documentation. The Cryptographic Officer role is referred to as Administrator in the vendor documentation.

These services are available when the module is configured both in FIPS and non-FIPS mode. The configuration settings required to enable FIPS mode are specified on page 9 of this document.

The User role is authenticated using the Limited Administrator password. 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.

The Cryptographic Officer role is authenticated using the Administrator password. The Cryptographic Officer role can show all status and configure cryptographic algorithms, cryptographic keys, certificates, and TLS 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.
- Session Management – Management access for VPN session management, such as setting and clearing logs, and enabling debugging events and traffic management.
- 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

Separation of roles is enforced by requiring users to authenticate using a password. The User role requires the use of a user password. The Cryptographic Officer role requires the use the Administrator password. Only one user may be logged in at any time.

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
- 3DES in CBC mode
- DES in CBC mode (for legacy systems)
- SHA-1
- DSA
- FIPS 186-2 Appendix 3.1 DRNG
- RSA
- HMAC-SHA-1

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

- MD5
- RC4
- Diffie-Hellman

Interfaces

Ethernet Interfaces

The cryptographic module provides six Ethernet interfaces. Each Ethernet interface is 10/100 auto-sensing with an RJ-45 connector. The Ethernet interfaces are labeled X0, X1, X2, X3, X4, and X5. Each Ethernet interface includes LINK and ACT LED's.

The Ethernet interfaces provide data input and data output.

Console Interface

The cryptographic module provides a console interface. The console interface is a DB-9 serial connector. The serial port provides a serial console. The serial console can be used for basic administration functions.

The console interface provides control input and status output.

Status LED Interface

The cryptographic module provides three Status LED's. 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 Status LED interface provides status output.

GUI Administration Interface

The cryptographic module provides a GUI administration interface.

The GUI administration interface provides control input and status output.

Power Interface

The cryptographic module provides one AC power interface.

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 passwords.
- The Administrator and Limited Administrator 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 60/96^8, 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.
- The following cryptographic algorithm self-tests are performed by the cryptographic module at power-up:

— Software integrity test (using 16-bit CRC EDC)
— DES-CBC Known Answer Test (firmware)
— Triple DES-CBC Known Answer Test (hardware and firmware)
— AES-CBC Known Answer Test (hardware and firmware)
— SHA-1 Known Answer Test
— HMAC-SHA-1 Known Answer Test
— DSA Signing and Verification Known Answer Test
— RSA Signing and Verification Known Answer Test

- The following conditional test is performed by the module:

— Continuous Random Number Generator Test on DRNG.

- 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 do not apply to this module as the module does not support the loading of unvalidated code.

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 password to at least eight characters.
- Do not enable the RADIUS server on the Users/Settings page.
- Use IKE with 3rd Party Certificates for IPSec Keying Mode when creating VPN tunnels.
- Use a computer directly connected to a LAN port when loading 3rd Party Certificates.

- Use a minimum of 1024-bits for all RSA keys.
- Use FIPS-approved encryption and authentication algorithms when creating VPN tunnels.
- Use Group 2 or Group 5 for IKE Phase 1 DH Group.
- The same RSA key cannot be used for both signing and encryption.
- Do not enable the Group VPN Policy.
- Do not enable HTTPS management.
- On the PRO 4060, do not enable Advanced Routing Services.
- Disable “Notify me when new firmware is available” from the System/Settings page.
- Enable FIPS mode from the System/Settings page by checking “FIPS Mode” checkbox.

The FIPS mode configuration can be determined by the state of the “FIPS Mode” checkbox on the System/Settings page and verification of the preceding steps.

Definition of Critical Security Parameters

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

- Data encryption keys: AES/TDES/DES keys used to encrypt data under IPSec.
- 3rd party certificates for encryption: RSA private key for IKE negotiation.
- Diffie-Hellman private key: Diffie-Hellman used for IKE negotiation.
- HMAC keys used for IKE negotiation and IPSec.
- DRNG seed keys: seed keys used with the DRNG specified in the FIPS 186-2, Appendix 3.1, with the SHA-based 'G' function.
- DRNG state: the state maintained by the DRNG.
- Authentication information: passwords used for operator authentication.

Public keys:

3rd party certificates for encryption: RSA public key for IKE negotiation.

DSA 1024-bit Public Key - Used for signature verification upon firmware load.

Diffie-Hellman public key: Diffie-Hellman keys used for IKE negotiation

All CSPs are zeroed by using the "Reset to Factory Defaults" command.

Definition of CSP Modes of Access

Table 2 — CSP Modes of Access describes the methods of accessing the individual CSPs. All operations require the user to be in the Cryptographic Officer role.

Table 2 — CSP Modes of Access

Access Method	Public/Private Keys	Data Encryption Keys	DRNG seed keys and state	DH Private Key	Authentication Information

Access Method	Public/Private Keys	Data Encryption Keys	DRNG seed keys and state	DH Private Key	Authentication Information
Import/upload	3rd party certificates can be imported into the cryptographic module.	Data encryption keys are generated on the module, not loaded or imported.	DRNG seed keys and state information can never be imported or uploaded.	D-H Private keys cannot be imported or uploaded.	Operators import authentication information when authenticating to the module.
Generate	Public/Private keys are not generated within the module.	Data encryption keys are agreed upon during the key agreement process.	DRNG seed keys and state are generated as a part of the FIPS 186-2 key generation process.	D-H Private keys are generated internally using the FIPS 186-2 DRNG.	Authentication information is not generated within the module.
Removal/deletion	3rd party certificates loaded on the cryptographic module can be deleted by following the procedure described in the user guidance.	Data encryption keys can be deleted by the commands described in the previous section, or when the "Restore To Factory Defaults" procedure is used, as described in the user guidance. All private key information is zeroized.	DRNG seed keys and state are deleted when the power is removed from the module.	D-H Keys are deleted with the Zeroization service.	Passwords are deleted when new ones are configured or when the "Restore To Factory Defaults" procedure is used. All password information is deleted.

Table 3 – 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	X	Session Management	Import/upload – authentication information.
X		Configuration Settings	Import/upload – 3rd party certificates Generate – Data encryption keys Generate – DRNG seed keys and state Generate – D-H keys
X		Key Zeroization	Remove – Private keys Remove – Data encryption keys Remove – DRNG seed keys and state Remove – Authentication information

Table 4 – Role/Services Matrix displays the cryptographic module services appropriate for each user role.

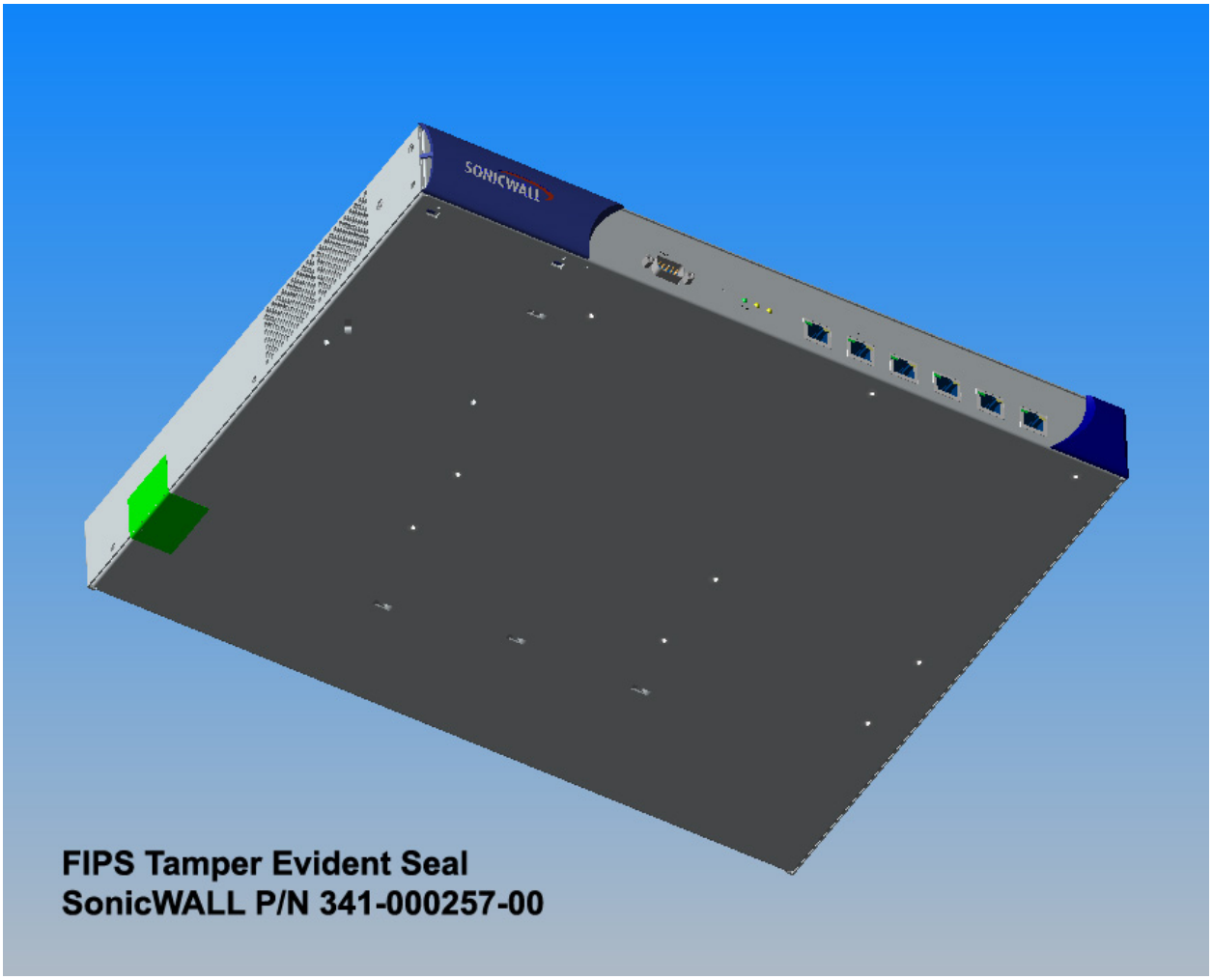
Table 4 – Role/Services Matrix

Role	Service
User Role	Query device statistics and basic configuration
Cryptographic Officer Role	Manage 3rd Party Certificates, VPN tunnels, administrator password, and device configuration

Cryptographic Boundary

The Cryptographic Boundary includes the entire device.

The chassis is sealed with a tamper-evident seal. The physical security of the module is intact if there is no evidence of tampering with the labels. The location of the tamper-evident labels is indicated in green below:



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.

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
3DES	Triple Data Encryption Standard
DES	Data Encryption Standard
CBC	Cipher Block Chaining
DSA	Digital Signature Algorithm
DRNG	Deterministic Random Number 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
D-H	Diffie-Hellman
GUI	Graphical User Interface
SHA	Secure Hash Algorithm
HMAC	Hashed Message Authentication Code

