SonicWALL TZ 180, TZ 180W, TZ 190, and TZ 190W

FIPS 140-2 Security Policy

Level 2

Version 1.4
Feb 19th, 2008

Copyright Notice

Table of Contents

Introduction

The SonicWALL TZ 180, TZ 180W, TZ 190, and TZ190W are multi-chip standalone cryptographic modules, with hardware versions as follows:

TZ 180 [HW P/N 101-500161-50 Rev. A]

TZ 180W [HW P/N 101-500160-50 Rev. A]

TZ 190 [HW P/N 101-500080-52 Rev. A]

TZ 190W [HW P/N 101-500101-52 Rev. A]

The TZ 180, TZ 180W, TZ 190, and TZ190W will hereafter be referred to as “the cryptographic module” or “the module”. The module firmware version is SonicOS v5.0.1. 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.

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	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Cryptographic Boundary

The Cryptographic Boundary includes the entire device and is defined as the physical perimeter of the metallic enclosure.

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 the red arrow in Figure 2 below:

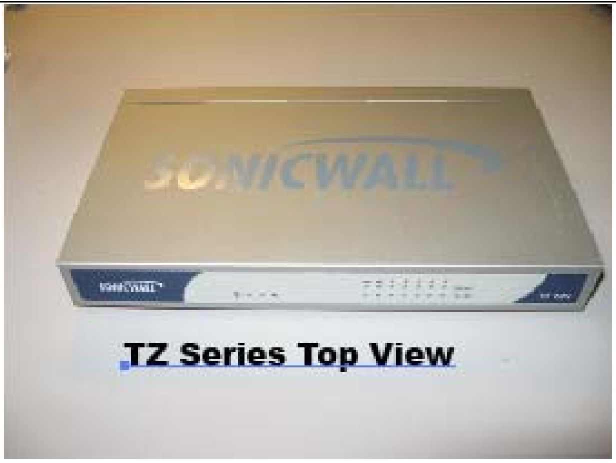

Figure 1

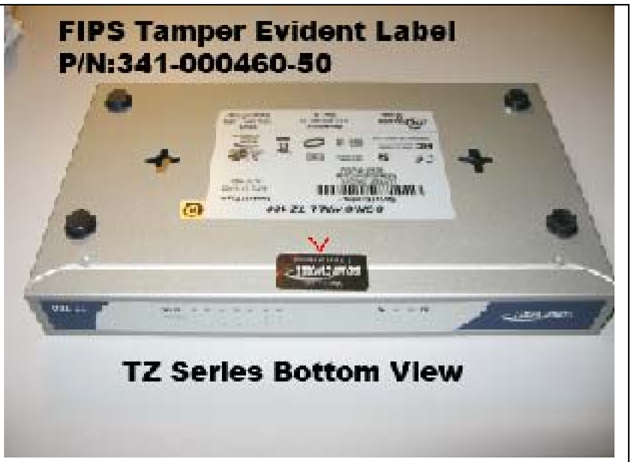

Figure 2

Pictures of each module are provided below.

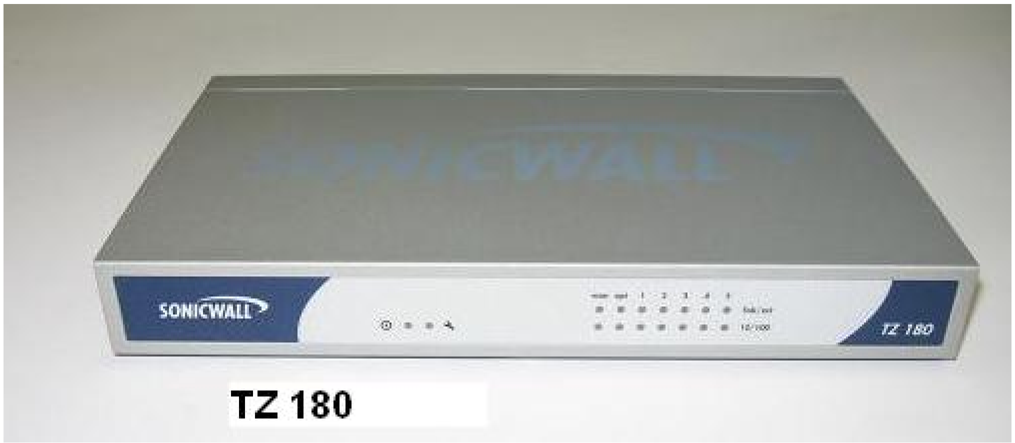

Figure 3

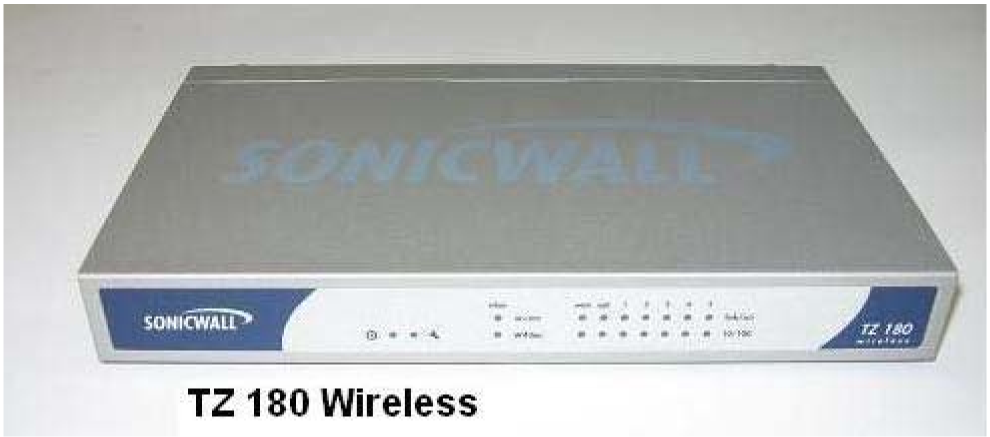

Figure 4

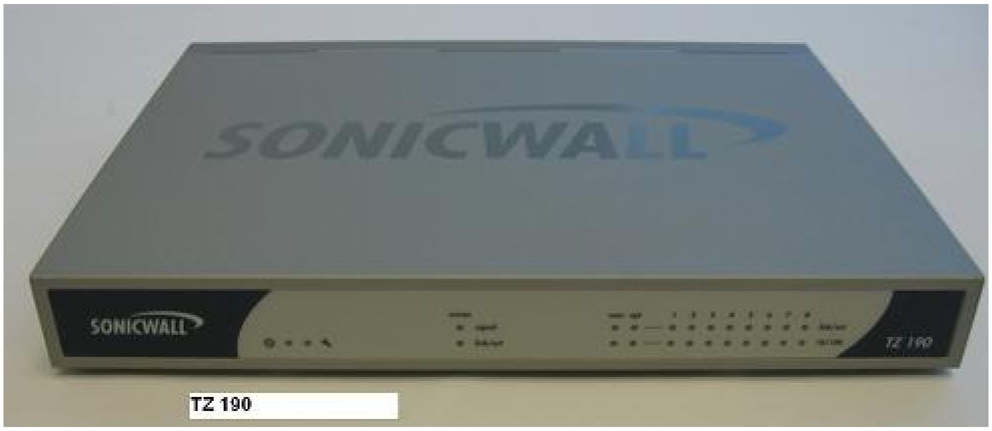

Figure 5

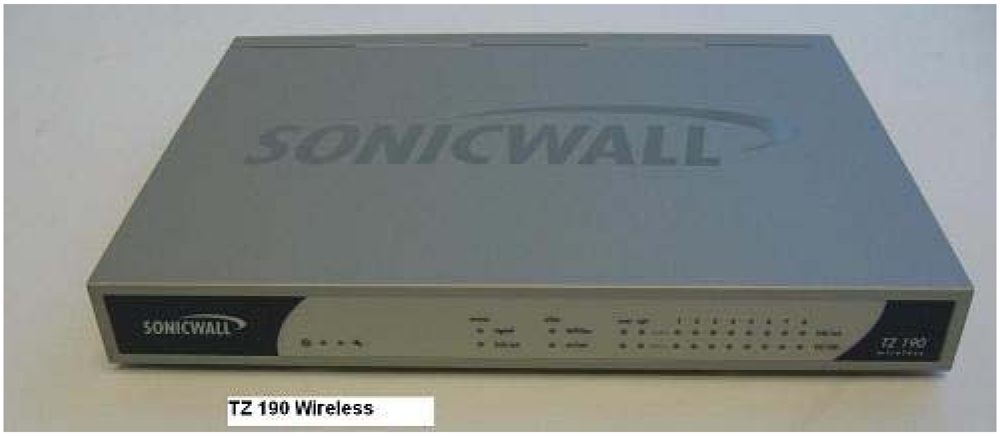

Figure 6

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 9 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, trace route, 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 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. 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

Separation of roles is enforced by requiring users to authenticate using a username and password. The User role requires the use of a username and password of a user entity belonging to the "Limited Administrators" group. The Cryptographic Officer role requires the use 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. #701)
- Triple-DES in CBC mode (Cert. #632)
- SHA-1 (Cert. #729)
- DSA (Cert. #266)
- RNG (Cert. #412)
- RSA (Cert. #327)

- HMAC-SHA-1 (Cert. #379)

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

- MD5 within MSCHAP
- RC4 within L2TP
- Diffie-Hellman within IKE (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength).
- NDRNG (used to seed the approved DRNG)

Interfaces

Ethernet Interfaces

The cryptographic module provides [Seven interfaces for TZ180/180W and 10 interfaces for TZ190/190W] Ethernet interfaces. Each Ethernet interface is [10/100/1000] auto-sensing with an [RJ-45 / SX/SC multimode fiber] connector. The Ethernet interfaces are labeled and each includes LINK and ACT LED's.

The Ethernet interfaces provide data input and data output.

Wireless Interfaces

The cryptographic module TZ180W/TZ190W provides one Wireless LAN interface. Each Wireless LAN interface is 802.11b/g wireless radio. The Wireless LAN interface is labeled and each includes ACT and WiFiSec LED's.

The Wireless LAN interface provides data input and data output.

Console Interface

The cryptographic module provides a console interface. The console interface is a [DB-9/RJ-45] serial connector. The serial port provides a serial console. The serial console can be used for basic administration functions.

The console interface provides 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 username and 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 are 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 authentication attempts, 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.
- The following cryptographic algorithm self-tests are performed by the cryptographic module at power-up:

— Software integrity test (using 16-bit CRC EDC)
— Triple-DES-CBC Known Answer Test
— AES-CBC Known Answer Test
— SHA-1 Known Answer Test
— HMAC-SHA-1 Known Answer Test
— DSA Signature Verification Pairwise Consistency Test
— RSA Signing and Verification Pairwise Consistency Test
— RNG KAT
— DH Pairwise Consistency Test

The module supports the following conditional self-tests:
— DRNG 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 password to at least eight characters.
- Do not enable the RADIUS server or LDAP on the Users/Settings page.
- Do not export PKCS #12 packages.
- 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 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 and Use SHA1 for Authentication
- The same RSA key cannot be used for both signing and encryption.
- Do not enable HTTPS management or SSH management
- Do not enable Advanced Routing Services
- Do not enable Group VPN management
- Do not enable Guest account
- Do not enable Read-Only Admin
- 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.
- FIPS operation does not include the cryptographic elements provided by native wireless security schemes WEP- Open System, WEP- Shared Key, WEP- Open System and Shared Key, WPA- PSK (Pre-Shared Key),WPA- EAP (Extensible ,authentication Protocol),WPA2- EAP,WPA2- PSK,WPA2- Auto – PSK, and WPA2- Auto - EAP. To utilize wireless networking in the defined FIPS environment, the WLAN must be configured for "Open System", and a FIPS compliant higher level method for confidentiality/integrity should be used, such as an IPsec VPN overlay, or some other approved application layer scheme.

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:

- IKE Shared Secret
- SKEYID
- SKEYID_d
- SKEYID_a
- SKEYID_e
- IKE Session Encryption Key
- IKE Session Authentication Key
- IKE RSA Private Key
- IPsec Shared Secret
- IPsec Session Encryption Key
- IPsec Session Authentication Key
- DH Private Key
- DRNG Seed Key
- Passwords

Public Keys

- Root CA Public Key
- Peer IKE RSA Public Key
- IKE RSA Public Key
- DSA Firmware Verification Key
- DH Public Key
- DH Peer Public Key

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

Definition of CSP Modes of Access

Table 2 describes the methods of accessing the individual CSPs.

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

Generate: The CSP is internally generated using the FIPS 186-2 DRNG.

Removal/Deletion: The CSP is actively destroyed.

Table 2 – 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 – DRNG Seed Key Generate – DH Private Key Generate –SKEYID Generate –SKEYID_d Generate –SKEYID_a Generate –SKEYID_e Generate –IKE RSA Private Key
X		Generate Log Reports	N/A
X		Configure VPN Settings	Generate – DRNG Seed Key Generate – DH Private Key Generate –SKEYID Generate –SKEYID_d Generate –SKEYID_a Generate –SKEYID_e

Role		**Service**	**Cryptographic Keys and CSPs Access Operation**
C.O.	**User**		
			Generate –IKE RSA Private Key Generate – IKE Shared Secret Generate –IKE Session Authentication Key Generate –IPsec Shared Secret Generate –IPsec Session Authentication Key
X		Set Encryption	Generate –IKE Session Encryption Key Generate –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 – DRNG 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 Remove –IPsec Shared Secret Remove –IPsec Session Encryption Key Remove –IPsec Session Authentication Key Remove – DH Private Key

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
Triple-DES	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
DH	Diffie-Hellman
GUI	Graphical User Interface
SHA	Secure Hash Algorithm
HMAC	Hashed Message Authentication Code