SonicWall, Inc.
SonicWALL TZ 300/TZ 300W, TZ 400/TZ 400W, TZ 500/TZ 500W, TZ 600, SOHOW, SM 9200, SM 9400, SM 9600 and NS$_a$ 2650, NS$_a$ 3600, NS$_a$ 3650, NS$_a$ 4600, NS$_a$ 4650, NS$_a$ 5600, NS$_a$ 5650, NS$_a$ 6600

Level 2

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.7

Date: September 5th, 2018

Copyright Notice

Table of Contents

List of Tables

List of Figures

1. Introduction

This document defines the Security Policy for the SonicWALL TZ 300/TZ 300W, TZ 400/TZ 400W, TZ 500/TZ 500W, TZ 600, SOHOW, SM 9200, SM 9400, SM 9600, NS$_a$ 2650, NS$_a$ 3600, NS$_a$ 3650, NS$_a$ 4600, NS$_a$ 4650, NS$_a$ 5600, NS$_a$ 5650, NS$_a$ 6600 models, hereafter denoted the Module. The Module is an Internet security appliance, which provides stateful packet filtering firewall, deep packet inspection, virtual private network (VPN), and traffic shaping services.

The Module is a multiple-chip standalone cryptographic module, in 19 configurations with hardware part numbers and versions as follows:

Table 1 – Cryptographic Module List

	Module	Hardware P/N and Version	Firmware Version
1	SOHOW	101-500410-54 Rev. E	SonicOS v6.5.1
2	TZ 300	101-500403-55 Rev. F	SonicOS v6.5.1
3	TZ 300W	101-500404-54 Rev. E	SonicOS v6.5.1
4	TZ 400	101-500405-55 Rev. F	SonicOS v6.5.1
5	TZ 400W	101-500406-54 Rev. E	SonicOS v6.5.1
6	TZ 500	101-500411-56 Rev. G	SonicOS v6.5.1
7	TZ 500W	101-500412-55 Rev. F	SonicOS v6.5.1
8	TZ 600	101-500413-56 Rev. G	SonicOS v6.5.1
9	NS$_a$ 2650	101-500452-50 Rev. A	SonicOS v6.5.1
10	NS$_a$ 3600	101-500459-54 Rev. E	SonicOS v6.5.1
11	NS$_a$ 3650	101-500514-50	SonicOS v6.5.1
12	NS$_a$ 4600	101-500458-54 Rev. E	SonicOS v6.5.1
13	NS$_a$ 4650	101-500451-50	SonicOS v6.5.1
14	NS$_a$ 5600	101-500457-54 Rev. E	SonicOS v6.5.1
15	NS$_a$ 5650	101-500517-50	SonicOS v6.5.1
16	NS$_a$ 6600	101-500456-54 Rev. E	SonicOS v6.5.1
17	SM 9200	101-500455-54 Rev. E	SonicOS v6.5.1
18	SM 9400	101-500454-54 Rev. E	SonicOS v6.5.1
19	SM 9600	101-500453-54 Rev. E	SonicOS v6.5.1

The Module firmware Version for all models is SonicOS v6.5.1. Note that the different hardware versions vary only in form factor, CPU, presence of wireless interfaces, and memory.

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated cryptographic modules. 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.

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

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	3
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
Overall	2

The overall FIPS validation level for the module is Security Level 2.

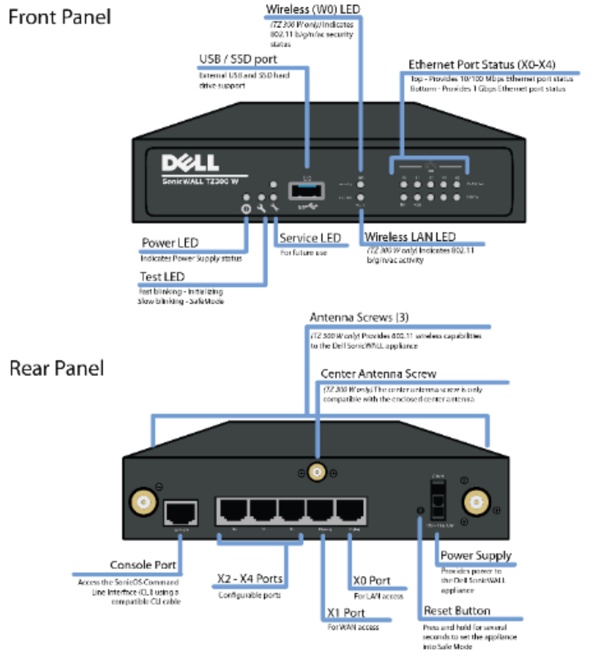
1.1 Module Description and Cryptographic Boundary

The physical form of the Module is depicted in Figure 1 through Figure 9. The Module is a multi-chip standalone embodiment. The cryptographic boundary is the surfaces and edges of the device enclosure, inclusive of the physical ports.

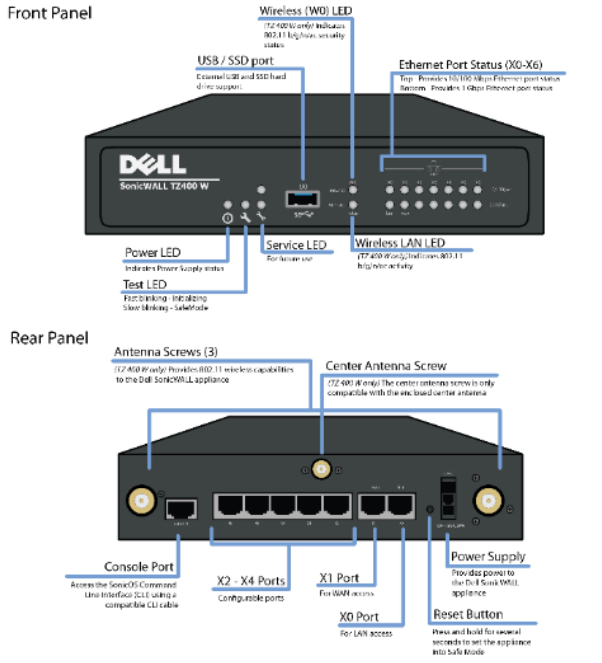
1.2 Ports and Interfaces

The Module’s ports and associated FIPS defined logical interface categories are listed in the tables in this section.

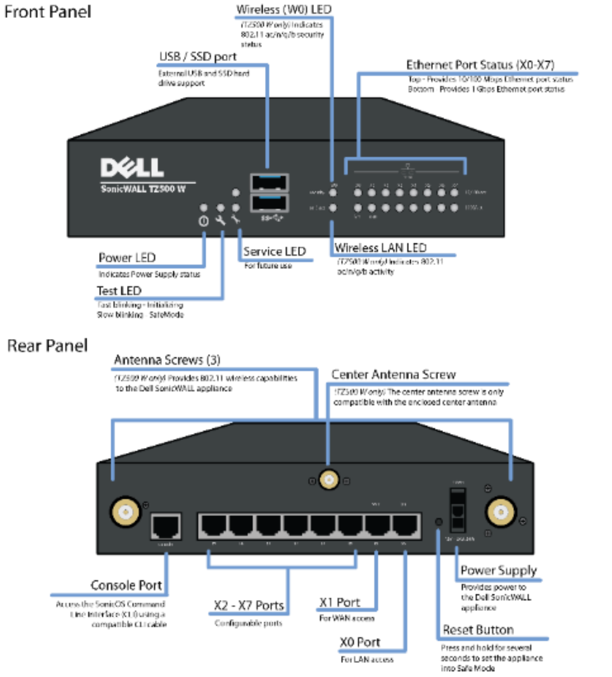
The images in Figure 1 and Figure 2 depict the physical ports for TZ 300/TZ 300W, TZ 400/TZ 400W, TZ 500/TZ 500W, TZ 600, and SOHOW.


Front Panel
Wireless (W0) LED
(TZ 300 W only) Indicates 802.11 b/g/n/ac security status
USB / SSD port
External USB and SSD hard drive support
Ethernet Port Status (X0-X4)
Top - Provides 10/100 Mbps Ethernet port status
Bottom - Provides 1 Gbps Ethernet port status
DELL
SonicWALL TZ300 W
Power LED
Indicates Power Supply status
Test LED
Fast blinking - Initializing
Slow blinking - SafeMode
Service LED
For future use
Wireless LAN LED
(TZ 300 W only) Indicates 802.11 b/g/n/ac activity
Rear Panel
Antenna Screws (3)
(TZ 300 W only) Provides 802.11 wireless capabilities to the Dell SonicWALL appliance
Center Antenna Screw
(TZ 300 W only) The center antenna screw is only compatible with the enclosed center antenna
Console Port
Access the SonicOS Command Line Interface (CLI) using a compatible CLI cable
X2 - X4 Ports
Configurable ports
X0 Port
For LAN access
X1 Port
For WAN access
Power Supply
Provides power to the Dell SonicWALL appliance
Reset Button
Press and hold for several seconds to set the appliance into Safe Mode

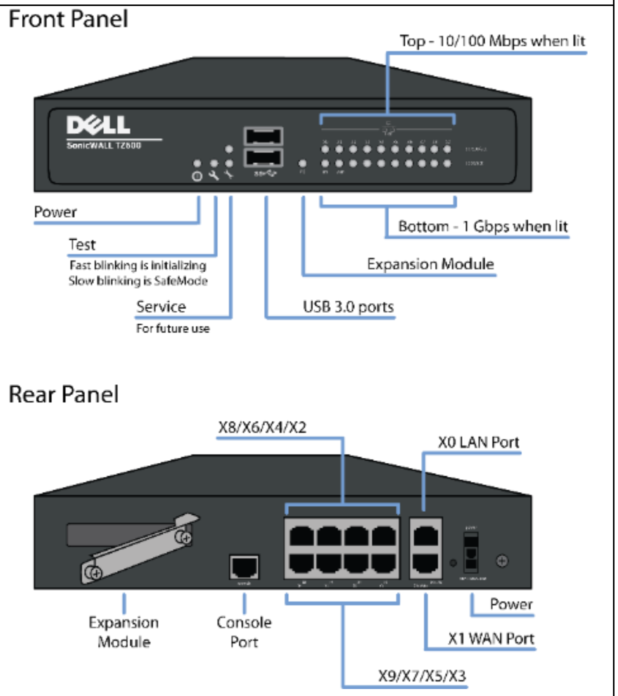
TZ 300W Physical Ports


Front Panel
Wireless (W0) LED
(TZ 400 W only) Indicates 802.11 b/g/n/ac security status
USB / SSD port
External USB and SSD hard drive support
Ethernet Port Status (X0-X6)
Top - Provides 10/100 Mbps Ethernet port status
Bottom - Provides 1 Gbps Ethernet port status
DELL
SonicWALL TZ400 W
Power LED
Indicates Power Supply status
Test LED
Fast blinking - Initializing
Slow blinking - SafeMode
Service LED
For future use
Wireless LAN LED
(TZ 400 W only) Indicates 802.11 b/g/n/ac activity
Rear Panel
Antenna Screws (3)
(TZ 400 W only) Provides 802.11 wireless capabilities to the Dell SonicWALL appliance
Center Antenna Screw
(TZ 400 W only) The center antenna screw is only compatible with the enclosed center antenna
Console Port
Access the SonicOS Command Line Interface (CLI) using a compatible CLI cable
X2 - X4 Ports
Configurable ports
X1 Port
For WAN access
X0 Port
For LAN access
Power Supply
Provides power to the Dell SonicWALL appliance
Reset Button
Press and hold for several seconds to set the appliance into Safe Mode

TZ 400W Physical Ports


Front Panel
Wireless (W0) LED
(TZ500 W only) Indicates 802.11 ac/n/g/b security status
USB / SSD port
External USB and SSD hard drive support
Ethernet Port Status (X0-X7)
Top - Provides 10/100 Mbps Ethernet port status
Bottom - Provides 1 Gbps Ethernet port status
DELL
SonicWALL TZ500 W
Power LED
Indicates Power Supply status
Test LED
Fast blinking - Initializing
Slow blinking - SafeMode
Service LED
For future use
Wireless LAN LED
(TZ500 W only) Indicates 802.11 ac/n/g/b activity
Rear Panel
Antenna Screws (3)
(TZ500 W only) Provides 802.11 wireless capabilities to the Dell SonicWALL appliance
Center Antenna Screw
(TZ500 W only) The center antenna screw is only compatible with the enclosed center antenna
Console Port
Access the SonicOS Command Line Interface (CLI) using a compatible CLI cable
X2 - X7 Ports
Configurable ports
X1 Port
For WAN access
X0 Port
For LAN access
Power Supply
Provides power to the Dell SonicWALL appliance
Reset Button
Press and hold for several seconds to set the appliance into Safe Mode

TZ 500W Physical Ports



TZ 600 Physical Ports

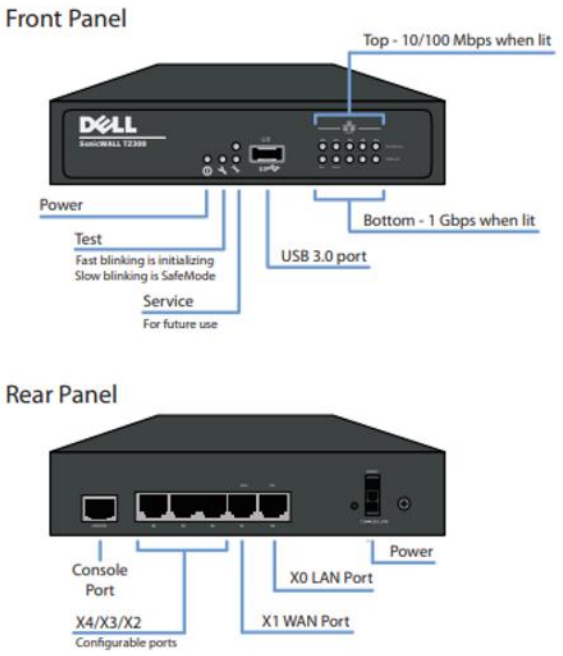
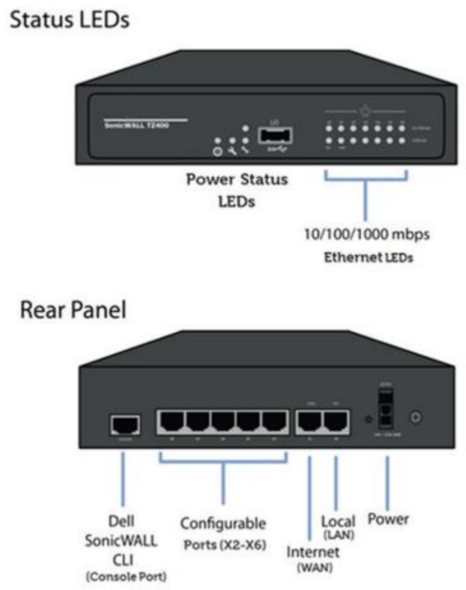
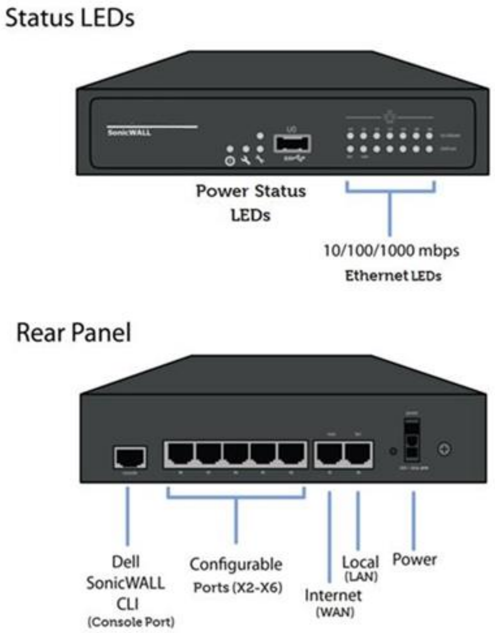
 Front Panel Top - 10/100 Mbps when lit Power Test Fast blinking is initializing Slow blinking is SafeMode Service For future use USB 3.0 port Bottom - 1 Gbps when lit Rear Panel Console Port X4/X3/X2 Configurable ports X1 WAN Port X0 LAN Port Power **TZ 300 Physical Ports**	 Status LEDs Power Status LEDs 10/100/1000 mbps Ethernet LEDs Rear Panel Dell SonicWALL CLI (Console Port) Configurable Ports (X2-X6) Local (LAN) Internet (WAN) Power **TZ 400 Physical Ports**
 Status LEDs Power Status LEDs 10/100/1000 mbps Ethernet LEDs Rear Panel Dell SonicWALL CLI (Console Port) Configurable Ports (X2-X6) Local (LAN) Internet (WAN) Power **TZ 500 Physical Ports**	

Figure 1 – TZ Series Ports

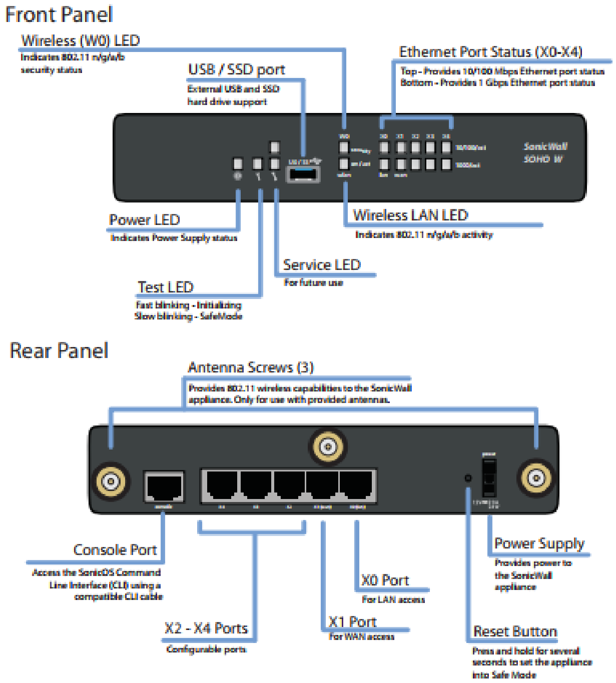

Front Panel
Wireless (W0) LED
Indicates 802.11 n/g/a/b security status
USB / SSD port
External USB and SSD hard drive support
Ethernet Port Status (X0-X4)
Top - Provides 10/100 Mbps Ethernet port status
Bottom - Provides 1 Gbps Ethernet port status
SonicWall SOHO W
Power LED
Indicates Power Supply status
Wireless LAN LED
Indicates 802.11 n/g/a/b activity
Service LED
For future use
Test LED
Fast blinking - Initializing
Slow blinking - SafeMode
Rear Panel
Antenna Screws (3)
Provides 802.11 wireless capabilities to the SonicWall appliance. Only for use with provided antennas.
Console Port
Access the SonicOS Command Line Interface (CLI) using a compatible CLI cable
X2 - X4 Ports
Configurable ports
X1 Port
For WAN access
X0 Port
For LAN access
Power Supply
Provides power to the SonicWall appliance
Reset Button
Press and hold for several seconds to set the appliance into Safe Mode

Figure 2 – SOHOW Physical Ports

Table 3 describes the physical ports (mapped to the figures above) and corresponding logical interfaces.

Table 3 – Front Panel Ports and Interfaces for TZ 300/TZ 300W, TZ 400/TZ 400W, TZ 500/TZ 500W, TZ 600 models

Physical Ports	Qty.	Description	Logical Interfaces
Front Panel			
Status LEDs	Varies	TZ 300W, TZ 400W, TZ 500W, SOHOW – 6 status LEDs TZ 300, TZ 400, TZ 500 – 4 status LEDs (No wireless) TZ 600- 5 status LEDs Power: Indicate module is receiving power. Test: Indicates module is initializing and performing self-tests. Service: Unused; for future use Wireless: Unused in Approved mode. M0: Expansion Module (Only for TZ 600)	Status output
Ethernet LEDs	2/port	Ethernet activity: 10/100 activity (top); 1G activity (bottom)	Status output
USB	Varies	TZ 300/TZ 300W, TZ 400/TZ 400W, SOHOW – 1 USB TZ 500/TZ 500W, TZ 600 – 2 USB	N/A

Physical Ports	Qty.	Description	Logical Interfaces
		Allows the attachment of an external device. Security Guidance is "not to be used in FIPS Mode"	
		Rear Panel	
Reset Button	1	Used to manually reset the appliance to Safe Mode. (Not available on TZ 600)	Control input
Power Interface	1	AC power interfaces	Power
Console	1	Serial console (local) interface.	Control In, Status Out
Ethernet Interfaces	Varies	TZ 300/TZ 300W (Qty 5) TZ 400/TZ 400W (Qty 7) TZ 500/TZ 500W (Qty 8) TZ 600 (Qty 10)	Control In, Status Out, Data input, Data output
Antenna Connectors	3	*For Antennas (TZ 300W, TZ 400W, TZ 500W models only; unused in Approved mode)*	N/A
Expansion	1	*(TZ 600 only) Expansion connector, unused, disconnected internally.*	N/A

Figure 3 shows the locations of the physical ports on the front of the SM 9200, SM 9400, and SM 9600.

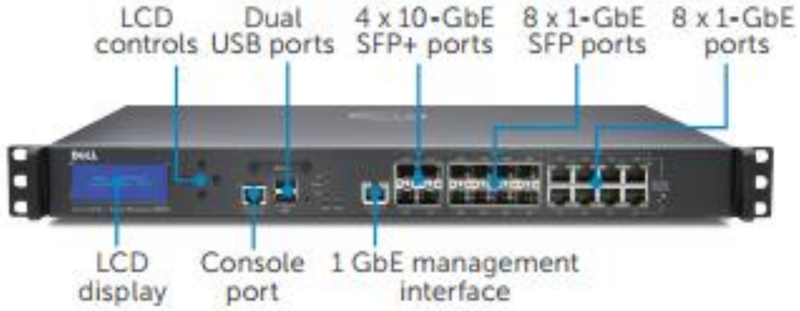


Figure 3– Super Massive Front Panel SM 9200, SM 9400, SM 9600

Table 4 describes the physical ports (mapped to Figure 3) and corresponding logical interfaces.

Table 4 – Front Panel Ports and Interfaces

Physical Ports	Qty.	Description	Logical Interfaces
LCD display	1	LCD status display	Status output

Physical Ports	**Qty.**	**Description**	**Logical Interfaces**
LCD controls	4	Controls for scrolling thru the LCD display options	Control input, status output
Serial Console Interface	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 Control input and status output
USB Interfaces	2	Allows the attachment of an external device. Security Guidance is “ not to be used in FIPS Mode”	N/A
Reset (Safe Mode) Button Interface	1	Used to manually reset the appliance to Safe Mode.	Control input
Status LED Interface	6	Power LEDs: Indicate module is receiving power. Test LED: Indicates module is initializing and performing self-tests. Alarm LED: Indicates alarm condition. M0: *Indicates expansion module*	Status output
Secure Digital High Capacity Port	1	*Currently not used and does not provide any service or function.*	N/A
Ethernet Management Interface	1	1Gbps RJ45 interface labeled as MGMT, includes LINK and ACT LEDs Management interface is solely used for Outband management of the device. The management interface provides dedicated access for the system administration via HTTP/HTTPS/SSH/SNMP and is not shared with other types of network traffic.	Control In, Status Out, data input and data output
Ethernet Interfaces	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, and control input (via the external GUI Administration interface)
Ethernet hot-pluggable SFP	8	4x 1GbE SFP interfaces supporting RJ-45/SX/SC multimode fiber connector with LINK and ACT LEDs.	Data input, data output, status output, and control input (via the external GUI Administration interface)

Physical Ports	Qty.	Description	Logical Interfaces
Ethernet 10GE hot-pluggable SFP	4	2x 10GbE SFP+ interfaces with LINK and ACT LEDs	Data input, data output, status output, and control input (via the external GUI Administration interface)

Figure 4 shows the locations of the physical ports on the back of the Super Massive modules.

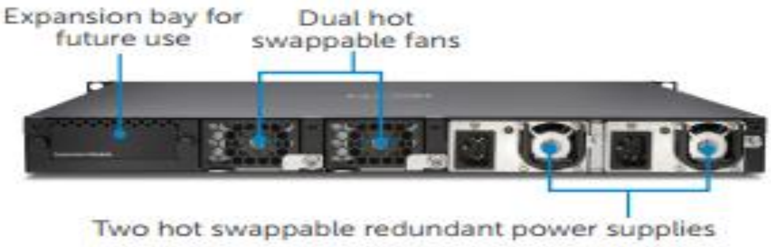

Expansion bay for future use
Dual hot swappable fans
Two hot swappable redundant power supplies

Figure 4 - Super Massive Back Panel for SM 9200, SM 9400, SM 9600

Table 5 describes the physical ports (mapped to Figure 2) and corresponding logical interfaces.

Table 5 – Back Panel Ports and Interfaces for SM 9200, SM 9400, SM 9600 mapped to Figure 4

Physical Ports	Qty.	Description	Logical Interfaces
Power Interface	2	AC power interfaces	Power
Expansion Bay	1	*Currently not used and does not provide any service or function.*	N/A
Fan Interface	2	Dual removable fan components	N/A

Figure 5 shows the locations of the physical ports on the front of the NSa 6600 module.

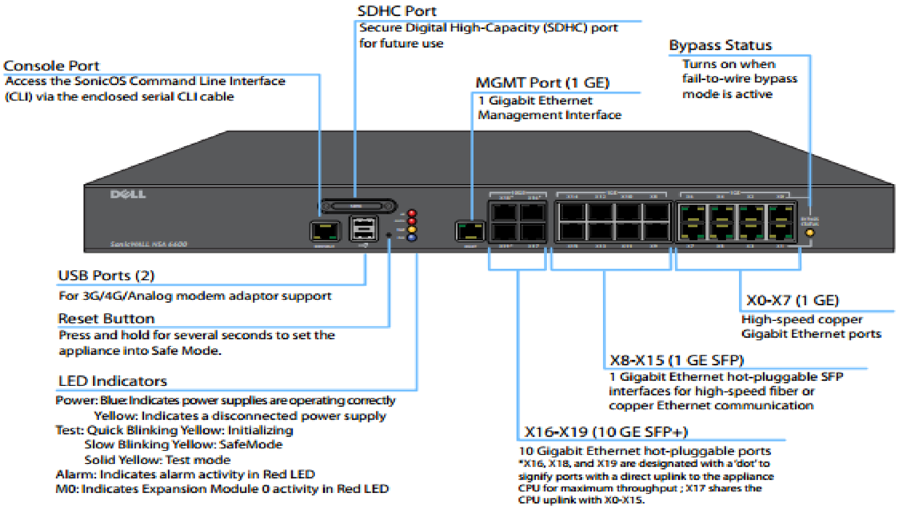

SDHC Port
Secure Digital High-Capacity (SDHC) port for future use
Bypass Status
Turns on when fail-to-wire bypass mode is active
Console Port
Access the SonicOS Command Line Interface (CLI) via the enclosed serial CLI cable
MGMT Port (1 GE)
1 Gigabit Ethernet Management Interface
DELL
SonicWALL NSA 6600
USB Ports (2)
For 3G/4G/Analog modem adaptor support
Reset Button
Press and hold for several seconds to set the appliance into Safe Mode.
LED Indicators
Power: Blue: Indicates power supplies are operating correctly
Yellow: Indicates a disconnected power supply
Test: Quick Blinking Yellow: Initializing
Slow Blinking Yellow: SafeMode
Solid Yellow: Test mode
Alarm: Indicates alarm activity in Red LED
M0: Indicates Expansion Module 0 activity in Red LED
X0-X7 (1 GE)
High-speed copper Gigabit Ethernet ports
X8-X15 (1 GE SFP)
1 Gigabit Ethernet hot-pluggable SFP interfaces for high-speed fiber or copper Ethernet communication
X16-X19 (10 GE SFP+)
10 Gigabit Ethernet hot-pluggable ports
*X16, X18, and X19 are designated with a 'dot' to signify ports with a direct uplink to the appliance CPU for maximum throughput ; X17 shares the CPU uplink with X0-X15.

Figure 5 – NS$_a$ 6600 Front Panel

Table 6 – Front Panel Ports and Interfaces for NS$_a$ 6600, NS$_a$ 5600, NS$_a$ 4600, NS$_a$ 3600 mapped to Figures 5 and 7

Physical Ports	Qty.	Description	Logical Interfaces
Serial Console Interface	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 Control input and status output only
USB Interfaces	2	Allows the attachment of an external device. Security Guidance is “not to be used in FIPS Mode”	N/A
Reset (Safe Mode) Button Interface	1	Used to manually reset the appliance to Safe Mode.	Control input
Status LED Interface	6	Power LEDs: Indicate module is receiving power. Test LED: Indicates module is initializing and performing self-tests. Alarm LED: Indicates alarm condition. M0: Indicates expansion module	Status output
Secure Digital High Capacity Port	1	*Currently not used and does not provide any service or function.*	N/A
Ethernet Management Interface	1	1Gbps RJ45 interface labeled as MGMT, includes LINK and ACT LEDs Management interface is solely used for Outband management of the device. The management interface provides dedicated access for the system administration via	Control In, Status Out, Data input, Data output

Physical Ports	Qty.	Description	Logical Interfaces
		HTTP/HTTPS/SSH/SNMP and is not shared with other types of network traffic.	
Ethernet Interfaces	Varies	NS$_a$ 6600: 8 x 1Gbe Eth interfaces NS$_a$ 5600, NS$_a$ 4600, NS$_a$ 3600: 12 x 1Gbe Eth interfaces 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)
Ethernet hot-pluggable SFP	Varies	NS$_a$ 6600: 8 x 1Gbe SFP ports NS$_a$ 5600, NS$_a$ 4600, NS$_a$ 3600: 4 x 1Gbe SFP ports 1GbE SFP interfaces supporting RJ-45/SX/SC multimode fiber connector with LINK and ACT LEDs.	Data input, data output, status output, and control input (via the external GUI Administration interface)
Ethernet 10GE hot-pluggable SFP	Varies	NS$_a$ 6600: 4 x 10Gbe SFP+ interfaces NS$_a$ 5600, NS$_a$ 4600, NS$_a$ 3600: 2 x 10Gbe SFP+ interfaces 10GbE SFP+ interfaces with LINK and ACT LEDs	Data input, data output, status output, and control input (via the external GUI Administration interface)

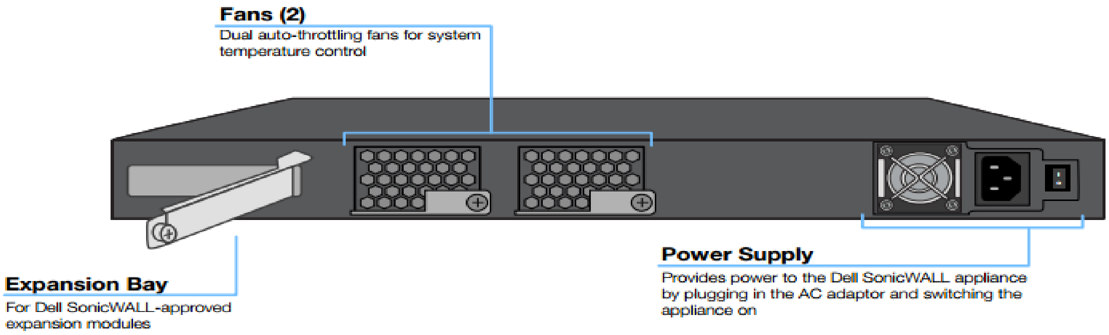

Fans (2)
Dual auto-throttling fans for system temperature control
Power Supply
Provides power to the Dell SonicWALL appliance by plugging in the AC adaptor and switching the appliance on
Expansion Bay
For Dell SonicWALL-approved expansion modules

Figure 6 – NS$_a$ 6600 Back Panel

Table 7 - Back Panel Ports and Interfaces mapped to Figures 6 and 8

Physical Ports	Qty.	Description	Logical Interfaces
Power Interface	1	AC power interfaces	Power
Expansion Bay	1	*Currently not used and does not provide any service or function.*	N/A
Fan Interface	2	Dual hot swappable fans (NS$_a$ 6600)	N/A

Physical Ports	Qty.	Description	Logical Interfaces
		Dual Fans (NS$_a$ 5600, NS$_a$ 4600, NS$_a$ 3600)	

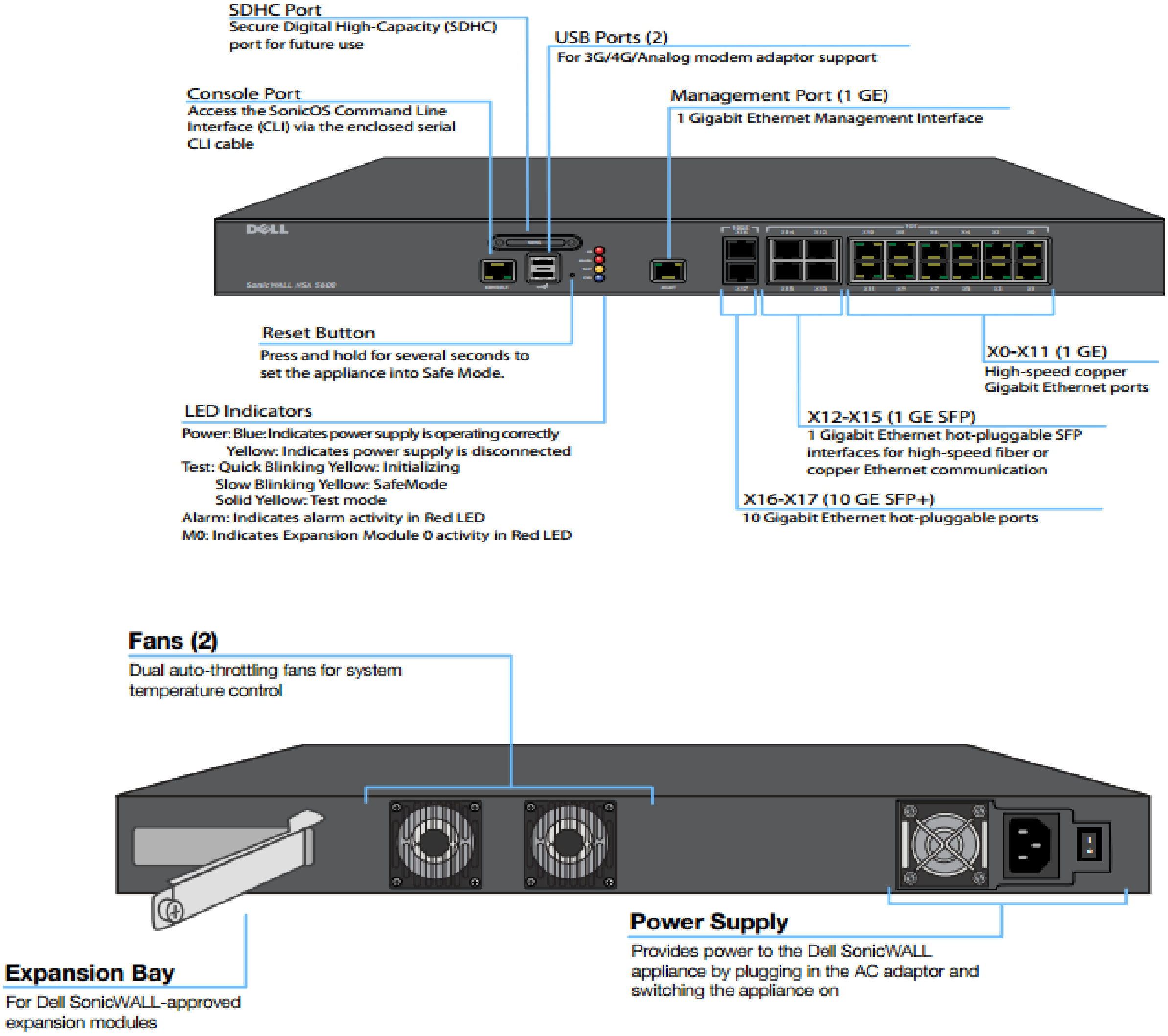

SDHC Port
Secure Digital High-Capacity (SDHC) port for future use
USB Ports (2)
For 3G/4G/Analog modem adaptor support
Console Port
Access the SonicOS Command Line Interface (CLI) via the enclosed serial CLI cable
Management Port (1 GE)
1 Gigabit Ethernet Management Interface
DELL
SonicWALL NSA 5600
Reset Button
Press and hold for several seconds to set the appliance into Safe Mode.
X0-X11 (1 GE)
High-speed copper Gigabit Ethernet ports
LED Indicators
Power: Blue: Indicates power supply is operating correctly
Yellow: Indicates power supply is disconnected
Test: Quick Blinking Yellow: Initializing
Slow Blinking Yellow: SafeMode
Solid Yellow: Test mode
Alarm: Indicates alarm activity in Red LED
M0: Indicates Expansion Module 0 activity in Red LED
X12-X15 (1 GE SFP)
1 Gigabit Ethernet hot-pluggable SFP interfaces for high-speed fiber or copper Ethernet communication
X16-X17 (10 GE SFP+)
10 Gigabit Ethernet hot-pluggable ports
Fans (2)
Dual auto-throttling fans for system temperature control
Power Supply
Provides power to the Dell SonicWALL appliance by plugging in the AC adaptor and switching the appliance on
Expansion Bay
For Dell SonicWALL-approved expansion modules

Figure 7 – NS$_a$ 5600, NS$_a$ 4600, NS$_a$ 3600 Front Panel

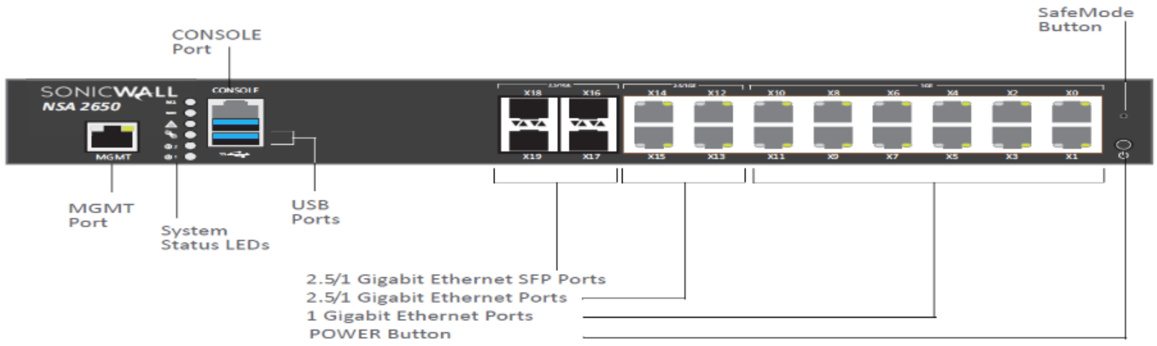


Figure 8 – NS$_a$ 3600, NS$_a$ 4600, NS$_a$ 5600 Back Panel

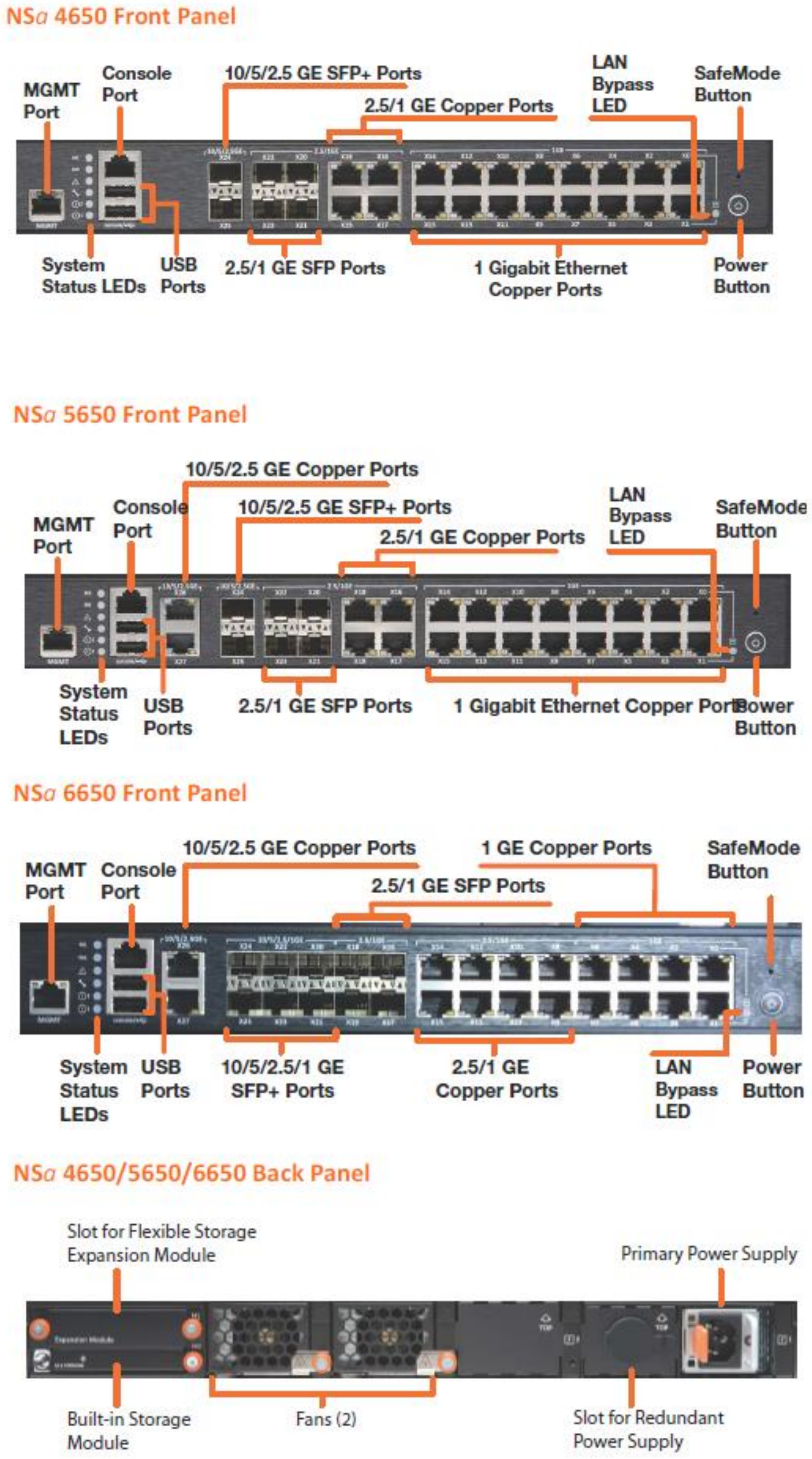


Figure 9 - NS$_a$ 2650, NS$_a$ 3650, NS$_a$ 4650, NS$_a$ 5650 Front Panel

Table 8 describes the physical ports (mapped in Figure 9) and corresponding logical interfaces for NS*a* 2650, NS*a* 3650, NS*a* 4650, NS*a* 5650

Table 8 – Ports and Interfaces for NS*a* 2650, NS*a* 3650, NS*a* 4650, NS*a* 5650

Physical Ports	**Qty.**	**Description**	**Logical Interfaces**
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. Control input and status output only
USB	2	Allows the attachment of an external device. Security Guidance is " not to be used in FIPS Mode"	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. M0/M1: Expansion Module activity	Status output
Expansion	1	*Expansion connector, unused, disconnected internally. Located in the front panel on the 2600, and in the rear panel in all other configurations.*	N/A
MGMT	1	1Gbps RJ45 isolated out-of-band management (MGMT) port, with integral LINK and ACT LEDs	Control input, status output, data input and data output
Ethernet [1Gbe]	Varies	NS*a* 2650, NS*a* 3650: 12 x 1Gbe Ethernet interfaces NS*a* 4650, NS*a* 5650: 16 x 1Gbe Ethernet interfaces 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
Ethernet [1/2.5Gbe]	4	1G/2.5G 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
1G/2.5G SFP	Varies	NS*a* 2650, NS*a* 4650, NS*a* 5650: 4x 1G/2.5G Ethernet interfaces NS*a* 3650: 8 x 1G/2.5G Ethernet interfaces 1GbE 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

Physical Ports	Qty.	Description	Logical Interfaces
10/5/2.5 GE SFP+	2	NS_a 2650 : 0 NS_a 3650, NS_a 4650, NS_a 5650:2 x 10/5/2/5G SFP+ interfaces 10GbE Ethernet hot-pluggable SFP+ interfaces with LINK and ACT LEDs	Data input, data output, status output, control input
10/5/2/5 GE copper Ports	2	NS_a 2650, NS_a 3650, NS_a 4650: 0 NS_a 5650: 2 x 10/5/2/5G copper Ethernet interfaces 10/5/2/5 Gbe copper Ethernet 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
Power	1	AC power input and switch	Power

Table 9 - Back Panel Ports and Interfaces for NS_a 2650, NS_a 3650, NS_a 4650, NS_a 5650 mapped to Figures 9

Physical Ports	Qty.	Description	Logical Interfaces
Power Interface	1	AC power interfaces	Power
Redundant power	1	Slot for redundant power supply	Power
Storage module	1	M0 storage module	Storage
Expansion Bay for storage	1	*Currently not used and does not provide any service or function.*	N/A
Fan Interface	2	Dual hot swappable fans Dual Fans	N/A

1.3 Modes of Operation

1.3.1 FIPS 140-2 Approved mode of Operation

The FIPS mode configuration can be determined by an operator, by checking the state of the “FIPS *Mo*de” checkbox on the System/Settings page over the web interface or issuing “show fips” over the console . When the “FIPS Mode” checkbox is selected, the module executes a compliance checking procedure, examining all settings related to the security rules described below. The operator is responsible for updating these settings appropriately during setup and will be prompted by the compliance tool if a setting has been modified taking the module out of compliance. The “FIPS Mode” checkbox and corresponding system flag (“fips”) which can be queried over the console will not be set unless all settings are compliant. The “FIPS Mode” checkbox and fips system flag are indicators that the module is running in the FIPS Approved mode of operation.

The module is not configured to operate in FIPS-mode by default. The following steps must be taken during set-up of the module to enable FIPS-mode of operation:

1. The default Administrator and User passwords shall be immediately changed and be at least eight (8) characters.
2. The RADIUS shared secret must be set to at least eight (8) characters.
3. Traffic between the module and the RADIUS server must be configured so that it is secured via an IPSec tunnel.
   Note: this step need only be performed if RADIUS is supported.
    - LDAP cannot be enabled in FIPS mode without being protected by TLS
    - LDAP cannot be enabled in FIPS mode without selecting 'Send LDAP Start TLS request'
    - LDAP cannot be enabled in FIPS mode without selecting 'Require valid certificate from server'
    - LDAP cannot be enabled in FIPS mode without valid local certificate for TLS

4. IKE must be configured with 3rd Party Certificates for IPsec Keying Mode when creating VPN tunnels.
    - RSA Certificates lengths must be 2048-bit or greater in size
5. When creating VPN tunnels, ESP must be enabled for IPSec.
6. FIPS-approved algorithms must be used for encryption and authentication when creating VPN tunnels.
7. Group 14, 19, 20 or 21 must be used for IKE Phase 1 DH Group. SHA-256 must be used for Authentication
8. Bandwidth management must be set to “ON”.
9. “Advanced Routing Services” must not be enabled.
10. “Group VPN management” must not be enabled.
11. SNMP or SSH must not be enabled.

Note: Once FIPS mode of operation is enabled SonicOS enforces all of the above items. Operators will not be allowed to enable these features while in FIPS mode of operation.

The module does not enforce but as a policy User should not enable the below feature while in FIPS mode of operation:

- Do not use USB interface
- In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption muse be established.

1.3.2 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. These services are not enabled by default, if operator selects to enable these services the system will transition to non-approved mode of operation.

- 802.11i wireless security

- AAA server authentication (the Approved mode requires operation of RADIUS only, within a secure VPN tunnel)
- SSH[1]
- SNMP[2]
- Wireless interface usage

2. Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 9 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
#5346	AES [197]	CBC [38A]	Key Sizes: 128, 192, 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 128, 192, 256	Encrypt
		GCM [38D][3]	Key Sizes: 128, 192, 256 Tag Len: 128	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
Vendor Affirmed	AES [IG A.3]	AES-CBC Ciphertext Stealing (CBC-CS1)	Key Sizes: 128, 192, 256	Encrypt, Decrypt
Vendor Affirmed	CKG [IG D.12]	[133] Section 6.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation
		[133] Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output		
		[133] Section 7.1 Direct symmetric key generation using unmodified DRBG output		
		[133] Section 7.3 Derivation of symmetric keys from a key agreement shared secret.		
		[133] Section 7.4 Derivation of symmetric keys from a pre-shared key		
		[133] Section 7.6 Combining multiple keys and other data		

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

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

[3] The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS and RFC 4106 and 7296 for IPSec/IKEv1 and IKEv2.

Cert	Algorithm	Mode	Description	Functions/Caveats
#1808	CVL: All of SP800-56A except KDF [56A]	FFC (Initiator, Responder)(Hybrid1, Ephem, Hybrid1Flow, OneFlow, Static)	FB, FC	Key Agreement
		ECC (Initiator, Responder)(FullUnified, EphemUnified, OnePassUnified, OnePassDH, StaticUnified)	P-224, P-256, P-384, P-521	
#1809	CVL: IKEv1 [135]	DSA, PSK[135]	SHA(256, 384, 512)	Key Derivation
	CVL: IKEv2 [135]	DH 224-521 bits	SHA(256, 384, 512)	
	CVL: TLS [135][4]	v1.0, v1.1	SHA 256, 384, 512	
	CVL: SSH [135]	v2	SHA-1	
	CVL:SNMP [135]		SHA-1	
#2066	DRBG [90Arev1]	Hash	SHA-256	Deterministic Random Bit Generation
#1381	DSA [186-4][5]		(L = 2048, N = 224) (L = 2048, N = 256) (L = 3072, N= 256)	KeyGen
			(L = 2048, N = 224) SHA(256, 384, 512) (L = 2048, N = 256) SHA(256, 384, 512) (L = 3072, N = 256) SHA(256, 384, 512)	PQG Gen
			(L = 1024, N = 160) SHA(1, 256, 384, 512) (L = 2048, N = 224) SHA(256, 384, 512) (L = 2048, N = 256) SHA(256, 384, 512)	PQG Ver

[4] SSH, SNMP, TLS 1.0 and 1.1 KDFs were CAVP tested but are not supported in the Approved mode of operation.

[5] DSA was CAVP tested but is only used as a pre-requisite for CVL Cert. #1808.

Cert	Algorithm	Mode	Description	Functions/Caveats
			(L = 3072, N = 256) SHA(256, 384, 512)	
			(L = 1024, N = 160) SHA(1, 256, 384, 512) (L = 2048, N = 224) SHA(1, 256, 384, 512) (L = 2048, N = 256) SHA(1, 256, 384, 512) (L = 3072, N = 256) SHA(1, 256, 384, 512)	SigVer
#1406 #1810 (CVL)	ECDSA [186-4]		P-224, P-256, P-384, P-521,	KeyGen
			P-192, P-224, P-256, P-384, P-521	PKV
			P-224 [6]SHA(1, 256, 384, 512) P-256 SHA(1, 256, 384, 512) P-384 SHA(1, 256, 384, 512) P-521 SHA(1, 256, 384, 512)	SigGen
			P-192 SHA(1, 256, 384, 512) P-224 SHA(1, 256, 384, 512) P-256 SHA(1, 256, 384, 512) P-384 SHA(1, 256, 384, 512) P-521 SHA(1, 256, 384, 512)	SigVer
#3543	HMAC [198]	SHA-1	Key Sizes: KS < BS λ = *12*	Message Authentication, KDF Primitive, Password Obfuscation
		SHA-256	Key Sizes: KS = BS λ = *32*	
		SHA-384	Key Sizes: KS = BS λ = *48*	
		SHA-512	Key Sizes: KS = BS λ = *64*	
#5346 #3543	KTS [IG G.8]	AES (Cert. #5346); HMAC (Cert. #3543)	AES (Key Sizes: 128, 192, 256); HMAC SHA(1, 256, 384, 512)	Encryption, Key Transport, Authentication using within TLS 1.2

#2861	RSA [186-4]	X9.31	n = 2048
			n = 3072
				KeyGen

		PKCS1_v1.5	n = 2048 SHA(256, 384, 512)
			n = 3072 SHA(256, 384, 512)
				SigGen

[6] ECDSA P-224 was been CAVP tested but are not supported in the Approved mode of operation.

Cert	Algorithm	Mode	Description	Functions/Caveats

		PKCS1_v1.5 [186-2 Legacy]	n = 1024 SHA-1
			n = 1536 SHA-1
			n = 2048 SHA-1
				SigVer

		PKCS1_v1.5 [186-4]	n = 1024 SHA(1, 256, 384, 512)
			n = 2048 SHA(1, 256, 384, 512)
			n = 3072 SHA(256, 384, 512)
				SigVer

#4297	SHS [180]	SHA-1 SHA-256 SHA-384 SHA-512		Message Digest Generation, Password Obfuscation
#2704	Triple-DES [67][7]	TCBC [38A]	Key Size: 192	Encrypt, Decrypt

Table 10 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
DH	Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
EC DH	EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)
RSA	RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
NDRNG (used only to seed the Approved DRBG)	NDRNG (internal entropy source) for seeding the Hash_DRBG. The module generates a minimum of 256 bits of entropy for key generation.

Table 11 – Security Relevant Protocols Used in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv1	Oakley Group 14, 19, 20, 21	Pre-shared key RSA/ECDSA digital signature	AES CBC 128/192/256 AES GCM 16 octet ICV	SHA 256/384/512

[7] Triple-DES was CAVP tested but is not available in the Approved mode of operation.

Protocol	Key Exchange	Auth	Cipher	Integrity
IKEv2	Oakley Group 14, 19, 20, 21	RSA/ECDA Digital Signature Shared Key Message Integrity Code	AES CBC 128/192/256 AES GCM 16 octet ICV	HMAC-SHA-1-96 HMAC-SHA-1-160 AES-128-GMAC AES-192-GMAC AES-256-GMAC HMAC-SHA-256-128 HMAC-SHA-384-192 HMAC-SHA-512-256
IPsec ESP	IKEv1 or IKEv2 with optional: Diffie-Hellman (L=2048, N=224, 256) EC Diffie-Hellman P-256, P-384	IKEv1, IKEv2	AES CBC 128/192/256	HMAC-SHA-1-96 HMAC-SHA-256-128 HMAC-SHA-384-192 HMAC-SHA-512-256
TLS 1.2 or SSL 3.1	RSA_WITH_AES_128_CBC_SHA RSA_WITH_AES_256_CBC_SHA RSA_WITH_AES_128_CBC_SHA256 RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384			

Note: no parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

1.3.3 Non-Approved Algorithms with No Security Claimed

The module supports the following non-Approved but allowed algorithms and protocols with no security claimed:

- Triple-DES (non-compliant)
- MD5 (no security claimed)
- PBKDF (non-complaint)

The operator must also follow the rules outlined in Section 1.3.1 and consult FIPS 140-2 IG 1.23 for further understanding of the use of functions where no security is claimed. Section 3.3 indicates the module services associated with these functions.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 3.3.

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

- IKE Shared Secret – Shared secret used during IKE Phase 1 (length 4 ~ 128 bytes)
- 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 Pre-Shared Key – ECDSA 2048, 3072, 4092 bits used to authenticate IKE connections.
- 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 Private Key – ECDSA 2048, 3072, 4092 bits and RSA 2048 bit 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 (384-bits)
- TLS Premaster Secret - used for the generation of Master Secret (384 bits)
- TLS Session Key - AES 128, 192, 256 key used to protect TLS connection
- TLS Integrity Key - HMAC 256/384/512 bit key used to check the integrity of TLS connection
- Diffie-Hellman/EC Diffie-Hellman - Diffie-Hellman Private Key (N = 224, 256) or EC DH P-256/P-384 used within IKE or TLS key agreement
- DRBG V and C values – Used to seed the Approved DRBG
- Entropy Input: 256-bits seed used to instantiate the DRBG
- RADIUS Shared Secret – Used for authenticating the RADIUS server to the module and vice versa
- Passwords – Authentication data

2.2 Public Keys

The following Public Keys are contained in the cryptographic module:

- Root CA Public Key – Used for verifying a chain of trust for receiving certificates
- Peer IKE Public Key – ECDSA 2048, 3048, 4092 bits and RSA 2048 bit key for verifying digital signatures from a peer device
- IKE Public Key – ECDSA 2048, 3048, 4092 bits and RSA 2048 bit key for verifying digital signatures created by the module
- Firmware Verification Key – 2048 bit ECDSA key used for verifying firmware during firmware load
- Diffie-Hellman/EC Diffie-Hellman Public Key – Diffie-Hellman 2048-bit key, EC Diffie-Hellman P-256/P-384 used within TLS key agreement
- Diffie-Hellman/EC Diffie-Hellman Peer Public Key – Diffie-Hellman 2048-bit key, EC DH P-256/P-384/P-521 [8]used within TLS key agreement
- Authentication Public Key – 2048-bit RSA public key used to authenticate the User
- TLS Public Key – RSA – 2048-bit public key used in the TLS handshake

[8] P-521 curve only available for IKEv1 and IKEv2

3. Roles, Authentication and Services

3.1 Assumption of Roles

The cryptographic module provides the roles described in Table 12. The cryptographic module does not provide a Maintenance role. 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 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 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 in Section 8 of this document.

Table 12 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Referred to as “Administrator” (individual user) or “SonicWALL Administrators” (user group) in the vendor documentation	Role-based and identify-based	Username and Password
User	Referred to as “Limited Administrator” (individual user) or “Limited Administrators” (user group) in the vendor documentation	Identity-based	Username and Password or Digital Signature

The Module supports concurrent operators. 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.

3.2 Authentication Methods

The cryptographic module provides authentication relying upon username/passwords or an RSA 2048-bit (at a minimum) digital signature verification.

Table 13 – Authentication Description

Authentication Method	Probability	Justification
CO and User password	The probability is 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.	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, hence, the probability is 1 in 96^8.

Authentication Method	Probability	Justification
User RSA 2048-bit (minimum) digital signature	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 = 5.8E-32, which is less than 1 in 100,000.	A 2048-bit RSA digital signature has a strength of 112-bits, hence the probability is 1/2^112.

3.3 Services

3.3.1 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

3.3.2 Crypto Officer Services

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.

- Show Status - Monitoring, pinging, traceroute, viewing logs.
- Configuration Settings – System configuration[9], 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[10]
    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
- Zeroize – Zeroizing cryptographic keys
- TLS – TLS used for the https configuration tool or network traffic over a TLS VPN
- IPsec VPN [11]– 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.

3.3.3 Unauthenticated services

- Module Reset - Firmware removal with configuration return to factory state
- NoAuth Function - Authenticates the operator and establishes secure channel.
- Show Status – LED activity and console message display

[9] Non-compliant Triple-DES implementation associated with the configuration setting is used to encrypt/decrypt signature files (internal to the module only). This function is considered obfuscation and cannot be used to compromise the module or store/transmit sensitive information.

[10] Note: Only validated firmware versions shall be loaded using the firmware upload service.

[11] MD5 (no security claimed) and keys derived from the non-conformant PBKDF are always encapsulated by the IPsec VPN service.

- Self-test Initiation – power cycle

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.

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.

All services implemented by the Module are listed in the table(s) below.

Table 14 – Authenticated Services

Service	**Description**	**CO**	**U**
Status Information	Viewing Logs, viewing network interface settings	X	X
Configuration management	Setting up VPN, setup filters, upload firmware, Auth directory configuration, creating user accounts	X	
Session Management	Audit configuration, Certificate management, DHCP setup	X	
Zeroize	Destroys all CSPs. Upon system all CSP in transient memory are erased	X	X
TLS	TLS used for HTTPS management of the module/ network traffic over TLS	X	
IPsec VPN	Module can configure/run traffic over IPsec VPN using certificates	X	

Table 15 – Unauthenticated Services

Service	**Description**
Module Reset	Reset the Module by activating the reset switch
NoAuth Function	Authenticates the operator and establishes secure channel.
Show Status	LCD Display available on only SM Series
Self-test Initiation	Power Cycle

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 20 can be utilized.

Table 16 defines the relationship between access to Security Parameters and the different module services. Table 17 defines the relationship between access to Public Keys and the different module services.

The modes of access shown in the tables are defined as:

- G = Generate: The module generates the CSP.
- I = Import: The CSP is entered into the module from an external source.
- R = Read: The module reads the CSP for output.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP to persistent storage.
- Z = Zeroize: The module zeroizes the CSP.

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

Table 16 – Security Parameters Access Rights within Services and CSPs

			CSPs																	
Service	**IKE Shared Secret**	**SKEYID**	**SKEYID_d**	**SKEYID_a**	**SKEYID_e**	**Preshared Key**	**IKE Session Encryption Key**	**IKE Session Authentication Key**	**IKE Private Key**	**IPsec Session Encryption Key**	**IPsec Session Authentication Key**	**TLS Master Secret**	**TLS Premaster Secret**	**TLS Session Key**	**TLS Integrity Key**	**DH/EC DH Private Key**	**DRBG V and C values**	**RADIUS Shared Secret**	**Entropy Input**	**Passwords**
Show Status	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Show Non-critical Configuration	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Monitor Network Status	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Log On	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		E
Log Off	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Clear Log	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Export Log	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Import/Export Certificates	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Filter Log	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-

Service			CSPs																
	IKE Shared Secret	SKEYID	SKEYID_d	SKEYID_a	SKEYID_e	Preshared Key	IKE Session Encryption Key	IKE Session Authentication Key	IKE Private Key	IPsec Session Encryption Key	IPsec Session Authentication Key	TLS Master Secret	TLS Premaster Secret	TLS Session Key	TLS Integrity Key	DH/EC DH Private Key	DRBG V and C values	RADIUS Shared Secret	Entropy Input	Passwords
Setup DHCP Server[12]	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Generate Log Reports	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Configure VPN Settings	-	-	-	-	-	IE	-	-	IG	-	-	-	-	-	-	IG	-	-		-
IPsec VPN	GE	GE	GE	GE	GE	-	GE	GE	GE	GE	GE	-	-	-	-	GE	GE	GE		-
TLS	-	-	-	-	-		-	-	-	-	-	GE	GE	GE	GE	-	-	-		-
Set Content Filter	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Upload Firmware	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Configure DNS Settings	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		-
Configure Access	-	-	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-		IE
Zeroize	Z	Z	Z	Z	Z	z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z		Z

[12] DHCP setup does not use CSPs, but DHCP server setup is performed with IPsec active. See below for IPsec VPN CSP usage.

Table 17 – Security Parameters Access Rights within Services and Public Keys

	Public Keys							
Service	**Root CA Public Key**	**IKE Public Key**	**TLS Public Key**	**Peer IKE Public Key**	**TLS Peer Public Key**	**Authentication Public Key**	**Firmware Verification Key**	**TLS Public Key**
Show Status	-	-	-	-	-	-	-	-
Show Non-critical Configuration	-	-	-	-	-	-	-	-
Monitor Network Status	-	-	-	-	-	-	-	-
Log On	-	-	-	-	-	-	-	-
Log Off	-	-	-	-	-	-	-	-
Clear Log	-	-	-	-	-	-	-	-
Export Log	-	-	-	-	-	-	-	-
Import/Export Certificates	-	-	-	-	-	-	-	-
Filter Log	-	-	-	-	-	-	-	-
Setup DHCP Server[13]	-	-	-	-	-	-	-	-
Generate Log Reports	-	-	-	-	-	-	-	-
Configure VPN Settings	I	IG	IG	-	-	-	-	-
IPsec VPN	E	E	E	IE	IE	IE	-	-
TLS	-	-	E	-	IE	IE	-	E
Set Content Filter	-	-	-	-	-	-	-	-

[13] DHCP setup does not use CSPs, but DHCP server setup is performed with IPsec active. See below for IPsec VPN CSP usage.

Upload Firmware	-	-	-	-	-	-	E	-
Configure DNS Settings	-	-	-	-	-	-	-	-
Configure Access	-	-	-	-	-	-	-	-
Zeroize	-	-	-	-	-	-	-	-

4. Self-tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand by power cycling the module.

The module performs the following algorithm KATs on power-up.

- Firmware Integrity: 16 bit CRC performed over all code in EEPROM
- AES: KATs: Encryption, Decryption; Modes: ECB, GCM; Key sizes: 128 bits
- DRBG: KATs: HASH DRBG; Security Strengths: 256 bits
- ECDSA: PCT: Signature Generation, Signature Verification; Curves/Key sizes: P-256
- HMAC: KATs: Generation, Verification; SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512
- RSA: KATs: Signature Generation, Signature Verification; Key sizes: 1024, 2048, 3072 bits
- SHA: KATs: SHA-1, SHA-256, SHA-384, SHA-512
- TDES: KATs: Encryption, Decryption; Modes: CBC; Key sizes: 2-key, 3-key[14]
- AES-CBC Ciphertext Stealing (CS): KATs: Encryption, Decryption; Modes: CBC-CS1; Key sizes: 128, 192, 256 bits
- DSA: KATs: Signature Generation, Signature Verification; Key sizes: 1024, 2048, 3072bits
- KDFs: IKEv1, IKEv2, TLS, SSH, SNMP[15]

The module performs the following conditional self-tests as indicated.

- DRBG and NDRNG Continuous Random Number Generator Tests per IG 9.8
- RSA Pairwise Consistency Test on RSA key pair generation
- ECDSA Pairwise Consistency Test on ECDSA key pair generation
- Firmware Load Test: 2048-bit ECDSA signed SHA-256 hash

When a new firmware image is loaded, the cryptographic module verifies the 2048-bit ECDSA signed SHA-256 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

[14] Triple-DES KATs are performed even if they are not supported in the Approved mode of operation

[15] The SSH and SNMP KDF KATs are performed if they are not supported in the Approved mode of operation

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.

The module performs the following critical self-tests. These critical function tests are performed for the SP 800-90A DRBG:

- SP 800-90A Instantiation Test
- SP 800-90A Generate Test
- SP 800-90A Reseed Test
- SP 800-90A Uninstantiate Test

5. Physical Security Policy

The chassis of the TZ series modules are sealed with one (1) tamper-evident seal, applied during manufacturing. The chassis of the rest of the modules are sealed with two (2) tamper-evident seals, applied during manufacturing. The physical security of the module is intact if there is no evidence of tampering with the seal. The locations of the tamper-evident seals are indicated by the red rectangles below in Figures 14-22. 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.

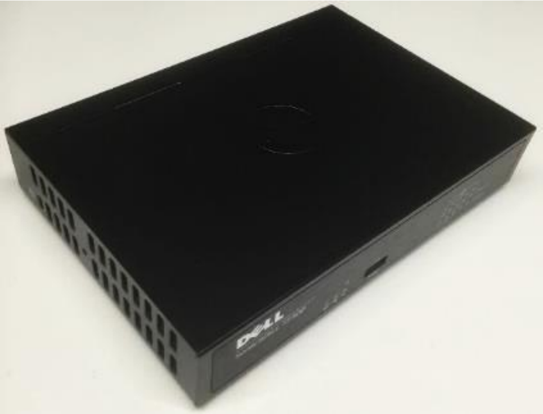


Figure 10: TZ 300 (Top, Left)

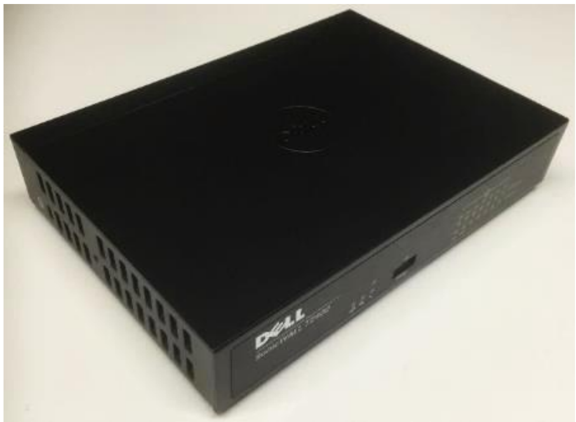


Figure 11: TZ 400 (Top, Left)

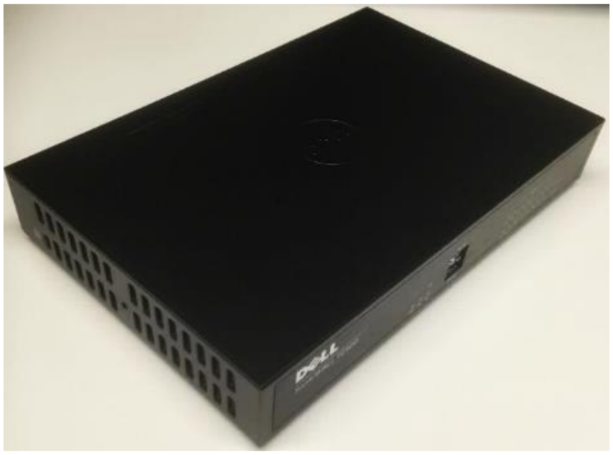


Figure 12: TZ 500 (Top, Left)

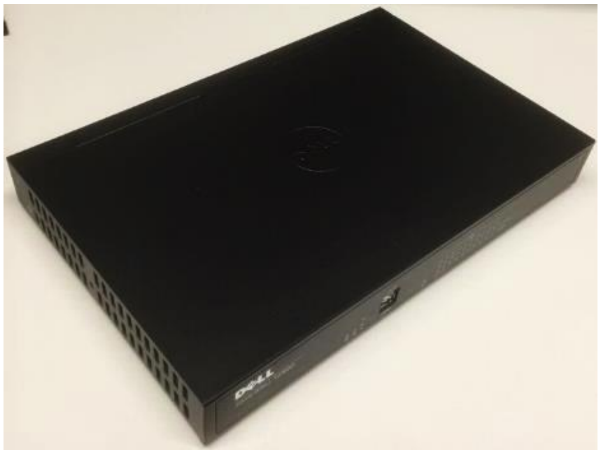


Figure 13: TZ 600 (Top, Left)

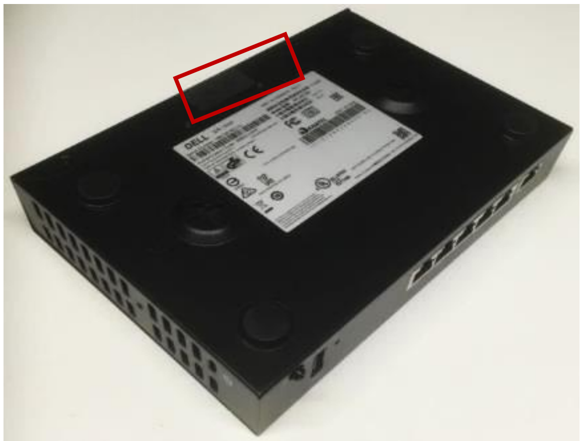


Figure 14: TZ 300 Right, Bottom View

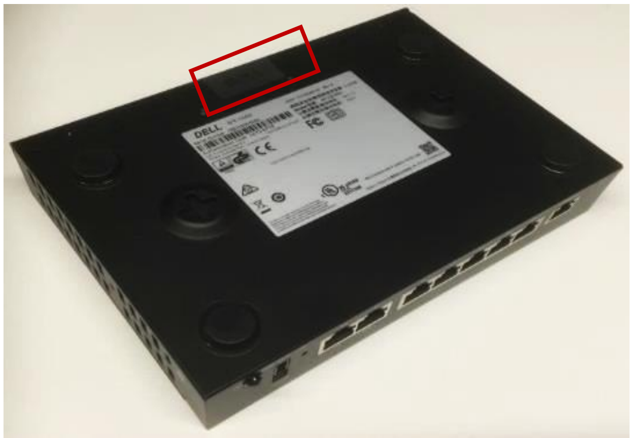


Figure 15: TZ 400 Right, Bottom View

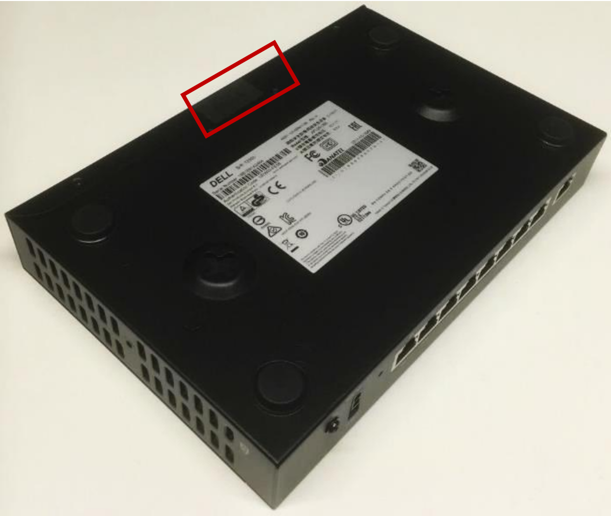


Figure 16: TZ 500 Right, Bottom, View

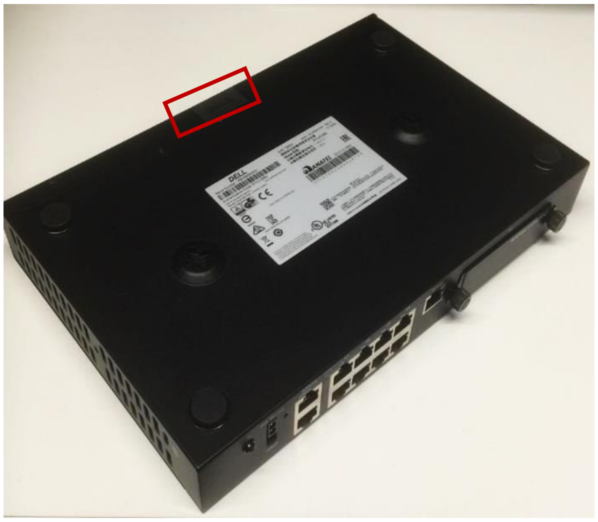


Figure 17: TZ 600 Right, Bottom View

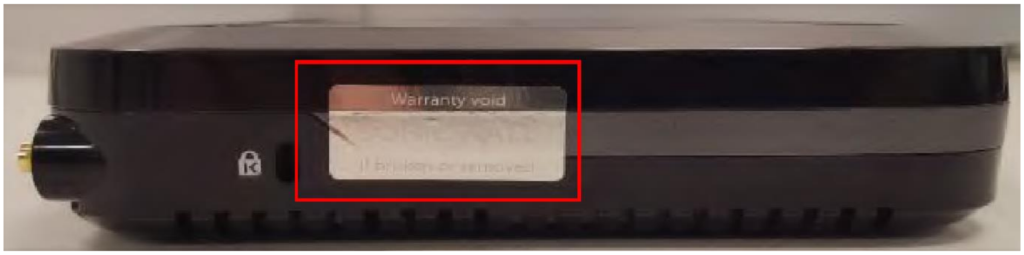


Figure 18: SOHOW (Left)

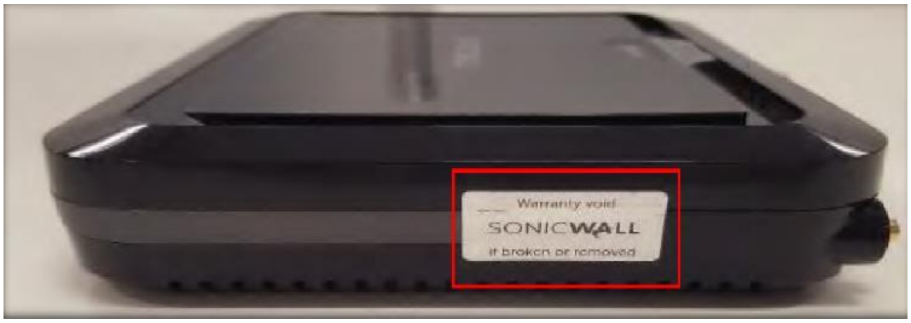
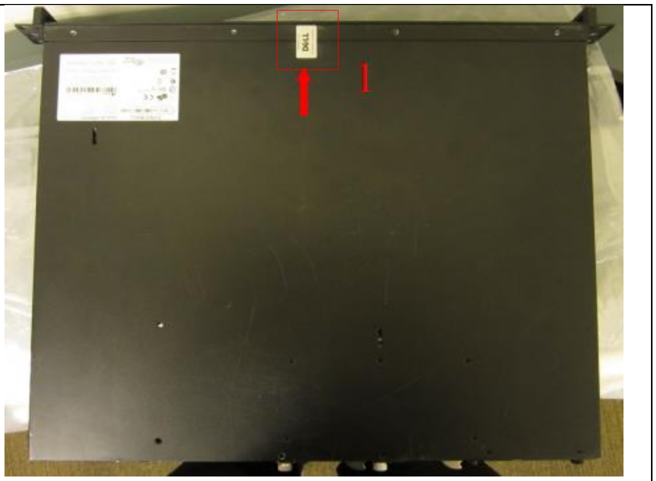
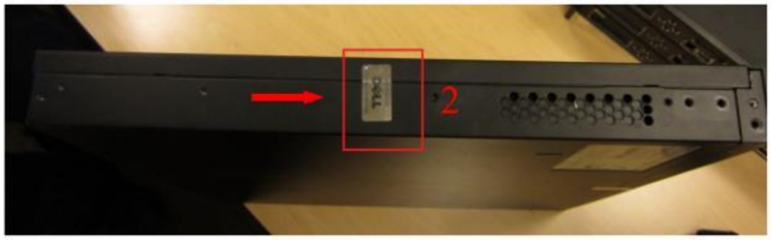


Figure 19: SOHOW (Right)

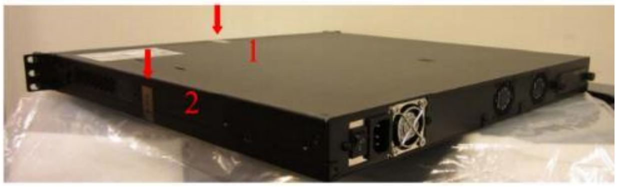
NS$_a$ 6600 Front



NS$_a$ 6600 Tamper Seal Location on underside, Front

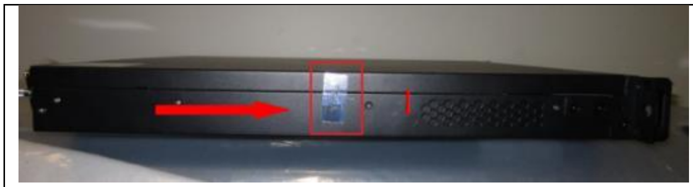


NS$_a$ 6600 Tamper-Evident Seal Location on Left Side

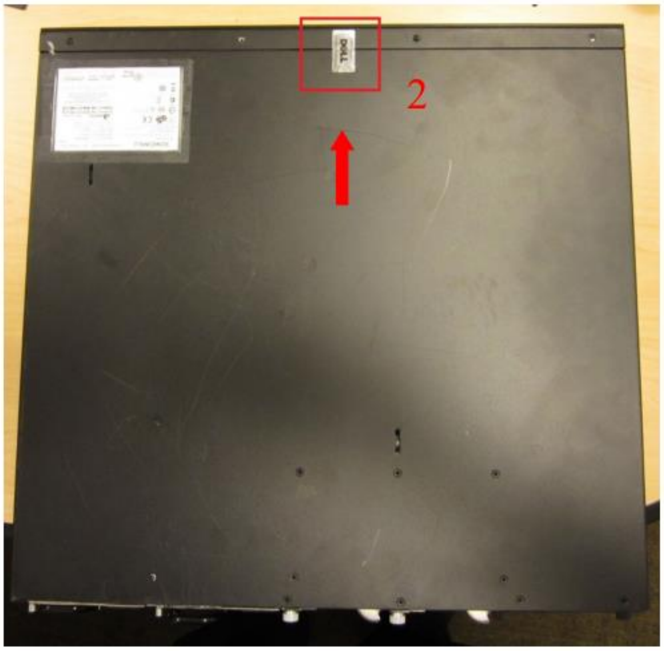


NS$_a$ 3600, NS$_a$ 4600, NS$_a$ 5600 Rear with Two Seals

Figure 20: NS$_a$ 6600, NS$_a$ 5600, NS$_a$ 4600, NS$_a$ 3600 Front and Back Seals



Super Massive with Tamper-Evident Seal on Left



Super Massive with Seal on underside, Front

Figure 21: SM 9600, SM 9400, SM 9200

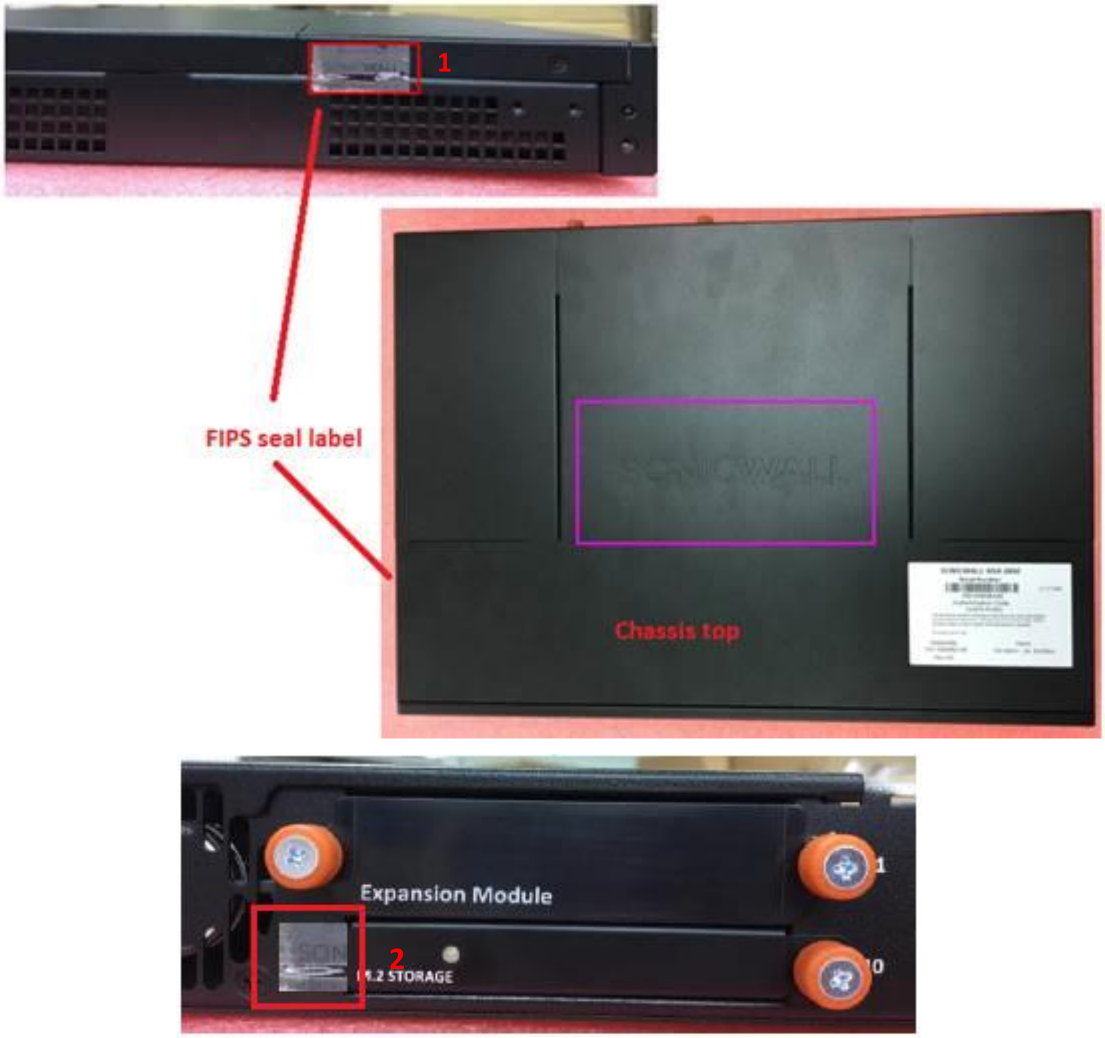


Figure 22: NS$_a$ 2650, NS$_a$ 3650, NS$_a$ 4650, NS$_a$ 5650 Tamper Evident Seal placement

6. 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 ECDSA signed by SonicWall, Inc.

7. Mitigation of Other Attacks Policy

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.

8. Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-2.

1. The module provides two distinct operator roles: User and Cryptographic Officer.
2. The module provides identity-based authentication.
3. The module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The module allows the operator to initiate power-up self-tests by power cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output are inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support a maintenance interface or role.
11. The module does not support manual key entry.
12. The module does not have any proprietary external input/output devices used for entry/output of data.
13. The module does not enter or output plaintext CSPs.
14. The module does not output intermediate key values.

9. References and Definitions

The following standards are referred to in this Security Policy.

Table 18 – References

Abbreviation	**Full Specification Name**
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, *January 2011*
[132]	*NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[186-2]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 2000.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[202]	*FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202, August 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*

Abbreviation	Full Specification Name
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[56A]	*NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised), March 2007*
[56Ar2]	*NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013*
[56Br1]	*NIST Special Publication 800-56A Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, September 2014*
[67]	*National Institute of Standards and Technology, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*

Table 19 – Acronyms and Definitions

Acronym	Definition
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

Acronym	Definition
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