FIPS 140-2 Non-Proprietary Security Policy for WatchGuard Firebox

M200, M300
M400, M500
M440
M4600, M5600

Version: 1.12
Mar 9, 2017

WatchGuard Firebox FIPS 140-2 Non-Proprietary Security Policy

Hardware:
Firebox M200, M300 (hardware model # ML3AE8)
Firebox M440 (hardware model # SL1AE24)
Firebox M400, M500 (hardware model # KL5AE8)
Firebox M4600 (hardware model # CL4AE24 with NIC modules WG8583 and WG8584, and with power supply WG8597)
Firebox M5600 (hardware model # CL5AE32 with NIC modules WG8583, WG8584, WG8585, and WG8022, and with power supply WG8598)

Firmware Version:
Fireware OS v11.11.2

Trademarks
WatchGuard
Firebox
Fireware

Regulatory compliance
FCC Class A Part 15

Contents

Introduction

This document is a FIPS 140-2 Security Policy for WatchGuard's Firebox Security System. This policy describes how the Firebox M200, M300, M400, M500, M440, M4600 and M5600 models (hereafter referred to as the 'module' or the 'Firebox module') meets the FIPS 140-2 security requirements and how to operate the module in a FIPS compliant manner.

This policy was created as part of the Level 2 FIPS 140-2 validation of the Firebox module.

The Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules* (FIPS 140-2) details the United States Federal Government requirements for cryptographic modules. Detailed information about the FIPS 140-2 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at http://csrc.nist.gov/groups/STM/cmvp/index.html.

Firebox Module Overview

WatchGuard® Firebox appliances are built for enterprise-grade performance with blazing throughput and numerous connectivity options. Advanced networking features include clustering, high availability (active/active), VLAN support, multi-WAN load balancing and enhanced VoIP security, plus inbound and outbound HTTPS inspection, to give the strong security enterprises need. And the Firebox appliances are completely configurable – turn on or off components and services to fit different network security deployment requirements.

WatchGuard's Firebox product family spans the full range of network environments, from SOHO to service provider, offering cost effective systems for any size of application. They detect and eliminate the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, inappropriate Web content and more in real time — without degrading network performance. The Firebox module delivers a full range of application level firewall and network-level services — application control, data loss prevention, advanced persistent threats blocker, VPN, intrusion prevention, web filtering, antivirus, antispam and traffic shaping — in dedicated, easily managed platforms.

The Firebox security system employs the powerful, secure, Fireware OS to achieve breakthrough price/performance. This system provides a critical layer of real-time, network-based antivirus protection that complements host-based antivirus software and supports "defense-in-depth" strategies without compromising performance or cost. They can be easily configured to provide antivirus protection, antispam protection and content filtering in conjunction with existing firewall, VPN, and related devices, or as complete network protection systems.

The Firebox module supports the IPSec industry standard for VPN, allowing VPNs to be configured between a Firebox module and any client or gateway/firewall that supports IPSec VPN. The Firebox module also provides SSLVPN services.

The Firebox module is defined as a multi-chip standalone cryptographic module consisting of production grade components contained in a physically protected enclosure. The entire enclosure is defined as the

cryptographic boundary of the cryptographic module. The cryptographic boundary for FIPS 140-2 certification is equivalent to the TOE boundary for Common Criteria (CC) certification.

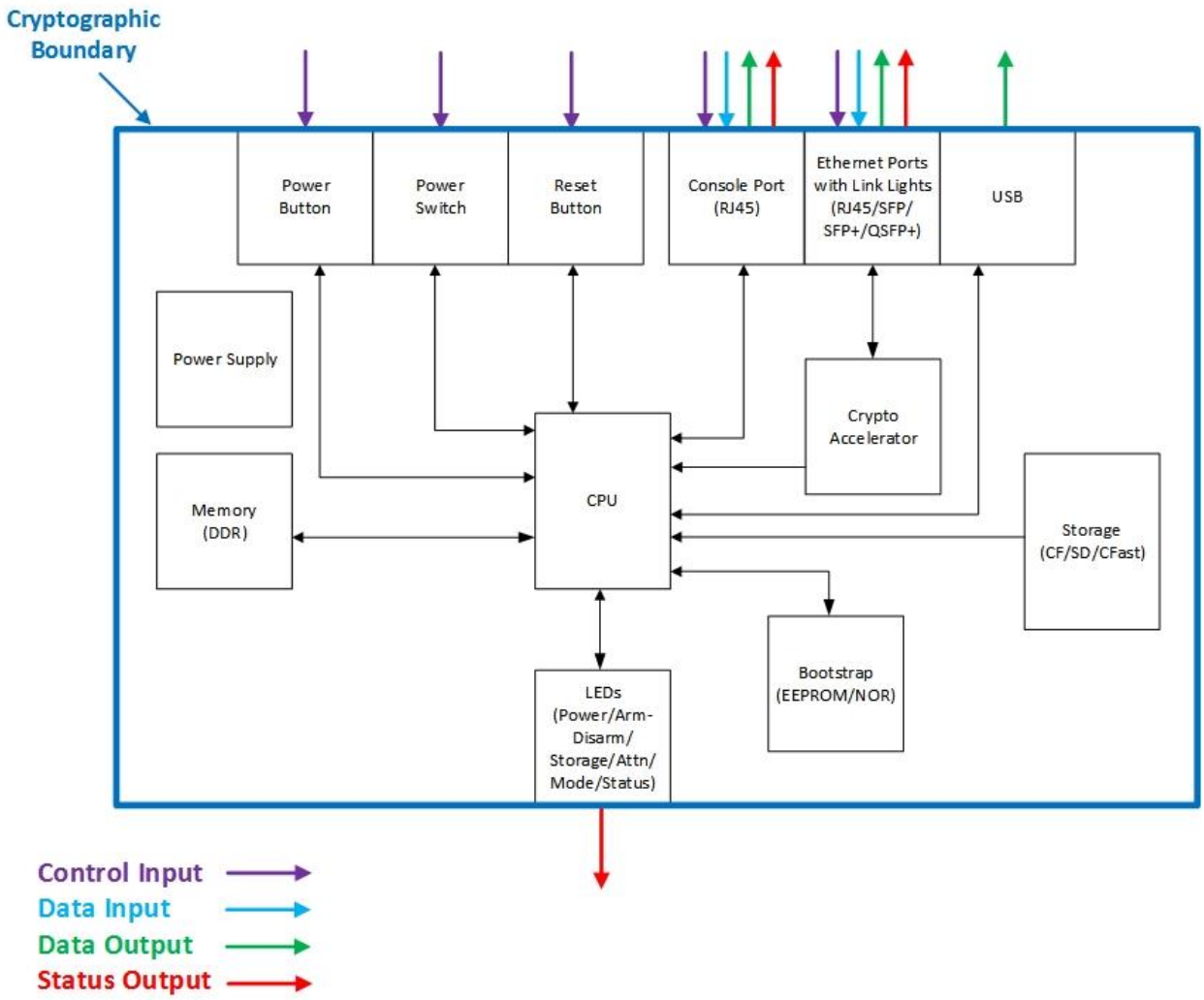


Figure 1: Cryptographic Module Block Diagram

Security Level

The WatchGuard Firebox appliances meet the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	2
Cryptographic Module Ports Specification	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	2

Roles, Services and Authentication

Module Access Methods

There are two convenient and secure ways to connect, configure and manage the module.

Web UI

The Firebox module provides a web based GUI based access to the module, which is the convenient way to configure the module. The Web UI requires a web browser on the management computer and an Ethernet connection between the module and the management computer.

A web-browser that supports Transport Layer Security (TLS) 1.2 is required for remote access to the Web UI when the modules are operating in FIPS mode.

The web browser is not part of the validated module boundary.

Command Line Interface

The Command Line Interface (CLI) is a rich, text based management tool for the module. The CLI provides access to all of the possible services and configuration options in the modules. The CLI uses a console or a network (Ethernet) connection between the module and the management computer. The console connection is a direct serial connection. Terminal emulation software is required on the management computer using either method. For network access, a Telnet or SSH client that supports the SSH v2.0 protocol is required. SSH v1.0 is not supported in FIPS mode.

The Telnet or SSH client is not part of the validated module boundary.

Roles

The module provides two pre-defined roles for users: User (status) and Cryptographic Officer (admin) role. One of these roles can be assumed by an operator after authenticating to the module remotely or through a console connection using a username/password combination. The module does not allow the creation of additional operator accounts or roles.

An operator assuming the Cryptographic Officer role has full read/write access to all of the functions and services of the module, including configuration, resetting or shutting down the module. This also implies that the Cryptographic Officer role includes all the accesses and privileges the User has.

The User is not allowed to make any changes to the configuration of the module. The User role is only for viewing and reporting the configuration and status of the module and its functions.

Operator accounts are differentiated by the username during authentication. More than one operator with User role can be connected to the module at any given time. However, there can be only one Cryptographic Officer login at any given time. Concurrent login attempts by the Cryptographic Officer are refused by the module.

It is not possible to change roles without re-authentication.

Services

The following table details the FIPS approved services available for each role, the types of access for each role, and the Keys or CSPs they affect. The role names are abbreviated as follows:
Cryptographic Officer - CO
User - U

R=Read Access, W=Write/ Delete Access, X=Execute Access

The Key/CSP is documented in section "Cryptographic Key Management" on page 57.

Table 2: FIPS approved services in Command Line Interface and Web UI access mode

Service	U	CO	Key/ CSP
authenticate to module	X	X	2, 3, 4, 5, 6, 7, 14, 15, 16, 17, 18, 19, 20, 21, 24, 25, 29, 30, 31, 32, 33, 34
show system status	R	R	16, 17, 19, 20
show FIPS mode enabled/disabled	R	R	16, 17, 19, 20
enable FIPS mode	N/A	W	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35
disable FIPS mode	N/A	W	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35
execute FIPS on-demand self-tests	N/A	X	2, 3, 16, 17, 19, 20, 26
set/reset password	N/A	WX	16, 17, 19, 20, 24
execute firmware download	N/A	X	16, 17, 19, 20, 25
execute system reboot	N/A	X	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35
execute system shutdown	N/A	X	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35
change system time	N/A	WX	16, 17, 19, 20
read/modify system/network configuration	R	RWX	16, 17, 19, 20
read/modify firewall policies.	R	RWX	16, 17, 19, 20
read/modify Gateway AV configuration	R	RWX	16, 17, 19, 20
read/modify spamBlocker configuration	R	RWX	16, 17, 19, 20
read/ modify WebBlocker configuration	R	RWX	16, 17, 19, 20
read/ modify VPN configuration	R	RWX	2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 28, 31, 32
read/modify IPS configuration	R	RWX	16, 17, 19, 20

read/ modify logging configuration	R	RWX	16, 17, 19, 20, 27
read log data	R	R	16, 17, 19, 20
manual Gateway AV/IPS signature update	N/A	RX	16, 17, 19, 20
restore factory default	N/A	W	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35

Approved Algorithms

The cryptographic module implements the following FIPS approved algorithms:

- Hardware:
  - Triple-DES
  - AES
  - SHS
  - HMAC

Table 3: FIPS approved algorithms for hardware

Algorithm	FIPS Validation Certificate Number
Triple-DES **TCBC**(KO 1 e/d)	2049, 2050, 2051, 2055, 2056
AES **CBC** (e/d; 128 , 192 , 256)	3670, 3671, 3672, 3676, 3677
SHS **SHA-1** (BYTE-only)	3085, 3086, 3087, 3091, 3092
HMAC **HMAC-SHA1** (**Key Sizes Ranges Tested**:KS<BS)	2417, 2418, 2419, 2423, 2424

Note: The algorithms listed above are implemented by the module when operating in a FIPS approved mode of operation. The certificates list additional modes and key sizes that are not accessible through the cryptographic module interfaces.

- Firmware:
  - Triple-DES
  - AES
  - SHS
  - HMAC
  - RSA
  - DRBG
  - IKEv1 KDF
  - TLS KDF

- SSH KDF
- SNMP KDF

Table 4: FIPS approved algorithms for firmware

Algorithm	FIPS Validation Certificate Number
Triple-DES **TCBC**(KO 1 e/d)	2171
AES **CBC** (e/d; 128 , 192 , 256) **CTR** (ext only; 128 , 192 , 256)	3960
SHS **SHA-1** (BYTE-only) **SHA-224** (BYTE-only) **SHA-256** (BYTE-only) **SHA-384** (BYTE-only) **SHA-512** (BYTE-only)	3266
HMAC **HMAC-SHA1** (**Key Sizes Ranges Tested**:KS<BS KS=BS KS>BS) **HMAC-SHA224** (**Key Sizes Ranges Tested**:KS<BS KS=BS KS>BS) **HMAC-SHA256** (**Key Sizes Ranges Tested**:KS<BS KS=BS KS>BS) **HMAC-SHA384** (**Key Sizes Ranges Tested**:KS<BS KS=BS KS>BS) **HMAC-SHA512** (**Key Sizes Ranges Tested**:KS<BS KS=BS KS>BS)	2580
RSA **FIPS186-2**: **ALG[ANSIX9.31]**: SIG(ver); 1024 , 1536 , 2048 , 3072 , 4096 , SHS: SHA-1 **ALG[RSASSA-PKCS1_V1_5]**: SIG(ver): 1024 , 1536 , 2048 , 3072 , 4096 , SHS: SHA-1 **FIPS186-4**: **186-4KEY(gen)**: FIPS186-4_Fixed_e (10001) ; **PGM**(**ProbRandom**: (2048 , 3072) **PPTT**:(C.2) **ALG[ANSIX9.31]** Sig(Gen): (2048 SHA(224 , 256 , 384 , 512)) (3072 SHA(224 , 256 , 384 , 512)) Sig(Ver): (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) **ALG[RSASSA-PKCS1_V1_5]** SIG(gen) (2048 SHA(224 , 256 , 384 , 512)) (3072 SHA(224 , 256 , 384 , 512))	2023

SIG(Ver) (1024 SHA(1 , 224 , 256 , 384 , 512)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) SHA DRBG	
DRBG **CTR_DRBG**: [Prediction Resistance Tested: Enabled and Not Enabled; BlockCipher_No_df: (AES-128 , AES-192 , AES-256) (AES)]	1160
CVL (IKEv1, TLS, SSH, SNMP) **IKEv1**(AUTH(PSK)) (256 (SHA 1 , 256 , 384 , 512)) (3072 (SHA 1 , 256 , 384 , 512)) (2048 (SHA 1 , 256 , 384 , 512)) SHA HMAC **TLS**(TLS1.2 (SHA 256 , 384)) SHA HMAC **SSH** (SHA 1) SHA **SNMP** SHA1	793

Note: The algorithms listed above are implemented by the module when operating in a FIPS approved mode of operation. The certificates list additional modes and key sizes that are not accessible through the cryptographic module interfaces.

The IKEv1, TLS, SSH, and SNMP protocols have not been tested by the CMVP or CAVP.

The minimum encryption strength of symmetric keys is 112 bits and the maximum is 256 bits.

Non-FIPS Approved But Allowed Algorithms

The cryptographic module implements the following non-FIPS approved but allowed algorithms:

- RSA key transport (with 2048 bit keys)
  - Key wrapping, key establishment methodology provides 112 bits of equivalent encryption strength
- Diffie Hellman
  - Key establishment, key agreement method provides 112 bits or 128 bits of equivalent encryption strength
- EC Diffie-Hellman
  - Key agreement, key establishment methodology provides 128 or 192 bits of equivalent encryption strength
- NDRNG

Non-FIPS Approved Services

The cryptographic module provides the following non-FIPS approved services:

- Mobile VPN with PPTP
- PPPoE
- Backup image to USB
- Authenticate to module*
- Read/modify VPN configuration*

* When used with a non-compliant Diffie-Hellman key size.

If any of these services are used, the cryptographic module is not operating in a FIPS approved mode of operation.

Non-FIPS Approved Algorithms

The cryptographic module implements the following non-FIPS approved algorithms:

- DES
- MD5
- TKIP
- The AES algorithm is non-compliant when used in CCM mode or when invoking the non-FIPS Approved "Backup image to USB" service
- RSA signature generation with SHA-1
- Use of HMAC-SHA-1 for MAC generation with key length >= 80 bits and < 112, and use of HMAC-SHA-1 for MAC verification with key length >= 80 bits and < 112 bits
- Use of SHA-1 for digital signature generation
- Password Based Key Derivation Function (for 128 bit AES key). Keys derived using a PBKDF cannot be used in a FIPS approved mode of operation
- Diffie Hellman
  - Key establishment, key agreement method is non-compliant when using key sizes with less than 112 bits of equivalent encryption strength

Alternating Bypass

The primary cryptographic function of the module is to act as a firewall, and as a VPN device. Encrypt and decrypt operations are performed on traffic based on firewall policies. The cryptographic module implements an alternating bypass feature based on VPN tunnels and firewall policies. Traffic can be encrypted/decrypted or passed as plaintext, depending on the VPN tunnel and selected policy.

Two actions must be taken by the Cryptographic Officer to transition between VPN bypass states. The Cryptographic Officer must first create the VPN gateway. The Cryptographic Officer must then create the VPN tunnel and tunnel route, and associate the VPN tunnel with a VPN policy.

Whether VPN bypass is enabled or not can be determined by examining the list of VPN gateways and VPN tunnels.

Authentication

Cryptographic Officer or User (referred to as Operator) must authenticate with a username and password combination to access the modules remotely or locally via the console. Remote operator authentication is done over HTTPS (TLS 1.2) or SSH (v2.0). The access to the module is based on firewall policy and authentication by IP address.

For end users (including CO or U) using module functionality and invoking the SSLVPN or IPSec encrypt/decrypt services, the module supports authentication with a username/password combination. The authentication is done over HTTPS over a dedicated port and it does not allow access to the module for any of the administrative purposes whatsoever.

The minimum password length is 8 characters when in FIPS mode. Using a strong password policy, where operator and end user passwords are at least 8 characters in length and use a mix of alphanumeric (printable) characters from the ASCII character set, the odds of guessing a password are 1 in 94^8 , which is far less than 1 in 1,000,000. The total password space is sufficiently large such that exceeding a 1 in 100,000 probability of correctly guessing the password in one minute would require approximately 6.1 x 10^{10} attempts per minute, which is beyond the operational capability of the module.

For end users invoking the IPSec encrypt/decrypt services, the module acts on behalf of the end user and negotiates a VPN connection with a remote module. The strength of authentication for IPSec services is based on the authentication method defined in the specific firewall policy: IKE pre-shared key or IKE RSA key (RSA certificate). The odds of guessing the authentication key for each IPSec method is:

- 1 in 94^8 for the IKE preshared key (based on an 8 character, ASCII printable key)
- 1 in 2^{112} for the IKE RSA key (based on a 2048 bit RSA key size, which is equivalent to 112 bits of security)

Therefore the minimum odds of guessing the authentication key for IPSec is 1 in 94^8 based on the IKE preshared key, or 1 in 2^{112} based on the IKE RSA key, which is far less than 1 in 1,000,000. The key size is sufficiently large such that exceeding a 1 in 100,000 probability of correctly guessing the key in one minute would require approximately 6.1 x 10^{10} attempts per minute (for preshared key) or 5.2 x 10^{28} attempts per minute (for RSA key) , which is beyond the operational capability of the module.

Interfaces

Physical ports and interfaces on the Firebox module can be categorized into the following logical interfaces:

- Data Input
- Data Output
- Control Input
- Status Output

All of the physical ports and interfaces are separated into the FIPS 140-2 logical interfaces, as described in the following tables. The logical interfaces may share a physical port. The firmware in the Firebox module separates and routes data to the appropriate internal firmware task associated with a logical interface based on port number, session, and/or command context.

Firebox M200 and Firebox M300

Figure 2: M200 and M300 Front View

Table 5: Front Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
RJ45 Ethernet Interfaces with link lights	8	Configurable ports can be data input or data output for External, LAN, or Optional. Link lights show connection speed and activity.	✓	✓	✓	✓
RJ45 Console Interface	1	Serial port for CLI access.	✓	✓	✓	✓
USB Interfaces	2	Used for backup, or to store a support snapshot.		✓		
Power LED	1	Lit green when the module is powered on.				✓
Arm/Disarm LED	1	This light is red after power-on or reboot. It turns green after successful module initialization.				✓
Storage LED	1	Lit yellow when there is activity on the SD card.				✓
Reset Button	1	Used to reset the module.			✓	

Figure 3: M200 and M300 Rear View

Table 6: Rear Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
Power Interface	1	Auto-sensing AC power supply.				
Power Switch	1	Controls power supplied to device.			✓	

Firebox M400 and Firebox M500

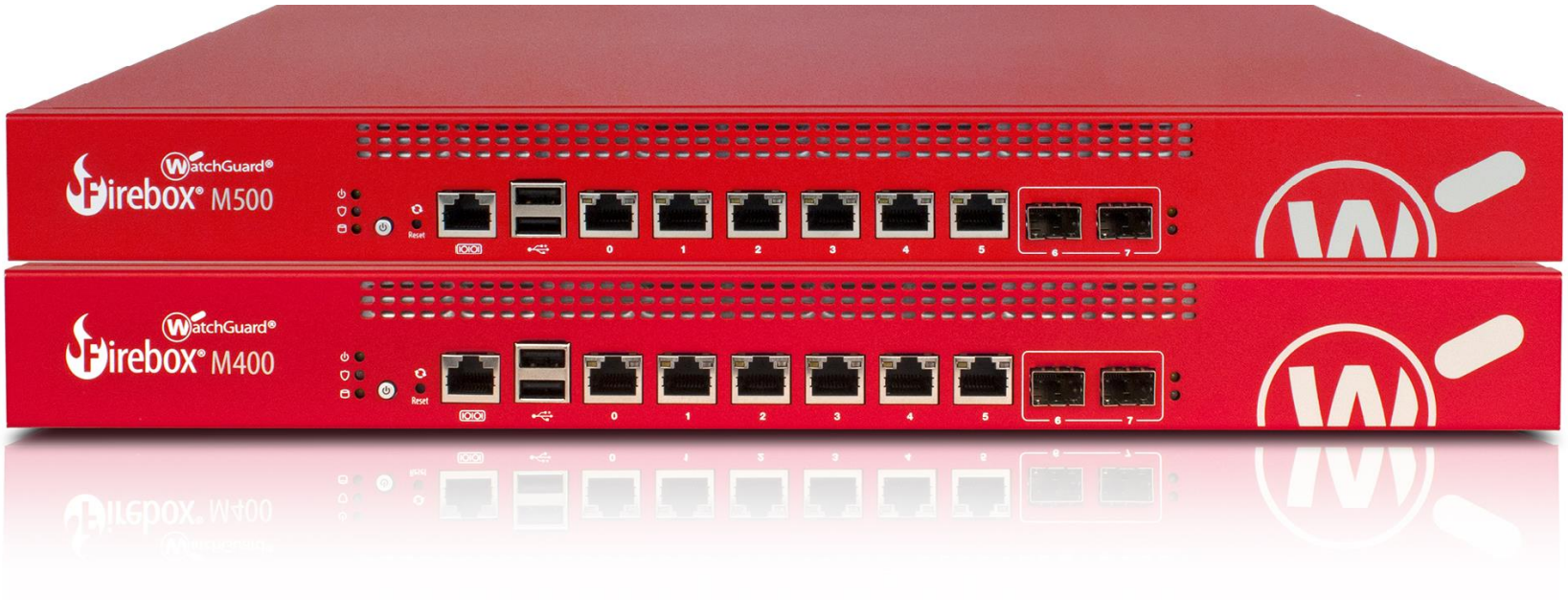


Figure 4: M400 and M500 Front View

Table 7: Front Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
RJ45 Ethernet Interfaces with link lights	6	Configurable ports can be data input or data output for External, LAN, or Optional. Link lights show connection speed and activity.	✓	✓	✓	✓
1 Gb SFP transceiver module	2	Configurable ports can be data input or data output for External, LAN, or Optional. Link lights show connection speed and activity.	✓	✓	✓	✓
RJ45 Console Interface	1	Serial port for CLI access.	✓	✓	✓	✓
USB Interfaces	2	Used for backup, or to store a support snapshot.		✓		
Power LED	1	Lit green when the module is powered on.				✓
Arm/Disarm LED	1	This light is red after power-on or reboot. It turns green after successful module initialization.				✓
Storage LED	1	Lit yellow when there is activity on the compact flash.				✓
Reset Button	1	Used to reset the module.			✓	
Power Button	1	Controls power supplied to device.			✓	

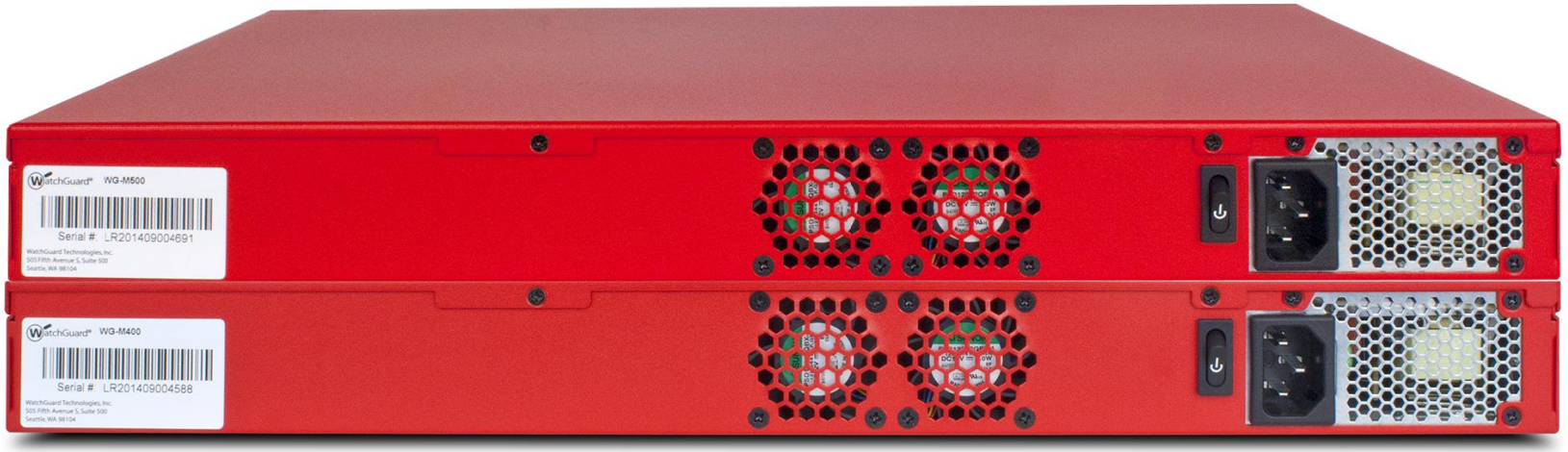


Figure 5: M400 and M500 Rear View

Table 8: Rear Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
Power Interface	1	Auto-sensing AC power supply.				
Power Switch	1	Controls power supplied to device.			✓	

Firebox M440

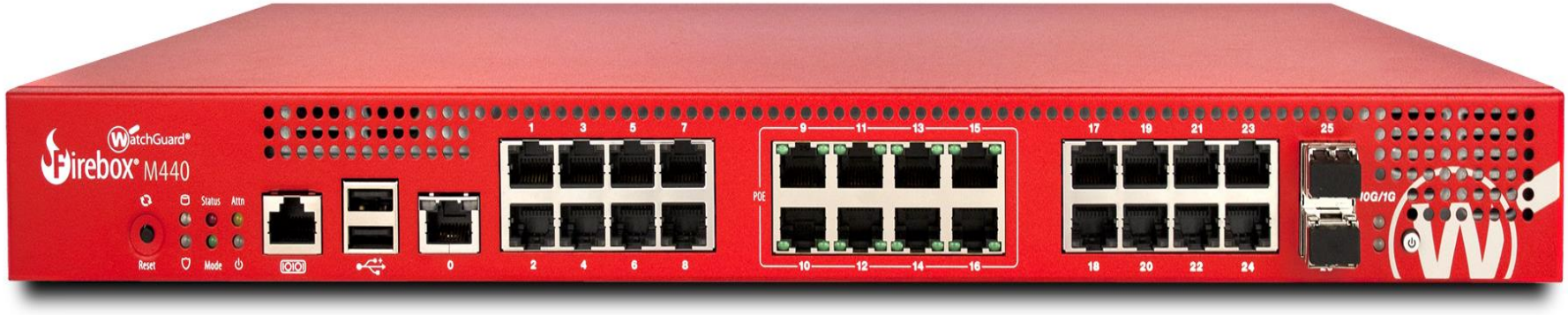


Figure 6: M440 Front View

Table 9: Front Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
RJ45 Ethernet Interfaces with link lights	25	Configurable ports can be data input or data output for External, LAN, or Optional. Link lights show connection speed and activity.	✓	✓	✓	✓
10 Gb SFP+ transceiver module	2	Configurable ports can be data input or data output for External, LAN, or Optional. Adjacent LEDs show connection speed and activity.	✓	✓	✓	✓
RJ45 Console Interface	1	Serial port for CLI access.	✓	✓	✓	✓
USB Interfaces	2	Used for backup, or to store a support snapshot.		✓		
Power LED	1	Lit green when the module is powered on.				✓
Attention indicator LED	1	The Attn indicator is yellow when you start the device with the Reset button pressed.				✓
Mode Indicator LED	1	The Mode indicator shows the status of the external network connection.				✓
Status indicator LED		The Status indicator shows when there is a management connection to the device.				✓
Arm/Disarm LED	1	This light is red after power-on or reboot. It turns green after successful module initialization.				✓

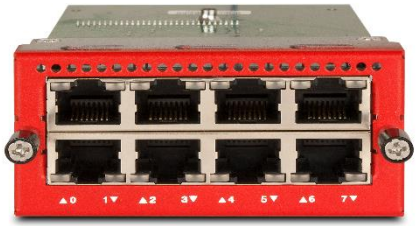
PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
Storage LED	1	Lit yellow when there is activity on the compact flash.				✓
Reset button	1	Used to reset the module.			✓	
Power Button	1	Controls power supplied to device.			✓	

Figure 7: M440 Rear View

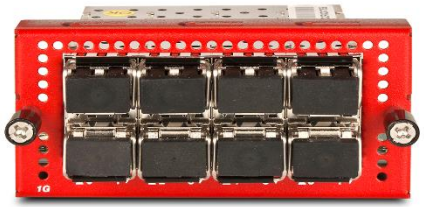
Table 10: Rear Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
Power Interface	1 (Optional second)	Auto-sensing AC power supply.				
Power Switch	1	Controls power supplied to device.			✓	

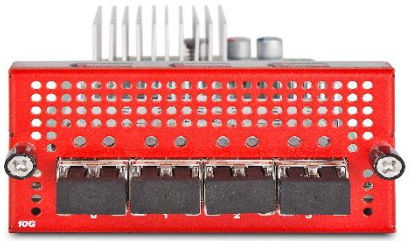
Firebox M4600



8 x 1 Gb Copper Module (WG8584)



8 x 1 Gb Fiber Module (WG8585)



4 x 10 Gb Fiber Module (WG8583)

2 x 40 Gb Fiber Module (WG8022)

Figure 8: M4600 Front View

Table 11: Front Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
Built In RJ45 Ethernet Interfaces with link lights	8	Configurable ports can be data input or data output for External, LAN, or Optional. Link lights show connection speed and activity.	✓	✓	✓	✓
Swappable Network Module Bays	2	Swapable NIC modules (8 x 1G RJ45, 8 x 1G SFP, 4 x 10G SFP+, and 2 x 40G QSFP+). Configurable ports can be data input or data output for External, LAN, or Optional. Link lights show connection speed and activity.	✓	✓	✓	✓
RJ45 Console Interface	1	Serial port for CLI access.	✓	✓	✓	✓
USB Interfaces	2	Used for backup, or to store a support snapshot.		✓		
Power LED	1	Lit green when the module is powered on.				✓
Arm/Disarm LED	1	This light is red after power-on or reboot. It turns green after successful module initialization.				✓
Storage LED	1	Lit yellow when there is activity on the CFast drive.				✓
Reset Button	1	Used to reset the module.			✓	
Power Button	1	Controls power supplied to device.			✓	

Figure 9: M4600 Rear View

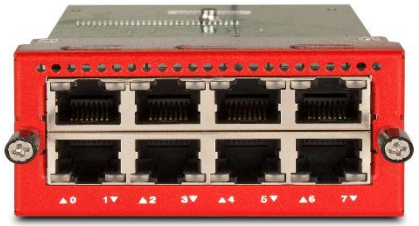
Table 12: Rear Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
Power Interface	2	Auto-sensing AC power supply.				
Power Switch	1	Controls power supplied to device.			✓	
Power Supply Alert Reset	1	Resets Power Supply Sensor			✓	

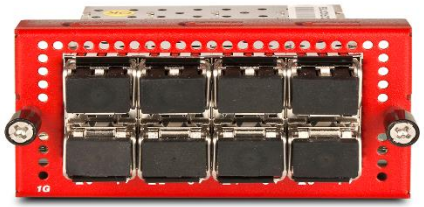
Table 13: M4600 Test Configuration

Model Number	Hardware Version	Optional NIC Modules	Module Tested with NIC Modules	Power Supply Part Number	Module Tested with One or Two Power Supplies:
Firebox M4600	CL4AE24	WG8022	WG8583	WG8597	Two
		WG8583	WG8584		
		WG8584			
		WG8585			

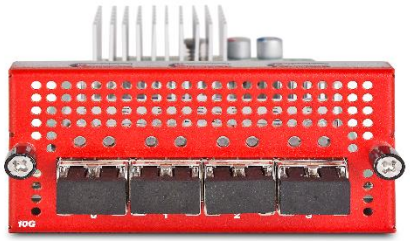
Firebox M5600



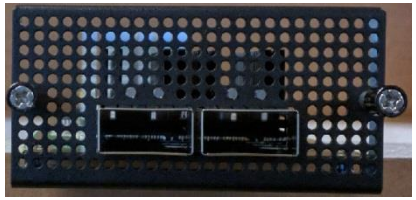
8 x 1 Gb Copper Module (WG8584)



8 x 1 Gb Fiber Module (WG8585)



4 x 10 Gb Fiber Module (WG8583)



2 x 40 Gb Fiber Module (WG8022)

Figure 10: M5600 Front View

Table 14: Front Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
Built In RJ45 Ethernet Interface with link lights	1	Configurable port can be data input or data output for External, LAN, or Optional. Link lights show connection speed and activity.	✓	✓	✓	✓
Swappable Network Module Bays	4	Swapable NIC modules (8 x 1G RJ45, 8 x 1G SFP, 4 x 10G SFP+, and 2 x 40G QSFP+). Configurable ports can be data input or data output for External, LAN, or Optional. Link lights show connection speed and activity.	✓	✓	✓	✓
RJ45 Console Interface	1	Serial port for CLI access.	✓	✓	✓	✓
USB Interfaces	2	Used for backup, or to store a support snapshot.		✓		
Power LED	1	Lit green when the module is powered on.				✓
Arm/Disarm LED	1	This light is red after power-on or reboot. It turns green after successful module initialization.				✓
Storage LED	1	Lit yellow when there is activity on the CFast drive.				✓
Reset Button	1	Used to reset the module.			✓	
Power Button	1	Controls power supplied to device.			✓	

Figure 11: M5600 Rear View

Table 15: Rear Panel Access

PORT NAME/TYPE	Number	Description	Data Input	Data Output	Control Input	Status Output
Power Interface	2	Auto-sensing AC power supply.				
Power Switch	1	Controls power supplied to device.			✓	
Power Supply Alert Reset	1	Resets Power Supply Sensor			✓	

Table 16: M5600 Test Configuration

Model Number	Hardware Version	Optional NIC Modules	Module Tested with NIC Modules	Power Supply Part Number	Module Tested with One or Two Power Supplies:
Firebox M5600	CL5AE32	WG8022	WG8022	WG8598	Two
		WG8583	WG8583		
		WG8584	WG8584		
		WG8585	WG8585		

FIPS 140-2 Compliant Operation

The Firebox module meets FIPS 140-2 Level 2 requirements. This section describes how to place and keep the Firebox module in a FIPS approved mode of operation.

Security Rules

The cryptographic module has the following security rules:

- The cryptographic module provides two distinct operator roles. These are the User role, and the Cryptographic Officer role.
- The cryptographic module provides role-based authentication relying upon usernames and passwords.
- The cryptographic module provides pre-shared key and RSA certificates for authentication when configuring VPN tunnels.

Self-Tests

- The cryptographic module performs the following self-tests at power-up:

  Hardware cryptographic algorithm tests:
  - Triple-DES encrypt KAT
  - Triple-DES decrypt KAT
  - AES encrypt KAT
  - AES decrypt KAT
  - SHA-1 KAT
  - HMAC-SHA-1 KAT

  Firmware cryptographic algorithm tests:
  - Triple-DES encrypt KAT
  - Triple-DES decrypt KAT
  - AES encrypt KAT
  - AES decrypt KAT
  - SHA-1 KAT
  - HMAC-SHA-1 KAT
  - HMAC-SHA-224 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - HMAC-SHA-512 KAT
  - RSA Sign KAT
  - RSA Verify KAT
  - DRBG KAT

Firmware integrity test:
- Firmware integrity test (using HMAC-SHA-1)

The results of the power-up self-tests are displayed on the console during the power-up sequence. The self-tests are run automatically at power-up without any operator intervention. The power-up self-tests are run before any networking interfaces are started, so that data output is inhibited while self-tests are running.

The power-up self-tests can also be initiated on demand by issuing the CLI command **fips selftest**.
1. Sample output (FIPS mode currently enabled):

```
The box will reboot, Please wait for a moment…
```

If any of the power-up tests fail, the cryptographic module enters the error state. Errors are displayed on the console. The following error indicator is displayed on the console: "FIPS self-test failure: shutting down". No security services are provided in the error state and data output is inhibited (the Firebox module is shutdown).

- The cryptographic module performs the following conditional tests:
  - RSA pairwise consistency test
  - DRBG continuous PRNG test
  - DRBG Instantiate, Reseed, Generate, and Uninstantiate health tests
  - Bypass test
  - Firmware load test (using HMAC-SHA-1)

  If the RSA pairwise consistency test, DRBG continuous PRNG test, or bypass test fails, the cryptographic module enters the error state. Errors are displayed on the console or internal logs. The following error indicator is displayed on the console: "FIPS self-test failure: shutting down". No security services are provided in the error state and data output is inhibited (the Firebox module is shutdown).

  If the firmware load test fails, the cryptographic module enters the firmware load test failure state. The firmware load error indicator has the following unique indicator: "Upload failure: -2 failed with -2". The new firmware image is not loaded. The Firebox module resumes normal operation after the error is logged.

Cryptographic Officer Guidance

This section describes the responsibilities of the Cryptographic Officer for installing, configuring, and ensuring proper operation of the validated Firebox module.

Secure Installation

The Cryptographic Officer must ensure that:
- The Firebox module is installed in a secure physical location.
- Physical access to the Firebox module is restricted to authorized personnel only.

Enabling FIPS Mode Operation

The cryptographic module is not configured to operate in FIPS mode by default. To operate in FIPS mode, do the following:

- Issue the CLI command **fips enable** to enable FIPS mode operation.
- Choose operator passwords (for Cryptographic Officer and User roles) with a minimum of 8 characters.
- Run **fips selftest** before making changes to the VPN configuration.
- SSLVPN tunnels use TLS 1.2. When configuring SSLVPN tunnels, only choose FIPS-approved authentication and encryption algorithms (SHA-1, SHA-256, SHA-512, Triple-DES, AES-128, AES-192, AES-256).
- When configuring IPSec VPN tunnels, only choose FIPS-approved authentication and encryption algorithms (SHA-1, SHA-256, SHA-384, SHA-512, Triple-DES, AES-128, AES-192, AES-256).
- When configuring IPSEc VPN tunnels, choose Diffie-Hellman Group 14 (2048 bit), Group 15 (3072 bit), Group 19 (256 bit elliptic curve), or Group 20 (384 bit elliptic curve) for IKE Phase 1 negotiation.
- When configuring IPSec VPN tunnels, use pre-shared keys or RSA certificates for authentication.
- Only use RSA certificates for TLS.
- Use a minimum of 2048-bits for all RSA keys.
- Do not use Mobile VPN with PPTP.
- Do not use PPPoE.
- Do not use WatchGuard System Manager to manage the appliance.
- Web browsers must be configured to only use TLS 1.2 and FIPS approved cipher suites.
- Telnet and SSH clients must be configured to use the SSH V2.0 protocol and RSA authentication. If the SSH client uses Diffie-Hellman key exchange, configure the client to use DH 2048 bit or greater.
- When using backup, the Cryptographic Officer must take possession of the USB device.
- Do not use the wireless interfaces.

Disabling FIPS Mode Operation

To disable FIPS mode, do the following:

- Issue the CLI command **restore factory-default all** (to disable FIPS mode and zeroize all keys and CSPs).

User Guidance

This section describes the responsibilities for Users of the validated Firebox module.

The User can determine if the cryptographic module is operating in FIPS mode by issuing the CLI command **show FIPS**.

1. Sample output (FIPS mode currently not enabled):

```
--
-- Current FIPS status
--
FIPS status : disabled
```

2. Sample output (FIPS mode currently enabled):

```
--
-- Current FIPS status
--
FIPS status : enabled
```

Tamper Evidence

All Critical Security Parameters are stored and protected within each appliance's tamper evident enclosure. Tamper evident labels must be applied for the module to operate in a FIPS approved mode of operation. It is the responsibility of the Cryptographic Office to properly place all tamper evident labels as described in this section, and the Cryptographic Officer should maintain control of unused labels in a secure location. The security labels recommended for FIPS 140-2 compliance are separately ordered (SKU WG8566). These security labels are designed to be very fragile and cannot be removed without visible signs of damage to the labels. Note that these labels are designed to be applied to a clean surface at 10°C or above.

The Cryptographic Officer must apply tamper evident labels at the locations shown in the Figures. Before the labels are applied, the Cryptographic Officer should ensure that the surface is clean, and that the air temperature is at 10°C or above. The surface should be cleaned using isopropyl alcohol and dried before applying the labels. After the labels are placed, the Cryptographic Officer should inspect the tamper evident labels periodically to verify they are intact.

If the tamper evident seals are found to be damaged or broken during inspection, the Cryptographic Officer can return the cryptographic module to a FIPS approved mode of operation by restoring the module to a factory default state, reinstalling, and applying new tamper evident labels.

Any attempt to open the device will damage the tamper evident seals or the material of the security appliance cover. Tamper evident seals can also be inspected for signs of tampering, which include the following: curled corners, rips, and slices.

The following is a photograph of the tamper evident labels that are used.

Figure 12: WatchGuard Firebox Tamper Evident Label

Firebox M200 and Firebox M300

One tamper evident label is required.

Figure 13: M200 Tamper Evident Label 1 Placement

Figure 14: M300 Tamper Evident Label 1 Placement

Firebox M400 and Firebox M500

One tamper evident label is required.

Figure 15: M400 Tamper Evident Label 1 Placement

Figure 16: M500 Tamper Evident Label 1 Placement

Firebox M440

Three tamper evident labels are required.

Figure 17: M440 Tamper Evident Label 1 Placement

Figure 18: M440 Tamper Evident Label 2 Placement

Figure 19: M440 Tamper Evident Label 3 Placement

Firebox M4600

Four tamper evident labels are required.

Figure 20: M4600 Tamper Evident Label 1 Placement

Figure 21: M4600 Tamper Evident Label 2 Placement

Figure 22: M4600 Tamper Evident Label 3/Label 4 Placement

Firebox M5600

Six tamper evident labels are required.

Figure 23: M5600 Tamper Evident Label 1 Placement

Figure 24: M5600 Tamper Evident Label 2 Placement

Figure 25: M5600 Tamper Evident Label 3/Label 4/Label5/Label 6 Placement

Cryptographic Key Management

Cryptographic Keys and Critical Security Parameters

The following table lists the cryptographic keys and Critical Security Parameters (CSPs) used by the cryptographic module:

Table 17: Cryptographic Keys and Critical Security Parameters

#	Key/CSP	Type/Size	Usage	Storage	Input	Output	Generation	Zeroization
1	DRBG seed	SP800-90A CTR_DRBG / 384 bits	Seed value for DRBG.	RAM (plain text)			Initial generation via entropy.[2]	Power off the appliance.
2	DRBG V	SP800-90A CTR_DRBG / 128 bits	Internal V value used by SP800-90A DRBG.	RAM (plain text)			Initial generation via DRBG.	Power off the appliance.
3	DRBG key	SP800-90A CTR_DRBG / 256 bits	Internal key value used by SP800-90A DRBG.	RAM (plain text)			Initial generation via DRBG.	Power off the appliance.
4	Diffie-Hellman shared secret	DH / 2048, 3072 bits	Shared secret used in Diffie-Hellman key exchange for IKE, TLS, and SSH sessions.	RAM (plain text)			Generated internally using Diffie-Hellman key exchange.	Terminate the session, or power off the appliance.
5	Diffie-Hellman private key	DH / 224, 256 bits	The private exponent used in Diffie-Hellman key exchange for IKE, TLS, and SSH sessions.	RAM (plain text)			Generated internally using DRBG.	Terminate the session, or power off the appliance.

#	Key/CSP	Type/Size	Usage	Storage	Input	Output	Generation	Zeroization
6	EC Diffie-Hellman shared secret	ECDH / P-256, P-384	Shared secret used in EC Diffie-Hellman key exchange for IKE and TLS sessions.	RAM (plain text)			Generated internally using EC Diffie-Hellman key exchange.	Terminate the session, or power off the appliance.
7	EC Diffie-Hellman private key	ECDH / 256, 384 bits	The private exponent used in EC Diffie-Hellman key exchange for IKE and TLS sessions.	RAM (plain text)			Generated internally using DRBG.	Terminate the session, or power off the appliance.
8	IKE pre-shared secret	Shared secret / 8 or more characters	Used by IKE for session authentication.	Local storage and RAM (plain text)	✓	✓	Entered by Cryptographic Officer.[1]	Delete the IPSec VPN configuration. Power off the appliance.
9	IKE session authentication key	HMAC-SHA1 / 160 bits HMAC-SHA-256 / 256 bits HMAC-SHA-384 / 384 bits HMAC-SHA-512 / 512 bits	Used to authenticate IKE negotiations.	RAM (plain text)			Generated internally using the negotiated pseudo random function (PRF) as defined in SP800-135 during IKE phase-1 exchange.	Terminate the session, or power off the appliance.

#	Key/CSP	Type/Size	Usage	Storage	Input	Output	Generation	Zeroization
10	IKE session encryption key	Triple-DES / 192 bits AES / 128,192,256 bits	Used to encrypt IKE negotiations.	RAM (plain text)			Generated internally using the negotiated pseudo random function (PRF) as defined in SP800-135 during IKE phase-1 exchange.	Terminate the session, or power off the appliance.
11	IPSec session authentication key	HMAC-SHA1 / 160 bits HMAC-SHA-256 / 256 bits HMAC-SHA-384 / 384 bits HMAC-SHA-512 / 512 bits	Exchanged using the IKE protocol. Used to authenticate IPSec traffic.	RAM (plain text)			Generated internally using the negotiated pseudo random function (PRF) as defined in SP800-135 during IKE phase-2 exchange.	Terminate the session, or power off the appliance.
12	IPSec session encryption key	Triple-DES / 192 bits AES / 128,192,256 bits	Exchanged using the IKE protocol. Used to encrypt IPSec traffic.	RAM (plain text)			Generated internally using the negotiated pseudo random function (PRF) as defined in SP800-135 during IKE phase-2 exchange.	Terminate the session, or power off the appliance.

#	Key/CSP	Type/Size	Usage	Storage	Input	Output	Generation	Zeroization
13	RSA private key	RSA / 2048, 3072, 4096 bits	The RSA private key used for IKE session authentication.	Local storage and RAM (plain text)	✓		Generated internally using DRBG or imported across an encrypted tunnel.	Restore the device to its factory default configuration.
14	TLS pre-master secret	Shared secret / 384 bits (using RSA), variable (using DH and ECDH)	Shared secret used in TLS exchange for TLS sessions.	RAM (plain text)			Generated internally using TLS protocol exchange.	Terminate the session, or power off the appliance.
15	TLS master secret	Shared secret / 384 bits	Shared secret used in TLS exchange for TLS sessions.	RAM (plain text)			Generated internally using TLS protocol exchange.	Terminate the session, or power off the appliance.
16	TLS session authentication key	HMAC-SHA1 / 160 bits HMAC-SHA-256 / 256 bits HMAC-SHA-384 / 384 bits HMAC-SHA-512 / 512 bits	Used to authenticate TLS traffic.	RAM (plain text)			Generated internally using the KDF as defined in SP800-135 during TLS protocol exchange.	Terminate the session, or power off the appliance.
17	TLS session encrypton key	Triple-DES / 192 bits AES / 128, 192, 256 bits	Used to encrypt TLS traffic.	RAM (plain text)			Generated internally using the KDF as defined in SP800-135 during TLS protocol exchange.	Terminate the session, or power off the appliance.

#	Key/CSP	Type/Size	Usage	Storage	Input	Output	Generation	Zeroization
18	RSA private key	RSA / 2048, 3072, 4096 bits	The RSA private key used for TLS authentication.	Local storage and RAM (plain text)			Generated internally using DRBG.	Restore the device to its factory default configuration.
19	SSH session authentication key	HMAC-SHA1 / 160 bits	Used by SSH for data integrity.	RAM (plain text)			Generated internally using the KDF as defined in SP800-135 during SSH protocol exchange.	Terminate the session, or power off the appliance.
20	SSH session key	AES / 128, 192, 256 bits	Used by SSH for session encryption.	RAM (plain text)			Generated internally using the KDF as defined in SP800-135 during SSH protocol exchange.	Terminate the session, or power off the appliance.
21	SSH RSA private key	RSA / 2048 bits	The RSA private key used for SSH authentication.	Local storage and RAM (plain text)			Generated internally using DRBG.	Restore the device to its factory default configuration.
22	SNMP password	Password / 8 or more characters	Used for deriving keys for SNMP authentication and encryption.	Local storage and RAM (plain text)	✓	✓	Entered by Cryptographic Officer or User.[1]	Overwrite with new password.

#	Key/CSP	Type/Size	Usage	Storage	Input	Output	Generation	Zeroization
23	SNMP session key	AES / 128	Used by SNMP for session encryption.	RAM (plain text)			Generated internally using the KDF as defined in SP800-135.	Terminate the session, or power off the appliance.
24	Passwords	Password / 8 or more characters	Used to authenticate Crypto-Officer and User logins.	Local storage and RAM (plain text)	✓	✓	Entered by Cryptographic Officer or User.[1]	Overwrite with new password.
25	Firmware load integrity key	HMAC-SHA1 / 160 bits	Used for firmware load test.	RAM (plain text)			Compiled into the firmware.	Install patch that deletes the firmware.
26	Firmware integrity key	HMAC-SHA1 / 160 bits	Used for firmware integrity test.	RAM (plain text)			Compiled into the firmware.	Install patch that deletes the firmware.
27	Dimension Log Server pre-shared secret	Shared secret / 8 or more characters	Used to authenticate connections to the log server.	Local storage and RAM (plain text)	✓	✓	Entered by Cryptographic Officer.[1]	Delete the log server configuration. Power off the appliance.

[1] Can be entered into the module in plain text over the serial console port from a non-networked computer.

[2] The minimum number of bits of entropy generated by the module for use in key generation is 276.

Public Keys

The following table lists the public keys used by the cryptographic module:

Table 18: Public Keys

#	Key/CSP	Type/Size	Usage	Storage	Input	Output	Generation	Zeroization
28	RSA public key	RSA / 2048, 3072, 4096 bits	Used by IKE for session authentication.	Local storage and RAM (plain text)	✓	✓	Generated using DRBG or imported across an encrypted tunnel.	Delete the IPSec VPN configuration. Power off the appliance.
29	RSA public key	RSA / 2048, 3072, 4096 bits	Used by Web UI clients for TLS authentication.	Local storage and RAM (plain text)		✓	Generated internally using DRBG.	Restore the device to its factory default configuration.
30	SSH RSA public key	RSA / 2048 bits	Used by SSH for authentication.	Local storage and RAM (plain text)		✓	Generated internally using DRBG.	Restore the device to its factory default configuration.
31	Diffie-Hellman public key	DH / 2048, 3072 bits	The public key used in Diffie-Hellman key exchange for IKE, TLS, and SSH sessions.	RAM (plain text)			Generated internally using Diffie-Hellman key exchange.	Terminate the session, or power off the appliance.
32	EC Diffie-Hellman public key	ECDH / P-256, P-384	The public key used in EC Diffie-Hellman key exchange for IKE and TLS sessions.	RAM (plain text)			Generated internally using EC Diffie-Hellman key exchange.	Terminate the session, or power off the appliance.

#	Key/CSP	Type/Size	Usage	Storage	Input	Output	Generation	Zeroization
33	SSLVPN RSA public key	RSA / 2048, 3072, 4096 bits	Used by SSLVPN clients for authentication.	Local storage and RAM (plain text)		✓	Generated internally using DRBG.	Restore the device to its factory default configuration.
34	HTTPS proxy RSA public key	RSA / 2048, 3072, 4096 bits	Used by HTTPS proxy clients for authentication.	Local storage and RAM (plain text)		✓	Generated internally using DRBG.	Restore the device to its factory default configuration.
35	HTTPS proxy authority RSA public key	RSA / 2048, 3072, 4096 bits	Used by the module for HTTPS proxy deep content inspection.	Local storage and RAM (plain text)		✓	Generated internally using DRBG.	Restore the device to its factory default configuration.

Mitigation of Other Attacks

The Firebox module includes optional capabilities of Intrusion Prevention System (IPS), Antivirus protection, Antispam, URL Filtering, Application Control, Data Loss Prevention, and Advanced Persistent Threats detection, in addition to capabilities described earlier. These capabilities are backed up by the WatchGuard proprietary proxy technology.

The proprietary Proxy technology enables the blocking of oversized files, supports blocking by file extension and blocking of traffic based on any Protocol Anomaly Detection (PAD).

The module offers an inbuilt default threat protection that protects the internal networks by performing behavioral analysis of traffic passing through the module. This can protect the module from direct attacks, based on TCP, ICMP, UDP, and IP protocols, such as Denial of Service (DoS), Distributed Denial of Service (DDoS), Synflood, and ping of death, etc. Access is denied or packets are dropped when an attack is detected. Attack parameters can be modified by the Cryptographic Officer to ensure that normal network traffic is not considered an attack.

Whenever a Gateway IPS, Gateway Antivirus, Antispam, WebBlocker, Application Control, Data Loss Prevention, or Advanced Persistent Threat event occurs, the module can record the event in the log and/or send an alarm to a Cryptographic Officer via a configured notification mechanism. The rest of this section provides additional information on different services of the Firebox module.

Gateway IPS Service

The WatchGuard Gateway IPS is a signature based component for detecting attacks passing through the module. Signature based attack detection mechanism works by identifying transmission patterns and other codes that indicate that a system might be under attack. Each signature is designed to detect a particular type of attack. The signatures for real-time IPS service are updated through the WatchGuard Gateway Intrusion Prevention Service. The module can be configured to securely automatically check for and download updated IPS packages from the WatchGuard servers, or they can be downloaded manually by the Cryptographic Officer. The IPS package is signed with the WatchGuard server's private key and verified by the module using the WatchGuard server's public key.

Gateway Antivirus Service

The Firebox Antivirus service scans web (HTTP), file transfer (FTP), Instant Messaging and email (POP3, IMAP, and SMTP) traffic passing through the module and removes and can optionally quarantine the infected content. The quarantined files and content are stored on the separate server outside the module. The Cryptographic Officer can review and delete quarantined files from the server. When any attachment is removed from the email, it is replaced with a replacement message that goes to the intended recipient of the email message.

The module can be configured to automatically check for and download updated AV signature and engine packages from the WatchGuard servers, or they can be downloaded manually by the Cryptographic Officer. The AV package is signed with the WatchGuard server's private key and verified

by the module using the WatchGuard server's public key. The module also is capable of updating the latest Antivirus engine securely through the Gateway Antivirus service.

Gateway Antivirus service also detects and removes malware such as adware, spyware, etc.

Quarantine Server which stores the emails and content is external to the module and not part of FIPS compliant module boundary.

spamBlocker Service

WatchGuard spamBlocker service can scan emails over SMTP, IMAP or POP3 protocols and can tag or discard email messages determined to be spam. Based on Recurrent Pattern Detection technology, optionally, this service can also quarantine the spam emails for administrators review. Spam detection methods also include black/white lists and return email DNS check. The spamBlocker Service also provides IP checking, URI address checking and email checksum analysis.

Quarantine Server which stores the emails and content is external to the module and is not part of the FIPS compliant module boundary.

WebBlocker Service

WatchGuard WebBlocker service offers URL filtering technology. WebBlocker service can be configured to scan HTTP and HTTPS protocol streams for banned URLs or web page content. The WebBlocker service uses a large database of URLs to block access to banned web sites and URLs based on content categories. The Cryptographic Officer can decide which categories of URLs are allowed by organization's security policy. The Cryptographic Officer can also configure URL filtering to block all or just some of the pages on a specific web site by using regular expressions. This feature can be used to deny access to parts of a web site without denying access to it completely. Also, the Cryptographic Officer can configure white and black lists to statically allow legitimate web pages or deny illegitimate web pages.

When a certain web page is blocked by the service, the end user is displayed a message that can be customized by the Cryptographic Officer using Web UI or Command Line Interface.

Application Control Service

WatchGuard Application Control, allows administrators to enforce acceptable use policies for users and groups by category, application, and application sub-functions. Using over 2,500 signatures and behavioral techniques, Application Control gives the administrator real-time and historical visibility into the use of applications on the network. The control and visibility given to the IT pro by WatchGuard Application Control helps organizations enforce acceptable use policies that are mandated by industry regulation, legal and political jurisdictions, corporate goals or culture.

WatchGuard's Application Control enables policy based monitoring, tracking, and blocking of over 1,800 unique web 2.0 and business applications. For example, administors can have granular control over the most important applications like Facebook and popular instant messaging applications e.g. allow MSN instant messaging, but disallow file transfer over MSN IM.

Data Loss Prevention Service

WatchGuard DLP prevents data breaches by scanning text and common file types to detect sensitive information. All data in motion, whether transferred via email, web, or FTP, is automatically inspected. Unlike other UTM DLP vendors, WatchGuard's subscription-based service includes a predefined library of more than 200 rules for 18 countries, covering personally identifiable information (PII), financial data, and healthcare information. Rule sets are updated monthly to stay current with data definitions and compliance mandates around the world.

Advanced Persistent Threat Blocker Service

WatchGuard APT Blocker focuses on behavior analysis to determine if a file is malicious. APT Blocker identifies and submits suspicious files to a cloud-based next-generation sandbox, a virtual environment where code is analyzed, emulated, and executed to determine its threat potential.

Modern malware including Advanced Persistent Threats (APTs) is designed to recognized and evade traditional defenses. APT Blocker's full system emulation – which simulates the physical hardware including CPU and memory – provides the most comprehensive level of protection against malware.

APT Blocker analyzes file types such as: Adobe PDF, Rich Text Format, Microsoft Office, Windows executable files, Android executable files, and Proxies (including POP3).

Definitions

AC – Alternating Current

AES – Advanced Encryption Standard

ANSI – American National Standards Institute

ASCII - American Standard Code for Information Interchange

AV – AntiVirus

CA – Certificate Authority

CBC – Cipher-Block Chaining

CC – Common Criteria

CF – Compact Flash

CFast – CompactFast

CLI – Command Line Interface

CO – Cryptographic Officer

CSP – Critical Security Parameter

DES – Data Encryption Standard

DH – Diffie-Hellman

DRBG – Deterministic Random Bit Generator

ECDSA – Elliptic Curve Digital Signature Algorithm

EEPROM – Electrically Erasable Programmable Read-Only Memory

FIPS – Federal Information Processing Standards

FTP – File Transfer Protocol

GUI – Graphical User Interface

HMAC – Hash Message Authentication Code

HTTPS – HyperText Transfer Protocol Secure

IMAP – Internet Message Access Protocol

IKE – Internet Key Exchange

IP – Internet Protocol

IPS – Intrusion Prevention System

IPSec – Internet Protocol Security

KAT – Known Answer Test

LAN – Local Area Network

LED – Light-Emitting Diode

MAC – Message Authentication Code

NIC – Network Interface Controller

NIST – National Institute of Standards and Technology

NOR – Negated OR flash

OS – Operating System

POP3 – Post Office Protocol 3

PPPoE – Point-to-Point Protocol over Ethernet

PPTP – Point-to-Point Tunneling Protocol

QSFP – Quad Small Form-factor Pluggable

RADIUS – Remote Authentication Dial In User Service

RC4 – Rivest Cipher 4

RSA – Rivest, Shamir, & Adelman algorithm

SD – Secure Digital

SFP – Small Form-factor Pluggable

SHA – Secure Hash Algorithm

SMTP – Simple Mail Transfer Protocol

SoHo – Small Office Home Office

SSH – Secure Shell protocol

SSLVPN – Secure Sockets Layer Virtual Private Network

TKIP – Temporal Key Integrity Protocol

TLS – Transport Layer Security

TOE – Target of Evaluation

Triple-DES – Triple Data Encryption Algorithm

UI – User Interface

USB – Universal Serial Bus

VLAN – Virtual Local Area Network

VoIP – Voice over Internet Protocol

VPN – Virtual Private Network

WAN – Wide Area Network

WAP – Wireless Access Point