FIPS 140-2 Non-Proprietary Security Policy

FortiGate Next-Generation Firewalls with FortiOS 6.4/7.0

FortiGate-40F Series, 60F Series (including FortiWiFi and FortiGateRugged), 80F Series, 100F Series, 200F Series, 600E Series, 1100E Series, 1800F Series, 2600F Series, 3300E Series, 3400E Series, 3600E Series, 4000F and 6000F Series

FortiGate Next-Generation Firewalls FIPS 140-2 Non-Proprietary Security Policy	
Document Version:	1.8
Publication Date:	Thursday, December 15, 2022
Description:	Documents FIPS 140-2 Level 2 Security Policy issues, compliancy and requirements for FIPS compliant operation.

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET KNOWLEDGE BASE

http://kb.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://www.fortinet.com/support/contact.html

FORTINET NSE INSTITUTE (TRAINING)

https://training.fortinet.com/

FORTIGUARD CENTER

https://fortiguard.com

FORTICAST

http://forticast.fortinet.com

END USER LICENSE AGREEMENT AND PRIVACY POLICY

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

FEEDBACK

Email: techdoc@fortinet.com

Thursday, December 15, 2022

FortiOS 6.4/7.0 FIPS 140-2 Non-Proprietary Security Policy

01-640-764263-20211126

TABLE OF CONTENTS

Overview

This document is a FIPS 140-2 Security Policy for Fortinet's FortiGate Next-Generation Firewalls with FortiOS versions 6.4 and 7.0. This policy describes how the FortiGate-40F Series, 60F Series, 80F Series, 100F Series, 200F Series, 600E Series, 1100E Series, 1800F Series, 2600F Series, 3300E Series, 3400E Series, 3600E Series, 4000F Series and 6000F Series (hereafter referred to as the 'modules') meet the FIPS 140-2 security requirements and how to operate the modules in a FIPS compliant manner. This policy was created as part of the FIPS 140-2 Level 2 validation of the modules.

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.

The modules meet the overall requirements for a FIPS 140-2 Level 2 validation.

Table 1: Validated module details

Module	Hardware ID*	Firmware
FortiGate-40F	C1AJ53	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGateRugged-60F	C1AJ89	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-60F	C1AJ22	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-61F	C1AJ23	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiWiFi-60F	C1AJ24	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiWiFi-61F	C1AJ25	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-80F	C1AK17	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-81F	C1AK18	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-100F	C1AJ43	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)

Module	Hardware ID*	Firmware
FortiGate-101F	C1AJ44	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-200F	C1AJ87	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-201F	C1AJ88	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-600E	C1AH98	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-601E	C1AH71	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-1100E	C1AJ67	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-1101E	C1AJ13	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-1800F	C1AJ82	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-1801F	C1AJ83	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-2600F	C1AK55	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-2601F	C1AK56	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-3300E	C1AJ42	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-3301E	C1AJ38	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-3400E	C1AH84	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-3401E	C1AH85	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-3600E	C1AH86	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)
FortiGate-3601E	C1AH57	FortiOS 6.4 (FIPS-CC-64-5) FortiOS 7.0 (FIPS-CC-70-6)

Module	Hardware ID*	Firmware
FortiGate-4200F	C1AH81	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-4201F	C1AJ94	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-4400F	C1AH79	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-4401F	C1AJ45	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-6300F	C1AG83	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-6301F	C1AG85	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-6500F	C1AG84	FortiOS 6.4 (FIPS-CC-64-5)
FortiGate-6501F	C1AG86	FortiOS 6.4 (FIPS-CC-64-5)

* - All Hardware ID's require tamper evident seal kit FIPS-SEAL-RED

References

This policy deals specifically with operation and implementation of the modules in the technical terms of the FIPS 140-2 standard and the associated validation program. Other Fortinet product manuals, guides and technical notes can be found at the Fortinet technical documentation website at https://docs.fortinet.com.

Additional information on the entire Fortinet product line can be obtained from the following sources:

- Find general product information in the product section of the Fortinet corporate website at https://www.fortinet.com/products.
- Find on-line product support for registered products in the technical support section of the Fortinet corporate website at https://www.fortinet.com/support.
- Find contact information for technical or sales related questions in the contacts section of the Fortinet corporate website at https://www.fortinet.com/contact.
- Find security information and bulletins in the FortiGuard Center of the Fortinet corporate website at https://www.fortiguard.com.

Introduction

The FortiGate family of Next Generation Firewalls spans the full range of network environments, from SOHO to service provider, offering cost effective systems for any size of application. FortiGate appliances 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. In addition to providing application level firewall protection, FortiGate appliances deliver a full range of network-level services — VPN, intrusion prevention, web filtering, antivirus, antispam and traffic shaping — in dedicated, easily managed platforms.

All FortiGate appliances employ Fortinet's unique FortiASIC content processing chip and the powerful, secure, FortiOS firmware achieve breakthrough price/performance. The unique, ASIC-based architecture analyzes content and behavior in real time, enabling key applications to be deployed right at the network edge where they are most effective at protecting enterprise networks. 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 modules support High Availability (HA) in both Active-Active (AA) and Active-Passive (AP) configurations.

FortiGate appliances support the IPsec industry standard for VPN, allowing VPNs to be configured between a FortiGate appliance and any client or gateway/firewall that supports IPsec VPN. FortiGate appliances also provide SSL VPN services using TLS 1.1 and 1.2.

Security Level Summary

The modules meet the overall requirements for a FIPS 140-2 Level 2 validation.

Table 2: Summary of FIPS security requirements and compliance levels

Security Requirement	Compliance Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	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

Module Descriptions

The FortiGate-40F Series, 60F Series, 80F Series, 100F Series, 200F Series, 600E Series, 1100E Series, 1800F Series, 2600F Series, 3300E Series, 3400E Series, 3600E Series and 4000F Series are hardware modules. They are multiple chip, standalone cryptographic modules consisting of production grade components contained in a physically protected enclosure in accordance with FIPS 140-2 Level 2 requirements. The extent of the cryptographic boundary for all modules is the outer metal chassis.

The FortiGate-600E/601E/6300F/6301F/6500F/6501F/4200F/4201F/4400F/4401F contain removable power supplies. These power supplies are excluded from the requirements of FIPS-140-2, on the basis that they provide no additional security.

The modules have a similar appearance and perform the same functions, but have different numbers and types of network interfaces, CPUs, etc.

The validated firmware versions are FortiOS 6.4 (FIPS-CC-64-5) and FortiOS 7.0 (FIPS-CC-70-6) .

Figures 1 to 17 are representative of the modules tested.

FortiGate-40F Series (FortiGate-40F)

- FortiGate-40F
- 5 network interfaces with status LEDs for each network interface (10x 10/100/1000 Base-T)
- 1x Fortinet SOC4 CPU (ARMv8)
- 1x Fortinet CP9XLite ASIC (embedded in SOC4)
- Desktop form factor

FortiGate-60F Series (FortiGate/FortiWiFi-60F/61F)

- 10 network interfaces with status LEDs for each network interface (10x 10/100/1000 Base-T)
- 1x Fortinet SOC4 CPU (ARMv8)
- 1x Fortinet CP9XLite ASIC (embedded in SOC4)
- Desktop form factor
- The FortiGate/FortiWiFi-60F are identical to the FortiGate/FortiWiFi-61F except the 61F models have an internal 128GB SSD where the 60F models do not

FortiGateRugged-60F

- 8 network interfaces with status LEDs for each network interface (6x 10/100/1000 Base-T, 2x 1GB SFP)
- 1x Fortinet SOC4 CPU (ARMv8)
- 1x Fortinet CP9XLite ASIC (embedded in SOC4)
- Desktop form factor

FortiGate-80F Series (FortiGate-80F/81F)

- 12 network interfaces with status LEDs for each network interface (10x 10/100/1000 Base-T, 2x 1GB SFP)
- 1x Fortinet SOC4 CPU (ARMv8)
- 1x Fortinet CP9XLite ASIC (embedded in SOC4)

- Desktop form factor
- The FortiGate-80F is identical to the FortiGate-811F except the 81F model has an internal 128GB SSD where the 80F model does not

FortiGate-100F Series (FortiGate-100F/101F)

- 28 network interfaces with status LEDs for each network interface (22x 10/100/1000 Base-T, 8x 1GB SFP, 2x 10GB SFP+)
- 1x Fortinet SOC4 CPU (ARMv8)
- 1x Fortinet CP9XLite ASIC (embedded in SOC4)
- 1u form factor
- The FortiGate-100F is identical to the FortiGate-101F except the 101F model has an internal 480GB SSD where the 100F model does not

FortiGate-200F Series (FortiGate-200F/201F)

- 30 network interfaces with status LEDs for each network interface (18x 10/100/1000 Base-T, 8x 1GB SFP, 4x 10GB SFP+)
- 1x Intel x86 CPU
- 2x Fortinet CP9 ASIC
- 1u form factor
- The FortiGate-200F is identical to the FortiGate-201F except the 201F model has an internal 480GB SSD where the 200F model does not

FortiGate-600E Series (FortiGate-600E/601E)

- 20 network interfaces status LEDs for each network interface (10x 10/100/1000 Base-T, 8x 1GB SFP, 2x 10GB SFP+)
- 1x Intel x86 CPU
- 2x Fortinet CP9 ASIC
- 1u form factor
- The FortiGate-600E is identical to the FortiGate-601E except the 601E model has internal 2x 240GB SSDs where the 600E model does not

FortiGate-1100E Series (FortiGate-1100E/1101E)

- 36 network interfaces with status LEDs for each network interface (18x 10/100/1000 Base-T, 8x 1GB SFP, 4x 10GB SFP+, 4x 25GB SFP28, 2x 40GB QSFP+)
- 1x Intel x86 CPU
- 2x Fortinet CP9 ASIC
- 2u form factor
- The FortiGate-1100E is identical to the FortiGate- 1101E except the 1101E model has 2x internal 480GB SSD where the 1100E model does not

FortiGate-1800F Series (FortiGate-1800F/1801F)

- 46 network interfaces with status LEDs for each network interface (18x 10/100/1000 Base-T, 8x 1GB SFP, 4x 10GB SFP+, 12x 25GB SFP28, 4x 40GB QSFP+)
- 1x Intel x86 CPU

- 4x Fortinet CP9 ASIC
- 2u form factor
- The FortiGate-1800F is identical to the FortiGate- 1801F except the 1801F model has 2x internal 1TB SSD where the 1800F model does not

FortiGate-2600F Series (FortiGate-2600F/2601F)

- 40 network interfaces with status LEDs for each network interface (18x 10/100/1000 Base-T, 2x 10GB SFP+, 16x 25GB SFP28, 4x 40GB QSFP+)
- 1x Intel x86 CPU
- 4x Fortinet CP9 ASIC
- 2u form factor
- The FortiGate-2600F is identical to the FortiGate- 2601F except the 2601F model has 2x internal 1TB SSD where the 2600F model does not

FortiGate-3300E Series (FortiGate-3300E/3301E)

- 38 network interfaces with status LEDs for each network interface (18x 10/100/1000 Base-T, 16x 10GB SFP+/25GB SFP28, 4x 40GB QSFP+)
- 1x Intel x86 CPU
- 8x Fortinet CP9 ASIC
- 2u form factor
- The FortiGate-3300E is identical to the FortiGate-3301E except the 3301E model has 2x internal 1TB SSD where the 3300E model does not

FortiGate-3400E Series (FortiGate-3400E/3401E)

- 30 network interfaces with status LEDs for each network interface (2x 10/100/1000 Base-T, 22x SFP+/SFP28, 4x QSFP28)
- 2x Intel x86 CPU
- 4x Fortinet CP9 ASIC
- 2u form factor
- The FortiGate-3400E is identical to the FortiGate-3401E except the 3401E model has 2x internal 2TB HDD where the 3400E model does not

FortiGate-3600E Series (FortiGate-3600E/3601E)

- 40 network interfaces with status LEDs for each network interface (2x 10/100/1000 Base-T, 30x SFP+/SFP28, 4x QSFP28)
- 1x Intel x86 CPU
- 8x Fortinet CP9 ASIC
- 2u form factor
- The FortiGate-3600E is identical to the FortiGate-3601E except the 3601E model has 2x internal 2TB HDD where the 3600E model does not

FortiGate-4200F Series (FortiGate-4200F/4201F)

- 30 network interfaces with status LEDs for each network interface (6x 10/100/1000 Base-T, 16x SFP28, 8x QSFP28)

- 2x Intel x86 CPU
- 8x Fortinet CP9 ASIC
- 3u form factor
- The FortiGate-4200F is identical to the FortiGate-4201F except the 4201F model has 2x internal 2TB HDD where the 4200F model does not

FortiGate-4400F Series (FortiGate-4400F/4401F)

- 34 network interfaces with status LEDs for each network interface (6x 10/100/1000 Base-T, 16x SFP28, 12x QSFP28)
- 4x Intel x86 CPU
- 16x Fortinet CP9 ASIC
- 4u form factor
- The FortiGate-4400F is identical to the FortiGate-4401F except the 4401F model has 2x internal 2TB HDD where the 4400F model does not

FortiGate-6000F Series (FortiGate-6300F/6301F/6500F/6501F)

The modules use two, distinct entropy sources - the entropy token and the Fortinet CP9 Security Processor. The entropy token provides entropy for the main PCB. The CP9 Security Processors provide entropy for the processor cards.

- The modules have 33 network interfaces with status LEDs for each network interface (2x 10/100/1000 Base-T, 24x 10/25GB SFP28, 4x40/100GB QSFP28, 3x 10GB SFP+)
- The modules each have one x86 compatible CPU on the main PCB
- The FortiGate-6000F/6301F has 6 processor cards each with its own x86 compatible CPU and two FortiASIC CP9 Security Processors.
- The FortiGate-6500F/6501F has 10 processor cards each with its own x86 compatible CPU and two FortiASIC CP9 Security Processors
- The FortiGate-6300F is identical to the Fortigate-6301F, except the 6301F has two 1TB internal hard drives while the 6300F does not
- The FortiGate-6500F is identical to the Fortigate-6501F, except the 6501F has two 1TB internal hard drives while the 6500F does not

Cryptographic Module Ports and Interfaces

All of the modules have status LEDs as described in the following table:

Table 3: Module Status LEDs

LED	State	Description
Power	Green	The module is powered on.
	Off	The module is powered off.

LED		State	Description
Status		Green	The module is running normally.
		Flashing	The module is starting up.
		Off	The module is powered off.
HA		Green	HA is enabled.
		Off	The unit is in standalone mode.
Alarm		Red	The unit has a major alarm.
		Amber	The unit has a minor alarm.
		Off	The unit is operating normally.
Ethernet Ports	Link/ACT	Green	Port is connected.
		Flashing	Port is sending/receiving data.
		Off	No link established.
	Speed	Green	Connected at 1000 Mbps.
		Amber	Connected at 100 Mbps
		Off	Connected at 10 Mbps
SFP and SFP+ Ports		Green	Port is connected.
		Flashing	Port is sending/receiving data.
		Off	No link established.

FortiGate-40F

Figure 1 - FortiGate-40F Front and Rear Panels

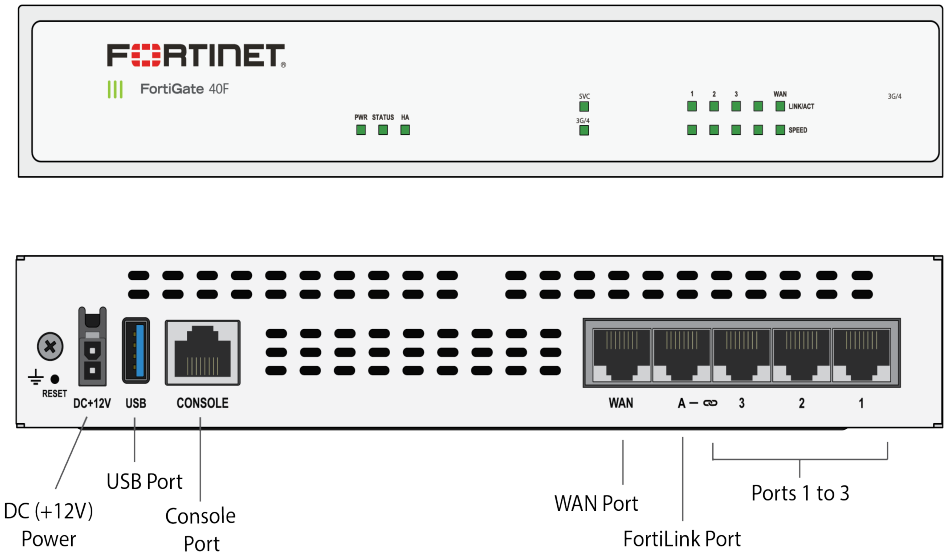

Table 4: FortiGate-40F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1-3, WAN Port, FortiLink Port	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Port	USB A	N/A	Control input, data output, data input	Configuration loading and archiving.
DC Power	N/A	N/A	Power	+12 VDC power connection

FortiGate-60F/61F

Figure 2 - FortiGate-60F/61F Front and Rear Panels

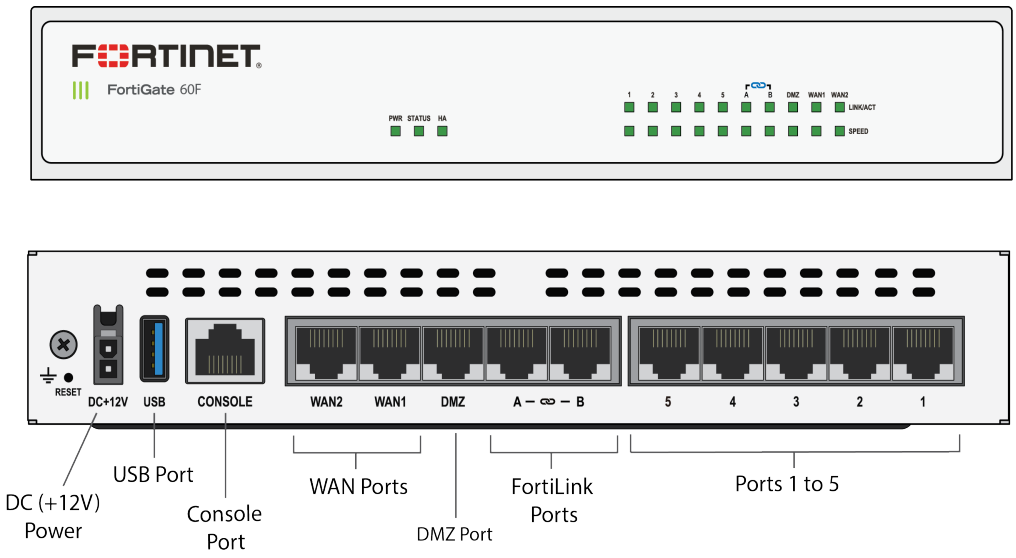

Table 5: FortiGate-60F/61F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1-5, WAN Ports, DMZ Port, FortiLink Ports	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Port	USB A	N/A	Control input, data output, data input	Configuration loading and archiving.
DC Power	N/A	N/A	Power	+12 VDC power connection

FortiWiFi-60F/61F

Figure 3 - FortiWiFi-61F Front and Rear Panels

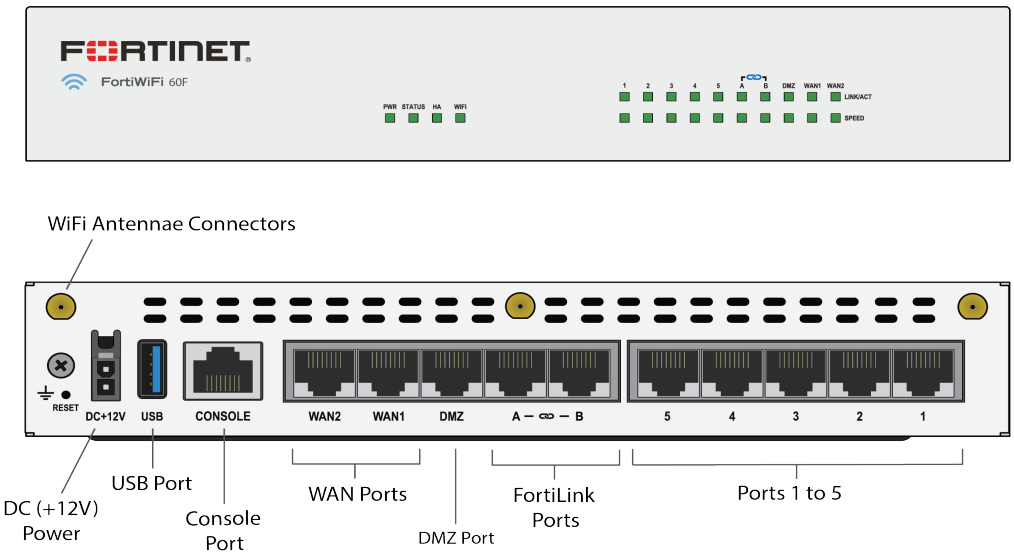

Table 6: FortiWiFi-61F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1-5, WAN Ports, DMZ Port, FortiLink Ports	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.
WiFi Antennae Connector	Antennae Connector	Up to 1Gbps or higher	Data input, data output, control input and status output	Wireless network connections using 802.11ac
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Port	USB A	N/A	Control input, data output, data input	Configuration loading and archiving.
DC Power	N/A	N/A	Power	+12 VDC power connection

FortiGateRugged-60F

Figure 4 - FortiGateRugged-60F Front and Rear Panels

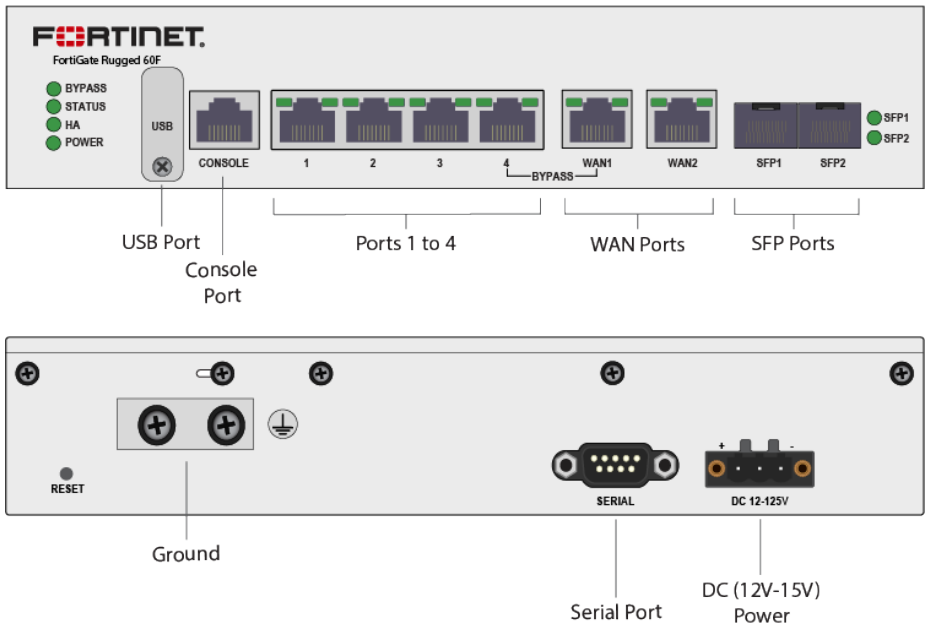

Table 7: FortiGateRugged-60F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1-4, WAN Ports,	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.
SFP Ports	SFP	1Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Port	USB A	N/A	Control input, data output, data input	Configuration loading and archiving.

Connector	Type	Speed	Supported Logical Interfaces	Description
Serial Port	DB9	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
DC Power	N/A	N/A	Power	12-15 VDC power connection

FortiGate-80F/81F

Figure 5 - FortiGate-80F/81F Front and Rear Panels

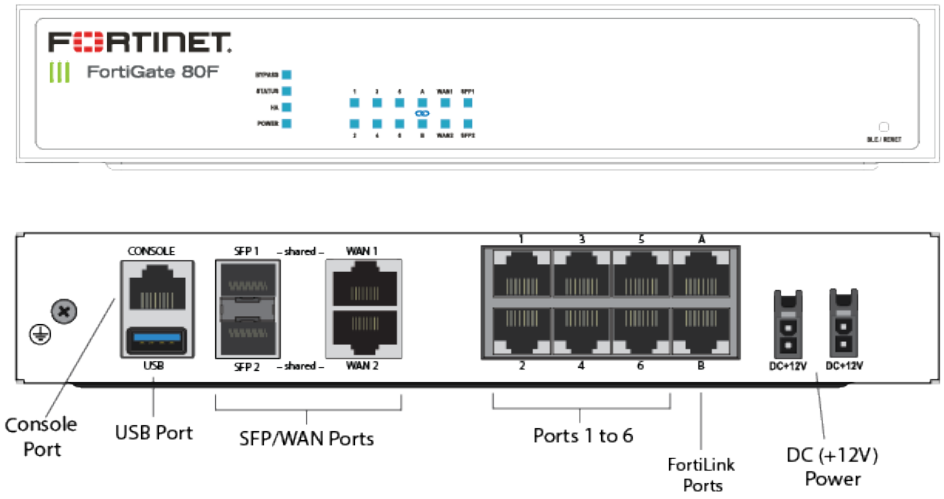

Table 8: FortiGate-80F/81F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1-6, WAN Ports, FortiLink Ports	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.

Connector	Type	Speed	Supported Logical Interfaces	Description
SFP Ports	SFP	1Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Port	USB A	N/A	Control input, data output, data input	Configuration loading and archiving.
DC Power	N/A	N/A	Power	+12 VDC power connection

FortiGate-100F/101F

Figure 6 - FortiGate-100F/101F Front and Rear Panels

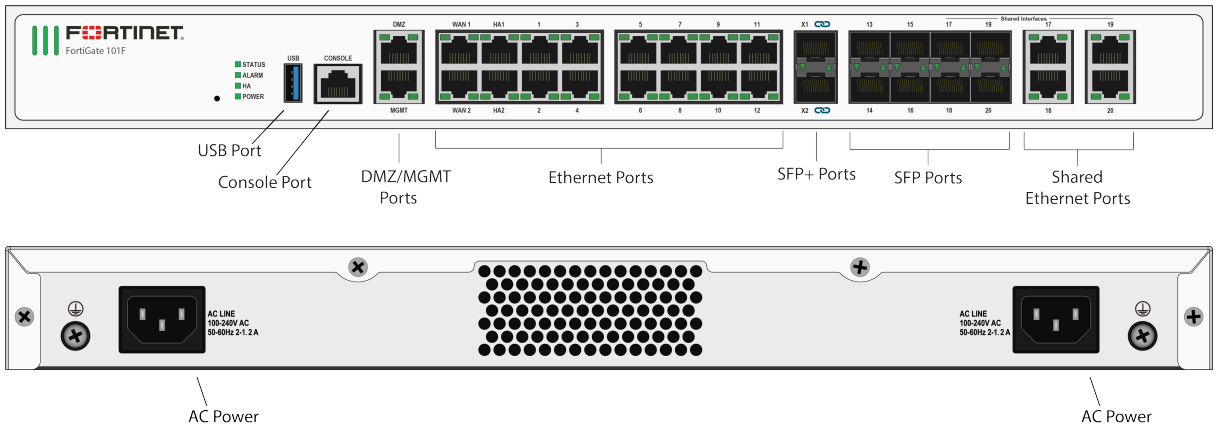

Table 9: FortiGate-100F/101F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
DMZ, MGMT, WAN, HA Ports, Ports 1-12 and Ports 17-20	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.

Connector	Type	Speed	Supported Logical Interfaces	Description
X Ports 1-2	SFP+	10 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 13-20	SFP	1 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Shared Ports 17-20	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Port	USB A	N/A	Control input, data output, data input	Configuration loading and archiving.
AC Power	N/A	N/A	Power	120/240VAC power connection.

FortiGate-200F/201F

Figure 7 - FortiGate-200F/201F Front and Rear Panels

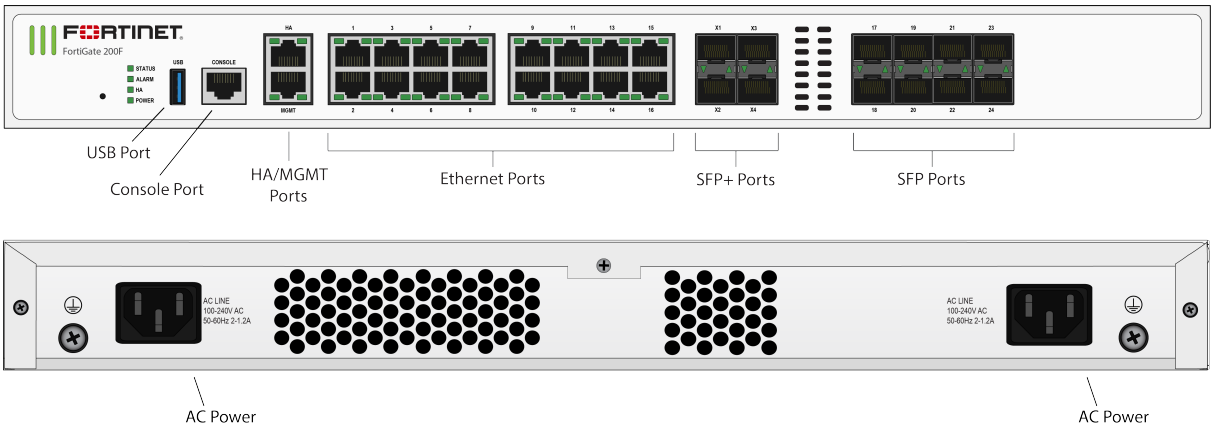

Table 10: FortiGate-200F/201F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
HA, MGMT Ports, Ports 1-16	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.
X Ports 1-4	SFP+	10 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 17-24	SFP	1 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Port	USB A	N/A	Control input, data output, data input	Configuration loading and archiving.
AC Power	N/A	N/A	Power	120/240VAC power connection.

FortiGate-600E/601E

Figure 8 - FortiGate-600E/601E Front and Rear Panels

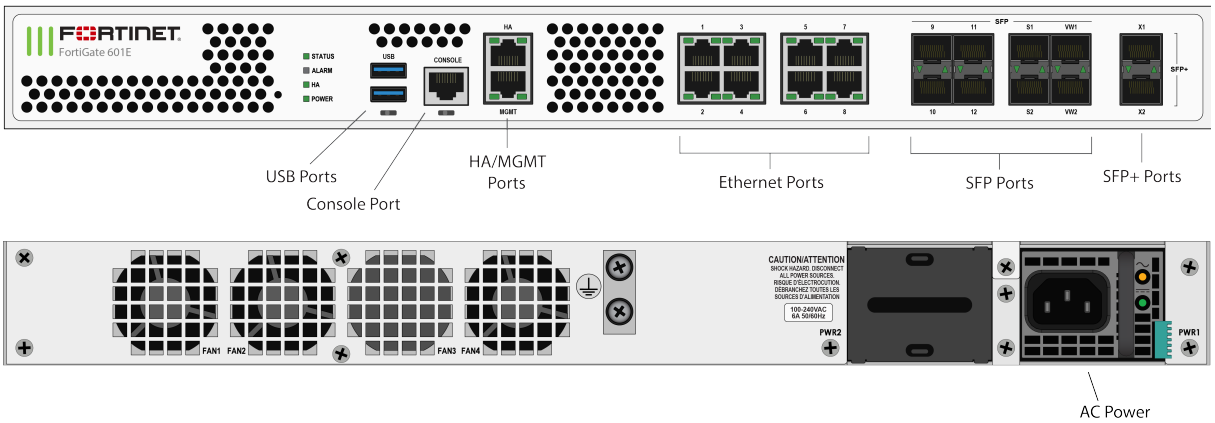

Table 11: FortiGate-600E/601E Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
MGMT, HA Ports and Ports 1-8	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
S, VW Ports and Ports 9-12	SFP	1 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
X Ports	SFP+	10 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
USB Ports	USB-A	N/A	Control input, data output, data input	Configuration loading and archiving.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
AC Power	N/A	N/A	Power	120/240VAC power connection.

FortiGate-1100E/1101E

Figure 9 - FortiGate-1100E/1101E Front and Rear Panels

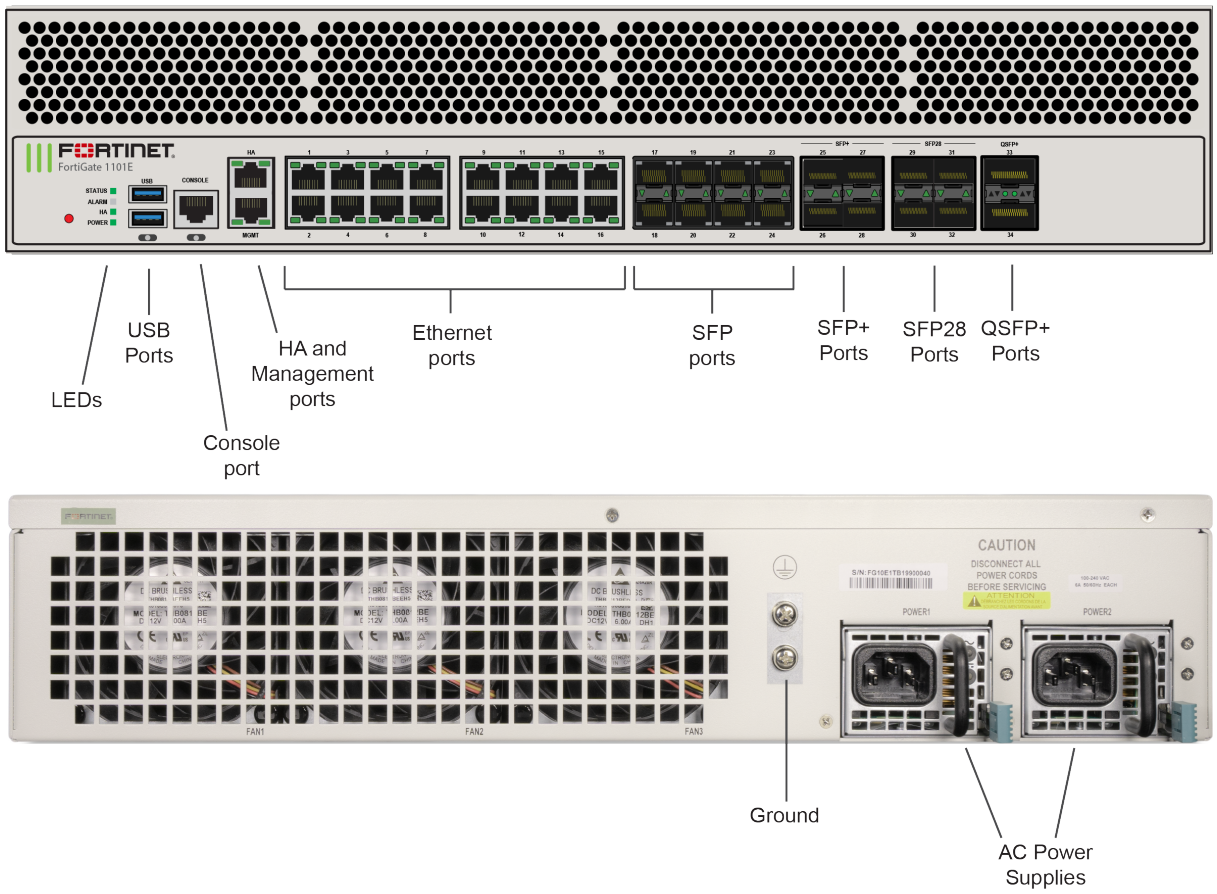

Table 12: FortiGate-1100E/1101E Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
MGMT and HA Ports	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Gigabit connection to 10/100/1000 copper networks.
Ports 1-16	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Gigabit connection to 10/100/1000 copper networks.
Ports 17-24	SFP	1 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 25-28	SFP+	10 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 29-32	SFP28	25 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 33-34	QSFP+	40 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
USB Port	USB-A	N/A	Control input, data output, data input	Configuration loading and archiving.

FortiGate-1800F/1801F

Figure 10 - FortiGate-1800F/1801F Front and Rear Panels

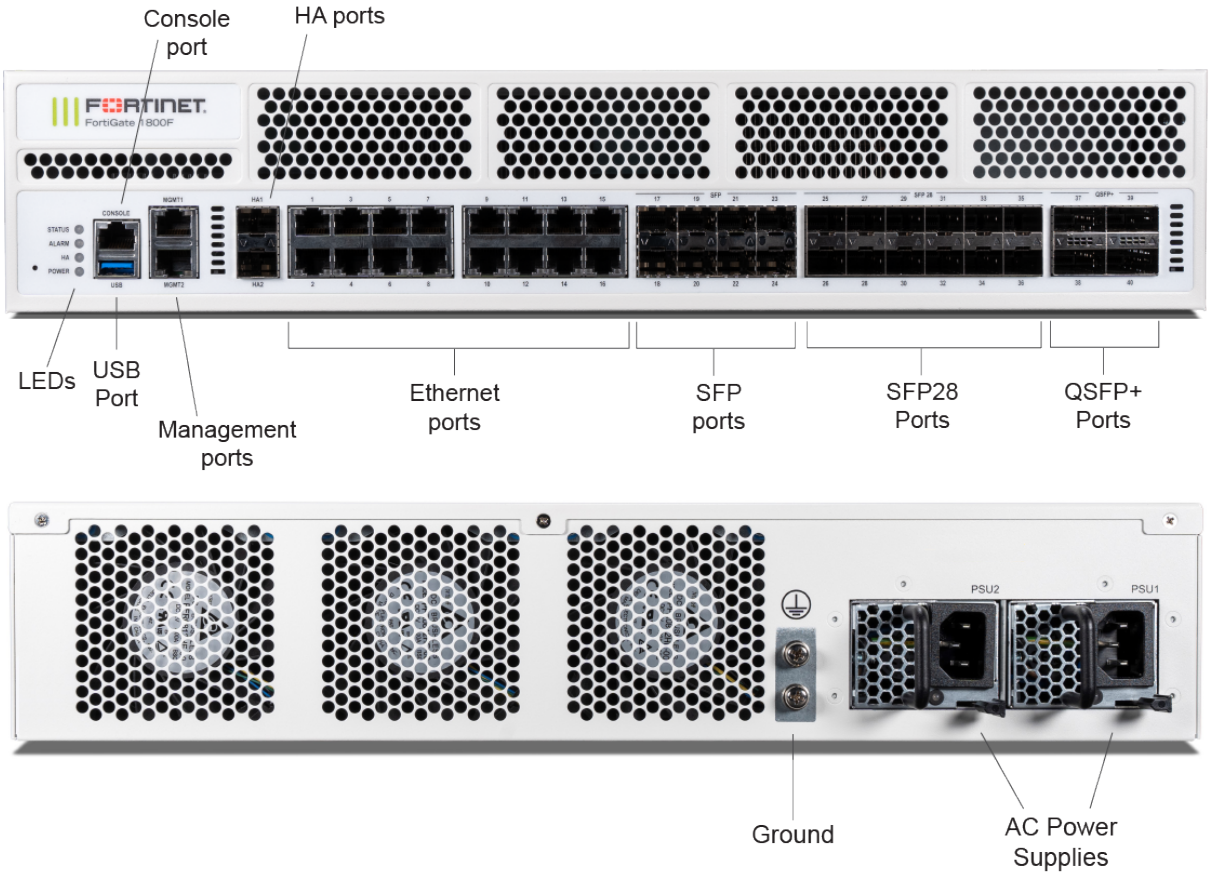

Table 13: FortiGate-1800F/1801F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
HA, MGMT Ports, Ports 1-16	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.
Ports 17-24	SFP	1 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 25-36	SFP+/SFP28	10 Gbps/ 25 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 37-40	QSFP+	40Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Port	USB A	N/A	Control input, data output, data input	Configuration loading and archiving.
AC Power	N/A	N/A	Power	120/240VAC power connection.

FortiGate-2600F/2601F

Figure 11 - FortiGate-2600F/2601F Front and Rear Panels

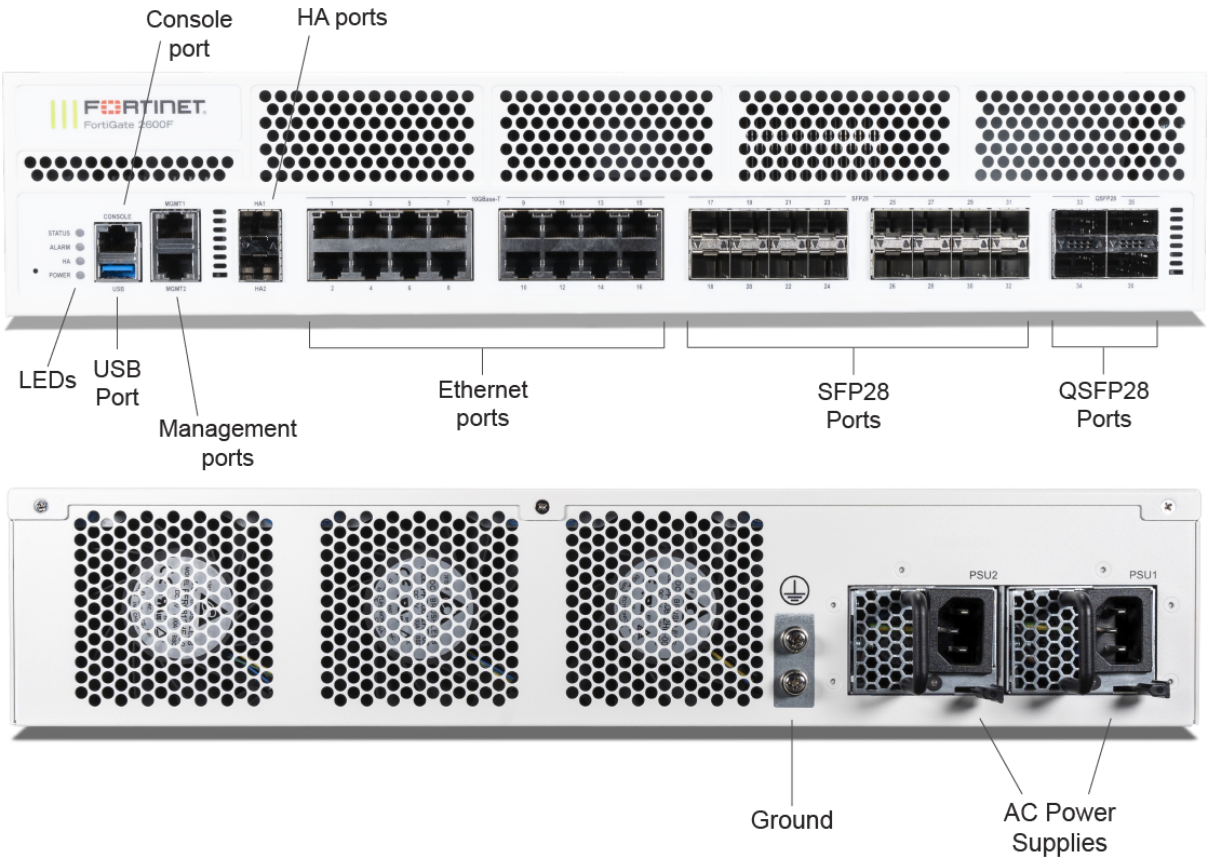

Table 14: FortiGate-2600F/2601F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
HA, MGMT Ports, Ports 1-16	RJ-45	10/100/1000 Base-T	Data input, data output, control input and status output	Connection to 10/100/1000 networks.
Ports 17-32	SFP28	25 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 33-36	QSFP28	40Gbps/ 100Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.

Connector	Type	Speed	Supported Logical Interfaces	Description
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
USB Port	USB A	N/A	Control input, data output, data input	Configuration loading and archiving.

FortiGate-3300E/3301E

Figure 12 - FortiGate-3300E/3301E Front and Rear Panels

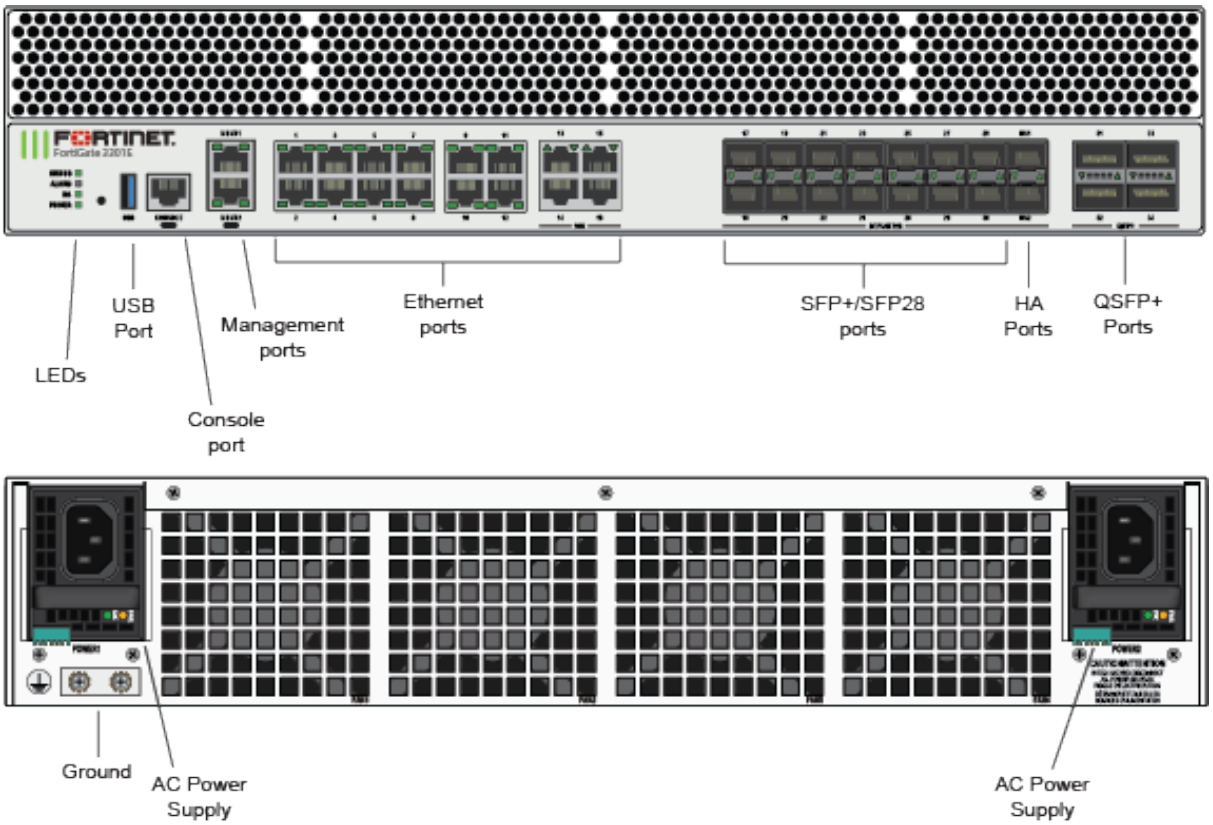

Table 15: FortiGate-3300E/3301E Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
MGMT Ports	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
HA Ports and Ports 1-22	SFP+/SFP28	10/25 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 23-26	QSFP28	100 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
USB Port	USB-A	N/A	Control input, data output, data input	Configuration loading and archiving.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
AC Power	N/A	N/A	Power	120/240VAC power connection.

FortiGate-3400E/3401E

Figure 13 - FortiGate-3400E/3401E Front and Rear Panels

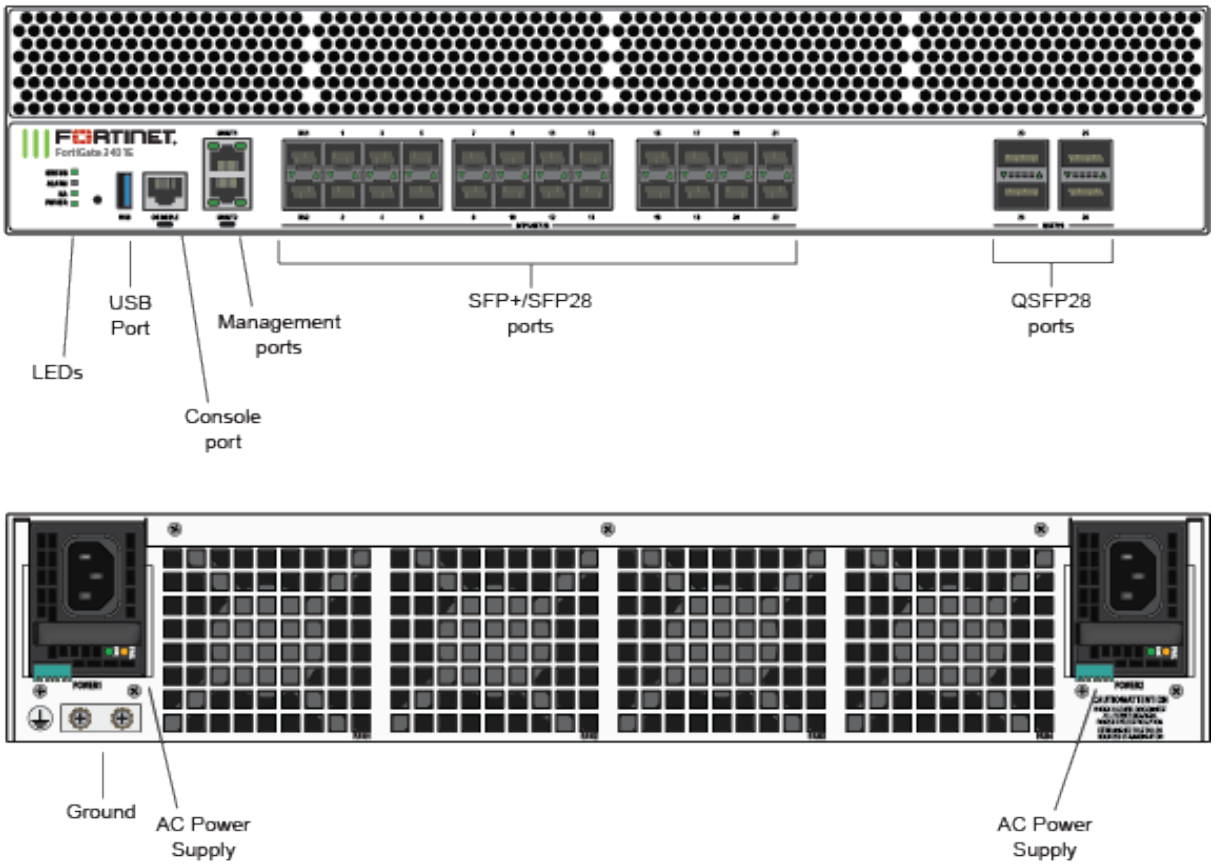

Table 16: FortiGate-3400E/3401E Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
MGMT Ports	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
HA Ports	SFP+/ SFP28	25 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 1-22	SFP+/ SFP28	25 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 23-26	QSFP28	100 Gbps	Data input, data output, control input and status output	Multimode fiber optic connections to gigabit optical networks.
USB Ports	USB-A	N/A	Control input, data output, data input	Configuration loading and archiving.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
AC Power	N/A	N/A	Power	120/240VAC power connection.

FortiGate-3600E/3601E

Figure 14 - FortiGate-3600E/3601E Front and Rear Panels

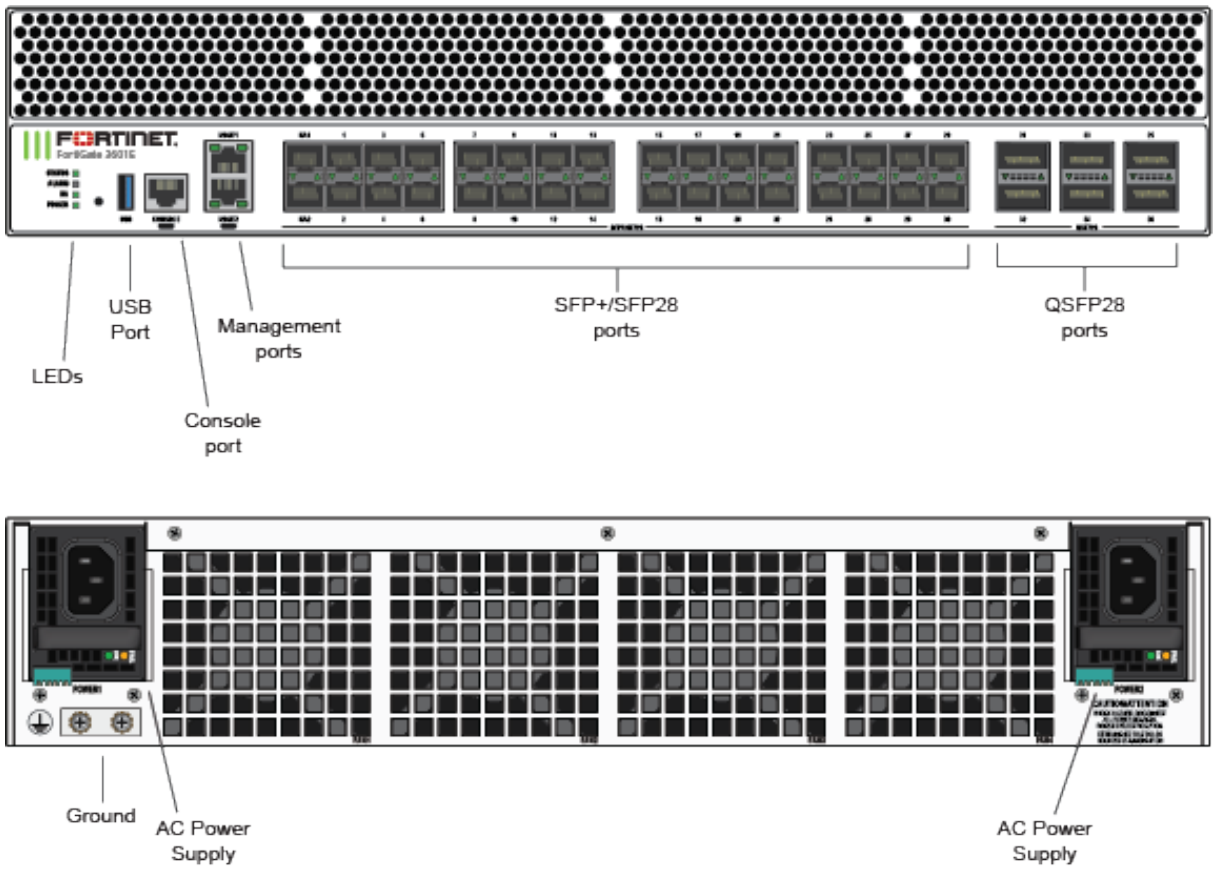

Table 17: FortiGate-3600E/3601E Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
MGMT Ports	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
HA Ports and Ports 1-30	SFP+/SFP28	10/25 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 31-36	QSFP28	100 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
USB Port	USB-A	N/A	Control input, data output, data input	Configuration loading and archiving.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
AC Power	N/A	N/A	Power	120/240VAC power connection.

FortiGate-4200/4201F

Figure 15 - FortiGate-4200/4201F Front and Rear Panels

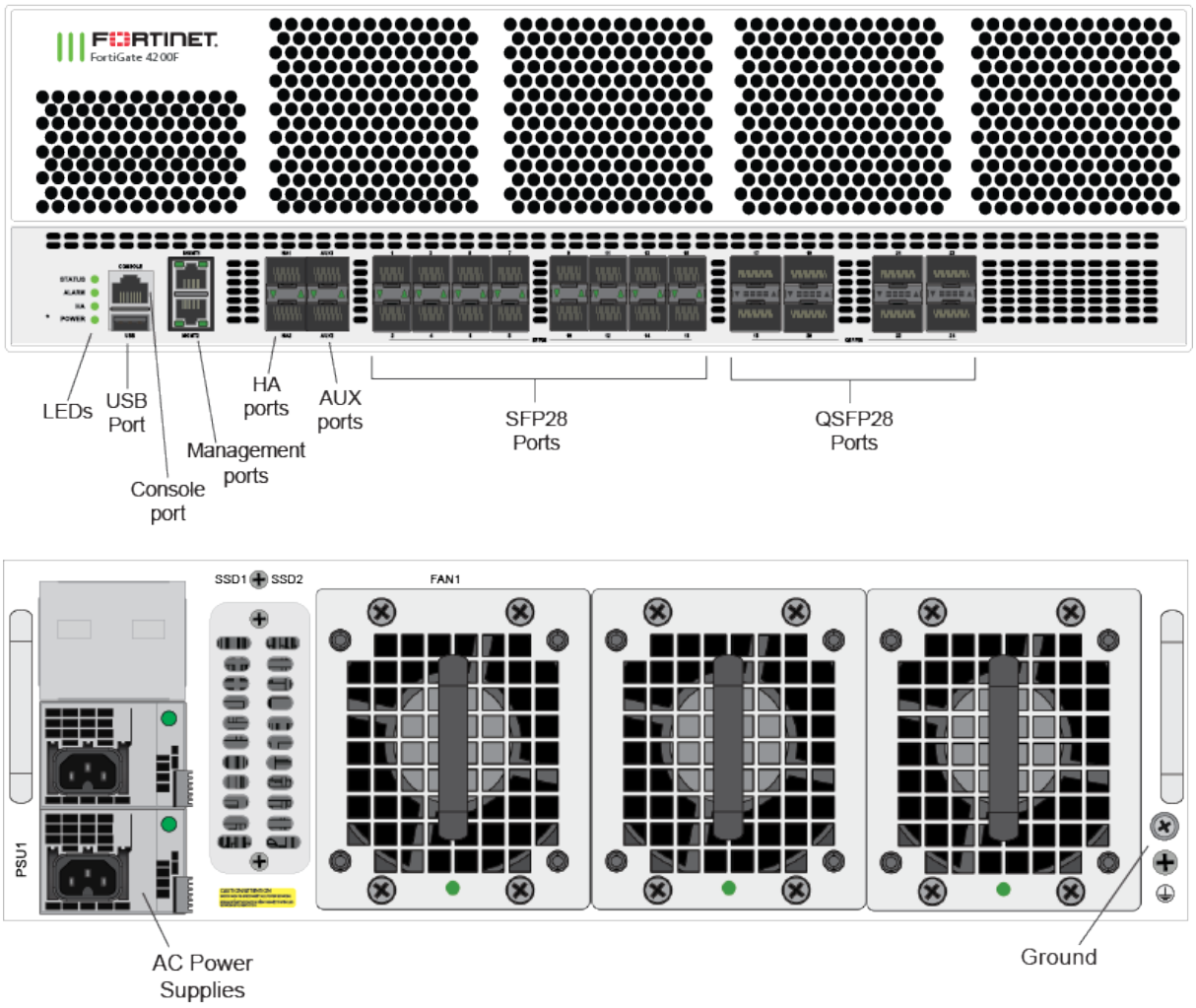

Table 18: FortiGate-4200/4201F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
MGMT ports	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.

Connector	Type	Speed	Supported Logical Interfaces	Description
HA and AUX ports	SFP28	25 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 1 to 16	SFP28	25 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 17 to 24	QSFP28	100 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
USB Port	USB-A	N/A	Control input, data output, data input	Configuration loading, archiving and entropy token.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
AC Power	N/A	N/A	Power	120/240VAC power connection.

FortiGate-4400/4401F

Figure 16 - FortiGate-4400/4401F Front and Rear Panels

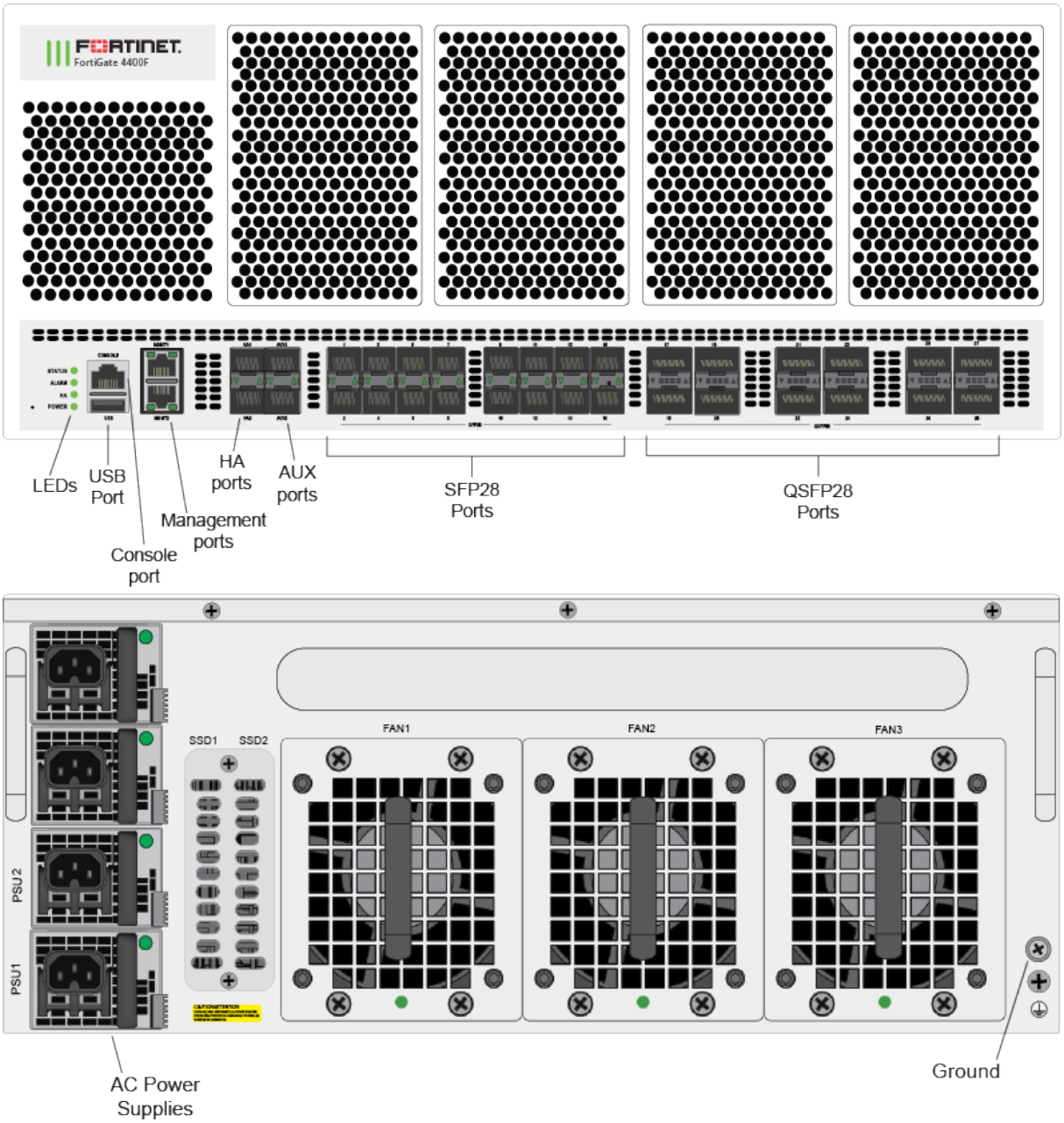

Table 19: FortiGate-4400/4401F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
MGMT ports	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
HA and AUX ports	SFP28	25 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 1 to 16	SFP28	25 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 17 to 28	QSFP28	100 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
USB Port	USB-A	N/A	Control input, data output, data input	Configuration loading, archiving and entropy token.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
AC Power	N/A	N/A	Power	120/240VAC power connection.

FortiGate-6300F/6301F and 6500F/6501F

Figure 17 - FortiGate-6300F/6301F and 6500F/6501F Front and Rear Panels

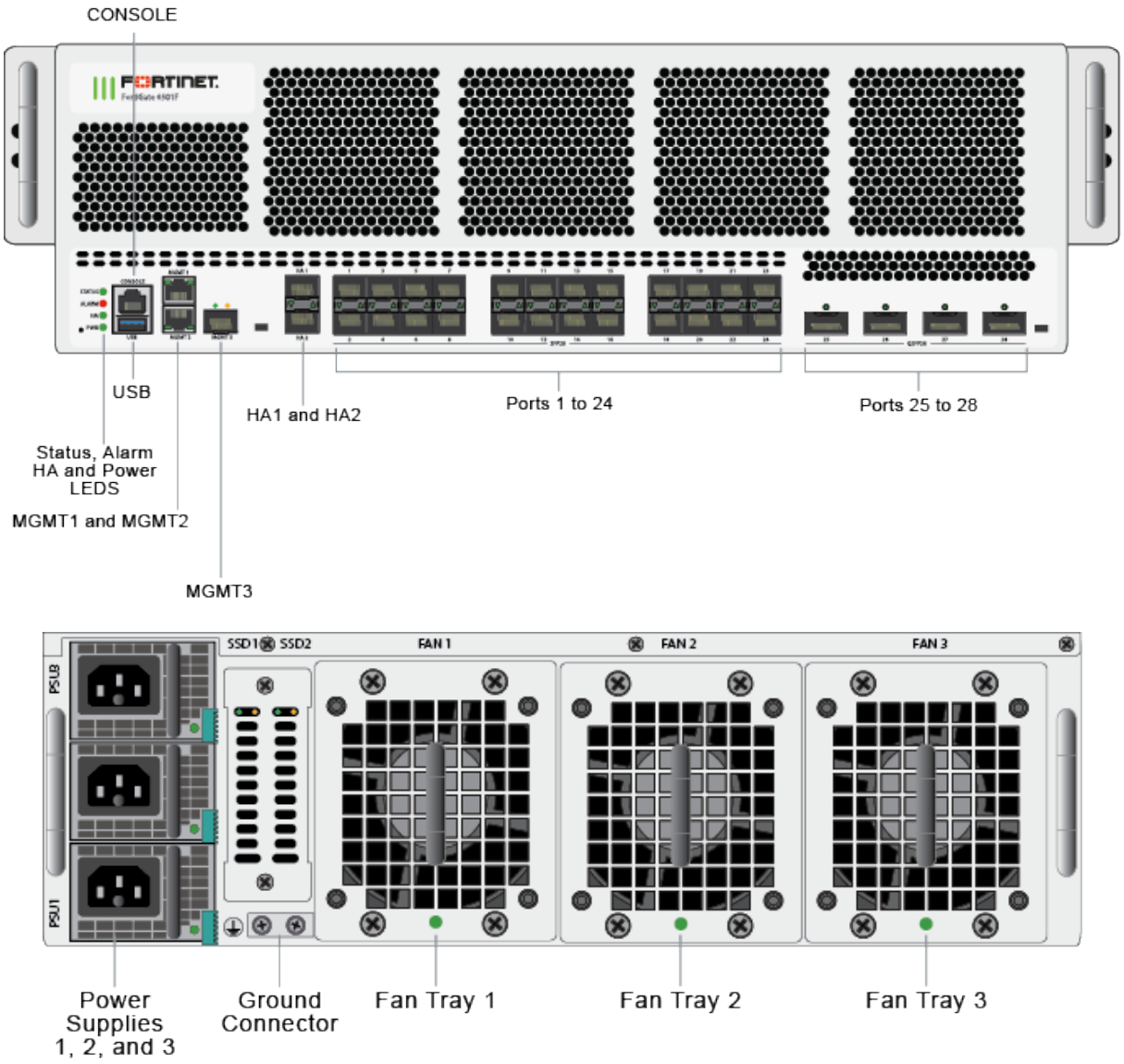

Table 20: FortiGate-6300F/6301F and 6500F/6501F Connectors and Ports

Connector	Type	Speed	Supported Logical Interfaces	Description
MGMT 1 and 2	RJ-45	10/100/1000 Base-T	Data input, data output, control input, and status output	Copper gigabit connection to 10/100/1000 copper networks.
MGMT 3, HA 1 and 2	SFP+	10 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.

Connector	Type	Speed	Supported Logical Interfaces	Description
Ports 1 to 24	SFP28	25 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
Ports 25 to 28	QSFP28	100 Gbps	Data input, data output, control input, and status output	Multimode fiber optic connections to gigabit optical networks.
USB Port	USB-A	N/A	Control input, data output, data input	Configuration loading, archiving and entropy token.
Console Port	RJ-45	9600 bps	Control input, status output	Optional connection to the management computer. Provides access to the command line interface (CLI).
AC Power	N/A	N/A	Power	120/240VAC power connection.

Web-Based Manager

The FortiGate web-based manager provides GUI based access to the modules and is the primary tool for configuring the modules. The manager requires a web browser on the management computer and an Ethernet connection between the FortiGate unit and the management computer.

A web-browser that supports Transport Layer Security 1.2 (or TLS 1.1 if permitted) is required for remote access to the web-based manager when the module is operating in FIPS-CC mode. HTTP access to the web-based manager is not allowed in FIPS-CC mode and is disabled.

Command Line Interface

The FortiGate Command Line Interface (CLI) is a full-featured, text based management tool for the module. The CLI provides access to all of the possible services and configuration options in the module. The CLI uses a console connection or a network (Ethernet) connection between the FortiGate unit 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-CC mode). Telnet access to the CLI is not allowed in FIPS-CC mode and is disabled.

Roles, Services and Authentication

Roles

When configured in FIPS-CC mode, the module provides the following roles:

- Crypto Officer
- Network User

The Crypto Officer role is initially assigned to the default 'admin' operator account. The Crypto Officer role has read-write-execute access to all of the module's administrative services. The initial Crypto Officer can create additional operator accounts. These additional accounts are assigned the Crypto Officer role and can be assigned a range of read-write-execute or read only access permissions including the ability to create operator accounts.

The modules also provide a Network User role for end-users (Users). Network Users can make use of the encrypt/decrypt services, but cannot access the modules for administrative purposes.

The module does not provide a Maintenance role.

FIPS Approved Services

The following tables detail the types of FIPS approved services available to each role in each mode of operation, the types of access for each role and the Keys or CSPs they affect.

The access types are abbreviated as follows:

Read Access	R
Write Access	W
Execute Access	E

Table 21: Services available to Crypto Officers

Service	Access	Key/CSP
connect to module locally using the console port	WE	N/A
connect to module remotely using TLS*	WE	Diffie-Hellman Keys, EC Diffie Hellman Keys,TLS Premaster Secret, TLS Master Secret, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Integrity Key, and HTTPS/TLS Session Encryption Key, DRBG v and key values, DRBG Output, DRBG Seed, Entropy String, TLS Server Signatures

Service	Access	Key/CSP
connect to module remotely using SSH*	WE	Diffie-Hellman Keys, SSH Server/Host Key, SSH Session Authentication Key, SSH Session Encryption Key, DRBG v and key values, DRBG Output, DRBG Seed, Entropy String
authenticate to module	WE	Crypto Officer Password
show system status	N/A	N/A
show FIPS-CC mode enabled/disabled (console/CLI only)	N/A	N/A
enable FIPS-CC mode of operation (console only)	WE	Configuration Integrity Key
key zeroization	W	All Keys
execute factory reset (disable FIPS-CC mode, console/CLI only)	W	N/A
execute FIPS-CC on-demand self-tests (console only)	E	Configuration Integrity Key, Firmware Integrity Key
add/delete crypto officers and network users	WE	Crypto Officer Password, Network User Password
set/reset crypto officers and network user passwords	WE	Crypto Officer Password, Network User Password
backup/restore configuration file	RWE	Configuration Encryption Key, Configuration Backup Key
read/set/delete/modify module configuration*	N/A	N/A
execute firmware update	WE	Firmware Update Key
read log data	N/A	N/A
delete log data (console/CLI only)	N/A	N/A
execute system diagnostics (console/CLI only)	N/A	N/A
enable/disable alternating bypass mode	N/A	N/A
read/set/delete/modify IPsec/SSL VPN configuration*	W	IPsec: IPsec Manual Authentication Key, IPsec Manual Encryption Key, IKE Pre-Shared Key, IKE RSA Key, IKE ECDSA Key, Diffie-Hellman Keys, EC Diffie-Hellman Keys SSL: HTTPS/TLS Server/Host Key, HTTPS/TLS Session Integrity Key, HTTPS/TLS Session Encryption Key
read/set/modify HA configuration	WE	HA Password, HA Encryption Key

Service	Access	Key/CSP
log offloading to remote FortiAnalyzer device*	E	OFTP Client Key, Diffie-Hellman Keys, EC Diffie-Hellman Keys, TLS Premaster Secret, TLS Master Secret, HTTPS/TLS Session Integrity Key, HTTPS/TLS Session Encryption Key, HTTPS/TLS Server/Host Key, DRBG v and key values, DRBG Output, DRBG Seed, Entropy String
generate CSR with RSA or ECDSA	WE	RSA keys, ECDSA keys

Table 22: Services available to Network Users in FIPS-CC mode

Service/CSP	Access	Key/CSP
connect to module remotely using TLS*	WE	Diffie-Hellman Keys, EC Diffie-Hellman Keys, TLS Premaster Secret, TLS Master Secret, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Integrity Key, HTTPS/TLS Session Encryption Key, DRBG v and key values, DRBG Output, DRBG Seed, Entropy String, TLS Server Signatures
authenticate to module	WE	Network User Password
IPsec VPN controlled by firewall policies*	E	IPsec: IPsec Manual Authentication Key, IPsec Manual Encryption Key, IPsec Session Authentication Key, IPsec Session Encryption Key, IKE Pre-Shared Key, IKE RSA Key, IKE ECDSA Key, IKE SKEYSEED, IKE Authentication Key, IKE Key Generation Key, IKE Session Encryption Key, Diffie-Hellman Keys, EC Diffie-Hellman Keys
SSL VPN controlled by firewall policies*	E	Network User Password, Diffie-Hellman Keys, EC Diffie-Hellman Keys, TLS Premaster Secret, TLS Master Secret, HTTPS/TLS Server/Host Key, HTTPS/TLS Session Integrity Key, HTTPS/TLS Session Encryption Key, DRBG v and key values, DRBG Output, DRBG Seed, Entropy String

Non-FIPS Approved Services

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

- Configuration backups using password protection
- L2TP and PPTP VPN
- Services marked with an asterisk (*) in Tables 21 and 22 are considered non-approved when using the following algorithms:
  - Non-compliant-strength Diffie-Hellman

The above services shall not be used in the FIPS approved mode of operation.

Authentication

The module implements identity based authentication. Crypto Officers must authenticate with a user-id and password combination to access the modules remotely or locally via the console. Remote Crypto Officer authentication is done over HTTPS (TLS) or SSH. The password entry feedback mechanism does not provide information that could be used to guess or determine the authentication data.

Authentication at level 3 is only applicable when identity-based authentication is enforced for the User role.

By default, Network User access to the modules is based on firewall policy and authentication by IP address or fully qualified domain names. Network Users can optionally be forced to authenticate to the modules using a username/password combination to enable use of the IPsec VPN encrypt/decrypt or bypass services. For Network Users invoking the SSL-VPN encrypt/decrypt services, the modules support authentication with a user-id/password combination. Network User authentication is done over HTTPS and does not allow access to the modules for administrative purposes.

The minimum password length is 8 characters when in FIPS-CC mode (maximum password length is 128 characters) chosen from the set of ninety four (94) characters. New passwords are required to include 1 uppercase character, 1 lowercase character, 1 numeric character, and 1 special character. The odds of guessing a password are 1 in 3,346,172,314,938,369 which is significantly lower than one in a million.

Note that Crypto Officer authentication over HTTPS/SSH and Network User authentication over HTTPS are subject to a limit of 3 failed authentication attempts in 1 minute; thus, the maximum number of attempts in one minute is 3. Therefore the probability of a success with multiple consecutive attempts in a one-minute period is 3 in 3,346,172,314,938,369 which is less than 1/100,000.

Crypto Officer authentication using the console is not subject to a failed authentication limit, but the number of authentication attempts per minute is limited by the bandwidth available over the serial connection which is a maximum of 115,200 bps which is 6,912,000 bits per minute. An 8 byte password would have 64 bits, so there would be no more than 108,000 passwords attempts per minute. Therefore the probability of success would be 1/({3,346,172,314,938,369}/108,000) which is less than 1/100,000.

For Network Users invoking the IPsec VPN encrypt/decrypt services, the module acts on behalf of the Network 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: IPsec manual authentication key, IKE pre-shared key, IKE RSA key (RSA certificate) or IKE ECDSA key (ECDSA certificate). The odds of guessing the authentication key for each IPsec method is:

- 1 in 16^40 for the IPsec Manual Authentication key (based on a 40 digit, hexadecimal key)
- 1 in 94^8 for the IKE Pre-shared 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)
- 1 in 2^128 for the IKE ECDSA Key (based on a P-256 curve ECDSA key size)

A gigabit ethernet connection is 1,048,576,000 bits per second which is 62,914,560,000 bits per minute. An 8-byte key would have 64 bits, so there could be no more than 983,040,000 password attempts per minute. Therefore, the minimum odds of guessing the IKE Preshared key for IPSec within a one-minute period is 1 in 94^8/983,040,000 which is less than 1 in 100,000. Similarly, for the IPsec Manual Authentication key, the minimum odds of Network Users guessing the key within a minute would be 1 in 16^40/393,216,000. Guessing the IKE RSA key within a minute would be 1 in 2^112/561,737,143. Guessing the IKE ECDSA key within a minute would be 1 in 2^128/491,520,000.

Physical Security

The modules meet FIPS 140-2 Security Level 2 requirements by using production grade components and an opaque, sealed enclosure. Access to the enclosure is restricted through the use of tamper-evident seals to secure the overall enclosure. The tamper-evident seals shall be installed for the module to operate in a FIPS Approved mode of operation. All Networking devices need tamper-evident seals to meet the FIPS 140-2 Level 2 Physical Security requirements.

The seals are red wax/plastic with black lettering that reads “Fortinet Security Seal”.

The tamper seals are not applied at the factory prior to shipping. It is the responsibility of the Crypto Officer to apply the seals before use to ensure full FIPS 140-2 compliance. Once the seals have been applied, the Crypto Officer must develop an inspection schedule to verify that the external enclosure of the modules and the tamper seals have not been damaged or tampered with in any way. Upon viewing any signs of tampering, the Crypto Officer must assume that the device has been fully compromised. The Crypto Officer is required to zeroize the cryptographic module by following the steps in the Key Zeroization section of the SP.

The Crypto Officer is responsible for securing and controlling any unused seals. The Crypto Office is also responsible for the direct control and observation of any changes to the modules such as reconfigurations where the tamper-evident seals are removed or installed to ensure the security of the module is maintained during such changes and ensuring the module is returned to a FIPS approved state.

The surfaces should be cleaned with 99% Isopropyl alcohol to remove dirt and oil before applying the seals. Ensure the surface is completely clean and dry before applying the seals. If a seal needs to be re-applied, completely remove the old seal and clean the surface with an adhesive remover before following the instructions for applying a new seal.

Seals can be requested through your Fortinet sales contact. Reference‘FIPS-SEAL-RED’ when requesting the seals. Specify the number of seals required based on the specific model as described below:

- The FortiGate-40F uses two seals to secure the external enclosure (see Figure 18).
- The FortiGate-60F/61F and FortiWiFi-60F/61F use three seals to secure the external enclosure (see Figure 19).
- The FortiGateRugged-60F uses one seal to secure the external enclosure (see Figure 20).
- The FortiGate-80F/81F use one seal to secure the external enclosure (Figure 21).
- The FortiGate-100F/101F use one seal to secure the external enclosure (Figure 22).
- The FortiGate-200F/201F use one seal to secure the external enclosure (Figure 23).
- The FortiGate-600E/601E use one seal to secure the external enclosure (Figure 24).
- The FortiGate-1100E/1101E use three seals to secure the external enclosure (Figure 25 and 26).
- The FortiGate-1800F/1801F and 2600F/2601F use three seals seal to secure the external enclosure (Figure 27 and 28).
- The FortiGate-3300E/3301E use three seals to secure the external enclosure (Figure 29, 30 and 31).
- The FortiGate-3400E/3401E and 3600E/3601E use three seals to secure the external enclosure (Figure 32 and 33).
- The FortiGate-4200F/4201F and 4400F/4401F use 4 seals to secure the external enclosure (Figure 34, 35 and 36).
- The FortiGate-6300F/6301F/6500F/6501F use three seals to secure the external enclosure (Figure 37 and 38)

Figure 18 - FortiGate-40F external enclosure seals, bottom

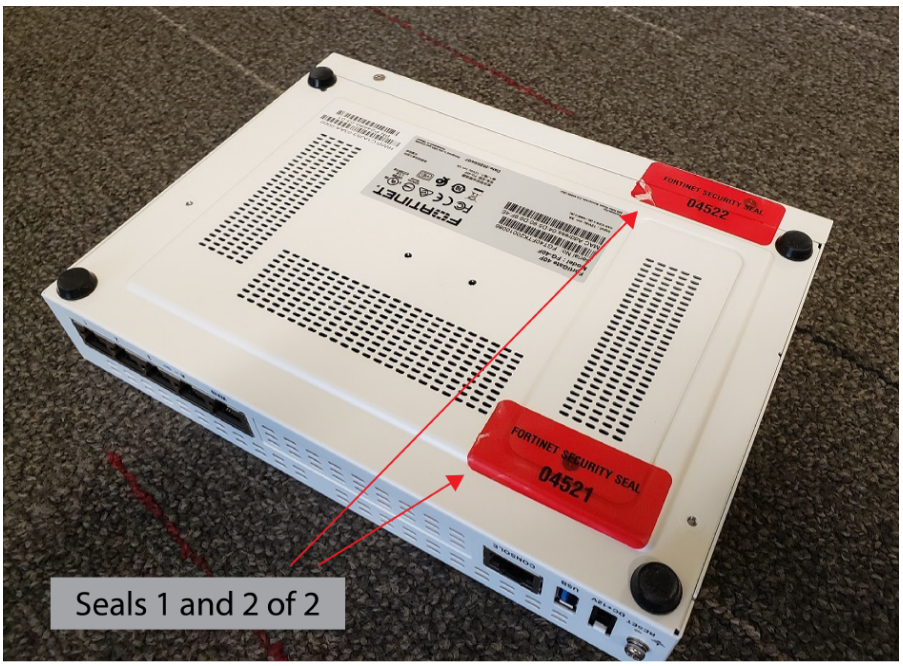

Figure 19 - FortiGate 60F/61F and FortiWiFi-60F/61F external enclosure seals, bottom

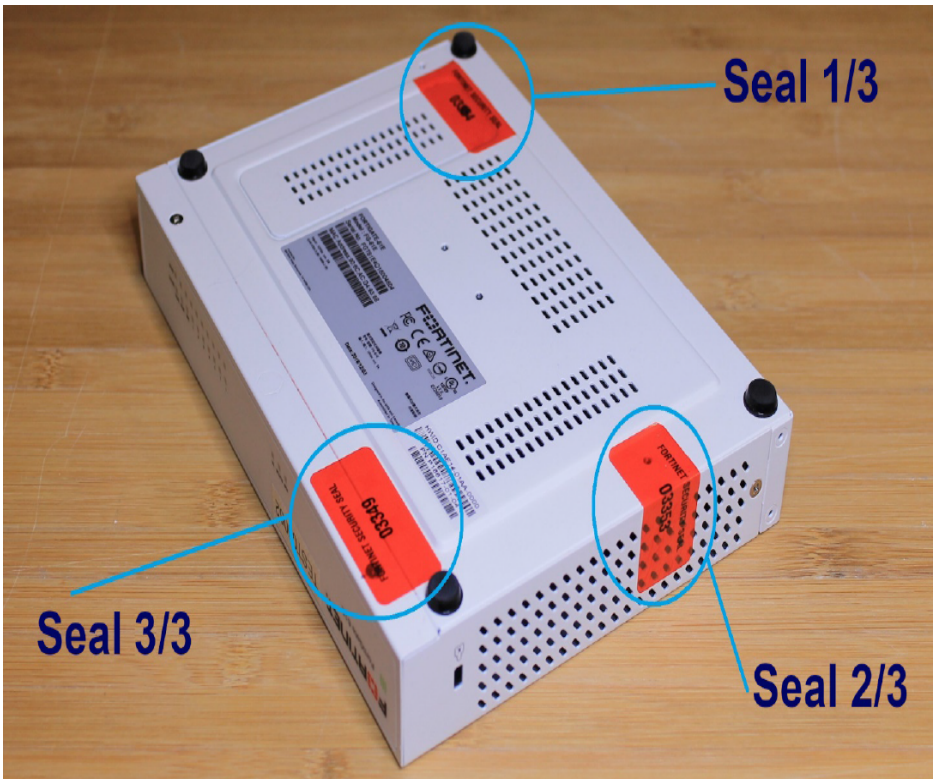

Figure 20 - FortiGateRugged-60F external enclosure seal, bottom

Figure 21 - FortiGate-80F/81F external enclosure seal, bottom

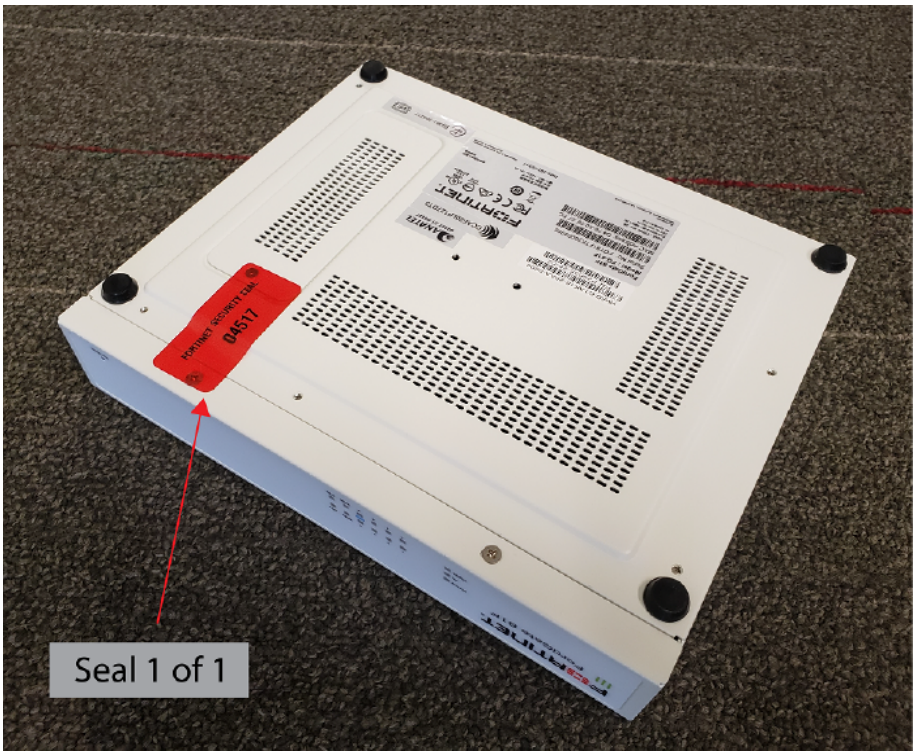

Figure 22 - FortiGate-100F/101F

Figure 23 - FortiGate-200F/201F

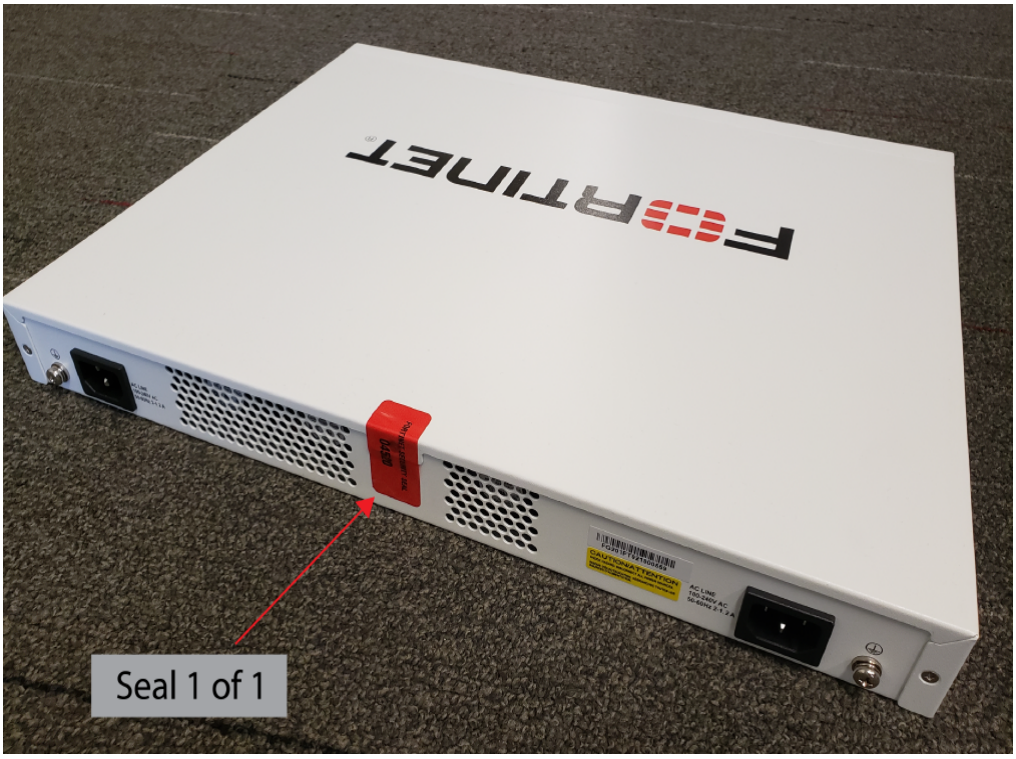

Figure 24 - FortiGate-600E/601E

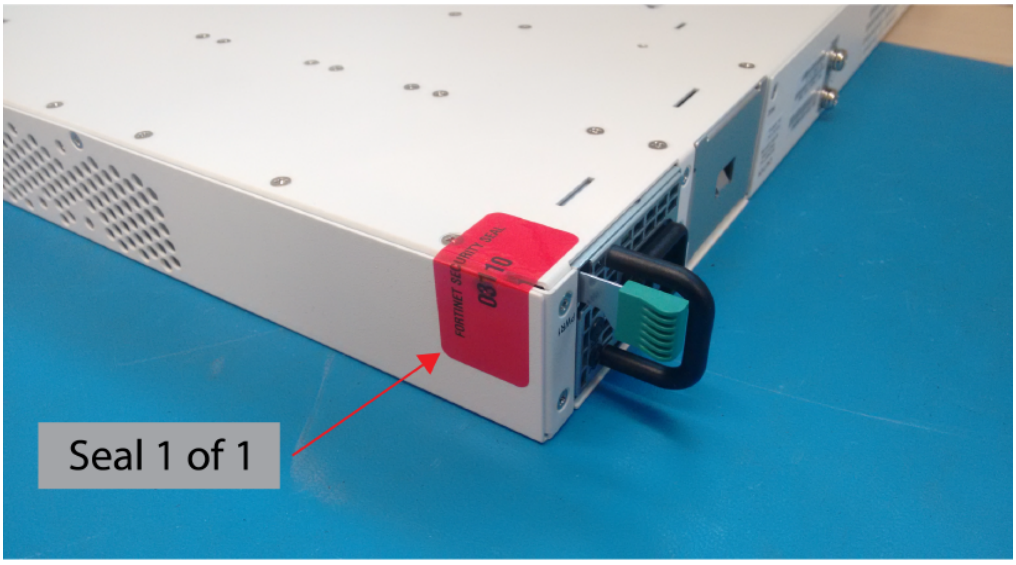

Figure 25 - FortiGate-1100E/1101E external enclosure seal, top, left side

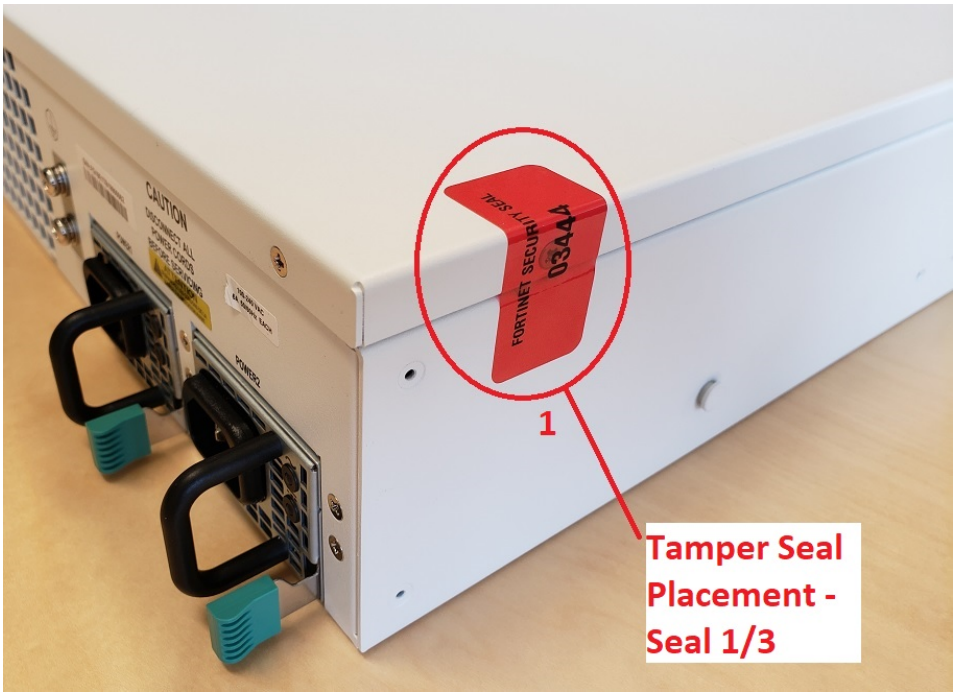

Figure 26 - FortiGate-1100E/1101E external enclosure seals, bottom, rear

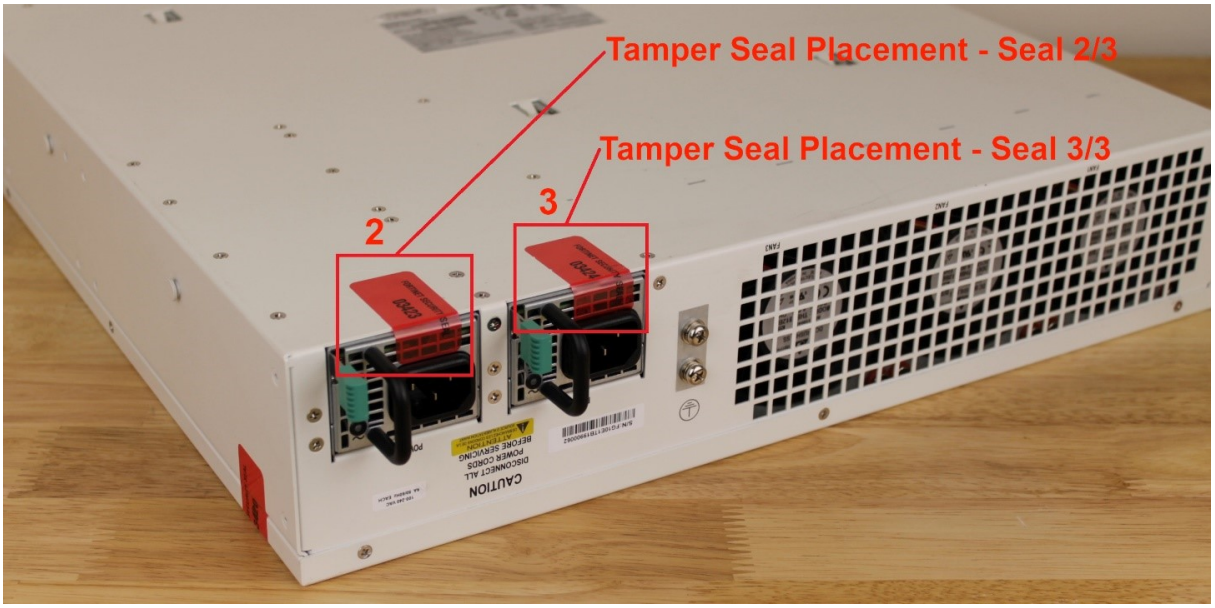

Figure 27 - FortiGate-1800F/1801F and 2600F/2601F external enclosure seal, rear, top

Figure 28 - FortiGate-1800F/1801F and 2600F/2601F power supply seals, rear

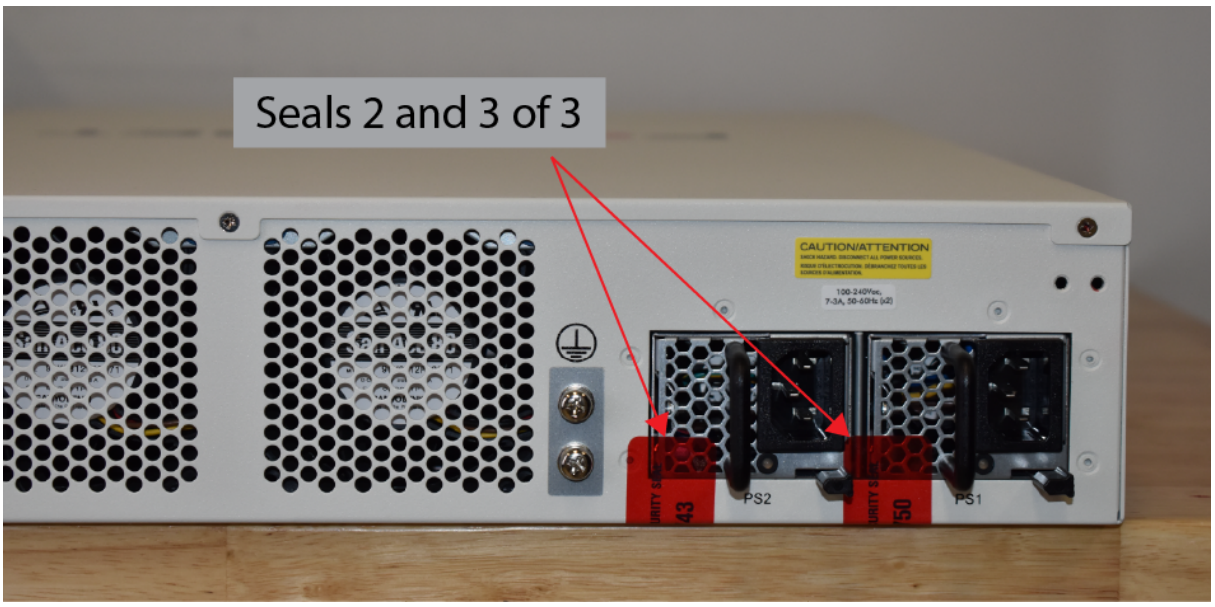

Figure 29 - FortiGate-3300E/3301E external enclosure seal, left side, top

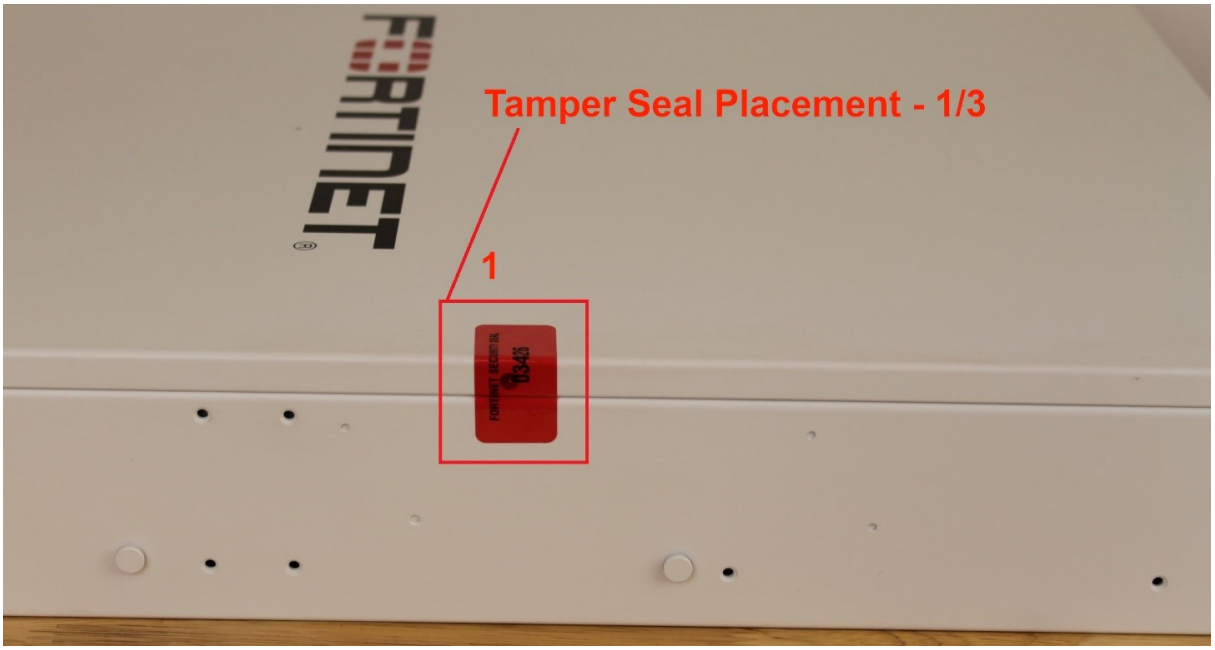

Figure 30 - FortiGate-3300E/3301E external enclosure seal, left side, back

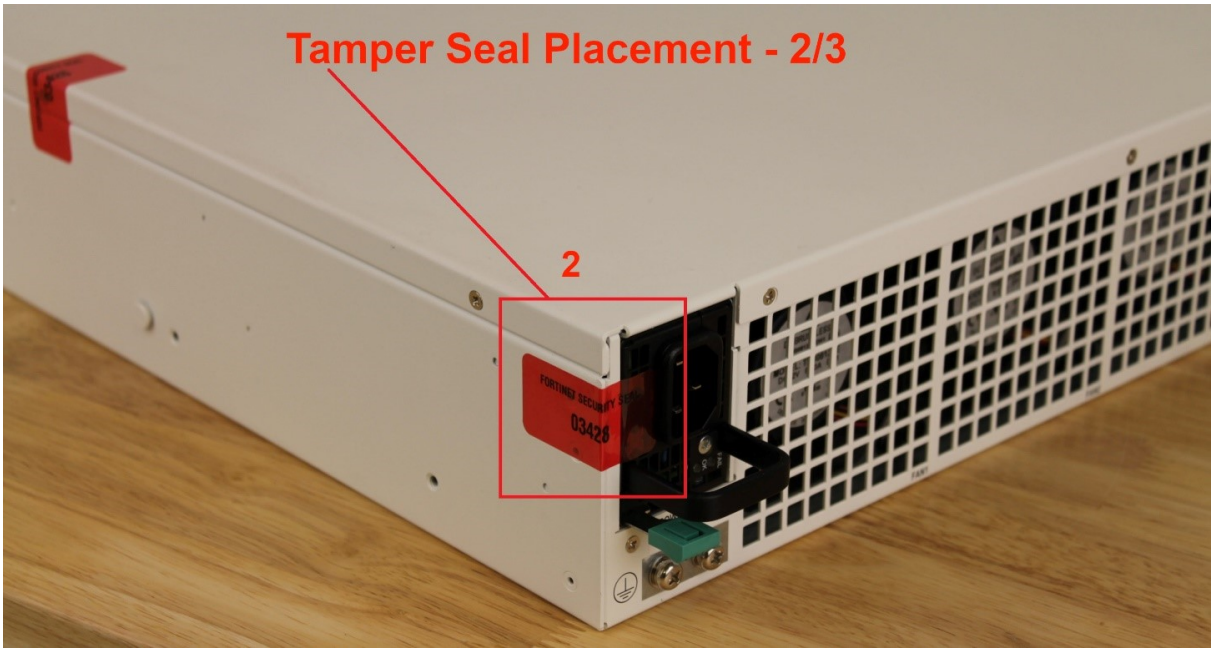

Figure 31 - FortiGate-3300E/3301E external enclosure seal, right side, back

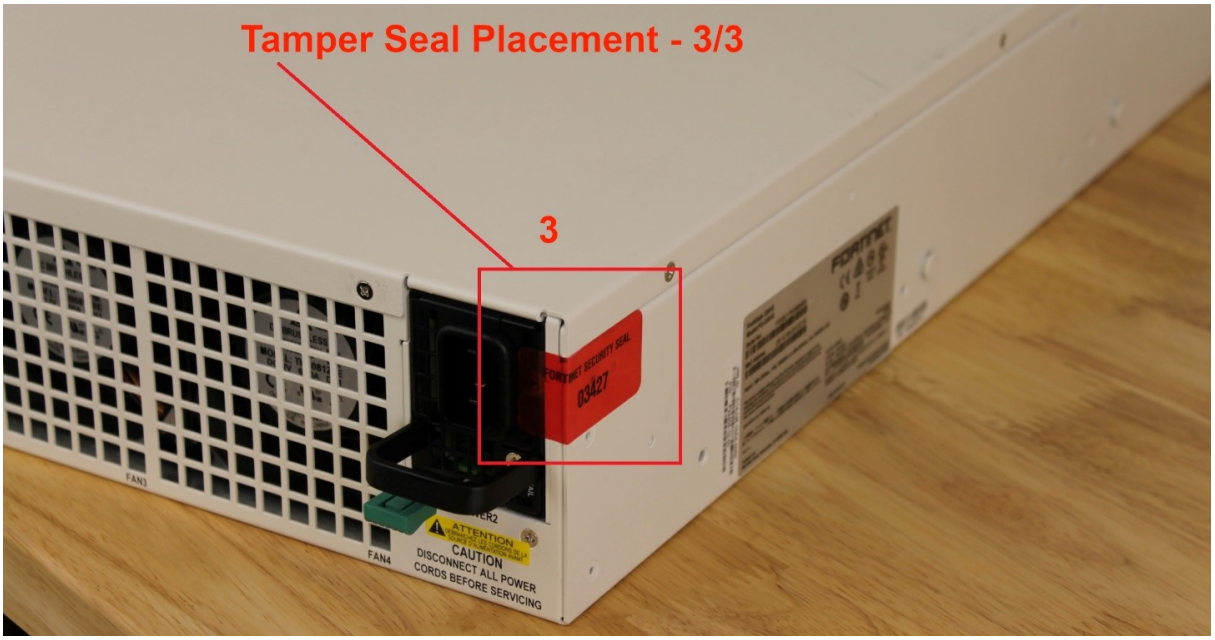

Figure 32 - FortiGate-3400/3401E and 3600E/3601E external enclosure seal, back, left side

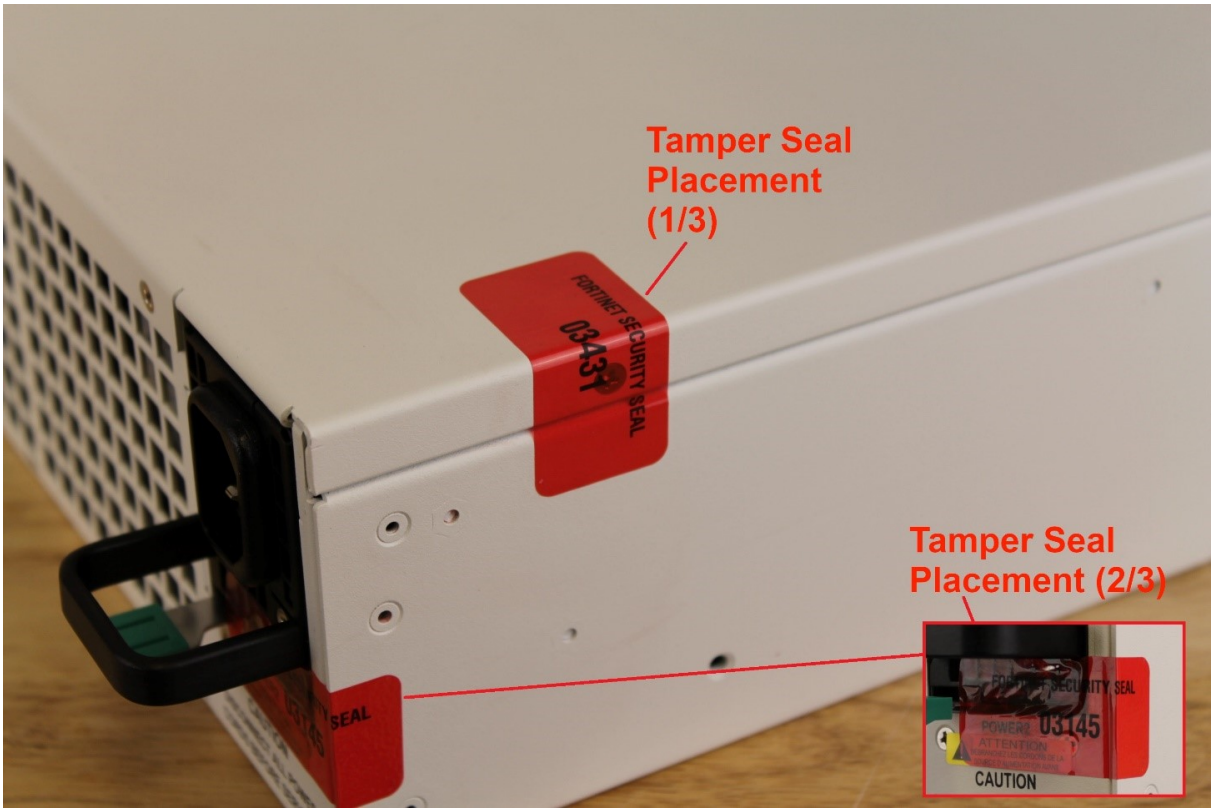

Figure 33 - FortiGate-3400E/3401E and 3600E/3601E external enclosure seal, back, right side

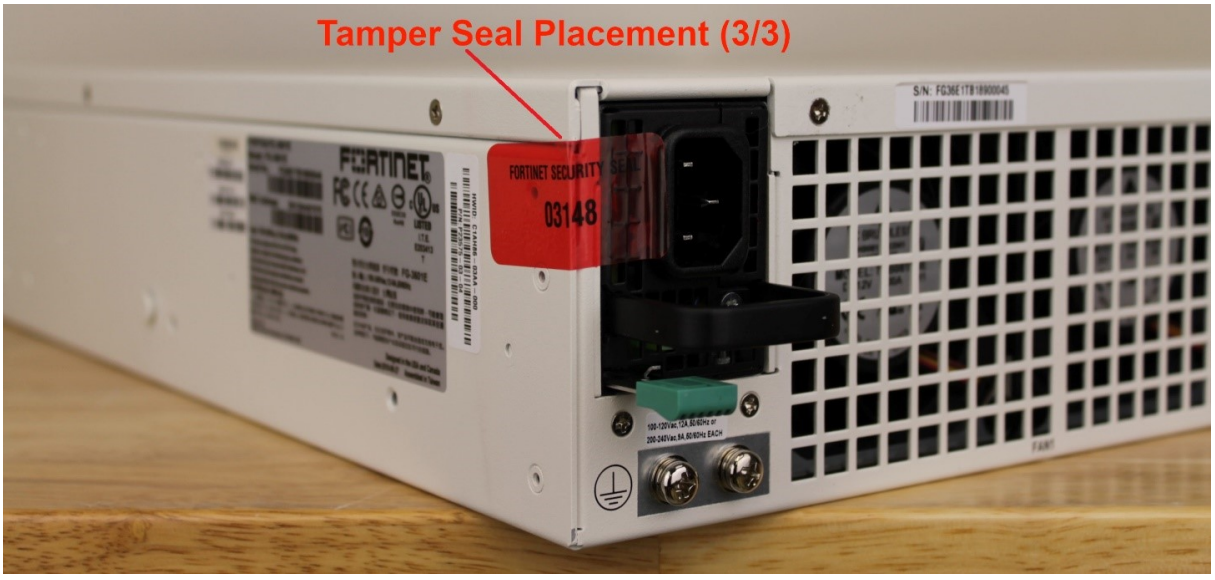

Figure 34 - FortiGate-4200F/4201F and 4400F/4401F external enclosure seal, back, right side

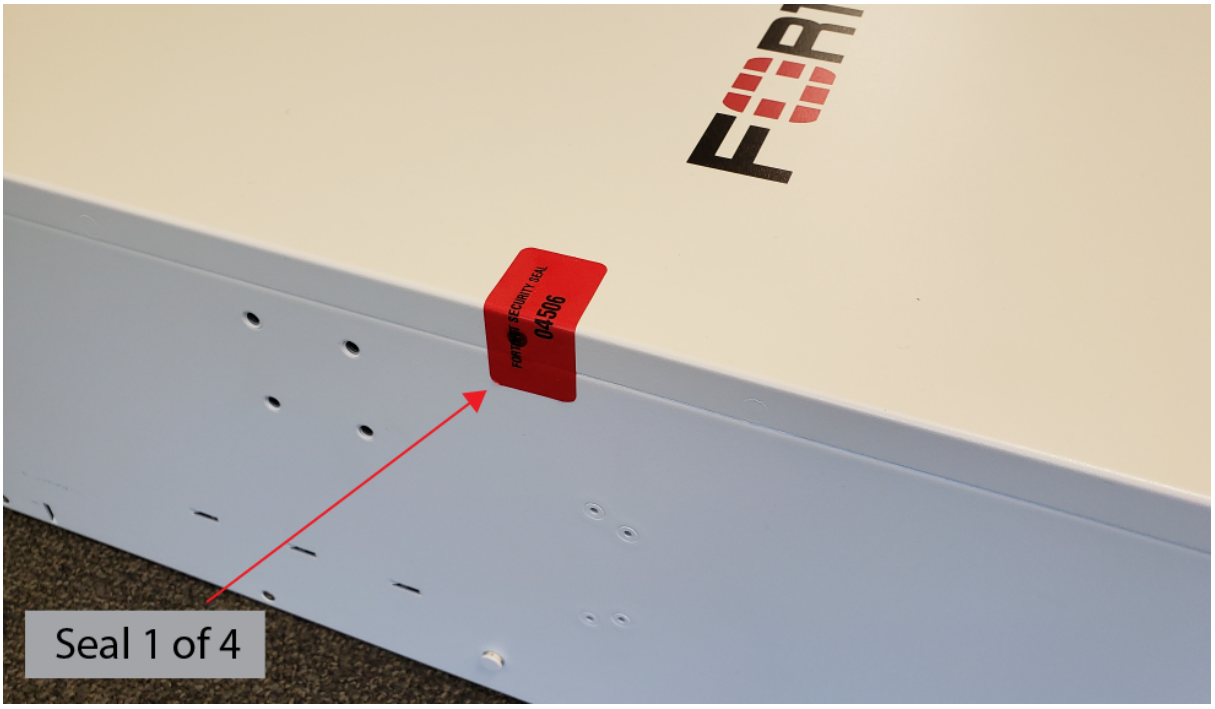

Figure 35 - FortiGate-4200F/4201F external enclosure seals, back

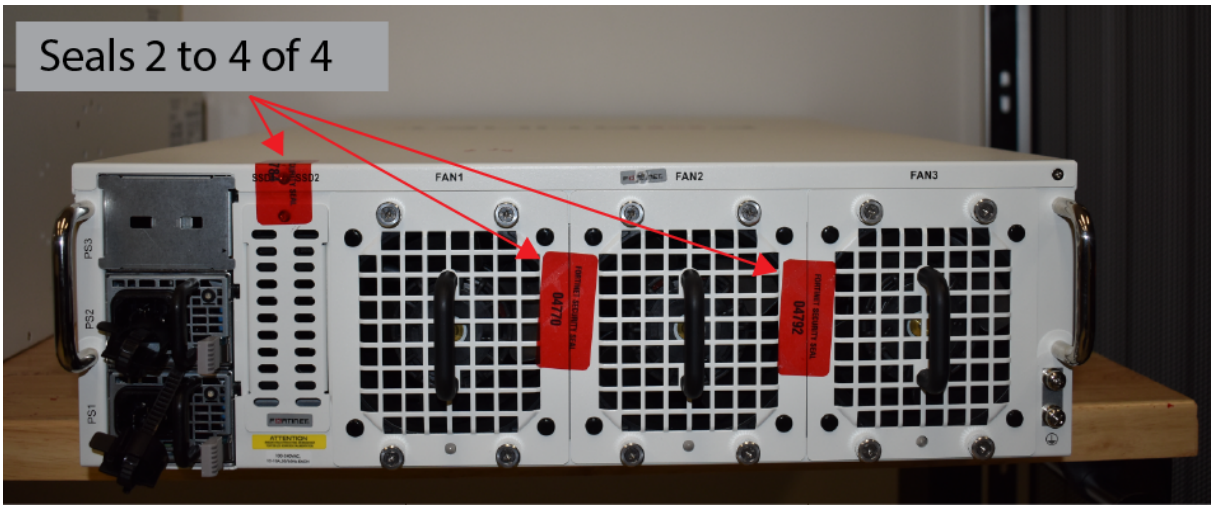

Figure 36 - FortiGate-4400F/4401F external enclosure seal, back

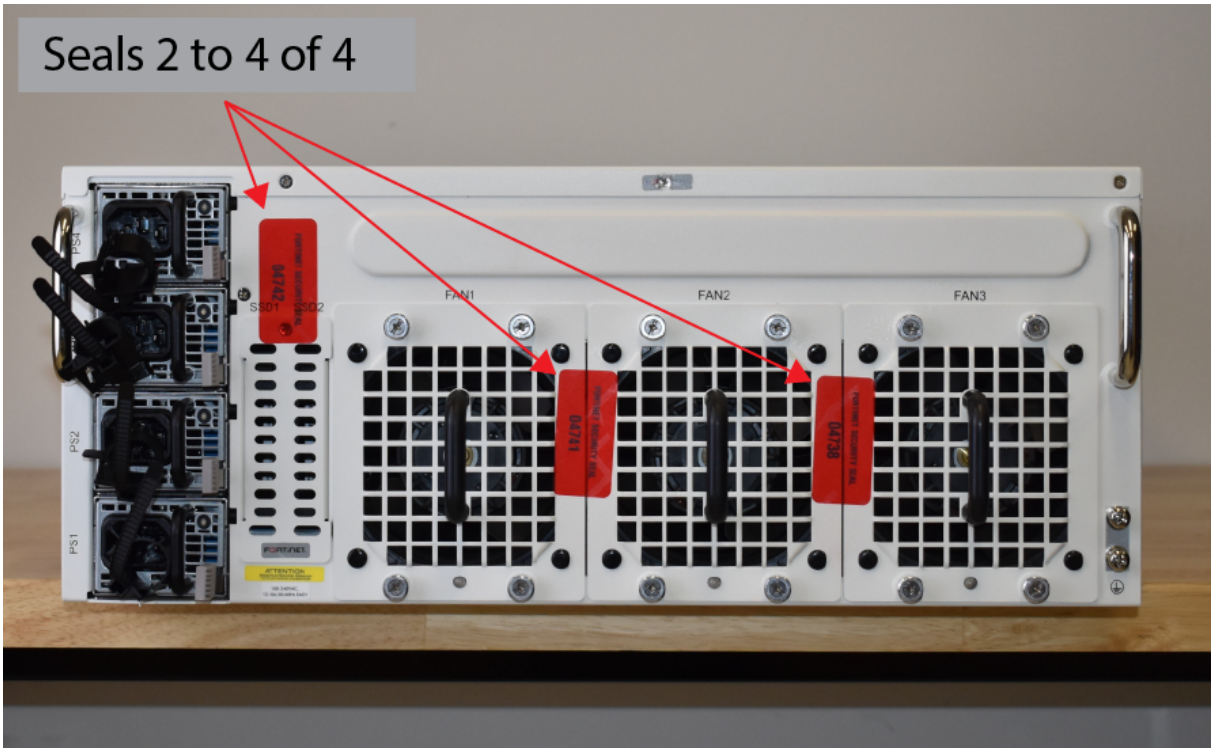

Figure 37 - FortiGate-6300F/6301F/6500F/6501F external enclosure seal 1, top, rear

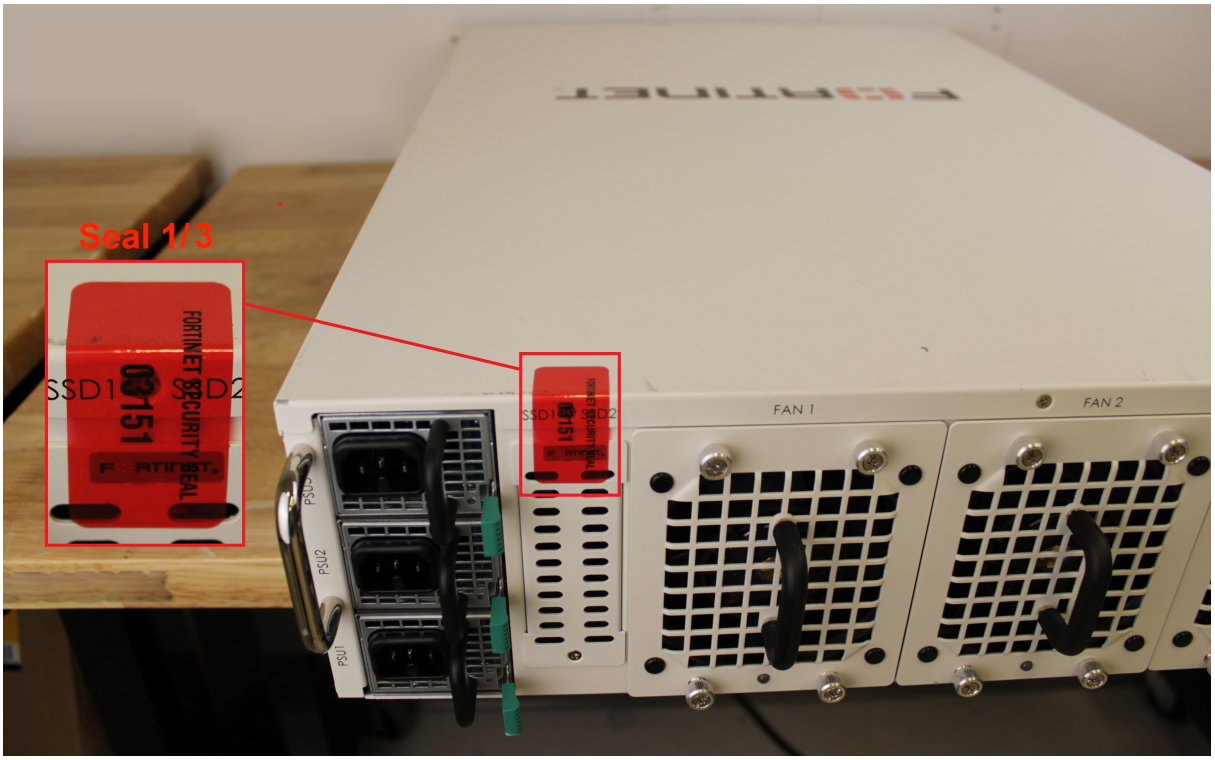

Figure 38 - FortiGate-6300F/6301F/6500F/6501F external enclosure seal 2 and 3, top, rear

Operational Environment

The modules consist of the combination of the FortiOS operating system and the FortiGate appliances. The FortiOS operating system can only be installed, and run, on a FortiGate appliance. The FortiOS operating system provides a proprietary and non-modifiable operating system.

Cryptographic Key Management

Random Number Generation

The modules use a firmware based, deterministic random bit generator (DRBG) that conforms to NIST Special Publication 800-90A.

Entropy

All modules (except the FortiGate-6300F/6301F/6500F/6501F modules) use either a Fortinet CP9 or CP9XLite security processor as the entropy source.

The FortiGate-6300F/6301F/6500F/6501F modules use both the Fortinet CP9 Security Processor and an entropy token (Araneus Alea II) as entropy sources. The entropy token provides entropy to the main PCB. The CP9 Security Processors provide entropy to each of the processor cards. The entropy token is not included in the boundary of the module and therefore no assurance can be made for the correct operation of the entropy token nor is there a guarantee of stated entropy.

In all cases the entropy source(s) seed the DRBG during the modules' boot process and periodically reseed the DRBG.

Entropy Strength

The entropy loaded into the approved AES-256 bit DRBG is 256 bits. The entropy source is over-seeded and then an HMAC-SHA-256 post-conditioning component (as per section 3.1.5.1.1 and/or 3.1.5.1.2 of SP 800-90B) is applied.

Reseed Period

The RBG is seeded from the Entropy Token or Security Processor during the boot process and then reseeded periodically. The default reseed period is once every 24 hours (1440 minutes) and is configurable (1 to 1440 minutes). The entropy token must be installed to complete the boot process and to reseed the RBG.

Key Zeroization

The zeroization process must be performed under the direct control of the operator. The operator must be present to observe that the zeroization method has completed successfully.

All keys and CSPs are zeroized by erasing the module's boot device and then power cycling the FortiGate unit. To erase the boot device, execute the following command from the CLI:

```
execute erase-disk <boot device>
```

The boot device ID may vary depending on the FortiGate module. Executing the following command will output a list of the available internal disks:

```
execute erase-disk ?
```

Algorithms

Table 23: FIPS approved algorithms

Algorithm	NIST Cert Number
CTR DRBG (NIST SP 800-90A) with AES 256 bits	A2225, A2229
AES in CBC mode (128, 192, and 256 bits)	A2225, A2229, A2240, A2242, A2269, A2270
AES in GCM mode (128, 256 bits)	A2225, A2229, A2240, A2242, A2269, A2270
SHA-1	A2225, A2229, A2240, A2242, A2269, A2270
SHA-224	A2269, A2270
SHA-256	A2269, A2270
SHA-384	A2269, A2270
SHA-512	A2269, A2270
HMAC SHA-1	A2225, A2229, A2240, A2242, A2269, A2270
HMAC SHA-224	A2269, A2270

Algorithm	NIST Cert Number
HMAC SHA-256	A2269, A2270
HMAC SHA-384	A2269, A2270
HMAC SHA-512	A2269, A2270
RSA PKCS 1.5 Key Pair Generation: 2048 and 3072-bit Signature Generation: 2048 and 3072-bit Signature Verification: 1024, 2048 and 3072-bit For legacy use, the module supports 1024-bit RSA keys and SHA-1 for signature verification	A2240, A2242, A2269, A2270
RSA PSS Signature Generation: 2048 3072, and 4096-bit Signature Verification: 1024, 2048, 3072 and 4096-bit	A2269, A2270
ECDSA Key Pair Generation: curve P-256	A2269, A2270
ECDSA Key Pair Generation: curve P-384	A2269, A2270
ECDSA Key Pair Generation: curve P-521	A2269, A2270
ECDSA Signature Generation: curves P-256, P-384 and P-521	A2269, A2270
ECDSA Signature Verification: curves P-256, P-384 and P-521	A2269, A2270
ECDSA Signature Generation: curve P-256	A2240, A2242
ECDSA Signature Verification: curve P-256	A2240, A2242

Algorithm	NIST Cert Number
CVL (KDF SSH) - AES 128 bit-, AES-192 bit, AES 256 bit - CBC (using SHA1, SHA-256)	A2269, A2270
CVL (KDF TLS 1.1 and 1.2 (using SHA-256, SHA-384, SHA-512))	A2269, A2270
CVL (KDF TLS 1.2 RFC7627(using SHA-256, SHA-384,SHA-512))	A2269, A2270
CVL (KDF IKE v1 (using SHA-1, SHA2-256, SHA2-384, SHA2-512))	A2269, A2270
CVL (KDF IKE v2 (using SHA-1, SHA2-256, SHA2-384, SHA2-512))	A2269, A2270
KAS-ECC-SSC SP800-56Ar3	A2269, A2270
KAS-FFC-SSC SP800-56Ar3	A2269, A2270
CVL (KDF SNMP) - Password length: 64 - 8192	A2269, A2270
ENT (P)	N/A

KTS (AES Certs. #A2269 and #A2270 [128, 256-bit AES-CBC] and HMAC Certs. #A2269 and #A2270; key establishment methodology provides 128 or 256 bits of encryption strength);

KTS (AES Certs. #A2269 and #A2270 [128, 256-bit AES-GCM]; key establishment methodology provides 128 or 256 bits of encryption strength);

KAS-ECC-SSC provides between 128 and 256 bits of encryption strength;

KAS-FFC-SSC provides 112 bits of encryption strength;

KAS (KAS-SSC Certs. #A2269 and #A2270, CVL Certs. #A2269 and #A2270);

For AES GCM IPsec/IKEv2, RFC 7296 is used to establish the shared secret SKEYSEED from which the AES GCM encryption keys are derived;

For ECDSA Signature Generation & Signature Verification, only curve P-256 is ACVP tested for models using the SOC4 processor.

Table 24: Non-FIPS approved algorithms. Not Allowed.

Algorithm
Diffie-Hellman is non-compliant when keys less than 2048 bits are used, since such keys do not provide the minimum required 112 bits of encryption strength.
The module implements the following non-NIST recommended curves: Curve25519 and Curve448. Until such time as NIST SP 800-186 is published, these curves remain non-recommended by NIST. The module may employ these curves for TLS interoperability; however, it is the responsibility of the operator to utilize cipher suites which contain only NIST Approved cryptography.

Note that the IKE, SSH, SNMP, and TLS protocols, other than the KDF, have not been tested by the CMVP or CAVP as per FIPS 140-2 Implementation Guidance D.11.

The module is compliant to IG A.5: GCM is used in the context of TLS and IKEv2/IPSec.

For TLS, The GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with SP 800-52 and in accordance with RFC 5246 for TLS key establishment. The AES GCM IV generation is in compliance with RFC 5288 and shall only be used for the TLS protocol version 1.2 to be compliant with FIPS140-2 IG A.5, Option 1 (“TLS protocol IV generation”); thus, those cipher suites implemented in the module that utilize AES-GCM are consistent with those specified in Section 3.3.1.1.2 of [SP800-52, Rev2]. During operational testing, the module was tested against an independent version of TLS and found to behave correctly.

For IPsec/IKEv2, the GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with RFCs 4106 and 7296. During operational testing, the module was tested against an independent version of IPsec with IKEv2 and found to behave correctly.

For SSH, the module is compliant with RFC 4252, 4253, and 5647.

In case the module’s power is lost and then restored, the key used for the AES GCM encryption or decryption shall be re-distributed. In addition, when the nonce_explicit part of the IV exhausts the maximum number of values for a session key a handshake is triggered to establish a new encryption key.

There are algorithms, modes, and keys that have been CAVs tested but are not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in the above tables are used by the module.

Note that the TLS KDF has only been CAVP tested for TLS 1.2 (and not TLS 1.1) for the FortiGate-6300F/6301F/6500F/6501F running FIPS-CC-64-3 firmware, and the FortiGate-40F/60F/61F/80F/81F/100F/101F, FortiGateRugged-60F, FortiWifi-60F/61F running FIPS-CC-70-3 firmware. For the aforementioned models, TLS 1.2 is the only TLS version that shall be used in the approved mode.

Cryptographic Keys and Critical Security Parameters

The following table lists all of the cryptographic keys and critical security parameters used by the modules. The following definitions apply to the table.

Table 25: Cryptographic Keys and Critical Security Parameters used in FIPS-CC mode

Key or CSP	Generation	Storage	Usage	Zeroization
Entropy string	Entropy Token or ENT (P)	Boot device Plain-text	Input string for the entropy pool	By erasing the Boot device and power cycling the module
DRBG seed	Internally generated	SDRAM SHA-256 hash	256 bit seed used by the DRBG (output from entropy token or ENT (P))	By erasing the Boot device and power cycling the module
DRBG output	Internally generated	SDRAM Plain-text	Random numbers used in cryptographic algorithms (256 bits)	By erasing the Boot device and power cycling the module
DRBG v and key values	Internally generated	SDRAM Plain-text	Internal state values for the DRBG 128 and 256	By erasing the Boot device and power cycling the module

Key or CSP	Generation	Storage	Usage	Zeroization
IPsec Manual Authentication Key	Electronic key entry	Boot device AES encrypted	Used as IPsec Session Authentication Key	By erasing the Boot device and power cycling the module
IPsec Manual Encryption Key	Electronic key entry	SDRAM Plain-text	Used as IPsec Session Encryption Key using AES (128, 256 bit)	By erasing the Boot device and power cycling the module
IPsec Session Authentication Key	Internally generated using DRBG	SDRAM Plain-text	IPsec peer-to-peer authentication using HMAC SHA-1 or HMAC SHA-256	By erasing the Boot device and power cycling the module
IPsec Session Encryption Key	Internally generated via DH or ECDH KAS	SDRAM Plain-text	VPN traffic encryption/decryption using AES (128, 256 bit)	By erasing the Boot device and power cycling the module
IKE SKEYSEED	Derived via KDF defined in SP800-135 (IKEv2)	SDRAM Plain-text	Used to generate IKE protocol keys	By erasing the Boot device and power cycling the module
IKE Pre-Shared Key	Electronic key entry	Boot device AES encrypted	Used to generate IKE protocol keys	By erasing the Boot device and power cycling the module
IKE Authentication Key	Internally generated using DRBG	SDRAM Plain-text	IKE peer-to-peer authentication using HMAC SHA-1 , -256, -384 or -512	By erasing the boot device and power cycling the module
IKE Key Generation Key	Internally generated using DRBG	SDRAM Plain-text	IPsec SA keying material	By erasing the boot device and power cycling the module
IKE Session Encryption Key	Internally generated via DH or ECDH KAS	SDRAM Plain-text	Encryption of IKE peer-to-peer key negotiation using or AES (128, 256 bit)	By erasing the boot device and power cycling the module
IKE RSA Key	Externally generated	Boot device AES encrypted	RSA private key used in the IKE protocol (2048 and 3072 bit signatures)	By erasing the boot device and power cycling the module

Key or CSP	Generation	Storage	Usage	Zeroization
IKE ECDSA Key	Externally generated	Boot device AES encrypted	ECSDA private key used in the IKE protocol (signatures using P-256, P-384 and P-521 curves)	By erasing the boot device and power cycling the module
Diffie-Hellman Keys	Internally generated using DRBG	SDRAM Plain-text	Key agreement and key establishment (Public key size of 2048 to 8192 bits with Private key size of 224 to 400 bits)	By erasing the boot device and power cycling the module
EC Diffie-Hellman Keys	Internally generated using DRBG	SDRAM Plain-text	Key agreement and key establishment (key pairs on the curves secp256r1, secp384r1 and secp521r1)	By erasing the boot device and power cycling the module
Firmware Update Key	Preconfigured	Boot device Plain-text	Verification of firmware integrity when updating to new firmware versions using RSA public key (firmware load test, 2048 bit signature)	By erasing the boot device and power cycling the module
Firmware Integrity Key	Preconfigured	Boot device Plain-text	Verification of firmware integrity in the firmware integrity test using RSA public key (firmware integrity test, 2048 bit signature)	By erasing the boot device and power cycling the module
TLS Premaster Secret	Internally generated via DH or ECDH KAS	SDRAM Plain-text	HTTPS/TLS keying material	By erasing the boot device and power cycling the module
TLS Master Secret	Internally generated from the TLS Premaster Secret	SDRAM Plain-text	384 bit master key used in the HTTPS/TLS protocols	By erasing the boot device and power cycling the module
HTTPS/TLS Server/Host Key	Preconfigured	Boot device AES encrypted	RSA private key used in the HTTPS/TLS protocols (key establishment, 2048 or 3072 bit)	By erasing the boot device and power cycling the module

Key or CSP	Generation	Storage	Usage	Zeroization
HTTPS/TLS Session Integrity Key	Internally generated using DRBG	SDRAM Plain-text	HMAC SHA-1, -256 or -384 key used for HTTPS/TLS session integrity	By erasing the boot device and power cycling the module
TLS Server Signatures	Preconfigured	Boot device Plain-text	rsa_pkcs1 & rsa_pss_ rsae signatures used in TLS	By erasing the boot device and power cycling the module
HTTPS/TLS Session Encryption Key	Internally generated via DH or ECDH KAS	SDRAM Plain-text	AES (128, 256 bit) key used for HTTPS/TLS session encryption	By erasing the boot device and power cycling the module
SSH Server/Host Key	Preconfigured	Boot device Plain-text	RSA private key used in the SSH protocol (key establishment, 2048 or 3072 bit)	By erasing the boot device and power cycling the module
SSH Session Authentication Key	Internally generated using DRBG	SDRAM Plain-text	HMAC SHA-1 or HMAC SHA-256 key used for SSH session authentication	By erasing the boot device and power cycling the module
SSH Session Encryption Key	Internally generated via DH or ECDH KAS	SDRAM Plain-text	AES (128, 256 bit) key used for SSH session encryption	By erasing the boot device and power cycling the module
Crypto Officer Password	Electronic key entry	Boot device SHA-256 hash	Used to authenticate operator access to the module	By erasing the boot device and power cycling the module
Configuration Integrity Key	Preconfigured	Boot device Plain-text	HMAC SHA-256 hash used for configuration bypass test	By erasing the boot device and power cycling the module
Configuration Encryption Key	Preconfigured	Boot device Plain-text	AES 256 bit key used to encrypt CSPs on the Boot device and in the backup configuration file (except for crypto officer passwords in the backup configuration file)	By erasing the boot device and power cycling the module

Key or CSP	Generation	Storage	Usage	Zeroization
Configuration Backup Key	Preconfigured	Boot device Plain-text	HMAC-SHA-256 key used to hash crypto officer passwords in the backup configuration file	By erasing the boot device and power cycling the unit
Network User Password	Electronic key entry	Boot device AES encrypted	Used to authenticate network user access to the module	By erasing the boot device and power cycling the unit
HA Password	Electronic key entry	Boot device AES encrypted	Used to authenticate FortiGate units in an HA cluster	By erasing the boot device and power cycling the unit
HA Encryption Key	Externally generated	Boot device AES encrypted	Encryption of traffic between units in an HA cluster using AES 128 bit key	By erasing the boot device and power cycling the unit
OFTP Client Key	Externally generated	Boot device AES encrypted	RSA private key used in the OFTP/TLS protocol (key establishment, 2048 bit signature)	By erasing the boot device and power cycling the module
RSA Keys	Internally generated using DRBG	Boot device Plain-text	RSA Key Pair from RSA CSR generation	By erasing the boot device and power cycling the module
ECDSA Keys	Internally generated using DRBG	Boot device Plain-text	ECDSA Key Pair from ECDSA CSR generation	By erasing the boot device and power cycling the module

The Generation column lists all of the keys/CSPs and their entry/generation methods. Electronically entered keys are entered by the operator electronically (as defined by FIPS) using the console or a management computer. Pre-configured keys are set as part of the firmware (hardcoded) and are not operator modifiable.

Externally generated keys are generated outside the module and loaded by the operator electronically and are not compliant with SP 800-133 unless they were generated by another FIPS validated module.

Alternating Bypass Feature

The primary cryptographic function of the module is as a firewall and VPN device. The module implements two forms of alternating bypass for VPN traffic: policy based (for IPsec and SSL VPN) and interface based (for IPsec VPN only).

Policy Based VPN

Firewall policies with IPsec or SSL-VPN mean that the firewall is functioning as a VPN start/end point for the specified source/destination addresses and will encrypt/decrypt traffic according to the policy. Firewall policies with an action of accept mean that the firewall is accepting/sending plaintext data for the specified source/destination addresses.

A firewall policy with an action of accept means that the module is operating in a bypass state for that policy. A firewall policy with IPsec or SSL-VPN means that the module is operating in a non-bypass state for that policy.

Interface Based VPN

Interface based VPN is supported for IPsec only. A virtual interface is created and any traffic routed to the virtual interface is encrypted and sent to the VPN peer. Traffic received from the peer is decrypted. Traffic through the virtual interface is controlled using firewall policies. However, unlike policy based VPN, the action is restricted to Accept or Deny and all traffic controlled by the policy is encrypted/decrypted.

When traffic is routed over the non-virtual interface, the module is operating in a bypass state. When traffic is routed over the virtual interface, the module is operating in a non-bypass state.

In both cases, two independent internal actions must be taken to create a bypass firewall policies.

Key Archiving

The module supports key archiving to a management computer as part of the module configuration file backup. Operator entered keys are archived as part of the module configuration file. The configuration file is stored in plain text, but keys in the configuration file are either AES encrypted using the Configuration Encryption Key or stored as a keyed hash using HMAC SHA-256 using the Configuration Backup Key.

Mitigation of Other Attacks

The module includes a real-time Intrusion Prevention System (IPS) as well as antivirus protection, web content filtering, DNS filtering, application control and data leak prevention. Use of these capabilities is optional.

The FortiOS IPS has two components: a signature based component for detecting attacks passing through the FortiGate appliance and a local attack detection component that protects the firewall from direct attacks. Functionally, signatures are similar to virus definitions, with each signature designed to detect a particular type of attack. The IPS signatures are updated through the FortiGuard IPS service. The IPS engine can also be updated through the FortiGuard IPS service.

FortiOS antivirus protection removes and optionally quarantines files infected by viruses from web (HTTP), file transfer (FTP), and email (POP3, IMAP, and SMTP) content as it passes through the FortiGate modules. FortiOS antivirus protection also controls the blocking of oversized files and supports blocking by file extension. Virus signatures are updated through the FortiGuard antivirus service. The antivirus engine can also be updated through the FortiGuard antivirus service.

FortiOS antispam protection tags (SMTP, IMAP, POP3) or discards (SMTP only) email messages determined to be spam. Multiple spam detection methods are supported including the FortiGuard managed antispam service.

FortiOS web filtering can be configured to provide web (HTTP) content filtering. FortiOS web filtering uses methods such as banned words, address block/exempt lists, and the FortiGuard managed content service.

FortiOS DNS filtering can be configured to provide web content (HTTP/HTTPS) content filtering based on DNS domain lookup. FortiOS DNS filtering uses the FortiGuard DNS database.

FortiOS application control can detect and take action against network traffic depending on the application generating the traffic. FortiOS application control uses the FortiGuard application control database.

FortiOS data leak prevention is used to prevent sensitive data from leaving your network. After sensitive data patterns are defined, data matching the patterns will either be blocked or logged and then allowed.

Whenever a IPS, antivirus, or other filtering event occurs, the modules can record the event in the log and/or send an alert email to an operator.

For complete information refer to the FortiGate Installation Guide for the specific module in question, the FortiGate Administration Guide and the FortiGate IPS Guide.

Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

The modules comply with EMI/EMC requirements for Class A devices as specified by Part 15, Subpart B, of the FCC rules. The following table lists the specific lab and report information for the modules.

FCC Report Information

Module	Lab Information	FCC Report Number
FG-40F	International Standards Laboratory No. 120 Lane 180, Hsin Ho Rd., Lung-Tan Dist., Tao Yuan City 325, Taiwan	ISL-19LE556FB
FG-60F/61F	International Standards Laboratory No. 120 Lane 180, Hsin Ho Rd., Lung-Tan Dist., Tao Yuan City 325, Taiwan	ISL-19LE636FB
FWF-60F/61F	International Standards Laboratory No. 120 Lane 180, Hsin Ho Rd., Lung-Tan Dist., Tao Yuan City 325, Taiwan	ISL-19LE636FB
FGR-60F	DEKRA Testing and Certification Co., Ltd. No. 5-22, Ruishukeng, Linkou District, New Taipei City, 24451, Taiwan	2150550R-E3012110013
FG-80F/81F	International Standards Laboratory No. 120 Lane 180, Hsin Ho Rd., Lung-Tan Dist., Tao Yuan City 325, Taiwan	ISL-20LE251FB
FG-100F/101F	International Standards Laboratory Corp. No.120, Lane 180, Hsin Ho Rd. Lung-Tan Dist., Tao Yuan City 325, Taiwan	ISL-19LE089FA
FG-200F/201F	Sporton International Inc No. 52, Huaya 1st Rd., Guishan Dist., Taoyuan City, Taiwan	FD081424
FG-600E/601E	DEKRA Testing and Certification Co., Ltd. No.372-2, Sec. 4, Zhongxing Rd. Zhudong Township, Hsinchu County 31061 Taiwan, R.O.C.	18C0020R-ITUSP01V00

Module	Lab Information	FCC Report Number
FG-1100E/1101E	DEKRA Testing and Certification Co., Ltd. No.372-2, Sec. 4, Zhongxing Rd., Zhudong Township, Hsinchu County 31061, Taiwan	1940014R-ITUSP01V00
FG-1800F/1801F	SPORTON INTERNATIONAL INC. EMC & Wireless Communications Laboratory No. 52, Huaya 1st Rd., Guishan Dist., Taoyuan City, Taiwan	FD021410-02
FG-2600F/2601F	SPORTON INTERNATIONAL INC. EMC & Wireless Communications Laboratory No. 52, Huaya 1st Rd., Guishan Dist., Taoyuan City, Taiwan	FD090712
FG-3300E/3301E	SPORTON INTERNATIONAL INC. EMC & Wireless Communications Laboratory No. 52, Huaya 1st Rd., Guishan Dist., Taoyuan City, Taiwan	FD942531
FG-3400E/3401E	DEKRA Testing and Certification Co., Ltd. No.372-2, Sec. 4, Zhongxing Rd., Zhudong Township, Hsinchu County 31061, Taiwan	18B0065R-ITUSP01V00
FG-3600E/3601E	DEKRA Testing and Certification Co., Ltd. No.372-2, Sec. 4, Zhongxing Rd., Zhudong Township, Hsinchu County 31061, Taiwan	18B0065R-ITUSP01V00
FG-4200F/4201F	SPORTON INTERNATIONAL INC. EMC & Wireless Communications Laboratory No. 52, Huaya 1st Rd., Guishan Dist., Taoyuan City, Taiwan	FD151422
FG-4400F/4401F	SPORTON INTERNATIONAL INC. EMC & Wireless Communications Laboratory No. 52, Huaya 1st Rd., Guishan Dist., Taoyuan City, Taiwan	FD141704
FG-6300F/6301F	Bay Area Compliance Laboratories Corp 1274 Anvilwood Avenue, Sunnyvale, CA 94089, USA	R1801021-15

Module	Lab Information	FCC Report Number
FG-6500F/6501F	Bay Area Compliance Laboratories Corp 1274 Anvilwood Avenue, Sunnyvale, CA 94089, USA	R1801021-15

FIPS 140-2 Compliant Operation

The Fortinet hardware is shipped in a non-FIPS 140-2 compliant configuration. The following steps must be performed to put the module into a FIPS compliant configuration:

1. Download the model specific FIPS validated firmware image and checksum from the Fortinet Support site at https://support.fortinet.com/.
2. Use a hashing utility on the downloaded firmware image to compare and verify the output against the result from the checksum listing.
3. Install the FIPS validated firmware image from a TFTP server using the BIOS boot menu. To access the BIOS boot menu, use the console connection and press any key when the "Press any key to display the configuration menu" option is displayed during the boot process. Then select "[G]: Get firmware image from TFTP server" and follow the instructions to complete the installation of the firmware image.
4. Install the entropy token (FortiGate-6300F/6301F/6500F/6501F only).
5. Enable the FIPS-CC mode of operation as per the "Enabling FIPS-CC Mode" section.

Additional information can be found in the FortiOS 6.4/7.0 "FIPS 140-2 and Common Criteria Technote" that can be found on the Fortinet technical documentation website at https://docs.fortinet.com.

In addition, FIPS 140-2 compliant operation requires both that you use the module in its FIPS-CC mode of operation and that you follow secure procedures for installation and operation of the FortiGate unit. You must ensure that:

- The FortiGate unit is configured in the FIPS-CC mode of operation.
- The FortiGate unit is installed in a secure physical location.
- Physical access to the FortiGate unit is restricted to authorized operators.
- The entropy token remains in the USB port during operation.
- Administrative passwords are at least 8 characters long.
- Administrative passwords are changed regularly.
- Administrator account passwords must have the following characteristics:
  - One (or more) of the characters must be capitalized
  - One (or more) of the characters must be lower case
  - One (or more) of the characters must be numeric
  - One (or more) of the characters must be non alpha-numeric (e.g. punctuation mark)
- Administration of the module is permitted using only validated administrative methods. These are:
  - Console connection
  - Web-based manager via HTTPS
  - Command line interface (CLI) access via SSH
- Diffie-Hellman groups of less than 2048 bits are not used.
- Client side RSA certificates must use 2048 bit or greater key sizes.
- Only approved and allowed algorithms are used.
- IPSec VPN tunnels using AES-GCM should be configured with a key lifetime of 98,000 KB to ensure a rekey after a maximum of 2^16 encryptions.

The module can be used in either of its two operation modes: NAT/Route or Transparent. NAT/Route mode applies security features between two or more different networks (for example, between a private network and the Internet). Transparent mode applies security features at any point in a network. The current operation mode is displayed on the web-based manager status page and in the output of the `get system status` CLI command.

Once the FIPS validated firmware has been installed and the module properly configured in the FIPS-CC mode of operation, the module is running in a FIPS compliant configuration. It is the responsibility of the CO to ensure the module only uses approved algorithms and services to maintain the module in a FIPS Approved mode of operation. Using any of the non-approved algorithms and services switches the module to a non-FIPS Approved mode of operation.

Enabling FIPS-CC mode

To enable the FIPS 140-2 compliant mode of operation, the operator must execute the following command from the Local Console:

```
config system fips-cc
   set status enable
end
```

The Operator is required to supply a password for the admin account which will be assigned to the Crypto Officer role.

The supplied password must be at least 8 characters long and correctly verified before the system will restart in FIPS-CC mode.

Upon restart, the module will execute self-tests to ensure the correct initialization of the module's cryptographic functions.

After restarting, the Crypto Officer can confirm that the module is running in FIPS-CC mode by executing the following command from the CLI:

```
get system status
```

If the module is running in FIPS-CC mode, the system status output will display the line:

```
FIPS-CC mode: enable
```

Self-Tests

Startup and Initialization Self-tests

The module executes the following self-tests during startup and initialization:

- Firmware integrity test using RSA 2048-bit signatures
- Configuration/VPN bypass test using HMAC SHA-256
- AES (128, 256 bit), CBC mode, encrypt known answer test
- AES (128, 256 bit) CBC mode, decrypt known answer test
- AES (128, 256 bit), GCM mode, encrypt known answer test
- AES (128, 256 bit), GCM mode, decrypt known answer test
- HMAC SHA-1 known answer test
- SHA-1 known answer test (tested as part of HMAC SHA-1 known answer test)
- SHA-224 known answer test (tested as part of HMAC-SHA-256 known answer test)
- HMAC SHA-256 known answer test
- SHA-256 known answer test (tested as part of HMAC SHA-256 known answer test)
- HMAC SHA-384 known answer test
- SHA-384 known answer test (tested as part of HMAC SHA-384 known answer test)
- HMAC SHA-512 known answer test
- SHA-512 known answer test (tested as part of HMAC SHA-512 known answer test)
- RSA 2048-bit signature generation known answer test
- RSA 2048-bit signature verification known answer test
- ECDSA pairwise consistency test
- DRBG known answer tests (as per SP 800-90A)
- Primitive-Z known answer test (KAS-FFC-SSC and KAS-ECC-SSC)
- IKEv1 KDF known answer test
- IKEv2 KDF known answer test
- TLS 1.1 KDF known answer test
- TLS 1.2 KDF known answer test
- SSH KDF known answer test

The results of the startup self-tests are displayed on the console during the startup process.

The startup self-tests can also be initiated on demand using the CLI command **`execute fips kat all`**(to initiate all self-tests) or **`execute fips kat <test>`** (to initiate a specific self-test).

When the self-tests are run, each implementation of an algorithm is tested - i.e. when the AES self-test is run, all AES implementations are tested.

Conditional Self-tests

The module executes the following conditional tests when the related service is invoked:

- Continuous entropy input test
- Continuous DRBG test
- RSA pairwise consistency test
- ECDSA pairwise consistency test using P-256 curve
- Configuration/VPN bypass test using HMAC SHA-256
- Firmware load test using RSA 2048-bit signatures

Critical Function Self-tests

The module also performs the following critical function self-tests applicable to the DRBG, as per NIST SP 800-90A Section 11:

- Instantiate test
- Generate test
- Reseed test

Error State

If any of the self-tests or conditional tests fail, the module enters an error state as shown by the console output below:

```
Self-tests failed
Entering error mode...
The system is going down NOW !!
The system is halted.
```

All data output and cryptographic services are inhibited in the error state.