

# FortiGate/FortiWiFi® 40F Series

**Secure SD-WAN  
Next Generation Firewall**



The FortiGate/FortiWiFi 40F series provides a fast and secure SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet’s Security-Driven Networking approach provides tight integration of the network to the new generation of security.

### Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevents and detects against known attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services
- Proactively blocks unknown sophisticated attacks in real-time with the Fortinet Security Fabric integrated AI-powered FortiSandbox

### Performance

- Engineered for Innovation using Fortinet’s purpose-built security processors (SPU) to deliver the industry’s best threat protection performance and ultra-low latency
- Provides industry-leading performance and protection for SSL encrypted traffic including the first firewall vendor to provide TLS 1.3 deep inspection

### Certification

- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs, ICASA, Virus Bulletin, and AV Comparatives

### Networking

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- Predefined compliance checklists analyze the deployment and highlight best practices to improve the overall security posture

### Security Fabric

- Enables Fortinet and Fabric-ready partners’ products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation
- Automatically builds Network Topology visualizations which discover IoT devices and provide complete visibility into Fortinet and Fabric-ready partner products

Firewall	IPS	NGFW	Threat Protection	Interfaces
<b>5 Gbps</b>	<b>1 Gbps</b>	<b>800 Mbps</b>	<b>600 Mbps</b>	Multiple GE RJ45   WiFi variants

Refer to the specifications table for details

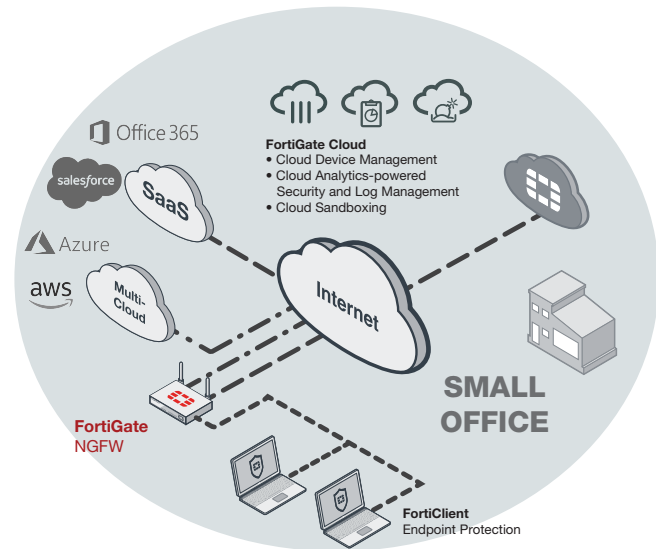
## Deployment

### Next Generation Firewall (NGFW)

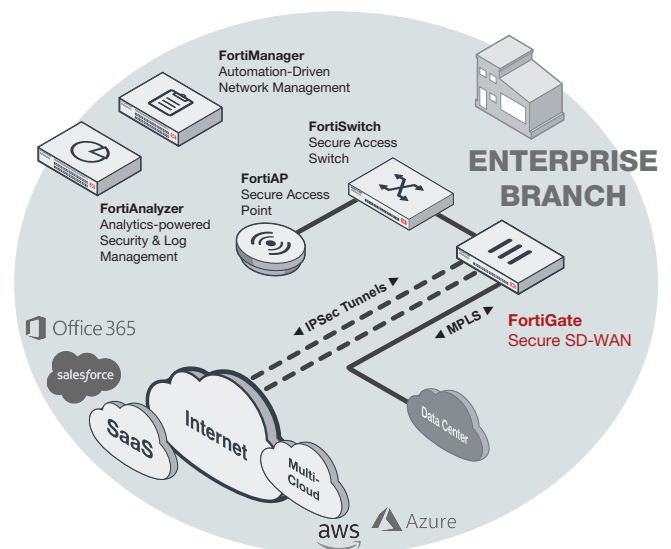
- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

### Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplification with zero touch deployment and centralized management with auto-provisioning, analytics and reporting
- Strong security posture with next generation firewall and real-time threat protection



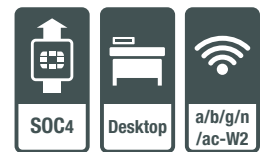
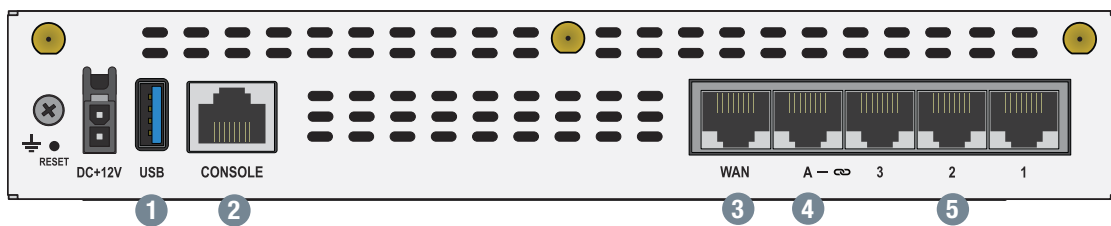
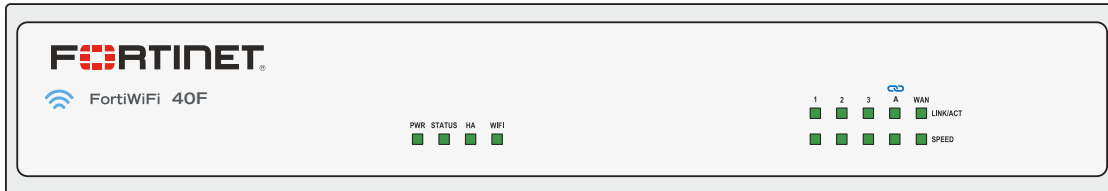
FortiWiFi 40F deployment in Small Office (NGFW)



FortiGate 40F deployment in Enterprise Branch (Secure SD-WAN)

## Hardware

### FortiGate/FortiWiFi 40F Series



## Interfaces

- |                        |                              |
|------------------------|------------------------------|
| 1. USB Port            | 4. 1x GE RJ45 FortiLink Port |
| 2. Console Port        | 5. 3x GE RJ45 Ethernet Ports |
| 3. 1x GE RJ45 WAN Port |                              |

### Powered by Purpose-built Secure SD-WAN ASIC SOC4



- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for best user experience on direct internet access
- Enables the best of breed NGFW Security and Deep SSL Inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

### 3G/4G WAN Connectivity

The FortiGate 40F Series includes a USB port that allows you to plug in a compatible third-party 3G/4G USB modem, providing additional WAN connectivity or a redundant link for maximum reliability.

### Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight yet highly reliable with a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

### Extends Security to Access Layer with FortiLink Ports

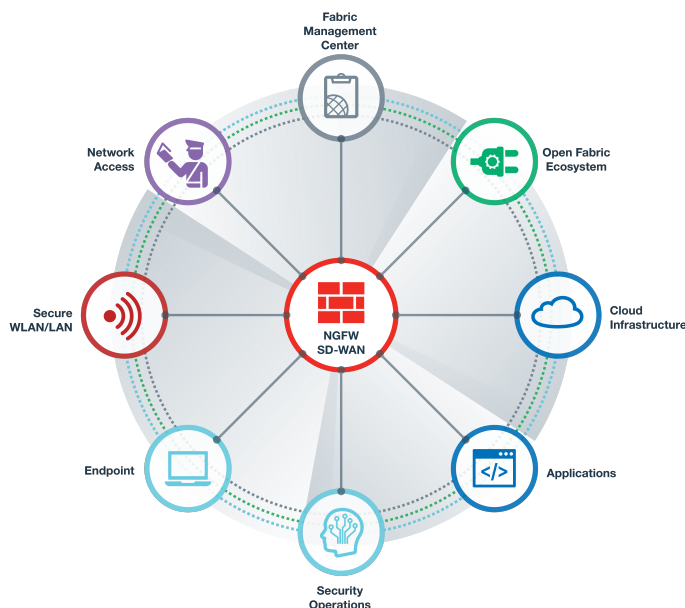
FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.

## Fortinet Security Fabric

### Security Fabric

The Security Fabric is the cybersecurity platform that enables digital innovations. It delivers broad visibility of the entire attack surface to better manage risk. Its unified and integrated solution reduces the complexity of supporting multiple-point products, while automated workflows increase operational speeds and reduce response times across the Fortinet deployment ecosystem. The Fortinet Security Fabric covers the following key areas under a single management center:

- **Security-Driven Networking** that secures, accelerates, and unifies the network and user experience
- **Zero Trust Network Access** that identifies and secures users and devices in real-time, on and off of the network
- **Dynamic Cloud Security** that protects and controls cloud infrastructures and applications
- **AI-Driven Security Operations** that automatically prevents, detects, isolates, and responds to cyber threats



### FortiOS

FortiGates are the foundation of the Fortinet Security Fabric—the core is FortiOS. All security and networking capabilities across the entire FortiGate platform are controlled with one intuitive operating system. FortiOS reduces complexity, costs, and response times by truly consolidating next-generation security products and services into one platform.

- A truly consolidated platform with a single OS and pane-of-glass for across the entire digital attack surface.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance.
- Leverage the latest technologies such as deception-based security.

- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support.
- Automatically prevent, detect, and mitigate advanced attacks within minutes with an integrated AI-driven security and advanced threat protection.
- Improve and unify the user experience with innovative SD-WAN capabilities with the ability to detect, contain, and isolate threats with automated segmentation.
- Utilize SPU hardware acceleration to boost network security performance.


## Services



FortiGuard Labs offer real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet’s solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world’s leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.



Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.

 For more information, please refer to [forti.net/fortiguard](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

	FORTIGATE 40F	FORTIWIFI 40F
<b>Hardware Specifications</b>		
GE RJ45 WAN / DMZ Ports		1
GE RJ45 Internal Ports		3
GE RJ45 FortiLink Ports		1
GE RJ45 PoE/+ Ports		–
Wireless Interface	–	802.11 a/b/g/n/ac-W2
USB Ports		1
Console (RJ45)		1
Internal Storage		–
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		1 Gbps
NGFW Throughput <sup>2,4</sup>		800 Mbps
Threat Protection Throughput <sup>2,5</sup>		600 Mbps
<b>System Performance</b>		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)		5/5/5 Gbps
Firewall Latency (64 byte UDP packets)		4 µs
Firewall Throughput (Packets Per Second)		7.5 Mpps
Concurrent Sessions (TCP)		700,000
New Sessions/Second (TCP)		35,000
Firewall Policies		5,000
IPsec VPN Throughput (512 byte) <sup>1</sup>		4.4 Gbps
Gateway-to-Gateway IPsec VPN Tunnels		200
Client-to-Gateway IPsec VPN Tunnels		250
SSL-VPN Throughput		490 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		200
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		310 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		320
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		55,000
Application Control Throughput (HTTP 64K) <sup>2</sup>		990 Mbps
CAPWAP Throughput (HTTP 64K)		3.5 Gbps
Virtual Domains (Default / Maximum)		10 / 10
Maximum Number of FortiSwitches Supported		8
Maximum Number of FortiAPs (Total / Tunnel Mode)		16 / 8
Maximum Number of FortiTokens		500
High Availability Configurations		Active / Active, Active / Passive, Clustering

	FORTIGATE 40F	FORTIWIFI 40F
<b>Dimensions</b>		
Height x Width x Length (inches)		1.5 x 8.5 x 6.3
Height x Width x Length (mm)		38.5 x 216 x 160
Weight		2.2 lbs (1 kg)
Form Factor		Desktop
<b>Operating Environment and Certifications</b>		
Input Rating		12Vdc, 3A
Power Required		Powered by External DC Power Adapter, 100–240V AC, 50–60 Hz
Maximum Current		100V AC / 0.2A, 240V AC / 0.1A
Power Consumption (Average / Maximum)	12.4 W / 15.4 W	13.6 W / 16.6 W
Heat Dissipation	52.55 BTU/hr	56.64 BTU/hr
Operating Temperature		32–104°F (0–40°C)
Storage Temperature		-31–158°F (-35–70°C)
Humidity		10–90% non-condensing
Noise Level		Fanless 0 dBA
Operating Altitude		Up to 7,400 ft (2,250 m)
Compliance		FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB
Certifications		ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN
<b>Radio Specifications</b>		
Multiple (MU) MIMO	–	3x3
Maximum Wi-Fi Speeds	–	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
Maximum Tx Power	–	20 dBm
Antenna Gain	–	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.

2. IPS (Enterprise Mix), Application Control, NGFW, and Threat Protection are measured with Logging enabled.

3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS, and Application Control enabled.

5. Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.

## Order Information

Product	SKU	Description
FortiGate 40F	FG-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports)
FortiWiFi 40F	FWF-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), Wireless (802.11a/b/g/n/ac-W2)

## Bundles



### FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	Unified Threat Protection	Threat Protection
FortiCare	ASE <sup>1</sup>	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	•
FortiGuard Antispam Service	•	•	•	•
FortiGuard Security Rating Service	•	•	•	•
FortiGuard Industrial Service	•	•	•	•
FortiGuard IoT Detection Service <sup>2</sup>	•	•	•	•
FortiConverter Service	•	•	•	•
IPAM Cloud <sup>2</sup>	•	•	•	•
SD-WAN Orchestrator Entitlement <sup>2</sup>	•	•	•	•
SD-WAN Cloud Assisted Monitoring	•	•	•	•
SD-WAN Overlay Controller VPN Service	•	•	•	•
FortiAnalyzer Cloud	•	•	•	•
FortiManager Cloud	•	•	•	•

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.4

# FortiGate/FortiWiFi® 30E

**Secure SD-WAN  
Next Generation Firewall**



The FortiGate/FortiWiFi 30E series provides a fast and secure SD-WAN solution in a compact fanless desktop form factor for enterprise branch offices and mid-sized businesses. Protects against cyber threats with system-on-a-chip acceleration and industry-leading secure SD-WAN in a simple, affordable, and easy to deploy solution. Fortinet’s Security-Driven Networking approach provides tight integration of the network to the new generation of security.

### Security

- Identifies thousands of applications inside network traffic for deep inspection and granular policy enforcement
- Protects against malware, exploits, and malicious websites in both encrypted and non-encrypted traffic
- Prevents and detects against known attacks using continuous threat intelligence from AI-powered FortiGuard Labs security services
- Proactively blocks unknown sophisticated attacks in real-time with the Fortinet Security Fabric integrated AI-powered FortiSandbox

### Performance

- Engineered for Innovation using Fortinet’s purpose-built security processors (SPU) to deliver the industry’s best threat protection performance and ultra-low latency
- Provides industry-leading performance and protection for SSL encrypted traffic including the first firewall vendor to provide TLS 1.3 deep inspection

### Certification

- Independently tested and validated best security effectiveness and performance
- Received unparalleled third-party certifications from NSS Labs, ICASA, Virus Bulletin, and AV Comparatives

### Networking

- Application aware routing with in-built SD-WAN capabilities to achieve consistent application performance and the best user experience
- Built-in advanced routing capabilities to deliver high performance with encrypted IPSEC tunnels at scale

### Management

- Includes a management console that is effective and simple to use, which provides a comprehensive network of automation & visibility
- Provides Zero Touch Provisioning leveraging Single Pane of Glass Management powered by the Fabric Management Center
- Predefined compliance checklists analyze the deployment and highlight best practices to improve the overall security posture

### Security Fabric

- Enables Fortinet and Fabric-ready partners’ products to provide broader visibility, integrated end-to-end detection, threat intelligence sharing, and automated remediation
- Automatically builds Network Topology visualizations which discover IoT devices and provide complete visibility into Fortinet and Fabric-ready partner products

Firewall	IPS	NGFW	Threat Protection	Interfaces
<b>950 Mbps</b>	<b>300 Mbps</b>	<b>200 Mbps</b>	<b>150 Mbps</b>	Multiple GE RJ45   WiFi variants

Refer to the specifications table for details

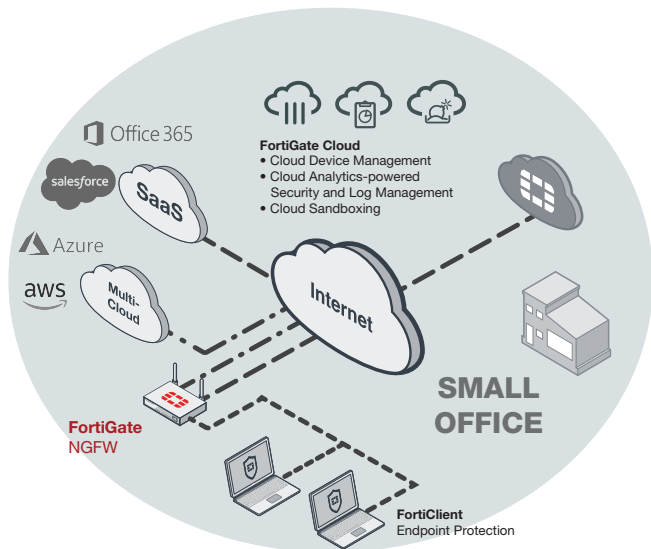
## Deployment

### Next Generation Firewall (NGFW)

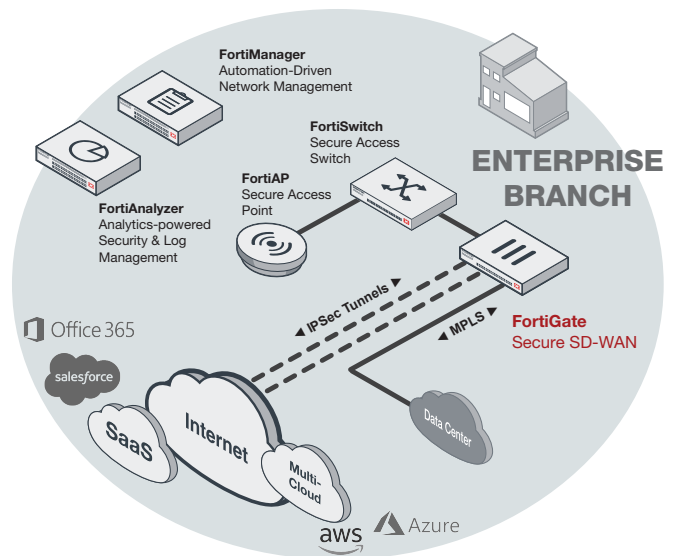
- Reduce the complexity and maximize your ROI by integrating threat protection security capabilities into a single high-performance network security appliance, powered by Fortinet's Security Processing Unit (SPU)
- Full visibility into users, devices, applications across the entire attack surface and consistent security policy enforcement irrespective of asset location
- Protect against network exploitable vulnerabilities with industry-validated IPS that offers low latency and optimized network performance
- Automatically block threats on decrypted traffic using the Industry's highest SSL inspection performance, including the latest TLS 1.3 standard with mandated ciphers
- Proactively block newly discovered sophisticated attacks in real-time with AI-powered FortiGuard Labs and advanced threat protection services included in the Fortinet Security Fabric

### Secure SD-WAN

- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplification with zero touch deployment and centralized management with auto-provisioning, analytics and reporting
- Strong security posture with next generation firewall and real-time threat protection



FortiWiFi 30E deployment in Small Office (NGFW)

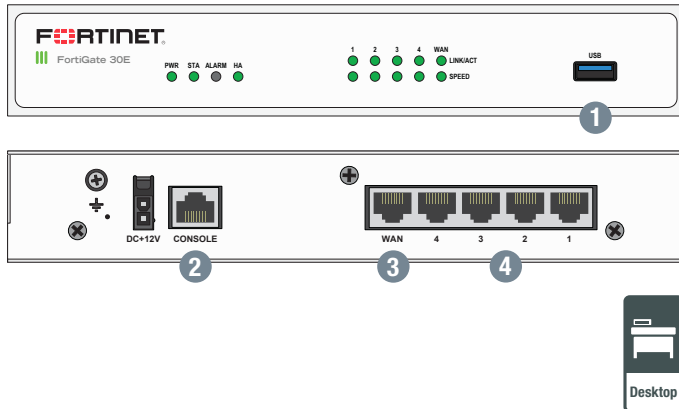


FortiGate 30E deployment in Enterprise Branch (Secure SD-WAN)

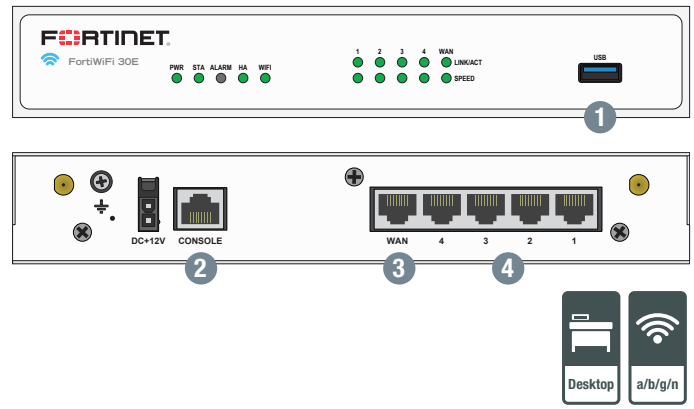


## Hardware

### FortiGate 30E



### FortiWiFi 30E



### Interfaces

1. USB Port
2. Console Port
3. 1x GE RJ45 WAN Port
4. 4x GE RJ45 Switch Ports

### Interfaces

1. USB Port
2. Console Port
3. 1x GE RJ45 WAN Port
4. 4x GE RJ45 Switch Ports

### Install in Minutes with FortiExplorer

The FortiExplorer wizard enables easy setup and configuration coupled with easy-to-follow instructions. FortiExplorer runs on popular iOS devices. Using FortiExplorer is as simple as starting the application and connecting to the appropriate USB port on the FortiGate. By using FortiExplorer, you can be up and running and protected in minutes.

### Wireless and 3G/4G WAN Extensions

The FortiGate supports external 3G/4G modems that allow additional or redundant WAN connectivity for maximum reliability. The FortiGate can also operate as a wireless access point controller to further extend wireless capabilities.

### Compact and Reliable Form Factor

Designed for small environments, you can simply place the FortiGate/FortiWiFi 30E on a desktop. It is small, lightweight yet highly reliable with superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

### Superior Wireless Coverage

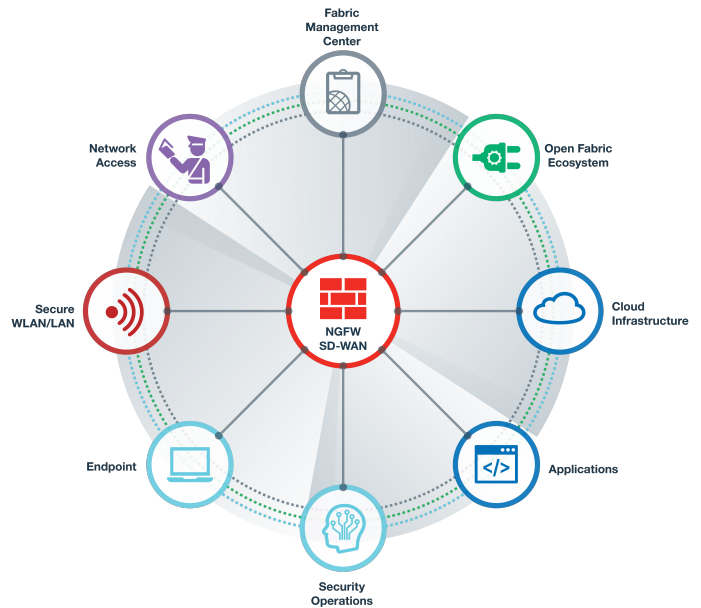
A built-in dual-band, dual-stream access point with internal antennas is integrated on the FortiWiFi 30E and provides speedy 802.11n coverage on 2.4 GHz or 5 GHz bands. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning, providing maximum protection for regulated environments.

## Fortinet Security Fabric

### Security Fabric

The Security Fabric is the cybersecurity platform that enables digital innovations. It delivers broad visibility of the entire attack surface to better manage risk. Its unified and integrated solution reduces the complexity of supporting multiple-point products, while automated workflows increase operational speeds and reduce response times across the Fortinet deployment ecosystem. The Fortinet Security Fabric covers the following key areas under a single management center:

- **Security-Driven Networking** that secures, accelerates, and unifies the network and user experience
- **Zero Trust Network Access** that identifies and secures users and devices in real-time, on and off of the network
- **Dynamic Cloud Security** that protects and controls cloud infrastructures and applications
- **AI-Driven Security Operations** that automatically prevents, detects, isolates, and responds to cyber threats



### FortiOS

FortiGates are the foundation of the Fortinet Security Fabric—the core is FortiOS. All security and networking capabilities across the entire FortiGate platform are controlled with one intuitive operating system. FortiOS reduces complexity, costs, and response times by truly consolidating next-generation security products and services into one platform.

- A truly consolidated platform with a single OS and pane-of-glass for across the entire digital attack surface.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance.
- Leverage the latest technologies such as deception-based security.

- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support.
- Automatically prevent, detect, and mitigate advanced attacks within minutes with an integrated AI-driven security and advanced threat protection.
- Improve and unify the user experience with innovative SD-WAN capabilities with the ability to detect, contain, and isolate threats with automated segmentation.
- Utilize SPU hardware acceleration to boost network security performance.


## Services



FortiGuard Labs offer real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet’s solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world’s leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.



Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.

 For more information, please refer to [forti.net/fortiguard](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

	FORTIGATE 30E	FORTIWIFI 30E
<b>Hardware Specifications</b>		
GE RJ45 Switch Ports		4
GE RJ45 WAN Port		1
USB Port		1
Console (RJ45)		1
Wireless Interface	–	802.11 a/b/g/n
<b>System Performance — Enterprise Traffic Mix</b>		
IPS Throughput <sup>2</sup>		300 Mbps
NGFW Throughput <sup>2,4</sup>		200 Mbps
Threat Protection Throughput <sup>2,5</sup>		150 Mbps
<b>System Performance</b>		
Firewall Throughput		950 Mbps
Firewall Latency (64 byte UDP packets)		130 µs
Firewall Throughput (Packets Per Second)		180 Kpps
Concurrent Sessions (TCP)		900,000
New Sessions/Second (TCP)		15,000
Firewall Policies		5,000
IPsec VPN Throughput (512 byte) <sup>1</sup>		75 Mbps
Gateway-to-Gateway IPsec VPN Tunnels		200
Client-to-Gateway IPsec VPN Tunnels		250
SSL-VPN Throughput		35 Mbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		100
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		125 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		120
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		45,000
Application Control Throughput (HTTP 64K) <sup>2</sup>		400 Mbps
CAPWAP Throughput (HTTP 64K)		850 Mbps
Virtual Domains (Default / Maximum)		5 / 5
Maximum Number of FortiSwitches Supported		8
Maximum Number of FortiAPs (Total / Tunnel Mode)		2 / 2
Maximum Number of FortiTokens		500
High Availability Configurations		Active/Active, Active/Passive, Clustering

	FORTIGATE 30E	FORTIWIFI 30E
<b>Dimensions</b>		
Height x Width x Length (inches)	1.61 x 8.27 x 5.24	
Height x Width x Length (mm)	41 x 210 x 133	
Weight	1.982 lbs (0.899 kg)	2.008 lbs (0.911 kg)
Form Factor	Desktop	
<b>Environment</b>		
Input Rating	12Vdc, 2A	
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50–60 Hz	
Maximum Current	100V / 0.6A, 240V / 0.4A	
Power Consumption (Average / Maximum)	13 / 15 W	16 / 19 W
Heat Dissipation	52 BTU/h	66 BTU/h
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	Fan-less 0 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
<b>Compliance</b>		
Regulatory Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
<b>Certifications</b>		
	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN	
<b>Radio Specifications</b>		
MIMO	2x2	
Maximum Wi-Fi Speeds	300 Mbps	
Maximum Tx Power	21 dBm	
Antenna Gain	2 dBi @ 5 GHz	2.4 dBi @ 2.4 GHz

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW, and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS, and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control, and Malware Protection enabled.

## Order Information

Product	SKU	Description
FortiGate 30E	FG-30E	5x GE RJ45 ports (Including 1x WAN port, 4x Switch ports)
FortiWiFi 30E	FWF-30E	5x GE RJ45 ports (Including 1x WAN port, 4x Switch ports), Wireless (802.11a/b/g/n)
Optional Accessory		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for supported products.

## Bundles



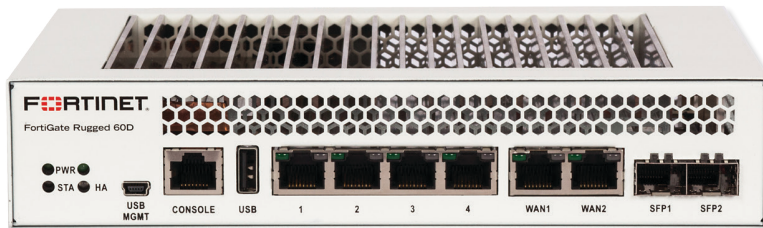
### FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	UTM	Threat Protection
FortiCare	ASE <sup>1</sup>	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiCASB SaaS-only Service	•	•		
FortiConverter Service	•			
SD-WAN Cloud Assisted Monitoring <sup>2</sup>	•			
SD-WAN Overlay Controller VPN Service <sup>2</sup>	•			
FortiAnalyzer Cloud <sup>2</sup>	•			
FortiManager Cloud <sup>2</sup>	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2

## FortiGate® Rugged Series



While traditional security solutions are designed and intended for the world of offices and corporations, **the FortiGate Rugged Series offers industrially-hardened, all-in-one security appliance that delivers specialized threat protection for securing critical industrial and control networks against malicious attacks.**



### Ruggedized Design

Fanless and use of robust components ensure reliable operation in harsh industrial environments.



### Consolidated Security Architecture

FortiGate running FortiOS consolidated security offers better protection and lower cost of ownership than multiple point products. Coupled with FortiGuard Industrial Security Service, it ensures that critical networks receive real-time protection.



### Ease of Management

Robust management systems that allow rapid provision and deployment, monitoring of device and threat status while providing actionable reports.

### Product Offerings

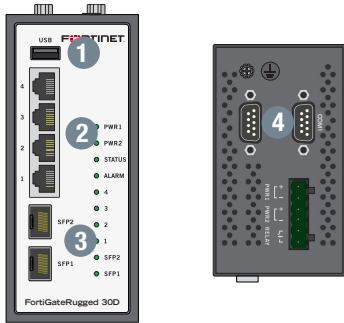
- FGR-30D** — Ruggedized compact security appliance with DIN mounting kit
- FGR-35D** — Security appliance with IP67 rating for outdoor environment
- FGR-60D** — SPU SoC Powered, high performance security and VPN gateway
- FGR-90D** — Robust ruggedized security appliance with wide operating temperature

### Third-Party Certifications



## Hardware

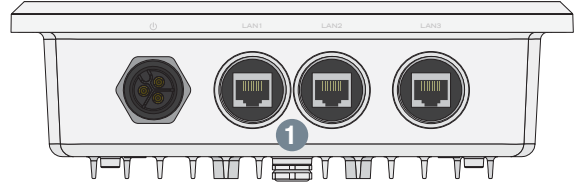
### FortiGate Rugged 30D



#### Interfaces

1. 1x USB Port
2. 4x GE RJ45 Ports
3. 2x GE SFP Slots
4. 2x DB9 Serial Interface/Console

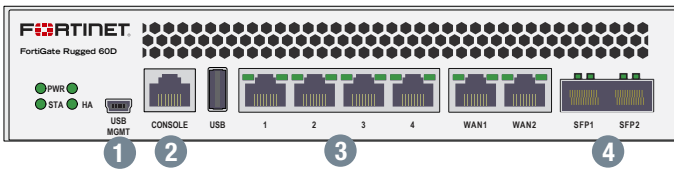
### FortiGate Rugged 35D



#### Interfaces

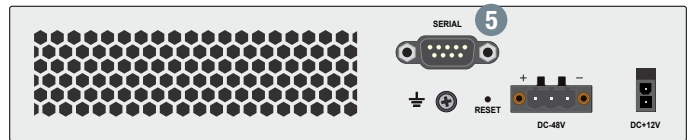
1. 3x GE RJ45 Ports

### FortiGate Rugged 60D



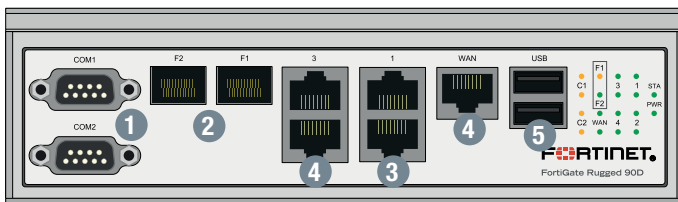
#### Interfaces

1. USB Management Port for FortiExplorer
2. Console Port (RJ45)
3. 4x GE RJ45 Ports



4. 2x Shared Media (GE RJ45 Ports / GE SFP Slots) Pairs
5. 1x DB9 Serial Interface

### FortiGate Rugged 90D



#### Interfaces

1. 2x DB9 Serial Interface/Console
2. 2x GE SFP Slots
3. 1x GE RJ45 Bypass Pair
4. 3x GE RJ45 ports
5. 2x USB interfaces

### Wireless and 3G/4G WAN Extensions

The FortiGate supports external 3G/4G modems that allow additional or redundant WAN connectivity for maximum reliability. The FortiGate can also operate as a wireless access point controller to further extend wireless capabilities.

### Compact, Ruggedized and Reliable Form Factor

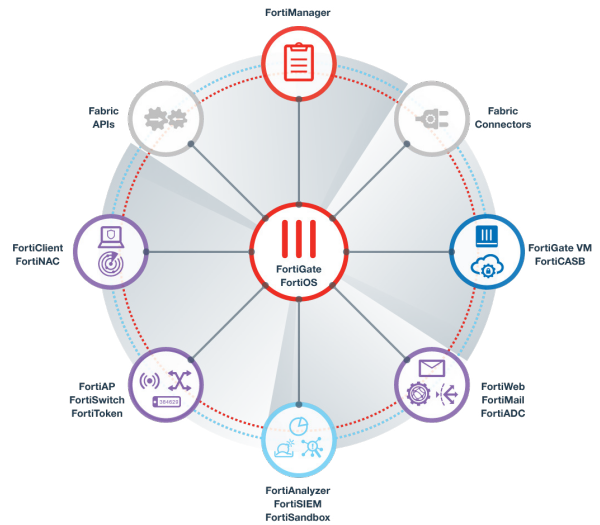
Designed for confined spaces and harsh environments, the ruggedized FortiGate can be mounted within an enclosure, on a wall or on a DIN rail. It is small and lightweight yet highly reliable with superior Mean Time Between Failure (MTBF), minimizing the chance of a network disruption. The hardware components meet high standards in both EMI and vibration tolerance with a wide thermal operating range supported.

# Fortinet Security Fabric

## Security Fabric

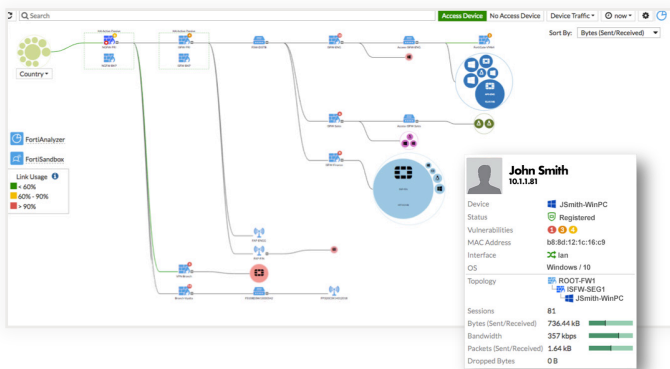
The Security Fabric delivers broad visibility, integrated AI-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and its ecosystem deployments. It allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network. All this is tied together under a single pane of glass management to deliver leading security capabilities across your entire environment while also significantly reducing complexity.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.



## FortiOS

Control all security and networking capabilities across the entire FortiGate platform with one intuitive operating system. Reduce complexity, costs, and response time with a truly consolidated next-generation security platform.



- A truly consolidated platform with a single OS and pane-of-glass for all security and networking services across all FortiGate platforms.
- Industry-leading protection: NSS Labs Recommended, VB100, AV Comparatives, and ICSA validated security and performance. Ability to leverage latest technologies such as deception-based security.
- Control thousands of applications, block the latest exploits, and filter web traffic based on millions of real-time URL ratings in addition to true TLS 1.3 support.
- Prevent, detect, and mitigate advanced attacks automatically in minutes with integrated AI-driven breach prevention and advanced threat protection.
- Improved user experience with innovative SD-WAN capabilities and ability to detect, contain and isolate threats with Intent-based Segmentation.
- Utilize SPU hardware acceleration to boost security capability performance.

## Services



FortiGuard Labs offers real-time intelligence on the threat landscape, delivering comprehensive security updates across the full range of Fortinet’s solutions. Comprised of security threat researchers, engineers, and forensic specialists, the team collaborates with the world’s leading threat monitoring organizations and other network and security vendors, as well as law enforcement agencies.



Our FortiCare customer support team provides global technical support for all Fortinet products. With support staff in the Americas, Europe, Middle East, and Asia, FortiCare offers services to meet the needs of enterprises of all sizes.

For more information, please refer to [forti.net/fortiguard](https://forti.net/fortiguard) and [forti.net/forticare](https://forti.net/forticare)

## Specifications

	FGR-30D	FGR-35D	FGR-60D	FGR-90D
<b>Interfaces and Modules</b>				
GE RJ45 Interfaces	4	3	4	3
GE RJ45 Bypass Pair	–	–	–	1
GE SFP Slots	2	–	–	2
Shared Media Pairs (GE RJ45 / GE SFP)	–	–	2	–
DB9 Serial Interface	2	–	1	2
USB (Client / Server)	1	–	1/1	1
RJ45 Console Port	–	–	1	–
Included Transceivers	None	None	None	None
<b>System Performance and Capacity</b>				
IPv4 Firewall Throughput (1518 UDP)	900 Mbps	550 Mbps	1.5 Gbps	2 Gbps
Firewall Latency (64 byte, UDP)	70 µs	90 µs	4 µs	51 µs
Firewall Throughput (Packets Per Second)	87 Kpps	52.5 Kpps	2.2 Mpps	84 Kpps
Concurrent Sessions (TCP)	750,000	750,000	500,000	2.5 Million
New Sessions/Second (TCP)	5,000	5,000	4,000	20,000
Firewall Policies	5,000	5,000	5,000	5,000
IPsec VPN Throughput (512 byte) <sup>1</sup>	45 Mbps	45 Mbps	1 Gbps	84 Mbps
Gateway-to-Gateway IPsec VPN Tunnels	200	200	200	200
Client-to-Gateway IPsec VPN Tunnels	250	250	500	1,000
SSL-VPN Throughput	25 Mbps	25 Mbps	30 Mbps	115 Mbps
Concurrent SSL-VPN Users (Recommended Maximum)	80	80	100	200
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>	50 Mbps	55 Mbps	15 Mbps	85 Mbps
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>	75	75	20	70
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>	45,000	45,000	15,000	72,000
Application Control Throughput (HTTP 64K)	210 Mbps	230 Mbps	95 Mbps	440 Mbps
Virtual Domains (Default / Maximum)	5 / 5	5 / 5	10 / 10	10 / 10
Maximum Number of FortiAPs (Total / Tunnel)	2 / 2	2 / 2	10 / 5	32 / 16
Maximum Number of FortiTokens	20	20	100	100
Maximum Number of Registered FortiClients	200	200	200	200
High Availability Configurations	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering	Active-Active, Active-Passive, Clustering
<b>System Performance — Optimal Traffic Mix</b>				
IPS Throughput <sup>2</sup>	230 Mbps	230 Mbps	200 Mbps	1.1 Gbps
<b>System Performance — Enterprise Traffic Mix</b>				
IPS Throughput <sup>2</sup>	180 Mbps	210 Mbps	95 Mbps	350 Mbps
NGFW Throughput <sup>2,4</sup>	45 Mbps	65 Mbps	40 Mbps	370 Mbps
Threat Protection Throughput <sup>2,5</sup>	16 Mbps	16 Mbps	23 Mbps	280 Mbps
<b>Dimensions and Power</b>				
Height x Width x Length (inches)	5.49 x 4.13 x 2.36	3.07 x 10.04 x 10.04	1.73 x 8.50 x 6.10	2.11 x 7.32 x 6.30
Height x Width x Length (mm)	139.5 x 105 x 60	78 x 255.09 x 255.09	44 x 216 x 155	53.5 x 186 x 160
Weight	1.46 lbs (0.668 kg)	3.986 lbs (1.808 kg)	3.5 lbs (1.6 kg)	2.4 lbs (1.08 kg)
Form Factor	Desktop	Outdoor mountable	Desktop	Desktop
IP Rating	IP20	IP67	IP20	IP40
Power Supply	Dual input, total 6 pin terminal block (12–48V DC) DC cables are not included. <sup>6</sup>	Terminal block (12–48V DC) DC cables are not included. <sup>7</sup>	-48V DC power supply and external 12V DC power adapter connection. AC adapter not included. DC Power connector supplied only. <sup>8</sup>	Dual input, total 6 pin terminal block (12–48V DC) AC adapter included. <sup>9</sup>
Power Consumption (Average / Maximum)	15.55 W / 15.92W	10.2 W / 10.5 W	11.6 W / 14 W	40 W / 49 W
Maximum Current	1.19A	0.83A	-48V DC / 0.5A	12–48V DC/ 4.08–1.02A
Heat Dissipation	54.29 BTU/h	35.81 BTU/h	40 BTU/h	167 BTU/h
<b>Operating Environment and Certifications</b>				
Operating Temperature	-40–158°F (-40–70°C)	-40–140°F (-40–60°C)	-4–140°F (-20–60°C)	-40–158°F (-40–70°C) <sup>10</sup>
Storage Temperature	-58–185°F (-50–85°C)	-58–185°F (-50–85°C)	-40–185°F (-40–85°C)	-40–185°F (-40–85°C)
Humidity	5–95% non-condensing	5–95% non-condensing	20–90% non-condensing	0–95% non-condensing
Operating Altitude	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)	Up to 7,400 ft (2,250 m)
Compliance	FCC Part 15 Class A, C-Tick, VCCI Class B, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI Class A, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, CE, UL/cUL, CB	FCC Part 15 Class A, C-Tick, VCCI Class A, CE, UL/cUL, CB



## Specifications

	FGR-30D	FGR-35D	FGR-60D	FGR-90D
<b>Certifications</b>	IEEE 1613 and IEC 61850-3 Certified ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN	IEEE 1613 and IEC 61850-3 Certified ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN	—	IEC 61850-3 and IEEE 1613 Emission Compliant ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.
4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.
6. AC adapter not supported.
7. AC adapter not supported. Requires fabricated DC cables (refer to QuickStart Guide).
8. Requires third-party AC adapter or DC cables. If wide temperature range is not required, SP-FG60C-PDC (0–40°C) may be acquired separately.
9. Additional AC adapter for dual redundant input is currently not available for order.
10. Excludes supplied power adapter which operates at smaller temperature range.

## Supported Protocols

### IPS and Application Control Support for Operational Technology/Industrial Control System

- ADDP
- BACnet
- CC-Link
- CIP
- CN/IP - EIA/CEA-852
- IEC 62056 - DLMS/COSEM
- DNP3
- ECHONET Lite
- LonTalk/EIA-709.1
- ELCOM 90
- EtherCAT Automation Protocol (EAP)
- Ethernet Global Data (EGD)
- EtherNet/IP
- Ether-S-Bus
- FL-net
- HART-IP
- IEC 60870-6 (TASE.2/ICCP)
- IEC 60870-5-104
- IEC 61850 (MMS)
- IEEE 1278.2 Distributed Interactive Simulation
- KNXnet/IP (EIBnet/IP)
- Modbus TCP
- MOXA
- MTConnect
- OPC UA (DA, HDA, AE)
- OpenADR
- PROFINET
- RTPS
- SafetyNet p
- Siemens S7, S7Plus, LOGO
- STANAG 4 406
- STANAG 5066
- IEEE C37.118 Synchrophasor
- Vedeer-Root



FortiGate Rugged 30D



FortiGate Rugged 35D



FortiGate Rugged 60D



FortiGate Rugged 90D

## Order Information

Product	SKU	Description
FortiGate Rugged 30D	FGR-30D	Ruggedized, 4x GE RJ45 ports, 2x GE SFP slots, 2x DB9 Serial. Maximum managed FortiAPs (Total / Tunnel) 2 / 2.
FortiGate Rugged 35D	FGR-35D	Ruggedized, IP67 rating for outdoor environment, 3x GE RJ45 Switch ports. Maximum managed FortiAPs (Total / Tunnel) 2 / 2.
FortiGate Rugged 60D	FGR-60D	Ruggedized, 4x GE RJ45 Switch ports, 2x Shared Media pairs (Including 2x GE RJ45 ports, 2x SFP slots). DB9 Serial. Maximum managed FortiAPs (Total / Tunnel) 10 / 5.
FortiGate Rugged 90D	FGR-90D	Ruggedized, 3x GE RJ45 ports, 1x GE RJ45 bypass pair, 2x SFP slots. 2x DB9 Serial/console. Dual power input. Maximum managed FortiAPs (Total / Tunnel) 32 / 16.
Optional Accessories		
1 GE SFP LX transceivers, SMF, -40–85°C operation	FR-TRAN-LX	1 GE SFP LX transceiver module, -40–85°C, over SMF, for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX transceivers, MMF, -40–85°C operation	FR-TRAN-SX	1 GE SFP SX transceiver module, -40–85°C, over MMF, for all systems with SFP and SFP/SFP+ slots.
1 GE SFP transceivers, 90km range, -40–85°C operation	FR-TRAN-ZX	1 GE SFP transceivers, -40–85°C operation, 90km range for all systems with SFP slots.

## Bundles



### FortiGuard Bundle

FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

Bundles	360 Protection	Enterprise Protection	UTM	Threat Protection
FortiCare	ASE <sup>1</sup>	24x7	24x7	24x7
FortiGuard App Control Service	•	•	•	•
FortiGuard IPS Service	•	•	•	•
FortiGuard Advanced Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
FortiGuard Web Filtering Service	•	•	•	
FortiGuard Antispam Service	•	•	•	
FortiGuard Security Rating Service	•	•		
FortiGuard Industrial Service	•	•		
FortiCASB SaaS-only Service	•	•		
FortiConverter Service	•			
SD-WAN Cloud Assisted Monitoring <sup>2</sup>	•			
SD-WAN Overlay Controller VPN Service <sup>2</sup>	•			
FortiAnalyzer Cloud <sup>2</sup>	•			
FortiManager Cloud <sup>2</sup>	•			

1. 24x7 plus Advanced Services Ticket Handling 2. Available when running FortiOS 6.2