

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, ICSA, 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

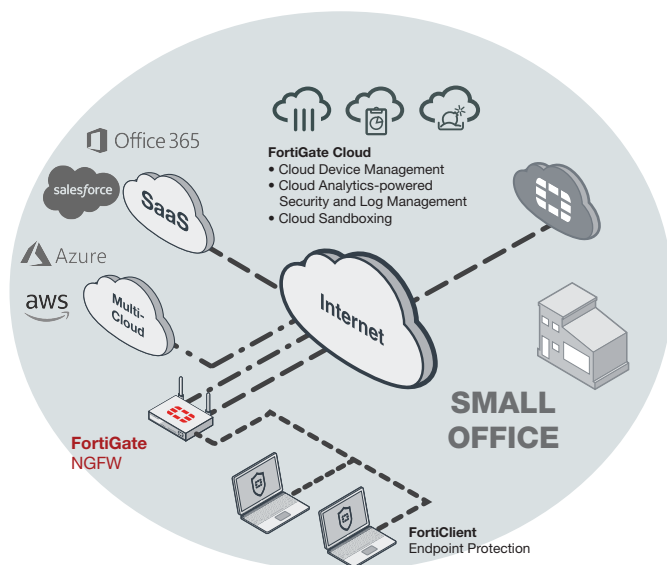
| Firewall | IPS | NGFW | Threat Protection | Interfaces |
|----------|----------|----------|-------------------|----------------------------------|
| 950 Mbps | 300 Mbps | 200 Mbps | 150 Mbps | Multiple GE RJ45 WiFi variants |

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

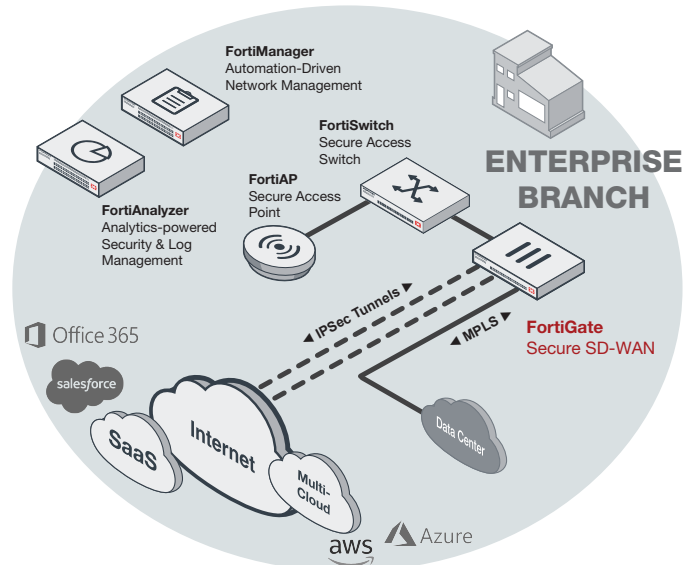


FortiWiFi 30E deployment in Small Office (NGFW)



Secure SD-WAN

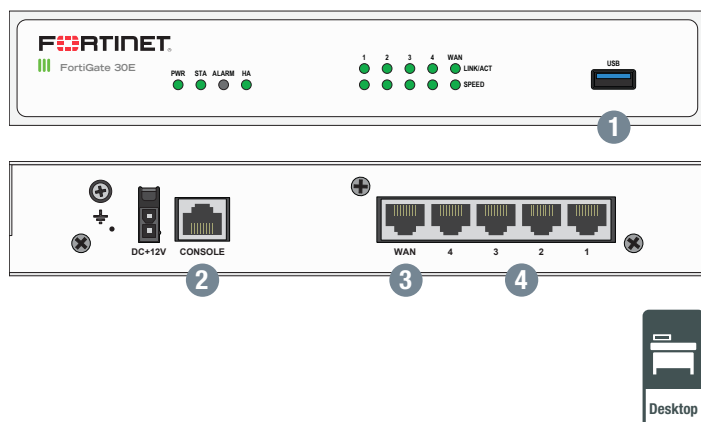
- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplification with zero touch deployment and centralized management with auto-provisioning, analytics and reporting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



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

Hardware

FortiGate 30E



Interfaces

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

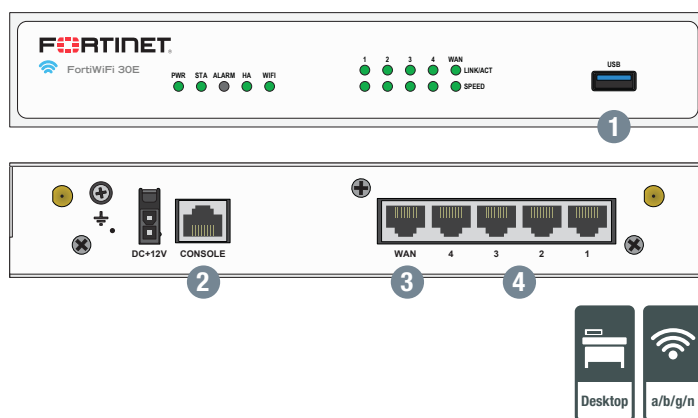
Install in Minutes with FortiExplorer

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.

FortiWiFi 30E



Interfaces

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

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

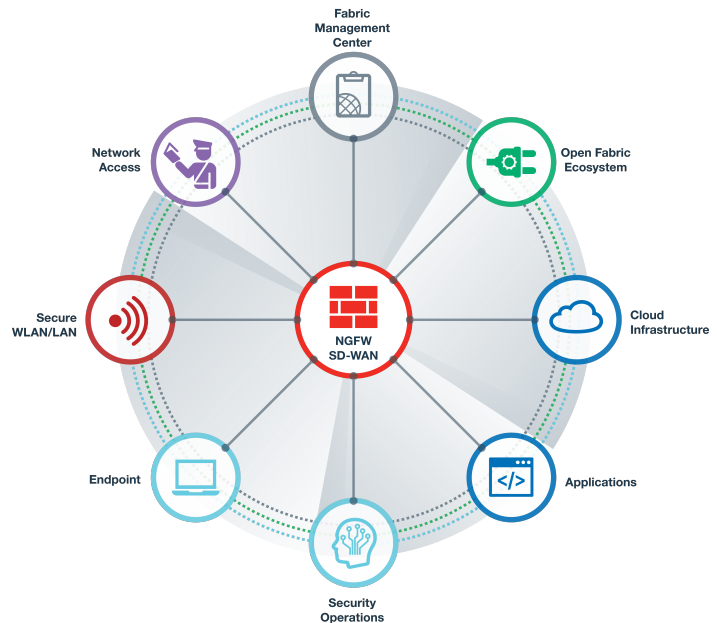
A built-in dual-band, dual-stream access point with internal antennas is integrated on the FortiWiFi 30E and provides speedy 802.11n coverage on 2.4 GHz or 5 GHz bands. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning, providing maximum protection for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



FortiCare™ Support Services

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 and forti.net/forticare

Specifications

| | FORTIGATE 30E | FORTIWIFI 30E |
|--|---|----------------|
| Hardware Specifications | | |
| GE RJ45 Switch Ports | 4 | |
| GE RJ45 WAN Port | 1 | |
| USB Port | 1 | |
| Console (RJ45) | 1 | |
| Wireless Interface | — | 802.11 a/b/g/n |
| System Performance — Enterprise Traffic Mix | | |
| IPS Throughput ² | 300 Mbps | |
| NGFW Throughput ^{2,4} | 200 Mbps | |
| Threat Protection Throughput ^{2,5} | 150 Mbps | |
| System Performance | | |
| 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) ¹ | 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) ³ | 125 Mbps | |
| SSL Inspection CPS (IPS, avg. HTTPS) ³ | 120 | |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³ | 45,000 | |
| Application Control Throughput (HTTP 64K) ² | 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 |
|---------------------------------------|---|----------------------|
| Dimensions | | |
| 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 | |
| Environment | | |
| 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) | |
| Compliance | | |
| Regulatory Compliance | FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB | |
| Certifications | | |
| | ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN | |
| Radio Specifications | | |
| 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 ¹ | 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 ² | • | | | |
| SD-WAN Overlay Controller VPN Service ² | • | | | |
| FortiAnalyzer Cloud ² | • | | | |
| FortiManager Cloud ² | • | | | |

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

FortiGate/FortiWiFi® 50E Series

FortiGate 50E, FortiWiFi 50E/-2R and FortiGate/FortiWiFi 51E

Secure SD-WAN
Next Generation Firewall



The FortiGate/FortiWiFi 50E 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, ICSCA, 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

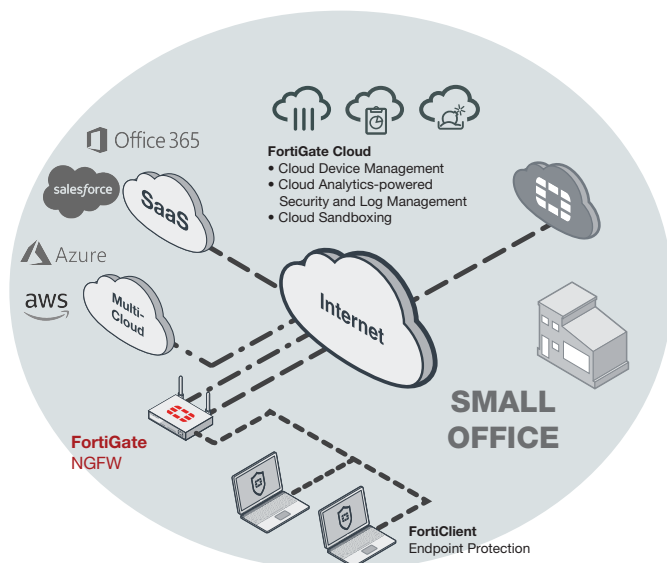
| Firewall | IPS | NGFW | Threat Protection | Interfaces |
|----------|----------|----------|-------------------|---|
| 2.5 Gbps | 350 Mbps | 220 Mbps | 160 Mbps | Multiple GE RJ45 WiFi variants Variants with dual radios Variants with internal storage |

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

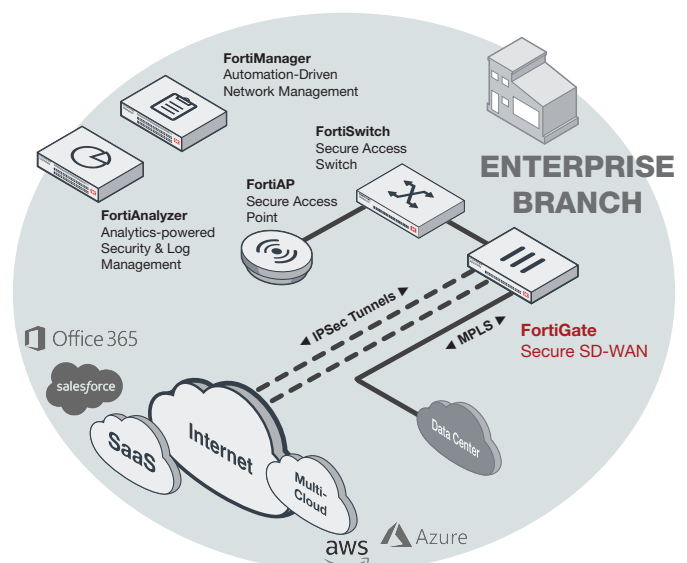


FortiWiFi 50E deployment in Small Office (NGFW)



Secure SD-WAN

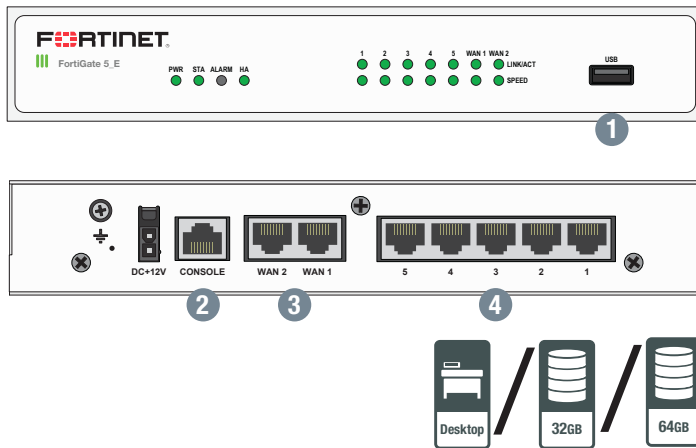
- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplification with zero touch deployment and centralized management with auto-provisioning, analytics and reporting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



FortiGate 50E deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate 50/51



Interfaces

1. USB Port
2. Console RJ45
3. 2x GE RJ45 WAN Ports
4. 5x GE RJ45 Switch Ports

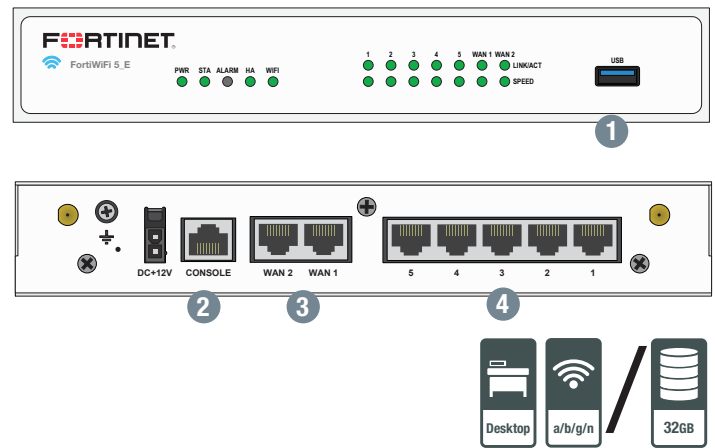
Install in Minutes with FortiExplorer

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.

FortiWiFi 50E/-2R and 51E



Interfaces

1. USB Port
2. Console RJ45
3. 2x GE RJ45 WAN Ports
4. 5x GE RJ45 Switch Ports

Compact and Reliable Form Factor

Designed for small environments, you can simply place the FortiGate/FortiWiFi 50E series 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

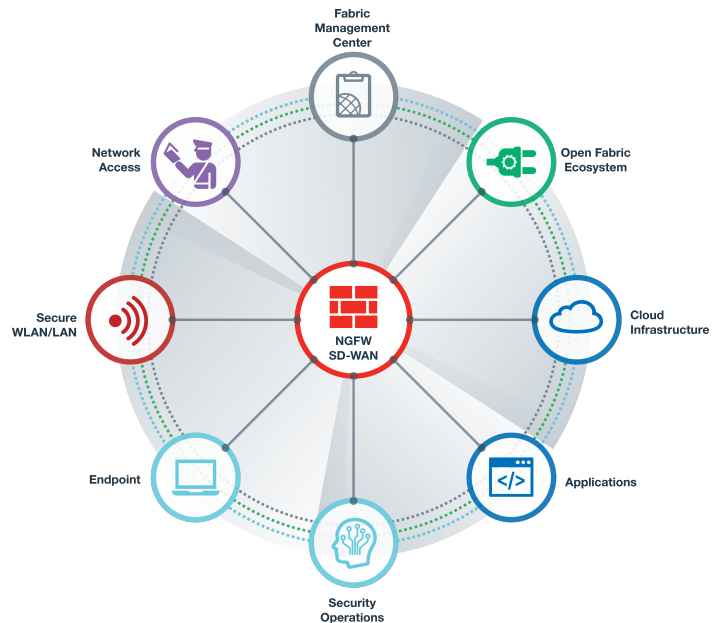
A built-in dual-band, dual-stream access point on the FortiWiFi 50E-2R provides speedy 802.11ac coverage on 2.4 GHz or 5 GHz bands. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning.

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

FortiGate is 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™ Security 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.



FortiCare™ Support Services

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 and forti.net/forticare

Specifications

| | FG-50E | FWF-50E | FWF-50E-2R | FG-51E | FWF-51E |
|--|-------------------------|------------------------------------|---|------------------------|------------------------------------|
| Hardware Specifications | | | | | |
| GE RJ45 Switch Ports | | | 5 | | |
| GE RJ45 WAN Ports | | | 2 | | |
| USB Ports | | | 1 | | |
| Console (RJ45) | | | 1 | | |
| Wireless Interface | — | 802.11 a/b/g/n | dual radio, 802.11a/b/g/n/ac | — | 802.11 a/b/g/n |
| Internal Storage | — | — | — | 1x 32 GB SSD | 1x 32 GB SSD |
| System Performance — Enterprise Traffic Mix | | | | | |
| IPS Throughput ² | | | 350 Mbps | | |
| NGFW Throughput ^{2,4} | | | 220 Mbps | | |
| Threat Protection Throughput ^{2,5} | | | 160 Mbps | | |
| System Performance | | | | | |
| Firewall Throughput | | | 2.5 Gbps | | |
| Firewall Latency (64 byte UDP packets) | | | 180 μs | | |
| Firewall Throughput (Packets Per Second) | | | 375 Kpps | | |
| Concurrent Sessions (TCP) | | | 1.8 Million | | |
| New Sessions/Second (TCP) | | | 21,000 | | |
| Firewall Policies | | | 5,000 | | |
| IPsec VPN Throughput (512 byte) ¹ | | | 90 Mbps | | |
| Gateway-to-Gateway IPsec VPN Tunnels | | | 200 | | |
| Client-to-Gateway IPsec VPN Tunnels | | | 250 | | |
| SSL-VPN Throughput | | | 100 Mbps | | |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | | | 200 | | |
| SSL Inspection Throughput (IPS, avg. HTTPS) ³ | | | 150 Mbps | | |
| SSL Inspection CPS (IPS, avg. HTTPS) ³ | | | 140 | | |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³ | | | 75,000 | | |
| Application Control Throughput (HTTP 64K) ² | | | 450 Mbps | | |
| CAPWAP Throughput (HTTP 64K) | | | 1.2 Gbps | | |
| Virtual Domains (Default / Maximum) | | | 5 / 5 | | |
| Maximum Number of FortiSwitches Supported | | | 8 | | |
| Maximum Number of FortiAPs (Total / Tunnel Mode) | | | 10 / 5 | | |
| Maximum Number of FortiTokens | | | 500 | | |
| High Availability Configurations | | | Active/Active, Active/Passive, Clustering | | |
| Dimensions | | | | | |
| Height x Width x Length (inches) | | | 1.44 x 8.52 x 5.5 | | |
| Height x Width x Length (mm) | | | 36.5 x 216 x 140 | | |
| Weight | 2.015 lbs (0.914 kg) | 2.041 lbs (0.926 kg) | 2.38 lbs (1.08 kg) | 2.04 lbs (0.925 kg) | 2.04 lbs (0.925 kg) |
| Form Factor | | | Desktop | | |
| Radio Specifications | | | | | |
| MIMO | — | 2x2 | 2x2 | — | 2x2 |
| Maximum Wi-Fi Speeds | — | 300 Mbps | 876 Mbps | — | 300 Mbps |
| Maximum Tx Power | — | 21 dBm | 21 dBm | — | 21 dBm |
| Antenna Gain | — | 2 dBi @ 5 GHz, 2.4dBi @ 2.4 GHz | 3 dBi @ 5 GHz, 2 dBi @ 2.4 GHz | — | 2 dBi @ 5 GHz, 2.4dBi @ 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.

Specifications

| | FG-50E | FWF-50E | FWF-50E-2R | FG-51E | FWF-51E |
|---|---|-----------|---------------|-----------|-----------|
| Operating Environment and Certifications | | | | | |
| Input Rating | 12Vdc, 2A | | | | |
| Power Required | Powered by External DC Power Adapter, 100–240V AC, 50–60 Hz | | | | |
| Maximum Current | 100 V / 0.6 A, 240 V / 0.4 A | | | | |
| Power Consumption (Average / Maximum) | 15 / 18 W | 18 / 22 W | 22.1 / 26.5 W | 16 / 20 W | 19 / 23 W |
| Heat Dissipation | 62 BTU/h | 75 BTU/h | 90 BTU/h | 67 BTU/h | 79 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 | Fanless 0 dBA | | | | |
| Operating Altitude | Up to 7,400 ft (2,250 m) | | | | |
| Regulatory Compliance | FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB | | | | |
| Certifications | ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN | | | | |

Order Information

| Product | SKU | Description |
|---------------------------|----------------|---|
| FortiGate 50E | FG-50E | 7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports) |
| FortiWiFi 50E | FWF-50E | 7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), Wireless (802.11a/b/g/n) |
| FortiWiFi 50E-2R | FWF-50E-2R | 7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), dual radio wireless (802.11a/b/g/n/ac) |
| FortiGate 51E | FG-51E | 7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), 32 GB SSD onboard storage |
| FortiWiFi 51E | FWF-51E | 7x GE RJ45 ports (including 2x WAN ports, 5x Switch ports), Wireless (802.11a/b/g/n), 32 GB SSD onboard storage |
| Optional Accessory | | |
| Rack Mount Tray | SP-RACKTRAY-02 | Rack mount tray for FG-30D, FG-40C, FG-50/51E, FG-60C, FG-60D/-POE, FG-70D, FG-80D, FG-90D/-POE, FAD-100E, FRC-100D, FWB-100D, FML-60D, FVE-100E. |

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 ¹ | 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 ² | • | | | |
| SD-WAN Overlay Controller VPN Service ² | • | | | |
| FortiAnalyzer Cloud ² | • | | | |
| FortiManager Cloud ² | • | | | |

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



www.fortinet.com

Copyright © 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

FortiGate/FortiWiFi® 60E Series

FortiGate 60E, 60E-POE, FortiWiFi 60E, FortiGate 61E, and FortiWiFi 61E

Secure SD-WAN
Next Generation Firewall



The FortiGate/FortiWiFi 60E 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, ICSA, 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

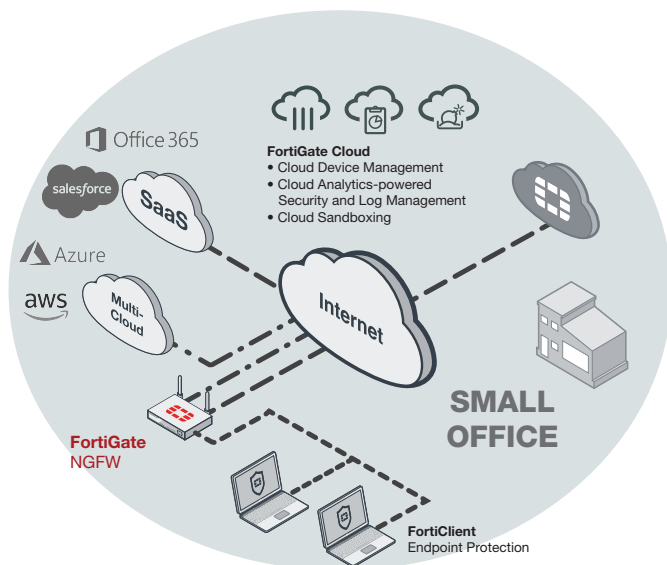
| Firewall | IPS | NGFW | Threat Protection | Interfaces |
|---------------|-----------------|-----------------|-------------------|--|
| 3 Gbps | 400 Mbps | 250 Mbps | 200 Mbps | Multiple GE RJ45 WiFi variants Variants with internal storage Variants with PoE/+ interfaces |

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

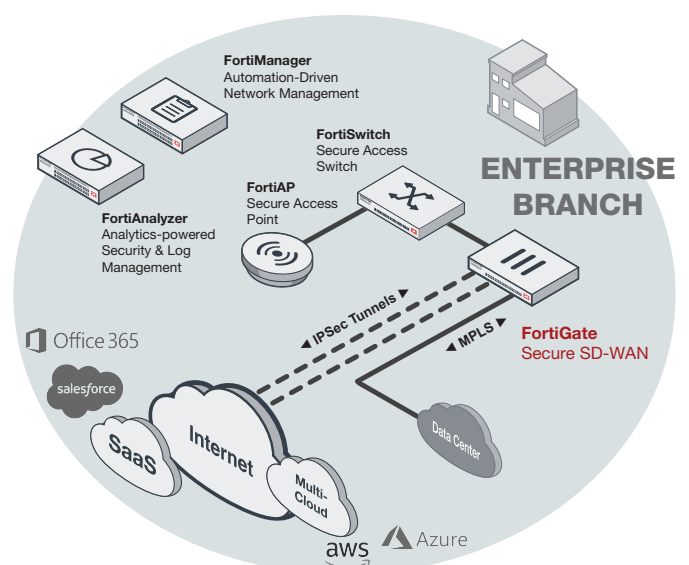


FortiWiFi 60E deployment in Small Office (NGFW)



Secure SD-WAN

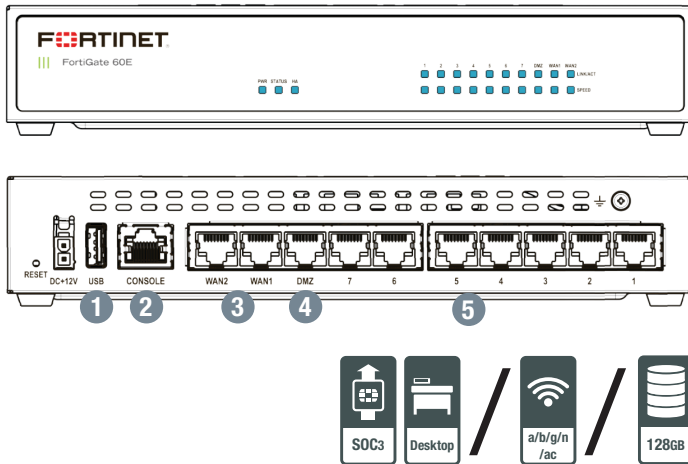
- Consistent business application performance with accurate detection, dynamic WAN path steering and optimization
- Multi-cloud access for faster SaaS adoption with end-to-end optimization
- Simplification with zero touch deployment and centralized management with auto-provisioning, analytics and reporting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



FortiGate 60E deployment in Enterprise Branch (Secure SD-WAN)

Hardware

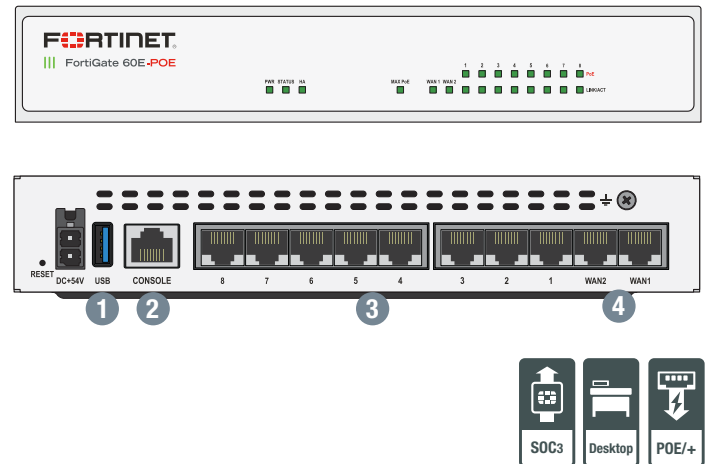
FortiGate/FortiWiFi 60E/61E



Interfaces

1. USB Port
2. Console Port
3. 2x GE RJ45 WAN Ports
4. 1x GE RJ45 DMZ Port
5. 7x GE RJ45 Internal Ports

FortiGate 60E-POE



Interfaces

1. USB Port
2. Console Port
3. 8x GE RJ45 PoE/+ Ports
4. 2x GE RJ45 WAN Ports

Powered by SPU SoC3

- Combines a RISC-based CPU with Fortinet's proprietary SPU content and network processors for unmatched performance
- Simplifies appliance design and enables breakthrough performance for smaller networks
- Supports firewall acceleration across all packet sizes for maximum throughput
- Delivers accelerated UTM content processing for superior performance and protection
- Accelerates VPN performance for high speed and secure remote access



3G/4G WAN Connectivity

The FortiGate/FortiWiFi 60E 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 superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

Superior Wireless Coverage

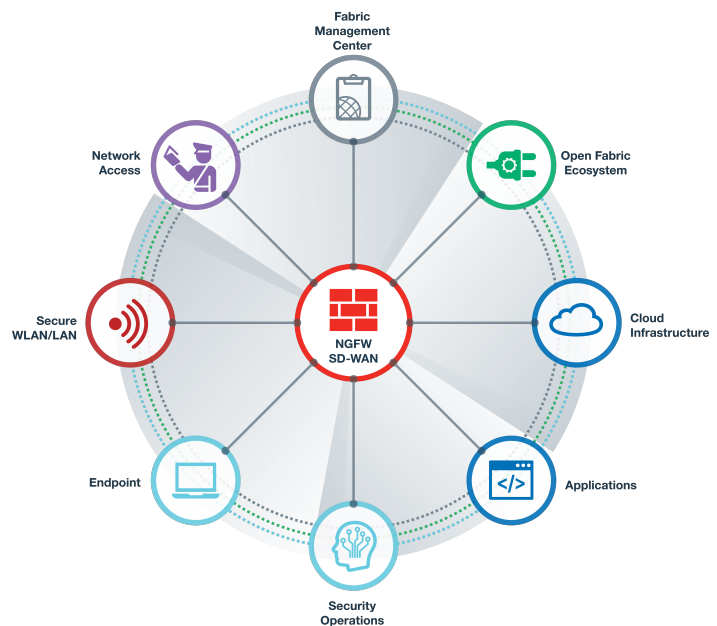
A built-in dual-band, dual-stream access point with internal antennas is integrated on the FortiWiFi 60E and provides speedy 802.11ac wireless access. The dual-band chipset addresses the PCI-DSS compliance requirement for rogue AP wireless scanning, providing maximum protection for regulated environments.

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™ Security 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.



FortiCare™ Support Services

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 and forti.net/forticare

Specifications

| | FORTIGATE 60E | FORTIGATE 60E-POE | FORTIWIFI 60E | FORTIGATE 61E | FORTIWIFI 61E |
|--|------------------|-------------------|---|------------------|---------------------------------------|
| Hardware Specifications | | | | | |
| GE RJ45 WAN / DMZ Ports | 2 / 1 | 2 | 2 / 1 | 2 / 1 | |
| GE RJ45 Internal Ports | 7 | — | 7 | 7 | |
| GE RJ45 PoE/+ Ports | — | 8 | — | — | |
| Wireless Interface | — | — | 802.11 a/b/g/n/ac | — | 802.11 a/b/g/n/ac |
| USB Ports | 1 | 1 | 1 | 1 | |
| Console (RJ45) | 1 | 1 | 1 | 1 | |
| Internal Storage | — | — | — | 1x 128 GB SSD | |
| System Performance — Enterprise Traffic Mix | | | | | |
| IPS Throughput ² | | | 400 Mbps | | |
| NGFW Throughput ^{2,4} | | | 250 Mbps | | |
| Threat Protection Throughput ^{2,5} | | | 200 Mbps | | |
| System Performance | | | | | |
| Firewall Throughput (1518 / 512 / 64 byte UDP packets) | | | 3 / 3 / 3 Gbps | | |
| Firewall Latency (64 byte UDP packets) | | | 3 μs | | |
| Firewall Throughput (Packets Per Second) | | | 4.5 Mpps | | |
| Concurrent Sessions (TCP) | | | 1.3 Million | | |
| New Sessions/Second (TCP) | | | 30,000 | | |
| Firewall Policies | | | 5,000 | | |
| IPsec VPN Throughput (512 byte) ¹ | | | 2 Gbps | | |
| Gateway-to-Gateway IPsec VPN Tunnels | | | 200 | | |
| Client-to-Gateway IPsec VPN Tunnels | | | 500 | | |
| SSL-VPN Throughput | | | 150 Mbps | | |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | | | 200 | | |
| SSL Inspection Throughput (IPS, avg. HTTPS) ³ | | | 135 Mbps | | |
| SSL Inspection CPS (IPS, avg. HTTPS) ³ | | | 135 | | |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³ | | | 75,000 | | |
| Application Control Throughput (HTTP 64K) ² | | | 650 Mbps | | |
| CAPWAP Throughput (HTTP 64K) | | | 890 Mbps | | |
| Virtual Domains (Default / Maximum) | | | 10 / 10 | | |
| Maximum Number of FortiSwitches Supported | | | 16 | | |
| Maximum Number of FortiAPs (Total / Tunnel Mode) | | | 30 / 10 | | |
| Maximum Number of FortiTokens | | | 500 | | |
| High Availability Configurations | | | Active / Active, Active / Passive, Clustering | | |
| Dimensions | | | | | |
| Height x Width x Length (inches) | | | 1.5 x 8.5 x 6.3 | | |
| Height x Width x Length (mm) | | | 38 x 216 x 160 | | |
| Weight | 1.9 lbs (0.9 kg) | 2.2 lbs (1.0 kg) | 1.9 lbs (0.9 kg) | 1.9 lbs (0.9 kg) | 1.9 lbs (0.9 kg) |
| Form Factor | | | Desktop | | |
| Radio Specifications | | | | | |
| Multiple User (MU) MIMO | — | — | 2x2 | — | 2x2 |
| Maximum Wi-Fi Speeds | — | — | 876 Mbps @ 5GHz, 300 Mbps @ 2.4GHz | — | 876 Mbps @ 5GHz, 300 Mbps @ 2.4GHz |
| Maximum Tx Power | — | — | 21 dBm | — | 21 dBm |
| Antenna Gain | — | — | 6 dBi @ 5 GHz, 3 dBi @ 2.4 GHz | — | 6 dBi @ 5 GHz, 3 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.

Specifications

| | FORTIGATE 60E | FORTIGATE 60E-POE | FORTIWIFI 60E | FORTIGATE 61E | FORTIWIFI 61E |
|--|---|-------------------|-----------------------------------|-----------------------------------|-----------------------------------|
| Operating Environment and Certifications | | | | | |
| Input Rating | 12Vdc, 3A | 12Vdc, 7A | 12Vdc, 3A | 12Vdc, 3A | 12Vdc, 3A |
| Power Required | Powered by External DC Power Adapter, 100–240V AC, 50–60 Hz | | | | |
| Maximum Current | 115V AC / 0.7 A, 230V AC / 0.48 A | 0.8A | 115V AC / 0.9A, 230V AC / 0.6A | 115V AC / 0.9A, 230V AC / 0.6A | 115V AC / 0.9A, 230V AC / 0.6A |
| Total Available PoE Power Budget* | – | 75 W | – | – | – |
| Power Consumption (Average / Maximum) | 11.5 / 14 W | 20 / 95 W | 12.6 / 15.2 W | 11.9 / 14.3 W | 13 / 16 W |
| Heat Dissipation | 48 BTU/h | 324 BTU/h | 52 BTU/h | 49 BTU/h | 55 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 | 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 | | | | |

* Maximum loading on each PoE/+ port is 30 W (802.3at).

Order Information

| Product | SKU | Description |
|-------------------|------------|---|
| FortiGate 60E | FG-60E | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port) |
| FortiGate 60E-POE | FG-60E-POE | 10x GE RJ45 ports (including 8x PoE/PoE+ ports, 2x WAN ports) |
| FortiWiFi 60E | FWF-60E | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), Wireless (802.11a/b/g/n/ac) |
| FortiGate 61E | FG-61E | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage |
| FortiWiFi 61E | FWF-61E | 10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), Wireless (802.11a/b/g/n/ac), 128 GB SSD onboard storage |

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 ¹ | 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 ² | • | • | | |
| FortiConverter Service | • | • | | |
| IPAM Cloud ² | • | | | |
| SD-WAN Orchestrator Entitlement ² | • | | | |
| 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



www.fortinet.com