Manuals+

Q & A | Deep Search | Upload

manuals.plus /

› FORTINET /

› Fortinet FortiGate-201F Unified Threat Protection Appliance User Manual

FORTINET FortiGate-201F

Fortinet FortiGate-201F Unified Threat Protection Appliance User Manual

Model: FortiGate-201F

1. Product Overview

The FortiGate-201F series is designed to provide an application-centric, scalable, and secure SD-WAN solution. It integrates Next-Generation Firewall (NGFW) capabilities suitable for mid-sized to large enterprises, typically deployed at campus or enterprise branch levels.

This appliance is engineered to prevent and detect known attacks through continuous threat intelligence from AI-powered FortiGuard Labs security services. It also proactively blocks unknown sophisticated attacks in real-time using the Fortinet Security Fabric's integrated AI-powered FortiSandbox.

The Security Fabric offers broad visibility, integrated AI-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and ecosystem deployments. This allows security to dynamically expand and adapt as workloads and data are added, ensuring protection for data, users, and applications across IoT, devices, and cloud environments.

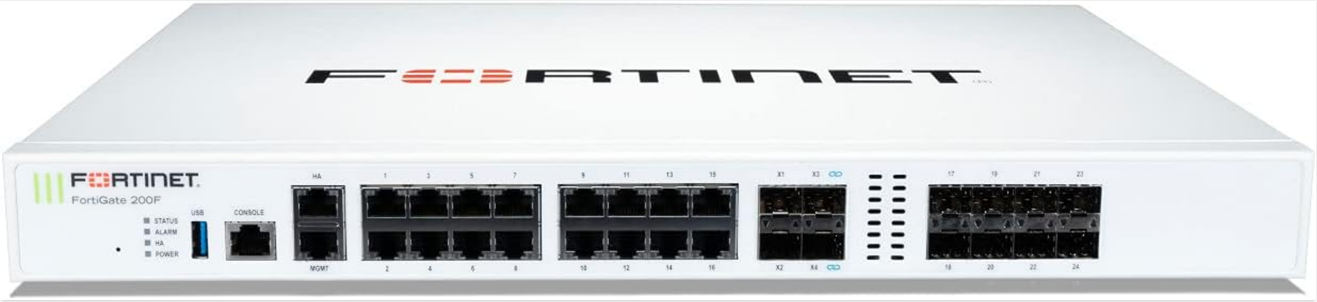


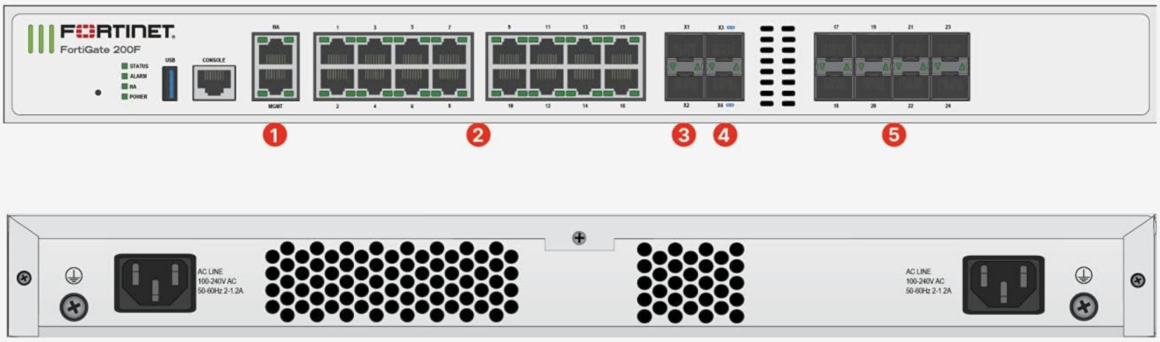
Figure 1: Front view of the FortiGate-201F appliance, showing various network ports and status indicators.

2. Key Features

- **Advanced Threat Protection:** Prevents and detects known and unknown attacks using AI-powered FortiGuard Labs and FortiSandbox.
- **SD-WAN Capabilities:** Provides a secure, application-centric, and scalable SD-WAN solution.
- **Fortinet Security Fabric Integration:** Delivers broad visibility, integrated AI-driven breach prevention, and

automated security operations.

- **High-Performance Hardware:** Features NP6XLite and CP9 hardware acceleration for efficient processing.
- **Extensive Connectivity:** Includes 18 x GE RJ45 ports (1 MGMT, 1 HA, 16 switch), 8 x GE SFP slots, and 4 x 10GE SFP+ slots.
- **Onboard Storage:** Equipped with 480GB onboard SSD storage.
- **FortiCare Support:** Includes 3-year 24x7 FortiCare support for prioritized assistance and application control services.



Interfaces

1. 2x GE RJ45 HA / MGMT Ports
2. 16x GE RJ45 Ports
3. 2x 10 GE SFP+ Slots
4. 2x 10 GE SFP+ FortiLink Slots
5. 8x GE SFP Slots

Hardware Features

NP6X Lite | CP9 | 1U | TPM | AC DUAL | / | 480GB

Figure 2: Detailed diagram of FortiGate-201F interfaces and hardware features, including port types and internal components.

3. Setup and Installation

3.1 Unpacking and Inspection

Carefully unpack the FortiGate-201F appliance from its packaging. Inspect the device for any signs of physical damage. Ensure all components listed in the packing slip are present.

3.2 Rack Mounting (Optional)

The FortiGate-201F is designed for rack mounting. Use the provided rack-mount kit to secure the appliance in a standard 19-inch equipment rack. Ensure adequate ventilation around the unit.

3.3 Connecting Power

Connect the power cables to the power supply units at the rear of the appliance and then to appropriate power outlets. The FortiGate-201F supports dual AC power supplies for redundancy.

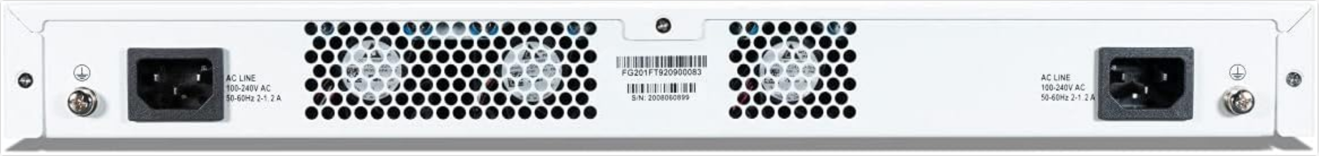


Figure 3: Rear view of the FortiGate-201F, highlighting the dual power supply inputs and cooling fans.

3.4 Network Connections

1. **Management Port (MGMT):** Connect an Ethernet cable from your management workstation to the MGMT port for initial configuration.
2. **HA Port:** If deploying in a High Availability (HA) cluster, connect the HA port to another FortiGate unit.
3. **WAN/LAN Ports:** Connect your Wide Area Network (WAN) and Local Area Network (LAN) cables to the appropriate GE RJ45, GE SFP, or 10GE SFP+ ports as per your network design.
4. **Console Port:** For direct console access, connect a serial cable from your workstation to the CONSOLE port.

3.5 Initial Configuration

Refer to the Fortinet documentation for detailed instructions on initial configuration, including setting up network interfaces, administrative access, and basic security policies. This typically involves accessing the device via a web browser or command-line interface (CLI).

4. Operating Instructions

The FortiGate-201F operates as a comprehensive network security appliance. Once configured, it will actively monitor and protect your network traffic.

4.1 Accessing the Management Interface

Access the FortiGate's web-based management interface by entering its IP address into a web browser. Log in with your administrative credentials. The dashboard provides an overview of system status, network activity, and security events.

4.2 Monitoring System Status

Regularly check the system status indicators on the front panel and the dashboard in the management interface. These indicators provide information on power, system health, and network activity.

- **POWER LED:** Indicates power status.
- **STATUS LED:** Indicates system operational status.
- **ALARM LED:** Indicates critical system alerts.
- **HA LED:** Indicates High Availability status.

4.3 Security Policy Management

Manage security policies to control traffic flow, apply threat protection profiles, and enforce access rules. Policies can be configured to inspect traffic for viruses, malware, intrusions, and other threats.

4.4 SD-WAN Configuration

Utilize the SD-WAN features to optimize network performance, manage multiple WAN links, and ensure application-centric routing. This includes configuring SD-WAN zones, rules, and performance SLAs.

4.5 Firmware Updates

Keep the FortiGate firmware updated to ensure the latest security features, bug fixes, and performance enhancements. Firmware updates are typically performed through the management interface or CLI.

5. Maintenance

Regular maintenance ensures optimal performance and longevity of your FortiGate-201F appliance.

5.1 Environmental Considerations

Ensure the operating environment is within specified temperature and humidity ranges. Maintain clear airflow around the appliance to prevent overheating. Avoid placing the unit near heat sources or in enclosed spaces.

5.2 Software Maintenance

- **Firmware Updates:** Regularly check for and apply the latest firmware versions.
- **FortiGuard Updates:** Ensure FortiGuard services (antivirus, IPS, web filtering, etc.) are receiving continuous updates for the most current threat intelligence.
- **Configuration Backups:** Periodically back up your FortiGate configuration to a secure location.

5.3 Hardware Inspection

Periodically inspect the physical condition of the appliance, including power cables, network cables, and ventilation openings. Clean any dust accumulation from the vents to maintain proper cooling.

6. Troubleshooting

This section provides solutions to common issues you might encounter with your FortiGate-201F.

6.1 No Power

- **Check Power Cables:** Ensure power cables are securely connected to both the appliance and the power outlet.
- **Verify Power Source:** Confirm that the power outlets are functional.
- **Inspect Power Supply:** If using dual power supplies, check if one is operational.

6.2 Network Connectivity Issues

- **Check Cable Connections:** Ensure all Ethernet and SFP/SFP+ cables are properly seated.
- **Verify Port Status:** Check the link/activity LEDs on the FortiGate ports and connected devices.
- **Review Configuration:** Confirm that network interface settings (IP addresses, VLANs) and security policies are correctly configured.
- **Test with Console:** Use the console port for direct access to diagnose network interface status via CLI.

6.3 Management Interface Inaccessible

- **IP Address:** Verify you are using the correct IP address for the management interface.

- **Network Path:** Ensure there is a network path between your workstation and the FortiGate.
- **Browser Issues:** Try a different web browser or clear browser cache.
- **Console Access:** If web access fails, use the console port to check network settings and service status.

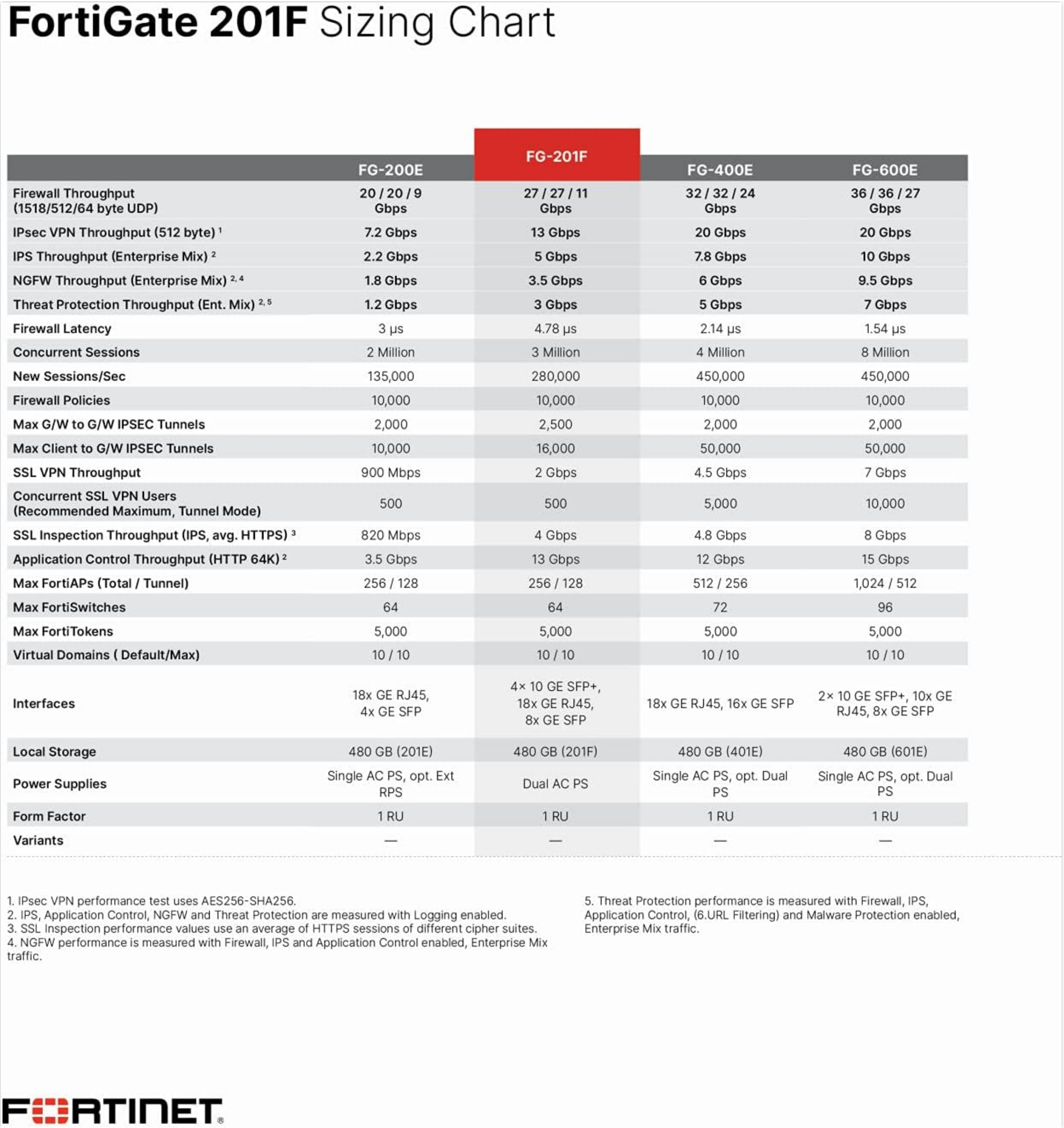
6.4 Performance Degradation

- **Resource Monitoring:** Check CPU, memory, and session usage from the dashboard.
- **Policy Optimization:** Review security policies for inefficiencies or excessive logging.
- **Firmware:** Ensure the latest firmware is installed.
- **FortiGuard Updates:** Verify FortiGuard services are up-to-date.

7. Technical Specifications

FortiGate-201F Hardware Specifications

Feature	Detail
Model Name	FortiGate-201F
Product Dimensions	13.5 x 17 x 1.7 inches
Item Weight	10.14 pounds
Manufacturer	Fortinet, Inc
Connectivity Technology	Ethernet
Wireless Communication Standard	802.11ac *(Note: This refers to general Fortinet capabilities; the 201F itself is a wired appliance.)*
Ports	18 x GE RJ45 (1 MGMT, 1 HA, 16 switch), 8 x GE SFP slots, 4 x 10GE SFP+ slots
Hardware Acceleration	NP6XLite and CP9
Onboard Storage	480GB SSD
Power Supplies	Dual AC (redundant)
Recommended Use	Security



FortiGate 201F Sizing Chart

	FG-200E	FG-201F	FG-400E	FG-600E
Firewall Throughput (1518/512/64 byte UDP)	**20 / 20 / 9 Gbps**	**27 / 27 / 11 Gbps**	**32 / 32 / 24 Gbps**	**36 / 36 / 27 Gbps**
IPsec VPN Throughput (512 byte) [1]	**7.2 Gbps**	**13 Gbps**	**20 Gbps**	**20 Gbps**
IPS Throughput (Enterprise Mix) [2]	**2.2 Gbps**	**5 Gbps**	**7.8 Gbps**	**10 Gbps**
NGFW Throughput (Enterprise Mix) [2, 4]	**1.8 Gbps**	**3.5 Gbps**	**6 Gbps**	**9.5 Gbps**
Threat Protection Throughput (Ent. Mix) [2, 5]	**1.2 Gbps**	**3 Gbps**	**5 Gbps**	**7 Gbps**
Firewall Latency	3 µs	4.78 µs	2.14 µs	1.54 µs
Concurrent Sessions	2 Million	3 Million	4 Million	8 Million
New Sessions/Sec	135,000	280,000	450,000	450,000
Firewall Policies	10,000	10,000	10,000	10,000
Max G/W to G/W IPSEC Tunnels	2,000	2,500	2,000	2,000
Max Client to G/W IPSEC Tunnels	10,000	16,000	50,000	50,000
SSL VPN Throughput	900 Mbps	2 Gbps	4.5 Gbps	7 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	500	500	5,000	10,000
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	820 Mbps	4 Gbps	4.8 Gbps	8 Gbps
Application Control Throughput (HTTP 64K) [2]	3.5 Gbps	13 Gbps	12 Gbps	15 Gbps
Max FortiAPs (Total / Tunnel)	256 / 128	256 / 128	512 / 256	1,024 / 512
Max FortiSwitches	64	64	72	96
Max FortiTokens	5,000	5,000	5,000	5,000
Virtual Domains (Default/Max)	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces	18x GE RJ45, 4x GE SFP	4× 10 GE SFP+, 18x GE RJ45, 8x GE SFP	18x GE RJ45, 16x GE SFP	2× 10 GE SFP+, 10x GE RJ45, 8x GE SFP
Local Storage	480 GB (201E)	480 GB (201F)	480 GB (401E)	480 GB (601E)
Power Supplies	Single AC PS, opt. Ext RPS	Dual AC PS	Single AC PS, opt. Dual PS	Single AC PS, opt. Dual PS
Form Factor	1 RU	1 RU	1 RU	1 RU
Variants	—	—	—	—

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS, 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, Enterprise Mix traffic.
5. Threat Protection performance is measured with Firewall, IPS, Application Control, (6.URL Filtering) and Malware Protection enabled, Enterprise Mix traffic.

Figure 4: FortiGate 201F Sizing Chart, providing performance metrics such as firewall throughput, IPS throughput, and SSL inspection capabilities.

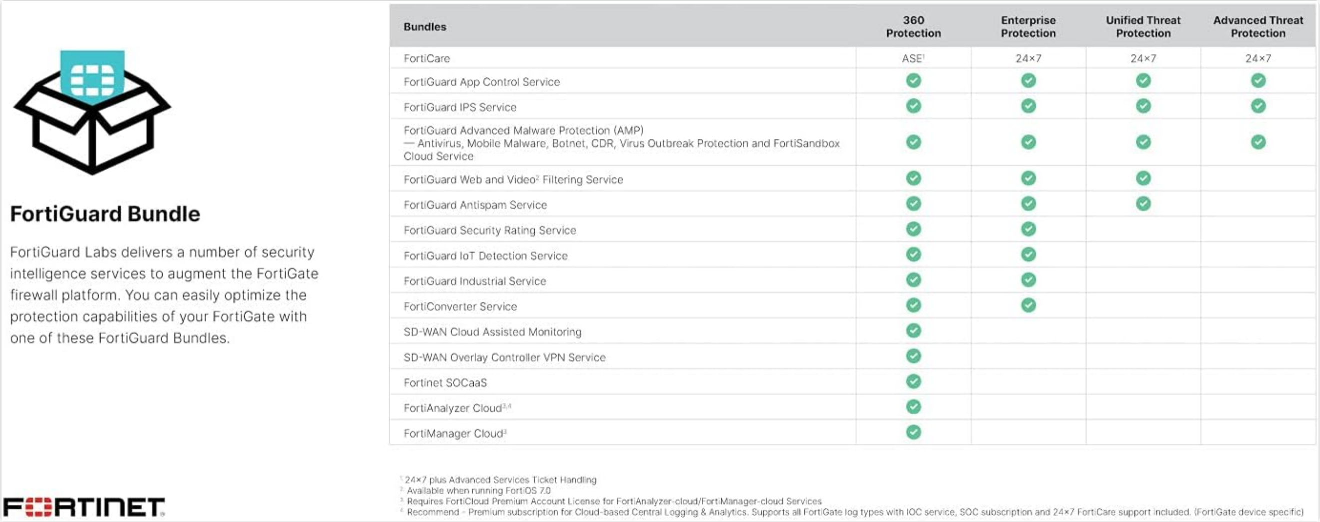
8. Warranty and Support

8.1 FortiCare Support

This FortiGate-201F appliance includes 3 years of 24x7 FortiCare support. FortiCare provides prioritized support, ensuring assistance is available around the clock, every day of the year. This service also includes application control services designed to protect your network and ensure resources are utilized for business objectives.

8.2 FortiGuard Unified Threat Protection (UTP)

The product bundle includes FortiGuard Unified Threat Protection (UTP) services. FortiGuard services deliver comprehensive security intelligence, including antivirus, intrusion prevention, web filtering, and anti-spam, to protect against a wide range of cyber threats.



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	Advanced Threat Protection
FortiCare	ASE[1]	24×7	24×7	24×7
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 and Video[2] Filtering Service	✓	✓	✓	
FortiGuard Antispam Service	✓	✓	✓	
FortiGuard Security Rating Service	✓	✓		
FortiGuard IoT Detection Service	✓	✓		
FortiGuard Industrial Service	✓	✓		
FortiConverter Service	✓	✓		
SD-WAN Cloud Assisted Monitoring	✓			
SD-WAN Overlay Controller VPN Service	✓			
Fortinet SOCaaS	✓			
FortiAnalyzer Cloud[3,4]	✓			
FortiManager Cloud[3]	✓			

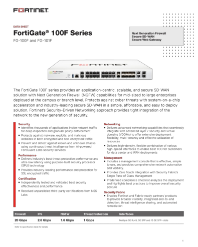
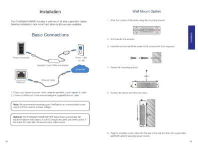
[1] 24×7 plus Advanced Services Ticket Handling
[2] Available when running FortiOS 7.0
[3] Requires FortiCloud Premium Account License for FortiAnalyzer-cloud/FortiManager-cloud Services
[4] Recommend - Premium subscription for Cloud-based Central Logging & Analytics. Supports all FortiGate log types with IOC service, SOC subscription and 24×7 FortiCare support included. (FortiGate device specific)

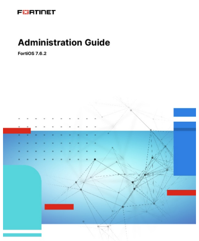
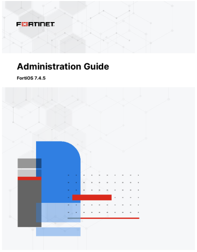
Figure 5: FortiGuard Bundle comparison chart, detailing the services included with various protection levels such as FortiCare, FortiGuard App Control, IPS, Advanced Malware Protection, and more.

8.3 Contacting Support

For technical assistance, warranty claims, or further information regarding your FortiGate-201F, please refer to the official Fortinet support portal or contact your authorized Fortinet reseller. Ensure you have your product serial number available when contacting support.
Official Fortinet Support: https://support.fortinet.com

Related Documents - FortiGate-201F

	FortiGate 1100E Series Next-Generation Firewall | Fortinet Fortinet FortiGate 1100E NGFW SD-WAN
	FortiGate 100F Series: Next Generation Firewall, Secure SD-WAN, and Secure Web Gateway Data Sheet Data sheet detailing the Fortinet FortiGate 100F Series (FG-100F, FG-101F), a scalable and secure SD-WAN solution with Next Generation Firewall (NGFW) and Secure Web Gateway capabilities for mid-sized to large enterprises. Features include system-on-a-chip acceleration, advanced threat protection, and comprehensive management.
	FortiGate/FortiWiFi Installation and Setup Guide Comprehensive guide to installing, setting up, and configuring FortiGate and FortiWiFi network security devices, covering physical installation options, various setup methods (GUI, Cloud, CLI), licensing, services, and the Fortinet Security Fabric.

	FortiOS 7.6.2 Administration Guide | Fortinet Network Security Comprehensive administration guide for FortiOS 7.6.2, detailing its features as a hybrid mesh firewall, SD-WAN, and ZTNA solution. Learn about setup, configuration, security profiles, and management for Fortinet's network security operating system.
	FortiOS 7.4.5 Administration Guide | Fortinet Comprehensive guide to administering FortiOS 7.4.5, the operating system for Fortinet's FortiGate Next-Generation Firewalls. Covers setup, configuration, security features, SD-WAN, ZTNA, and more for robust network protection.
	FortiGate 200F Series QuickStart Guide This guide provides essential information for setting up and operating the FortiGate 200F Series firewall, including hardware overview, setup options, and basic configuration.