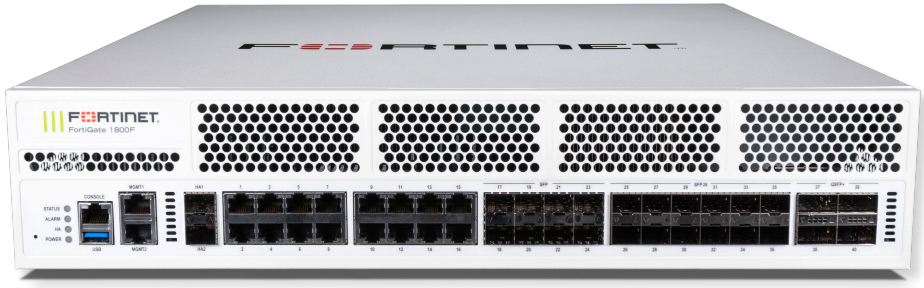
DATA SHEET

FortiGate®1800F Series

FortiGate 1800F and 1801F

Next Generation Firewall
Segmentation
Secure Web Gateway
IPS
Mobile Security



The FortiGate 1800F series delivers high performance next generation firewall (NGFW) capabilities for large enterprises and service providers. With multiple high-speed interfaces, high-port density and high-throughput, ideal deployments are at the enterprise edge, hybrid and hyperscale data center core and across internal segments. Leverage industry-leading IPS, SSL inspection and advanced threat protection to optimize your network's performance. Fortinet's Security-Driven Networking securely integrates with the new generation of cybersecurity solutions.

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
198 Gbps	**13 Gbps**	**11 Gbps**	**9.1 Gbps**	Multiple GE RJ45, GE SFP, 10GE SFP+ HA, GE SFP28 and 40GE QSFP+ Ports

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 security effectiveness, 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

Segmentation

- Segmentation that adapts to any network topology, delivering end-to-end security from the branch level to data centers and extending to multiple clouds
- Reduce security risks by improving network visibility from the components of the Fortinet Security Fabric, which adapt access permissions to current levels of trust and enforce access control effectively and efficiently
- Delivers defense in depth security powered by high-performance L7 inspection and remediation by Fortinet's SPU, while delivering third party validated TCO of per protected Mbps
- Protects critical business applications and helps implement any compliance requirements without network redesigns

Secure Web Gateway (SWG)

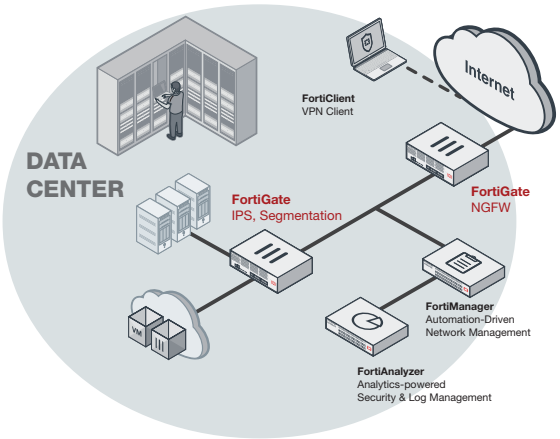
- Secure web access from both internal and external risks, even for encrypted traffic at high performance
- Enhanced user experience with dynamic web and video caching
- Block and control web access based on user or user groups across URL's and domains
- Prevent data loss and discover user activity to known and unknown cloud applications
- Block DNS requests against malicious domains
- Multi-layered advanced protection against zero-day malware threats delivered over the web

IPS

- Purpose-built security processors delivering industry validated IPS performance with high throughput and low latency
- Deploy virtual patches at the network level to protect against network exploitable vulnerabilities and optimize network protection time
- Deep packet inspection at wire speeds offers unparalleled threat visibility into network traffic including traffic encrypted with the latest TLS 1.3
- Proactively block newly discovered sophisticated attacks in real-time with advanced threat protection provided by the intelligence services of the Fortinet Security Fabric

Mobile Security for 4G, 5G, and IOT

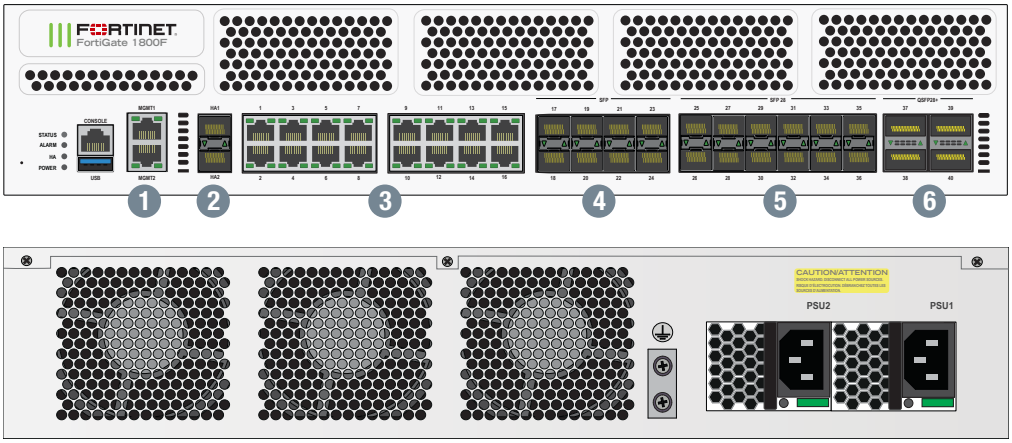
- Experience high performance networking speeds with FQ, CGAT and accelerated IPv4 and IPv6 traffic, powered by multiple SPUs and 4G SGi LAN and 5G N6 security.
- RAN Access Security with highly scalable and best performing IPsec aggregation and control security gateway (SecGW)
- User plane security enabled by full Threat Protection and visibility into GTP-U inspection
- 4G Signaling security to inspect various protocols such as SCTP, Diameter, GTP-C, SIP and provide protection against attacks
- 4G and 5G cores IoT signaling storm protection
- High-speed interfaces to enable deployment flexibility

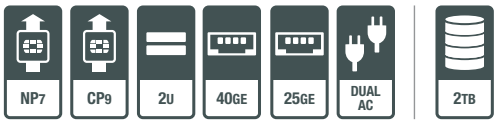


FortiGate 1800F deployment in data center (NGFW, IPS, and Intent-based Segmentation)

Hardware

FortiGate 1800F Series





Interfaces

1. 2 x GE RJ45 MGMT Ports
2. 2 x 10GE SFP+ HA Slots
3. 16 x GE RJ45 Ports
4. 8 x GE SFP Slots
5. 12 x 25GE SFP28/10GE SFP+/GE SFP
6. 4 x 40GE QSFP+ Slots

Powered by SPU

- Custom SPU processors deliver the power you need to detect malicious content at multi-Gigabit speeds
- Other security technologies cannot protect against today's wide range of content and connection-based threats because they rely on general-purpose CPUs, causing a dangerous performance gap
- SPU processors provide the performance needed to block emerging threats, meet rigorous third-party certifications, and ensure that your network security solution does not become a network bottleneck

Network Processor

Fortinet's latest SPU NP7 Hyperscale architecture is a purpose-built network processor that delivers accelerated hardware performance for FortiOS:

- IPv4/IPv6, SCTP, unicast, multicast and anycast
- CAPWAP, VXLAN and GRE IP tunneling
- IPSec VPN (including Suite B)
- DDoS protection in hardware against volumetric attacks, fragment reassembly, traffic shaping and priority queuing
- Elephant Flows of up to 100Gbps

Content Processor

The SPU CP9 content processor works outside of the direct flow of traffic, providing high-speed cryptography and content inspection services including:

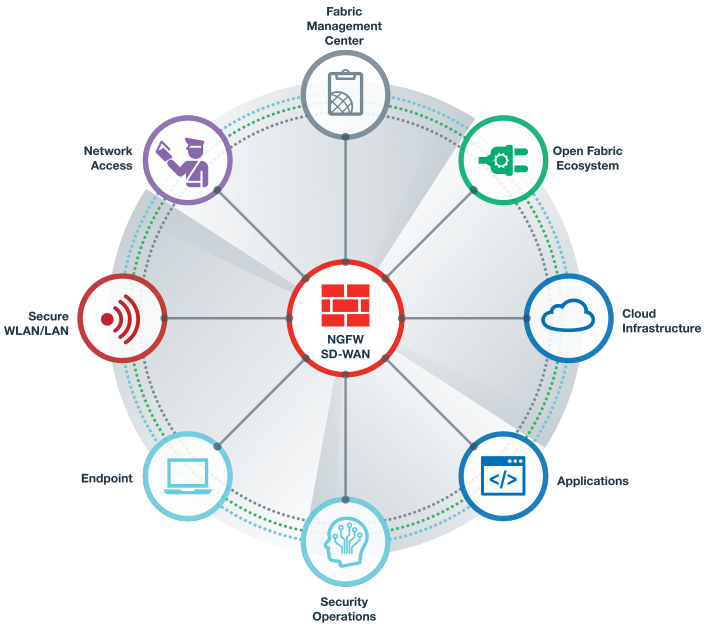
- Signature-based content inspection acceleration
- Encryption and decryption offloading

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 overs 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 threat



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

	FG-1800F	FG-1801F
Hardware Specifications		
Hardware Accelerated GE RJ45 Ports	16	
Hardware Accelerated GE SFP Slots	8	
Hardware Accelerated 25 GE SFP28/10GE SFP+ HA Ports	12	
Hardware Accelerated 40GE QSFP+ Slots	4	
GE RJ45 Management Ports	2	
10GE SFP+ HA Ports	2	
USB 3.0 Port	1	
Console RJ45 Port	1	
Onboard Storage	-	2x 1TB NVMe SSD
Included Transceivers	2x SFP+ (SR 10GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	13 Gbps	
NGFW Throughput [2, 4]	11 Gbps	
Threat Protection Throughput [2, 5]	9.1 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	198 / 197 / 140 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP)	198 / 197 / 140 Gbps	
Firewall Latency (64 byte, UDP)	4 µs	
Firewall Throughput (Packet per Second)	210 Mpps	
Concurrent Sessions (TCP)	12 Million	
New Sessions/Second (TCP)	750,000	
Firewall Policies	100,000	
IPsec VPN Throughput (512 byte) [1]	65 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	20,000	
Client-to-Gateway IPsec VPN Tunnels	100,000	
SSL-VPN Throughput	11 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10,000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	17 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	9,500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	1.3 Million	
Application Control Throughput (HTTP 64K) [2]	34 Gbps	
CAPWAP Throughput (HTTP 64K)	TBA	
Virtual Domains (Default / Maximum)	10 / 250	
Maximum Number of FortiSwitches Supported	128	
Maximum Number of FortiAPs (Total / Tunnel)	4,096 / 1,024	
Maximum Number of FortiTokens	20,000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-1800F	FG-1801F
Dimensions and Power		
Height x Width x Length (inches)	3.5 x 17.25 x 21.1	
Height x Width x Length (mm)	88.4 x 438 x 536	
Weight	30.2 lbs (13.7 kg)	30.4 lbs (13.8 kg)
Form Factor	2RU	
Power Source	100–240VAC, 50-60 Hz	
Maximum Current	7A@100VAC, 3A@240VAC	
Maximum Power Consumption	388.3W	
Average Power Consumption	543.6W	
Heat Dissipation	1,854.84 BTU/hr	
Redundant Power Supplies	Yes, Hot swappable	
Operating Environment and Certifications		
Operating Temperature	32–104°F (0–40°C)	
Storage Temperature	-31–158°F (-35–70°C)	
Humidity	10–90% non-condensing	
Noise Level	62.74 dBA	
Operating Altitude	Up to 7,400 ft (2,250 m)	
Compliance	FCC Part 15 Class A, C-Tick, VCCI, CE, UL/cUL, CB	
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6	

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 1800F	FG-1800F	4 x 40 GE QSFP+ slots, 12 x 25 GE SFP28 /10GE SFP+ slots, 2x10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports, SPU NP7 and CP9 hardware accelerated
FortiGate 1801F	FG-1801F	4 x 40 GE QSFP+ slots, 12 x 25 GE SFP28 /10GE SFP+ slots, 2x10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports, SPU NP7 and CP9 hardware accelerated, 2x 1TB on board SSD storage
Optional Accessories		
1 GE SFP LX transceiver module	FG-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 transceiver module	FG-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX transceiver module	FG-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ transceiver module, short range	FG-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ transceiver module, long range	FG-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ active direct attach cable, 10m / 32.8 ft	SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10m / 32.8 ft for all systems with SFP+ and SFP/SFP+ slots.
25 GE SFP28 transceiver module, long range	FG-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for all systems with SFP28 slots.
25 GE/10 GE Dual Rate SFP28 Transceiver Module, Short Range	FG-TRAN-SFP28-SR	25 GE/10 GE dual rate SFP28 transceiver module, short range for all systems with SFP28/SFP+ slots.
40 GE QSFP+ Transceivers, Short Range	FG-TRAN-QSFP+SR	40 GE QSFP+ transceivers, short range for all systems with QSFP+ slots.
40 GE QSFP+ Transceivers, Short Range, BiDi	FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceivers, short range BiDi for systems with QSFP+ slots.
40 GE QSFP+ Transceivers, Long Range	FG-TRAN-QSFP+LR	40 GE QSFP+ transceivers, long range for all systems with QSFP+ slots.
Rack mount sliding rails	SP-FG3040B-RAIL	Rack mount sliding rails for FG-1000C/-DC, FG-1100/1101E, FG-1200D, FG-1500D/-DC, FG-1800F, FG-2000E, FG-2500E, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC and FG-3950B/-DC.
AC power supply	SP-FG1800F-PS	AC power supply for FG-1800/1801F

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

FORTINET®

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.