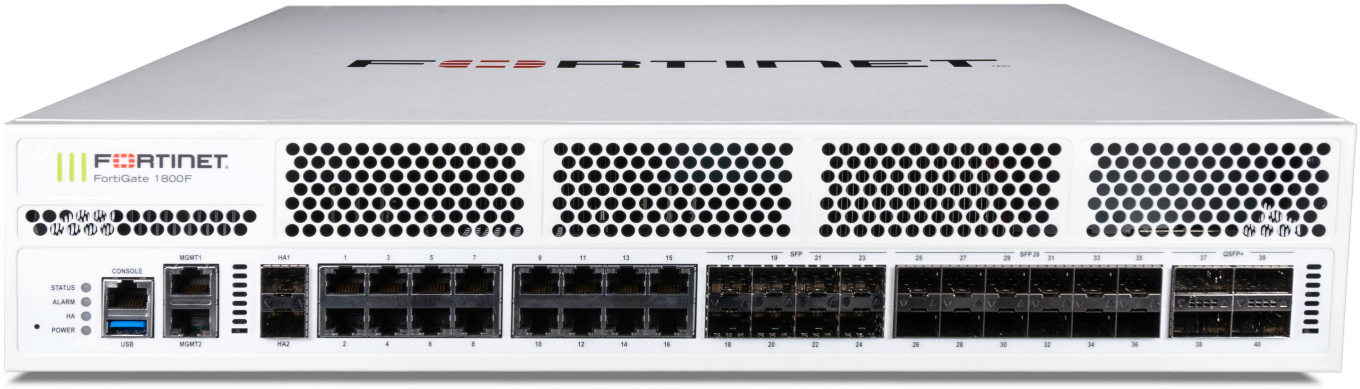
FortiGate 1800F Series

FG-1800F/-DC and 1801F/-DC



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

Security-Driven Networking FortiOS delivers converged networking and security.

Unparalleled Performance with Fortinet's patented / SPU / vSPU processors.

Enterprise Security with consolidated AI / ML-powered FortiGuard Services.

Hyperscale Security to secure any edge at any scale.

High Performance with Flexibility

The FortiGate 1800F Series enables organizations to build security-driven networks that can weave security deep into their datacenter and across their hybrid IT architecture to protect any edge at any scale.

Powered by a rich set of AI/ML-based FortiGuard Services and an integrated security fabric platform, the FortiGate 1800F Series delivers coordinated, automated, end-to-end threat protection across all use cases.

The industry's first integrated Zero Trust Network Access (ZTNA) enforcement within an NGFW solution, FortiGate 1800F automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

IPS	NGFW	Threat Protection	Interfaces
22 Gbps	17 Gbps	15 Gbps	Multiple GE RJ45, 25 GE SFP28 / 10 GE SFP+ / GE SFP and 100GE / 40 GE QSFP+ slots

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

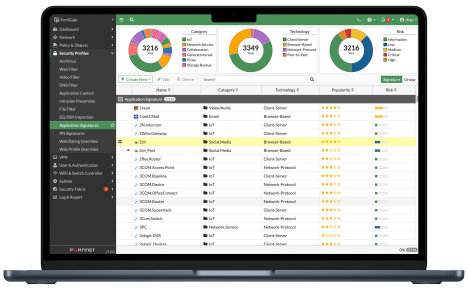
FortiOS powers all FortiGate deployments whether a physical or virtual device, as a container, or as a cloud service. This universal deployment model enables the consolidation of many technologies and use cases into a simplified, single policy and management framework. Its organically built best-of-breed capabilities, unified operating system, and ultra-scalability allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of security policies, and enables centralized management across large-scale networks with the following key attributes:

- Interactive drill-down and topology viewers that display real-time status
- On-click remediation that provides accurate and quick protection against threats and abuses
- Unique threat score system correlates weighted threats with users to prioritize investigations

Intuitive easy to use view into the network and endpoint vulnerabilities



Visibility with FOS Application Signatures

FortiConverter Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

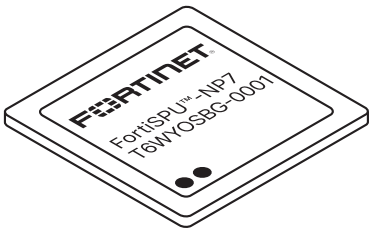
The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

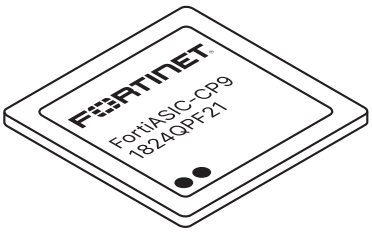
ASIC Advantage



Network Processor 7 NP7

Network Processors operate inline to deliver unmatched performance and scalability for critical network functions. Fortinet's breakthrough SPU NP7 network processor works in line with FortiOS functions to deliver:

- Hyperscale firewall, accelerated session setup, and ultra-low latency
- Industry-leading performance for VPN, VXLAN termination, hardware logging, and elephant flows



Content Processor 9 CP9

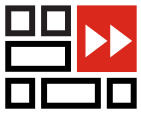
Content Processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload, and accelerated antivirus processing

FortiCare Services

Fortinet is dedicated to helping our customers succeed, and every year FortiCare Services help thousands of organizations get the most from our Fortinet Security Fabric solution. Our lifecycle portfolio offers Design, Deploy, Operate, Optimize, and Evolve services. Operate services offer device-level FortiCare Elite service with enhanced SLAs to meet our customer's operational and availability needs. In addition, our customized account-level services provide rapid incident resolution and offer proactive care to maximize the security and performance of Fortinet deployments.

Use Cases

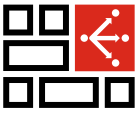


Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection

Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security—from the branch to the datacenter and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services detects and prevents known, zero-day, and unknown attacks



Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-any where models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

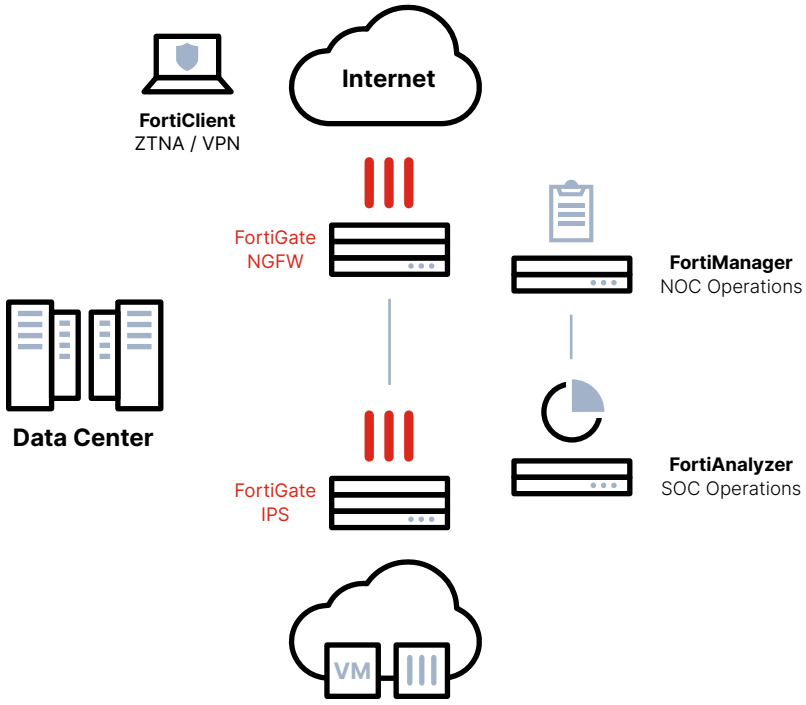
HyperScale

- Purpose-built SPUs power FortiOS to consolidate networking and security and deliver ultra-scalable Security-Driven Networks
- Unparalleled ultra-high performance offers the industry's highest number of connections and connections per second performance combined with security-enabled performance to safeguard business-critical applications
- Hardware assisted anti-DDoS prevents volumetric attacks and delivers strong security posture

Mobile Security for 4G, 5G, and IoT

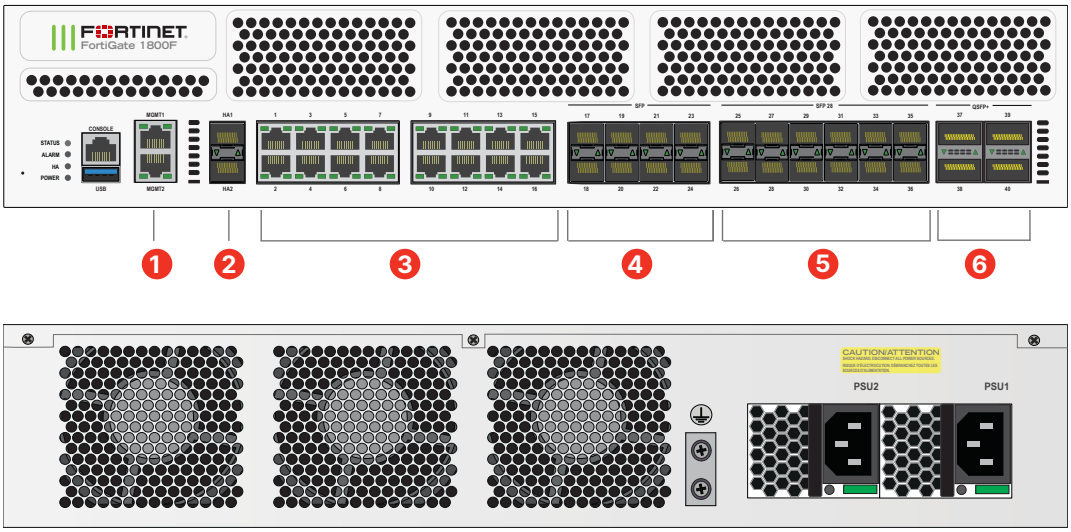
- SPU-accelerated, high performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/ DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- RAN Access Security with highly scalable and highest-performing IPsec aggregation and control Security Gateway (SecGW)
- User plane security enabled by full threat protection and visibility into GTP-U inspection

Datacenter Deployment (NGFW, IPS, Segmentation)



Hardware

FortiGate 1800F Series

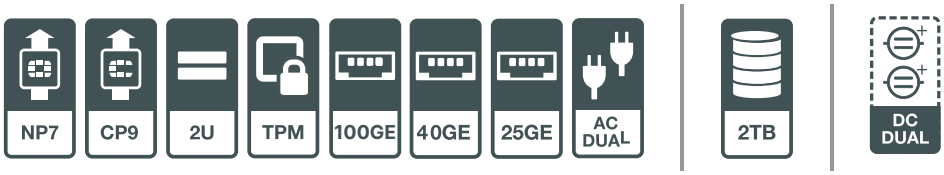


Interfaces

1. 2 x GE RJ45 MGMT Ports
2. 2 × 10 GE SFP+ / GE SFP HA Slots
3. 16 x GE RJ45 Ports
4. 8 x GE SFP Slots
5. 12 × 25 SFP28 / 10 GE SFP+ / GE SFP Slots
6. 4 × 100 GE QSFP28 / 40 GE QSFP+ Slots*

* FortiOS 7.4+ is required for 100 GE support

Hardware Features



Specifications

	FG-1800F/-DC	FG-1801F/-DC
Interfaces and Modules		
Hardware Accelerated GE RJ45 Ports	16	
Hardware Accelerated GE SFP Slots	8	
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ / GE SFP Slots	12	
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	4	
GE RJ45 Management Ports	2	
10 GE SFP+ / GE SFP HA Slots	2	
USB 3.0 Port	1	
Console RJ45 Port	1	
Onboard Storage	0	2× 1 TB NVMe SSD
Trusted Platform Module (TPM)	Yes	
Included Transceivers	2x SFP+ (SR 10 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	22 Gbps	
NGFW Throughput [2, 4]	17 Gbps	
Threat Protection Throughput [2, 5]	15 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)	3.22 µs	
Firewall Throughput (Packet per Second)	210 Mpps	
Concurrent Sessions (TCP)	12 Million / 40 Million*	
New Sessions/Second (TCP)	750 000 / 2 Million*	
Firewall Policies	100 000	
IPsec VPN Throughput (512 byte)[1]	55 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]	12 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS)[3]	9500	
SSL Inspection Concurrent Session (IPS, avg HTTPS)[3]	1.3 Million	
Application Control Throughput (HTTP 64K)[2]	34 Gbps	
CAPWAP Throughput (HTTP 64K)	65 Gbps	
Virtual Domains (Default / Maximum)	10 / 250	
Maximum Number of FortiSwitches Supported	196	
Maximum Number of FortiAPs (Total /Tunnel)	4096 / 2048	
Maximum Number of FortiTokens	20 000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-1800F/-DC	FG-1801F/-DC
Dimensions and Power		
Height x Width x Length (inches)	3.5 × 17.25 × 21.1	
Height x Width x Length (mm)	88.4 × 438 × 536	
Weight	30.2 lbs (13.7 kg)	30.4 lbs (13.8 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 2RU	
AC Power Supply	100–240VAC, 50/60 Hz	
AC Current (Maximum)	7A@100VAC, 3A@240VAC	
DC Power Supply	-48V to -60V DC	
DC Current (Maximum)	20A	
Power Consumption (Average / Maximum)	410.9 W / 459.1 W	414.9 W / 463.1 W
Heat Dissipation	1565.53 BTU/h	1579.2 BTU/h
Power Efficiency Rating	80Plus Compliant	
Redundant Power Supplies Hot Swappable	Yes (Default dual AC PSU for 1+1 Redundancy)	
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	
Forced Airflow	Side and Front to Back	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	USGv6/IPv6	

* Requires Hyperscale Firewall License

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.

Ordering Information

Product	SKU	Description
FortiGate 1800F	FG-1800F	4 × 100GE/40GE QSFP28 slots, 12 × 25GE SFP28 /10GE SFP+ slots, 2×10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports. SPU NP7 and CP9 accelerated, dual AC power supplies.
FortiGate 1801F	FG-1801F	4 × 100GE/40GE QSFP28 slots, 12 × 25GE SFP28 /10GE SFP+ slots, 2×10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports, 2×1TB on board SSD storage. SPU NP7 and CP9 accelerated, dual AC power supplies.
FortiGate 1800F-DC	FG-1800F-DC	4 × 100GE/40GE QSFP28 slots, 12 × 25GE SFP28 /10GE SFP+ slots, 2×10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports. SPU NP7 and CP9 accelerated, dual DC power supplies.
FortiGate 1801F-DC	FG-1801F-DC	4 × 100GE/40GE QSFP28 slots, 12 × 25GE SFP28 /10GE SFP+ slots, 2×10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports, 2×1TB on board SSD storage. SPU NP7 and CP9 accelerated, dual DC power supplies.
Hyperscale Firewall License FG1KF2KF	LIC-FGT-HYPSC-1K2K	Hyperscale Firewall License for FortiGate FG1800F/FG1801F/ FG2600F/ FG2601F Series for hardware acceleration.
Optional Accessories	**SKU**	**Description**
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-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	FN-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, 10 m/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.
10 GE Copper SFP+ RJ45 Transceiver (30 m Range)	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module.
10 Gbase-ER SFP+ Transceivers	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range.
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately)
10 GE SFP+ Transceiver Module, (connects to FN-TRAN-SFP+BD27, ordered separately)	FN-TRAN-SFP+BD33	10GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately)
25 GE SFP28 Transceiver Module, Long Range	FN-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	FN-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	FN-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	FN-TRAN-QSFP+LR	40 GE QSFP+ transceivers, long range for all systems with QSFP+ slots.
40 GE QSFP+ to 4× 10 GE SFP+ optical breakout, 1 m	FG-TRAN-QSFP-4XSFP	40 GE QSFP+ parallel breakout MPO to 4x LC connectors, 1 m reach, transceivers not included.
100 / 40 GE QSFP28 BIDI Transceiver Module	FN-TRAN-QSFP28-BIDI	100 GE / 40 GE QSFP28 BIDI transceiver module, short range, for systems with QSFP28 slots
100 GE QSFP28 Transceivers	FN-TRAN-QSFP28-SR	100GE QSFP28 transceiver module, 4 channel parallel fiber, short range for systems with QSFP28 Slots
100 GE QSFP28 Transceivers, Long Range	FN-TRAN-QSFP28-LR	100GE QSFP28 transceiver module, 4 channel parallel fiber, 10km long range for systems with QSFP28 Slots
100 GE QSFP28 Transceivers	FN-TRAN-QSFP28-CWDM4	100GE QSFP28 transceiver module, LC connectors, 2KM for systems with QSFP28 Slots
100 GE QSFP28 Transceiver Module, Short Range BiDi	FN-TRAN-QSFP28-BIDI-I	100 GE QSFP28 BIDI transceiver module, short range, for systems with QSFP28 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.
DC Power Supply	SP-FG1800F-DC-PS	DC power supply for FG-1800/1801F and FG-2600/2601.
25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-SFP28-1	25 GE SFP28 passive direct attach cable 1m for systems with SFP28 slots.
25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-SFP28-3	25 GE SFP28 passive direct attach cable 3m for systems with SFP28 slots.
25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-SFP28-5	25 GE SFP28 passive direct attach cable 5m for systems with SFP28 slots.
40 GE QSFP+ Passive Direct Attach Cable 1 m	SP-CABLE-FS-QSFP+1	40GE QSFP+ Passive Direct Attach Cable, 1 m for Systems with QSFP+ slots.
40 GE QSFP+ Passive Direct Attach Cable 3 m	SP-CABLE-FS-QSFP+3	40GE QSFP+ Passive Direct Attach Cable, 3 m for Systems with QSFP+ slots.
40 GE QSFP+ Passive Direct Attach Cable 5 m	SP-CABLE-FS-QSFP+5	40GE QSFP+ Passive Direct Attach Cable, 5 m for Systems with QSFP+ slots.
100 GE QSFP28 Breakout to 4× 25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-QSFP28-4SFP28-1	100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable, 1m
100 GE QSFP28 Breakout to 4× 25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-QSFP28-4SFP28-3	100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable, 3m
100 GE QSFP28 Breakout to 4× 25 GE SFP28 Passive Direct Attach Cable	FN-CABLE-QSFP28-4SFP28-5	100 GE QSFP28 breakout to 4× 25 GE SFP28 passive direct attach cable, 5m

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates	included with FortiCare Subscription			
	GeoIP DB Updates				
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Full features available when running FortiOS 7.4.1
2. Desktop Models only

FortiGuard Bundles

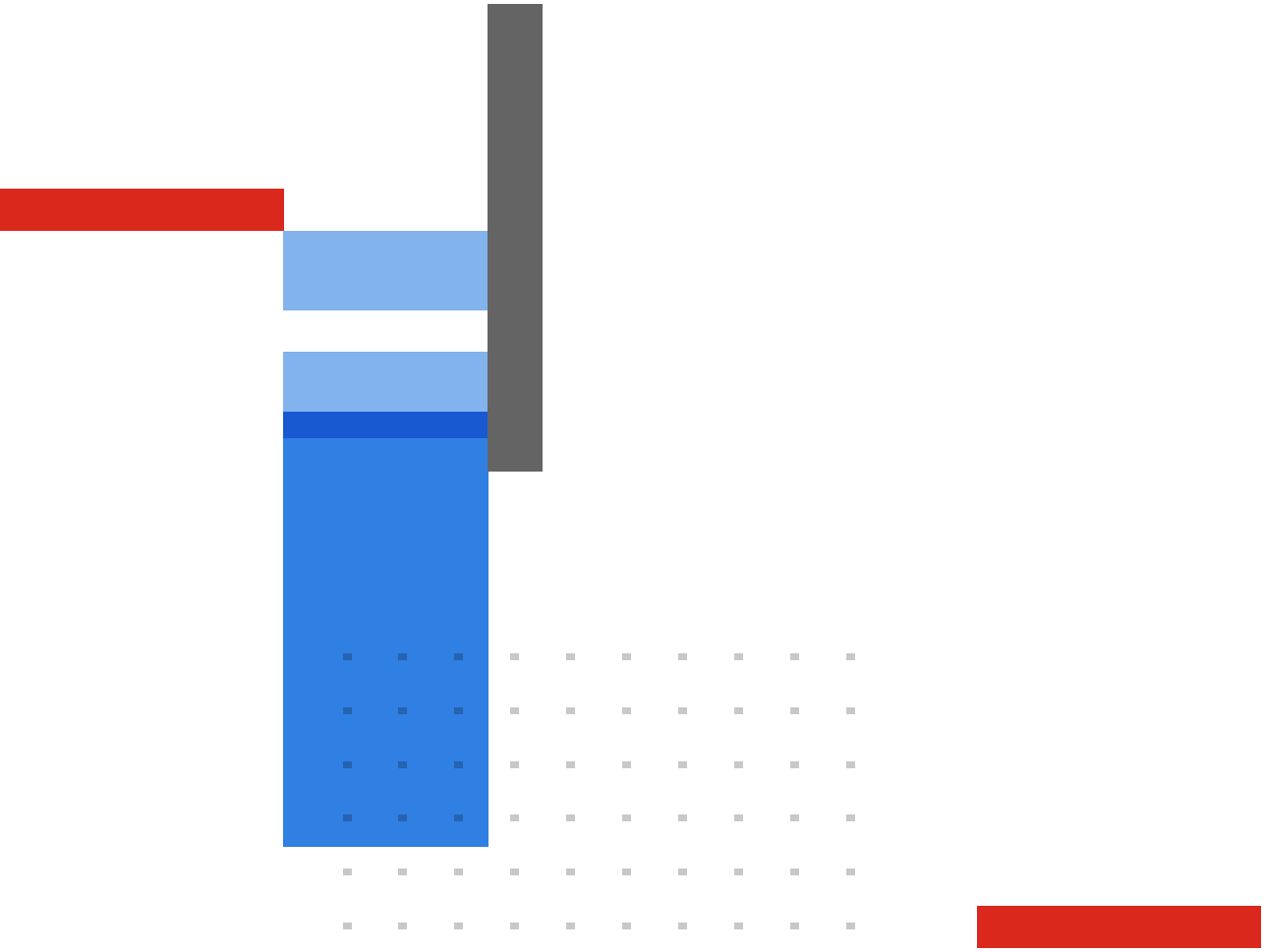
FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Elite

FortiCare Elite services offers enhanced service-level agreements (SLAs) and accelerated issue resolution. This advanced support offering provides access to a dedicated support team. Single-touch ticket handling by the expert technical team streamlines resolution. This option also provides Extended End-of-Engineering-Support (EoE's) of 18 months for added flexibility and access to the new FortiCare Elite Portal. This intuitive portal provides a single unified view of device and security health.

Fortinet CSR Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

October 12, 2023

FG-1800F-DAT-R35-20231012