

DATA SHEET

FortiGate® 800D

Next Generation Firewall Secure SD-WAN



The FortiGate 800D delivers next generation firewall capabilities for mid-sized to large enterprises, with the flexibility to be deployed at the campus or enterprise branch. Protect against cyber threats with security processor powered high performance, security efficacy and deep visibility.

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
- Prevent and detect against known and unknown attacks using continuous threat intelligence from Al powered FortiGuard Labs security services

Performance

- Delivers industry's best threat protection performance and ultra-low latency using purpose built-security processor (SPU) technology
- Provides industry-leading performance and protection for SSL encrypted traffic

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

- Best of Breed SD-WAN capabilities to enable application steering using WAN path control for high quality of experience
- Delivers advanced networking capabilities, high-performance, and scalable IPsec VPN capabilities to consolidate networking and security

Management

- Includes management console that's effective, simple to use, and provides comprehensive network automation & visibility.
- Provides Zero Touch Integration with Security Fabric's Single Pane of Glass Management
- Predefined compliance checklist analyzes the deployment and highlights best practices to improve 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
36 Gbps	4.2 Gbps	4 Gbps	3 Gbps	Multiple GE RJ45, GE SFP, 10 GE SFP+ slots and bypass GE RJ45 pairs

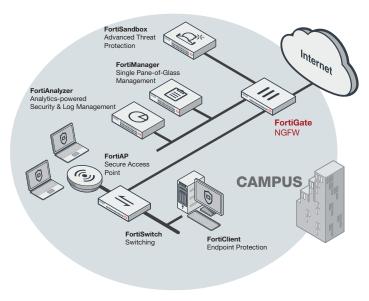
Deployment



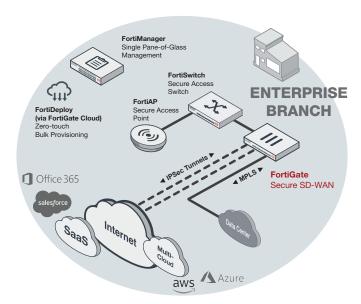
- Reduce complexity by combining threat protection security capabilities into single high-performance network security appliance
- Identify and stop threats with powerful intrusion prevention beyond port and protocol that examines the actual applications in your network traffic
- Delivers industry's highest SSL inspection performance using industry-mandated ciphers while maximizing ROI
- Proactively blocks newly discovered sophisticated attacks in real-time with advanced threat protection



- Secure direct Internet access for Cloud applications for improved latency and reduce WAN cost spending
- High-performance and cost-effective threat protection capabilities
- WAN Path Controller and Link Health Monitoring for better application performance
- Security Processor powered industry's best IPsec VPN and SSL Inspection performance
- Simplified Management and Zero-Touch deployment



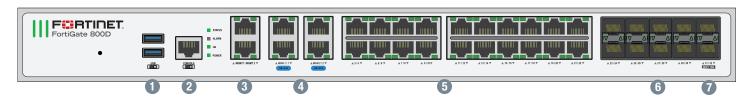
FortiGate 800D deployment in Campus (NGFW)



FortiGate 800D deployment in Enterprise Branch (Secure SD-WAN)

Hardware

FortiGate 800D





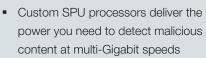


Interfaces

- 1. USB Ports
- 2. Console Port
- 3. 2x GE RJ45 Management Ports
- 4. 2x Bypass GE RJ45 Pairs

- 5. 20x GE RJ45 Ports
- 6. 8x GE SFP Slots
- 7. 2x 10 GE SFP+ Slots

Powered by SPU





- 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 new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

- Superior firewall performance for IPv4/IPv6, SCTP and multicast traffic with ultra-low latency down to 2 microseconds
- VPN, CAPWAP and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload and packet defragmentation
- Traffic shaping and priority queuing

Content Processor

The SPU CP8 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

10 GE Connectivity

High speed connectivity is essential for network security segmentation. The FortiGate 800D provides 10 GE slots that simplify network designs without relying on additional devices to bridge desired connectivity.



Fortinet Security Fabric

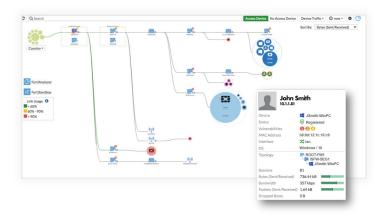
Security Fabric

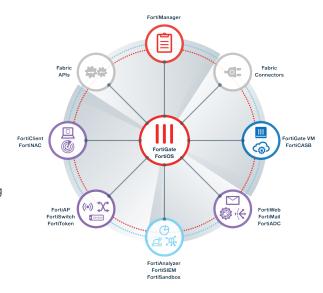
The Security Fabric delivers broad visibility, integrated Al-driven breach prevention, and automated operations, orchestration, and response across all Fortinet and its ecosystem deployments. It allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly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

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

FortiOS

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





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

Services



FortiGuard[™] Security Services

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



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

Interfaces and Modules		FORTIGATE 800D			
Hardware Accelerated GE SFP Slots 8 Hardware Accelerated GE RJ45 Ports 20 Accelerated GE RJ45 Bypass Interfaces 4 GE RJ45 Management / HA Ports 2 USB Ports (Client / Server) 1 / 2 Console Port 1 Onboard Storage 1x 240 GB SSD Included Transceivers 2x SFP (SX 1 GE) System Performance — Enterprise Traffic Mix IPS Throughput 2 4.2 Cbps NGFW Throughput 2 4.2 Cbps NGFW Throughput 2 4.2 Cbps NGFW Throughput 2 4.2 Cbps System Performance and Capacity IPv4 Firewall Throughput 36 / 36 / 22 Gbps Threat Protection Throughput 36 / 36 / 22 Gbps Included Transceivers 3 Gbps System Performance and Capacity IPv4 Firewall Throughput 36 / 36 / 22 Gbps IPv4 Firewall Throughput 36 / 36 / 22 Gbps Included Transceivers 3 Gbps System Performance and Capacity IPv4 Firewall Throughput 36 / 36 / 22 Gbps Include Transceivers 3 Gbps System Performance and Capacity IPv4 Firewall Throughput 36 / 36 / 22 Gbps Include Transceivers 36 / 36 / 22 Gbps Include Transceivers 3 Gbps Include T	Interfaces and Modules				
Hardware Accelerated GE RJ45 Bypass Interfaces	Hardware Accelerated 10 GE SFP+ Slots	2			
Accelerated GE RJ45 Bypass Interfaces 4 GE RJ45 Management / HA Ports 2 USB Ports (Client / Server) 1 / 2 Console Port 1 Onboard Storage 1x 240 GB SSD Included Transceivers 2x SFP (SX 1 GE) System Performance — Enterprise Traffic Mix IPS Throughput 2 4.2 Gbps NGFW Throughput 2-4 4 Gbps Threat Protection Throughput 2-5 3 Gbps System Performance and Capacity IPV4 Firewall Throughput 4 36 / 36 / 22 Gbps (1518 / 512 / 64 byte, UDP) IPV6 Firewall Throughput (B4 byte, UDP) IPrewall Throughput (Packet per Second) 33 Mpps Concurrent Sessions (TCP) 280,000 Firewall Photicies 10,000 IPsec VPN Throughput (512 byte) 200 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 5,000 SSL-INSpection Throughput (IPS, avg. HTTPS) 3 3,9 Gbps SSL Inspection Concurrent Session (RPS, avg. HTTPS) 3 3,9 Gbps SSL Inspection Concurrent Session (RPS, avg. HTTPS) 3 3,9 Gbps SSL Inspection Concurrent Session (RPS, avg. HTTPS) 3 3,9 Gbps SSL Inspection Concurrent Session (RPS, avg. HTTPS) 3 3,9 Gbps SSL Inspection Concurrent Session (RPS, avg. HTTPS) 4 9 Gbps CAPWAP Throughput (IPS, avg. HTTPS) 5 5,000 (RPS, avg. HTTPS) 5 5,000 Maximum Number of FortiNeines 5,000 Maximum Number of FortiOkens 5,000 Maximum Number of FortiOkens 5,000 Maximum Number of FortiOkens 5,000	Hardware Accelerated GE SFP Slots	8			
Commonstrate	Hardware Accelerated GE RJ45 Ports	20			
USB Ports (Client / Server)	Accelerated GE RJ45 Bypass Interfaces	4			
Console Port 1 Onboard Storage 1x 240 GB SSD Included Transceivers 2x SFP (SX 1 GE) System Performance — Enterprise Traffic Mix IPS Throughput ² 4.2 Gbps NGFW Throughput ².⁴ 4 Gbps Threat Protection Throughput ².⁵ 3 Gbps System Performance and Capacity IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 36 / 36 / 22 Gbps IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) 3 µS Firewall Throughput (Packet per Second) 33 Mpps Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) ¹ 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 3.9 Gbps SSL Inspection Throughput (IPS, avg. HTTPS) ³ 3.9 Gbps SSL Inspection Concurrent Session 380,000 (IPS, avg. HT	GE RJ45 Management / HA Ports	2			
Onboard Storage 1x 240 GB SSD Included Transceivers 2x SFP (SX 1 GE) System Performance — Enterprise Traffic Mix IPS Throughput 2 4.2 Gbps NGFW Throughput 2.4 4 Gbps Threat Protection Throughput 2.5 3 Gbps System Performance and Capacity Pv4 Firewall Throughput 36 / 36 / 22 Gbps IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 36 / 36 / 22 Gbps IPv6 Firewall Throughput (Packet per Second) 3 µS Firewall Latency (64 byte, UDP) 3 µS Firewall Throughput (Packet per Second) 3 Mpps Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) 1 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 380	USB Ports (Client / Server)	1/2			
Included Transceivers 2x SPP (SX 1 GE)	Console Port	1			
System Performance — Enterprise Traffic Mix IPS Throughput 2 4.2 Gbps NGFW Throughput 2.4 4 Gbps Threat Protection Throughput 2.5 3 Gbps System Performance and Capacity IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 36 / 36 / 22 Gbps (1518 / 512 / 64 byte, UDP) 3 μs Firewall Throughput (Packet per Second) 33 Mpps Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) 1 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-Inspection Throughput (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 2,5 Gbps	Onboard Storage	1x 240 GB SSD			
PS Throughput 2	Included Transceivers	2x SFP (SX 1 GE)			
NGFW Throughput 2.4 4 Gbps Threat Protection Throughput 2.5 3 Gbps System Performance and Capacity 36 / 36 / 22 Gbps IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 36 / 36 / 22 Gbps IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) 3 μs Firewall Latency (64 byte, UDP) 3 μs Firewall Throughput (Packet per Second) 33 Mpps Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) 1 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) 5,000 SSL Inspection Corps (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) 3 2,900 Application Control Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444	System Performance — Enterprise Traffic Mix				
Threat Protection Throughput 2.5 3 Gbps System Performance and Capacity IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 36 / 36 / 22 Gbps IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) 3 μs Firewall Latency (64 byte, UDP) 3 μs Firewall Throughput (Packet per Second) 33 Mpps Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 Psec VPN Throughput (512 byte) 1 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 5,000 SSL Inspection CPS (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 360,000	IPS Throughput ²	4.2 Gbps			
System Performance and Capacity 36 / 36 / 22 Gbps IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) 36 / 36 / 22 Gbps IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) 3 µs Firewall Latency (64 byte, UDP) 3 µs Firewall Throughput (Packet per Second) 33 Mpps Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 Psec VPN Throughput (512 byte) 1 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 5,000 SSL Inspection CPS (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 360,000 (IPS, avg. HTTPS) 3 2,400 <	NGFW Throughput 2,4	4 Gbps			
Pv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) Pv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) Firewall Throughput (1518 / 512 / 86 byte, UDP) Firewall Latency (64 byte, UDP) S μs Firewall Throughput (Packet per Second) S μs S μ	Threat Protection Throughput 2,5	3 Gbps			
(1518 / 512 / 64 byte, UDP) IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP) 36 / 36 / 22 Gbps Firewall Latency (64 byte, UDP) 3 μs Firewall Throughput (Packet per Second) 33 Mpps Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) ¹ 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 55,000 SSL Inspection Throughput (IPS, avg. HTTPS) ³ 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) ³ 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) ³ 2,400 SSL Inspection Control Throughput (HTTP 64K) ² 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients<	System Performance and Capacity				
(1518 / 512 / 86 byte, UDP) 3 µs Firewall Latency (64 byte, UDP) 3 µs Firewall Throughput (Packet per Second) 33 Mpps Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) ¹ 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 5,000 SSL Inspection Throughput (IPS, avg. HTTPS) ³ 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) ³ 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) ³ 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) ³ 2,5 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000		36 / 36 / 22 Gbps			
Firewall Throughput (Packet per Second) 33 Mpps Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) 1 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 5SL Inspection Throughput (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) 3 2,60ps Application Control Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000		36 / 36 / 22 Gbps			
Concurrent Sessions (TCP) 5 Million New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) ¹ 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 5SL Inspection Throughput (IPS, avg. HTTPS) ³ 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) ³ 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) ³ 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) ³ 2,5 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	Firewall Latency (64 byte, UDP)	3 µs			
New Sessions/Second (TCP) 280,000 Firewall Policies 10,000 IPsec VPN Throughput (512 byte) ¹ 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 5 SSL Inspection Throughput (IPS, avg. HTTPS) ³ 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) ³ 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³ 380,000 (IPS, avg. HTTPS) ³ 9 Gbps CAPWAP Throughput (HTTP 64K) ² 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	Firewall Throughput (Packet per Second)	33 Mpps			
Firewall Policies 10,000 IPsec VPN Throughput (512 byte) ¹ 20 Gbps Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 5,000 SSL Inspection Throughput (IPS, avg. HTTPS) ³ 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) ³ 2,400 SSL Inspection Concurrent Session 380,000 (IPS, avg. HTTPS) ³ 9 Gbps CAPWAP Throughput (HTTP 64K) ² 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	Concurrent Sessions (TCP)	5 Million			
Psec VPN Throughput (512 byte) 20 Gbps Gateway-to-Gateway Psec VPN Tunnels 2,000 Client-to-Gateway Psec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) SSL Inspection Throughput (PS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (PS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session 380,000 (PS, avg. HTTPS) 3 3,9 Gbps SL Inspection Concurrent Session 380,000 SSL Inspection Concurrent Session 360,000 SSL Inspection Concurrent Session 380,000 SSL Inspection Charles 3	New Sessions/Second (TCP)	280,000			
Gateway-to-Gateway IPsec VPN Tunnels 2,000 Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 55.000 SSL Inspection Throughput (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 380,000 (IPS, avg. HTTPS) 3 400 Application Control Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	Firewall Policies	10,000			
Client-to-Gateway IPsec VPN Tunnels 50,000 SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users 5,000 (Recommended Maximum, Tunnel Mode) 5,000 SSL Inspection Throughput (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 380,000 (IPS, avg. HTTPS) 3 400 Application Control Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	IPsec VPN Throughput (512 byte) 1	20 Gbps			
SSL-VPN Throughput 2.2 Gbps Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) 5,000 SSL Inspection Throughput (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 380,000 (IPS, avg. HTTPS) 3 9 Gbps CAPWAP Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	Gateway-to-Gateway IPsec VPN Tunnels	2,000			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) 5,000 SSL Inspection Throughput (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 380,000 Application Control Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	Client-to-Gateway IPsec VPN Tunnels	50,000			
(Recommended Maximum, Tunnel Mode) SSL Inspection Throughput (IPS, avg. HTTPS) 3 3.9 Gbps SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 380,000 Application Control Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	SSL-VPN Throughput	2.2 Gbps			
SSL Inspection CPS (IPS, avg. HTTPS) 3 2,400 SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 380,000 Application Control Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000		5,000			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) 3 380,000 Application Control Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	SSL Inspection Throughput (IPS, avg. HTTPS) 3	3.9 Gbps			
(IPS, avg. HTTPS) 3 Application Control Throughput (HTTP 64K) 2 9 Gbps CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	SSL Inspection CPS (IPS, avg. HTTPS) 3	2,400			
CAPWAP Throughput (1444 byte, UDP) 5.5 Gbps Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	•	380,000			
Virtual Domains (Default / Maximum) 10 / 10 Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	Application Control Throughput (HTTP 64K) ²	9 Gbps			
Maximum Number of FortiSwitches Supported 64 Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	CAPWAP Throughput (1444 byte, UDP)	5.5 Gbps			
Maximum Number of FortiAPs (Total / Tunnel) 1024 / 512 Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiTokens 5,000 Maximum Number of Registered FortiClients 2,000	Maximum Number of FortiSwitches Supported	64			
Maximum Number of Registered FortiClients 2,000	Maximum Number of FortiAPs (Total / Tunnel)	1024 / 512			
<u>-</u>	Maximum Number of FortiTokens	5,000			
High Availability Configurations Active-Active, Active-Passive, Clustering	Maximum Number of Registered FortiClients	2,000			
	High Availability Configurations	Active-Active, Active-Passive, Clustering			

	FORTIGATE 800D			
Dimensions and Power				
Height x Width x Length (inches)	1.75 x 17.0 x 16.4			
Height x Width x Length (mm)	44.45 x 432 x 416			
Weight	10 N lbs /8 6 kg)			
Form Factor	1 RH			
Wall Mountable	No			
AC Power Supply	100-240V AC, 60-50 Hz			
Power Consumption (Average / Maximum)	128 W / 187 W			
Current (Maximum)	110V/7A, 220V/3.5A			
Heat Dissipation	636 BTU/h			
Redundant Power Supplies	(Hot Swappable) optional			
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	55 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.
- 5. Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.



Order Information

Product	SKU	Description
FortiGate 800D	FG-800D	22x GE RJ45 ports, $4x$ GE RJ45 with Bypass Protection, $8x$ GE SFP slots, $2x$ 10 GE SFP+ slots, SPU NP6 and CP8 hardware accelerated, 240 GB Internal onboard SSD storage.
Optional Accessories/Spares	SKU	Description
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.
AC Power Supply	SP-FG600C-PS	AC power supply for FG-600C, FG-800C, FG-800D and FG-1000C.

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.

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 © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiGate®, FortiGate®, 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 Fortinets General Councils, with a purches, what has present that expressly warrants that the identified performance for perform according to certain 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 Fortinets 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.

FST-PROD-DS-GT8H FG-800D-DAT-R17-201906