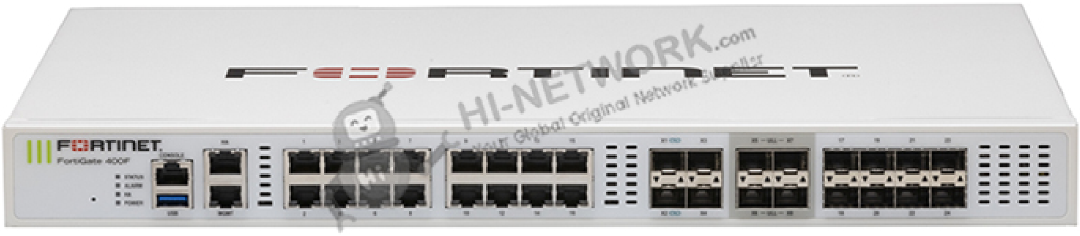
Overview

The FortiGate 400F Series NGFW combines AI-powered security and machine learning to deliver Threat Protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 400F Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks.

Universal ZTNA automatically controls, verifies, and facilitates user access to applications, reducing lateral threats by providing access only to validated users. Ultra-fast Threat Protection and SSL Inspection provides security at the edge you can see without impacting performance.



IPS	NGFW	Threat Protection	Interfaces
12 Gbps	10 Gbps	9 Gbps	Multiple GE RJ45, 10GE SFP+ Slots, GE SFP Slots

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 AI-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 for best-in-class security effectiveness and performance

Networking

- Delivers advanced networking capabilities that seamlessly integrate with advanced layer 7 security and virtual domains (VDOMs) to offer extensive deployment flexibility, multi-tenancy and effective utilization of resources
- Delivers high-density, flexible combination of various high-speed interfaces to enable best TCO for customers for data center and WAN deployments

Management

- Includes a management console that is effective, simple to use, and provides comprehensive network automation and visibility
- Provides Zero Touch Integration with Fortinet’s 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

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

FortiConverter Migration 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

FortiGuard AI-Powered Security

FortiGuard’s rich suite of security services counter threats in real time using AI-powered, coordinated protection designed by FortiGuard Labs security threat researchers, engineers, and forensic specialists.

Web Security

Advanced cloud-delivered URL, DNS (Domain Name System), and Video Filtering providing complete protection for phishing and other web born attacks while meeting compliance. Additionally, its dynamic inline CASB (Cloud Access Security Broker) service is focused on securing business SaaS data, while inline ZTNA traffic inspection and ZTNA posture check provide per-sessions access control to applications. It also integrates with the FortiClient Fabric Agent to extend protection to remote and mobile users.

Content Security

Advanced content security technologies enable the detection and prevention of known and unknown threats and file-based attack tactics in real-time. With capabilities like CPRL (Compact Pattern Recognition Language), AV, inline Sandbox, and lateral movement protection make it a complete solution to address ransomware, malware, and credential-based attacks.

Device Security

Advanced security technologies are optimized to monitor and protect IT, IIoT, and OT (Operational Technology) devices against vulnerability and device-based attack tactics. Its validated near-real-time IPS intelligence detects, and blocks known and zero-day threats, provides deep visibility and control into ICS/OT/SCADA protocols, and provides automated discovery, segmentation, and pattern identification-based policies.

Advanced Tools for SOC/NOC

Advanced NAC and SOC management tools attached to your NGFW provide simplified and faster time-to-activation.

SOC-as-a-Service

Includes tier-one hunting and automation, log location, 24x7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

Fabric Rating Security Best Practices

Includes supply chain virtual patching, up-to-date risk and vulnerability data to deliver quicker business decisions, and remediation for data breach situations.

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

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-anywhere models, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

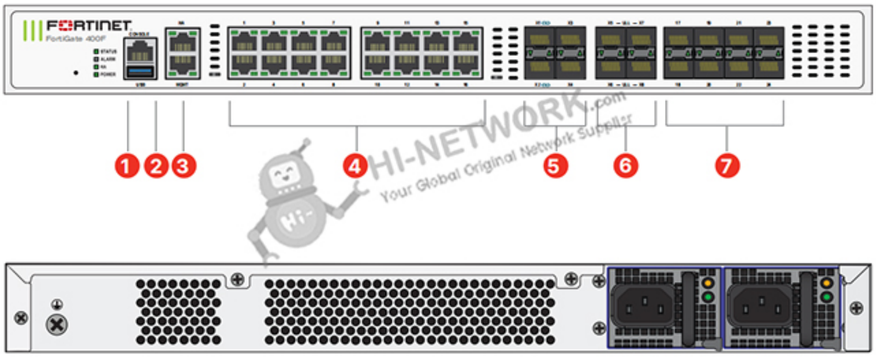
Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access—every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

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

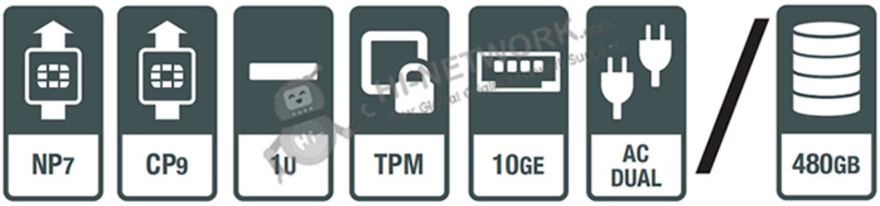
Hardware



Interfaces

(1)	1x USB Ports	(5)	4 x 1GE/10GE SFP+ Slots
(2)	1x Console Port	(6)	4 x 10GE SFP+ Ultra Low Latency Slots
(3)	2 x GE RJ45 MGMT/HA Ports	(7)	8x 1GE SFP Slots
(4)	16x GE RJ45 Ports		

Hardware Features



Get More Information

Do you have any question about the FG-400F?

Contact us now via info@hi-network.com.

Specification

FortiGate 400F Specification	
Interfaces and Modules	
Hardware Accelerated GE RJ45 Interfaces	16
Hardware Accelerated GE SFP Slots	8
Hardware Accelerated 10GE SFP+ Slots	4
Hardware Accelerated 10GE SFP+ Ultra Low Latency Slots	4
GE RJ45 Management Ports	2
USB Ports	1
RJ45 Console Port	1
Onboard Storage	NIL
Trusted Platform Module (TPM)	Yes
Included Transceivers	2x SFP (SX 1 GE)
System Performance — Enterprise Traffic Mix	
IPS Throughput	12 Gbps
NGFW Throughput	10 Gbps
Threat Protection Throughput	9 Gbps
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	79.5 / 78.5 / 70 Gbps
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	79.5 / 78.5 / 70 Gbps
Firewall Latency (64 byte, UDP)	4.19 μs / 2.5 μs
Firewall Throughput (Packet per Second)	105 Mpps
Concurrent Sessions (TCP)	7.8 Million
New Sessions/Second (TCP)	500,000
Firewall Policies	10,000
IPsec VPN Throughput (512 byte)	55 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	2,000
Client-to-Gateway IPsec VPN Tunnels	50,000
SSL-VPN Throughput	3.6 Gbps
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	5,000
SSL Inspection Throughput (IPS, avg. HTTPS)	8 Gbps
SSL Inspection CPS (IPS, avg. HTTPS)	6,000

SSL Inspection Concurrent Session (IPS, avg. HTTPS)	800,000
Application Control Throughput (HTTP 64K)	28 Gbps
CAPWAP Throughput (HTTP 64K)	65 Gbps
Virtual Domains (Default / Maximum)	10 / 10
Maximum Number of FortiSwitches Supported	72
Maximum Number of FortiAPs (Total / Tunnel)	512 / 256
Maximum Number of FortiTokens	5,000
High Availability Configurations	Active-Active, Active-Passive, Clustering
Dimensions and Power	
Height x Width x Length (inches)	1.75 x 17.0 x 15.0
Height x Width x Length (mm)	44.45 x 432 x 380
Weight	14.11 lbs (6.4 kg)
Form Factor	Rack Mount, 1 RU
Power Consumption (Average / Maximum)	154.8 W / 189.2 W
Power Source	100–240V AC, 50/60Hz
Current (Maximum)	6A
Heat Dissipation	645.58 BTU/h
Power Supply 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	5–90% non-condensing
Noise Level	LPA 48 dBA / LWA 55 dBA
Operating Altitude	Up to 10 000 ft (3048 m)
Noise Level	LPA 48 dBA / LWA 55 dBA
Airflow	Side and Front to Back
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB
Certifications	ICSA Labs: Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6/IPv6

Want to Buy

Get a Quote

Learn More about Hi-Network

Search our Resource Library

Follow us on LinkedIn

Contact for Sales or Support

Contact HI-NETWORK.COM For Global Fast Shipping

HongKong Office Tel: +00852-66181601

HangZhou Office Tel: +0086-571-86729517

Email: info@hi-network.com

Skype: echo.hinetwork

WhatsApp Business: +8618057156223