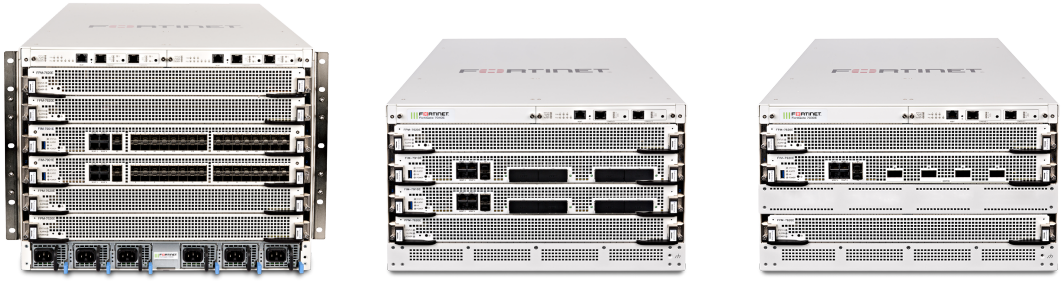
FortiGate 7000E Series

FG-7060E, FG-7040E, and FG-7030E



Highlights

Leader in the Gartner Magic Quadrant™ for Hybrid Mesh Firewall.

Secure 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 7000E Series enables organizations to build security-driven networks, forming the foundation of a robust Hybrid Mesh Firewall architecture. This approach weaves security deep into their datacenter and across their hybrid IT environment, protecting any edge at any scale.

Powered by a rich set of AI/ML-based FortiGuard Services and an integrated security fabric platform, the FortiGate 7000E 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 7000E automatically controls, verifies, and facilitates user access to applications, delivering consistent convergence with a seamless user experience across your distributed network.

The industry's first integrated Zero Trust Network Access (ZTNA) enforcement within an NGFW solution, FortiGate 7000E Series automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

Model	IPS	NGFW	Threat Protection	Interfaces
7060E-8/-9	120/200 Gbps	100/120 Gbps	80/96 Gbps	Multiple 10 GE SFP+/SFP, 40 GE QSFP+, 100 GE CFP2/QSFP28
7040E-8/-9	60/100 Gbps	50/60 Gbps	40/48 Gbps	Multiple 10 GE SFP+/SFP, 40 GE/ 100 GE QSFP28
7030-E	60 Gbps	50 Gbps	35 GBps	Multiple 10 GE SFP+/SFP, 40 GE/100 GE QSFP28

Use Cases



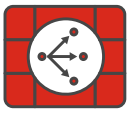
Next Generation Firewall (NGFW)

- 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



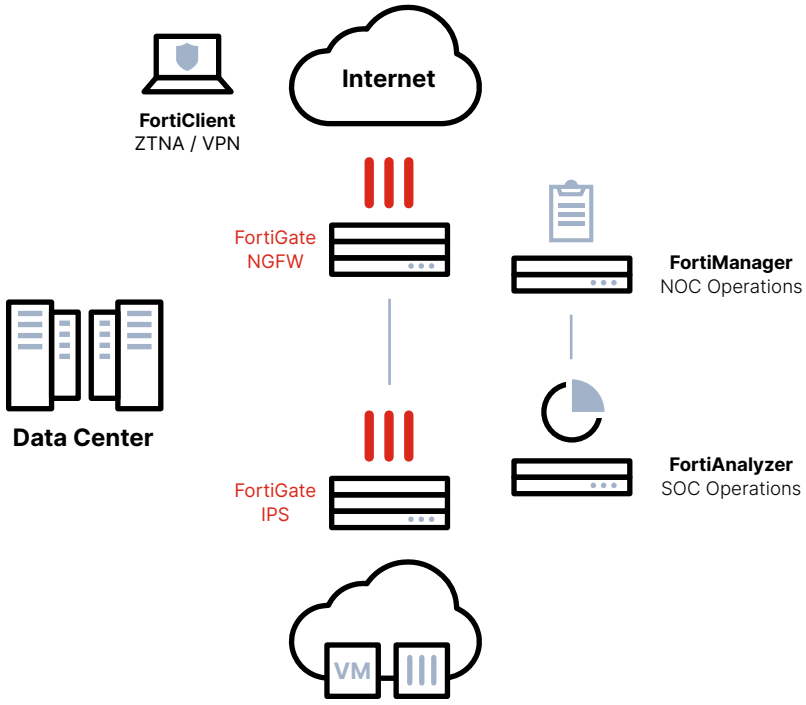
Secure SD-WAN

- 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

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)



Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Real-Time Quantum-Safe Network Security Operating System

FortiOS is Fortinet's natively AI-powered and quantum-safe operating system (OS) that powers the Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. It provides a unified framework for securing networks across on-premises, cloud, hybrid environments, and the convergence of IT, OT, and IoT.

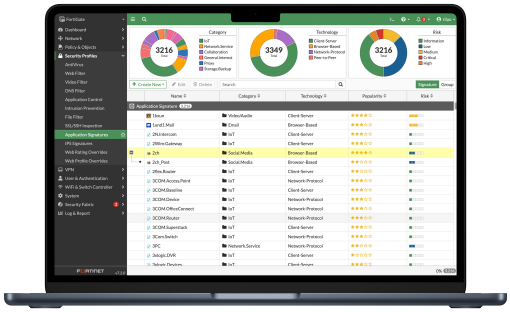
By converging networking and security functions into a single operating system, organizations can manage network and security more effectively to detect, investigate, and respond to incidents faster. This unified architecture simplifies operations, eliminates security silos, and allows organizations to scale securely without multiple tools or management complexity.

FortiOS also incorporates AI-driven capabilities that enhance threat detection, automate network activity analysis, and deliver more precise remediation guidance. Together, FortiGate firewalls and FortiOS provide intelligent, adaptive protection that reduces complexity, improves operational efficiency, and strengthens security across modern hybrid environments.

Learn more about what's new in FortiOS:
https://www.fortinet.com/products/fortigate/fortios



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 AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Powered by real-time AI enhanced threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero days and evasive, sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. Consists of intrusion prevention system (IPS) which uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, uncovers hidden command-and-control activity, and applies virtual patches for newly discovered vulnerabilities. Application control improves security compliance and provides real-time visibility into applications and usage including generative AI (GenAI) applications.

Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of millions of URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This service includes data loss/leakage prevention in files, GenAI applications and Images via OCR (optical character recognition). This ensures visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. The inline CASB service, secures SaaS applications in use, providing broad visibility and granular control over SaaS access, usage, and data.

Zero-day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown and zero-day malware in real time, delivering sub-second protection across all NGFWs. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

Attack surface visibility and compliance

The FortiGuard Attack Surface Security Service provides continuous, compliance-ready monitoring of your Fortinet Security Fabric infrastructure. It calculates your overall security posture rating by scoring controls against vulnerabilities, misconfigurations, and sub-optimal settings, while offering specific remediation guidelines for devices found out of configuration. It maintains continuous compliance with PCI DSS, CIS Controls, and Fortinet security best practices.

OT security

With over 2400 virtual patches, 1600+ OT applications, and 3500+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for 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.

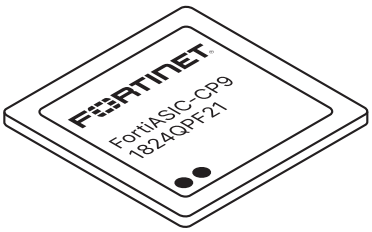
ASIC Advantage



Network Processor 6 NP6

Fortinet's new breakthrough SPU NP6 network processor works in line with FortiOS functions delivering:

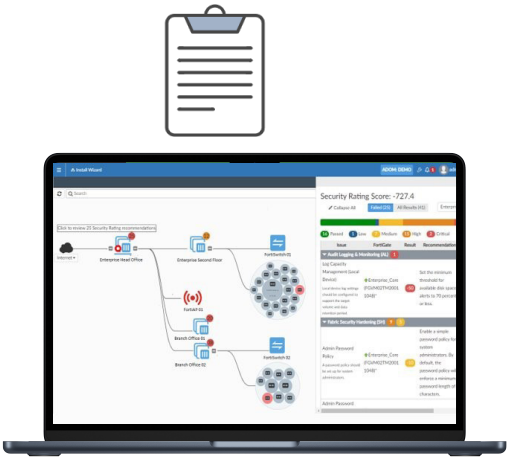
- Superior firewall performance for IPv4/IPv6, SCTP, and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing



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



Intuitive view and clear insights into network security posture with FortiManager

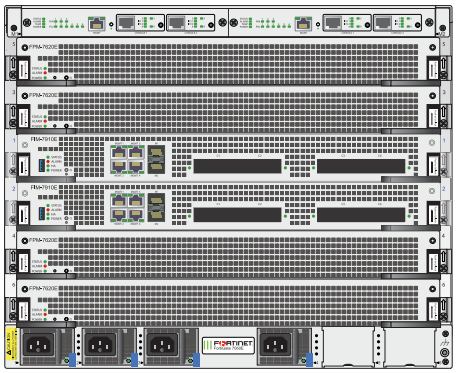
AI-powered, automation-driven, enterprise-class centralized management at scale

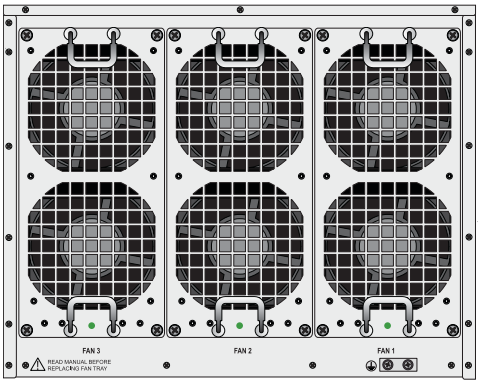
FortiManager, powered by FortiAI-Assist, provides centralized, single-pane management for the Fortinet Security Fabric, unifying configuration, policy, and responses across thousands of devices. It converges networking and security management, enabling consistent policy enforcement across SD-WAN, ZTNA, SASE, and branch environments while delivering real-time visibility and automated network operations.

FortiAI-Assist helps with Day 0–1 provisioning and Day N troubleshooting and maintenance. AI agents collaborating via a unified Model Context Protocol (MCP) framework automates goal-driven tasks toward a self-healing operation.

FortiManager integrates with FortiSOC for contextual insights and fabric-wise response. It also supports ecosystem integrations, and open APIs for extended automation. ADOM-based administration and FortiManager clusters enables resilient control across distributed networks.

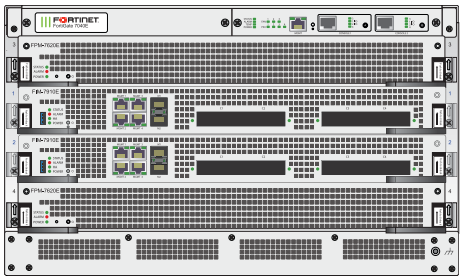
Hardware

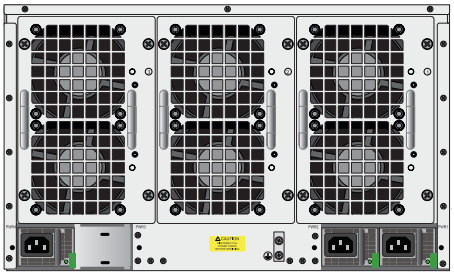




FortiGate 7060E

Next Generation eight-unit, 19-inch, six-slot rack mount chassis supporting up to four Fortinet Processor Modules (FPM) and two Fortinet Interface Modules (FIM).





FortiGate 7040E and 7030E

The FG-7040E is a Next Generation six-unit, 19-inch, four-slot rack mount chassis with two Fortinet Processor Modules (FPM) and two Fortinet Interface Modules (FIM). The FG-7030E three-slot rack mount chassis comes with two FPM and one bundled FIM.

FORTIGATE	7060E-8 / 7060E-9-(DC)*	7040E-8 / 7040E-9-(DC)	7030E
Hardware Specifications			
Fortinet Processor Module (FPM) Slots	4	2	2
Fortinet Interface Module (FIM) Slots	2	2	1
Shelf Manager	2	1	1
System Performance and Capacity			
Firewall Throughput (1518 / 512 / 64 byte, UDP)	630 / 630 / 340 Gbps	315 / 310 / 200 Gbps	155 / 155 / 155 Gbps
Firewall Latency (64 byte, UDP)	7.00 µs	7.00 µs	7.00 µs
Firewall Throughput (Packet per Second)	510 Mpps	300 Mpps	220 Mpps
Concurrent Sessions (TCP)	320 Million	160 Million	160 Million
New Sessions/Sec (TCP)	1.8 Million	950 000	900 000
Firewall Policies	200 000	200 000	200 000
IPsec VPN Throughput (512 byte)	100 Gbps	100 Gbps	40 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	16 000	16 000	16 000
Client-to-Gateway IPsec VPN Tunnels	64 000	64 000	64 000
SSL-VPN Throughput	15 Gbps	15 Gbps	15 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	48 000	48 000	48 000
IPS Throughput (Enterprise Mix) [1]	120 / 200 Gbps	60 / 100 Gbps	60 Gbps
SSL Inspection Throughput [2]	79.9 / 120 Gbps	39.9 / 60 Gbps	39.9 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) [3]	47 000	32 500	32 500
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	24 Million	12 Million	12 Million
Application Control Throughput [3]	160 Gbps	80 Gbps	65 Gbps
NGFW Throughput [4]	100 / 120 Gbps	50 / 60 Gbps	50 Gbps
Threat Protection Throughput [5]	80 / 96 Gbps	40 / 48 Gbps	35 Gbps
CAPWAP Throughput	N/A	N/A	N/A
Virtual Domains (Default / Maximum)	10 / 500	10 / 500	10 / 500
Maximum Number of FortiSwitches Supported	256	256	256
Maximum Number of FortiAPs (Total / Tunnel Mode)	N/A	N/A	N/A
High Availability Configurations	Active-Active (FGSP), Active-Passive, Clustering	Active-Active (FGSP), Active-Passive, Clustering	Active-Active (FGSP), Active-Passive, Clustering

Specifications

FORTIGATE	7060E-8 / 7060E-9-(DC)*	7040E-8 / 7040E-9-(DC)	7030E
Dimensions			
Height x Width x Length (inches)	14.0 × 17.3 × 25.6	10.5 × 17.3 × 25.6	10.5 × 17.3 × 25.6
Height x Width x Length (mm)	355.6 × 440 × 651	266.7 × 440 × 650	266.7 × 440 × 650
Weight	210.2 lbs (95.4 kg)	153.3 lbs (69.6 kg)	134.9 lbs (61.3 kg)
Form Factor (supports EIA/non-EIA standards)	8 RU	6 RU	6 RU
Power and Environment			
Power Required	AC (configured with 4 PSUs in a 3+1 redundant configuration, an additional 2 PSUs can be added for additional redundancy)	AC (configured with 3 PSUs in a 2+1 redundant configuration, an additional PSU can be added for additional redundancy)	AC (configured with 3 PSUs in a 2+1 redundant configuration, an additional PSU can be added for additional redundancy)
Power Consumption (Maximum / Average) **	3277 / 2330 W	2500 / 1800 W	1940 / 1390 W
AC Current (Maximum)	12A@100V, 10A@240V	12A@100V, 10A@240V	12A@100V, 10A@240V
Heat Dissipation (Maximum) **	11 184 BTU/h	8530 BTU/h	6619 BTU/h
DC Power Supply	-48V DC	-48V DC	–
DC Current (Maximum)	30A per feed (3+3)	30A per feed (2+2)	–
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)
Humidity	20% to 90% non-condensing	20% to 90% non-condensing	20% to 90% non-condensing
Compliance			
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB

* Performance specifications for FG-7060 are based on 4 FPM combination.

** Based on all default included components.

Note: All performance values are "up to" and vary depending on system configuration. IPsec VPN performance is based on 512 byte UDP packets using AES-256+SHA1. 1. IPS performance is measured using 1 Mbyte HTTP and Enterprise Traffic Mix. 2. SSL Inspection is measured with IPS enabled and HTTP traffic, using TLS v1.2 with AES256-SHA. 3. Application Control performance is measured with 64 Kbytes HTTP traffic. 4. NGFW performance is measured with IPS and Application Control enabled, based on Enterprise Traffic Mix. 5. Threat Protection performance is measured with IPS and Application Control and Malware protection enabled, based on Enterprise Traffic Mix.

For complete, up-to-date and detailed feature set, please refer to the Administration Handbook and FortiOS Datasheet.

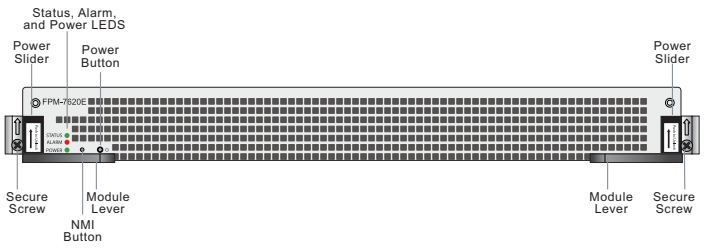
Modules

Fortinet Processor Module 7620E

NP6
CP9

The latest purpose-built SPU CP9 accelerated processor module with superior content processing throughput and protection. The device runs on FortiOS — the most powerful security operating system in the world.

Power and Environment	FG-7620E
Power Consumption (Average/Maximum)	320 / 410 W
Heat Dissipation (Average)	1395 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)
Storage Temperature	-31°F to 158°F (-35°C to 70°C)
Humidity	20% to 90% non-condensing
Compliance	
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB

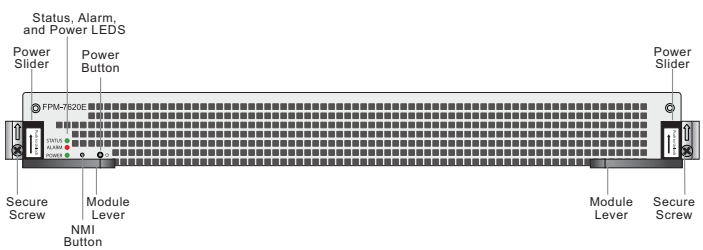


Fortinet Processor Module 7630E

NP6
CP9

The latest purpose-built SPU CP9 accelerated processor module with superior content processing throughput and protection. The device runs on FortiOS — the most powerful security operating system in the world.

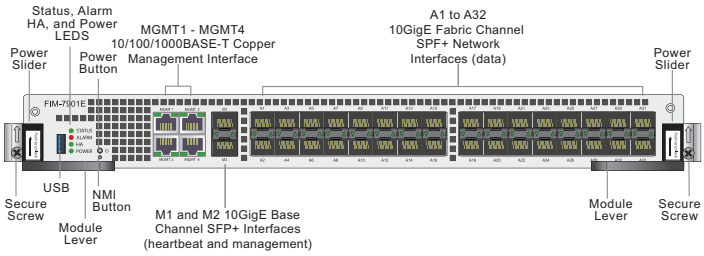
Power and Environment	FG-7630E
Power Consumption (Average/Maximum)	320 / 410 W
Heat Dissipation (Average)	1395 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)
Storage Temperature	-31°F to 158°F (-35°C to 70°C)
Humidity	20% to 90% non-condensing
Compliance	
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB



Modules

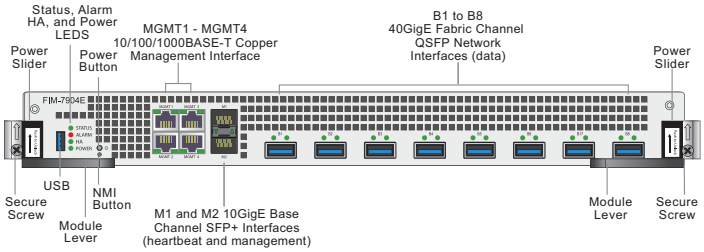
Fortinet Interface Module 7901E

High-performance, SPU DP2 accelerated networking blade with 32x GE/10 GE SFP/+ slots.



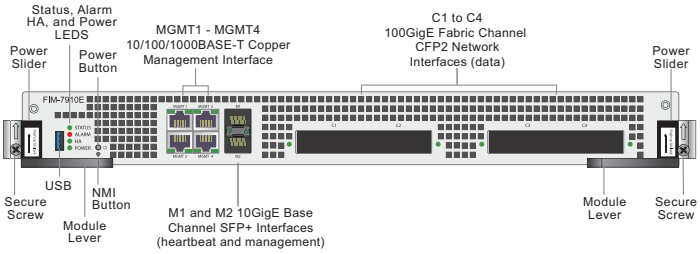
Fortinet Interface Module 7904E

High-performance, SPU DP2 accelerated networking blade with 8× 40 GE QSFP+ slots.



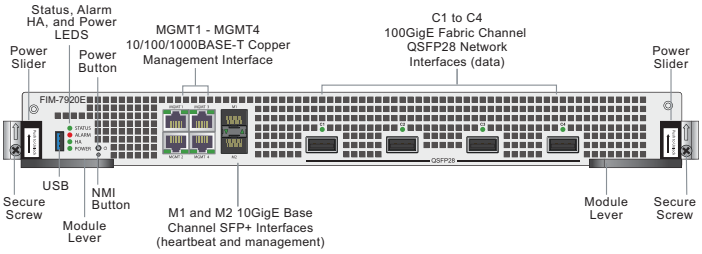
Fortinet Interface Module 7910E

High-performance, SPU DP2 accelerated networking blade with 4× 100 GE CFP2 slots.



Fortinet Interface Module 7920E

High-performance, SPU DP2 accelerated networking blade with 4× 100 GE QSFP28 slots.



	FIM-7901E	FIM-7904E	FIM-7910E	FIM-7920E
Interfaces				
Network Interfaces	32x GE/10 GE SFP/+	8× 40 GE QSFP+	4× 100 GE CFP2	4× 100 GE QSFP28
Base Channel Interfaces	2× 10 GE SFP+	2× 10 GE SFP+	2× 10 GE SFP+	2× 10 GE SFP+
Management Interfaces	4x GE RJ45	4x GE RJ45	4x GE RJ45	4x GE RJ45
Included Transceivers	2x SFP+ SR	2x SFP+ SR	2x SFP+ SR	2x SFP+ SR
Power and Environment				
Power Consumption (Average / Maximum)	260 / 450 W	260 / 450 W	260 / 450 W	410 / 460 W
Heat Dissipation	1531 BTU/h	1531 BTU/h	1531 BTU/h	1565 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)	-31°F to 158°F (-35°C to 70°C)
Humidity	20% to 90% non-condensing	20% to 90% non-condensing	20% to 90% non-condensing	20% to 90% non-condensing
Compliance				
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB

Bundle Matrix

SKU	Components					
Bundle	**Chassis**	**Processing Module**	**I/O Module 1**	**I/O Module 2**	**Power Supplies**	**Services and Licenses**
FG-7030E-SFP10G	FG-7030E (2x FPMs, 1x FIM)	2x FPM-7620E	Select from: FIM-7901E-C FIM-7904E-C FIM-7910E-C FIM-7920E-C	Select from: FIM-7901E-C FIM-7904E-C FIM-7910E-C FIM-7920E-C	3x PSU, 1x PSU Optional	Chassis-based pricing—Individual and bundled FortiGuard security services and FortiCare support subscription services: Threat Protection Bundle, UTM Bundle, Enterprise Bundle and FortiCare360 Chassis-based pricing—Add on licenses such as VDOM and Endpoint Compliance
FG-7030E-QSFP28	FG-7030E (2x FPMs, 1x FIM)	2x FPM-7620E	Select from: FIM-7901E-C FIM-7904E-C FIM-7910E-C FIM-7920E-C	Select from: FIM-7901E-C FIM-7904E-C FIM-7910E-C FIM-7920E-C	3x PSU, 1x PSU Optional	
FG-7040E-8	FG-7040E (2x FPMs, 2x FIMs)	2x FPM-7620E	Select from: FIM-7901E-C FIM-7904E-C FIM-7910E-C FIM-7920E-C	Select from: FIM-7901E-C FIM-7904E-C FIM-7910E-C FIM-7920E-C	3x PSU, 1x PSU Optional	
FG-7060E-8	FG-7060E (2x FPMs, 2x FIMs)	2x FPM-7630E 2x FPM-7630E Optional	Select from: FIM-7901E-C FIM-7904E-C FIM-7910E-C FIM-7920E-C	Select from: FIM-7901E-C FIM-7904E-C FIM-7910E-C FIM-7920E-C	4x PSU, 2x PSU Optional	

NOTE: FIM-79XXE-C are only meant to be used with the FG7040E-8/FG-7040E-8-DC/FG7060E-8/FG7060E-8-DC Bundles. Please use FIM-79XXE for ordering spares.

Ordering Information

Product	SKU	Description
FortiGate 7030E-SFP10G	FG-7030E-SFP10G	6U 3-slot chassis with 2x FPM-7620E processor modules, 1x FIM-7901E module with 32× 10 GE SFP+ slots, 1x manager module, and 3x hot swappable redundant PSU.
FortiGate 7030E-QSFP28	FG-7030E-QSFP28	6U 3-slot chassis with 2x FPM-7620E processor modules, 1x FIM-7920E module with 4× 100 GE QSFP28 slots, 1x manager module, and 3x hot swappable redundant PSU.
FortiGate 7040E-8	FG-7040E-8	6U 4-slot chassis with 2x FPM-7620E processor modules, 2x FIM-79xxE-C specified at purchase, 1x manager module and 3x hot swappable redundant PSU.
FortiGate 7040E-8-DC	FG-7040E-8-DC	6U 4-slot chassis with 2x FPM-7620E processor modules, 2x FIM-79xxE-C specified at purchase, 1x manager module and 3x hot swappable redundant DC PSU.
FortiGate 7040E-9	FG-7040E-9	6U 4-slot chassis with 2x FPM-7630E processor modules, 2x FIM-79xxE-C specified at purchase, 1x manager module and 3x hot swappable redundant PSU.
FortiGate 7040E-9-DC	FG-7040E-9-DC	6U 4-slot chassis with 2x FPM-7630E processor modules, 2x FIM-79xxE-C specified at purchase, 1x manager module and 3x hot swappable redundant DC PSU.
FortiGate 7060E-8	FG-7060E-8	8U 6-slot chassis with 2x FPM-7620E processor modules, 2x FIM-79xxE-C specified at purchase, 2x manager module and 4x hot swappable redundant PSU.
FortiGate 7060E-8-DC	FG-7060E-8-DC	8U 6-slot chassis with 2x FPM-7620E processor modules, 2x FIM-79xxE-C specified at purchase, 2x manager modules and 4x hot swappable redundant DC-DC PSU.
FortiGate 7060E-9	FG-7060E-9	8U 6-slot chassis with 2x FPM-7630E processor modules, 2x FIM-79xxE-C specified at purchase, 2x manager module and 4x hot swappable redundant PSU.
FortiGate 7060E-9-DC	FG-7060E-9-DC	8U 6-slot chassis with 2x FPM-7630E processor modules, 2x FIM-79xxE-C specified at purchase, 2x manager modules and 4x hot swappable redundant DC-DC PSU.
FortiGate 7060E-DC Chassis	FG-7060E-DC-Chassis	FG-7060E chassis including 2x system management modules, 3x fan modules and 4x DC PSU.
Training		
FortiGate Chassis-based Firewall Platform (FGT 7000) Training - two days	FT-FGT-CHS	Course description: https://training.fortinet.com/local/staticpage/view.php?page=library_fortigate-7000-series Upcoming sessions: https://training.fortinet.com/calendar/view.php/Course:FortiGate_7000_Series Price includes lab access and course material (Lab and Study guides). Exam voucher not included.

* Each FIM is packed individually and comes with 2× 10 GE SFP+ SR transceivers at no charge.

NOTE: All optional/spare components are for replacement usage and should not be used to assemble a bundle as only bundles have the necessary subscriptions.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

For hard-coded firmware ceilings for a specific software version, visit: Maximum Values Table Tool.

The link to the max value table: https://docs.fortinet.com/max-value-table?product_family=fortigate&family=fortigate

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles			
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection	SD-WAN
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•	
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct, AI-based Heurestic AV, FortiGate Cloud Sandbox[1]	•	•	•	•	
	URL, DNS and Video Filtering — URL, DNS and Video Filtering, Malicious Certificate[1]	•	•	•		
	Anti-Spam		•	•		
	AI-based Inline Malware Prevention	•	•			
	Data Loss Prevention (DLP)[2]	•	•			
	IoT Security — IoT Device Detection, IoT Vulnerability Correlation, and Virtual Patching[3]		•			•
	Security Rating (and Outbreak Check)[3]		•			•
	OT Security—OT Device Detection, OT Vulnerability Correlation and Virtual Patching, OT Application Control and IPS[2]	•				
	Application Control	----------included with FortiCare Subscription----------				
	Inline CASB[1]	----------included with FortiCare Subscription----------				
SD-WAN and SASE Services	SD-WAN SLA Database					•
	SD-WAN Underlay and Application Monitoring Service					•
	SD-WAN Overlay Orchestration Service					•
	SD-WAN Connector for FortiSASE Secure Private Access					•
	FortiSASE Starter Kit for n* Users[4]					•
	One Year Cloud-based Log Retention					•
	FortiTelemetry Cloud					•
NOC and SOC Services	FortiConverter Service for One Time Configuration Conversion	•	•			
	Managed FortiGate Service—Available 24×7, with Fortinet NOC Experts Performing Device Setup, Network, And Policy Change Management	•				
	FortiManagement Cloud—Management, Analysis, and One Year Log Retention	•				
	FortiManager Cloud	•				
	FortiAnalyzer Cloud	•				
	FortiGuard SOCaaS—24×7 Cloud-Based Managed Log Monitoring, Incident Triage, and SOC Escalation Service	•				
Hardware and Software Support	FortiCare Essentials	Desktop models only				
	FortiCare Premium[3]	•	•	•	•	•
	FortiCare Elite	•				
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing	----------included with FortiCare Subscription----------				

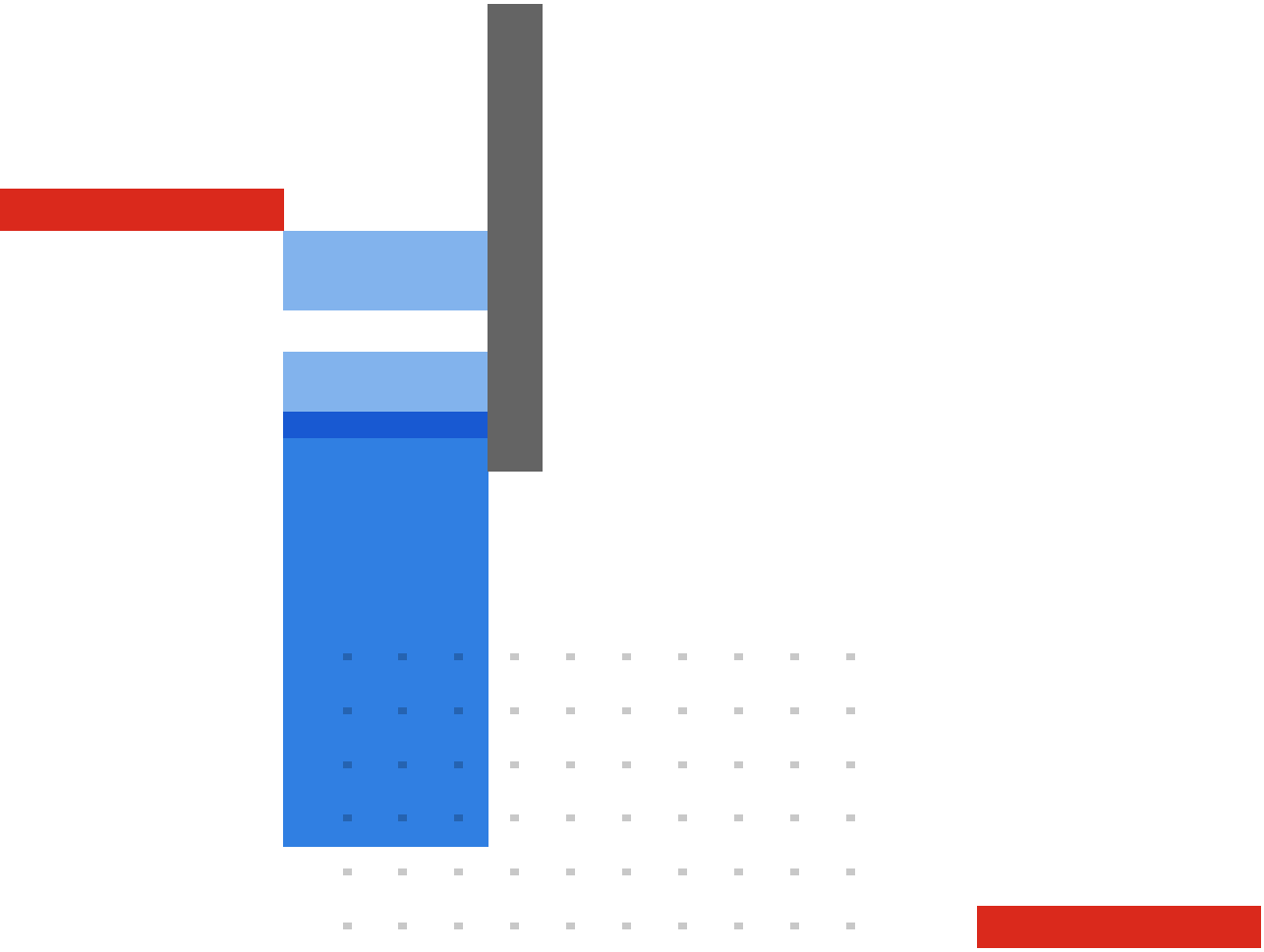
1. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards. Services including Content Disarm and Reconstruct, DNS and Video Filtering, and Inline CASB are not available for FortiGate/FortiWiFi 30G and 50G series in any OS build.
2. Full features available when running FortiOS 7.4.1.
3. Not available for SD-WAN Bundle SKU FC-10-XXXXX-1387-02-DD.
4. Only supported on FortiGate/FortiWiFi models from the 70F (F-series and all later series) and FGR-60G onwards. See the FortiSASE Ordering Guide for supported models and corresponding user license allocations.

FortiGuard AI-Powered Security Bundles offer curated security services to combat known, unknown, zero-day, and emerging AI threats. They protect against malicious content, web threats, and secure IT/OT/IoT devices, applications, users, and data. All bundles include FortiCare Premium Services with 24×7×365 support, one-hour critical response, and next-business-day noncritical response.

Fortinet's FortiCare Services support the Security Fabric throughout its lifecycle—Design, Deploy, Operate, Optimize, and Evolve. FortiCare Elite delivers enhanced SLAs, rapid issue resolution, dedicated support, 18 months of extended engineering support, and a unified portal for device and security health, improving operational efficiency and deployment performance.

Fortinet Corporate Social Responsibility 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

Copyright © 2026 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 SVP Legal and above, 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.

October 1, 2026

FG-7000E-DAT-R47-20261001