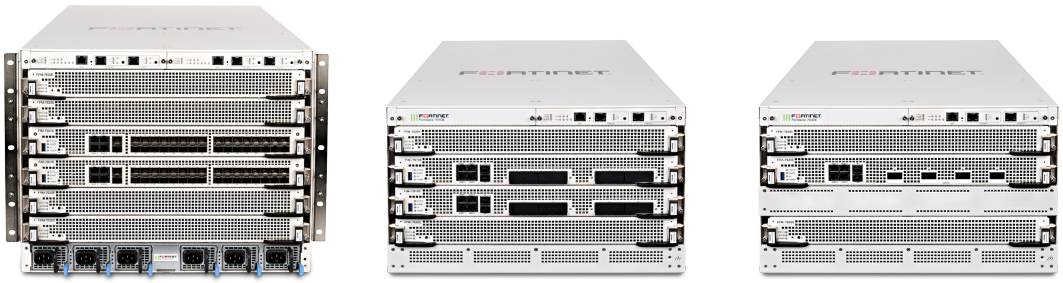
FortiGate 7000E Series

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



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and WAN Edge Infrastructure.

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 delivers high performance security-driven networks to large enterprises and service providers 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 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 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

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.

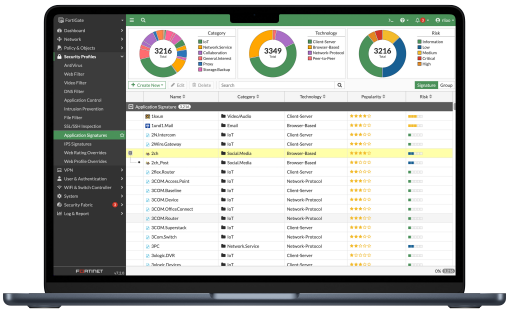
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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.

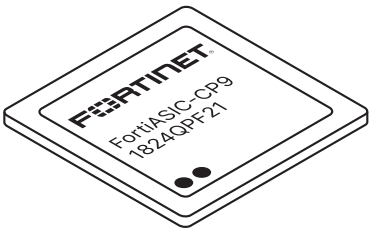
ASIC Advantage



Network Processor 6 NP6

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

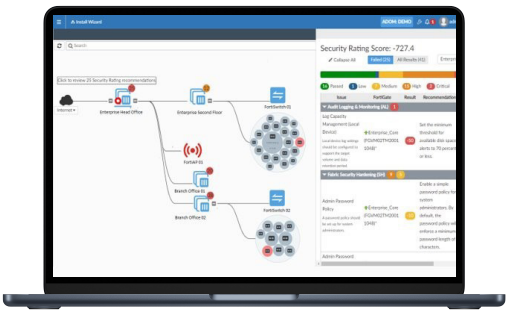
- Superior firewall performance for IPv4/IPv6, SCTP, and multicast traffic with ultra-low latency
- VPN, CAPWAP, and IP tunnel acceleration
- Anomaly-based intrusion prevention, checksum offload, and packet defragmentation
- Traffic shaping and priority queuing



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

Centralized Network and Security Management at Scale

FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving as the fundamental component for deploying Hybrid Mesh Firewalls.

Use Cases



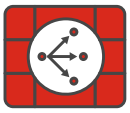
Next Generation Firewall (NGFW)

- 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



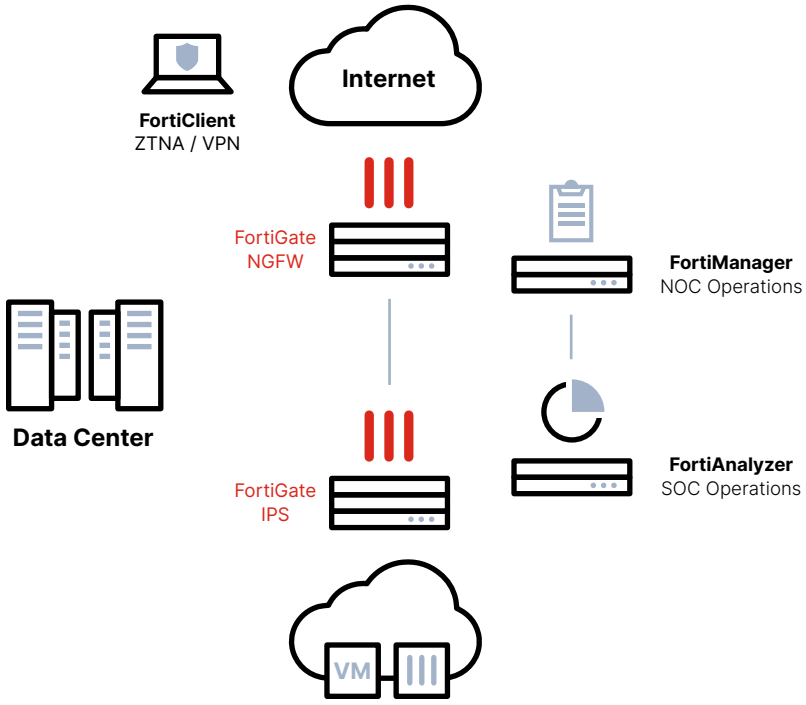
Secure SD-WAN

- 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

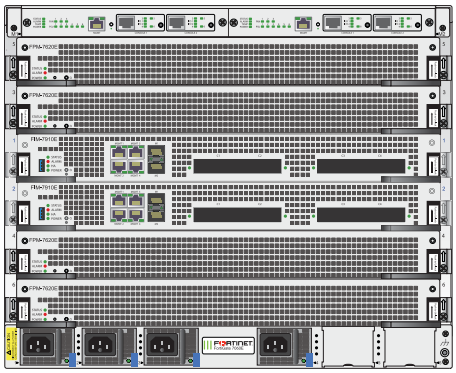
Mobile Security for 4G, 5G, and IoT

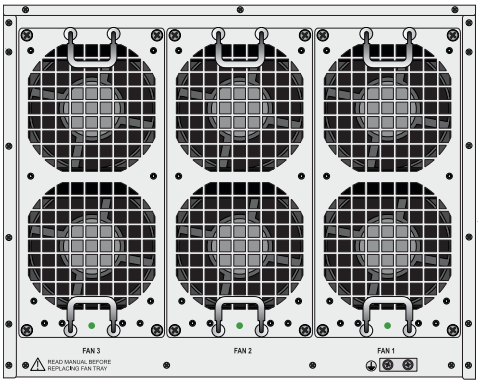
- SPU-accelerated, high performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/ DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- RAN Access Security with highly scalable and highest-performing IPsec aggregation and control Security Gateway (SecGW)
- User plane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

Datacenter Deployment (NGFW, IPS, Segmentation)



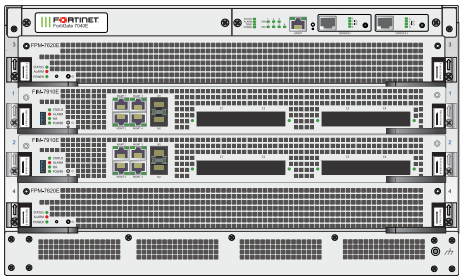
Hardware

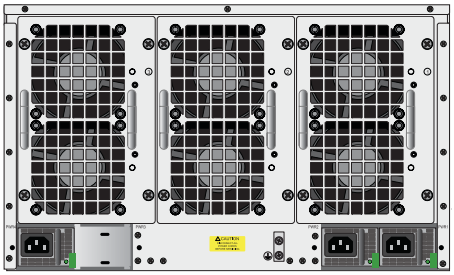




FortiGate 7060E

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.

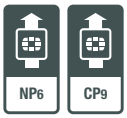
** Based on all default included components.

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.

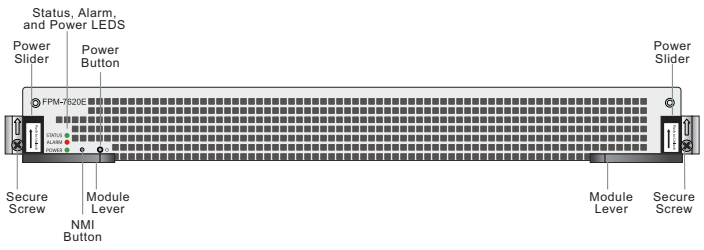
Modules

Fortinet Processor Module 7620E

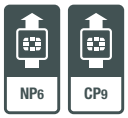


The latest purpose-built SPU CP9 accelerated processor module with superior content processing throughput and protection. The device runs on FortiOS — the most powerful security operating system in the world.

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

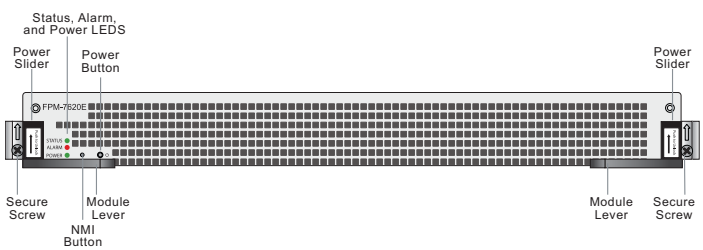


Fortinet Processor Module 7630E



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.

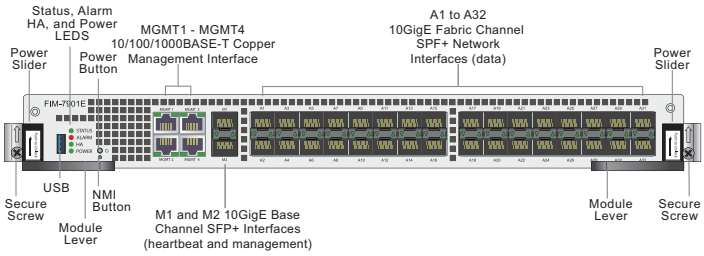
Power and Environment	FG-7630E
Power Consumption (Average/Maximum)	320 / 410 W
Heat Dissipation (Average)	1395 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)
Storage Temperature	-31°F to 158°F (-35°C to 70°C)
Humidity	20% to 90% non-condensing
Compliance	
Certifications	FCC, ICES, CE, RCM, VCCI,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



Modules

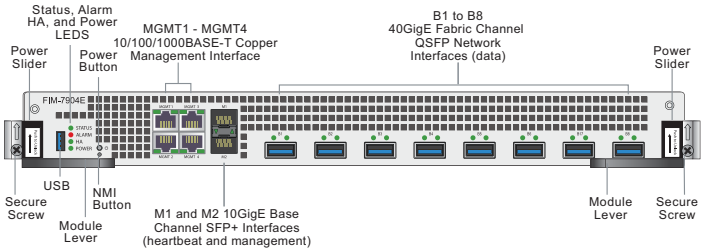
Fortinet Interface Module 7901E

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



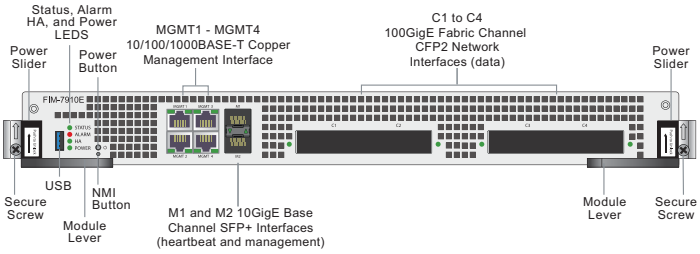
Fortinet Interface Module 7904E

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



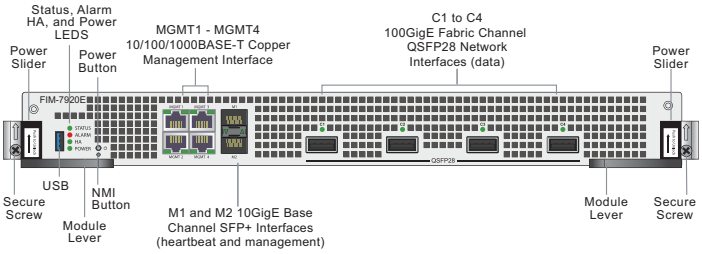
Fortinet Interface Module 7910E

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.

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [3], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]	•			
	Application Control		included with FortiCare Subscription		
	Inline CASB [3]		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	•			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth) [2]	•			
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	•			
	FortiGate 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 [2]	•			
	FortiCare Premium	•	•	•	•
	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. Full features available when running FortiOS 7.4.1.
2. Desktop Models only.
3. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards.

FortiGuard Bundles

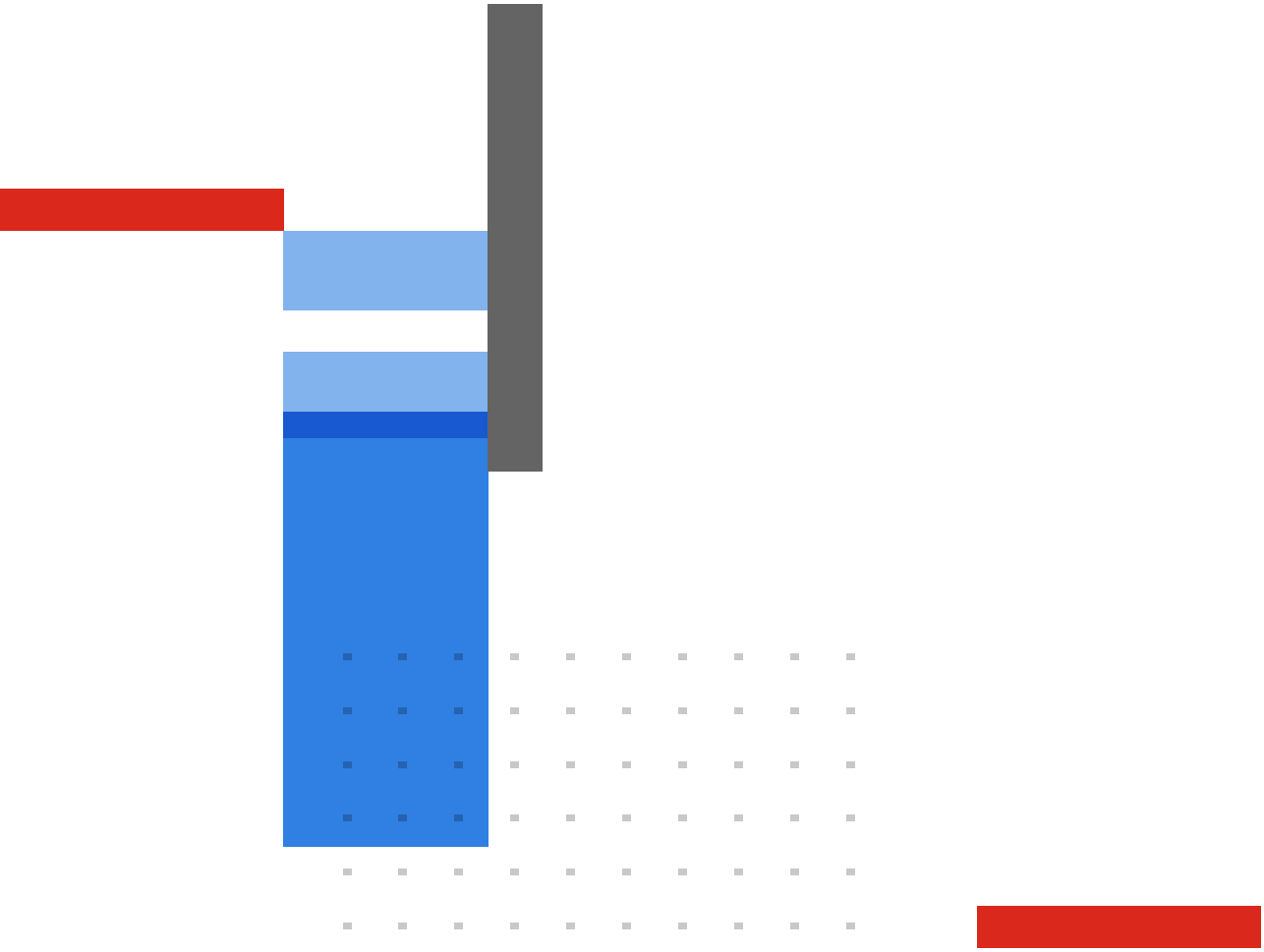
FortiGuard Labs delivers a number of security intelligence services to augment the FortiGate firewall platform. You can easily optimize the protection capabilities of your FortiGate with one of these FortiGuard Bundles.

FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive lifecycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service variants, offers heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an Extended End-of-Engineering-Support of 18 months, providing flexibility. Access the intuitive FortiCare Elite Portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet 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 © 2024 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 Chief Legal Officer, 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.

May 29, 2024

FG-7000E-DAT-R43-20240529