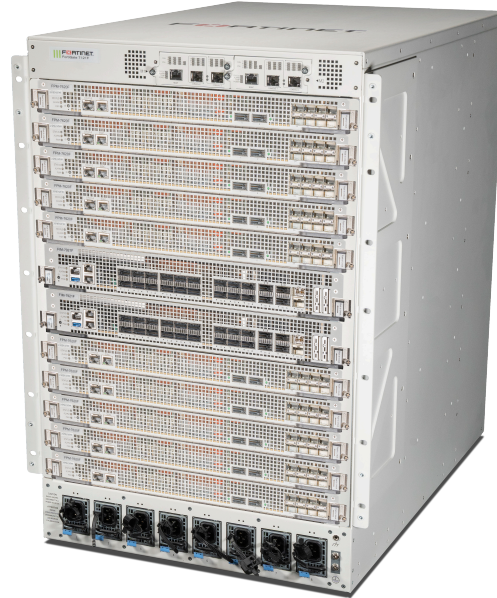


FortiGate 7121F Series

FG-7121F, FIM-7921F, FIM-7941F, and FPM-7620F



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 7121F 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 7121F 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 7121F automatically controls, verifies, and facilitates user access to applications delivering consistent convergence with a seamless user experience.

IPS	NGFW	Threat Protection	Interfaces
675 Gbps	550 Gbps	520 Gbps	25 GE SFP28 / 10 GE SFP+ / GE SFP 100 GE QSFP28 / 40 GE QSFP+ 400 GE QSFP-DD



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

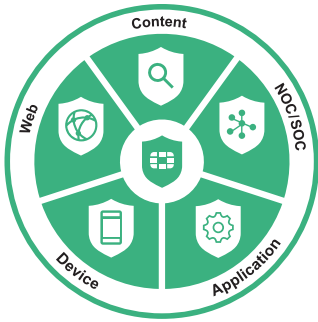


Visibility with FOS Application Signatures

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

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

SOC-as-a-Service

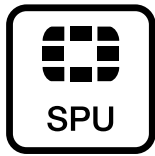
Includes tier-one hunting and automation, log location, 24x7 SOC analyst experts, managed firewall and endpoint functions, and alert triage.

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:

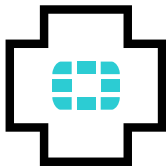
- Hyperscale firewall, accelerated session setup, and ultra-low latency
- Industry-leading performance for VPN, VXLAN termination, hardware logging, and elephant flows



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



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

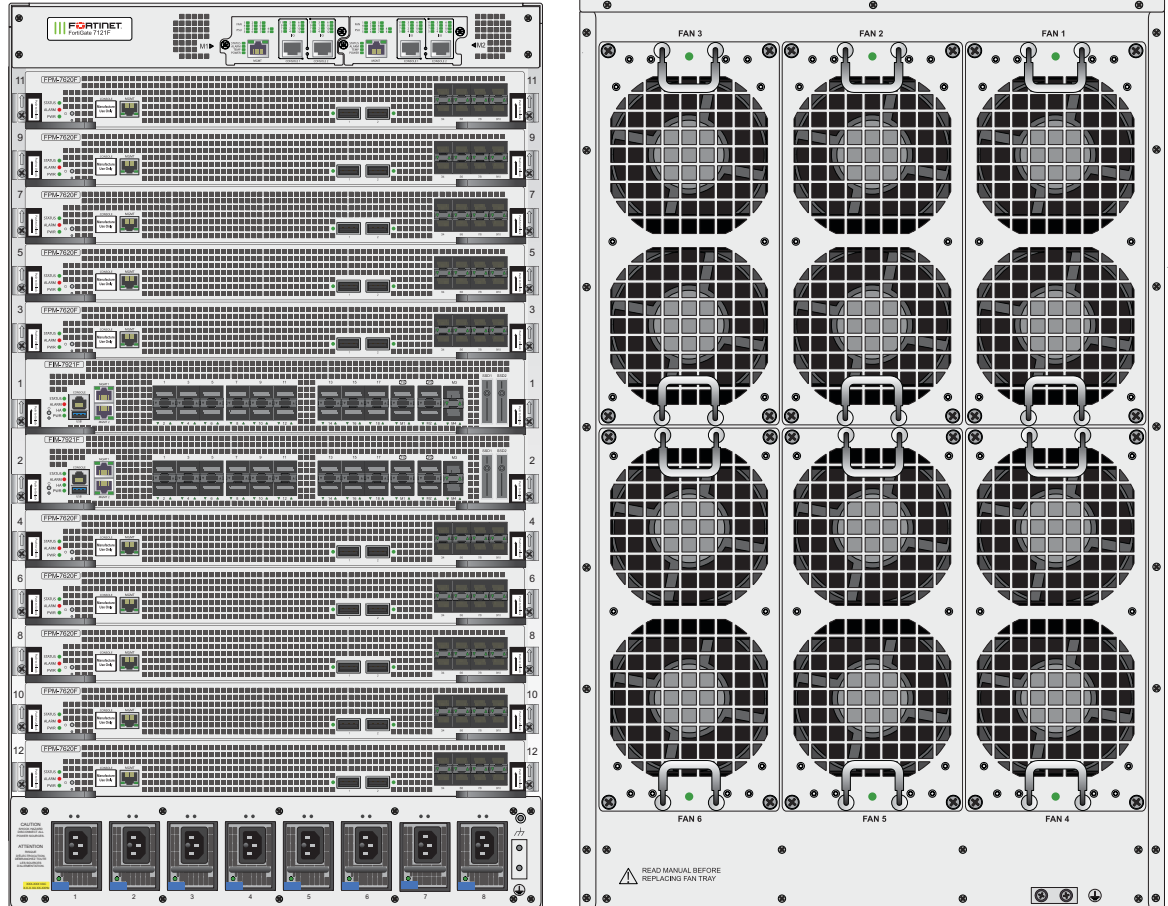
- SPU-accelerated, high performance CGNAT and IPv6 migration options, including: NAT44, NAT444, NAT64/ DNS64, NAT46 for 4G Gi/sGi, and 5G N6 connectivity and security
- RAN Access Security with highly scalable and highest-performing IPsec aggregation and control Security Gateway (SecGW)
- User plane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

Datacenter Deployment (NGFW, IPS, Segmentation)



Hardware

FortiGate 7121F

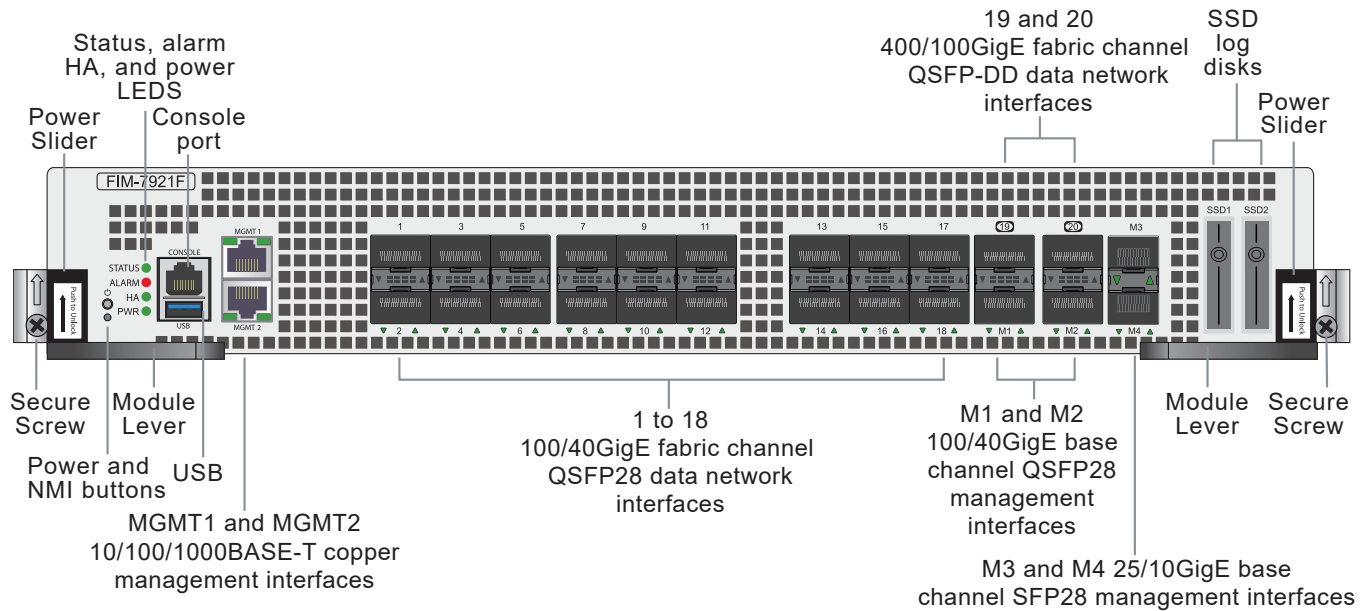


Trusted Platform Module (TPM)

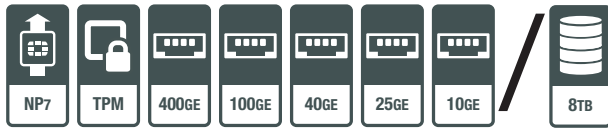
The FortiGate 7121F Series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

Hardware

Fortinet Interface Module FIM-7921F and FIM-7941F



Hardware Features



Specifications

	FIM-7921F	FIM-7941F
Hardware Interfaces		
Hardware Accelerated 400 GE QSFP-DD / 100 GE QSFP28 / 40 GE QSFP+ Slots	2 ¹	2 ¹
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	18 ²	18 ³
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Management/HA Slots	2	2
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ SFP Management/HA Slots	2	2
GE RJ45 Management Ports	2	2
USB Ports	1	1
Console Ports	1	1
Onboard Storage	2 × 4 TB SSD	2 × 4 TB SSD
Included Transceivers	2 × 10 GE SFP+ SR	2 × 10 GE SFP+ SR
Dimensions and Power		
Height x Width x Length (inches)	2.48 × 17.11 × 18.56	2.48 × 17.11 × 18.56
Height x Width x Length (mm)	63 × 435 × 471.3	63 × 435 × 471.3
Weight	21.48 lbs (9.75 kg)	25.66 lbs (11.65 kg)
Power Consumption (Average / Maximum)	568 W / 597 W	598 W / 630 W
Current (Maximum)	50A	53A
Heat Dissipation (Average)	2036 BTU/h	2149 BTU/h
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-31°–158°F (-35°–70°C)	-31°–158°F (-35°–70°C)
Humidity	10%–90% non-condensing	5%–90% non-condensing
Compliance		
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	

1. Both ports 19 and 20 can be configured as split ports

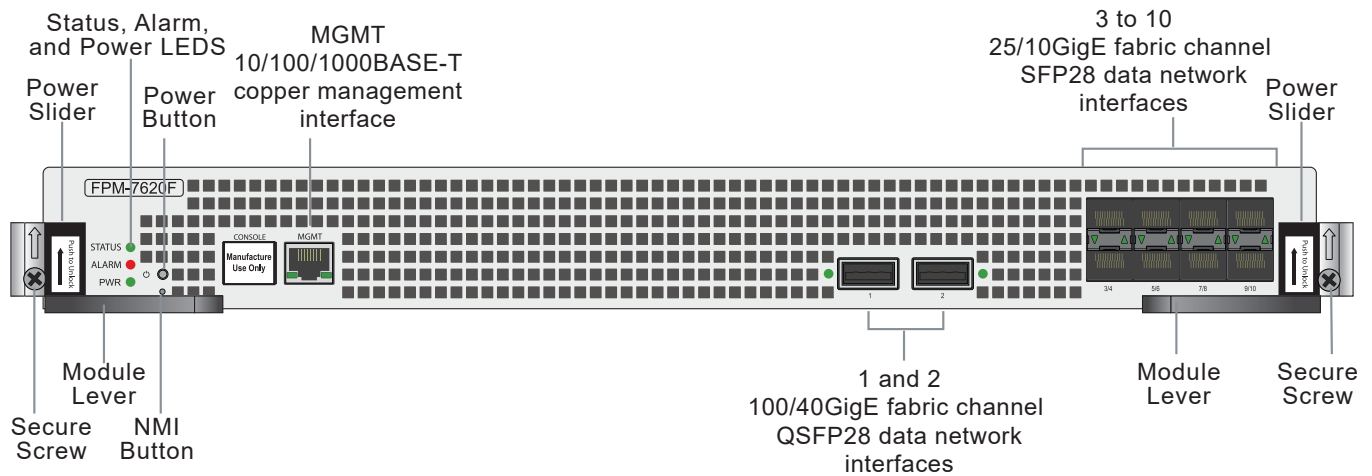
2. Ports 1-8 can be configured as split ports

3. Ports 1-18 can be configured as split ports



Hardware

Fortinet Processor Module FPM-7620F



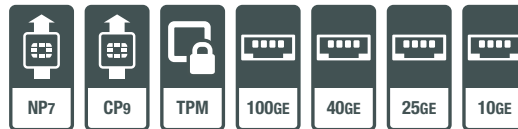
Specifications

FPM-7620F	
Hardware Interfaces	
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	2
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots	8
GE RJ45 Management Ports	1
Console Ports	1
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP packets)	396 / 395 / 263 Gbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP packets)	396 / 395 / 263 Gbps
Firewall Latency (64 byte, UDP)	7.50 µs
Firewall Throughput (Packet per Second)	39 286 Mpps
Concurrent Sessions (TCP)	100 Million
New Sessions/Sec (TCP)	900K
Firewall Policies	200 000 (system wide)
IPsec VPN Throughput (512 byte) ⁶	63 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	4000
Client-to-Gateway IPsec VPN Tunnels	26 000
SSL-VPN Throughput ⁷	13.7 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	30 000
IPS Throughput (Enterprise Mix) ¹	67.5 Gbps
SSL Inspection Throughput ²	54 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³	48 000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	10 Million
Application Control Throughput ³	150 Gbps
NGFW Throughput ⁴	55 Gbps

Note: All performance values are "up to" and vary depending on system configuration.

- IPsec VPN performance test uses AES256-SHA256.
- IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
- SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

Hardware Features



FPM-7620F	
Threat Protection Throughput ⁵	52 Gbps
CAPWAP Throughput	N.A.
Virtual Domains (Default / Maximum)	10 / 500
Maximum Number of FortiTokens	2000
Maximum Number of FortiSwitches Supported	300
Maximum Number of FortiAPs (Total / Tunnel Mode)	N.A.
High Availability Configurations	Active-Passive, Active-Active
Dimensions and Power	
Height x Width x Length (inches)	1.69 x 17.11 x 18.56
Height x Width x Length (mm)	43 x 435 x 471
Weight	16.19 lb. (7.35 kg)
Power Consumption (Average / Maximum)	675 W / 716 W
Current (Maximum)	60A
Heat Dissipation (Average)	2442 BTU/h
Operating Temperature	32°–104°F (0°–40°C)
Storage Temperature	-13°–158°F (-25°–70°C)
Humidity	20%–90% non-condensing
Compliance	
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB

- NGFW performance is measured with Firewall, IPS and Application Control enabled.
- Threat Protection performance is measured with Firewall, IPS, Application Control, URL filtering, and Malware Protection with sandboxing enabled.
- Measured with VPN load balancing.
- Measured on single FPM only.



Specifications

	FG-7121F*
Interfaces and Modules	
Hardware Accelerated 400 GE QSFP-DD / 100 GE QSFP28 / 40 GE QSFP+ Slots	4
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Slots	56
Hardware Accelerated 100 GE QSFP28 / 40 GE QSFP+ Management/HA Slots	4
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ Slots	80
Hardware Accelerated 25 GE SFP28 / 10 GE SFP+ SFP Management/HA Slots	4
GE RJ45 Management Ports	4
USB Ports	2
Console Ports	14
Onboard Storage	4 × 4 TB SSD
Included Transceivers	4 × 10 GE SFP+ SR
System Performance - Enterprise Traffic Mix	
IPS Throughput ²	675 Gbps
NGFW Throughput ^{2,4}	550 Gbps
Threat Protection Throughput ^{2,5}	520 Gbps
System Performance and Capacity	
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP packets)	1.89 / 1.88 / 1.129 Tbps
IPv6 Firewall Throughput (1518 / 512 / 86 byte, UDP packets)	1.89 / 1.88 / 1.129 Tbps
Firewall Latency (64 byte, UDP)	7.50 μs
Firewall Throughput (Packet per Second)	1680 Mpps
Concurrent Sessions (TCP)	1 Billion
New Sessions/Sec (TCP)	9 Million
Firewall Policies	200 000
IPsec VPN Throughput (512 byte) ⁶	630 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	40 000
Client-to-Gateway IPsec VPN Tunnels	260 000
SSL-VPN Throughput ⁷	13.7 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	30 000
IPS Throughput (Enterprise Mix) ¹	675 Gbps
SSL Inspection Throughput ³	540 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³	480 000
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	100 Million
Application Control Throughput ³	1.5 Tbps
NGFW Throughput ⁴	550 Gbps
Threat Protection Throughput ⁵	520 Gbps
CAPWAP Throughput	N.A.
Virtual Domains (Default / Maximum)	10 / 500

	FG-7121F*
System Performance and Capacity	
Maximum Number of FortiTokens	20 000
Maximum Number of FortiSwitches Supported	300
Maximum Number of FortiAPs (Total / Tunnel Mode)	N.A.
High Availability Configurations	Active-Active (FGSP), Active-Passive, Clustering
Dimensions and Power	
Height x Width x Length (inches)	28.63 × 17.33 × 26.6
Height x Width x Length (mm)	727.2 × 440 × 675.5
Weight (maximum)	447.36 lbs (203.1 kg)
Form Factor (supports EIA/non-EIA standards)	16 RU 10 Slots for FPM and 2 Slots for FIM (default configuration 2xFPM-7620F and 2xFIM-7921F)
Power Required	200 to 240 VAC (50/60 Hz)
Power Consumption (Maximum / Average)	9754 W / 8296 W
AC Current (Maximum)	8 × 10A
Heat Dissipation (Maximum)	33 261 BTU/h
Operating Environment and Certifications	
Operating Temperature	32°–104°F (0°–40°C)
Storage Temperature	-31°–158°F (-35°–70°C)
Humidity	20%–90% non-condensing
Compliance	
Certifications	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB

* Performance specifications for FG-7121F are based on 10 FPM combination.

Note: All performance values are "up to" and vary depending on system configuration.

1. IPsec VPN performance test uses AES256-SHA256.
2. IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.
3. SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

4. NGFW performance is measured with Firewall, IPS and Application Control enabled.
5. Threat Protection performance is measured with Firewall, IPS, Application Control, URL filtering, and Malware Protection with sandboxing enabled.
6. Measured with VPN load balancing.
7. Measured on single FPM only.



Ordering Information

Product	SKU	Description
FortiGate 7121F*	FG-7121F	16U 12-slot chassis with 2x FPM-7620F Processor Module, 2x FIM-7921F I/O Module, 2x Management Module and 8x hot swappable redundant PSU.
FortiGate-7121F-2	FG-7121F-2	16U 12-slot chassis with 2x FPM-7620F Processor Module, 2x FIM-7941F I/O Module, 2x Management Module and 8x hot swappable redundant PSU.
FortiGate-7121F-DC	FG-7121F-DC	16U 12-slot chassis with 2x FPM-7620F Processor Module, 2x FIM-7921F I/O Module, 2x Management Module and 8x hot swappable redundant PSU 2KW DC-DC (without DC combiner).
OPTIONAL / SPARE ITEMS	SKU	DESCRIPTION
Processor Module		
FPM-7620F Module	FPM-7620F	Hot swappable processing module for 7xxxF series - FortiASIC NP7 and CP9 hardware accelerated. 2x QSFP28 and 8x SFP28 ports.
I/O Module		
FIM-7921F Module**	FIM-7921F	Hot swappable I/O module for 7xxxF series - FortiASIC NP7 hardware accelerated. 2x GE RJ45 Management ports, 2x QSFP-DD ports, 20x QSFP28 ports, 2x SFP28 ports. 2x 4TB local log storage.
FIM-7941F Module**	FIM-7941F	Hot swappable I/O module for 7xxxF series - FortiASIC NP7 hardware accelerated. 2x GE RJ45 Management ports, 2x QSFP-DD ports, 20x QSFP28 ports, 2x SFP28 ports. 2x 4TB local log storage.
Accessories		
Fan Module	FG-7121F-FAN	FG-7121F Fan module.
Power Supply	FG-7121F-PS-2KAC	FG-7121F power supply 2KW AC.
FortiGate-7121F-AC-Chassis	FG-7121F-CH	FG-7121F chassis with 2x system management module, 8x PSU and 6x FAN module.
FortiGate-7121F-DC-Chassis	FG-7121F-DC-CH	FG-7121F chassis with 2x system management module, 8x DC PSU and 6x FAN module, 8x DC input cable.
FG-7121F-DC-Combiner	FG-7121F-DC-COMBINER	1U rack mounted chassis containing 8x DC combiner module to support A+B input redundancy for FG-7121F-DC.
Transceivers		
1GE SFP RJ45 transceiver module	FN-TRAN-GC	1GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1GE SFP SX transceiver module	FN-TRAN-SX	1GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1GE SFP LX transceiver module	FN-TRAN-LX	1GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10GE copper SFP+ RJ45 Transceiver (30m range)	FN-TRAN-SFP+GC	10GE copper SFP+ RJ45 Fortinet Transceiver (30m range) for systems with SFP+ slots.
10GE SFP+ transceiver module, short range	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10GE SFP+ transceiver module, long range	FN-TRAN-SFP+LR	10GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10Gbase-ER SFP+ transceivers	FN-TRAN-SFP+ER	10Gbase-ER SFP+ transceivers for FortiSwitch and FortiGate, 1550nm. Single Mode. 40km range for systems with SFP+ slots.
25GE SFP28 transceiver module, short range	FN-TRAN-SFP28-SR	25GE/10GE Dual Rate SFP28 transceiver module, short range for all systems with SFP28/SFP+ slots.
25GE SFP28 transceiver module, long range	FN-TRAN-SFP28-LR	25GE SFP28 transceiver module, long range for all systems with SFP28 slots.
40GE QSFP+ transceivers, short range	FN-TRAN-QSFP+SR	40GE QSFP+ transceivers, short range for all systems with QSFP+ slots.
40GE QSFP+ transceivers, long range	FN-TRAN-QSFP+LR	40GE QSFP+ transceivers, long range for all systems with QSFP+ slots.
100GE QSFP28 transceivers	FN-TRAN-QSFP28-SR	100GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.
100 GE QSFP28 transceivers, long range	FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, 4 channel parallel fiber, long range for all systems with QSFP28 slots.
100 GE QSFP28 transceivers	FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 slots.
400 GE QSFPDD transceiver module, 10km range	FN-TRAN-QSFPDD-LR4	400 GE QSFPDD transceiver module, 10km range, SMF, for systems with QSFP-DD slots
400 GE QSFPDD transceiver module, 2km range	FN-TRAN-QSFPDD-FR4	400 GE QSFPDD transceiver module, 2km range, SMF, for systems with QSFP-DD slots
400 GE QSFPDD transceiver module, 4 channel parallel fiber	FN-TRAN-QSFPDD-DR4	400 GE QSFPDD transceiver module, 4 channel parallel fiber, short range, for systems with QSFP-DD slots
400 GE QSFPDD transceiver module, 8 channel parallel fiber	FN-TRAN-QSFPDD-SR8	400 GE QSFPDD transceiver module, 8 channel parallel fiber, short range, for systems with QSFP-DD slots
400 GE QSFPDD passive Direct Attach Cable, 1m	FN-CABLE-QSFPDD-DAC-01	400 GE QSFPDD passive Direct Attach Cable, 1m, for systems with QSFP-DD slots.
400 GE QSFPDD passive Direct Attach Cable, 2.5m	FN-CABLE-QSFPDD-DAC-B5	400 GE QSFPDD passive Direct Attach Cable, 2.5m, for systems with QSFP-DD slots.

* The FG-7121F has Chassis-based pricing. Individual and bundled FortiGuard security services and FortiCare support subscription services such as Threat Protection Bundle, UTM Bundle, Enterprise Bundle, and FortiCare360 are on a chassis-based pricing. License such as VDOM and Endpoint Compliance are also included in the chassis-based pricing.

** Each FIM is packed individually and comes with 2x 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
Security Services	FortiGuard IPS Service	•	•	•	•
	FortiGuard Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	FortiGuard Web Security — URL and web content, Video and Secure DNS Filtering	•	•	•	
	FortiGuard Anti-Spam		•	•	
	FortiGuard IoT Detection Service	•	•		
	FortiGuard Industrial Security Service	•	•		
	FortiCloud AI-based Inline Sandbox Service ¹	•			
NOC Services	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiGuard Security Fabric Rating & Compliance Monitoring Service	•	•		
	FortiConverter Service	•	•		
	FortiGuard SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
SOC Services	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	FortiGuard Application Control				
	FortiCloud ZTNA Inline CASB Service ¹				
	Internet Service (SaaS) DB Updates				
	GeolP DB Updates				included with FortiCare Subscription
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

1. Available when running FortiOS 7.2



FortiGuard Bundles

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

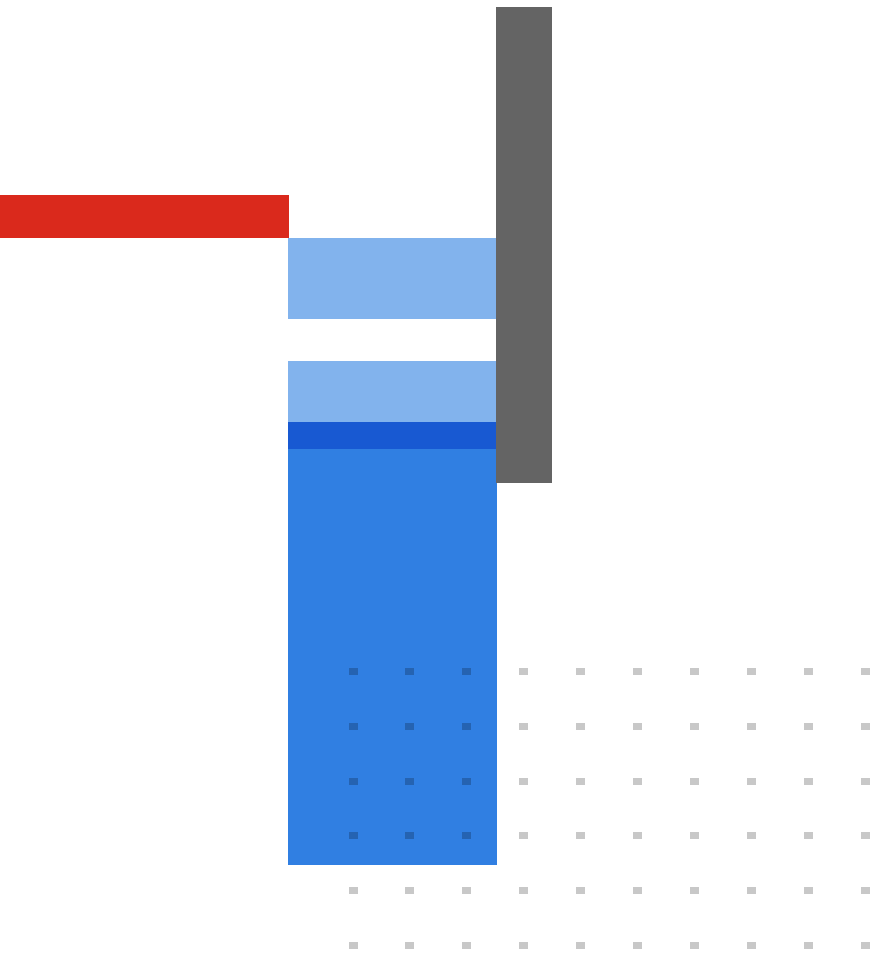
FortiCare Elite

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

Fortinet CSR Policy

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





FORTINET

www.fortinet.com

Copyright © 2023 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 General Counsel, 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.

January 24, 2023

FG-7121F-DAT-R10-20230124