

**PROPOSTA COMERCIAL****À****COMPANHIA CAMPOLARGUENSE DE ENERGIA – COCEL****Ref.: LICITAÇÃO N.º 018/2024**

Prezados Senhores:

Tem a presente a finalidade de apresentar a nossa proposta para locação de servidor de FIREWALL, de acordo com as quantidades e características constantes do Anexo I, do **Edital de Licitação n.º 018/2024**, considerando:

1. que o prazo de validade da é de 60 (sessenta) dias, contados a partir da data da abertura da referida proposta;
2. que o local de entrega e instalação é na Rua Rui Barbosa, n.º 520 – Campo Largo – PR, SEDE da COCEL;
3. que o prazo de entrega de instalação é de até 15 (quinze) dias, contados da assinatura do contrato;
4. que o prazo de pagamento da primeira parcela é de 30 (trinta) dias após a data de instalação e as demais a partir do 30º (trigésimo) dia da data do primeiro pagamento, sendo o mesmo efetuado no prazo de 08 (oito) dias úteis a contar da data de entrega das notas Fiscais na sede da COCEL;
5. que os equipamentos em questão terão garantia durante a vigência do contrato;
6. que concordamos em firmar o contrato para fornecimento do(s) objeto(s) relacionados nesta proposta, pelo(s) preço(s) apresentado através do lance registrado e oferecido por nosso representante credenciado;
7. que o preço ofertado é de:

**ITEM ÚNICO** – Locação de 1 (uma) unidade SERVIDOR DE FIREWALL. DEMAIS CARACTERISTICAS CONFORME DESCRITO NO TERMO DE REFERÊNCIA – ANEXO I DO PRESENTE EDITAL. **MARCA FORTINET, MODELO FORTIGATE-100F, É DE R\$ 4.000,00 (QUATRO MIL REAIS) MENSAL, TOTALIZANDO A IMPORTÂNCIA DE R\$ 240.000,00 (DUZENTOS E QUARENTA MIL REAIS) PARA O PERIODO DE 60 MESES.**

8. declaramos que confirmaremos com nova proposta, no prazo de até 03 (três) dias úteis, os itens que foram apresentados lances com novos preços, e julgado como vencedor do certame;
9. declaramos ainda que, nos preços estão incluídos os custos diretos e indiretos, bem como administração, lucro e imprevistos, inclusive todos os tributos (ICMS, SUBST., IPI E OUTROS) sujeitos em decorrência da presente Proposta;
10. que concordamos com as demais disposições do Edital, e reconhecemos à COCEL, o direito de aceitar ou rejeitar todas as propostas sem que nos assista qualquer direito indenizatório.

Curitiba/PR, 04 de abril de 2024.

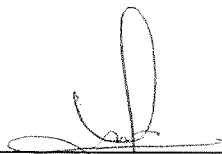
11.064.603/0001-73

SIGMA SERVIÇOS DE TECNOLOGIA LTDA

R. São Francisco, 232 Sala. 1311

CENTRO - CEP 80.020-190

CURITIBA PR



INGRID MAGDIELE DE LIMA COSTA

PROCURADORA

CPF:

**Dados da empresa para formalização do contrato caso sejamos vencedor:**

Razão Social: SIGMA SERVIÇOS DE TECNOLOGIA LTDA

Endereço: Rua São Francisco, 232 - Sala 1311, Andar 13 – Bloco Green Center - Centro

Município: Curitiba UF: Paraná CEP: 80020-190

Telefone: (41) 3360-6630 Email: licitacao@tmtelecom.com.br

CNPJ: 11.064.603/0001-73 Inscrição: 904.913.71-57

**Dados do Representante legal:**

Nome: Ingrid Magdiele de Lima Costa

Endereço: Rua São Francisco, 232 - Sala 1311, Andar 13 – Bloco Green Center - Centro

Município: Curitiba UF: Paraná CEP: 80020-190

CPF/MF: [REDACTED]

Cargo/Função: Analista de Licitações

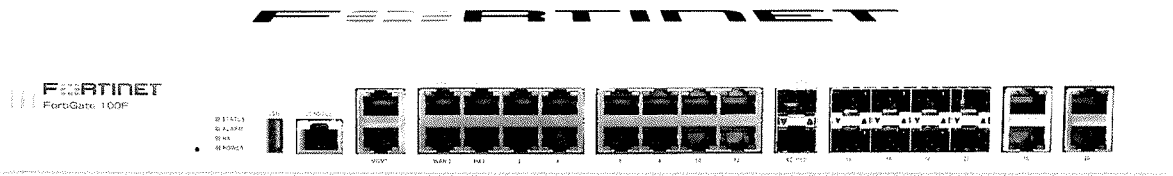
CIRG N.º: [REDACTED]

Expedida por: SSP/PR



# FortiGate 100F Series

FG-100F and FG-101F



## Highlights

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

**Security-Driven Networking** FortiOS delivers converged networking and security.

**State-of-the-Art Unparalleled Performance** with Fortinet's patented / SPU / VSPU processors.

**Enterprise Security** with consolidated AI / ML-powered FortiGuard Services.

**Deep Visibility** into applications, users, and devices beyond traditional firewall techniques.

## AI/ML Security and Deep Visibility

The FortiGate 100F Series NGFW combines AI-powered security and machine learning to deliver Threat Protection at any scale. Get deeper visibility into your network and see applications, users, and devices before they become threats.

Powered by a rich set of AI/ML security capabilities that extend into an integrated security fabric platform, the FortiGate 100F Series delivers secure networking that is broad, deep, and automated. Secure your network end to end with advanced edge protection that includes web, content, and device security, while network segmentation and secure SD-WAN reduce complexity and risk in hybrid IT networks.

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

IPS	NGFW	Threat Protection	Interfaces
2.6 Gbps	1.6 Gbps	1 Gbps	Multiple GE RJ45, GE SFP and 10 GE SFP+ slots

*R* *A*



Available in



Appliance



Virtual



Hosted



Cloud



Container

## FortiOS Everywhere

### FortiOS, Fortinet's Advanced Operating System

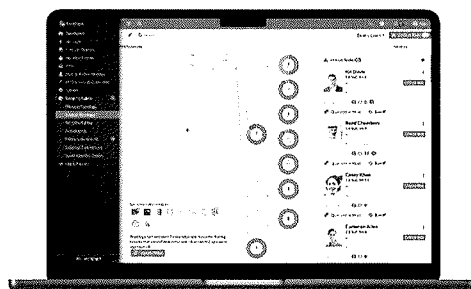
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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.

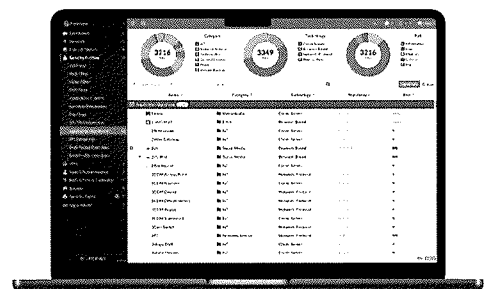
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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/ML 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

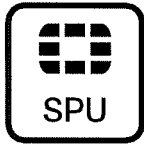
Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® 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.

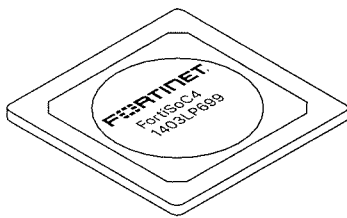


## Secure Any Edge at Any Scale



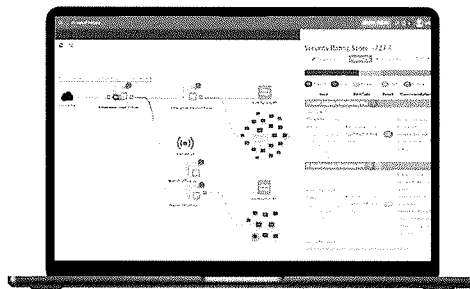
### Powered by Security Processing Unit (SPU)

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.



### Powered by Purpose-Built Secure SD-WAN ASIC SOC4

- Combines a RISC-based CPU with Fortinet's proprietary Security Processing Unit (SPU) content and network processors for unmatched performance
- Delivers industry's fastest application identification and steering for efficient business operations
- Accelerates Psec VPN performance for best user-experience on direct internet access
- Enables best of breed NGFW Security and deep SSL inspection with high performance
- Extends security to access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity
- Reduces environmental footprint by saving on average over 60% in power consumption compared to previous generation of FortiGate models



*Intuitive view and clear insights into network security posture with FortiManager*

### Centralized Network and Security Management at Scale

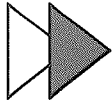
FortiManager, the centralized management solution from Fortinet, enables integrated management of the Fortinet security fabric, including devices like FortiGate, FortiSwitch, and FortiAP. It simplifies and automates the oversight of network and security functions across diverse environments, serving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



*R*

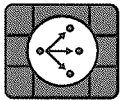
*✓*

## Use Cases



### Next Generation Firewall (NGFW)

- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications across the attack surface
- Fortinet's patented SPU (Security Processing Unit) technology provides industry-leading high-performance protection



### Secure SD-WAN

- FortiGate WAN Edge powered by one OS and unified security and management framework and systems transforms and secures WANs
- Delivers superior quality of experience and effective security posture for work-from-anywhere modes, SD-Branch, and cloud-first WAN use cases
- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing



### Universal ZTNA

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

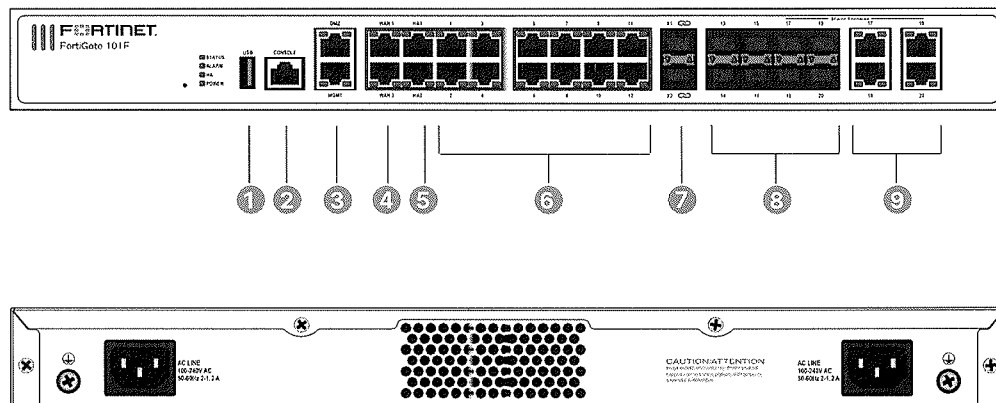


### Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security—from the branch to the datacenter and across multi-cloud environments
- Ultra-scalable, low latency, VXLAN segmentation bridges physical and virtual domains with Layer 4 firewall rules
- Prevents lateral movement across the network with advanced, coordinated protection from FortiGuard Security Services detects and prevents known, zero-day, and unknown attacks

## Hardware

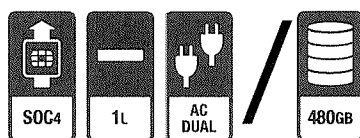
### FortiGate 100F Series



### Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/DMZ Ports
4. 2 x GE RJ45 WAN Ports
5. 2 x GE RJ45 HA Ports
6. 12 x GE RJ45 Ports
7. 2 x 10 GE SFP+ FortiLink Slots
8. 4 x GE SFP Slots
9. 4 x GE RJ45/ SFP Shared Media Pairs

### Hardware Features



### Dual Power Supplies

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 100F Series offers dual built-in non-hot swappable power supplies.

### Access Layer Security

FortiLink protocol enables you to converge security and the network access by integrating the FortiSwitch into the FortiGate as a logical extension of the NGFW. These FortiLink enabled ports can be reconfigured as regular ports as needed.



## Specifications

	FORTIGATE 100F	FORTIGATE 101F		FORTIGATE 100F	FORTIGATE 101F
<b>Interfaces and Modules</b>			<b>Dimensions and Power</b>		
Hardware Accelerated GE RJ45 Ports		12	Height x Width x Length (inches)		1.73 × 17 × 10
Hardware Accelerated GE RJ45 Management/ HA/ DMZ Ports		1 / 2 / 1	Height x Width x Length (mm)		44 × 432 × 254
Hardware Accelerated GE SFP Slots		4	Weight	7.25 lbs (3.29 kg)	7.56 lbs (3.43 kg)
Hardware Accelerated 10 GE SFP+ FortiLink Slots (default)		2	Form Factor (supports EIA/non-EIA standards)		Rack Mount, 1 RU
GE RJ45 WAN Ports		2	AC Power Supply		100–240V AC, 50/60 Hz
GE RJ45 or SFP Shared Ports *		4	Power Consumption (Average / Maximum)	26.5 W / 29.5 W	35.3 W / 39.1 W
USB Port		1	Current (Maximum)		100V / 1A, 240V / 0.5A
Console Port		1	Heat Dissipation	100.6 BTU/h	121.13 BTU/h
Onboard Storage	0	1 × 480 GB SSD	Redundant Power Supplies		Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)
Included Transceivers		0			
<b>System Performance — Enterprise Traffic Mix</b>			<b>Power Supply Efficiency Rating</b>		80Plus Compliant
IPS Throughput <sup>2</sup>		2.6 Gbps	<b>Operating Environment and Certifications</b>		
NGFW Throughput <sup>2,4</sup>		1.6 Gbps	Operating Temperature		32°F to 104°F (0°C to 40°C)
Threat Protection Throughput <sup>2,5</sup>		1 Gbps	Storage Temperature		-31°F to 158°F (-35°C to 70°C)
<b>System Performance and Capacity</b>			Humidity		10% to 90% non-condensing
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)		20 / 16 / 10 Gbps	Noise Level		40.4 dBA
Firewall Latency (64 byte, UDP)		4.97 µ	Forced Airflow		Side to Back
Firewall Throughput (Packet per Second)		15 Mp/s	Operating Altitude		Up to 10 000 ft (3048 m)
Concurrent Sessions (TCP)		1.5 Million	Compliance		FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI
New Sessions/Second (TCP)		53 000	<b>Certifications</b>		USGv6/IPv6
Firewall Policies		13 000			
IPsec VPN Throughput (512 byte) <sup>1</sup>		11.5 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels		2000			
Client-to-Gateway IPsec VPN Tunnels		13 000			
SSL-VPN Throughput		1 Gbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)		500			
SSL Inspection Throughput (IPS, avg. HTTPS) <sup>3</sup>		1 Gbps			
SSL Inspection CPS (IPS, avg. HTTPS) <sup>3</sup>		1800			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) <sup>3</sup>		135 000			
Application Control Throughput (HTTP 64K) <sup>2</sup>		2.2 Gbps			
CAPWAP Throughput (HTTP 64K)		13 Gbps			
Virtual Domains (Default / Maximum)		0 / 13			
Maximum Number of FortiSwitches Supported		32			
Maximum Number of FortiAPs (Total / Tunnel)		128 / 64			
Maximum Number of FortiTokens		5000			
High Availability Configurations		Active-Active, Active-Passive, Clustering			

\* Latency based on Ultra Low Latency (ULL ports)

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

<sup>1</sup> IPsec VPN performance test uses AES256-SHA256.

<sup>2</sup> IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

<sup>3</sup> SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

<sup>4</sup> NGFW performance is measured with Firewall, IPS and Application Control enabled.

<sup>5</sup> Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

<sup>6</sup> Uses RSA-2048 certificate.



*[Handwritten signature]*

*[Handwritten signature]*

## Ordering Information

Product	SKU	Description
FortiGate 100F	FG-100F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10 GE SFP+ FortiLinks, dual power supplies redundancy.
FortiGate 101F	FG-101F	22x GE RJ45 ports (including 2x WAN ports, 1x DMZ port, 1x Mgmt port, 2x HA ports, 16x switch ports with 4 SFP port shared media), 4 SFP ports, 2x 10 GE SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy.
Optional Accessories	SKU	Description
1 GE SFP RJ45 Transceiver Module	FN-TRAN-3C	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceivers, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10GE SFP+ Transceiver Module, 30 km Long Range	FN-TRAN-SFP+BD27	10GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10GE SFP+ Transceiver Module, 30 km Long Range	FN-TRAN-SFP+BD33	10GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
10 GE SFP+ Passive Direct Attach Cable 1m	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 3m	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 5m	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.

## Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS Service	•	•	•	•
	Anti-Malware Protection (AMP) — Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection and FortiSandbox Cloud Service	•	•	•	•
	URL, DNS & Video Filtering Service	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malware Prevention Service	•	•		
	Data Loss Prevention Service <sup>1</sup>	•	•		
	OT Security Service (OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) <sup>1</sup>	•			
	Application Control		included with FortiCare Subscription		
	CASB SaaS Control		included with FortiCare Subscription		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring Service	•			
	SD-WAN Overlay-as-a-Service for SaaS-based overlay network provisioning	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	FortiSASE subscription including cloud management and 10Mbps bandwidth license <sup>2</sup>	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) <sup>1</sup>	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials <sup>2</sup>	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Internet Service (SaaS) DB Updates				
	GeoIP DB Updates		included with FortiCare Subscription		
	Device/OS Detection Signatures				
	Trusted Certificate DB Updates				
	DDNS (v4/v6) Service				

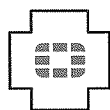
1. Full features available when running FortiOS 7.4.1

2. Desktop Models only



### 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 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.



[www.fortinet.com](http://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 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 disavows 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 4, 2024

FG-100F-DAT-R35-20240104