FASTHELP

Proposta

Comercial

FAST HELP INFORMÁTICA LTDA - CNPJ: 05.889.039/0001-25 –
Endereço: TR SIA/SUL Trecho 03 Lote 990 – Ed. Itaú - 3º andar (cobertura) - Guará- Brasília/DF – CEP: 71.200-030
Telefax: (61) 3363-8636 – E-mail: comercial@fasthelp.com.br – www.fasthelp.com.br

Fasthelp20th

Sobre
a FastHelp

- **20 ANOS** DE EXPERIÊNCIA NO MERCADO

- ESPECIALIZADA EM **SERVIÇOS E SOLUÇÕES** EM CIBERSEGURANÇA

- **+250** CLIENTES

- PRESENTE EM **TODO TERRITÓRIO NACIONAL**

- ATENDIMENTO AO **SETOR PÚBLICO E PRIVADO**
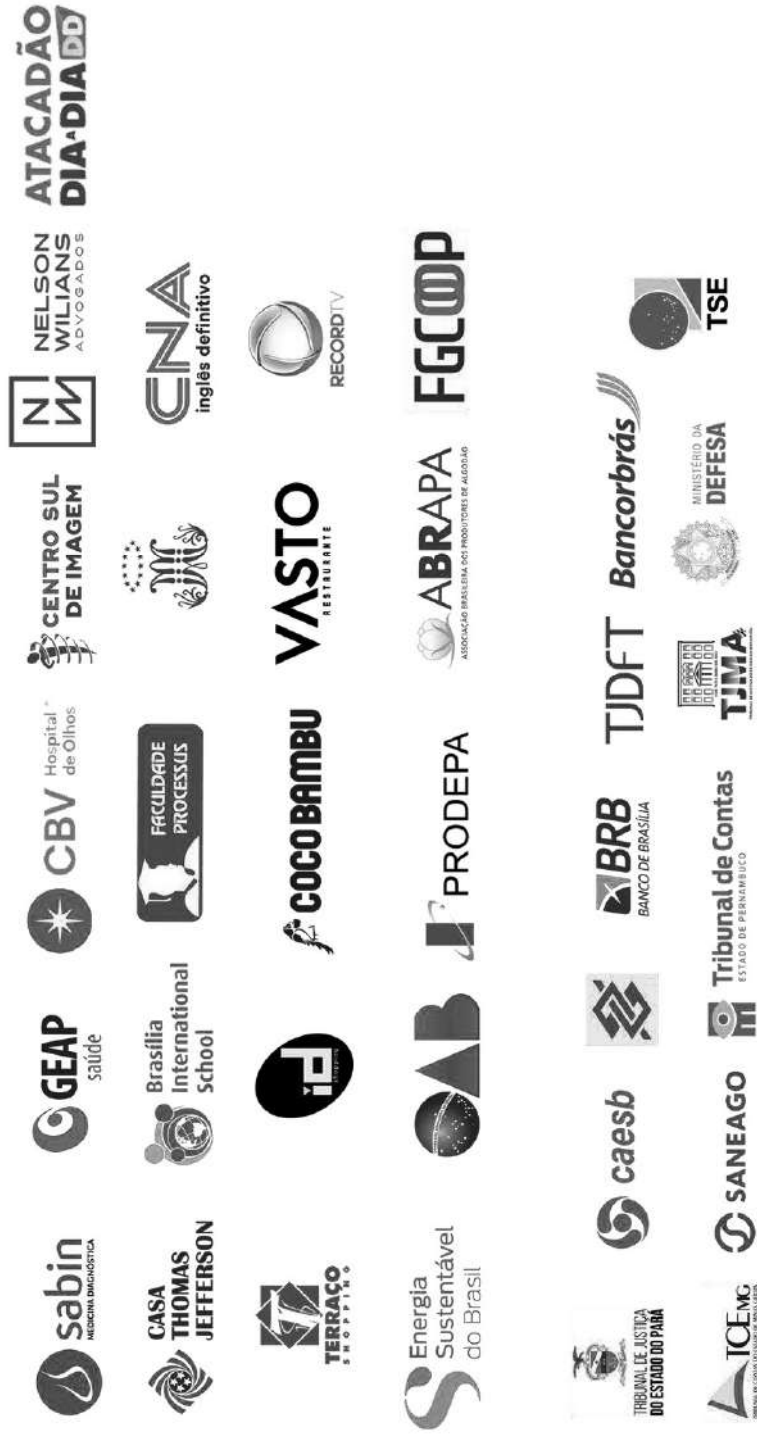
- SERVIÇOS E SOLUÇÕES PARA **TODAS AS VERTICAIS DE NEGÓCIO**

Great Place To Work — Certificada — Jan.2023 – Jan.2024 — BRASIL

CERTIGOV — PRATA — Válido até 30/08/2025 — FAST HELP

FASTHELP CERTIFIED — ISO 27001

FASTHELP CERTIFIED — ISO 9001–2015

Nossas
INSTALAÇÕES

Algumas empresas
que acreditam no nosso trabalho
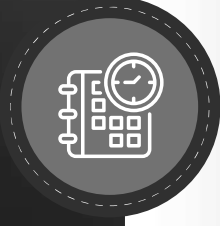
PORQUE ESCOLHER
a FastHelp

Soluções únicas para ampliar a disponibilidade do ambiente de negócio de nossos clientes. Defenda sua empresa com o mesmo conhecimento de quem ataca. Escolha suas armas.
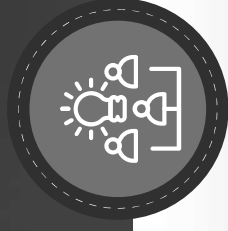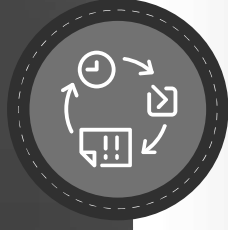
Projetos e serviços personalizados para as suas necessidades

Treinamento para Clientes e Equipe interna.

Serviços únicos e sob medida com disponibilidade 24/7.

Qualidade profissional dos serviços prestados por uma equipe altamente qualificada.
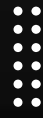
Nossas Soluções

SEGURANÇA DA INFORMAÇÃO:

Para todos os tamanhos, contra todas as ameaças!

- SOC / MDR
- Cloud Service
- NDR e Visibilidade de Rede
- Pentest
- Next generation firewall
- Proteção Endpoint/Mobile
- E-mail Security Gateway
- SIEM / SOAR / UEBA

- CASB / SASE / SSE / ZTNA
- VPN
- IPS
- DLP - Data Loss Prevention
- DNS Segura
- Gestão de ativos
- Cloud Security

- WAF
- Balanceamento de carga
- Gerenciamento de identidade
- PAM / Cofre de senhas
- Gerenciamento e análise de vulnerabilidades
- Conscientização de usuários em SI

- Network Access Control
- Security Web Gateway
- Backup & recovery
- Criptografia
- Proteção da marca - Brand Protection Cybersecurity

Parceria com os Fabricantes
LÍDERES DE MERCADO

kaspersky · paloalto NETWORKS · Forcepoint · SOPHOS · TREND MICRO

VERITAS · arcserve · securiti · Extreme networks · Trellix

WatchGuard · aruba · IBM Security · CYBERARK · A10

FORTINET · BeyondTrust · tenable · veeAM · aws

appgate · Qualys · HSC HIGH SECURITY CENTER · f5 · Gigamon

PENTERA

SOC
Security Operation Center

Fiel ao seu DNA pioneiro, a FastHelp se manteve de olho nas tendências do setor e, há 7 anos, passou a investir no SOC (Security Operation Center), antecipando a demanda de empresas de todos os setores por soluções que lhes permitam delegar a gestão em segurança da informação a especialistas, permitindo-lhes focar no que fazem de melhor: desenvolver os próprios negócios.

A SEGURANÇA CIBERNÉTICA é tão complexa, e se move tão rapidamente que a maioria das organizações simplesmente não conseguem gerenciá-la de forma efetiva por conta própria.

BENEFÍCIOS DO SOC PARA O SEU NEGÓCIO

Expansão da sua força de trabalho

Redução dos riscos aos se negócio

Atendimento a Regulação – Compliance

Visibilidade

Fast Cloud

Estamos empolgados em anunciar a inauguração da nossa nova unidade de negócios dedicada a soluções em Cloud. Com o compromisso de impulsionar a transformação digital da sua empresa, oferecemos uma gama completa de serviços que garantem mais agilidade, segurança e eficiência.

Por que escolher nossas soluções em Cloud?

Redução de Custos:
Minimize investimentos em infraestrutura física e reduza despesas operacionais com modelos de pagamento por uso.

Escalabilidade Sob Medida:
Ajuste rapidamente seus recursos conforme a demanda do seu negócio cresce, sem desperdícios.

Desempenho Elevado:
Garanta alta performance com nossos servidores otimizados e suporte técnico especializado.

Segurança de Ponta:
Proteja seus dados com as mais avançadas tecnologias de segurança e conformidade.

Inovação Contínua:
Esteja sempre à frente com acesso às mais recentes inovações tecnológicas e atualizações automáticas.

IMPLEMENTAÇÃO PERSONALIZADA

Nossa área de Gestão de Projetos é responsável por garantir que todos os pontos do contrato sejam entregues com eficiência e eficácia, fazendo a ponte entre a área Comercial, Suporte Técnico e o nossos clientes.

Uma das características mais importantes do serviço gerenciado da Fast é nossa capacidade de implementação personalizada das soluções. Assim conseguimos atender clientes das mais variadas infraestruturas com qualidade e eficiência.
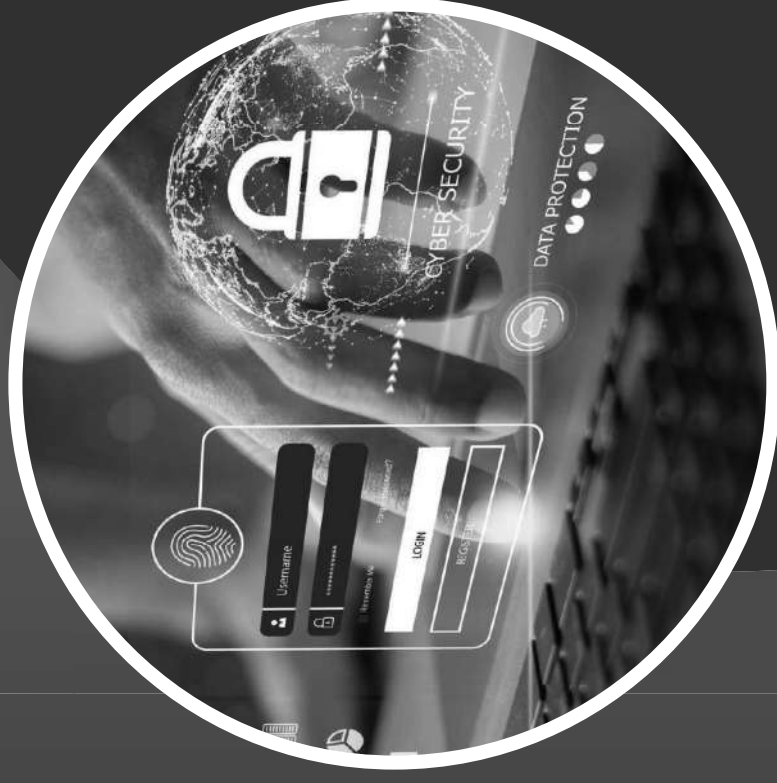
Conecte-se
conosco

Instagram: @fasthelp_cybersecurity
LinkedIn: FastHelp Segurança da Informação

comercial@fasthelp.com.br

+55 (61) 3363-8636

www.fasthelp.com.br

SIA/SUL Trecho 3, Lote 990, Edifícil Itaú –
Cobertura. Brasília, DF

FASTHELP 20

Fasthelp 20th

www.fasthelp.com.br

PROPOSTA COMERCIAL

A

**AGÊNCIA REGULADORA DE ÁGUAS, ENERGIA E SANEAMENTO BÁSICO
DO DISTRITO FEDERAL - ADASA**

**REF.: PREGÃO ELETRÔNICO Nº 90011/2024
PROCESSO ADMINISTRATIVO Nº 00197-00001310/2024-68**

Prezados Senhores,

A empresa **FAST HELP INFORMÁTICA LTDA**, inscrita no CNPJ 05.889.039/0001-25, inscrição estadual nº 07.448.780/001-31, sediada na SIA/SUL Trecho 03, Lote 990 – Cobertura Edifício Itaú, Brasília-DF, CEP 71200-030, por intermédio de seu representante legal, o Sr Paulo Ferreira Ribeiro, portador da Carteira de Identidade nº 14966239 – SSP/SP, e do CPF nº 516.902.336-72, submete à apreciação de V.S, nossa proposta comercial relativa ao pregão em epígrafe, para aquisição de equipamento de segurança da informação tipo firewall, incluídos instalação e configuração, além de licença de uso e suporte técnico por um período de 36 meses, de acordo com as especificações do edital e anexos.

Produto/Serviço	Quantidade	Modelo	Marca	Valor Unitário R$	Valor Total R$
Firewall	02	600F	Fortinet	R$ 109.260,21	R$ 218.520,42
Licenciamento 36 meses	02	600F	Fortinet	R$ 163.743,03	R$ 327.486,06
Suporte Técnico 24x7x365	01	-	-	R$ 27.777,64	R$ 27.777,64
Instalação	01	-	-	R$ 17.115,88	R$ 17.115,88
				Valor Global R$	**R$ 590.900,00**

Valor Global da Proposta: R$ 590.900,00 (quinhentos e noventa mil e novecentos reais).

Validade da Proposta: 60 (sessenta) dias, a contar da data de sua apresentação.

Após examinar todas as cláusulas e condições estipuladas no Edital em referência, apresentamos nossa proposta nos termos consignados no mencionado ato convocatório e seus anexos, com os quais concordamos plenamente.

Estão inclusos todos os tributos, custos e despesas diretas ou indiretas, sendo de nossa inteira responsabilidade, ainda, os que porventura venham a ser omitidos na proposta ou incorretamente cotados.

FAST HELP INFORMÁTICA LTDA - CNPJ: 05.889.039/0001-25 **–**
Endereço: TR SIA/SUL Trecho 03 Lote 990 **–** Ed. Itaú - 3º andar (cobertura) - Guará- Brasília/DF **–** CEP: 71.200-030
Telefax: (61) 3363-8636 **–** E-mail: comercial@fasthelp.com.br **–** www.fasthelp.com.br

Caso nos seja adjudicado o objeto da licitação, comprometemos em cumprir as obrigações assumidas no prazo determinado no documento de convocação, e, para esse fim, fornecemos os seguintes dados:

Dados da Empresa:
- **Razão Social:** Fast Help Informática LTDA
- **CNPJ:** 05.889.039/0001-25
- **Inscrição Estadual:** 07.448.780/001-31
- **Endereço:** Sia/Sul Trecho 03, Lt 990, Cobertura Ed. Itaú, Brasília-DF, CEP: 71200-030.
- **Telefone:** (61) 3363-8636
- **E-mail:** comercial@fasthelp.com.br

Dados do Representante Legal:
- **Nome:** Paulo Ferreira Ribeiro
- **Endereço:** Sia/Sul Trecho 03, Lt 990, Cobertura Ed. Itaú, Brasília-DF, CEP: 71200-030.
- **Função**: Diretor Executivo
- **CPF:** 516.902.336-72
- **RG:** 14966239 Expedido por: SSP/SP
- **Nacionalidade:** Brasileiro
- **Telefone:** (61) 3363-8636 E-mail: comercial@fasthelp.com.br

Dados Bancários:
- **Código do Banco:** 001
- **Banco:** Banco do Brasil S/A
- **Agência:** 1231-9
- **Conta corrente:** 38.515-8
- **Praça de Pagamento:** Brasília

Declaramos estar de acordo com todas as condições estipuladas no edital e seus anexos.

Brasília (DF), 16 de outubro de 2024.

PAULO FERREIRA RIBEIRO
SÓCIO / PROPRIETÁRIO

FAST HELP INFORMÁTICA LTDA - CNPJ: 05.889.039/0001-25 –
Endereço: TR SIA/SUL Trecho 03 Lote 990 – Ed. Itaú - 3° andar (cobertura) - Guará- Brasília/DF – CEP: 71.200-030
Telefax: (61) 3363-8636 – E-mail: comercial@fasthelp.com.br – www.fasthelp.com.br

Documentos

Técnicos

FAST HELP INFORMÁTICA LTDA - CNPJ: 05.889.039/0001-25 –
Endereço: TR SIA/SUL Trecho 03 Lote 990 – Ed. Itaú - 3º andar (cobertura) - Guará- Brasília/DF – CEP: 71.200-030
Telefax: (61) 3363-8636 – E-mail: comercial@fasthelp.com.br – www.fasthelp.com.br

CERTIFICADO DE PARCERIA

Date: 2024-October-08

Fortinet, Inc. reconhece que: Fast Help

Localizado na Rua:
SIA Trecho 3, Lote 990, Ed. Itau, Cobertura, Brasília, Distrito Federal 71.200-030, Brazil;

É atualmente um parceiro autorizado no BR a vender os produtos da Fortinet nas seguintes qualificações:

- Nivel de certificações: Select
- Modelo de Negócio: Integrator

Este certificado é válido por 180 dias.

Sempre que o FortiPartner, identificado anteriormente, comprar os serviços de suporte e estes forem registrados e contratados junto à Fortinet, a Fortinet concorda em oferecer os suportes cabíveis de acordo com os termos do contrato de suporte da Fortinet, disponível em https://support.fortinet.com. A garantia do equipamento Fortinet é limitado às garantias do fabricante que se encontram no site, http://www.fortinet.com/doc/legal/EULA.pdf.

Este certificado se dá na condição do FortiPartner manter seu contrato vigente com a Fortinet e seguir as políticas e diretrizes da Fortinet. O programa de parceiros da Fortinet e suas diretrizes estão disponíveis em http://www.fortinet.com/partners/partner_program/fpp.html. Não obstante serem parceiros autorizados, os FortiPartners não representam a Fortinet e consequentemente não podem fazer declarações em nome da Fortinet.
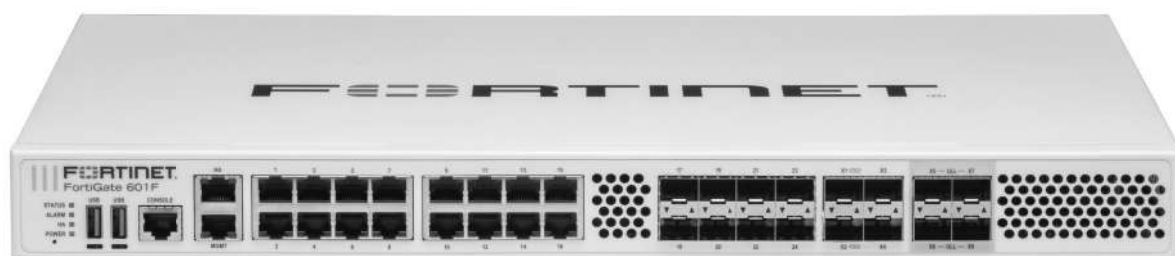
Manufacturer Confirmation

Gonzalo Ruiz
VP of Legal and Compliance Americas

FORTINET, INC.
909 Kifer Road
Sunnyvale, CA 94086

Telephone: +1-866-868-3678
Email: sales@fortinet.com
Website: www.fortinet.com

FORTINET

FortiGate 600F Series

Highlights

Gartner® Magic Quadrant™ Leaders for both Network Firewalls and WAN Edge Infrastructure

Secure Networking with FortiOS for converged networking and security

State-of-the-art unparalleled performance with Fortinet's patented SPU and vSPU processors

Enterprise security with consolidated AI/ML-powered FortiGuard services

Deep visibility into applications, users, and devices beyond traditional firewall techniques

Artificial Intelligence, Machine Learning Security with Deep Visibility

The FortiGate 600F series next-generation firewall (NGFW) combines artificial intelligence (AI)-powered security and machine learning (ML) 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 Fortinet ASIC technology, the 600F series delivers industry-leading threat detection capabilities, allowing for faster identification and mitigation of cyberthreats. Powered by a rich set of AI/ML security capabilities that extend into an integrated Security Fabric platform, the FortiGate 600F 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 zero-trust network access (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
14 Gbps	11.5 Gbps	10.5 Gbps	Multiple 25GE SFP28, 10GE SFP+, GE SFP Slots and GE RJ45

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, malware, zero days, and sophisticated AI-powered 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 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 hybrid working models, SD-Branch, and cloud-first WAN use cases

- Achieve operational efficiencies at any scale through automation, deep analytics, and self-healing

Universal ZTNA

- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies

- Provide extensive authentications, checks, and enforce policy prior to granting application access every time

- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

Segmentation

- Dynamic segmentation adapts to any network topology to deliver true end-to-end security from the branch to the data center 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

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. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. With over 18,000 signatures, our industry-leading intrusion prevention system (IPS) uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, and applying virtual patches for newly discovered vulnerabilities. Anti-malware protection defends against both known and unknown file-based threats, combining antivirus and sandboxing for multi-layered security. Application control improves security compliance and provides real-time visibility into applications and usage.

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 over 300 million URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks. FortiGuard Labs blocks over 500 million malicious/phishing/spam URLs weekly, and blocks 32,000 botnet command-and-control attempts every minute, demonstrating the robust protection offered through Fortinet.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This includes data loss prevention to ensure visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. Our inline cloud access security broker service protects data in motion, at rest, and in the cloud, enforcing compliance standards and managing account, user, and cloud app usage. Services also assess infrastructure, validate configurations, and highlight risks and vulnerabilities, including IoT device detection and vulnerability correlation.

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 malware in real time, delivering sub-second protection across all NGFWs. The service also integrates the MITRE ATT&CK matrix to speed up investigations. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

OT security

With over 1000 virtual patches, 1100+ OT applications, and 3300+ 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.

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

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

FortiOS is the operating system that powers Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. FortiOS provides a unified framework for managing and securing networks, cloud-based, hybrid, or a convergence of IT, OT, and IoT. FortiOS enables seamless and efficient interoperation across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances overall security posture. Together, FortiGate and FortiOS create intelligent, adaptive protection to help organizations reduce complexity, eliminate security silos, and optimize user experience.

By integration generative AI (GenAI), FortiOS further enhances the ability to analyze network traffic and threat intelligence, detects deviations or anomalies more effectively, and provides more precise remediation recommendations, ensuring minimum performance impact without compromising security.

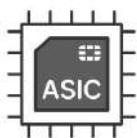Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios

Intuitive easy to use view into the network and endpoint vulnerabilities

Comprehensive view of network performance, security, and system status

Fortinet ASICs: Unrivaled Security, Unprecedented Performance

Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

Network processor NP7

Network processors operate in line to deliver unmatched performance and scalability for critical network functions. Fortinet's breakthrough SPU NP7 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 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

FortiManager

Centralized management at scale for distributed enterprises

FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides real-time monitoring of the entire managed infrastructure and automates network operation workflows. Leveraging GenAI in FortiAI, it further enhances Day 0–1 configurations and provisioning, and Day N troubleshooting and maintenance, unlocking the full potential of the Fortinet Security Fabric and significantly boosting operational efficiency.

GenAI in FortiManager helps manage networks effortlessly—generates configuration and policy scripts, troubleshoots issues, and executes recommended actions.

FortiConverter Service
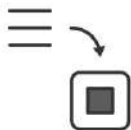
Migration to FortiGate NGFW made easy

The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. 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.

FortiCare Services

Expertise at your service

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides 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 and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

Hardware

FortiGate 600F Series
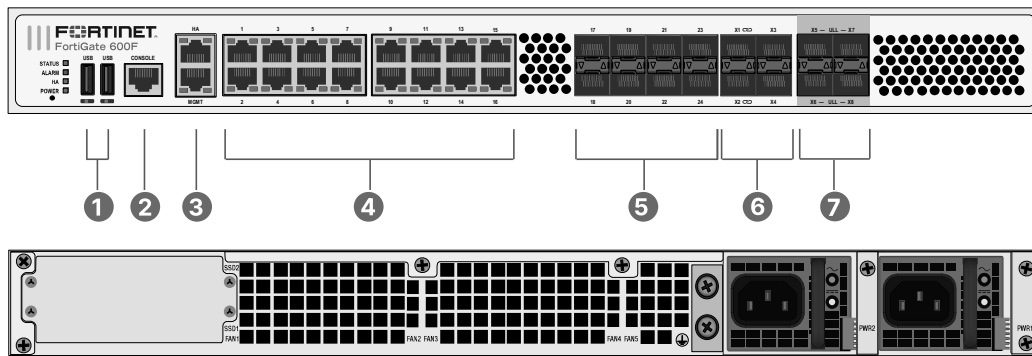
Interfaces

1. 2 x USB Ports
2. 1 x Console Port
3. 2 x GE RJ45 MGMT/HA Ports
4. 16 x GE RJ45 Slots
5. 8 x GE SFP Slots
6. 4 x 10GE/GE SFP+/SFP Slots
7. 4x 25GE/10GE SFP28/ SFP+ Ultra Low Latency Slots

Hardware Features

NP7 | CP9 | TPM | 1RU | 25GE | DUAL AC | 480GB

Trusted Platform Module (TPM)

The FortiGate 600F 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.

Dual power supply

Power supply redundancy is essential in the operation of mission-critical networks. The FortiGate 600F series offers dual built-in non-hot swappable power supplies.

Access layer security

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

Specifications

	FG-600F	FG-601F
Interfaces and Modules		
Hardware Accelerated GE RJ45 Interfaces	16	
Hardware Accelerated GE SFP Slots	8	
Hardware Accelerated 10GE SFP+ / GE SFP Slots	4	
Hardware Accelerated 25GE SFP28/ 10GE SFP+ Ultra Low Latency Slots	4	
GE RJ45 MGMT/HA Ports	2	
USB Ports	2	
RJ45 Console Port	1	
Onboard Storage	0	2× 240 GB SSD
Trusted Platform Module (TPM)	⊘	
Bluetooth Low Energy (BLE)	⊘	
Signed Firmware Hardware Switch	—	
Included Transceivers	2x SFP (SX 1 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	14 Gbps	
NGFW Throughput [2, 4]	11.5 Gbps	
Threat Protection Throughput [2, 5]	10.5 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	139 / 137.5 / 70 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	139 / 137.5 / 70 Gbps	
Firewall Latency (64 byte, UDP)	4.12 µs / 2.5 µs*	
Firewall Throughput (Packet per Second)	105 Mpps	
Concurrent Sessions (TCP)	8 Million	
New Sessions/Second (TCP)	550 000	
Firewall Policies	30 000	
IPsec VPN Throughput (512 byte) [1]	55 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	50 000	
SSL-VPN Throughput	4.3 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	10 000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	9 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	7500	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	840 000	
Application Control Throughput (HTTP 64K) [2]	32 Gbps	
CAPWAP Throughput (HTTP 64K)	64.5 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	96	
Maximum Number of FortiAPs (Total / Tunnel)	1024 / 512	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-600F	FG-601F
Dimensions and Power		
Height x Width x Length (inches)	1.75 × 17.0 × 15.0	
Height x Width x Length (mm)	44.45 × 432 × 380	
Weight	15.6 lbs (7.1 kg)	16.2 lbs (7.35 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1 RU	
AC Power Consumption (Average / Maximum)	169 W / 255 W	174 W / 260 W
AC Power Input	100–240V AC, 50/60Hz	
AC Current (Maximum)	6A@100V	
Heat Dissipation	871 BTU/h	888 BTU/h
Redundant Power Supplies (Hot Swappable)	Yes (comes with 2PSU default)	
Power Supply Efficiency Rating	80Plus Compliant	
Operating Environment and Certifications		
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	5% to 90% non-condensing	
Noise Level	55 dBA	
Airflow	Side and Front to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	
Certifications	USGv6/IPv6	

* Latency based on Ultra Low Latency (ULL ports)

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 and Malware Protection enabled.

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 Heuristic 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 AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.
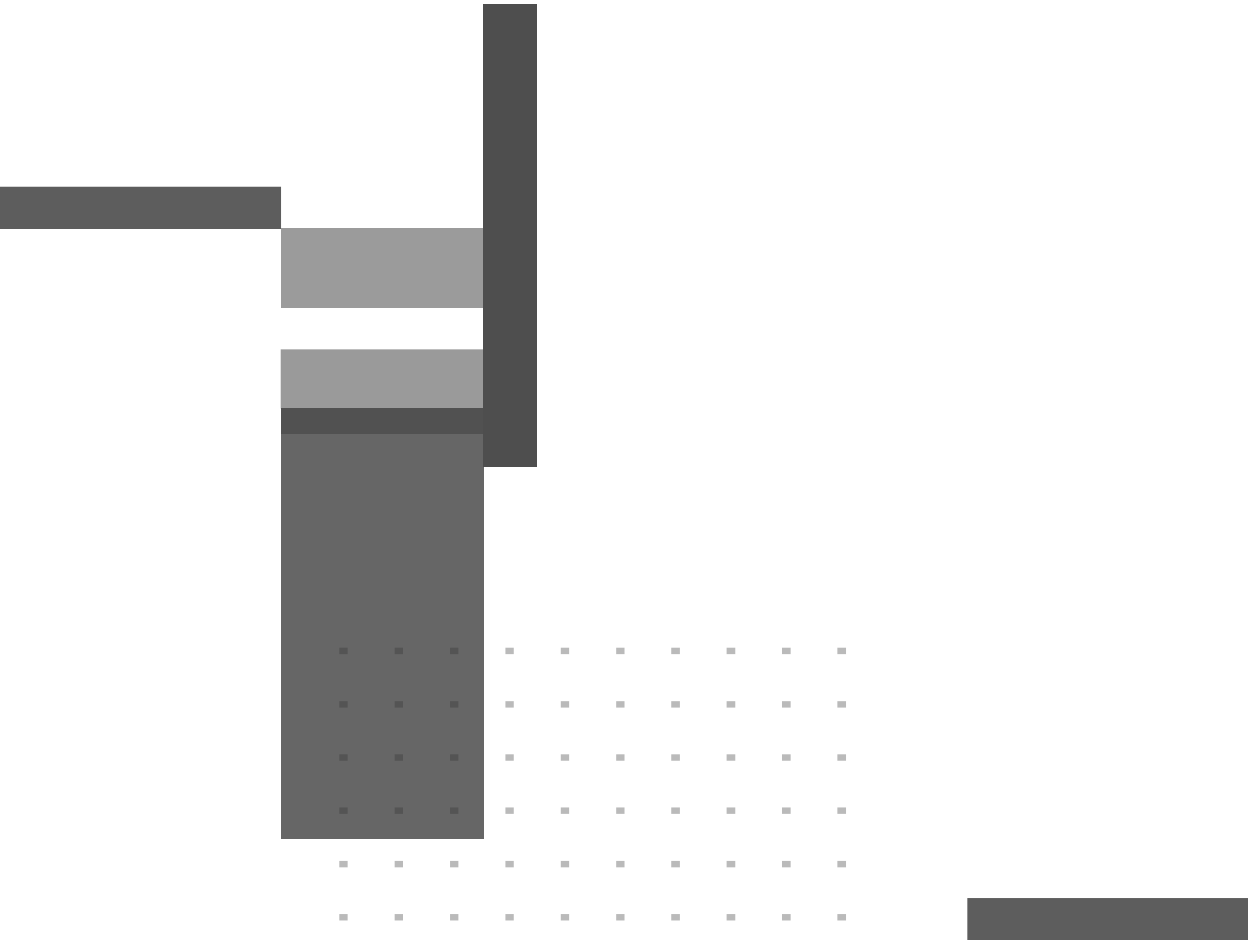
Ordering Information

Product	SKU	Description
FortiGate 600F	FG-600F	4× 25G SFP28 slots, 4× 10GE SFP+ slots, 18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, SPU NP7 and CP9 hardware accelerated, dual AC power supplies.
FortiGate 601F	FG-601F	4× 25G SFP28 slots, 4× 10GE SFP+ slots, 18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 8x GE SFP slots, SPU NP7 and CP9 hardware accelerated, 480GB onboard SSD storage, dual AC power supplies.
Optional Accessories		
AC Power Supply	SP-FG400F-PS	AC power supply for FG-400/401F, FG-600/601F, power cable SP-FGPCOR-XX sold separately.
Transceivers		
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	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.
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+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 30 km Long Range	FN-TRAN-SFP+BD27	10 GE SFP+ transceiver module, 30KM long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10 GE SFP+ Transceiver Module, 30 km Long Range	FN-TRAN-SFP+BD33	10 GE 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+ Transceiver Module, 80km Extreme Long Range	FN-TRAN-SFP+ZR	10GE SFP+ transceiver module, 80km extreme long range, for systems with SFP+ and SFP/SFP+ slots.
25 GE SFP28 Transceiver Module, Short Range	FN-TRAN-SFP28-SR	25 GE/10GE Dual Rate SFP28 transceiver module, short range for all systems with SFP28/SFP+ slots.
25 GE SFP28 Transceiver Module, Long Range	FN-TRAN-SFP28-LR	25 GE SFP28 transceiver module, long range for all systems with SFP28 slots.
Cables		
10 GE SFP+ Passive Direct Attach Cable, 1m Range	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m range, for systems with SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable 3m Range	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m range, for systems with SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable, 5m Range	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m range, for systems with SFP+ slots.
25 GE SFP28 Passive Direct Attach Cable, 1m Range	FN-CABLE-SFP28-1	25 GE SFP28 passive direct attach cable, 1m range, for systems with SFP28 slots.
25 GE SFP28 Passive Direct Attach Cable 3m Range	FN-CABLE-SFP28-3	25 GE SFP28 passive direct attach cable, 3m range, for systems with SFP28 slots.
25 GE SFP28 Passive Direct Attach Cable, 5m Range	FN-CABLE-SFP28-5	25 GE SFP28 passive direct attach cable, 5m range, for systems with SFP28 slots.

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

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.

F⊟RTINET

www.fortinet.com

FASTHELP

(61) 3363-8636

www.fasthelp.com.br   **comercial@fasthelp.com.br**

SIA/SUL Trecho 03, Lote 990 – cobertura Edifício Itaú, Brasília-DF, CEP: 71200-030