protocolo

De: Licitação <licitacao@camarapaulinia.sp.gov.br>
Enviado em: terça-feira, 28 de novembro de 2023 14:35
Para: protocolo@camarapaulinia.sp.gov.br
Assunto: ENC: PREGÃO PRESENCIAL Nº 013/2023 PROCESSO Nº 087/2023 DE 17/10/2023 - VOGEL SOLUÇÕES EM TELECOM. E INFORMÁTICA S/A
Anexos: Recurso Administrativo_DJUR 15712.pdf; fortigate-fortiwifi-40f-series.pdf

Lucas Alvarez Tafarello
Adjunto Legislativo
lucas@camarapaulinia.sp.gov.br
(19) 3874-7895

De: CLAUDIO PEREIRA COSTA <claudio.pereira@algartelecom.com.br>
Enviada em: terça-feira, 28 de novembro de 2023 14:33
Para: licitacao@camarapaulinia.sp.gov.br
Cc: Editais <editais@algartelecom.com.br>; Walace Bernard Guimaraes <walace@algartelecom.com.br>; Davidson Oliveira Fagundes <davidsonof@algartelecom.com.br>; JeanKarlo Rodrigues da Cunha <jeank@algartelecom.com.br>; Fabiano De Souza Terra <fabianost@algartelecom.com.br>
Assunto: PREGÃO PRESENCIAL Nº 013/2023 PROCESSO Nº 087/2023 DE 17/10/2023 - VOGEL SOLUÇÕES EM TELECOM. E INFORMÁTICA S/A

AO ILUSTRÍSSIMO SENHOR PREGOEIRO DESIGNADO PELA CÂMARA MUNICIPAL DE PAULÍNIA/SP

REFERENTE: EDITAL DE PREGÃO PRESENCIAL Nº 013/2023 - PROCESSO Nº 087/2023 DE 17/10/2023

VOGEL SOLUÇÕES EM TELECOMUNICAÇÕES E INFORMÁTICA S/A, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 05.872.814/0001-30, com endereço na Avenida Professor Vicente Rao, nº 1262, Bairro Jardim Petrópolis, na cidade de São Paulo/SP, por seu representante legal apresentar o presente RECURSO ADMINISTRATIVO, em face de ato administrativo do pregoeiro ocorrido na sessão pública do Pregão Presencial nº 013/2023, onde consta registrada a habilitação e arrematação do Lote 01 pela empresa BEST FIBRA TV E ENTRETENIMENTOS E TELECOMUNICAÇOES LTDA., mesmo estando esta, em desconformidade com o item 1 do Memorial Descritivo – Características Mínimas, bem como demais fatos, fundamentos e argumentos ***expostos na peça recursal em anexo.***

A ora recorrente, nos termos do item 10.5 do Edital, manifestou motivada intenção de recurso aos 23/11/2023, iniciando-se, aos 24/11/2023, o prazo de 03 (três) dias úteis para apresentação das razões, conforme item 10.7 do Edital.
Apreende-se que a data limite para interposição do presente recurso administrativo se dá aos **28/11/2023**, sendo este, portanto, próprio e tempestivo.

Assim sendo, solicitamos que este recurso seja acolhido tempestivamente e pedimos, gentilmente, **acusar o recebimento.**

Fico à disposição.

Att.

Cláudio Pereira Costa
Consultor Vendas Diretas - Governo.
Ribeirão Preto/SP.
Cel.: (16) 9.9796-4600
E-mail: claudio.pereira@algartelecom.com.br

https://algartelecom.com.br/empresas/governo

ILUSTRÍSSIMO SENHOR PREGOEIRO DESIGNADO PELA CÂMARA MUNICIPAL DE PAULÍNIA/SP

EDITAL DE PREGÃO PRESENCIAL Nº 013/2023
PROCESSO Nº 087/2023 DE 17/10/2023

VOGEL SOLUÇÕES EM TELECOMUNICAÇÕES E INFORMÁTICA S/A, pessoa jurídica de direito privado, inscrita no CNPJ sob o nº 05.872.814/0001-30, com endereço na Avenida Professor Vicente Rao, nº 1262, Bairro Jardim Petrópolis, na cidade de São Paulo/SP, por seu representante legal apresentar o presente

RECURSO ADMINISTRATIVO

em face de ato administrativo do pregoeiro ocorrido na sessão pública do Pregão Presencial nº 013/2023, ***onde consta registrada a habilitação e arrematação do Lote 01 pela empresa BEST FIBRA TV E ENTRETENIMENTOS E TELECOMUNICAÇOES LTDA., mesmo estando esta, em desconformidade com o item 1 do Memorial Descritivo – Características Mínimas,*** bem como demais fatos, fundamentos e argumentos a seguir expostos.

I. CERTAME E TEMPESTIVIDADE

1. O certame em questão, regido pelo Edital de Pregão Presencial nº 013/202, tipo menor preço por lote, tornou público o interesse da Câmara Municipal de Paulínia/SP na contratação de empresa para fornecimento de links de acesso à rede mundial de computadores (Internet) e Appliance (equipamento de segurança) em comodato visando a atendimento das

necessidades da Câmara Municipal de Paulínia, conforme condições e especificações constantes das cláusulas do Edital e seus anexos.

2. A sessão ocorreu aos 23/11/2023 no Plenário da Câmara Municipal de Paulínia e terminou com a arrematação e habilitação da empresa BEST FIBRA TV ENTRETENIMENTOS E TELECOMUNICAÇÕES LTDA para o Lote 01, mesmo estando, esta, em desconformidade com as disposições do Edital e de seus anexos.

3. A ora recorrente, nos termos do item 10.5 do Edital, manifestou motivada intenção de recurso aos 23/11/2023, iniciando-se, aos 24/11/2023, o prazo de 03 (três) dias úteis para apresentação das razões, conforme item 10.7 do Edital.

4. Apreende-se que a data limite para interposição do presente recurso administrativo se dá aos **28/11/2023,** sendo este, portanto, próprio e tempestivo.

II. RAZÕES DE RECURSO

5. Conforme será demonstrado a seguir, a condução do certame, exercida pelo Ilustre Pregoeiro, não se encontra de acordo com a legislação aplicável aos procedimentos licitatórios, bem como as próprias orientações e regras do Instrumento Convocatório que regem o presente Certame, de modo que é imperiosa a sua declaração de nulidade.

6. Diz-se isso justamente pelo fato de que, apesar de afirmar, o Ilustre Pregoeiro, que houve a devida verificação da documentação apresentada pela ora recorrida, concluindo-se pela habilitação dela, em simples análise é possível apreender que a BEST FIBRA TV ENTRETENIMENTOS E TELECOMUNICAÇÕES LTDA não cumpriu os requisitos obrigatórios de habilitação, qualificação e capacidade técnicas exigidos pelo instrumento convocatório.

7. Não havendo como admitir sua declaração de habilitação e arrematação como dotadas de validade, já que houve descumprimento dos requisitos dispostos no item 1 do Memorial Descritivo – Anexo I do Edital, nos termos de tudo o que se demonstra a seguir.

II.I DESCUMPRIMENTO DO ITEM 1 (CARACTERÍSTICAS MÍNIMAS DO FIREWALL) DO MEMORIAL DESCRITIVO, ANEXO I DO EDITAL. EQUIPAMENTO INDICADO PELA RECORRIDA NÃO ATENDE AOS REQUISITOS DO EDITAL E SEUS ANEXOS.

8. Para o fornecimento e execução dos serviços, o órgão contratante estabelece condições específicas no Edital e seus anexos, como é o caso das características mínimas para o Firewall, previstas no item 1 do Memorial Descritivo, anexo do Edital.

9. Analisando a documentação juntada pela empresa BEST FIBRA TV, tem-se que o equipamento apresentado por ela foi o modelo FORTGATE 40F.

10. Contudo, conforme as especificações exigidas para referida solução no Memorial Descritivo, resta evidente que o equipamento apresentado pela vencedora não atenderá a demanda da Câmara Municipal de Paulínia, justamente por não suportar os requisitos mínimos solicitados, conforme se vê no quadro comparativo abaixo:

	Termo de Referência	FG/FWF-40F
Firewall Throughput (1518/512/64 byte UDP)	20 Gbps	5 / 5 / 5 Gbps
IPsec VPN Throughput (512 byte) 1	11,5 Gbps	4,4 Gbps
IPS Throughput (Enterprise Mix) 2	1 Gbps	1 Gbps
NGFW Throughput (Enterprise Mix) 2, 4	-	800 Mbps
Threat Protection Throughput (Ent. Mix) 2, 5	-	600 Mbps
Firewall Latency	-	2.97 µs
Concurrent Sessions	1.5 Million	700000
New Sessions/Sec	56000	35000
Firewall Policies	-	5000
Max G/W to G/W IPSEC Tunnels	200	200
Max Client to G/W IPSEC Tunnels	200	250
SSL VPN Throughput	1 Gbps	490 Mbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	-	200
SSL Inspection Throughput (IPS, avg. HTTPS) 3	1 Gbps	310 Mbps
Application Control Throughput (HTTP 64K) 2	1 Gbps	990 Mbps
Max FortiAPs (Total / Tunnel)	-	16 / 8
Max FortiSwitches	-	8
Max FortiTokens	-	500
Virtual Domains (Default/Max)	-	10 / 10
Interfaces	Possuir ao menos 16x interfaces GE RJ45; Possuir ao menos 2x interfaces 10GE SFP+;	5x GE RJ45
Local Storage	-	-
Power Supplies	-	Single AC PS
Form Factor	-	Desktop
Variants	-	WiFi, 3G4G

Algar Telecom

11. Verifica-se que a solução de Firewall oferecida pela vencedora é insuficiente em diversos pontos, quando comparada às características solicitadas pelo Edital (vide anexo com todas as especificações do FORTGATE 40F).

12. Há que se destacar, que para os itens que demandam a capacidade em tráfego, não serão suportados pelo Firewall FG-40F o tráfego para as VPNs IPSEC, o tráfego para as VPNs SSL e tráfego para controle de aplicação.

13. Ainda, para os volumes de sessões, não serão atendidas as demandas de conexões concorrentes e o de novas sessões por segundo.

14. Em verdade, nota-se que o FG-40F suporta apenas 5 conexões GE de interface RJ45, porém, o termo de referência demanda 16 dessas mesmas interfaces, além de duas interfaces SFP de 10GE.

15. Portanto, por meio da análise da documentação, resta claro que no momento da sessão, a recorrida apresentou equipamento divergente do solicitado, que não atende aos termos e condições do órgão contratante, contrariando o disposto no Memorial Descritivo.

16. Desta feita, não é possível o pregoeiro habilitar e declarar vencedora a licitante que não atendeu aos requisitos do edital e seus anexos, devendo assim, inabilitar e desclassificar a recorrida ante o completo descumprimento das características exigidas com relação à solução apresentada, nos termos do art. 4º, XVI da Lei 10.520/02:

> Art. 4º A fase externa do pregão será iniciada com a convocação dos interessados e observará as seguintes regras:
> (...)
> XVI - se a oferta não for aceitável ou se o licitante desatender às exigências habilitatórias, o pregoeiro examinará as ofertas subseqüentes e a qualificação dos licitantes, na ordem de classificação, e assim sucessivamente, até a apuração de uma que atenda ao edital, sendo o respectivo licitante declarado vencedor;

17. Interpretação contrária afrontaria o basilar Princípio da Vinculação ao Instrumento Convocatório, uma vez que as regras traçadas para o procedimento licitatório devem ser fielmente observadas e atendidas por todos os envolvidos, tanto pela Administração Pública quanto pelas licitantes participantes (art. 3º da Lei nº 8.666/93).

18. Cumpre, assim, dar prevalência ao princípio constitucional da isonomia e bem assim aos princípios da vinculação ao instrumento convocatório e do julgamento objetivo, diante dos fatos, com fulcro no art. 109, § 4º, da Lei nº 8.666/93, é necessário a retratação da decisão que declarou a empresa BEST FIBRA TV ENTRETENIMENTOS E TELECOMUNICAÇÕES LTDA classificada/habilitada.

19. O intuito basilar dos regramentos que orientam as aquisições pela Administração Pública é a contratação da proposta que lhe seja mais vantajosa, obedecidos os princípios básicos da **legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade**, e demais que lhes são correlatos.

20. Nessa linha está o entendimento do TCU-Tribunal de Contas da União, órgão fiscalizador:

> AUSÊNCIA DE **APRESENTAÇÃO** DE DOCUMENTO EXIGIDO EM EDITAL. CONCLUSÃO OBTIDA PELO TRIBUNAL DE ORIGEM. REVISÃO. SÚMULA 7/STJ. 1. O Tribunal de origem **entendeu que a empresa licitante não cumpriu disposição contida no edital** referente à apresentação de declaração em atendimento ao disposto no art. 27, V, da Lei n. 8.666 /93. STJ. Diário 08/09/2014.
>
> Número do Protocolo: 65990/2010. Data de Julgamento: 03-03-2011 EMENTA MANDADO DE SEGURANÇA – LICITAÇÃO – MODALIDADE CONCORRÊNCIA – DESCUMPRIMENTO DE EXIGÊNCIA DO EDITAL – PRINCÍPIO DA VINCULAÇÃO DO ATO CONVOCATÓRIO – ART. 41 DA LEI Nº 8.666/93 – SEGURANÇA DENEGADA. A Administração Pública **somente exerce seu poder discricionário no momento de elaboração do Edital de Licitação, após, ela está vinculada às regras dispostas no Edital, em observância ao Princípio da Vinculação do Ato Convocatório, disposto no artigo 41, da Lei nº 8.666/93, cuja inobservância enseja a inabilitação do concorrente**. Acórdão 11907/2011-Segunda Câmara | Relator: AUGUSTO SHERMAN. TCU

21. Portanto, é imperioso que **seja revisto o ato de declaração de classificada da recorrida, considerando-a como inabilitada para todos os fins de direito, em especial, por descumprimento do Memorial Descritivo, anexo I do Edital, quanto às características exigidas para a solução de Firewall.**

III. PEDIDOS

22. Por todo o exposto, **requer** a Vossa Senhoria que:

i) seja recebido e processado o presente recurso, pois próprio e tempestivo;

ii) que seja reconsiderada a decisão recorrida do pregoeiro que declarou classificada/habilitada/vencedora a empresa BEST FIBRA TV ENTRETENIMENTOS E COMUNICAÇÕES LTDA., sem que esta cumprisse com os requisitos técnicos obrigatórios exigidos no Instrumento Convocatório, em especial o previsto no item 1 do Memorial Descritivo, que exige condições específicas para a solução de Firewall que será utilizada durante a prestação de serviço pela contratada, comprovando o desenquadramento da recorrida, para declará-la inabilitada, e que prossiga o curso do processo convocando o próximo colocado;

Ressalta-se que a interposição do presente recurso administrativo não prejudica a interposição de medida judicial cabível e necessária para resguardar a legalidade do certame, que atualmente encontra-se prejudicada pelas irregularidades apontadas nesse recurso, o qual merece total acolhimento e provimento.

Nestes termos, pede deferimento.

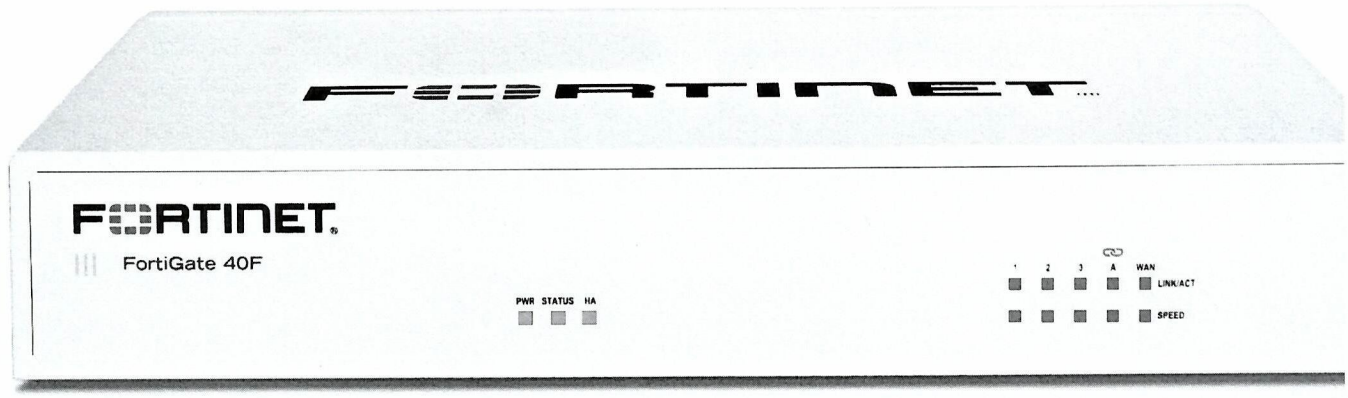
De Uberlândia/MG, para Paulínia/SP, 27 de novembro de 2023.

VOGEL SOLUÇÕES EM TELECOMUNICAÇÕES E INFORMÁTICA S.A

Representante legal

FortiGate FortiWiFi 40F Series

FG-40F, FG-40F-3G4G, FWF-40F, FWF-40F-3G4G



Highlights

Gartner Magic Quadrant Leader for both Network Firewalls and SD-WAN.

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

Unparalleled Performance with Fortinet's patented SoC processors.

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

Simplified Operations with centralized management for networking and security, automation, deep analytics, and self-healing.

Converged Next-Generation Firewall (NGFW) and SD-WAN

The FortiGate Next-Generation Firewall 40F series is ideal for building security-driven networks at distributed enterprise sites and transforming WAN architecture at any scale.

With a rich set of AI/ML-based FortiGuard security services and our integrated Security Fabric platform, the FortiGate FortiWiFi 40F series delivers coordinated, automated, end-to-end threat protection across all use cases.

FortiGate has the industry's first integrated SD-WAN and zero-trust network access (ZTNA) enforcement within an NGFW solution and is powered by one OS. FortiGate 40F automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.

IPS	NGFW	Threat Protection	Interfaces
1 Gbps	800 Mbps	600 Mbps	Multiple GE RJ45 | WiFi variants

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

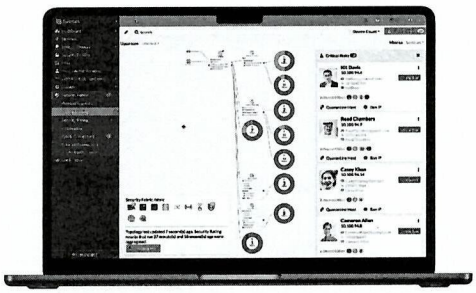
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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 organically built best-of-breed capabilities, unified operating system, and ultra-scalability. The solution allows organizations to protect all edges, simplify operations, and run their business without compromising performance or protection.

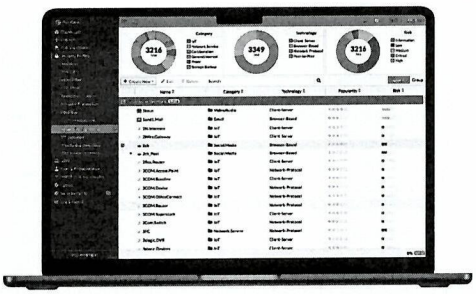
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

FortiOS expands visibility and control, ensures the consistent deployment and enforcement of a simplified, single policy and management framework. Its security policies enable 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.

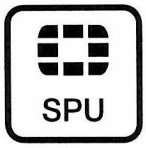
Zero-Day Threat Prevention

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.

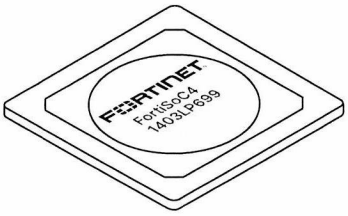
Secure Any Edge at Any Scale



Powered by Security Processing Unit (SPU)

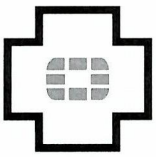
Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

ASIC Advantage



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 IPsec 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



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)

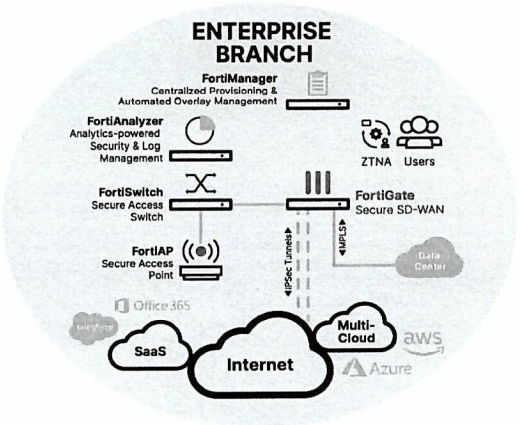
- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications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

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

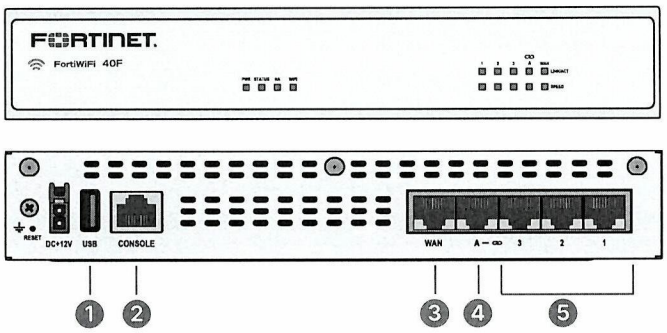
Universal ZTNA

- 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



Hardware

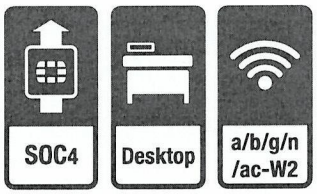
FortiGate FortiWifi 40F Series



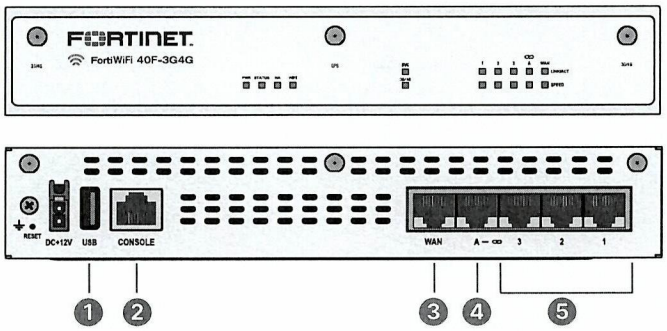
Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x GE RJ45 WAN Port
4. 1 x GE RJ45 FortiLink Port
5. 3 x GE RJ45 Ethernet Ports

Hardware Features



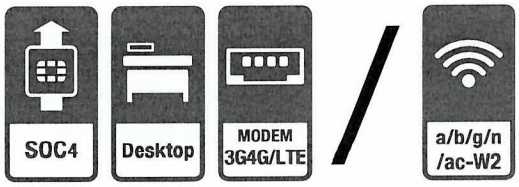
FortiGate FortiWifi 40F-3G4G



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 1 x GE RJ45 WAN Port
4. 1 x GE RJ45 FortiLink Port
5. 3 x GE RJ45 Ethernet Ports

Hardware Features



Compact and Reliable Form Factor

Designed for small environments, you can place it on a desktop or wall-mount it. It is small, lightweight, yet highly reliable with a superior MTBF (Mean Time Between Failure), minimizing the chance of a network disruption.

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 40F	FORTIWIFI 40F	FORTIGATE 40F-3G4G	FORTIWIFI 40F-3G4G
Interfaces and Modules				
Hardware Accelerated GE RJ45 WAN / DMZ Ports	1	1	1	1
Hardware Accelerated GE RJ45 Internal Ports	3	3	3	3
Hardware Accelerated GE RJ45 FortiLink Ports (Default)	1	1	1	1
Hardware Accelerated GE RJ45 PoE/+ Ports	0	0	0	0
Cellular Modem	-	-	3G4G LTE	3G4G LTE
Wireless Interface	0	Single Radio (2.4GHz/5GHz) 802.11 /a/b/g/n/ac-W2	0	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
Antenna Ports (SMA)	0	3	3	6
USB Ports	1	1	1	1
Console Port (RJ45)	1	1	1	1
SIM Slots (Nano SIM)	0	0	2	2
Onboard Storage	0	0	0	0
Included Transceivers	0	0	0	0
System Performance — Enterprise Traffic Mix				
IPS Throughput [2]	1 Gbps			
NGFW Throughput [2, 4]	800 Mbps			
Threat Protection Throughput [2, 5]	600 Mbps			
System Performance and Capacity				
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	5 / 5 / 5 Gbps			
Firewall Latency (64 byte, UDP)	2.97 µs			
Firewall Throughput (Packet per Second)	7.5 Mpps			
Concurrent Sessions (TCP)	700 000			
New Sessions/Second (TCP)	35 000			
Firewall Policies	5000			
IPsec VPN Throughput (512 byte) [1]	4.4 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	250			
SSL-VPN Throughput	490 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200			
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	310 Mbps			
SSL Inspection CPS (IPS, avg. HTTPS) [3]	320			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000			
Application Control Throughput (HTTP 64K) [2]	990 Mbps			
CAPWAP Throughput (HTTP 64K)	3.5 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiSwitches Supported	8			
Maximum Number of FortiAPs (Total / Tunnel)	16 / 8			
Maximum Number of FortiTokens	500			
High Availability Configurations	Active-Active, Active-Passive, Clustering			

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.

Specifications

	FORTIGATE 40F	FORTIWIFI 40F	FORTIGATE 40F-3G4G	FORTIWIFI 40F-3G4G
Dimensions and Power				
Height x Width x Length (inches)	1.5 × 8.5 × 6.3		1.6 × 8.5 × 6.3	
Height x Width x Length (mm)	38.5 × 216 × 160		40.5 × 216 × 160	
Weight	2.2 lbs (1 kg)		2.2 lbs (1 kg)	
Form Factor (supports EIA/non-EIA standards)	Desktop		Desktop	
Input Rating	12Vdc, 3A		12Vdc, 3A	
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz		Powered by external DC power adapter 100-240V AC, 50/60 Hz	
Current (Maximum)	100V AC / 0.2A, 240V AC / 0.1A		100V AC / 0.3A, 240V AC / 0.2A	
Power Consumption (Average / Maximum)	7.74 W / 9.46 W	14.6 W / 16.6 W	15.8 W / 18.6 W	18.6 W / 19.8 W
Heat Dissipation	52.55 BTU/h	56.64 BTU/h	63.5 BTU/h	67.6 BTU/h
Operating Environment and Certifications				
Operating Temperature	32°–104°F (0°–40°C)			
Storage Temperature	-31°–158°F (-35°–70°C)			
Humidity	10%–90% non-condensing			
Noise Level	Fanless 0 dBA			
Operating Altitude	Up to 7400 ft (2250 m)			
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB			
Certifications	USGv6/IPv6			
Radio Specifications				
Multiple (MU) MIMO	N/A	3 × 3	N/A	3 × 3
Maximum Wi-Fi Speeds	N/A	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	N/A	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz
Maximum Tx Power	N/A	20 dBm	N/A	20 dBm
Antenna Gain	N/A	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz	N/A	3.5 dBi @ 5GHz, 5 dBi @ 2.4 GHz
Regional Compatibility				
Regions	N/A		All Regions	
Modem Model	N/A		Sierra Wireless EM7565 (2 SIM Slots, Active/Passive)	
LTE Category	N/A		CAT-12	
LTE Bands	N/A		B1, B2, B3, B4, B5, B7, B8, B9, B12, B13, B18, B19, B20, B26, B28, B29, B30, B32, B41, B42, B43, B46, B48, B66	
UMTS/HSPA+	N/A		B1, B2, B4, B5, B6, B8, B9, B19	
WCDMA	N/A		-	
CDMA 1xRTT/EV-DO Rev A	N/A		-	
GSM/GPRS/EDGE	N/A		-	
Module Certifications	N/A		FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Diversity	N/A		Yes	
MIMO	N/A		Yes	
GNSS Bias	N/A		Yes	

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 [1]	•	•		
	OT Security Service (OT Detection, OT Vulnerability correlation, Virtual Patching, OT Signature / Protocol Decoders) [1]	•			
	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 [2]	•			
NOC and SOC Services	FortiGuard Attack Surface Security Service (IoT Detection, IoT Vulnerability Correlation, and Security Rating Updates) [1]	•	•		
	FortiConverter Service	•	•		
	Managed FortiGate Service	•			
	FortiGate Cloud (SMB Logging + Cloud Management)	•			
	FortiAnalyzer Cloud	•			
	FortiAnalyzer Cloud with SOCaaS	•			
	FortiGuard SOCaaS	•			
Hardware and Software Support	FortiCare Essentials	•			
	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 Elite

FortiCare Elite offers enhanced SLAs and quick issue resolution through a dedicated support team. It provides single-touch ticket handling, extended Extended End-of-Engineering-Support for 18 months, and access to the new FortiCare Elite Portal for a unified view of device and security health.

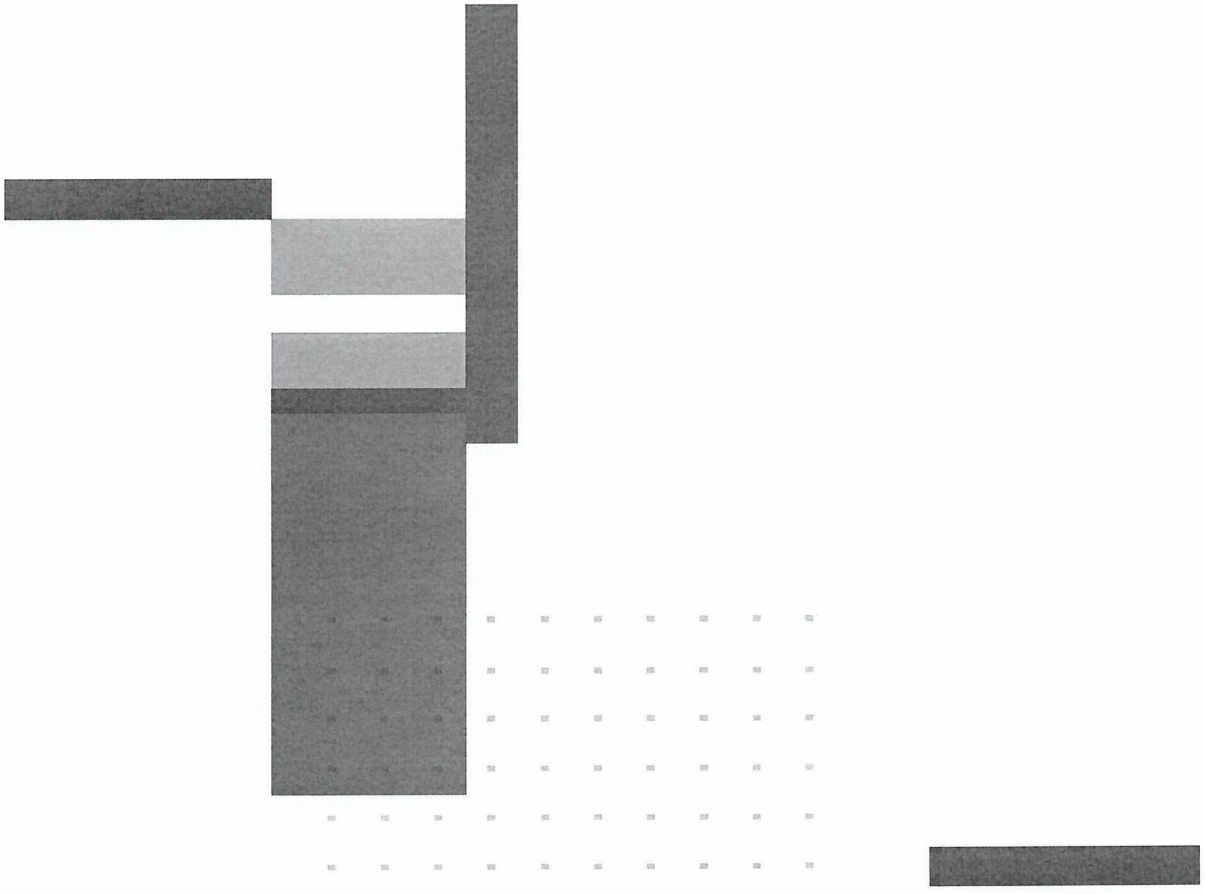
Ordering Information

Product	SKU	Description
FortiGate 40F	FG-40F	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports).
FortiWiFi 40F	FWF-40F-[RC]	5 x GE RJ45 ports (including 4 x Internal Ports, 1 x WAN Ports), Wireless (802.11a/b/g/n/ac-W2).
FortiGate 40F-3G4G	FG-40F-3G4G	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, external SMA WWAN antennas included.
FortiWiFi 40F-3G4G	FWF-40F-3G4G-[RC]	5 x GE RJ45 ports (Including 1 x WAN port, 4 x Switch ports) with Embedded 3G/4G/LTE wireless wan module, Wireless (802.11a/b/g/n/ac-W2), external SMA WWAN and wireless antennas included.
Optional Accessories		
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E series and F series desktop models are backwards compatible with SP-RackTray-01. For list of compatible FortiGate products, visit our Documentation website, docs.fortinet.com
AC Power Adaptor	SP-FG-40F-PA-10(-XX)	Pack of 10 AC power adaptors for FG/FWF-40F, come with interchangeable power plugs. (XX=various countries code).
Wall Mount Kits	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-40F series, FG/FWF-60F series, FG-80F, FG-81F and FG-80F-Bypass.

[RC] = regional code: A, B, D, E, F, I, J, N, P, S, V, and Y

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

October 17, 2023

FGFWF-40F-DAT-R30-20231017