PREGÃO PRESENCIAL Nº 28/2023 ANEXO II
MODELO DE PROPOSTA DE PREÇOS

À ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAÍBA

Proposta para atendimento do objeto destinado a Assembleia Legislativa da Paraíba, em conformidade com o Edital de Pregão Presencial **nº 28/2023**, autorizado pelo Processo Administrativo **nº 3244/2023.**

Para tanto, oferecemos a este Poder Legislativo o preço para o item abaixo, observadas as exigências e especificações de que tratam o **ANEXO I – TERMO DE REFERÊNCIA.**

LOTE	ITEM	Descrição serviço	Qtd	Unidade	Valor Unitário	Valor Total Mensal	Valor Total Anual
02	01	Solução de Segurança de Redes NGFW **TIPO 1** com 60 meses de atualização de firmware, atualização automática bases de dados, suporte e garantia do fabricante. FABRICANTE: FORTINET MODELO: FG-100F Atendendo todos os itens do termo de referência	0 2	Assinatura	R$ 3.045,00	R$ 6.090,00	R$ 73.080,00
	02	Solução de Segurança de Redes NGFW **TIPO 2** com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante. FABRICANTE: FORTINET MODELO: FG-60F Atendendo todos os itens do termo de referência	02	Assinatura	R$ 1.815,00	R$ 3.630,00	R$ 43.560,00
	03	Serviços de solução de controle de acesso a rede (NAC) com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante. FABRICANTE: FORTINET MODELO: FWB-400E Atendendo todos os itens do termo de referência	01	Assinatura	R$ 14.700,00	R$ 14.700,00	R$ 176.400,00
	04	Solução de segurança de aplicações WEB e API - Firewall de Aplicação (WAF) com 60 meses de atualização de firmware, atualização automática bases de dados, suporte e garantia do fabricante. FABRICANTE: FORTINET MODELO: FNC-CA-VM Atendendo todos os itens do termo de referência	01	Assinatura	R$ 2.680,00	R$ 2.680,00	R$ 32.160,00
		VALORES TOTAIS MENSAL E ANUAL DO LOTE II				R$ 27.100,00	R$ 325.200,00

A validade da presente proposta é de 60 (sessenta) dias corridos, contados da sua abertura, observado o disposto no *caput* e parágrafo único do art. 110 da Lei no 8.666/93.

Os preços ofertados já incluem a entrega e retirada dos itens no local determinado.

Informamos, por oportuno, que no preço estão incluídos todos os custos diretos e indiretos para o perfeito fornecimento do objeto, inclusive os encargos da legislação social, trabalhista, previdenciária, englobando tudo o que for necessário para a execução total e completa do objeto licitado, conforme especificações constantes no Edital e seus Anexos.

Os dados da nossa empresa são:

EMPRESA: TELTEC SOLUTIONS LTDA	**CNPJ:** 04.892.991/0001-15	
INSCRIÇÃO ESTADUAL: 254.353.290	**INSCRIÇÃO MUNICIPAL:** 417.510-7	
OPTANTE PELO SIMPLES : NÃO		
ENDEREÇO: RUA MIGUEL DAUX, 100 – COQUEIROS – FLORIANÓPOLIS/SC		
FONE/FAX: (48) 3031-3450 / (65) 98126-6811		
E-MAIL: teltec@teltecsolutions.com.br / ana@teltecsolutions.com.br	**SITE:** www.teltecsolutions.com.br	
DADOS BANCARIOS		
BANCO: BRASIL	**AGÊNCIA: 3077-5**	**CONTA:** 7555-8

04 892 991/0001-15
TELTEC SOLUTIONS LTDA
Rua: Miguel Daux, 100
COQUEIROS - CEP 88080-220
FLORIANÓPOLIS - SC

Declaramos, para todos os fins, que o fornecimento do objeto se dará de acordo com as especificações definidas nesta proposta e respeitando o estabelecido no Edital e seus Anexos.

João Pessoa, 12 de dezembro de 2023.

Lucas Silvino da Silva
RG 2509339 SSP/PB CPF 051.748.624-52

PREGÃO PRESENCIAL Nº 28/2023 ANEXO II
MODELO DE PROPOSTA DE PREÇOS

À ASSEMBLEIA LEGISLATIVA DO ESTADO DA PARAÍBA

Proposta para atendimento do objeto destinado a Assembleia Legislativa da Paraíba, em conformidade com o Edital de Pregão Presencial **nº 28/2023**, autorizado pelo Processo Administrativo **nº 3244/2023.**

Para tanto, oferecemos a este Poder Legislativo o preço para o item abaixo, observadas as exigências e especificações de que tratam o **ANEXO I – TERMO DE REFERÊNCIA.**

LOTE	ITEM	Descrição serviço	Qtd	Unidade	Valor Unitário	Valor Total Mensal	Valor Total Anual
02	01	Solução de Segurança de Redes NGFW **TIPO 1** com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante. FABRICANTE: FORTINET MODELO: FG-100F Atendendo todos os itens do termo de referência	0 2	Assinatura	R$ 11.000,00	R$ 22.000,00	R$ 264.000,00
	02	Solução de Segurança de Redes NGFW **TIPO 2** com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante. FABRICANTE: FORTINET MODELO: FG-60F Atendendo todos os itens do termo de referência	02	Assinatura	R$ 6.000,00	R$ 12.000,00	R$ 144.000,00
	03	Serviços de solução de controle de acesso a rede (NAC) com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante. FABRICANTE: FORTINET MODELO: FWB-400E Atendendo todos os itens do termo de referência	01	Assinatura	R$ 16.000,00	R$ 16.000,00	R$ 192.000,00
	04	Solução de segurança de aplicações WEB e API - Firewall de Aplicação (WAF) com 60 meses de atualização de firmware, atualização automática de bases de dados, suporte e garantia do fabricante. FABRICANTE: FORTINET MODELO: FNC-CA-VM Atendendo todos os itens do termo de referência	01	Assinatura	R$ 3.500,00	R$ 3.500,00	R$ 42.000,00
	VALORES TOTAIS MENSAL E ANUAL DO LOTE II					R$ 53.500,00	R$ 642.000,00

A validade da presente proposta é de 60 (sessenta) dias corridos, contados da sua abertura, observado o disposto no *caput* e parágrafo único do art. 110 da Lei no 8.666/93.

Os preços ofertados já incluem a entrega e retirada dos itens no local determinado.

Informamos, por oportuno, que no preço estão incluídos todos os custos diretos e indiretos para o perfeito fornecimento do objeto, inclusive os encargos da legislação social, trabalhista, previdenciária, englobando tudo o que for necessário para a execução total e completa do objeto licitado, conforme especificações constantes no Edital e seus Anexos.

Os dados da nossa empresa são:

EMPRESA: TELTEC SOLUTIONS LTDA	**CNPJ:** 04.892.991/0001-15	
INSCRIÇÃO ESTADUAL: 254.353.290	**INSCRIÇÃO MUNICIPAL:** 417.510-7	
OPTANTE PELO SIMPLES : NÃO		
ENDEREÇO: RUA MIGUEL DAUX, 100 – COQUEIROS – FLORIANÓPOLIS/SC		
FONE/FAX: (48) 3031-3450 / (65) 98126-6811		
E-MAIL: [redacted]	**SITE:** [redacted]	
DADOS BANCARIOS		
BANCO: BRASIL	**AGÊNCIA: 3077-5**	**CONTA:** 7555-8

04 892 991/0001-15

TELTEC SOLUTIONS LTDA

Rua: Miguel Daux, 100

COQUEIROS - CEP 88080-220
FLORIANÓPOLIS - SC

Declaramos, para todos os fins, que o fornecimento do objeto se dará de acordo com as especificações definidas nesta proposta e respeitando o estabelecido no Edital e seus Anexos.

João Pessoa, 12 de dezembro de 2023.

Lucas Silvino da Silva

Lucas Silvino da Silva
RG 2509339 SSP/PB CPF 051.748.624-52

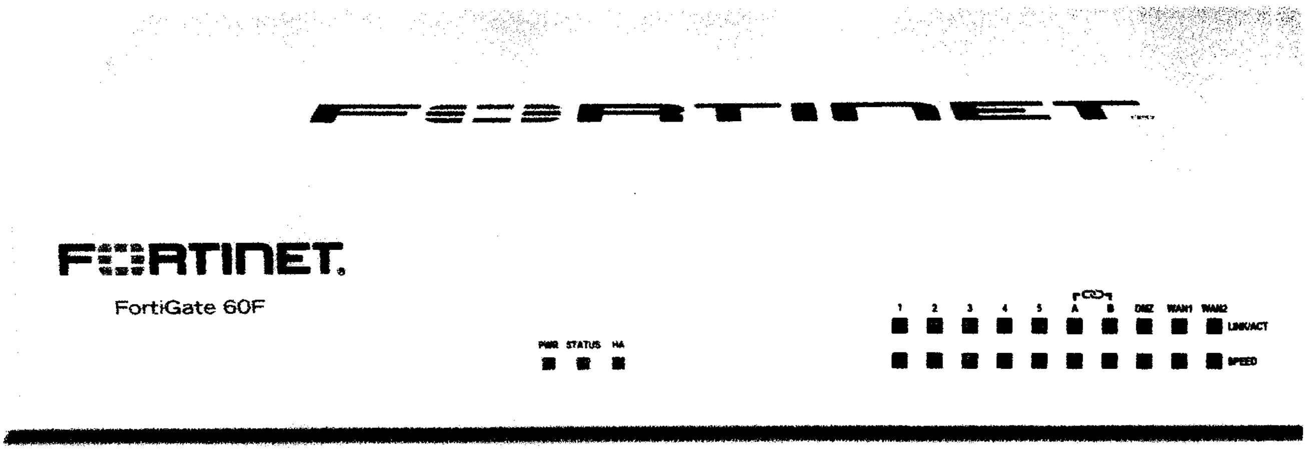
FORTINET

Data Sheet

FortiGate FortiWiFi 60F Series

FG-60F, FG-61F, FWF-60F, and FWF-61F

[redacted]



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 60F 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 60F 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 FortiWiFi 60F automatically controls, verifies, and facilitates user access to applications, delivering consistency with a seamless and optimized user experience.

IPS	NGFW	Threat Protection	Interfaces
1.4 Gbps	1 Gbps	700 Mbps	Multiple GE RJ45 | Variants with internal storage | WiFi variants

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

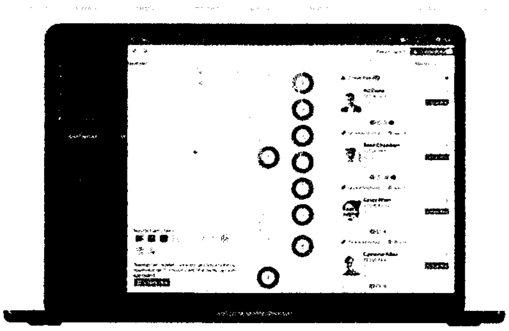
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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.

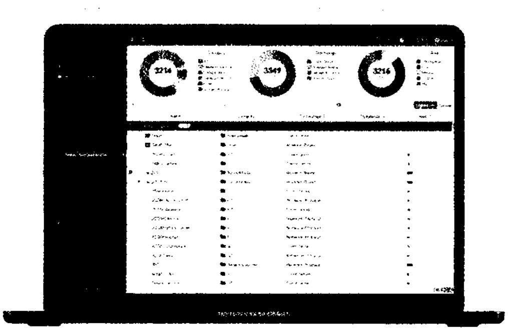
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more. It provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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.

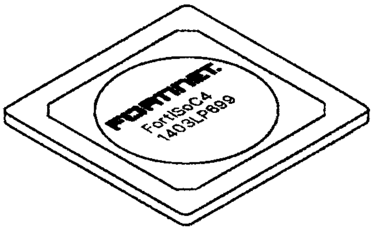
Secure Any Edge at Any Scale

SPU

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)

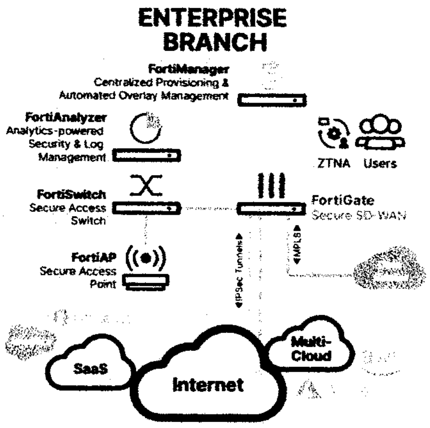
- FortiGuard Labs' suite of AI-powered Security Services—natively integrated with your NGFW—secures web, content, and devices and protects networks from ransomware and sophisticated cyberattacks
- Real-time SSL inspection (including TLS 1.3) provides full visibility into users, devices, and applications 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

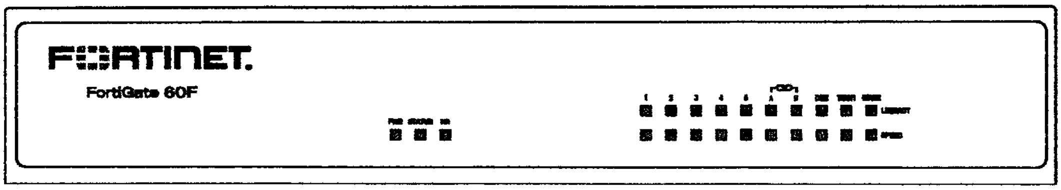
Universal ZTNA

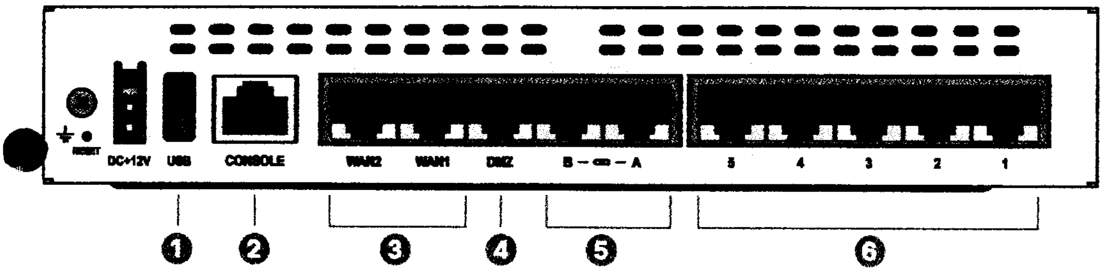
- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access - every time
- Agent-based access with FortiClient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



Hardware

FortiGate FortiWiFi 60F/61F

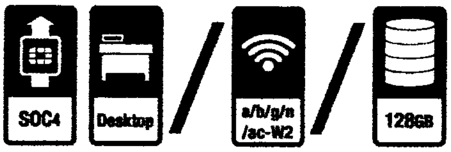




Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 WAN Ports
4. 1 x GE RJ45 DMZ Port
5. 2 x GE RJ45 FortiLink Ports
6. 5 x GE RJ45 Internal 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 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Hardware Specifications				
GE RJ45 WAN / DMZ Ports	2 / 1	2 / 1	2 / 1	2 / 1
GE RJ45 Internal Ports	5	5	5	5
GE RJ45 FortiLink Ports (Default)	2	2	2	2
Wireless Interface	–	–	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2	Single Radio (2.4GHz/5GHz), 802.11 a/b/g/n/ac-W2
USB Ports	1	1	1	1
Console (RJ45)	1	1	1	1
Internal Storage	–	1 × 128 GB SSD	–	1 × 128 GB SSD
System Performance — Enterprise Traffic Mix				
IPS Throughput [2]	1.4 Gbps			
NGFW Throughput [2, 4]	1 Gbps			
Threat Protection Throughput [2, 5]	700 Mbps			
System Performance				
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	10/10/6 Gbps			
Firewall Latency (64 byte UDP packets)	3.3 μs			
Firewall Throughput (Packets Per Second)	9 Mpps			
Concurrent Sessions (TCP)	700 000			
New Sessions/Second (TCP)	35 000			
Firewall Policies	5000			
IPsec VPN Throughput (512 byte) [1]	6.5 Gbps			
Gateway-to-Gateway IPsec VPN Tunnels	200			
Client-to-Gateway IPsec VPN Tunnels	500			
SSL-VPN Throughput	900 Mbps			
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200			
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	630 Mbps			
SSL Inspection CPS (IPS, avg. HTTPS) [3]	400			
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	55 000			
Application Control Throughput (HTTP 64K) [2]	1.8 Gbps			
CAPWAP Throughput (HTTP 64K)	8 Gbps			
Virtual Domains (Default / Maximum)	10 / 10			
Maximum Number of FortiSwitches Supported	24			
Maximum Number of FortiAPs (Total / Tunnel Mode)	64 / 32			
Maximum Number of FortiTokens	500			
High Availability Configurations	Active-Active, Active-Passive, Clustering			
Dimensions				
Height x Width x Length (inches)	1.5 × 8.5 × 6.3			
Height x Width x Length (mm)	38.5 × 216 × 160 mm			
Weight	2.23 lbs (1.01 kg)			
Form Factor	Desktop			
Radio Specifications				
Multiple User (MU) MIMO	–	–	3×3	
Maximum Wi-Fi Speeds	–	–	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	
Maximum Tx Power	–	–	20 dBm	
Antenna Gain	–	–	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz	

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 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Operating Environment and Certifications				
Power Rating	12Vdc, 3A			
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz			
Maximum Current	100Vac/1.0A, 240Vac/0.6A			
Power Consumption (Average / Maximum)	10.17 W / 12.43 W	17.2 W / 18.7 W	17.2 W / 18.7 W	17.5 W / 19.0 W
Heat Dissipation	42.4 BTU/hr	42.4 BTU/hr	63.8 BTU/hr	64.8 BTU/hr
Operating Temperature	32°–104°F (0°–40°C)			
Storage Temperature	-31°–158°F (-35°–70°C)			
Humidity	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			

Subscriptions

			Bundles		
Service Category	**Service Offering**	**A-la-carte**	**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**		included with FortiCare Subscription		
	GeoIP DB Updates				
	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 60F	FG-60F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port)
FortiGate 61F	FG-61F	10x GE RJ45 ports (including 7x Internal ports, 2x WAN ports, 1x DMZ port), 128 GB SSD onboard storage
FortiWiFi 60F	FWF-60F-[RC]	10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2)
FortiWiFi 61F	FWF-61F-[RC]	10x GE RJ45 ports (including 7x Internal Ports, 2x WAN Ports, 1x DMZ Port), Wireless (802.11 a/b/g/n/ac-W2), 128GB SSD onboard storage
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-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, and 80E/81E
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-60F and FG/FWF-80F series

[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.

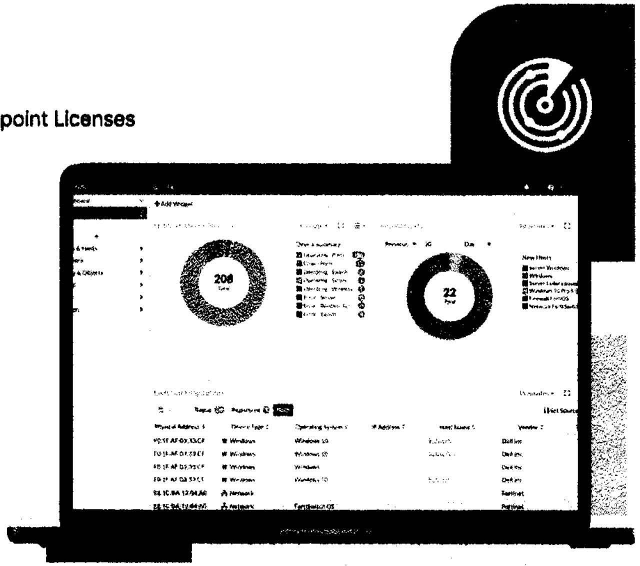
www.fortinet.com

October 17, 2023

FGFWF-60F-DAT-R37-20231017

FortiNAC

FortiNAC F Series Hardware, VM, and Endpoint Licenses



Highlights

- Implement dynamic network scanning to classify and analyze device behaviors using continuous, automated techniques
- Maintain an updated inventory of all network devices, including BYOD, IoT, OT, and IoMT
- Continuously assess risks for every endpoint using real-time threat intelligence and behavioral patterns
- Adopt Zero Trust architecture for better device security and simplified management
- Integrate with various third-party network tools ensuring compatibility
- Relay real-time contextual data to SIEM, improving incident response. Ensure always-on identity checks and follow least privilege access, reinforcing the Zero Trust approach

Visibility, Zero Trust Access and Incident Response for Connected Assets and Users

FortiNAC™ continues to be a cutting-edge network access control solution, enabling organizations to enforce network access policies and assure adherence to security protocols in light of increasingly sophisticated threats. It provides a comprehensive snapshot of all devices and users on the network, facilitating granular control of access based on user roles, device types, network locations, and now the behavioral patterns of devices and users.

The solution's capability now extends beyond automated onboarding of new endpoints; it incorporates real-time threat intelligence and continuous risk assessment of devices, leveraging machine learning and AI technologies from FortiGuard Services. Given the rising prominence of BYOD (Bring Your Own Device) and IoT (Internet of Things), FortiNAC's continuous monitoring and immediate remediation of non-compliant devices have become even more crucial.

Moreover, FortiNAC's integration goes beyond third-party security solutions; it integrates with a wide range of cloud-based platforms and DevOps tools to ensure seamless and secure network operations in hybrid IT environments. FortiNAC leverages its integration with FortiAnalyzer to gain deep insight into network security posture, encompassing real-time visibility, predictive analytics, and more robust compliance reporting. With FortiNAC, organizations can more effectively secure their network against unauthorized access, potential threats, and increasingly, the insider threats, aligning with the emerging Zero Trust security model that emphasizes "never trust, always verify".

Available in

Appliance

Virtual

Features

Granular Visibility Across the Network for Every Device and User

FortiNAC leverages AI and machine learning from FortiGuard Security Services to provide detailed profiling of devices, including headless devices and IoT assets on your network. This profiling incorporates multiple information sources, behavior patterns, and real-time threat intelligence to accurately identify and assess what is on your network.

Seamless Integration and Control Across Diverse Environments

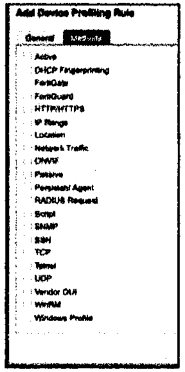
With the power of micro-segmentation and Zero Trust policies, FortiNAC allows for configuration changes on switches and wireless products from an extended range of vendors. It amplifies the reach of the Security Fabric across multi-cloud, hybrid IT, and heterogeneous environments, implementing "never trust, always verify' principles.

Automated Responsiveness

FortiNAC reacts to network events in real-time to contain threats before they spread, utilizing a broad and customizable set of automation policies. Leveraging AI, these policies can instantly trigger configuration changes and remediation actions when targeted behavior or anomalies are observed, aligning with the Zero Trust model's dynamic and proactive approach.

New FortiNAC-F

FortiNAC introduces the new FortiNAC-F OS with hardened virtual and physical appliances that increase security and compliance capabilities. Following the tradition of providing the reliable platforms of Fortinet, the new FortiNAC-F will extend the performance capability and introduce new features.



Add Device Profiling Rule

General | Methods

- Active
- DHCP Fingerprinting
- FortiGate
- FortiGuard
- HTTP/HTTPS
- IP Range
- Location
- Network Traffic
- ONVIF
- Passive
- Persistent Agent
- RADIUS Request
- Script
- SNMP
- SSH
- TCP
- Telnet
- UDP
- Vendor OUI
- WinRM
- Windows Profile

FortiNAC 21 Profiling Methods for Device Classification

Highlights

Granular Device Visibility

The essence of securing a dynamic, ever-evolving network lies in comprehending its makeup. FortiNAC leverages AI and machine learning from FortiGuard Security Services, goes beyond merely "seeing" everything on the network—it comprehends and analyzes. It scans your network to discover every user, application, and device. Using a variety of techniques—it profiles each element based on observed behavior, real-time threat intelligence, as well as tapping into FortiGuard's IoT Services, a cloud-based database for identification lookups.

Scanning can be active or passive, utilizing permanent agents, dissolvable agents, or agentless approaches. Moreover, FortiNAC can evaluate a device against pre-approved profiles, noting any discrepancies or software updates required to patch vulnerabilities. With FortiNAC, the network isn't just known—it's understood, assessed, and continually monitored.

Besides recognizing the entire network, FortiNAC's advanced visibility incorporates passive traffic analysis, leveraging Fortinet FortiGate appliances as sensors to identify anomalous behavior patterns. These patterns can indicate a potential compromise, triggering real-time alerts for the SOC team and aligning with the proactive threat containment approach integral to the Zero Trust model.

Highlights

Network Security and Intelligent Segmentation

After successful classification of devices and user identification, FortiNAC now integrates advanced segmentation techniques to ensure only authorized users and devices have access to requisite resources, thus preventing unauthorized intrusion. Through its progressive role-based network access control, FortiNAC allows for strategic network segmentation by logically grouping similar data and applications, limiting access to a particular set of users or devices. This strategy effectively confines a compromised device, thereby inhibiting its ability to traverse the network and inflict damage on other resources. FortiNAC not only fortifies the protection of sensitive data and vital assets but also ensures adherence to internal, industrial, and government regulations and mandates.

Device Integrity Verification and Malware Prevention

FortiNAC emphasizes on the importance of device integrity prior to network connection, significantly reducing the risk and potential spread of malicious software. As a device attempts to join the network, FortiNAC assesses its configuration for compliance. Any non-compliant configuration is promptly managed; for instance, the device may be allocated to an isolated or restricted access VLAN, devoid of any access to corporate resources. This feature has become increasingly relevant with the rise of IoT devices and remote work trends, ensuring a secure and controlled network environment.

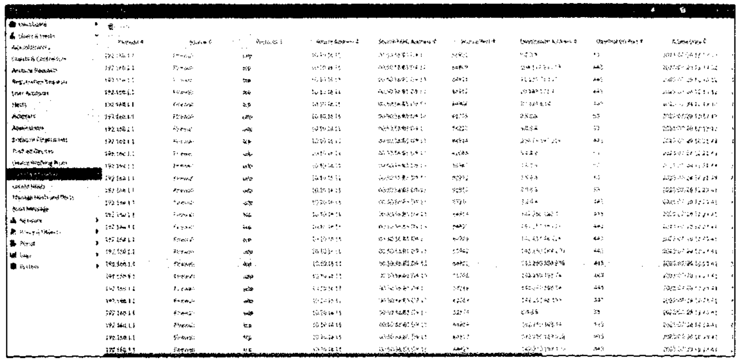
Intelligent Monitoring and Automated Reaction

FortiNAC proactively supervises the network continuously, examining endpoints to verify their compliance with predefined profiles. Leveraging modern security tactics, FortiNAC rescreens devices to prevent any possible bypassing of network access security via MAC-address spoofing. Further, FortiNAC is equipped to identify irregularities in traffic patterns, a vital feature considering the growing complexities in network usage patterns with the rise of cloud and edge computing. This passive anomaly detection function operates symbiotically with FortiGate appliances. Upon recognizing a compromised or susceptible endpoint as a potential risk, FortiNAC promptly instigates an automated reaction, quarantining the endpoint in real-time, furthering its commitment to maintaining a secure and controlled network environment.

Highlights

FortiGate Sessions View

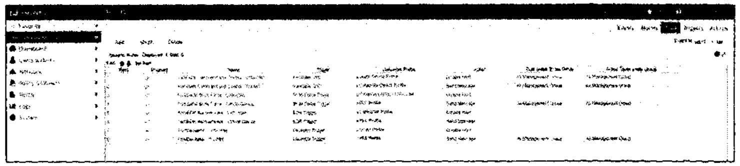
The FortiGate Sessions view adds the ability to accept netflow data from third party devices. Flows from other devices would also show up in this view.



FortiNAC 21 Profiling Methods for Device Classification

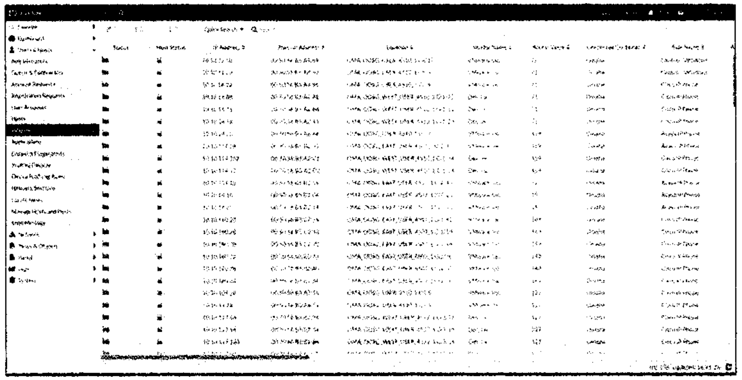
Security Fabric Integrations

FortiNAC integrates with multiple Fortinet products such as FortiGate, FortiSIEM, FortiAnalyzer, FortiEDR, and FortiDeceptor. The Security Rules are triggered by syslog/snmp messages from the other Fortinet products as shown below.

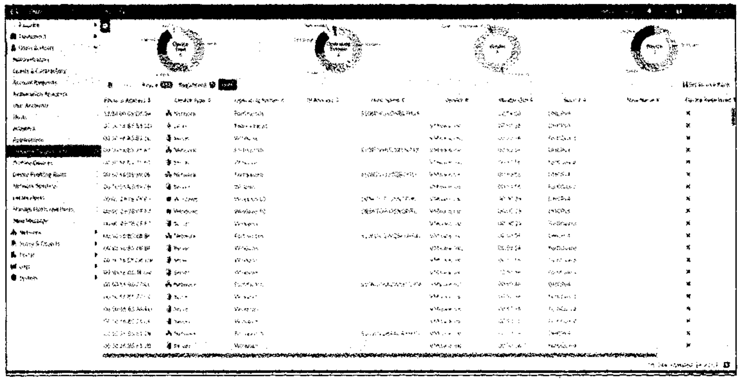


FortiNAC Security Rules

Integration



FortiNAC Adapter View



FortiNAC New Endpoint Fingerprints View

Integration

Extensive integration with desktop security software, directories, network infrastructure, and third-party security systems provides unparalleled visibility and control across the network environment.

The FortiNAC family integrates

- More than 3000 devices with unique MIB OIDs
- More than 2000 models including switches, access points, and network controllers
- More than 90 vendors in networking, security, and communication industries

with the following vendor and models as examples*.

Network Infrastructure	Adtran, Aerohive, AlaxalA Networks, Alcatel-Lucent, Allied Telesis, Alteon, APC, Apple, APRESIA Systems, Avaya, Brocade/Foundry Networks/Ruckus, Cisco/Meraki, D-Link, Extreme/Enterasys/Siemens, H3C, HP/Colubris/3Com/Aruba, Intel, Juniper, NEC, Riverbed/Xirrus, and SonicWall
Security Infrastructure	CheckPoint, Cisco/SourceFire, Cyphort, FireEye, Juniper/Netscreen, Qualys, Sonicwall, Tenable
Authentication and Directory Services	RADIUS — Cisco ACS, Free RADIUS, Microsoft IAS, LDAP — Google SSO, Microsoft Active Directory, OpenLDAP
Operating Systems	Android, Apple MAC OSX and iOS, Linux, Microsoft Windows
Endpoint Security Applications	Authentium, Avast, AVG, Avira, Blink, Bullguard, CA, ClamAV, Dr. Web, Enigma, ESET, F-Prot, F-Secure, G Data, Intego, Javacool, Lavasoft, Lightspeed, McAfee, Microsoft, MicroWorld, Norman, Norton, Panda, PC Tools, Rising, Softwin, Sophos, Spyware Bot, Sunbelt, Symantec, Trend Micro, Vexira, Webroot SpySweeper, Zone Alarm
Mobile Device Management	AirWatch, Google GSuite, MaaS360, Microsoft InTune, Mobile Iron, XenMobile, JAMF, Nozomi Networks

* FortiNAC can be integrated with other vendors and technologies in addition to those listed here. This list represents integrations that have been validated in both test lab and production network environments.

TR

ASSEMBLEIA LEGISLATIVA PARAÍBA C.P.L.

Deployment Options

Easy Deployment

FortiNAC is a flexible and scalable solution that spans from mid-size to very large enterprise deployments. There are three elements to the FortiNAC solution.

- Application and Control (required)
- Management (optional)
- FortiAnalyzer for Reports (optional)

The Application provides the visibility, and the Control provides the configuration capabilities and automated responsiveness features. The Management portion enables the sharing of concurrent users across a multi-server deployment. FortiAnalyzer provides reports and analytics based on the information gathered from the network through FortiNAC.

FortiNAC can be deployed in virtual machines (VMWare/Hyper-V/ AWS/ Azure/ KVM) or on hardware appliances. The Application and Control Servers can be deployed in a variety of sizes, depending on the number of ports they need to support. FortiNAC is ideal for support distributed architectures, including SD-Branch locations.

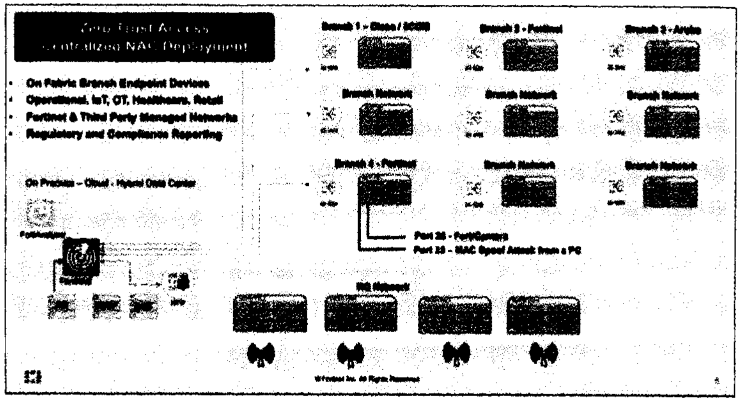
High Availability

FortiNAC offers High Availability for disaster recovery to ensure redundancy. This state is achieved through active and passive instances where the passive (backup) becomes active when the main is no longer functioning normally. FortiNAC Manager can manage multiple high availability clusters distributed throughout the network as needed.

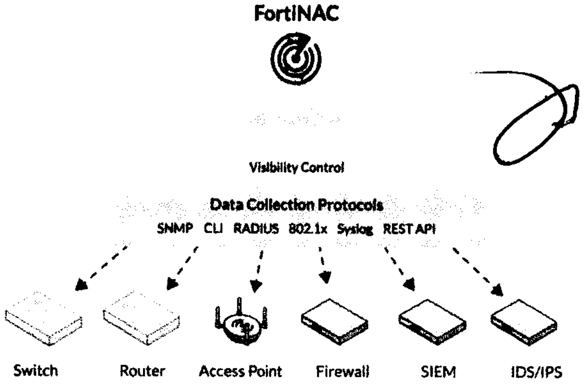
Deployment Options

Centralized Architecture

FortiNAC is an 'out of band' solution, meaning it does not sit in-line of user traffic. This architecture allows FortiNAC to be deployed centrally and manage many remote locations. Visibility, control, and response are achieved by integrating with, and leveraging the capabilities of, the network infrastructure. Control can be applied at the point of connection, at the very edge of the network while security device integrations allow FortiNAC to process security alerts and treat them as triggers for automated threat mitigation through customizable work flows.


Zero Trust Access
Centralized NAC Deployment
On Fabric Branch Endpoint Devices
Operational, IoT, OT, Healthcare, Retail
Fortinet & Third Party Managed Networks
Regulatory and Compliance Reporting
Branch 2 - Fortinet
Branch 3 - Aruba
Branch Network
Branch Network
Branch Network
Branch 4 - Fortinet
Branch Network
Branch Network
On Premise - Cloud - Hybrid Data Center
Port 15 - MAC Spoof Attack from a PC
HQ Network
© Fortinet Inc. All Rights Reserved

Data collection is gathered from multiple sources using a variety of methods. SNMP, CLI, RADIUS, SYSLOG, API and DHCP fingerprints can all be used to achieve the detailed end-to-end visibility necessary to create a truly secure environment.



Licensing

FortiNAC Licensing

FortiNAC offers flexible deployment options based on the level of coverage and functionality desired.

Base License

The BASE license level provides easy, one-step IoT security solution to close pressing endpoint security gaps by seeing all endpoint devices on the network, automating authorization, and enabling micro-segmentation and network lockdown. The BASE license level is appropriate for organizations that need to secure IoT and headless devices, and enable network lockdown with dynamic VLAN steering, but do not require more advanced user/network controls or automated threat response.

Plus License

The PLUS license level builds on all the functionality of BASE with enhanced visibility and more advanced Network Access Controls and automated provisioning for users, guests, and devices as well as reporting and analytics. The reporting and analytics can greatly assist in providing audit documentation of compliance. The PLUS license level is appropriate for organizations that want complete endpoint visibility and a granular control, but do not require automated threat response.

Pro License

The PRO license level provides the ultimate in visibility, control and response. PRO license offers real-time endpoint visibility, comprehensive access control, and automated threat response and delivers contextual information with triaged alerts. The PRO license level is appropriate for organizations that want complete endpoint visibility, a flexible NAC solution with granular controls, as well as accurate event triage and real-time automated threat response.

Licensing

		FORTINAC LICENSE TYPES	BASE	PLUS	PRO
Visibility	Network	Network Discovery	✓	✓	✓
		Rogue Identification	✓	✓	✓
		Device Profiling and Classification	✓	✓	✓
	Endpoint	Enhanced Visibility	✓	✓	✓
		Anomaly Detection	✓	✓	✓
		MDM Integration	✓	✓	✓
		Persistent Agent	✓	✓	✓
	User	Authentication		✓	✓
		Captive Portal		✓	✓
Automation / Control		Network Access Policies	✓	✓	✓
		IoT Onboarding with Sponsor	✓	✓	✓
		Rogue Device Detection and Restriction	✓	✓	✓
		Firewall Segmentation	✓	✓	✓
		MAC Address Bypass (MAB)	✓	✓	✓
		Full RADIUS (EAP)	✓	✓	✓
		BYOD / Onboarding		✓	✓
		Guest Management		✓	✓
		Endpoint Compliance		✓	✓
		Web and Firewall Single Sign-on	✓	✓	✓
Incident Response		Event Correlation			✓
		Extensible Actions and Audit Trail			✓
		Alert Criticality and Routing			✓
		Guided Triage Workflows			✓
Integrations		Inbound Security Events			✓
		Outbound Security Events	✓	✓	✓
		REST API	✓	✓	✓
Reporting		Customizable Reports	✓	✓	✓

Services

FortiCare Services

As your business rapidly evolves, it is critical to advance your security capabilities as well. Often though, you do not have expertise within your organization to deploy, operate, and maintain these new capabilities or are up against tight deadlines to implement change. We understand this challenge and help thousands of organizations every year tackle this problem with FortiCare Services.

Our experts provide accelerated implementation of your technology, reliable assistance through advanced support, and proactive care to ensure your success with Fortinet investment. No matter the size or location of your organization, we are ready to provide you with an elevated experience to help you achieve your business goals with superior security and performance.

FortiCare Support

A FortiCare Support contract entitles you not only to receive updates to the FortiNAC firmware, but also receive two important feeds.

1. Network device database update FortiNAC supports more than 2500 switching, wireless, or firewall devices on the market. As new devices are released, FortiNAC's network device database should be updated to reflect these new models. The weekly update from the FortiNAC team will keep your deployment up to date.
2. FortiGuard IoT Service. One of the means that FortiNAC has to identify devices is to use the cloud-look up service hosted by FortiGuard Labs. A FortiCare Support contract entitles you to use that service at no additional cost, giving you access to a database of millions of devices.

Specifications

	FNC-M-550F	FNC-CA-600F	FNC-CA-500F
System			
CPU	AMD EPYC 7413 24 Core, 2.65GHz Base Freq.		Intel Xeon E-2278GE 8 Core 3.3GHz Base Freq.
Memory	32GB DDR4 memory		16GB DDR4 memory
Hard Disk	2× 960GB SSDs		2× 960GB SSDs
BMC	N/A		N/A
Network Interface	1x GbE RJ45 and 4× 10GbE SFP+		4x GbE RJ45
RAID Card	N/A		N/A
RAID Configuration	Software RAID1		
Console Access	RJ45 type COM port for CLI		
Form Factor	1U Rack Mount		
Dimensions			
Height x Width x Length (inches)	1.73" x 17.20" x 24"		1.73" x 17.32" x 19.69"
Height x Width x Length (mm)	44 × 437 × 610		44 × 440 × 500
Weight	41 lbs (18.6 kg)		32 lbs (14.51 kg)
Environment			
Power Supply	Hot Plug, 1+1 Redundant PSU		Hot Plug, 1+1 Redundant PSU
Input Power	225 watt		174 Watt
Input Current	2.3A@100V, 0.94A@240V		1.5A@100V; 0.625A@240V
Cooling	5x system fans		4x system fans
Panel Display	N/A		N/A
Heat Dissipation	767.731867425 BTU/h		511.82124495 BTU/h
Operation Temperature Range	32°-104°F (0°-40°C)		32°-104°F (0°-40°C)
Storage Temperature Range	-4°-158°F (-20°-70°C)		-4°-158°F (-20°-70°C)
Humidity (Operating) **Humidity (Non-operating)**	5% to 90% non-condensing		5% to 90% non-condensing
Certification			
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), and European Union (CE).		
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), and European Union (CE).		
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).		

* The console port can be used for access if the appliance has an issue i.e. you can connect a monitor and a keyboard to it. FortiNAC does not use the console port for access

Specifications

	FNC-CA-700F
System	
CPU	AMD EPYC 7543P 32 Core, 2.8GHz Base Freq.
Memory	96GB DDR4 memory
Hard Disk	2× 960GB SSDs
BMC	N/A
Network Interface	1x GbE RJ45 and 4× 10GbE SFP+
RAID Card	N/A
RAID Configuration	Software RAID1
Console Access	RJ45 type COM port for CLI
Form Factor	1U Rack Mount
Dimensions	
Height x Width x Length (inches)	1.73 × 17.20 × 24
Height x Width x Length (mm)	44 × 437 × 610
Weight	41 lbs (18.6 kg)
Environment	
Power Supply	Hot Plug, 1+1 Redundant PSU
Input Power	375 Watt
Input Current	3.75A@100V, 1.57A@240V
Cooling	5x system fans
Panel Display	N/A
Heat Dissipation	1279.553112375 BTU/h
Operation Temperature Range	32°-104°F (0°-40°C)
Storage Temperature Range	-4°-158°F (-20°-70°C)
Humidity (Operating) **Humidity (Non-operating)**	5% to 90% non-condensing
Certification	
Safety	Certified as applicable by Product Safety authorities worldwide, including United States (NRTL), Canada (SCC), and European Union (CE).
Electromagnetic (EMC)	Certified as applicable by EMC authorities worldwide, including United States (FCC), Canada (ICES), and European Union (CE).
Materials	Certified as applicable by Materials authorities worldwide, including European Union (ROHS) and China (ROHS).

* The console port can be used for access if the appliance has an issue i.e. you can connect a monitor and a keyboard to it. FortiNAC does not use the console port for access.

Hardware Server Sizing

Appliance

HARDWARE			
Hardware Server	**Type**	**Target Environment**	**Capacity**[1]
FortiNAC-CA-500F	Standalone Appliance (Integrated Control Server and Application Server)	Small Environments	Manages up to 5000 ports in the network
FortiNAC-CA-600F	High Performance Control and Application Server	Medium Environments	Manages up to 15 000 ports in the network
FortiNAC-CA-700F	Ultra High Performance Control and Application Server	Large Environments with few Persistent Agents	Manages up to 25 000 ports in the network
FortiNAC-M-550F	Management Appliance (Provides centralized management when multiple appliances are deployed)	Multi-site environments with multiple appliances	Can manage up to 50 CA servers with latencies up to 600ms in lab environment

1 Ports in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total port counts not total number of devices.

VM Server Resource Sizing

Virtual

VIRTUAL MACHINE							
VM OS	**SKU**	**Ports in the Network**[1]	**Target Environment**	**CPU Reference**	**vCPU Qty**[2]	**Memory (GB)**	**Disk (GB)**
FortiNAC-OS		Up to 5 000	Small	Intel Xeon E-2278 GE 3.3 GHz 8C/16T	8	16	100
	FNC-CAX-VM	Up to 15 000	Medium	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100
		Up to 25 000	Large	AMD Milan EPYC 7543P 2.8 GHz 32C/64T	32	96	100
	FNC-MX-VM	Up to 50 CA Servers	Large	AMD Milan EPYC 7413 2.65 GHz 24C/48T	24	32	100

[1] Ports in the network = total number of switch ports + maximum number of concurrent wireless connections. FortiNAC sizes the appliance capacity based on total ports count, not total number of devices.

[2] The values in the vCPU column were determined by using the CPUs in the CPU reference column and are guidelines only. VM resources may vary based on individual environments.

Ordering Information

PRODUCT	SKU	DESCRIPTION
Appliances		
FortiNAC-CA-500F	FNC-CA-500F	FortiNAC Network Control and Application Server (F Series)
FortiNAC-CA-600F	FNC-CA-600F	FortiNAC High Performance Network Control and Application Server (F Series)
FortiNAC-CA-700F	FNC-CA-700F	FortiNAC Ultra High Performance Network Control and Application Server (F Series)
FortiNAC-M-550F	FNC-M-550F	FortiNAC Network Manager (F Series)
Virtual Machines		
FortiNAC Control and Application extended VM	FNC-CAX-VM	FortiNAC Control and Application eXtended VM Server (VMWare or Hyper-V or AWS or Azure or KVM) (Running FortiNAC-OS)
FortiNAC Manager extended VM	FNC-MX-VM	FortiNAC Manager eXtended VM Server (VMware or Hyper-V or AWS or Azure or KVM) (Running FortiNAC-OS)
Perpetual Licenses		
FortiNAC BASE License 100	LIC-FNAC-BASE-100	FortiNAC BASE License for 100 concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 1K	LIC-FNAC-BASE-1K	FortiNAC BASE License for 1K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 10K	LIC-FNAC-BASE-10K	FortiNAC BASE License for 10K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC BASE License 50K	LIC-FNAC-BASE-50K	FortiNAC BASE License for 50K concurrent endpoint devices. The BASE license provides Endpoint Visibility and Dynamic VLAN Steering.
FortiNAC PLUS License 100	LIC-FNAC-PLUS-100	FortiNAC PLUS License for 100 concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 1K	LIC-FNAC-PLUS-1K	FortiNAC PLUS License for 1K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 10K	LIC-FNAC-PLUS-10K	FortiNAC PLUS License for 10K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PLUS License 50K	LIC-FNAC-PLUS-50K	FortiNAC PLUS License for 50K concurrent endpoint devices. All the functionality of BASE with more advanced Network Access Controls and automated provisioning for users, guests, and devices.
FortiNAC PRO License 100	LIC-FNAC-PRO-100	FortiNAC PRO License for 100 concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 1K	LIC-FNAC-PRO-1K	FortiNAC PRO License for 1K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 10K	LIC-FNAC-PRO-10K	FortiNAC PRO License for 10K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
FortiNAC PRO License 50K	LIC-FNAC-PRO-50K	FortiNAC PRO License for 50K concurrent endpoint devices. PRO license level provides the ultimate in visibility, control and response.
Subscription Licenses		
Visibility (BASE)	FC1-10-FNAC1-215-01-DD	License for 25 concurrent endpoints. MOQ 500.
	FC2-10-FNAC1-215-01-DD	License for 500 concurrent endpoints. MOQ 500.
	FC3-10-FNAC1-215-01-DD	License for 10K concurrent endpoints. MOQ 500.
Visibility and Control (PLUS)	FC1-10-FNAC1-213-01-DD	License for 25 concurrent endpoints. MOQ 500.
	FC2-10-FNAC1-213-01-DD	License for 500 concurrent endpoints. MOQ 500.
	FC3-10-FNAC1-213-01-DD	License for 10K concurrent endpoints. MOQ 500.
Visibility, Control, and Response (PRO)	FC2-10-FNAC1-209-01-DD	License for 25 concurrent endpoints. MOQ 500.
	FC3-10-FNAC1-209-01-DD	License for 500 concurrent endpoints. MOQ 500.
	FC4-10-FNAC1-209-01-DD	License for 10K concurrent endpoints. MOQ 500.

FORTINET. www.fortinet.com

October 12, 2023

FNC-DAT-R23-20231012

FORTINET

DATA SHEET

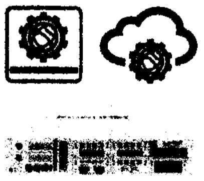
FortiWeb™

Available in:

Appliance Virtual Machine SaaS Cloud Container

Web Application and API Protection

FortiWeb 100E, 400E, 600E, 1000F, 2000F, 3000F, 4000F, VM, and Container



FortiWeb is a web application firewall (WAF) that protects web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations.

Using machine learning to model each application, FortiWeb defends applications from known vulnerabilities and from zero-day threats. High performance physical, virtual appliances and containers deploy on-site or in the public cloud to serve any size of the organization — from small businesses to service providers, carriers, and large enterprises.

Web Application Protection

Multi layer protection against the OWASP Top 10 application attacks including machine learning to defend against known and unknown attacks.

API Protection

Protect your APIs from malicious actors by automatically enforcing positive and negative security policies. Seamlessly integrate API security into your CI/CD pipeline.

Bot Mitigation

Protect websites, mobile applications, and APIs from automated attacks with advanced bot mitigation that accurately differentiates between good bot traffic and malicious bots. FortiWeb Bot Mitigation provides the visibility and control you need without slowing down your users with unnecessary captchas or challenges.

Highlights

- Machine learning that detects and blocks threats while minimizing false positives
- Advanced Bot Mitigation effectively protect web assets without imposing friction on legitimate users
- Protection for APIs, including those used to support mobile applications
- Enhanced protection with Fortinet Security Fabric integration
- Simplified attack investigation with Threat Analytics
- Third-party integration and virtual patching

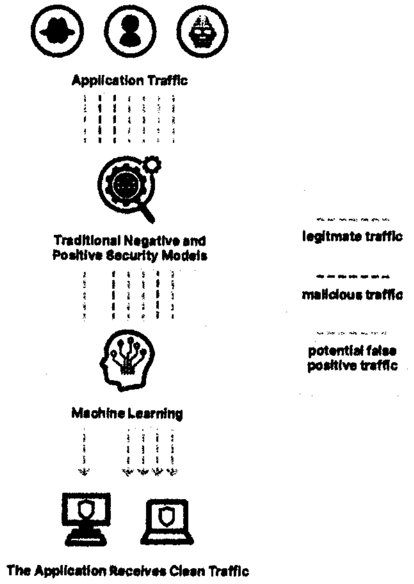
FortiCare Worldwide 24/7 Support

support.fortinet.com

FortiGuard Security Services

www.fortiguard.com

HIGHLIGHTS


Application Traffic
Traditional Negative and Positive Security Models
legitmate traffic
malicious traffic
potential false positive traffic
Machine Learning
The Application Receives Clean Traffic

FortiWeb goes beyond traditional negative and positive security models (attack signatures, IP address reputation, protocol validation, and so on), and applies a second layer of machine learning-based analytics to detect and block malicious anomalies while minimizing false positives.

Machine Learning Improves Detection and Drives Operational Efficiency

FortiWeb's multi-layer approach provides two key benefits: superior threat detection and improved operational efficiency.

FortiWeb's ability to detect anomalous behavior relative to the specific application being protected enables the solution to block unknown, never-before-seen exploits, providing your best protection against zero-day attacks targeting your application.

Operationally, FortiWeb machine learning relieves you of time-consuming tasks such as remediating false positives or manually tuning WAF rules. FortiWeb continually updates the model as your application evolves, so there is no need to manually update rules every time you update your application. FortiWeb enables you to get your code into production faster, eliminating the need for time-consuming manual WAF rules tuning and troubleshooting the false positives that plague less advanced WAFs.

0

Block Zero Day Threats

Comprehensive Web Application Security

Using an advanced multi-layered and correlated approach, FortiWeb provides complete security for your web-based applications from the OWASP Top 10 and many other threats. FortiWeb's first layer of defense uses traditional WAF detection engines (e.g. attack signatures, IP address reputation, protocol validation, and more) to identify and block malicious traffic, powered by intelligence from Fortinet's industry leading security research from FortiGuard Labs. FortiWeb's machine learning detection engine then examines traffic that passes this first layer, using a continuously updated model of your application to identify malicious anomalies and block them as well.

API Discovery and Protection

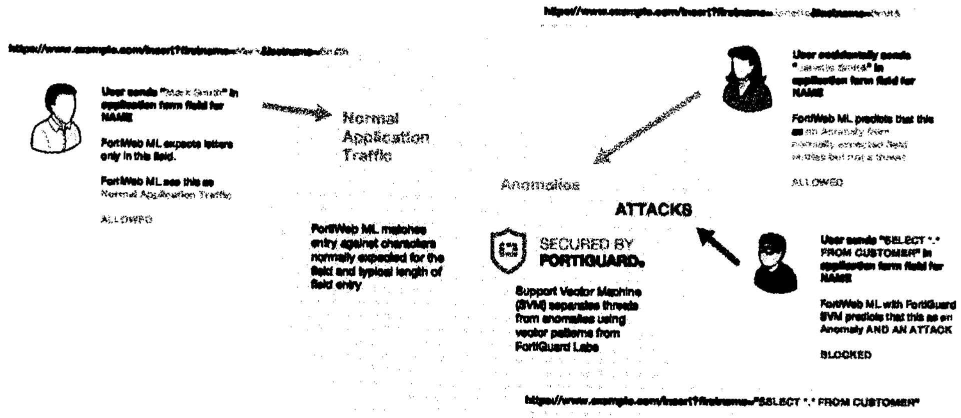
Fueling the digital transformation APIs have become increasingly popular, providing the backbone for mobile applications, automated business to business operations and ease of management across applications. However, with their popularity they also increase the attack surface with additional exposed application surfaces that organizations must secure. Fortinet's FortiWeb web application firewall provides the right tools to address threats to APIs. FortiWeb API Discovery and Protection uses machine learning algorithms to automatically discover APIs by continuously evaluating application traffic. Discovery is an integral role for establishing a positive security model and FortiWeb protects your critical APIs based on your profiled API inventory. FortiWeb can also integrate out of the box policies together with an automatically generated positive security model policy that is based on your organization's schema specification (OpenAPI, XML and generic JSON are supported schemas) to protect against API exploits. FortiWeb schema validation can be integrated into the CI/CD pipeline, automatically generating an updated positive security model policy once the API is updated..

Bot Mitigation

FortiWeb protects against automated bots, webs scrapers, crawlers, data harvesting, credential stuffing and other automated attacks to protect your web assets, mobile APIs, applications, users and sensitive data. Combining machine learning with policies such as threshold based detection, Bot deception and Biometrics based detection with superior good bot identification FortiWeb is able to block malicious bot attacks while reducing friction on legitimate users. With advanced tracking techniques FortiWeb can differentiate between humans, automated requests and repeat offenders, track behavior over time to better identify humans from bots and enforce CAPTCHA challenges when required. Together with FortiView, FortiWeb's graphical analysis dashboard organizations can quickly identify attacks and differentiate from good bots and legitimate users.

HIGHLIGHTS

FortiWeb's machine learning accurately detects anomalies and identifies which are threats. Unlike prevailing auto-learning detection models used by other WAF vendors that treat every anomaly as a threat, FortiWeb's precision nearly eliminates false positive detections and catches attack types that others cannot.

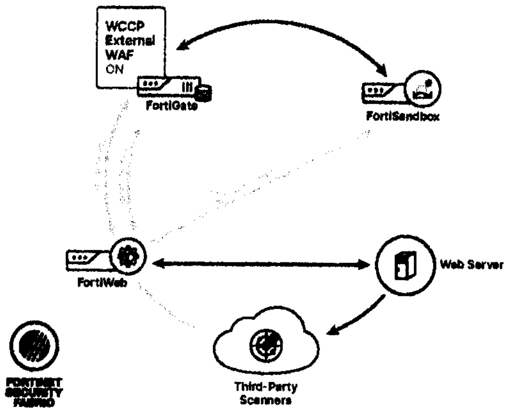

https://www.example.com/insert?firstname=Mark&lastname=Smith
User sends "Mark Smith" in application form field for NAME
FortiWeb ML expects letters only in this field.
FortiWeb ML see this as Normal Application Traffic
ALLOWED
Normal Application Traffic
FortiWeb ML matches entry against characters normally expected for the field and typical length of field entry
https://www.example.com/insert?firstname=Janet&lastname=Smith
User accidentally sends "Janette Smith" in application form field for NAME
FortiWeb ML predicts that this as an Anomaly from normally expected field entries but not a threat
ALLOWED
Anomalies
ATTACKS
SECURED BY FORTIGUARD.
Support Vector Machine (SVM) separates threats from anomalies using vector patterns from FortiGuard Labs
User sends "SELECT *.* FROM CUSTOMER" in application form field for NAME
FortiWeb ML with FortiGuard SVM predicts that this as an Anomaly AND AN ATTACK
BLOCKED
https://www.example.com/insert?firstname="SELECT *.* FROM CUSTOMER"

FortiWeb's AI-based machine learning evaluates application requests to determine if they are normal, benign anomalies, or anomalies that are threats.

Deep Integration into the Fortinet Security Fabric and Third-Party Scanners

As the threat landscape evolves, many new threats require a multi-pronged approach for protecting web-based applications. Advanced Persistent Threats that target users can take many different forms than traditional single-vector attack types and can evade protections offered only by a single device. FortiWeb's integration with FortiGate and FortiSandbox extend basic WAF protections through synchronization and sharing of threat information to both deeply scan suspicious files and share infected internal sources.

FortiWeb also provides integration with leading third-party vulnerability scanners including Acunetix, HP WebInspect, IBM AppScan, Qualys, ImmuniWeb and WhiteHat to provide dynamic virtual patches to security issues in application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules by FortiWeb to protect the application until developers can address them in the application code.



Integration with other Fortinet Security Fabric elements, including FortiGate and FortiSandbox, delivers APT protection and extends vulnerability scanning with leading third-party providers.

HIGHLIGHTS

Solving the Challenge of False Threat Detections

False positive threat detections can be very disruptive and force many administrators to loosen security rules on their web application firewalls to the point where many often become a monitoring tool rather than a trusted threat avoidance platform. The installation of a WAF may take only minutes, however fine-tuning can take days, or even weeks. Even after setup, a WAF can require regular checkups and tweaks as applications and the environment change.

FortiWeb's AI-based machine learning addresses false positive and negative threat detections without the need to tediously manage whitelists and fine-tune threat detection policies. With near 100% accuracy, the dual layer machine learning engines detect anomalies and then determine if they are threats unlike other methods that block all anomalies regardless of their intent. When combined with other tools, including user tracking, session tracking, and threat weighting, FortiWeb virtually eliminates all false detection scenarios.

Advanced Graphical Analysis and Reporting

FortiWeb includes a suite of graphical analysis tools called FortiView. Similar to other Fortinet products such as FortiGate, FortiWeb gives administrators the ability to visualize and drill-down into key elements of FortiWeb such as server/IP configurations, attack and traffic logs, attack maps, OWASP Top 10 attack categorization, and user activity. FortiView for FortiWeb lets administrators quickly identify suspicious activity in real time and address critical use cases such as origin of threats, common violations, and client/device risks.

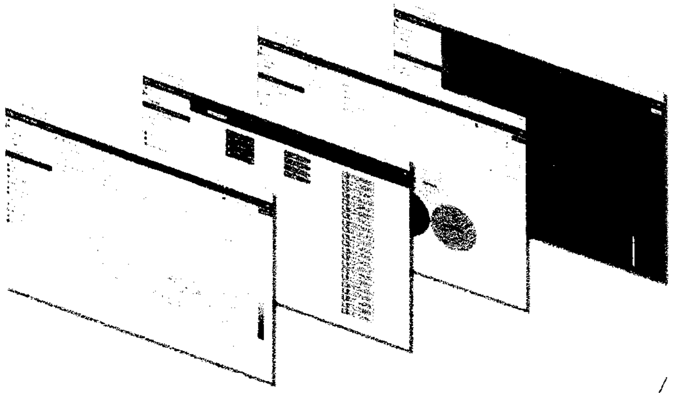
Secured by FortiGuard

Fortinet's Award-winning FortiGuard Labs is the backbone for many of FortiWeb's layers in its approach to application security. Offered as five separate options, you can choose the FortiGuard services you need to protect your web applications. FortiWeb IP address reputation service protects you from known attack sources like botnets, spammers, anonymous proxies, and sources known to be infected with malicious software.

FortiWeb Security Service is designed just for FortiWeb including items such as application layer signatures, machine learning threat models, malicious robots, suspicious URL patterns, and web vulnerability scanner updates. Credential Stuffing Defense checks login attempts against FortiGuard's list of compromised credentials and can take actions ranging from alerts to blocking logins from suspected stolen user ids and passwords. The FortiWeb Cloud Sandbox subscription enables FortiWeb to integrate with Fortinet's cloud-sandbox service. Finally, FortiWeb offers FortiGuard's top-rated antivirus engine that scans all file uploads for threats that can infect your servers or other network elements.

VM and Public Cloud Options

FortiWeb provides maximum flexibility in supporting your virtual and hybrid environments. The virtual versions of FortiWeb support all the same features as our hardware-based devices and can be deployed in VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, and Docker platforms. FortiWeb is also available for AWS, Azure, Google Cloud, and Oracle Cloud as a VM, and as WAF as a Service. For more information, see Fortiweb-Cloud.com.



FortiView for FortiWeb

ASSEMBLEIA LEGISLATIVA PARAÍBA C.P.L. 175

FEATURES

Deployment Options

- Reverse Proxy
- Inline Transparent
- True Transparent Proxy
- Offline Sniffing
- WCCP

Web Security

- AI-based Machine Learning
- Automatic profiling (white list)
- Web server and application signatures (black list)
- IP address reputation
- IP address geolocation
- HTTP RFC compliance
- Native support for HTTP/2
- WebSocket protection and signature enforcement
- Man in the Browser (MiTB) protection

Application Attack Protection

- OWASP Top 10
- Cross Site Scripting
- SQL Injection
- Cross Site Request Forgery
- Session Hijacking
- Built-in Vulnerability Scanner
- Third-party scanner integration (virtual patching)
- File upload scanning with AV and sandbox

Security Services

- Malware detection
- Virtual patching
- Protocol validation
- Brute force protection
- Cookie signing and encryption
- Threat scoring and weighting
- Syntax-based SQLi and XSS detection
- HTTP Header Security
- Custom error message and error code handling
- Operating system intrusion signatures
- Known threat and zero-day attack protection
- L4 Stateful Network Firewall
- DoS prevention
- Advanced correlation protection using multiple security elements
- Data leak prevention
- Web Defacement Protection

Application Delivery

- Layer 7 server load balancing
- URL Rewriting
- Content Routing
- HTTPS/SSL Offloading
- HTTP Compression
- Caching

Authentication

- Active and passive authentication
- Site Publishing and SSO
- RSA Access for 2-factor authentication
- LDAP, RADIUS, and SAML support
- SSL client certificate support
- CAPTCHA and Real Browser Enforcement (RBE)

API Protection

- Machine Learning based API Discovery and Protection
- XML and JSON protocol conformance
- CI/CD integration
- Schema verification
- API Gateway
- Web services signatures

Bot Mitigation

- Machine Learning based Bot Mitigation
- Biometrics Based Detection
- Threshold Based Detection
- Bot Deception
- Know Bots

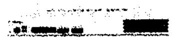
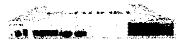
Management and Reporting

- Web user interface
- Command line interface
- FortiView graphical analysis and reporting tools
- Central management for multiple FortiWeb devices
- Active/Active HA Clustering
- REST API
- Centralized logging and reporting
- User/device tracking
- Real-time dashboards
- Bot dashboard
- OWASP Top 10 attack categorization
- Geo IP Analytics
- SNMP, Syslog and Email Logging/ Monitoring
- Administrative Domains with full RBAC

Other

- IPv6 Ready
- HTTP/2 to HTTP 1.1 translation
- HSM Integration
- Seamless PKI integration
- Attachment scanning for ActiveSync/MAPI applications, OWA, and FTP
- High Availability with Config-sync for syncing across multiple active appliances
- Auto setup and default configuration settings for simplified deployment
- Setup Wizards for common applications and databases
- Preconfigured for common Microsoft applications; Exchange, SharePoint, OWA
- OpenStack support for FortiWeb VMs
- Predefined security policies for Drupal and Wordpress applications
- WebSockets support

SPECIFICATIONS

	FORTIWEB 100F	FORTIWEB 400E	FORTIWEB 600E
Hardware			
10/100/1000 Interfaces (RJ-45 ports)	4	4 GE RJ45, 4 SFP GE	4 GE RJ45 (2 bypass), 4 SFP GE
10G BASE-SR SFP+ Ports	—	—	—
SSL/TLS Processing	Software	Software	Hardware
USB Interfaces	2	2	2
Storage	32 GB SSD	480 GB SSD	480 GB SSD
Form Factor	Desktop	1U	1U
Trusted Platform Module (TPM)	No	No	No
Power Supply	Single	Single	Dual
System Performance			
Throughput	50 Mbps	250 Mbps	750 Mbps
Latency	<5ms	<5ms	<5ms
High Availability	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering
Application Licenses	Unlimited	Unlimited	Unlimited
Administrative Domains	—	32	32

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

Dimensions			
Height x Width x Length (inches)	1.61 × 8.27 × 5.24	1.73 × 17.24 × 16.38	1.73 × 17.24 × 16.38
Height x Width x Length (mm)	41 × 210 × 133	44 × 438 × 416	44 × 438 × 416
Weight	2.3 lbs (1.1 kg)	22 lbs (9.97 kg)	22 lbs (9.97 kg)
Rack Mountable	Optional	Yes	Yes
Environment			
Power Required	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz	100–240V AC, 50–60 Hz
Maximum Current	110V/1.2A, 220V/1.2A	100V/5A, 240V/3A	100V/5A, 240V/3A
Power Consumption (Average)	18 W	109 W	109 W
Heat Dissipation	74 BTU/h	446.3 BTU/h	446.3 BTU/h
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-13°–158°F (-25°–70°C)	-13°–158°F (-25°–70°C)	-13°–158°F (-25°–70°C)
Forced Airflow	N/A (fanless)	Front to Back	Front to Back
Humidity	10%–90% non-condensing	10%–90% non-condensing	10%–90% non-condensing
Compliance			
Safety Certifications	FCC Class A Part 15, RCM, VCCI, CE, UL/cUL, CB	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL

SPECIFICATIONS

	FORTIWEB 1000F	FORTIWEB 2000F	FORTIWEB 3000F	FORTIWEB 4000F
Hardware				
10/100/1000 interfaces (RJ45 ports)	8 bypass, 4x SFP GE (non-bypass)	4GE (4 bypass), 4 SFP GE	8GE (8 bypass)	8GE (8 bypass)
10G BASE-SR SFP+ Ports	2	4	10 (2 bypass)	10 (2 bypass)
40G QSFP	-	-	-	2 bypass
SSL/TLS Processing	Hardware	Hardware	Hardware	Hardware
USB Interfaces	2	2	2	2
Storage	2× 480 GB SSD	2 × 480 GB SSD	2 × 960 GB SSD	2 × 960 GB SSD
Form Factor	2U	2U	2U	2U
Trusted Platform Module (TPM)	No	Yes	Yes	Yes
Power Supply	Dual Hot Swappable	Dual Hot Swappable	Dual Hot Swappable	Dual Hot Swappable
System Performance				
Throughput	2.5 Gbps	5 Gbps	10 Gbps	70 Gbps
Latency	<5ms	<5ms	<5ms	<5ms
High Availability	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering	Active/Passive, Active/Active Clustering
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	64	96	96	192

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

Dimensions				
Height x Width x Length (inches)	3.46 × 16.93 × 19.73	3.5 × 17.2 × 20.8	3.5 × 17.5 × 22.6	3.5 × 17.5 × 22.6
Height x Width x Length (mm)	88 × 430 × 501.20	88 × 438 × 530	88 × 444 × 574	88 × 444 × 574
Weight	28 lbs (12.8 kg)	33 lbs (15 kg)	56.2 lbs (22.5 kg)	56.2 lbs (22.5 kg)
Rack Mountable	Yes, with flanges	Yes	Yes	Yes
Environment				
Power Required	100–240V AC, 50–60 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz	100–240V AC, 60–50 Hz
Maximum Current	100V/5A, 240V/3A	120V/6A, 240V/3A	120V/2.8A, 240V/1.3A	120V/3A, 240V/1.5A
Power Consumption (Average)	140 W	200 W	200 W	248.5 W
Heat Dissipation	471 BTU/h	1433 BTU/h	1045.5 BTU/h	1219.8 BTU/h
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-4°–158°F (-20°–70°C)	-4°–158°F (-20°–70°C)	-4°–158°F (-20°–70°C)	-4°–158°F (-20°–70°C)
Forced Airflow	Front to Back	Front to Back	Front to Back	Front to Back
Humidity	5%–90% non-condensing	5%–90% non-condensing	5%–90% non-condensing	5%–90% non-condensing
Compliance				
Safety Certifications	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL	FCC Class A Part 15, RCM, VCCI, CE, UL/CB/cUL

SPECIFICATIONS

VIRTUAL MACHINES	FORTIWEB-VM (1 vCPU)	FORTIWEB-VM (2 vCPU)	FORTIWEB-VM (4 vCPU)	FORTIWEB-VM (8 vCPU)	FORTIWEB-VM (16 vCPU)
System Performance					
HTTP Throughput	25 Mbps	100 Mbps	500 Mbps	3 Gbps	6 Gbps
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	4 to 64 based on the amount of memory allocated				
Virtual Mechine					
Hypervisor Support	VMware, Microsoft Hyper-V, Citrix XenServer, Open Source Xen, VirtualBox, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and Oracle Cloud. Please see FortiWeb VM Installation Guide for versions supported.				
vCPU Support (Minimum / Maximum)	1	2	2 / 4	2 / 8	2 / 16
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10	1 / 10
Storage Support (Minimum / Maximum)	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB	40 GB / 2 TB
Memory Support (Minimum / Maximum)	1024 MB / Unlimited for 64-bit	1024 MB / Unlimited for 64-bit	1024 MB / Unlimited for 64-bit	1024 MB / Unlimited for 64-bit	1024 MB / Unlimited for 64-bit
Recommended Memory	8 GB	8 GB	16 GB	32 GB	64 GB
High Availability Support	Yes	Yes	Yes	Yes	Yes

Actual performance values may vary depending on the network traffic and system configuration. Performance metrics were observed using 4 x Intel(R) Xeon(R) Gold 6242 CPU @ 2.80GHz running VMware ESXI 6.7 with 8 GB of vRAM assigned to the 1 vCPU and 2 vCPU FortiWeb Virtual Appliance, 16 GB assigned to the 4 vCPU, 32 GB assigned to the 8 vCPU and 64 GB assigned to the 16 vCPU FortiWeb Virtual Appliance.

CONTAINER APPLIANCES	FORTIWEB-VMC01	FORTIWEB-VMC02	FORTIWEB-VMC04	FORTIWEB-VMC08
System Performance				
HTTP Throughput (Maximum)	25 Mbps	100 Mbps	500 Mbps	3 Gbps
Application Licenses	Unlimited	Unlimited	Unlimited	Unlimited
Administrative Domains	4 to 64 based on the amount of memory allocated			
Virtual Appliance				
Container Manager Support	Docker			
Network Interface Support (Minimum / Maximum)	1 / 10	1 / 10	1 / 10	1 / 10
Storage Support (Minimum / Maximum)	30 GB / 500 GB	30 GB / 500 GB	30 GB / 500 GB	30 GB / 500 GB
Memory Support (Minimum)	4 GB	4 GB	4 GB	4 GB
Recommended Memory	8 GB	8 GB	8 GB	8 GB
High Availability Support	No	No	No	No

Throughputs and other metrics are maximum values permitted for each version. Actual performance values may vary depending on the network traffic and system configuration.

ORDER INFORMATION

Product	SKU	Description
FortiWeb 100E	FWB-100E	Web Application Firewall — 4x GE RJ45 ports, 4 GB RAM,1× 32 GB SSD storage.
FortiWeb 400E	FWB-400E	Web Application Firewall — 4x GE RJ45 ports, 4x GE SFP ports, 480 GB SSD storage.
FortiWeb 600E	FWB-600E	Web Application Firewall — 4x GE RJ45 ports (2x bypass), 4x GE SFP ports, 480 GB SSD storage.
FortiWeb 1000F	FWB-1000F	Web Application Firewall — 2× 10 GE SFP+ ports, 8x GE RJ45 bypass ports, 4x GE SFP ports, 2 x GE management ports, dual AC power supplies, 2× 480 GB SSD storage
FortiWeb 2000F	FWB-2000F	Web Application Firewall - 4 × 10GE SFP+ ports, 4 x GE RJ45 bypass ports, 4 x GE SFP ports, 2 x GE management ports, dual AC power supplies, 2×480GB SSD storage.
FortiWeb 3000F	FWB-3000F	Web Application Firewall - 10 × 10GE SFP+ ports (2 bypass), 8 x GE RJ45 bypass ports, 2 x GE management ports, dual AC power supplies, 2×960GB SSD storage.
FortiWeb 4000F	FWB-4000F	Web Application Firewall - 2 × 40GE bypass ports, 10 × 10GE SFP+ ports (2 bypass), 8 x GE RJ45 bypass ports, 2 x GE management ports, dual AC power supplies, 2×960GB SSD storage.
FortiWeb-VM01	FWB-VM01	FortiWeb-VM, up to 1 vCPU supported. 64-bit OS.
FortiWeb-VM02	FWB-VM02	FortiWeb-VM, up to 2 vCPUs supported. 64-bit OS.
FortiWeb-VM04	FWB-VM04	FortiWeb-VM, up to 4 vCPUs supported. 64-bit OS.
FortiWeb-VM08	FWB-VM08	FortiWeb-VM, up to 8 vCPUs supported. 64-bit OS.
FortiWeb-VM16	FWB-VM16	FortiWeb-VM, up to 16 vCPUs supported. 64-bit OS.
FortiWeb-VMC01	FWB-VMC01	FWB-VMC01 for container-based environments. Up to 25 Mbps throughput.
FortiWeb-VMC02	FWB-VMC02	FWB-VMC02 for container-based environments. Up to 100 Mbps throughput.
FortiWeb-VMC04	FWB-VMC04	FWB-VMC04 for container-based environments. Up to 500 Mbps throughput.
FortiWeb-VMC08	FWB-VMC08	FWB-VMC08 for container-based environments. Up to 2 Gbps throughput.
Central Manager 10	FWB-CM-BASE	FortiWeb Central Manager license key, manage up to 10 FortiWeb devices, VMware vSphere.
Central Manager Unlimited	FWB-CM-UL	FortiWeb Central Manager license key, manage unlimited number of FortiWeb devices, VMware vSphere.

The following SKUs adopt the annual subscription licensing scheme:

Product	SKU	Description
FortiWeb-VM01-S Standard	FC1-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (1 CPU) with Standard bundle included.
FortiWeb-VM01-S Advanced	FC1-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (1 CPU) with Advanced bundle included.
FortiWeb-VM02-S Standard	FC2-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (2 CPU) with Standard bundle included.
FortiWeb-VM02-S Advanced	FC2-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (2 CPU) with Advanced bundle included.
FortiWeb-VM04-S Standard	FC3-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (4 CPU) with Standard bundle included.
FortiWeb-VM04-S Advanced	FC3-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (4 CPU) with Advanced bundle included.
FortiWeb-VM08-S Standard	FC4-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (8 CPU) with Standard bundle included.
FortiWeb-VM08-S Advanced	FC4-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (8 CPU) with Advanced bundle included.
FortiWeb-VM16-S Standard	FC5-10-WBVMS-916-02-DD	Subscription license for FortiWeb-VM (16 CPU) with Standard bundle included.
FortiWeb-VM16-S Advanced	FC5-10-WBVMS-633-02-DD	Subscription license for FortiWeb-VM (16 CPU) with Advanced bundle included.

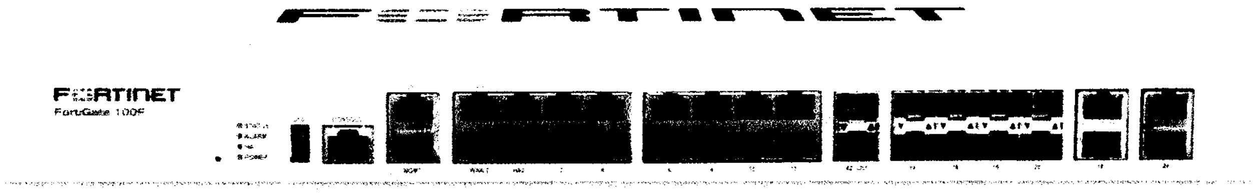
FORTINET. www.fortinet.com

FORTINET

FortiGate 100F Series

FG-100F and FG-101F

[redacted]



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

FortiOS Everywhere

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS, Fortinet's Advanced Operating System

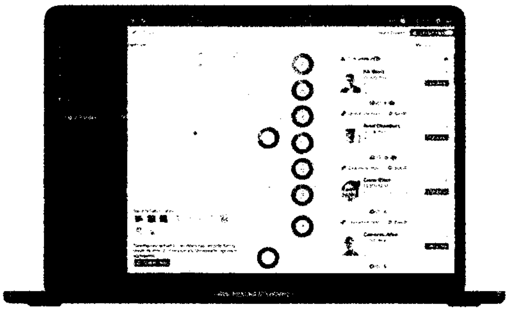
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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.

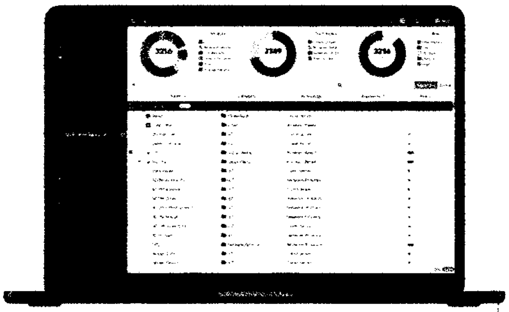
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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 Migration 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

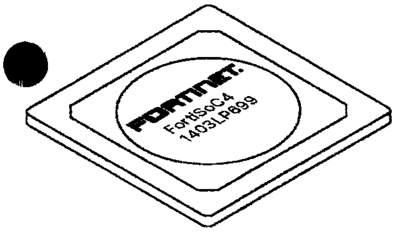
The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

SPU

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 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
- Reduces environmental footprint by saving on average over 60% in power consumption compared to previous generation of FortiGate models

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

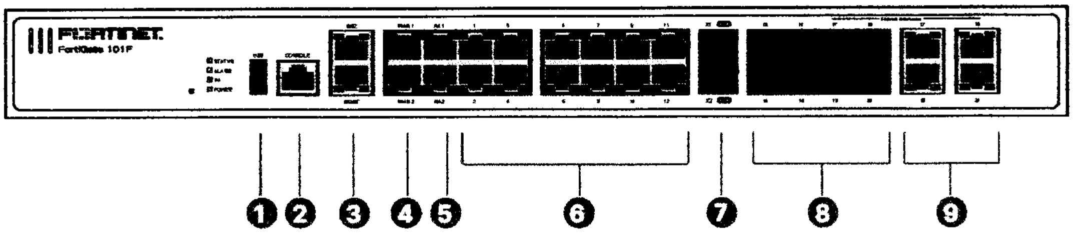
- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access—every time
- Agent-based access with FortiClient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

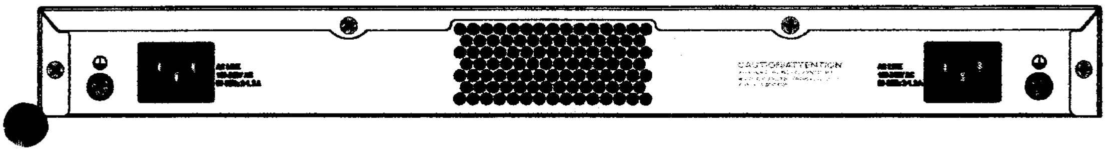
Segmentation

- 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 × 10 GE SFP+ FortiLink Slots
8. 4 x GE SFP Slots
9. 4 x GE RJ45/ SFP Shared Media Pairs

Hardware Features

SOC4 | 1U | AC DUAL / 480GB

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
Interfaces and Modules		
Hardware Accelerated GE RJ45 Ports	12	
Hardware Accelerated GE RJ45 Management/ HA/ DMZ Ports	1 / 2 / 1	
Hardware Accelerated GE SFP Slots	4	
Hardware Accelerated 10 GE SFP+ FortiLink Slots (default)	2	
GE RJ45 WAN Ports	2	
GE RJ45 or SFP Shared Ports *	4	
USB Port	1	
Console Port	1	
Onboard Storage	0	1× 480 GB SSD
Included Transceivers	0	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	2.6 Gbps	
NGFW Throughput [2,4]	1.6 Gbps	
Threat Protection Throughput [2,5]	1 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	20 / 18 / 10 Gbps	
Firewall Latency (64 byte, UDP)	4.97 μs	
Firewall Throughput (Packet per Second)	15 Mpps	
Concurrent Sessions (TCP)	1.5 Million	
New Sessions/Second (TCP)	56 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) [1]	11.5 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	16 000	
SSL-VPN Throughput	1 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	500	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	1 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	1800	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	135 000	
Application Control Throughput (HTTP 64K) [2]	2.2 Gbps	
CAPWAP Throughput (HTTP 64K)	15 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
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	

	FORTIGATE 100F	FORTIGATE 101F
Dimensions and Power		
Height x Width x Length (inches)	1.73 × 17 × 10	
Height x Width x Length (mm)	44 × 432 × 254	
Weight	7.25 lbs (3.29 kg)	7.56 lbs (3.43 kg)
Form Factor (supports EIA/non-EIA standards)	Rack Mount, 1 RU	
AC Power Supply	100–240V AC, 50/60 Hz	
Power Consumption (Average / Maximum)	26.5 W / 29.5 W	35.3 W / 39.1 W
Current (Maximum)	100V / 1A, 240V / 0.5A	
Heat Dissipation	100.6 BTU/h	121.13 BTU/h
Redundant Power Supplies	Yes (Default dual non-swappable AC PSU for 1+1 Redundancy)	
Power Supply Efficiency Rating	80Plus Compliant	
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	40.4 dBA	
Forced Airflow	Side to Back	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC Part 15B, Class A, CE, RCM, VCCI, UL/cUL, CB, BSMI	
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.

[6] Uses RSA-2048 certificate.

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, 2× 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, 2× 10 GE SFP+ FortiLinks, 480GB onboard storage, dual power supplies redundancy.

Optional Accessories	SKU	Description
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.
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

			[illegible]		
Service Category	Service Offering	A-la-carte	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		included with FortiCare Subscription		
	GeoIP DB Updates				
	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.

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

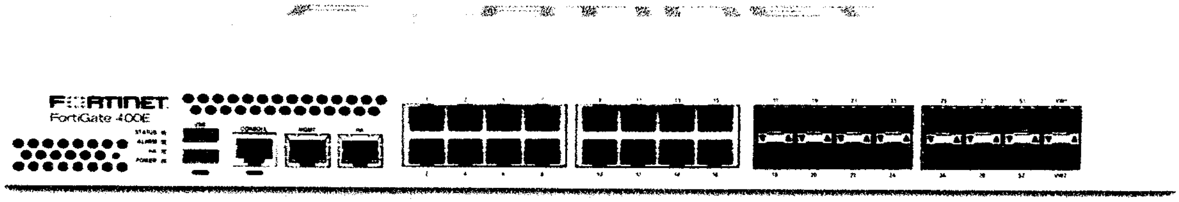
FG-100F-DAT-R34-20231017

FORTINET

FortiGate 400E Series

FG-400E, FG-401E, and FG-401E-DC

[redacted]



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 400E 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 400E 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
7.8 Gbps	6 Gbps	5 Gbps	Multiple GE RJ45 and GE SFP Slots | DC Variant

OS

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

FortiOS, Fortinet's Advanced Operating System

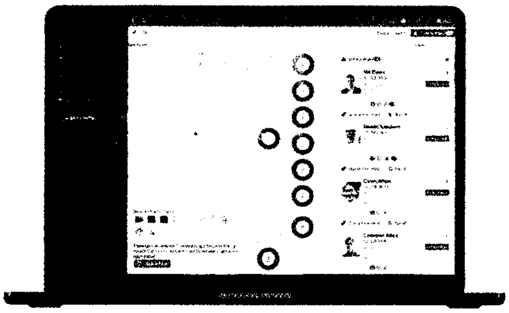
FortiOS enables the convergence of high performing networking and security across the Fortinet Security Fabric. Because it can be deployed anywhere, it delivers consistent and context-aware security posture across network, endpoint, and multi-cloud environments.

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.

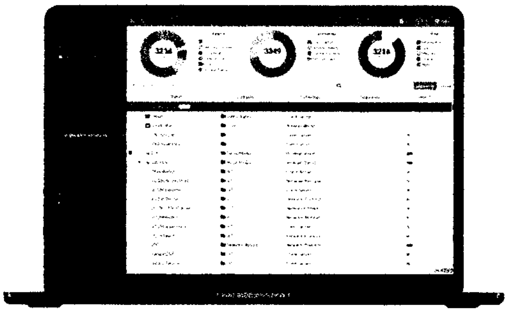
FortiOS dramatically expands the Fortinet Security Fabric's ability to deliver advanced AI/ML-powered services, inline advanced sandbox detection, integrated ZTNA enforcement, and more, provides protection across hybrid deployment models for hardware, software, and Software-as-a-Service with SASE.

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 Migration Service

FortiConverter Service provides hassle-free migration to help organizations transition from a wide range of legacy firewalls to FortiGate Next-Generation Firewalls quickly and easily. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

FortiGuard Services

Network and File Security

Services provide protection against network-based and file-based threats. This consists of Intrusion Prevention (IPS) which uses AI/M models to perform deep packet/SSL inspection to detect and stop malicious content, and apply virtual patching when a new vulnerability is discovered. It also includes Anti-Malware for defense against known and unknown file-based threats. Anti-malware services span both antivirus and file sandboxing to provide multi-layered protection and are enhanced in real-time with threat intelligence from FortiGuard Labs. Application Control enhances security compliance and offers real-time application visibility.

Web / DNS Security

Services provide protection against web-based threats including DNS-based threats, malicious URLs (including even in emails), and botnet/command and control communications. DNS filtering provides full visibility into DNS traffic while blocking high-risk domains, and protects against DNS tunneling, DNS infiltration, C2 server ID and Domain Generation Algorithms (DGA). URL filtering leverages a database of 300M+ URLs to identify and block links to malicious sites and payloads. IP Reputation and anti-botnet services prevent botnet communications, and block DDoS attacks from known sources.

SaaS and Data Security

Services address numerous security use cases across application usage as well as overall data security. This consists of Data Leak Prevention (DLP) which ensures data visibility, management and protection (including blocking exfiltration) across networks, clouds, and users, while simplifying compliance and privacy implementations. Separately, our Inline Cloud Access Security Broker (CASB) service protects data in motion, at rest, and in the cloud. The service enforces major compliance standards and manages account, user and cloud application usage. Services also include capabilities designed to continually assess your infrastructure, validate that configurations are working effectively and secure, and generate awareness of risks and vulnerabilities that could impact business operations. This includes coverage across IoT devices for both IoT detection and IoT vulnerability correlation.

Zero-Day Threat Prevention

Zero-day threat prevention entails Fortinet's AI-based inline malware prevention, our most advanced sandbox service, to analyze and block unknown files in real-time, offering sub-second protection against zero-day and sophisticated threats across all NGFWs. The service also has a built-in MITRE ATT&CK® matrix to accelerate investigations. The service focuses on comprehensive defense by blocking unknown threats while streamlining incident response efforts and reducing security overhead.

OT Security

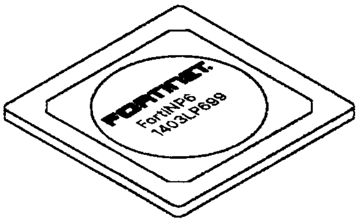
The service provides OT detection, OT vulnerability correlation, virtual patching, OT signatures, and industry-specific protocol decoders for overall robust defense of OT environments and devices.

Secure Any Edge at Any Scale

Powered by Security Processing Unit (SPU)

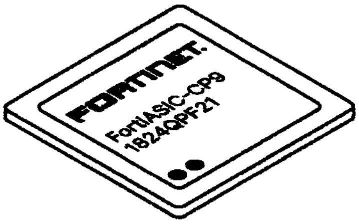
Traditional firewalls cannot protect against today's content- and connection-based threats because they rely on off-the-shelf hardware and general-purpose CPUs, causing a dangerous performance gap. Fortinet's custom SPU processors deliver the power you need—up to 520Gbps—to detect emerging threats and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

ASIC Advantage



Network Processor 6 NP6
Fortinet's new, breakthrough SPU NP6 network processor works inline with FortiOS functions delivering:

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



Content Processor 9 CP9
Content Processors act as co-processors to offload resource-intensive processing of security functions. The ninth generation of the Fortinet Content Processor, the CP9, accelerates resource-intensive SSL (including TLS 1.3) decryption and security functions while delivering:

- Pattern matching acceleration and fast inspection of real-time traffic for application identification
- IPS pre-scan/pre-match, signature correlation offload, and accelerated antivirus processing

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

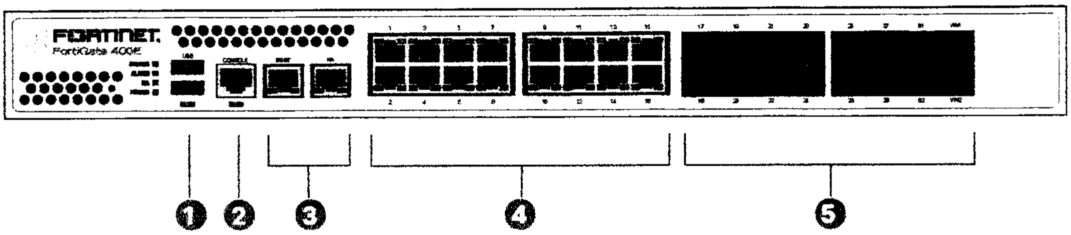
- Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies
- Provide extensive authentications, checks, and enforce policy prior to granting application access—every time
- Agent-based access with FortiClient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

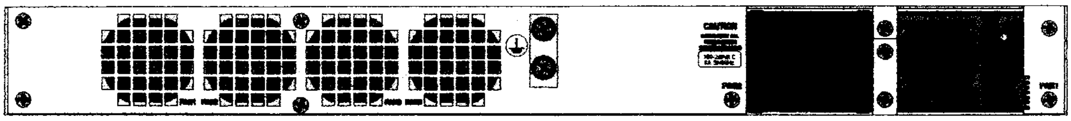
Segmentation

- 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 400E 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 Ports
5. 16 x GE SFP Slots

Hardware Features

NP6 | CP9 | 1U | AC DUAL / 480GB

Specifications

	FG-400E	FG-401E/DC
Interfaces and Modules		
Hardware Accelerated GE RJ45 Interfacess	16	
Hardware Accelerated GE SFP Slots	16	
GE RJ45 Management Ports	2	
USB Ports	2	
RJ45 Console Port	1	
Onboard Storage	0	2× 240 GB SSD
Included Transceivers	2x SFP (SX 1 GE)	
System Performance — Enterprise Traffic Mix		
IPS Throughput [2]	7.8 Gbps	
NGFW Throughput [2, 4]	6 Gbps	
Threat Protection Throughput [2, 5]	5 Gbps	
System Performance and Capacity		
IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP)	32 / 32 / 24 Gbps	
IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP)	32 / 32 / 24 Gbps	
Firewall Latency (64 byte, UDP)	2.14 μs	
Firewall Throughput (Packet per Second)	36Mpps	
Concurrent Sessions (TCP)	4 Million	
New Sessions/Second (TCP)	450 000	
Firewall Policies	10 000	
IPsec VPN Throughput (512 byte) [1]	20 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	2000	
Client-to-Gateway IPsec VPN Tunnels	50 000	
SSL-VPN Throughput	4.5 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	5000	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	4.8 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	4000	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	300 000	
Application Control Throughput (HTTP 64K) [2]	12 Gbps	
CAPWAP Throughput (HTTP 64K)	14.8 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	72	
Maximum Number of FortiAPs (Total / Tunnel)	512 / 256	
Maximum Number of FortiTokens	5000	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FG-400E	FG-401E/DC
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	16.4 lbs (7.4 kg)	16.9 lbs (7.9 kg)
Form Factor	Rack Mount, 1 RU	
AC Power Consumption (Average / Maximum)	109 W / 214 W	115 W / 221 W
AC Power Input	100–240V AC, 50/60Hz	
AC Current (Maximum)	6A	
DC Power Input		-48V to -60V DC
DC Current (Maximum)		11.5A
DC Current (Nominal)		4.6A
DC Power Consumption (Average / Maximum)		115W / 221W
Heat Dissipation	730 BTU/h	754 BTU/h
Redundant Power Supplies (Hot Swappable)	Optional	
Power Supply Efficiency Rating	80Plus Compliant	
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	48 dBA	
Airflow	Side and Front to Back	
Operating Altitude	Up to 7400 ft (2250 m)	
Compliance	FCC Part 15 Class A, RCM, VCCI, CE, UL/ cUL, CB	
Certifications	USGv6/IPv6	

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.

Ordering Information

Product	SKU	Description
FortiGate 400E	FG-400E	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 16x GE SFP slots, SPU NP6 and CP9 hardware accelerated.
FortiGate 401E	FG-401E	18x GE RJ45 ports (including 1x MGMT port, 1x HA port, 16x switch ports), 16x GE SFP slots, SPU NP6 and CP9 hardware accelerated, 2× 240 GB onboard SSD storage.
FortiGate 401E-DC	FG-401E-DC	18 x GE RJ45 ports (including 1 x MGMT port, 1 X HA port, 16 x switch ports), 16 x GE SFP slots, SPU NP6 and CP9 hardware accelerated, 2× 240GB onboard SSD storage, 1 DC power supply.
Optional Accessories		
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.
Optional Power Supply	SP-FG300E-PS	AC power supply for FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FAZ-200F/300F/800F and FMG-200F/300F.
DC Power Supply	SP-FG300E-DC-PS	DC power supply for FG-401E-DC and FG-1100E-DC.

Subscriptions

			Bundles		
Service Category	Service Offering	A-la-carte	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		included with FortiCare Subscription		
	GeoIP DB Updates				
	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.

9

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

FG-400E-DAT-R19-20231017