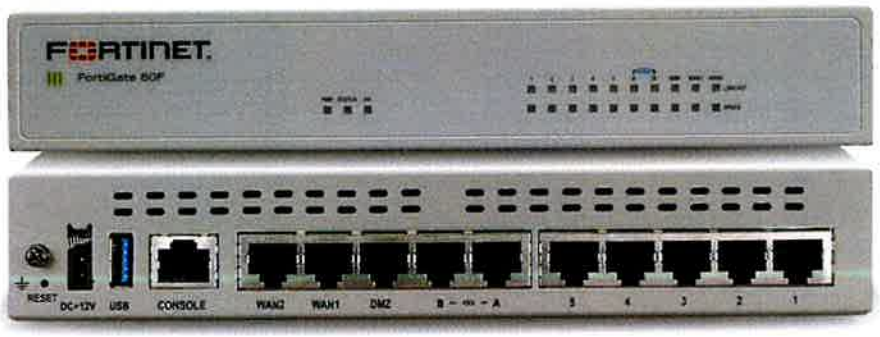
Solución propuesta

Ítem 1 Switch

Producto: FortiGate-60F Hardware plus 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP)
Número de Parte: FG-60F-BDL-950-12
Cantidad: Setenta y cinco (75) unidades
Soporte y licencia: Un (1) año



iQtek

Matriz de Cumplimiento

Ítem 1 Switch		
Especificaciones Técnicas Requeridas	***Especificaciones Técnicas Ofertadas***	***Cumple***
Fortigate FG-60F	Bundle FortiGate-60F Hardware plus 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP)	✓
Dos (2) GE RJ45 WAN	FortiGate-60F with 2 x GE RJ45 WAN Ports	✓
Un (1) puerto DMZ	FortiGate-60F with 1 x GE RJ45 DMZ Port	✓
Cinco (5) puertos internos RJ45.	FortiGate-60F with 5 x GE RJ45 Internal Ports	✓
Garantía Hardware Plus de un (1) año Premium FortiCare y protección unificada contra amenazas (UTP) FortiGuard.	1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP)	✓
Equipos nuevos (no remanufacturados).	Brand New Device	✓

Nota: Para obtener más información sobre el producto, favor consultar hoja de datos (datasheet) anexo.

Condiciones

Condiciones de Pago

Aceptamos las condiciones de pago descritas en el pliego de anticipo de pago de anticipo del 20% del monto presupuestado y adjudicado y 80% restante luego de haber entregado la totalidad de lo adjudicado.

Duración del Suministro

Los bienes serán entregados en los períodos detallados a continuación:

Equipo	Tiempo de Entrega
Ítem 1	Cuarenta y cinco (45) a noventa (90) días calendario.

Validez de la oferta

Nuestra oferta permanecerá vigente por un periodo de sesenta (60) de días, a partir de la fecha de apertura de ofertas.

Franklyn Geovanny Ciprian Goodin, en Calidad de Representante Legal, debidamente autorizado para actuar en nombre y representante de **IQtek Solutions, S.R.L.**

Firma

IQtek, S.R.L. RNC 130576967 Santo Domingo, R.D.

Certificado de Revendedor Autorizado

Fecha: 7 de febrero de 2025
Junta Central Electoral de la Republica Domincana

Reference: JCE-CCC-CP-2025-0004

Fortinet, Inc. ("Fortinet") opera a través de un canal de distribuidores y revendedores independientes. A la vista de ello, Fortinet confirma por la presente que: IQtek Solutions S.R.L

con domicilio social en: Calle Gala #8, Arroyo Hondo Viejo, Santo Domingo, RD., Santo DOmingo, 9999, DOMINICAN REPUBLIC;

es actualmente un revendedor (FortiPartner) autorizado para vender productos y servicios de Fortinet en DO conforme a las siguientes designaciones:

- Nivel de contrato: Expert
- Modelo de negocio: Integrator
- Especializaciones: SD-WAN, Data Center

Este certificado se emite en la fecha señalada arriba y es válido por un periodo de 180 días a partir de dicha fecha.

Siempre y cuando el FortiPartner identificado anteriormente haya adquirido servicios de soporte,, y estos hayan sido, efectivamente, registrados y contratados con Fortinet, Fortinet se compromete a proporcionar dicho servicio de soporte para los productos aplicables de conformidad con los términos del contrato de soporte de Fortinet disponibles en la dirección: https://support.fortinet.com. . Los productos de Fortinet son distribuidos de conformidad con los términos y la garantía de Fortinet establecidos en el acuerdo de licencia de usuario final (End User License Agreement) disponible en la dirección: http://www.fortinet.com/doc/legal/EULA.pdf.

La validez de este Certificado se encuentra sujeta a que el FortiPartner mantenga su contrato vigente con Fortinet y que éste cumpla las políticas y directrices de Fortinet. El programa de partners de Fortinet y sus directrices están disponibles en http://www.fortinet.com/partners/partner_program/fpp.html. Sin perjuicio de lo anterior, los FortiPartner no representan a Fortinet y, por consiguiente, no están autorizados a emitir declaraciones vinculantes por o para Fortinet.

Manufacturer Confirmation

Gonzalo Ruiz
VP of Legal and Compliance Americas

Por favor tenga en cuenta que, sin perjuicio de cualquier disposición en contrario: (1) las obligaciones de Fortinet, Inc. (Fortinet) relacionadas con especificaciones de productos, licencias, soporte, suscripciones, certificaciones, garantías y cualquier otra aseveración son: (a) inválidas para productos que hayan sido manipulados o modificados por terceros y (b) sujetas en todos los aspectos a los procesos, políticas, términos y estándares de Fortinet, mismos que Fortinet puede modificar en cualquier momento a su entera y absoluta discreción; (2) Fortinet se reserva el derecho a modificar los planes técnicos y de hoja de ruta y las fechas de lanzamiento en cualquier momento a su entera y absoluta discreción; (3) Fortinet no se responsabiliza y declina toda responsabilidad por errores ortográficos, gramaticales, tipográficos, de traducción o de impresión; (4) este documento tiene únicamente fines informativos, no es un instrumento jurídicamente vinculante y no pretende crear, ni crea, ninguna obligación contractual o garantía por parte de Fortinet, ni impedimento promisorio o derecho a confiar en las declaraciones aquí contenidas; (5) las declaraciones aquí contenidas sobre el rendimiento y las características de los productos pueden ser contextuales, por ejemplo, basadas en pruebas realizadas en un entorno particular, como un entorno de laboratorio, y pueden no ser precisas en todos los contextos, como en un entorno real; (6) el firmante de este documento basa cualquier declaración aquí contenida en su conocimiento al momento de la firma, sin obligación alguna de investigar las declaraciones aquí contenidas, estar confiando plenamente en la revisión y aportación de otros; (7) los productos y servicios no se ofrecen de forma gratuita y los derechos sólo se conceden u otorgan sujetos al pago total a Fortinet y sus distribuidores y revendedores, todas las ventas son definitivas, y se aplican las políticas y términos y condiciones de Fortinet, a título enunciativo, más no limitativo, el EULA estándar de Fortinet y los términos de soporte, algunos de los cuales se encuentran en https://www.fortinet.com/corporate/about-us/legal.html ; y, (8) Fortinet no tiene obligación alguna de actualizar, ni tiene intención de actualizar, las declaraciones aquí contenidas, incluso si, por ejemplo, el firmante se entera de que las declaraciones en este documento son, de hecho, falsas o que los planes cambien.

IQtek S.R.L. RNC 130676967 Santo Domingo, R.D.

Revisiones

Versión	Revisión	Fecha	Autor(es)	Nota
1				

Confidencialidad

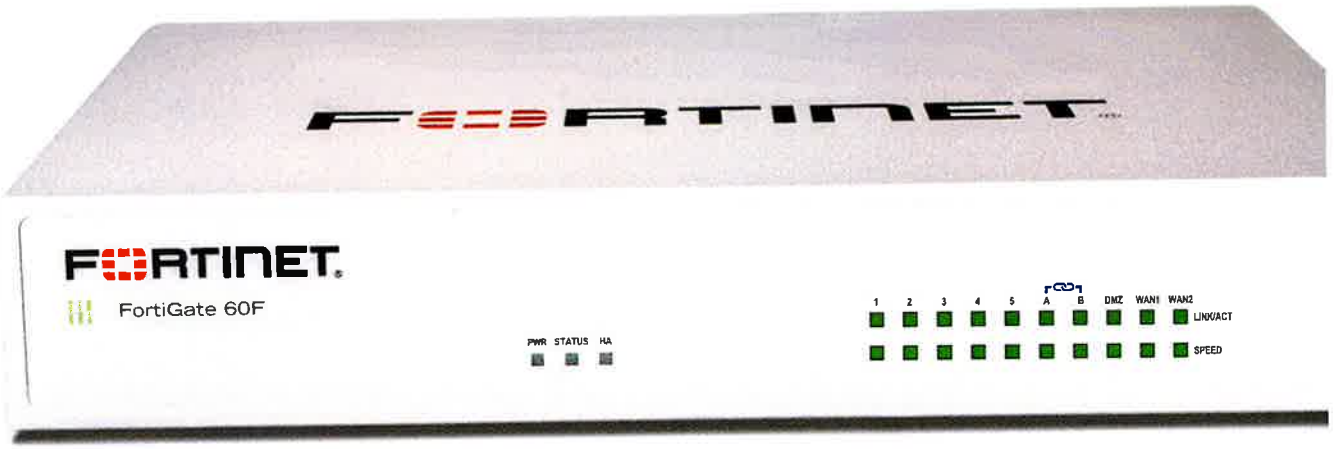
Junta Central Electoral (en lo adelante EL CLIENTE) e **IQTEK SOLUTIONS** (en lo adelante IQTEK) acuerdan no divulgar el contenido de esta documentación de servicios profesionales y suministro de equipos a terceras partes a menos que no sean empleados de EL CLIENTE o IQTEK (colectivamente como LAS PARTES) con necesidad especifica de conocer su contenido, en cuyo caso dichas personas deberán comprometerse a no revelar la información confidencial relacionada con el proyecto que figura en el presente documento.

Uso Exclusivo

LAS PARTES acuerdan que el contenido de este documento es de uso exclusivo de dichas partes, para el consumo técnico, administrativo y comercial de referencia para los servicios presentados por IQTEK, las configuraciones, despliegue y trabajos sugeridos por IQTEK en las facilidades de EL CLIENTE.

La finalidad de este documento es ilustrativa, el mismo no puede ser tomado como referencia por ninguna de LAS PARTES como instrumento o soporte para ningún tipo de alcance o contrato de proyectos futuros.

FortiGate FortiWiFi Serie 60F



Altamente derechos

Gartner®MagicQuadrant™ Líderes Tanto para firewalls de red como para SD-WAN

Rendimiento sin igual
Habilitado por Fortinet ASIC patentado y el sistema operativo FortiOS

Protección de nivel empresarial con servicios de seguridad potenciados por IA de FortiGuard

Operaciones simplificadas con gestión centralizada
Para redes y seguridad, flujos de trabajo automatizados, análisis profundos y autorreparación.

SD-WAN inclusivoy
Controlador inalámbrico en cada dispositivo FortiGate sin costo adicional

Amplia cartera Para cualquier presupuesto y necesidad empresarial

Cortafuegos convergente de próxima generación y SD-WAN

Las series FortiGate y FortiWiFi 60F integran firewall, SD-WAN y seguridad en un solo dispositivo, lo que las hace perfectas para construir redes seguras en sitios empresariales distribuidos y transformar la arquitectura WAN a cualquier escala.

La serie 60F está equipada con FortiOS, el primer sistema operativo de seguridad y redes convergentes de la industria. Esta convergencia permite a las empresas proteger de manera eficiente y óptima las dinámicas infraestructuras digitales actuales.

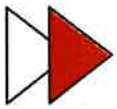
Como piedra angular de la plataforma Fortinet Security Fabric, FortiGate NGFW funciona a la perfección con los servicios de seguridad impulsados por IA de FortiGuard para brindar protección contra amenazas coordinada, automatizada y de extremo a extremo en tiempo real.

La familia 60F está construida sobre el ASIC patentado basado en SD-WAN, que ofrece un rendimiento inigualable en comparación con las CPU tradicionales con un menor costo y un menor consumo de energía. Este diseño específico para la aplicación y el procesador multinúcleo integrado aceleran aún más la convergencia de las funciones de red y seguridad en la familia 60F para optimizar las conexiones seguras y brindar una experiencia de usuario sólida en las sucursales.

IPS	GNF	Protección contra amenazas	Interfaces
1,4 Gbps	1 Gbps	700 Mbps	Múltiples GE RJ45 | Variantes con almacenamiento interno | Variantes WiFi

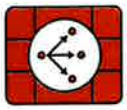
Casos de uso

Protección perimetral



- Proteja las redes del tráfico malicioso, protéjase contra amenazas basadas en archivos, bloquee ataques basados en la web y proteja aplicaciones y datos con los servicios de seguridad con tecnología de inteligencia artificial FortiGuard integrados de forma nativa
- Inspeccionar y controlar el tráfico entrante y saliente según políticas de seguridad definidas
- Realice una inspección SSL en tiempo real (incluido TLS 1.3) con visibilidad completa de los usuarios, dispositivos y aplicaciones en toda la superficie de ataque
- Acelere el rendimiento, la protección y la eficiencia energética con la SPU patentada de Fortinet con tecnologías de seguridad y redes convergentes

SD-WAN segura



- FortiGate permite el mejor borde WAN de su clase con SD-WAN integrado, optimización de WAN, seguridad y administración unificada desde un único sistema operativo FortiOS
- FortiGate, construido sobre un ASIC patentado basado en SD-WAN, ofrece una identificación de aplicaciones más rápida para evitar demoras en el acceso a las aplicaciones y acelera el rendimiento de la superposición independientemente de la ubicación.
- Mejora el trabajo híbrido con una solución SASE integral al integrar SD-WAN entregada en la nube con el borde del servicio de seguridad (SSE)
- Logra eficiencias operativas a cualquier escala a través de la automatización, el análisis profundo y la autorreparación.

Sucursal segura

- La plataforma Fortinet Security Fabric permite que los NGFW de FortiGate descubran y aseguren automáticamente los dispositivos IoT para una incorporación más rápida a las sucursales
- FortiGate, totalmente integrado con los conmutadores Ethernet seguros FortiSwitch y los puntos de acceso FortiAP, extiende fácilmente la seguridad a WAN, LAN y WLAN en sucursales para una protección unificada y una conectividad confiable.
- Los productos FortiGate y Fortinet funcionan a la perfección con FortiManager para centralizar la visibilidad y simplificar la gestión en todas las ubicaciones para los equipos de TI.
- El soporte de FortiGate HA garantiza la protección continua de la red y minimiza el tiempo de inactividad en caso de fallas de hardware o interrupciones de la red.

Servicios de seguridad con tecnología de inteligencia artificial FortiGuard

Los servicios de seguridad potenciados por IA de FortiGuard forman parte de la defensa en capas de Fortinet y están estrechamente integrados en nuestros NGFW FortiGate y otros productos. Estos servicios, que incorporan la información de amenazas más reciente de FortiGuard Labs, protegen a las organizaciones contra los vectores de ataque y las amenazas modernas, incluidos los ataques de día cero y los sofisticados ataques potenciados por IA.

Seguridad de redes y archivos

Los servicios de seguridad de archivos y redes protegen contra amenazas basadas en archivos y redes. Con más de 18 000 firmas, nuestro sistema de prevención de intrusiones (IPS) líder en la industria utiliza modelos de IA/ML para la inspección profunda de paquetes/SSL, la detección y el bloqueo de contenido malicioso y la aplicación de parches virtuales para vulnerabilidades recién descubiertas. La protección antimalware defiende contra amenazas basadas en archivos conocidas y desconocidas, combinando antivirus y sandboxing para una seguridad de múltiples capas. El control de aplicaciones mejora el cumplimiento de la seguridad y proporciona visibilidad en tiempo real de las aplicaciones y el uso.

Seguridad web/DNS

Los servicios de seguridad de DNS y Web protegen contra ataques basados en DNS, URL maliciosas (incluidas las de los correos electrónicos) y comunicaciones de botnets. El filtrado de DNS bloquea todo el espectro de ataques basados en DNS, mientras que el filtrado de URL utiliza una base de datos de más de 300 millones de URL para identificar y bloquear enlaces maliciosos. Mientras tanto, los servicios de reputación de IP y antibotnets protegen contra la actividad de botnets y los ataques DDoS. FortiGuard Labs bloquea más de 500 millones de URL maliciosas, de phishing y spam por semana, y bloquea 32 000 intentos de comando y control de botnets cada minuto, lo que demuestra la sólida protección que ofrece Fortinet.

SaaS y seguridad de datos

Los servicios de seguridad de datos y SaaS cubren las necesidades de seguridad clave para el uso de aplicaciones y la protección de datos. Esto incluye la prevención de pérdida de datos para garantizar la visibilidad, la gestión y la protección (bloqueo de la exfiltración) de los datos en movimiento en redes, nubes y usuarios. Nuestro servicio de agente de seguridad de acceso a la nube en línea protege los datos en movimiento, en reposo y en la nube, aplicando estándares de cumplimiento y administrando el uso de cuentas, usuarios y aplicaciones en la nube. Los servicios también evalúan la infraestructura, validan las configuraciones y destacan los riesgos y las vulnerabilidades, incluida la detección de dispositivos IoT y la correlación de vulnerabilidades.

Prevención de amenazas de día cero

La prevención de amenazas de día cero se logra mediante la prevención de malware en línea impulsada por IA para analizar el contenido de los archivos a fin de identificar y bloquear malware desconocido en tiempo real, lo que brinda protección en menos de un segundo en todos los NGFW. El servicio también integra la matriz MITRE ATT&CK para acelerar las investigaciones. Integrado en los NGFW FortiGate, el servicio brinda una defensa integral al bloquear amenazas desconocidas, agilizar la respuesta a incidentes y reducir la sobrecarga de seguridad.

Seguridad OT

Con más de 1000 parches virtuales, más de 1100 aplicaciones OT y más de 3300 reglas de protocolo, las capacidades de seguridad OT integradas detectan amenazas dirigidas a la infraestructura OT, realizan correlaciones de vulnerabilidades, aplican parches virtuales y utilizan decodificadores de protocolo específicos de la industria para una defensa sólida de los entornos y dispositivos OT.

Disponible en

Aparato

Virtual

Alojado

Nube

Recipiente

FortiOS en todas partes

FortiOS, el sistema operativo de seguridad de red en tiempo real de Fortinet

FortiOS es el sistema operativo que impulsa la plataforma Fortinet Security Fabric, lo que permite la aplicación de políticas de seguridad y una visibilidad integral en toda la superficie de ataque. FortiOS proporciona un marco unificado para gestionar y proteger redes, basadas en la nube, híbridas o una convergencia de TI, OT e IoT. FortiOS permite una interoperabilidad fluida y eficiente entre los productos de Fortinet con una protección consistente y consolidada impulsada por IA en los entornos híbridos actuales.

A diferencia de las soluciones puntuales tradicionales, Fortinet adopta un enfoque holístico de la ciberseguridad, con el objetivo de reducir las complejidades, eliminar los silos de seguridad y mejorar la eficiencia operativa. Al consolidar las funciones de seguridad en una única plataforma, FortiOS simplifica la gestión, reduce los costes y mejora la seguridad general. Juntos, FortiGate y FortiOS crean una protección inteligente y adaptativa para ayudar a las organizaciones a reducir la complejidad, eliminar los silos de seguridad y optimizar la experiencia del usuario.

Al integrar IA generativa (GenAI), FortiOS mejora aún más la capacidad de analizar el tráfico de la red y la inteligencia sobre amenazas, detecta desviaciones o anomalías de manera más efectiva y brinda recomendaciones de reparación más precisas, lo que garantiza un impacto mínimo en el rendimiento sin comprometer la seguridad.

Obtenga más información sobre las novedades de FortiOS.https://www.fortinet.com/products/fortigate/fortios

Vista intuitiva y fácil de usar de la red y
vulnerabilidades de puntos finales

Visión integral del rendimiento de la red,
seguridad y estado del sistema

ASIC de Fortinet: seguridad sin igual, rendimiento sin precedentes

Impulsado por el único SPU especialmente diseñado

Los firewalls tradicionales no pueden proteger contra las amenazas actuales basadas en contenido y conexión porque dependen de unidades centrales de procesamiento (CPU) de uso general listas para usar, lo que deja una brecha de seguridad peligrosa. Las SPU personalizadas de Fortinet ofrecen la potencia que necesita para aumentar radicalmente la velocidad, la escala y la eficiencia, al mismo tiempo que mejoran enormemente la experiencia del usuario y reducen los requisitos de espacio y energía. Las SPU de Fortinet ofrecen hasta 520 Gbps de rendimiento protegido para detectar amenazas emergentes y bloquear contenido malicioso, al tiempo que garantizan que su solución de seguridad de red no se convierta en un cuello de botella en el rendimiento.

Los ASIC de Fortinet están diseñados para ser energéticamente eficientes, lo que genera un menor consumo de energía y un mejor costo total de propiedad. Ofrecen un rendimiento líder en la industria, manejan más tráfico y realizan inspecciones de seguridad más rápido, reducen la latencia para un procesamiento más rápido de los paquetes y minimizan los retrasos de la red.

Las SPU de Fortinet están diseñadas con funciones de seguridad integradas como confianza cero, SSL, IPS y VXLAN, por nombrar solo algunas, mejorando drásticamente el rendimiento de estas funciones que los competidores tradicionalmente implementan en el software.

SD-WANASICSP4 segura

- Combina una CPU basada en RISC con procesadores de red y contenido SPU patentados de Fortinet para un rendimiento inigualable
- Ofrece la identificación y dirección de aplicaciones más rápida de la industria para operaciones comerciales eficientes.
- Acelera el rendimiento de VPN IPsec para la mejor experiencia de usuario en el acceso directo a Internet
- Permite la mejor seguridad NGFW y una inspección SSL profunda con alto rendimiento
- Extiende la seguridad a la capa de acceso para permitir la transformación de SD-Branch con conectividad de punto de acceso y conmutador acelerada e integrada

Gestión unificada para una seguridad y eficiencia óptimas

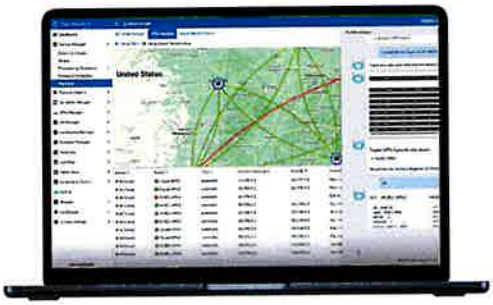
Ya sea una pequeña empresa o una gran empresa, Fortinet proporciona control centralizado, visibilidad y automatización para su infraestructura de seguridad.

FortiManager: gestión centralizada a escala para empresas distribuidas

FortiManager, con tecnología de FortiAI, es una solución de gestión centralizada para Fortinet Security Fabric. Optimiza el aprovisionamiento masivo y la gestión de políticas para FortiGate, FortiGate VM, seguridad en la nube, SD-WAN, SD-Branch, FortiSASE y ZTNA en entornos híbridos. Además, FortiManager proporciona monitoreo en tiempo real de toda la infraestructura administrada y automatiza los flujos de trabajo de operación de red. Al aprovechar GenAI en FortiAI, mejora aún más las configuraciones y el aprovisionamiento del día 0 al 1, y la resolución de problemas y el mantenimiento del día N, liberando todo el potencial de Fortinet Security Fabric y aumentando significativamente la eficiencia operativa.

FortiGateCloud: gestión simplificada para pequeñas y medianas empresas

FortiGate Cloud es un servicio SaaS que ofrece administración simplificada, análisis de seguridad e informes para los NGFW FortiGate de Fortinet para ayudarlo a administrar sus dispositivos de manera más eficiente y reducir el riesgo cibernético. Simplifica la implementación inicial, la configuración y la administración continua de FortiGates y dispositivos conectados en sentido descendente, como FortiAP, FortiSwitch y FortiExtender, con aprovisionamiento sin intervención. Proporciona visibilidad histórica y en tiempo real de los análisis de tráfico y las amenazas de seguridad para reducir los riesgos y mejorar la postura de seguridad. Vea diversas amenazas, tráfico web y eventos del sistema almacenados en la nube durante hasta un año, con informes predefinidos para cumplir con el cumplimiento y brindar información útil.



GenAI en FortiManager ayuda a administrar redes sin esfuerzo: genera configuraciones y políticas scripts, solucionar problemas y ejecutar acciones recomendadas

FortiGate Cloud ofrece una solución intuitiva de gestión y análisis con visibilidad de extremo a extremo, Registro e informes para SMB.

Servicio FortiConverter

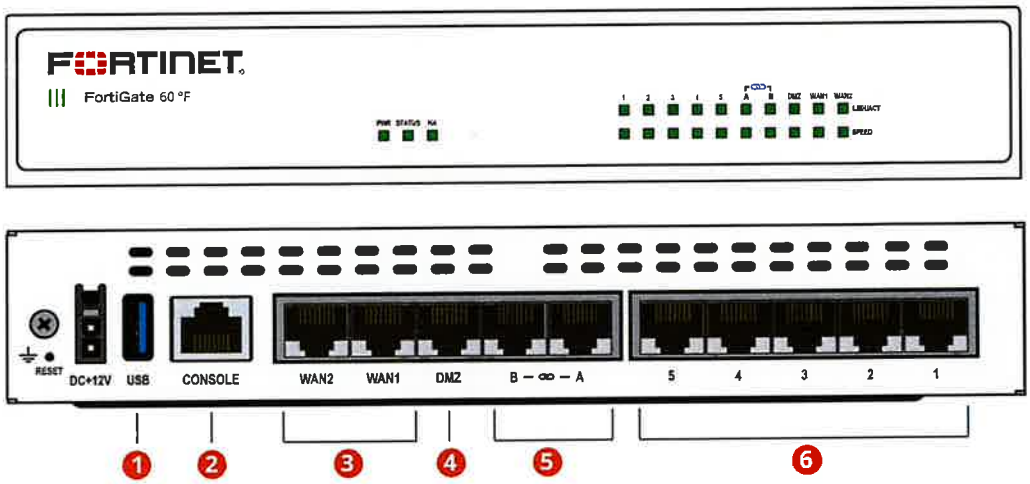
La migración a FortiGateNGFW es sencilla

El servicio FortiConverter ofrece una migración sin complicaciones para ayudar a las organizaciones a realizar una transición rápida y sencilla desde una amplia gama de firewalls heredados a NGFW FortiGate. El servicio elimina errores y redundancias mediante el empleo de las mejores prácticas con metodologías avanzadas y procesos automatizados. Las organizaciones pueden acelerar la protección de su red con la última tecnología FortiOS.

Hardware

FortiGate FortiWiFi 60F/61F

SoC4 | DE OFICINA | a/b/g/n/ac-W2 | 128 GB



Interfaces

1. 1 puerto USB
2. 1 x puerto de consola
3. 2 puertos WAN GE RJ45
4. 1 puerto DMZ GE RJ45
5. 2 puertos GE RJ45 FortiLink
6. 5 puertos internos GE RJ45

Características del hardware

Seguridad de la capa de acceso

El protocolo FortiLink permite que la seguridad y el acceso a la red converjan al integrar FortiSwitch en FortiGate como una extensión lógica del firewall. Estos puertos habilitados para FortiLink se pueden reconfigurar como puertos normales según sea necesario.

Factor de forma compacto y confiable

Diseñado para entornos pequeños, FortiGate puede instalarse en un escritorio o en la pared. Es pequeño, liviano y, sin embargo, altamente confiable, con un tiempo de inactividad superior entre fallas, lo que minimiza la posibilidad de interrupción de la red.

Presupuesto

	FORTIGADO 60F	FORTIGADO 61F	FORTIWIFI 60F	FORTIWIFI 61F
Especificaciones de hardware				
Puertos GERJ45WAN/DMZ	2 / 1	2 / 1	2 / 1	2 / 1
Puertos internos GERJ45	5	5	5	5
Puertos FortiLink GERJ45 (predeterminados)	2	2	2	2
Interfaz inalámbrica	—	—	Radio única (2,4 GHz/5 GHz), 802.11 a/b/g/n/ac-W2	Radio única (2,4 GHz/5 GHz), 802.11 a/b/g/n/ac-W2
Puertos USB	1	1	1	1
Consola (RJ45)	1	1	1	1
Almacenamiento interno	—	1 x SSD de 128 GB	—	1 x SSD de 128 GB
Módulo de plataforma confiable (TPM)	—	—	—	—
Bluetooth de bajo consumo (BLE)	—	—	—	—
Firmware firmadoConmutador de hardware	—	—	—	—
Rendimiento del sistema: combinación de tráfico empresarial				
Rendimiento IPS[2]	1,4 Gbps			
Rendimiento de NGFW[2,4]	1 Gbps			
Protección contra amenazasRendimiento[2,5]	700 Mbps			
Rendimiento del sistema				
Rendimiento del firewall (paquetes UDP de 1518/512/64 bytes)	10/10/6 Gbps			
Latencia del firewall (paquetes UDP de 64 bytes)	[illegible]			
Rendimiento del firewall (paquetes por segundo)	[illegible]			
Sesiones concurrentes (TCP)	700 000			
Nuevas sesiones por segundo (TCP)	35 000			
Políticas de firewall	2000			
Rendimiento de IPsecVPN (512 bytes)[1]	6,5 Gbps			
Túneles IPsecVPNTuneles de puerta de enlace a puerta de enlace	200			
Túneles IPsecVPNTuneles de cliente a puerta de enlace	500			
Rendimiento de SSL-VPN[6]	900 Mbps			
Usuarios de SSL-VPNUsimultáneos[6] (RecomendadoMáximo,Modo Túnel)	200			
Rendimiento de inspección SSL (IPS, HTTPS promedio)[3]	630 Mbps			
Inspección SSLCPS (IPS, promedio HTTPS)[3]	400			
Inspección SSLSesión simultánea (IPS, promedio HTTPS)[3]	55 000			
Rendimiento de control de aplicaciones (HTTP64K)[2]	1,8 Gbps			
Rendimiento CAPWAP (HTTP64K)	8 Gbps			
Dominios virtuales (predeterminado/máximo)	10 / 10			
Número máximo de FortiSwitches compatibles	24			
Número máximo de FortiAP (total/modo túnel)	64 / 32			
Número máximo de FortiTokens	500			
Configuraciones de alta disponibilidad	Activo-activo, activo-pasivo, agrupamiento			
Dimensiones				
Alto x Ancho x Largo (pulgadas)	1,5 x 8,5 x 6,3			
Alto x Ancho x Largo (mm)	38,5 x 216 x 160 mm			
Peso	2,23 libras (1,01 kg)			
Factor de forma	De oficina			

Nota: Todos los valores de rendimiento son "hasta" y varían según la configuración del sistema.

[1] La prueba de rendimiento de VPN IPsec utiliza AES256-SHA256.

[2] IPS (Enterprise Mix), Control de aplicaciones, NGFW y Protección contra amenazas se miden con el registro habilitado.

[3] Los valores de rendimiento de inspección SSL utilizan un promedio de sesiones HTTPS de diferentes Suites de cifrado.

[4] El rendimiento de NGFW se mide con Firewall, IPS y Control de aplicaciones habilitados.

[5] El rendimiento de protección contra amenazas se mide con Firewall, IPS, Control de aplicaciones y Protección contra malware habilitados.

[6] SSL VPN no compatible con FortiOS 7.6.0 y superiores.

Presupuesto

	FORTIGADO 60F	FORTIGADO 61F	FORTIWIFI 60F	FORTIWIFI 61F
Entorno operativo y certificaciones				
Potencia nominal	12 V CC, 3 A			
Potencia requerida	Alimentado por un adaptador de corriente CC externo, 100-240 V CA, 50/60 Hz			
Corriente máxima	100 V CA/1,0 A, 240 V CA/0,6 A			
Consumo de energía (promedio/máximo)	10,17 W / 12,43 W	17,2 W / 18,7 W	17,2 W / 18,7 W	17,5 W / 19,0 W
Disipación de calor	42,4 BTU/hora	42,4 BTU/hora	63,8 BTU/hora	64,8 BTU/hora
Temperatura de funcionamiento	32 °F a 104 °F (0 °C a 40 °C)			
Temperatura de almacenamiento	- 31 °F a 158 °F (-35 °C a 70 °C)			
Humedad	10% a 90% sin condensación			
Nivel de ruido	Sin ventilador 0 dBA			
Altitud de operación	Hasta 7400 pies (2250 m)			
Cumplimiento	FCC, CIEM, CE, RCM, VCCI, BSMI, UL/cUL, CB			
Certificaciones	USGv6/IPv6			
Especificaciones de la radio				
Múltiples usuarios (MU)MIMO	—	—	3x3	
Velocidades máximas de WI-FI	—	—	1300 Mbps a 5 GHz, 450 Mbps a 2,4 GHz	
Potencia máxima de transmisión	—	—	20 dBm	
Ganancia de antena	—	—	3,5 dBi a 5 GHz, 5 dBi a 2,4 GHz	

Suscripciones

Categoría de servicio	Oferta de servicios	A la carta	Paquetes: Empresa Protección	Paquetes: Amenaza unificada Protección	Paquetes: Amenaza avanzada Protección
Seguridad FortiGuard Servicios	IPS: direcciones URL maliciosas/de botnets	•	•	•	•
	Protección contra malware (AMP): antivirus, dominios de botnets, malware móvil, protección contra brotes de virus, desarme y reconstrucción de contenido1, Anti-virus heurístico basado en IA, FortiGateCloudSandbox	•	•	•	•
	Filtrado de URL, DNS y vídeo: URL, DNS y vídeo3Filtrado, certificado malicioso	•	•	•	
	Anti-spam		•	•	
	Prevención de malware en línea basada en IA3	•	•		
	Prevención de pérdida de datos (DLP)1	•	•		
	AttackSurfaceSecurity: detección de dispositivos de IoT, correlación de vulnerabilidades de IoT y aplicación de parches virtuales, calificación de seguridad, OutbreakCheck	•	•		
	OTSecurity: detección de dispositivos OT, correlación de vulnerabilidades OT y aplicación de parches virtuales, control de aplicaciones OTA e IPS1	•			
	Control de aplicaciones		incluido con la suscripción a FortiCare		
	CASB en línea3		incluido con la suscripción a FortiCare		
SD-WAN y SASE Servicios	Monitoreo de calidad y ancho de banda subyacente de SD-WAN	•			
	SD-WANOverlay como servicio	•			
	Conector SD-WAN para acceso privado seguro FortiSASE	•			
	Conector SASE para administración de borde segura FortiSASES (con ancho de banda de 10 Mbps)2	•			
NOC y SOC Servicios	Servicio FortiConverter para conversión de configuración única	•	•		
	Servicio FortiGate administrado: disponible las 24 horas, los 7 días de la semana, con expertos de Fortinet NOC que realizan la configuración de dispositivos, la red y la gestión de cambios de políticas	•			
	FortiGateCloud: gestión, análisis y retención de registros durante un año	•			
	FortiManagerCloud	•			
	FortiAnalyzerCloud	•			
	FortiGuardSOCaaS: monitoreo de registros administrado, clasificación de incidentes y servicio de escalamiento SOC basado en la nube las 24 horas, los 7 días de la semana	•			
Hardware y Soporte de software	Elementos esenciales de FortiCare1	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Servicios básicos	Detección de dispositivos y sistemas operativos, GeoIP, Certificados CA confiables, IP de servicios de Internet y botnets, DDNS (v4/v6), Protección local, PSIRTCheck, Anti-Phishing		Incluido con la suscripción a FortiCare		

1. Todas las funciones disponibles cuando se ejecuta FortiOS 7.4.1.

2. Sólo modelos de escritorio.

3. No disponible para las series FortiGate/FortiWiFi 40F, 60E, 60F, 80E y 90E desde la versión 7.4.4 en adelante.

Paquetes de seguridad con tecnología de inteligencia artificial FortiGuard para FortiGate

Los paquetes de seguridad con tecnología de inteligencia artificial de FortiGuard ofrecen una selección completa y meticulosamente seleccionada de servicios de seguridad para combatir amenazas conocidas, desconocidas, de día cero y emergentes basadas en inteligencia artificial. Estos servicios están diseñados para evitar que el contenido malicioso vulnere sus defensas, proteger contra amenazas basadas en la web, proteger dispositivos en entornos de TI/OT/IoT y garantizar la seguridad de aplicaciones, usuarios y datos. Todos los paquetes incluyen los servicios premium de FortiCare con disponibilidad las 24 horas, los 7 días de la semana, los 365 días del año, respuesta en una hora para problemas críticos y respuesta al siguiente día hábil para asuntos no críticos.

Servicios FortiCare

Fortinet prioriza el éxito del cliente a través de los servicios FortiCare, optimizando la solución Fortinet Security Fabric. Nuestros servicios integrales de ciclo de vida incluyen diseño, implementación, operación, optimización y evolución. FortiCare Elite, una de las ofertas de servicios, proporciona acuerdos de nivel de servicio mejorados y una rápida resolución de problemas con un equipo de soporte dedicado. Esta opción de soporte avanzado incluye un soporte extendido de fin de ingeniería de 18 meses, que ofrece flexibilidad y acceso al portal intuitivo FortiCare Elite para una vista unificada del estado de seguridad y del dispositivo, agilizando la eficiencia operativa y maximizando el rendimiento de la implementación de Fortinet.

Información de pedidos

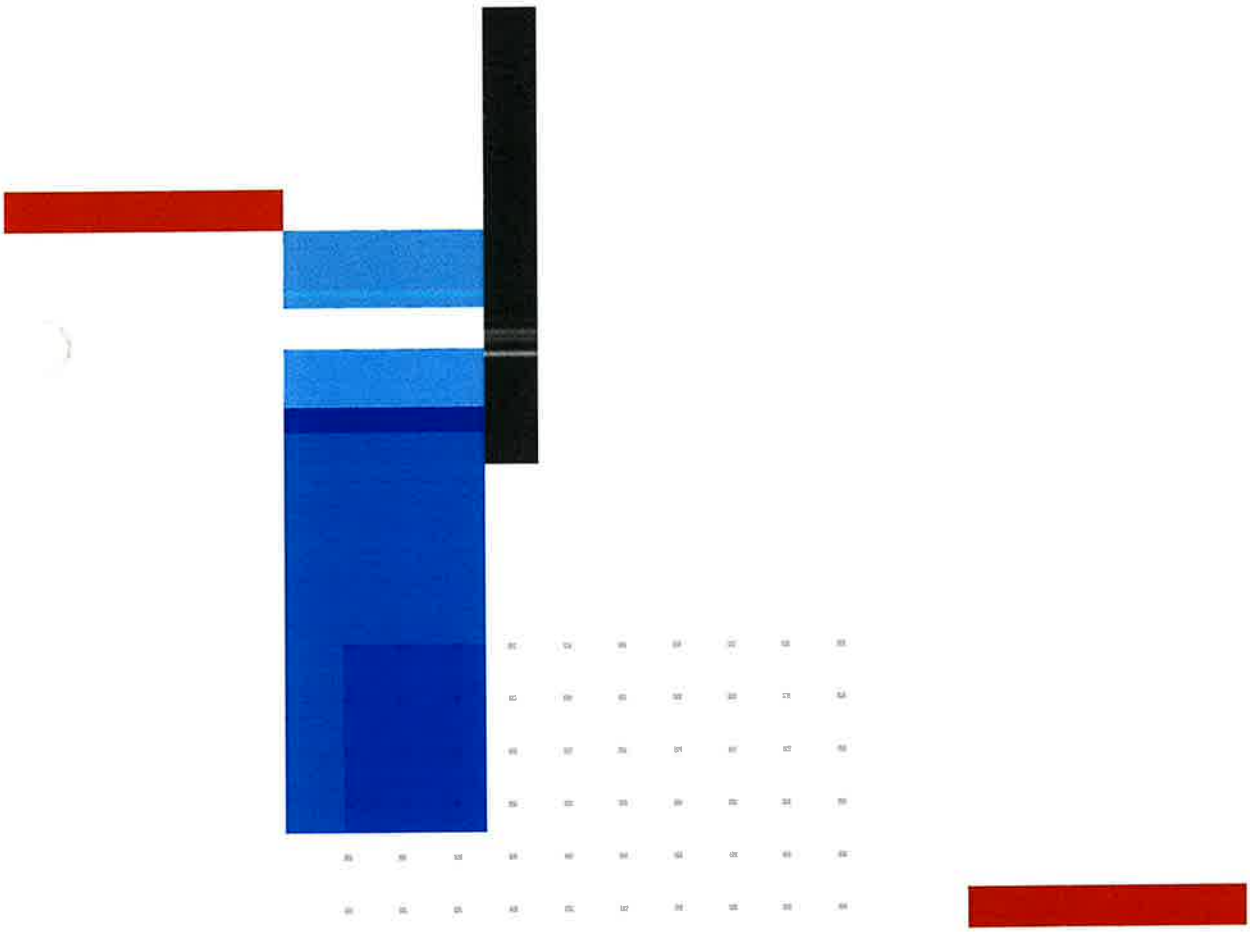
Producto	Código SKU	Descripción
FortiGate 60F	FG-60F	10 puertos GE RJ45 (incluidos 7 puertos internos, 2 puertos WAN, 1 puerto DMZ).
FortiGate 61F	FG-61F	10 puertos GE RJ45 (incluidos 7 puertos internos, 2 puertos WAN, 1 puerto DMZ), almacenamiento integrado SSD de 128 GB.
FortiWiFi 60F	FWF-60F-[RC]	10 puertos GE RJ45 (incluidos 7 puertos internos, 2 puertos WAN, 1 puerto DMZ), inalámbrico (802.11 a/b/g/n/ac-W2).
FortiWiFi 61F	FWF-61F-[RC]	10 puertos GE RJ45 (incluidos 7 puertos internos, 2 puertos WAN, 1 puerto DMZ), conexión inalámbrica (802.11 a/b/g/n/ac-W2), almacenamiento integrado SSD de 128 GB.
Accesorios opcionales		
Bandeja para montaje en rack	SP-RACKTRAY-02	Las bandejas para montaje en bastidor para todos los modelos de escritorio de las series E y F de FortiGate son compatibles con SP-RackTray-01. Para obtener una lista de productos FortiGate compatibles, visite nuestro sitio web de documentación, docs.fortinet.com.
Adaptador de corriente alterna	SP-FG60E-PDC-5	Paquete de 5 adaptadores de alimentación de CA para FG/FWF 60E/61E, 60F/61F y 80E/81E.
Kit de montaje en pared	SP-FG60F-MONTAJE-20	Paquete de 20 kits de montaje en pared para las series FG/FWF-60F y FG/FWF-80F.

[RC] = código regional: A, B, D, E, F, I, J, N, P, S, V e Y.

Visita https://www.fortinet.com/resources/ordering-guides para guías de pedidos relacionadas.

Política de Responsabilidad Social Corporativa de Fortinet

Fortinet se compromete a impulsar el progreso y la sostenibilidad para todos a través de la ciberseguridad, con respeto por los derechos humanos y prácticas comerciales éticas, haciendo posible un mundo digital en el que siempre pueda confiar. Usted declara y garantiza a Fortinet que no utilizará los productos y servicios de Fortinet para participar o apoyar de ninguna manera violaciones o abusos de los derechos humanos, incluidos aquellos que impliquen censura ilegal, vigilancia, detención o uso excesivo de la fuerza. Los usuarios de los productos de Fortinet deben cumplir con lasAcuerdo de licencia de usuario final de Fortinety denunciar cualquier sospecha de violación del EULA a través de los procedimientos descritos en elPolítica de denuncia de irregularidades de Fortinet.



14 de noviembre de 2024