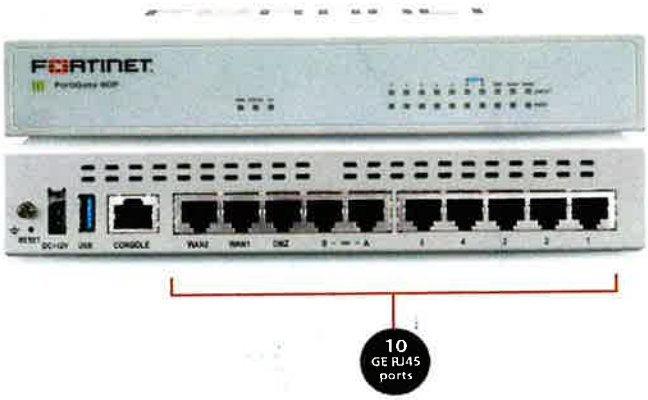
Viernes 10 febrero de 2025
Santo Domingo, República Dominicana

Junta Central Electoral
Av. 27 de febrero esquina, Av. Gregorio
Luperón, Santo Domingo 11113
NO.JCE-CCC-CP-2025-0004
Adquisición de Switches Fortigate FG-60F

Asunto: Ficha Técnica del Equipo Ofertado

1. **FortiGate-60F Hardware plus 24×7 FortiCare and FortiGuard Unified Threat Protection (UTP)**



- **Rendimiento de IPS 2:** 1,4 Gbps
- **Rendimiento NGFW 2:** 1 Gbps
- **Rendimiento de protección contra amenazas 2:** 700 Mbps
- **Rendimiento del firewall (paquetes UDP de 1518/512/64 bytes):** 10/10/6 Gbps
- **Latencia del firewall (paquetes UDP de 64 bytes):** 3,3 µs
- **Rendimiento del firewall (paquetes por segundo):** 9 Mpps
- **Sesiones Simultáneas (TCP):** 700 000
- **Nuevas sesiones/segundo (TCP):** 35 000

- **Políticas de cortafuegos:** 2000
- **Rendimiento de VPN IPsec (512 bytes) 1:** 6,5 Gbps
- **Túneles VPN IPsec de puerta de enlace a puerta de enlace:** 200
- **Túneles VPN IPsec de cliente a puerta de enlace:** 500
- **Rendimiento SSL-VPN6:** 900 Mbps
- **Usuarios simultáneos de SSL-VPN6 (máximo recomendado, modo túnel):** 200
- **Rendimiento de inspección SSL (IPS, HTTPS promedio) 3:** 630 Mbps
- **Inspección SSL CPS (IPS, HTTPS promedio) 3:** 400
- **Sesión simultánea de inspección SSL (IPS, HTTPS promedio) 3:** 55 000
- **Rendimiento de control de aplicaciones (HTTP 64K) 2:** 1,8 Gbps
- **Rendimiento CAPWAP (HTTP 64K):** 8 Gbps
- **Dominios virtuales (predeterminado/máximo):** 10/10
- **Número máximo de FortiSwitches admitidos:** 24
- **Número máximo de FortiAP (modo total/túnel):** 64/32
- **Número máximo de FortiTokens:** 500
- **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)

2. FortiCare and FortiGuard Unified Threat Protection (UTP) 24/7 vigente por 1 año

- Control de Aplicaciones NGFW
- IPS
- Antivirus
- Botnet
- IP/Reputación de Dominio
- Seguridad Móvil
- Filtrado Web
- Antispam
- Nube FortiSandbox
- Protección contra Brotes de Virus
- Desarma de Contenido y Reconstrucción
- 24x7x365 Servicios de Soporte de FortiCare

Junta Central Electoral
Garantía de Identidad y Democracia

10 de febrero de 2025

JUNTA CENTRAL ELECTORAL

ESPECIFICACION DE CANTIDAD

JCE-CCC-CP-2025-0004

Item	Descripción de Bien, Obra o Servicio	Unidad	Cantidad
1	**FortiGate** **Marca y Modelo:** Fortinet **(FortiGate-60F)** **General:** **Almacenamiento interno:** 1x 128 **Rendimiento de IPS:** 1.4 Gbps **Rendimiento del firewall:** 10/10/6 Gbps **Firewall Latency:** 3.3 µs **10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port).** **Incluye** 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) **Vigencia por 12 meses**	UD	75

TCO NETWORKS, SRL
TCO NETWORKS Connecting the future
Depto. de Ventas

Luis G. Portes
Gerente

Junta Central Electoral
Garantía de Identidad y Democracia

10 de Febrero 2025
Santo Domingo,

JUNTA CENTRAL ELECTORAL

CARTA DE ENTREGA

Distinguidos señores:
Contrataciones y compra.

Mediante la presente hacemos constar que en caso de salir adjudicados en el proceso de compra referencia **JCE-CCC-CP-2025-0004** tiempos de entrega son los establecidos en el siguiente cuadro:

Item	Descripción de Bien, Obra o Servicio	Unidad	Cantidad	Tiempo de Entrega
1	**FortiGate** **Marca y Modelo:** Fortinet **(FortiGate-60F)** **General:** **Almacenamiento interno:** 1x 128 **Rendimiento de IPS:** 1.4 Gbps **Rendimiento del firewall:** 10/10/6 Gbps **Firewall Latency:** 3.3 µs **10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port).** **Incluye** 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) **Vigencia por 12 meses**	UD	75	5 a 6 semanas

Actividades y tiempo indicados comienzan una vez recibida la orden de compra.

Los tiempos mencionados en la tabla anterior son contemplados para entrega en el horario de 09:00 A.M. a 5:00 P.M

Se despide,

Luis G. Portes
Gerente

TCO NETWORKS, SRL
TCO NETWORKS Connecting the future
Depto. de Ventas
RNC 1-31-16528-5

Junta Central Electoral
Garantía de Identidad y Democracia

10 de Febrero de 2025,
Santo Domingo, República Dominicana

JUNTA CENTRAL ELECTORAL

CARTA DE GARANTÍA

Distinguidos señores: Mediante la presente hacemos constar que en caso de salir adjudicados en el proceso de compra referencia: **JCE-CCC-CP-2025-0004** el tiempo de garantía son los establecidos en el **siguiente cuadro:**

Item	Descripción de Bien, Obra o Servicio	Unidad	Cantidad	Tiempo de Garantia
1	**FortiGate** **Marca y Modelo:** Fortinet **(FortiGate-60F)** **General:** **Almacenamiento interno:** 1x 128 **Rendimiento de IPS:** 1.4 Gbps **Rendimiento del firewall:** 10/10/6 Gbps **Firewall Latency:** 3.3 µs **10 x GE RJ45 ports (including 7 x Internal Ports, 2 x WAN Ports, 1 x DMZ Port).** **Incluye** 1 Year FortiCare Premium and FortiGuard Unified Threat Protection (UTP) **Vigencia por 12 meses**	UD	75	1 año

Dichos tiempos comienzan una vez recibido los equipos conforme.

Sin nada más que agregar,

Luis G. Portes
Gerente

TCO NETWORKS, SRL
TCO NETWORKS Connecting the future
Depto. de Ventas
RNC 1-31-16526-5

Junta Central Electoral
Garantía de Identidad y Democracia

10 de Febrero de 2025,
Santo Domingo, República Dominicana

Señores

JUNTA CENTRAL ELECTORAL

Atención

GERENCIA DE COMPRAS Y CONTRATACIONES

Asunto

CARTA CONDICIONES DE PAGO

Por medio de la presente, la empresa **TCO NETWORKS** nos comprometemos en caso de ser adjudicado en el proceso: **JCE-CCC-CP-2025-0004**referente a: **"ADQUISICION DE SWITCHES",** con base en el criterio de descentralización de la gestión operativa, otorgamos un crédito a la Entidad de **Sesenta (60) días** luego de emitida la factura y aceptado conforme los equipos.

Agradeciendo el que nos tomen en cuenta, nos despedimos muy cordialmente.

Luis G. Porte
Gerente

TCO NETWORKS, SRL
TCO NETWORKS Connecting the future
Depto. de Ventas
RNC 1-31-16526-5

Certificado de Revendedor Autorizado

Fecha: 6 de febrero de 2025
Junta Central Electoral

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: Tco Networks SRL

con domicilio social en: Eugenio Deschamps 11, Santo Domingo, D. N. 10131, Dominican Republic;

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

- Nivel de contrato: Select
- Modelo de negocio: Integrator

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.

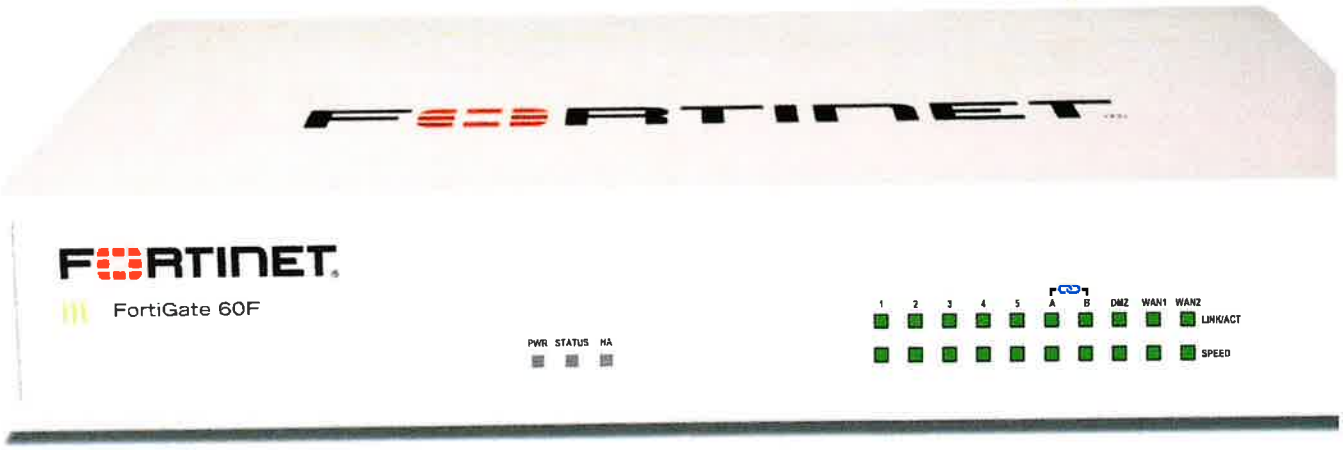
La validez de este Certificado se encuentra sujeta a que el FortiPartner mantenga su contrato vigente con Fortinet y que éste cumpla las políticas y directrices de Fortinet. El programa de partners de Fortinet y sus directrices están disponibles en http://www.fortinet.com/partners/partner_program/fpp.html. 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

TCO NETWORKS, SRL
TCO NETWORKS
Connecting the future
Depto. de Ventas
RNC 1-31-16524-3

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, y puede 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.

FortiGate FortiWiFi Serie 60F



Reflejos

Cuadrante mágico de Gartner® Líderes para ambas redes Cortafuegos y SD-WAN

Rendimiento incomparable habilitado por el ASIC patentado de Fortinet y el Sistema operativo FortiOS

Protección de nivel empresarial con FortiGuard impulsado por IA Servicios de seguridad

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

SD-WAN inclusivo y controlador inalámbrico en cada Dispositivo FortiGate sin costo costo extra

Amplio portafolio para cualquier presupuesto y necesidad empresarial

Firewall convergente de próxima generación y SD-WAN

Las series FortiGate y FortiWiFi 60F integran firewall, SD-WAN y seguridad en un solo dispositivo. dispositivo, lo que los hace perfectos 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 seguridad coordinada y automatizada.
Protección contra amenazas de extremo a extremo en tiempo real.

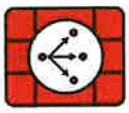
La familia 60F está construida sobre el ASIC patentado basado en SD-WAN, que ofrece una experiencia inigualable. Rendimiento superior al de las CPU tradicionales con un menor costo y un menor consumo de energía. Este diseño específico para aplicaciones y el procesador multinúcleo integrado aceleran aún 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

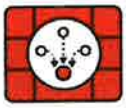
Protección perimetral

- Proteja las redes del tráfico malicioso, protéjase contra amenazas basadas en archivos, bloquee ataques basados en la web y proteja aplicaciones y datos con FortiGuard AI-Powered integrado de forma nativa.
  Servicios de seguridad
- 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 gestión 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 retrasos en el acceso a las aplicaciones y acelerar el rendimiento de la superposición independientemente de la ubicación
- Mejora el trabajo híbrido con una solución SASE integral mediante la integración de la nube SD-WAN con borde de servicio de seguridad (SSE)
- Logra eficiencias operativas a cualquier escala a través de la automatización, análisis profundos y autogestión.
  cicatrización



Sucursal segura

- La plataforma Fortinet Security Fabric permite que los NGFW de FortiGate detecten y detecten automáticamente
  Dispositivos IoT seguros para una incorporación más rápida a las sucursales
- Totalmente integrado con los conmutadores Ethernet seguros FortiSwitch y los puntos de acceso FortiAP, FortiGate 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 perfectamente 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 el caso de fallos de hardware o interrupciones de la red

Servicios de seguridad impulsados por IA de FortiGuard

Los servicios de seguridad impulsados por IA de FortiGuard son 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 basados en 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 correos electrónicos) y comunicaciones de botnets. El filtrado de DNS bloquea todo el espectro de DNS ataques basados en URL, 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 anti-botnets protegen contra la actividad de botnets y los ataques DDoS. FortiGuard Labs bloquea más de 500 millones de enlaces maliciosos/phishing/ envía spam a URL semanales 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 integradas Las capacidades de seguridad de OT detectan amenazas dirigidas a la infraestructura de OT, realizan correlaciones de vulnerabilidad, aplican parches virtuales y utilizan decodificadores de protocolo específicos de la industria para una seguridad robusta. Defensa de entornos y dispositivos OT.

Disponible en

Aparato

Virtual

Alojado

Nube

Recipiente

FortiOS en todas partes

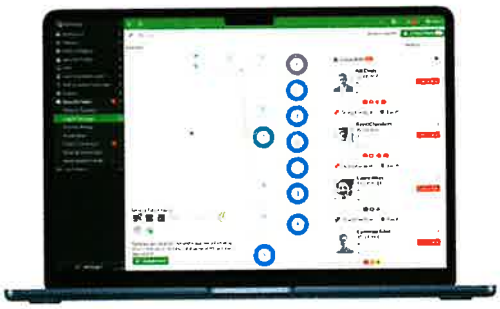
FortiOS, el sistema operativo de seguridad de red en tiempo real de Fortinet

FortiOS es el sistema operativo que impulsa la plataforma Fortinet Security Fabric, lo que permite la aplicación de políticas de seguridad y visibilidad integral en toda la superficie de ataque.
FortiOS ofrece 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.

AI 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



Vulnerabilidades de puntos finales de uso Intuitivo y sencillo

Ver en la red y

Vista integral del rendimientode la red, la seguridad y el estado del sistema

ASIC de Fortinet: seguridad inigualable, 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, lo que mejora drásticamente el rendimiento de estas funciones que los competidores tradicionalmente implementan en el software.

ASIC seguro SD-WAN SP4

- Combina una CPU basada en RISC con contenido SPU patentado de Fortinet y procesadores de red para un rendimiento inigualable
- Ofrece la identificación y dirección de aplicaciones más rápida de la industria para lograr negocios eficientes. operaciones
- 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 aceleración y conectividad de punto de acceso y conmutador integrado

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 la 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.

FortiGate Cloud: 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 ayudaa administrar redes sin esfuerzo: generar scripts de configuración y políticas, solucionar problemas y ejecutar acciones recomendadas

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

Servicio FortiConverter

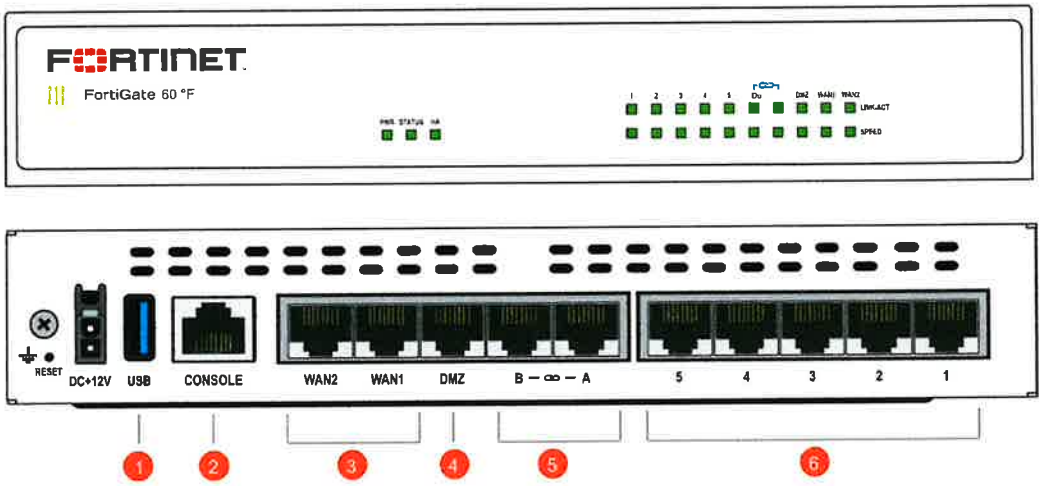
La migración a FortiGate NGFW se hizo fácil

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

	FORTIGATO 60F	FORTIGATO 61F	FORTIWIFI 60F	FORTIWIFI 61F
Especificaciones de hardware				
Puertos WAN/DMZ RJ45 de GE	2 / 1	2 / 1	2 / 1	2 / 1
Puertos internos GE RJ45	5	5	5	5
Puertos GE RJ45 FortiLink (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)	—	—	—	—
Conmutador de hardware con firmware firmado	—	—	—	—
Rendimiento del sistema: combinación de tráfico empresarial				
Rendimiento de IPS [2]		1,4 Gbps		
Rendimiento de NGFW 2, 4		1 Gbps		
Rendimiento de protección contra amenazas 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/Segunda (TCP)		35 000		
Políticas de firewall		2000		
Rendimiento de VPN IPsec (512 bytes) [1]		6,5 Gbps		
Túneles VPN IPsec de puerta de enlace a puerta de enlace		200		
Túneles VPN IPsec de cliente a puerta de enlace		500		
Rendimiento de SSL-VPN6		900 Mbps		
Usuarios simultáneos de SSL-VPN6 (Máximo recomendado, modo túnel)		200		
Rendimiento de inspección SSL (IPS, HTTPS promedio) 3		630 Mbps		
Inspección SSL CPS (IPS, HTTPS promedio) 3		400		
Inspección SSL de sesión concurrente (IPS, HTTPS promedio) 3		55 000		
Rendimiento de control de aplicaciones (HTTP 64K) 2		1,8 Gbps		
Rendimiento CAPWAP (HTTP 64K)		8 Gbps		
Dominios virtuales (predeterminado/máximo)		10 / 10		
Número máximo de FortiSwitches admitidos		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 conjuntos de cifrado.

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

5 El rendimiento de la protección contra amenazas se mide con Firewall, IPS, Control de aplicaciones y Protección contra malware habilitada.

6 SSL VPN no compatible con FortiOS 7.6.0 y superior

Presupuesto

	FORTIGATO 60F	FORTIGATO 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 °F)		
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				
MIMO de múltiples usuarios (MU)	—	—	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 la 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 y de botnets	•	•	•	•
	Protección antimalware (AMP): antivirus, dominios de botnets, malware móvil, Protección contra brotes de virus, Desarme y reconstrucción de contenido 3, Anti-virus heurístico basado en IA, FortiGate Cloud Sandbox	•	•	•	•
	Filtrado de URL, DNS y vídeo — Filtrado de URL, DNS y vídeo 3 , Certificado malicioso	•	•	•	
	Anti-spam		•	•	
	Prevención de malware en línea basada en IA 3	•	•		
	Prevención de pérdida de datos (DLP) 1	•	•		
	Seguridad de la superficie de ataque: detección de dispositivos IoT, vulnerabilidades de IoT Correlación y parches virtuales, calificación de seguridad, verificación de brotes	•	•		
	Seguridad OT: detección de dispositivos OT, correlación de vulnerabilidades OT y Aplicación de parches virtuales, control de aplicaciones OT e IPS 1	•			
	Control de aplicaciones		incluido con la suscripción a FortiCare		
	CASB 3 en línea		incluido con la suscripción a FortiCare		
SD-WAN y SASE Servicios	Monitoreo de calidad y ancho de banda subyacente de SD-WAN	•			
	Superposición SD-WAN como servicio	•			
	Conector SD-WAN para acceso privado seguro FortiSASE	•			
	Conector SASE para FortiSASE Secure Edge Management (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 del dispositivo, la red y la gestión de cambios de políticas	•			
	FortiGate Cloud: gestión, análisis y retención de registros durante un año	•			
	Nube FortiManager	•			
	Nube FortiAnalyzer	•			
	FortiGuard SOCaaS monitoreo de registros administrado basado en la nube las 24 horas, los 7 días de la semana, clasificación de incidentes y servicio de escalamiento de SOC	•			
Hardware y Soporte de software	Elementos esenciales de FortiCare 2	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Servicios básicos	Detección de dispositivos y sistemas operativos, GeoIP, certificados CA de confianza, Internet Servicios e IP de botnets, DDNS (v4/v6), protección local, comprobación PSIRT, Antiphishing		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 de FortiGuard para FortiGate

Los paquetes de seguridad potenciados por IA 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 IA. 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 brinda 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

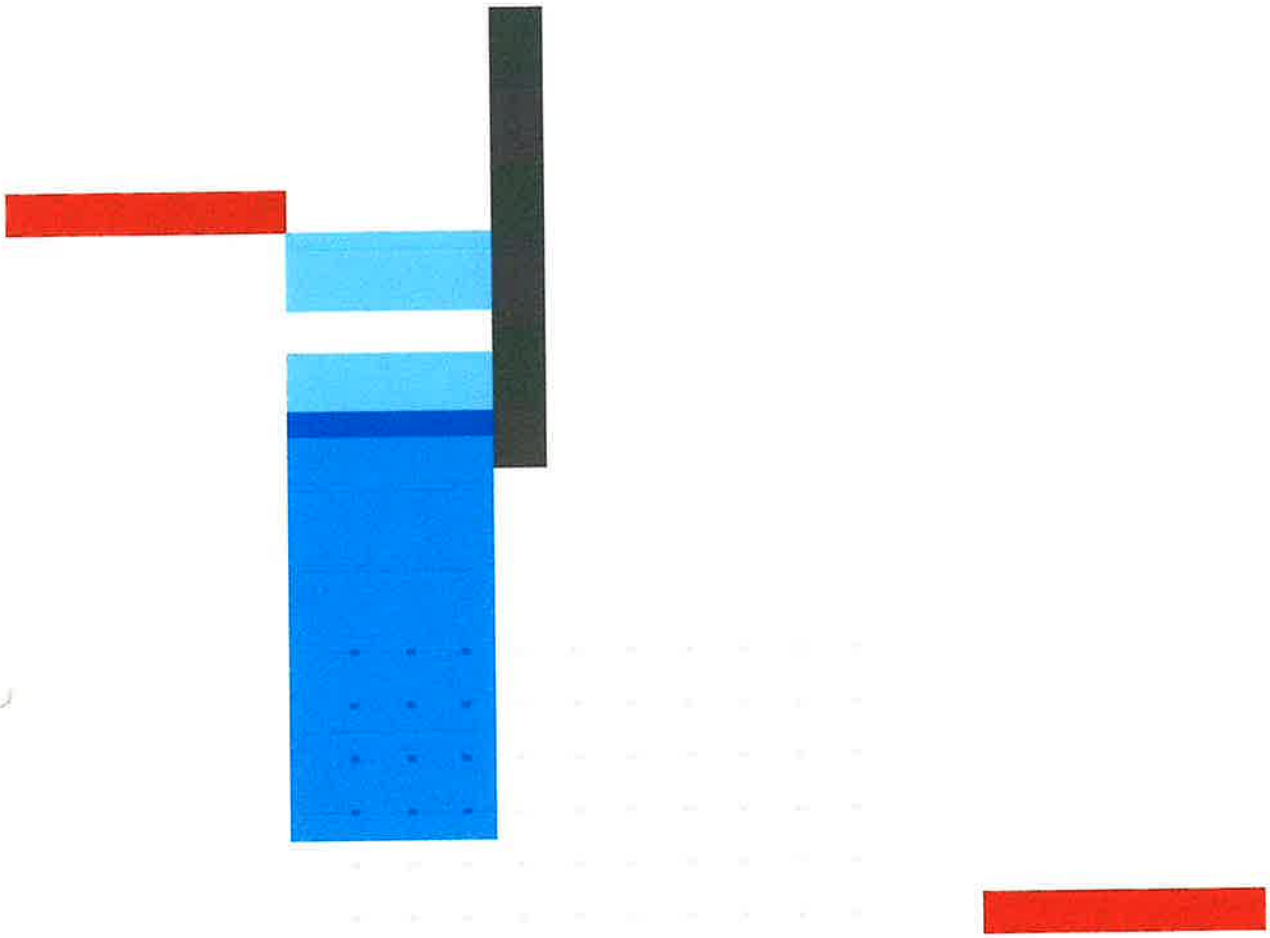
Producto	SKU	Descripción
FortiGate 60F	FG-60F	10 puertos GE RJ45 (incluidos 7 puertos internos, 2 puertos WAN, 1 puerto DMZ)
FortiGate 61F	FG-61F	10 puertos GE RJ45 (incluidos 7 puertos internos, 2 puertos WAN, 1 puerto DMZ), almacenamiento SSD integrado de 128 GB
FortiWiFi 60F	FWF-60F-[RC]	10 puertos GE RJ45 (incluidos 7 puertos internos, 2 puertos WAN, 1 puerto DMZ), conexión inalámbrica (802.11 a/b/g/n/ac-W2)
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 de montaje en bastidor para todos los modelos de escritorio de las series E y F de FortiGate son compatibles con SP-RackTray-01. Para ver la lista de modelos compatibles, consulte la página 10. Productos FortiGate, 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/8
Kit de montaje en pared	SP-FG60F-MOUNT-20	Paquete de 20 kits de montaje en pared para sistemas 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 el EULA de Fortinet e informar cualquier sospecha de violación del EULA a través de los procedimientos descritos en la Política de denuncia de irregularidades de Fortinet .



FORTINET

www.fortinet.com

14 de noviembre de 2024

FGRWP-POF-DAT-R44-2024