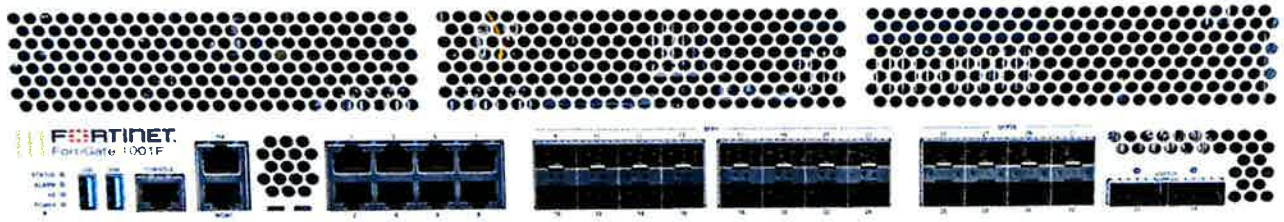
Serie FortiGate 1000F

FG-1000F y FG-1001F



Reflejos

Cuadrante Mágico de Gartner Líder de ambas Redes Cortafuegos y SD-WAN.

Redes basadas en seguridad FortiOS ofrece seguridad y redes convergentes.

Rendimiento incomparable con procesadores / SPU / vSPU patentados de Fortinet.

Seguridad empresarial con servicios FortiGuard consolidados impulsados por IA/ML.

Seguridad de hiperescala para asegurar cualquier borde a cualquier escala.

Alto rendimiento con flexibilidad

La serie FortiGate 1000F permite a las organizaciones construir redes basadas en seguridad que pueden integrar la seguridad profundamente en su centro de datos y en su arquitectura de TI híbrida para proteger cualquier borde a cualquier escala.

Impulsada por un amplio conjunto de servicios FortiGuard basados en AI/ML y una plataforma de estructura de seguridad integrada, la serie FortiGate 1000F ofrece protección contra amenazas coordinada, automatizada y de extremo a extremo en todos los casos de uso.

FortiGate 1000F, la primera aplicación integrada de Zero Trust Network Access ZTNA de la industria dentro de una solución NGFW, controla, verifica y facilita automáticamente el acceso de los usuarios a las aplicaciones, brindando una convergencia consistente con una experiencia de usuario perfecta.

IPS	NGFW	Protección contra amenazas	Interfaces
19 Gbps	15 Gbps	13 Gbps	Múltiples 10/1 GE RJ45, 100 GE QSFP28, 40 GE Ranuras QSFP+, 25 GE SFP28, 10 GE SFP+

Disponible en

Aparato

Virtual

Alojado

Nube

Envase

FortiOS en todas partes

FortiOS, el sistema operativo avanzado de Fortinet

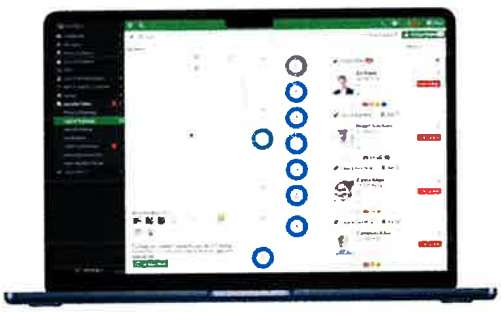
FortiOS permite la convergencia de redes y seguridad de alto rendimiento en Fortinet Security Fabric. Debido a que se puede implementar en cualquier lugar, ofrece una postura de seguridad consistente y consciente del contexto en entornos de red, endpoints y múltiples nubes.

FortiOS impulsa todas las implementaciones de FortiGate, ya sea un dispositivo físico o virtual, como contenedor o como servicio en la nube. Este modelo de implementación universal permite la consolidación de muchas tecnologías y casos de uso en un marco de gestión y política único y simplificado. Sus mejores capacidades construidas orgánicamente, su sistema operativo unificado y su ultra escalabilidad permiten a las organizaciones proteger todos los bordes, simplificar las operaciones y administrar sus negocios sin comprometer el rendimiento o la protección.

FortiOS amplía drásticamente la capacidad de Fortinet Security Fabric para ofrecer IA/
Los servicios basados en ML, la detección avanzada en línea de entornos aislados, la aplicación integrada de ZTNA y más, brindan protección en modelos de implementación híbrida para hardware, software y software como servicio con SASE.

FortiOS amplía la visibilidad y el control, garantiza la implementación y aplicación consistentes de políticas de seguridad y permite la administración centralizada en redes de gran escala con los siguientes atributos clave:

- Visores interactivos de topología y desglose que muestran el estado en tiempo real
- Corrección con un solo clic que brinda protección precisa y rápida contra amenazas y abusos
- El exclusivo sistema de puntuación de amenazas correlaciona las amenazas ponderadas con los usuarios para priorizar las investigaciones.



Intuitivo para visualizar en la red y fácil uso

vulnerabilidades de endpoints

Visibilidad con FOS: Firmas de aplicaciones

Servicio FortiConverter

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

Servicios FortiGuard

Seguridad impulsada por IA de FortiGuard

El rico conjunto de servicios de seguridad de FortiGuard contrarresta las amenazas en tiempo real utilizando protección coordinada impulsada por IA diseñada por investigadores de amenazas de seguridad, ingenieros y especialistas forenses de FortiGuard Labs.

Seguridad Web

URL, DNS (sistema de nombres de dominio) y filtrado de video avanzados entregados en la nube que brindan protección completa contra phishing y otros ataques web mientras cumplen con el cumplimiento.

Además, su servicio dinámico CASB (Cloud Access Security Broker) en línea se centra en proteger los datos SaaS empresariales, mientras que la inspección de tráfico ZTNA en línea y la verificación de postura ZTNA brindan control de acceso por sesión a las aplicaciones. También se integra con FortiClient Fabric Agent para extender la protección a usuarios remotos y móviles.

Seguridad del contenido

Las tecnologías avanzadas de seguridad de contenidos permiten la detección y prevención de amenazas conocidas y desconocidas y tácticas de ataque basadas en archivos en tiempo real. Con capacidades como CPRL (lenguaje compacto de reconocimiento de patrones), AV, Sandbox en línea y protección de movimiento lateral, lo convierten en una solución completa para abordar ransomware, malware y ataques basados en credenciales.

Seguridad del dispositivo

Las tecnologías de seguridad avanzadas están optimizadas para monitorear y proteger los dispositivos de TI, IIoT y OT (tecnología operativa) contra vulnerabilidades y tácticas de ataque basadas en dispositivos. Su inteligencia IPS validada casi en tiempo real detecta y bloquea amenazas conocidas y de día cero, proporciona visibilidad y control profundos de los protocolos ICS/OT/SCADA y proporciona políticas automatizadas basadas en identificación de patrones, segmentación y descubrimiento.

Herramientas avanzadas para SOC/NOC

Las herramientas avanzadas de administración de NAC y SOC adjuntas a su NGFW brindan un tiempo de activación simplificado y más rápido.

SOC como servicio

Incluye búsqueda y automatización de primer nivel, ubicación de registros, expertos en análisis de SOC las 24 horas al día, 7 días a la semana, funciones de firewall y terminales administradas y clasificación de alertas.

Mejores prácticas de seguridad de clasificación de tejido

Incluye parches virtuales en la cadena de suministro, datos actualizados sobre riesgos y vulnerabilidades para brindar decisiones comerciales más rápidas y remediación de situaciones de violación de datos.

Asegure cualquier borde a cualquier escala

Desarrollado por la Unidad de procesamiento de seguridad (SPU)

Los cortafuegos tradicionales no pueden proteger contra las amenazas actuales basadas en el contenido y la conexión porque dependen de hardware disponible en el mercado y de CPU de uso general, lo que provoca una brecha de rendimiento peligrosa. Los procesadores SPU personalizados de Fortinet brindan la potencia que necesita (hasta 520 Gbps) para detectar amenazas emergentes y bloquear contenido malicioso mientras garantiza que su solución de seguridad de red no se convierta en un cuello de botella en el rendimiento.

Ventaja ASIC

Procesador de red 7 NP7

Los procesadores de red operan en línea para ofrecer rendimiento y escalabilidad inigualables para funciones de red críticas. Fortinet

El innovador procesador de red SPU NP7 funciona en línea con las funciones de FortiOS para entregar:

- Firewall de hiperescala, sesión acelerada configuración y latencia ultrabaja
- Rendimiento líder en la industria para VPN, Terminación de VXLAN, registro de hardware y flujos de elefante

Procesador de contenido 9 CP9

Los procesadores de contenido actúan como coprocesadores para descargar el procesamiento de funciones de seguridad que requiere muchos recursos. La novena generación del procesador de contenido de Fortinet, el CP9, acelera las funciones de seguridad y descifrado SSL (incluido TLS 1.3) que requieren muchos recursos al tiempo que ofrece:

- Aceleración de coincidencia de patrones y Inspección rápida del tráfico en tiempo real para la identificación de aplicaciones.
- Pre-escaneo/pre-coincidencia de IPS, descarga de correlación de firmas y procesamiento antivirus acelerado

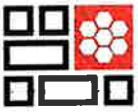
Servicios FortiCare

Fortinet se dedica a ayudar a nuestros clientes a tener éxito y cada año los servicios FortiCare ayudan a miles de organizaciones a aprovechar al máximo nuestra solución Fortinet Security Fabric. Nuestro portafolio de ciclo de vida ofrece servicios de diseño, implementación, operación, optimización y evolución. Los servicios Operate ofrecen el servicio FortiCare Elite a nivel de dispositivo con SLA mejorados para satisfacer las necesidades de nuestros clientes. necesidades operativas y de disponibilidad. Además, nuestros servicios personalizados a nivel de cuenta brindan una resolución rápida de incidentes y ofrecen atención proactiva para maximizar la seguridad y el rendimiento de las implementaciones de Fortinet.

Casos de uso

Firewall de próxima generación (NGFW)

- El conjunto de servicios de seguridad impulsados por IA de FortiGuard Labs, integrado de forma nativa con su NGFW: protege la web, el contenido y los dispositivos y protege las redes contra ransomware y ciberataques sofisticados
- La inspección SSL en tiempo real (incluido TLS 1.3) proporciona visibilidad completa de los usuarios, dispositivos y aplicaciones en toda la superficie de ataque
- La tecnología SPU (Unidad de procesamiento de seguridad) patentada de Fortinet proporciona protección de alto rendimiento líder en la industria



Segmentación

- La segmentación dinámica se adapta a cualquier topología de red para brindar verdadera seguridad de extremo a extremo, desde la sucursal hasta el centro de datos y en entornos de múltiples nubes.
- La segmentación VXLAN ultraescalable y de baja latencia une los dominios físicos y virtuales con reglas de firewall de capa 4
- Previene el movimiento lateral a través de la red con protección avanzada y coordinada de FortiGuard Security Services detecta y previene ataques conocidos, de día cero y ataques desconocidos

SD-WAN segura

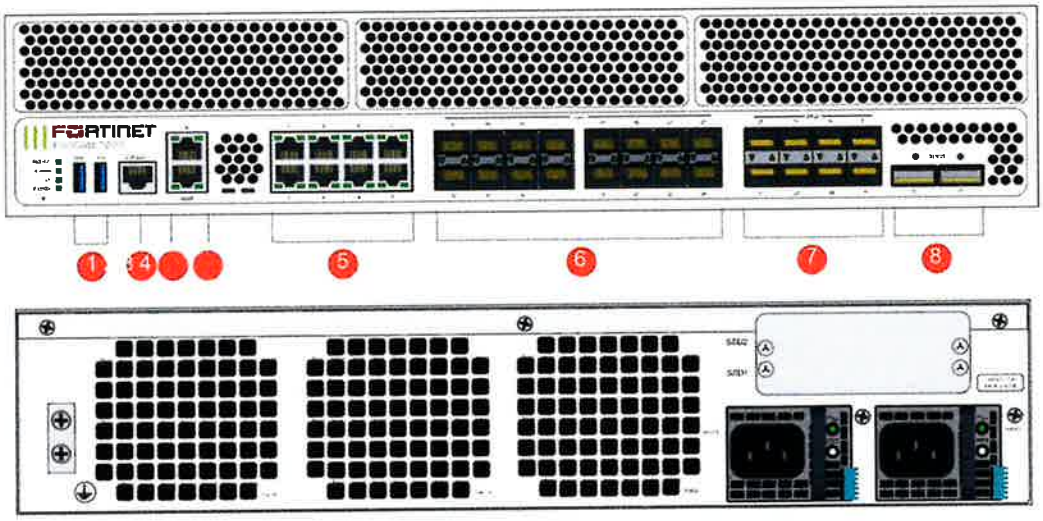
- FortiGate WAN Edge impulsado por un sistema operativo y un marco y sistemas de seguridad y administración unificados transforma y protege las WAN
- Ofrece una calidad superior de experiencia y una postura de seguridad efectiva para modelos de trabajo desde cualquier lugar, SD-Branch y casos de uso de WAN que priorizan la nube.
- Lograr eficiencias operativas a cualquier escala mediante automatización, análisis profundo y autosanación

Seguridad móvil para 4G, 5G e IoT

- Opciones de migración CGNAT e IPv6 de alto rendimiento y aceleración por SPU, que incluyen: NAT44, NAT444, NAT64/DNS64, NAT46 para conectividad y seguridad 4G Gi/sGi y 5G N6
- Seguridad de acceso RAN con agregación IPsec altamente escalable y de mayor rendimiento y control de puerta de enlace de seguridad (SecGW)
- Seguridad en el plano de usuario habilitada por protección total contra amenazas y visibilidad de la inspección GTP-U

Hardware

Serie FortiGate 1000F



Interfaces

1. 2 USB
2. 1 puerto de consola
3. 1 puerto de gestión GE RJ45
4. 1 puerto 2,5 GE/GE HA
5. 8 ranuras RJ45 de 10 GE / 5 GE / 2,5 GE / GE / 100 M
6. Ranuras 16 x 10 GE SFP+ / GE SFP
7. 8 ranuras 25 GE SFP28 / 10 GE SFP+ / GE SFP
8. 2 ranuras 100 GE QSFP28 / 40 GE QSFP+

Características de hardware

Especificaciones

	FG-1000F	FG-1001F
Interfaces y módulos		
Hardware acelerado 100 GE QSFP28/40 Ranuras GE QSFP+	2	
Hardware acelerado 25 GE SFP28 / 10 ranuras GE SFP+/GE SFP	8	
Hardware acelerado 10 GE SFP+ / GE SFP Ranuras	8	
Ranuras RJ45 de 10 GE / 5 GE / 2,5 GE / GE / 100 M con aceleración de hardware	8	
Puerto 2,5 GE/GE HA	1	
Puertos de gestión 10GE/GE RJ45	1	
Puertos USB (Cliente/Servidor)	2/2	
Puerto de consola	1	
Almacenamiento a bordo	2x 480GB	
Módulo de plataforma confiable (TPM)	Sí	
Transceptores incluidos	2x SFP SX	
Rendimiento del sistema: combinación de tráfico empresarial		
Rendimiento de IPS [2]	19 Gbps	
Rendimiento de NGFW 2, 4	15 Gbps	
Rendimiento de protección contra amenazas 2, 5	13 Gbps	
Rendimiento y capacidad del sistema		
Rendimiento del firewall IPv4 (1518/512/64 bytes, UDP)	198/190/134 Gbit/s	
Rendimiento del firewall IPv6 (1518/512/86 bytes, UDP)	198/196/134 Gbit/s	
Latencia del firewall (64 bytes, UDP)	3,45 µs	
Rendimiento del firewall (paquetes por segundo)	201 Mpp	
Sesiones simultáneas (TCP)	7,5 millones	
Nuevas sesiones/segundo (TCP)	650 000	
Políticas de cortafuegos	100 000	
Rendimiento de VPN IPsec (512 bytes)1	55 Gbps	
Túneles VPN IPsec de puerta de enlace a puerta de enlace	20 000	
Túneles VPN IPsec de cliente a puerta de enlace	100 000	
Rendimiento SSL-VPN6	5,3 Gbps	
Usuarios simultáneos de SSL-VPN (Máximo recomendado, modo túnel)	10 000	
Rendimiento de la inspección SSL (IPS, HTTPS promedio)3	10 Gbps	
CPS de inspección SSL (IPS, HTTPS promedio)3	11 000	
Sesión simultánea de inspección SSL (IPS, HTTPS promedio)3	600 000	
Rendimiento del control de aplicaciones (HTTP 64K)2	44 Gbps	
Rendimiento CAPWAP (HTTP 64K)	65 Gbps	
Dominios virtuales (predeterminado/máximo)	10 / 250	
Número máximo de FortiSwitches Soportado	196	
Número máximo de FortiAP (Total / Túnel)	4096/1024	
Número máximo de FortiTokens	20 000	
Configuraciones de alta disponibilidad	Activo-Activo, Activo-Pasivo, Agrupación	

	FG-1000F	FG-1001F
Dimensiones y potencia		
Alto x Ancho x Largo (pulgadas)	3,5 x 17,44 x 17,63	
Alto x Ancho x Largo (mm)	88,9 x 443 x 447,4	
Peso	21,94 libras (9,95 kg)	22,71 libras (10,3 kg)
Factor de forma (compatible con estándares EIA/no EIA)	Montaje en bastidor 2RU	
Fuente de alimentación de CA	100–240 VCA, 50/60 Hz	
Corriente CA (máxima)	6A@120VCA, 3A@240VCA	
Consumo de energía (promedio/máximo)	210W / 408W	215W / 415W
Disipación de calor	1211 BTU/hora	1229 BTU/hora
Clasificación de eficiencia de la fuente de alimentación	Cumple con 80Plus	
Fuentes de alimentación redundantes (Intercambiables en caliente)	Sí (viene con 2PSU por defecto)	
Entorno operativo y certificaciones		
Temperatura de funcionamiento	32°–104°F (0°–40°C)	
Temperatura de almacenamiento	-31°–158°F (-35°–70°C)	
Humedad	10%–90% sin condensación	
Nivel de ruido	66,7 dBA	
Flujo de aire forzado	Desde adelante hacia atrás	
Altitud de funcionamiento	Hasta 10 000 pies (3048 m)	
Cumplimiento	FCC Parte 15 Clase A, RCM, VCCI, CE, UL/cUL, CB	
Certificaciones	Laboratorios ICSA, Firewall, IPsec, IPS, Antivirus, SSL-VPN, USGv6/IPv6	

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 la inspección SSL utilizan un promedio de sesiones HTTPS de diferentes conjuntos de cifrado.

4 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 Utiliza el certificado RSA-2048.

Suscripciones

Categoría de servicio	Oferta de servicios	A la carta	Paquetes		
			Protección empresarial	Amenaza unificada Proteccion	Amenaza avanzada Proteccion
Servicios de seguridad	Servicio FortiGuard IPS	•	•	•	•
	Protección antimalware (AMP) FortiGuard: Antivirus, malware móvil, botnet, CDR, virus Protección contra brotes y FortiSandbox Cloud Servicio	•	•	•	•
	FortiGuard Web Security: URL y contenido web , Video y filtrado DNS seguro	•	•	•	
	FortiGuard Antispam		•	•	
	Servicio de detección de IoT FortiGuard	•	•		
	Servicio de Seguridad Industrial FortiGuard	•	•		
	Servicio Sandbox en línea basado en IA de FortiCloud 1	•			
Servicios NOC	FortiGate Cloud (Registro SMB + Nube Gestión)	•			
	Calificación y cumplimiento de FortiGuard Security Fabric Servicio de Monitoreo	•	•		
	Servicio FortiConverter	•	•		
	Ancho de banda subyacente FortiGuard SD-WAN y Servicio de Monitoreo de Calidad	•			
Servicios SOC	Nube FortiAnalyzer	•			
	Nube FortiAnalyzer con SOCaaS	•			
Soporte de hardware y software FortiCare Essentials		•			
	FortiCare Premium	•	•	•	•
	FortiCare Élite	•			
Servicios básicos	Control de aplicaciones FortiGuard				
	Servicio CASB en línea FortiCloud ZTNA 1				
	[illegible]		incluido con la suscripción FortiCare		
	[illegible]				
	[illegible]				
	[illegible]				
	Servicio DDNS (v4/v6)				

1. Disponible cuando se ejecute FortiOS 7.2

Paquetes FortiGuard

FortiGuard Labs ofrece una serie de servicios de inteligencia de seguridad para ampliar la plataforma de firewall FortiGate. Puede optimizar fácilmente las capacidades de protección de su FortiGate con uno de estos paquetes FortiGuard.

FortiCare Élite

Los servicios FortiCare Elite ofrecen acuerdos de nivel de servicio (SLA) mejorados y resolución acelerada de problemas. Esta oferta de soporte avanzado brinda acceso a un equipo de soporte dedicado. La gestión de tickets con un solo toque por parte del equipo técnico experto agiliza la resolución. Esta opción también proporciona soporte extendido de fin de ingeniería (EoE) de 18 meses para mayor flexibilidad y acceso al nuevo portal FortiCare Elite. Este portal intuitivo proporciona una vista única y unificada del estado de seguridad y del dispositivo.

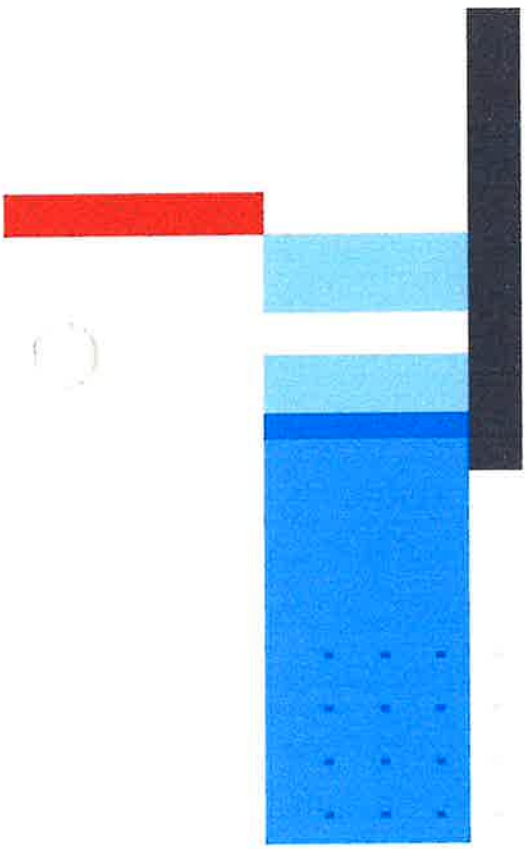
Política de RSC de Fortinet

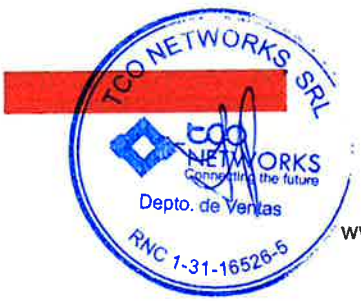
Fortinet está comprometido a impulsar el progreso y la sostenibilidad para todos a través de la ciberseguridad, con respeto por los derechos humanos y las prácticas comerciales éticas, haciendo posible un mundo digital que usted Siempre puedo confiar. Usted declara y garantiza a Fortinet que no utilizará 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 productos 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.

Información sobre pedidos

Producto	SKU	Descripción
FortiGate 1000F	FG-1000F	2 ranuras QSFP28 de 100 GE, , 8 ranuras SFP28 de 25 GE, 16 ranuras SFP+ de 10 GE, 8 puertos RJ45 BASE-T de 10 GE, 1 puerto MGMT de 1 GE, 1 puerto HA de 2,5 GE, SPU NP7 y CP9 acelerado por hardware, fuentes de alimentación de CA duales.
FortiGate 1001F	FG-1001F	2 ranuras QSFP28 de 100 GE , 8 ranuras SFP28 de 25 GE, 16 ranuras SFP+ de 10 GE, 8 ranuras 10 GE BASE-T RJ45 puertos, 1 puerto MGMT de 1 GE, 1 puerto HA de 2,5 GE, aceleración por hardware SPU NP7 y CP9, almacenamiento integrado SSD de 960 GB, fuentes de alimentación de CA duales.

Accesorios Opcionales	SKU	Descripción
Rieles deslizantes para montaje en bastidor	SP-FG3040B-CARRIL	Rieles deslizantes de montaje en bastidor para FG-1000C/-DC, FG-1200D, FG-1500D/DC, FG-3040B/-DC, FG-3140B/-CC, FG-3240C -DC, FG-3000D -DC FG-3000 3001F, FG-3100D/-DC, FG-3200D/-DC FG-3400/3401E, FG3600/3601E, FG-3700D/ -DC, FG-3700DX, FG-3810D/-DC y FG-3950B/-DC.
Fuente de alimentación de CA	SP-FG400F-PS	La fuente de alimentación de CA para FG-400/401F, FG-600/601F y FG-1000 1001F. El cable de alimentación SP-FGPCOR-XX se vende por separado.
1 módulo transceptor GE SFP LX	FN-TRAN-LX	1 módulo transceptor GE SFP LX para todos los sistemas con ranuras SFP y SFP/SFP+.
1 módulo transceptor GE SFP RJ45	FN-TRAN-GC	1 módulo transceptor GE SFP RJ45 para todos los sistemas con ranuras SFP y SFP/SFP+.
1 módulo transceptor GE SFP SX	FN-TRAN-SX	1 módulo transceptor GE SFP SX para todos los sistemas con ranuras SFP y SFP SFP+.
Módulo transceptor RJ45 SFP+ de 10 GE	FN-TRAN-SFP+GC	Módulo transceptor 10 GE SFP+ RJ45 para sistemas con ranuras SFP+.
Módulo transceptor SFP+ de 10 GE, corto alcance	FN-TRAN-SFP+SR	Módulo transceptor SFP+ de 10 GE, de corto alcance para todos los sistemas con ranuras SFP+ y SFP/SFP+.
Módulo transceptor SFP+ de 10 GE, largo alcance	FN-TRAN-SFP+LR	Módulo transceptor SFP+ de 10 GE, de largo alcance para todos los sistemas con ranuras SFP+ y SFP/SFP+.
Módulo transceptor SFP+ de 10 GE, rango extendido	FN-TRAN-SFP+ER	Módulo transceptor SFP+ de 10 GE, rango extendido para todos los sistemas con ranuras SFP+ y SFP/SFP+.
Cable de conexión directa activa SFP+ de 10 GE, 10 m 32,8 pies	SP-CABLE-ADASFP+	Cable de conexión directa activa SFP+ de 10 GE, 10 m/32,8 pies para todos los sistemas con ranuras SFP+ y SFP/SFP+.
Módulo transceptor 25 GE SFP28, corto alcance	FN-TRAN-SFP28-SR	Módulo transceptor SFP28 de 25 GE, de corto alcance para todos los sistemas con ranuras SFP28.
Módulo transceptor 25 GE SFP28, largo alcance	FN-TRAN-SFP28-LR	Módulo transceptor SFP28 de 25 GE de largo alcance para todos los sistemas con ranuras SFP28.
Módulo transceptor QSFP+ de 40 GE corto alcance	FN-TRAN-QSFP+SR	Módulo transceptor QSFP+ de 40 GE, de corto alcance para todos los sistemas con ranuras QSFP+.
Módulo transceptor QSFP+ de 40 GE BiDi de corto alcance	FG-TRAN-QSFP+SR-BIDI	Módulo transceptor QSFP+ de 40 GE, BiDi de corto alcance para todos los sistemas con ranuras QSFP+.
Módulo transceptor QSFP+ de 40 GE largo alcance	FN-TRAN-QSFP+LR	Módulo transceptor QSFP+ de 40 GE, de largo alcance para todos los sistemas con ranuras QSFP+.
Transceptores 100 GE QSFP28, corto alcance	FN-TRAN-QSFP28-SR	100 transceptores GE QSFP28, fibra paralela de 4 canales, corto alcance para todos los sistemas con ranuras QSFP28.
100 transceptores GE QSFP28 largo alcance	FN-TRAN-QSFP28-LR	100 transceptores GE QSFP28, fibra paralela de 4 canales largo alcance para todos los sistemas con ranuras QSFP28.
100 transceptores GE QSFP28, CWDM4	FN-TRAN-QSFP28-CWDM4	Transceptores QSFP28 de 100 GE, conectores LC, 2KM para todos los sistemas con ranuras QSFP28.





FORTINET

www.fortinet.com

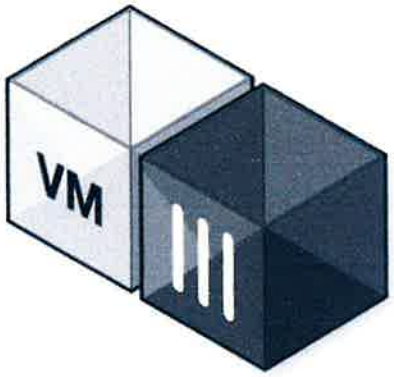
Noviembre de 2012

FORTINET

Dispositivos virtuales FortiGate®

Seguridad consolidada para entornos virtualizados

Completo ecosistema de seguridad de extremo a extremo para el centro de datos definido por software. Fortinet permite y facilita el recorrido de la empresa a través del proceso de consolidación del centro de datos.



Fortinet ofrece dispositivos de seguridad físicos y virtualizados para proteger planos de datos únicos. Ofrece, por un lado, capacidades de seguridad y rendimiento inigualables, al mismo tiempo que permite el crecimiento y la evolución del centro de datos en consolidación n degradación del servicio ni cuellos de botella, sin comprometer la seguridad y con un retorno de la inversión inigualable, cumpliendo con los resultados de un sistema robusto definido por software. marco de seguridad.

Los dispositivos virtuales FortiGate le permiten mitigar los puntos ciegos mediante la implementación de controles de seguridad críticos dentro de su infraestructura virtual. También le permiten aprovisionar rápidamente infraestructura de seguridad cuando y donde sea necesario. Los dispositivos virtuales FortiGate cuentan con todos los servicios de seguridad y redes comunes a los dispositivos FortiGate tradicionales basados en hardware. Con la incorporación de dispositivos virtuales de Fortinet, puede implementar una combinación de hardware y dispositivos virtuales, operando juntos y administrados desde una plataforma de administración centralizada común.

La completa línea de dispositivos virtuales de seguridad de Fortinet admite más de 16 soluciones.

Fortigate Virtual

Beneficios del electrodoméstico

Los dispositivos virtuales FortiGate ofrecen protección contra una amplia gama de amenazas, con soporte para todos los servicios de seguridad y redes que ofrece el sistema operativo FortiOS. Además, los electrodomésticos ofrecen:

§ Mayor visibilidad dentro de la infraestructura virtualizada

§ Capacidad de implementación rápida

§ Capacidad para administrar dispositivos virtuales y dispositivos físicos desde una plataforma de administración de panel único

§ Licencia simple sin cargos por usuario

§ Soporte para virtualización múltiple y Plataformas en la nube

§ Soporte completo para FortiHypervisor Implementaciones que permiten seguridad de velocidad de línea en el requisito de vCPE.

§ Amplia gama de opciones de licencias para adaptarse a cualquier requisito de infraestructura

§ Modelos habilitados para VDOM para múltiples inquilinos entornos

PLATAFORMA

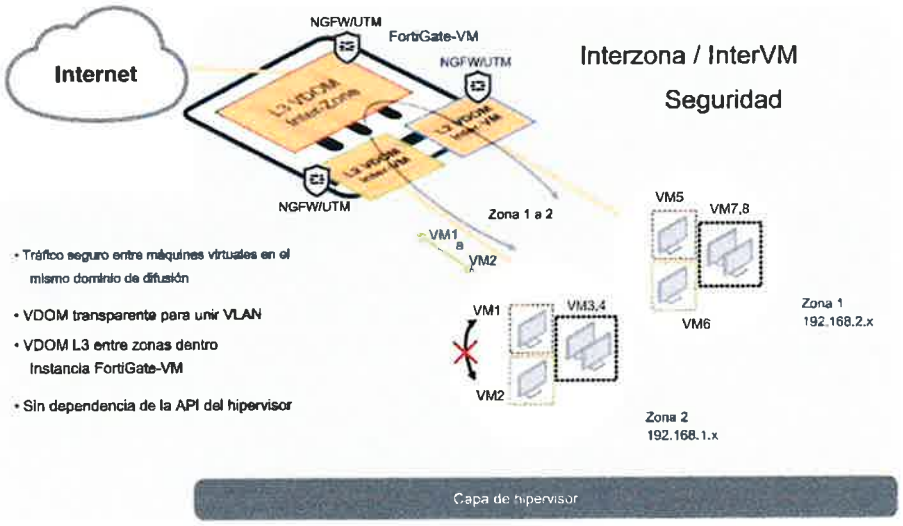
Elección del factor de forma

En la actualidad, pocas organizaciones utilizan 100 % hardware o 100 % infraestructura de TI virtual, lo que crea la necesidad de contar con dispositivos de hardware y dispositivos virtuales en su estrategia de seguridad. Fortinet le permite crear la solución de seguridad adecuada para su entorno con hardware y dispositivos virtuales para proteger el núcleo y el borde y aumentar la visibilidad y el control de las comunicaciones dentro de la infraestructura virtualizada. Los dispositivos físicos o virtuales FortiManager le permiten administrar y actualizar fácilmente sus activos de seguridad de Fortinet (hardware, virtuales o ambos) desde un único panel.

Seguridad multiamenaza

Utilizando el avanzado sistema operativo FortiOS™, los dispositivos FortiGate neutralizan eficazmente una amplia gama de amenazas de seguridad que enfrenta su entorno virtualizado. Ya sea que se implementen en el borde como defensa de primera línea o en lo profundo de la infraestructura virtual para seguridad entre zonas, los dispositivos FortiGate protegen su infraestructura con algunas de las medidas de seguridad más efectivas disponibles en la actualidad al habilitar las funciones de seguridad que necesita.

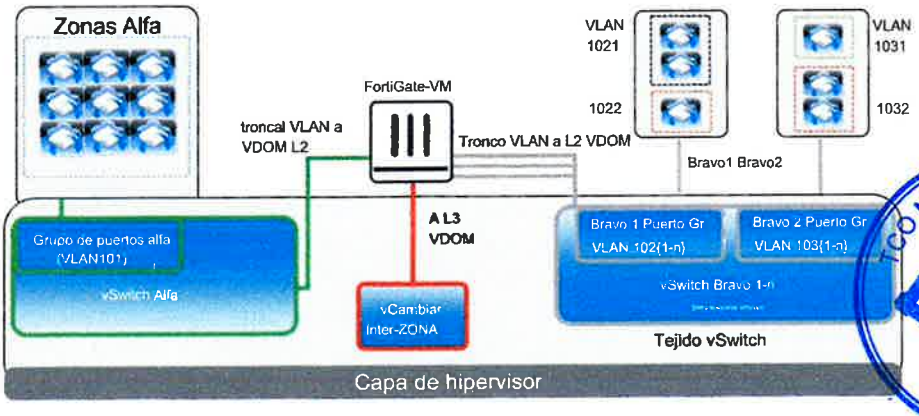
DESPLIEGUE



Todo el tráfico entre máquinas virtuales en las zonas Bravo está sujeto a un escaneo UTM completo a través de L2 VDOM.

El tráfico entre zonas está sujeto a un firewall completo de próxima generación y escaneo UTM por parte de L3 VDOM.

Todas las máquinas virtuales de Alpha Zone pueden comunicarse entre sí libremente.

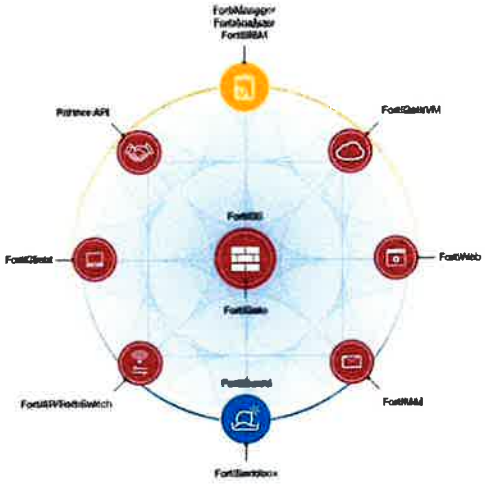


TEJIDO DE SEGURIDAD FORTINET

Tela de seguridad

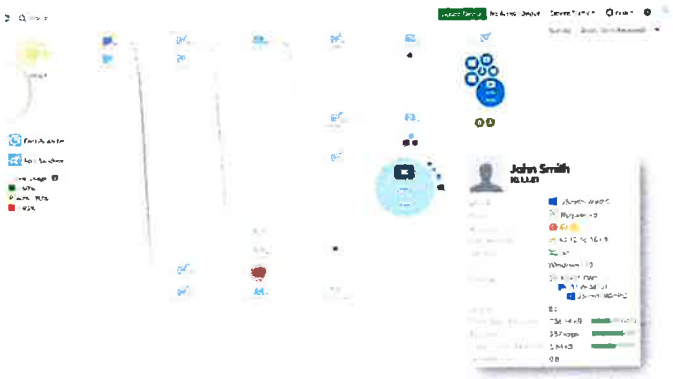
Security Fabric permite que la seguridad se expanda y adapte dinámicamente a medida que se agregan más y más cargas de trabajo y datos. La seguridad sigue y protege sin problemas los datos, los usuarios y las aplicaciones mientras se mueven entre IoT, dispositivos y entornos de nube en toda la red.

FortiGates son la base de Security Fabric y amplían la seguridad a través de la visibilidad y el control al integrarse estrechamente con otros productos de seguridad de Fortinet y soluciones de Fabric-Ready Partner.



FortiOS

Controle todas las capacidades de seguridad y redes en toda la plataforma FortiGate con un sistema operativo intuitivo. Reduzca los gastos operativos y ahorre tiempo con una plataforma de seguridad de próxima generación verdaderamente consolidada.



§ Una plataforma verdaderamente consolidada con un sistema operativo para todos los servicios de seguridad y redes para todas las plataformas FortiGate.

§ Protección líder en la industria: Recomendado por NSS Labs, VB100, AV Comparatives e ICSA validaron la seguridad y el rendimiento.

§ Controle miles de aplicaciones, bloquee los exploits más recientes y filtre el tráfico web en función de millones de clasificaciones de URL en tiempo real.

§ Prevenga, detecte y mitigue ataques avanzados automáticamente en minutos con protección avanzada contra amenazas integrada.

§ Satisfaga sus necesidades de red con amplias capacidades de enrutamiento, conmutación y SD-WAN.

§ Utilice la aceleración del hardware SPU para aumentar el rendimiento de la capacidad de seguridad.

Para obtener más información, consulte la hoja de datos de FortiOS disponible en www.fortinet.com

SERVICIOS

Servicios de seguridad FortiGuard™

FortiGuard Labs ofrece inteligencia en tiempo real sobre el panorama de amenazas, brindando actualizaciones de seguridad integrales en toda la gama de soluciones de Fortinet. Compuesto por investigadores de amenazas a la seguridad, ingenieros y especialistas forenses, el equipo colabora con las principales organizaciones de monitoreo de amenazas del mundo y otros proveedores de redes y seguridad, así como con agencias encargadas de hacer cumplir la ley.

Servicios de soporte FortiCare™

Nuestro equipo de atención al cliente de FortiCare brinda soporte técnico global para todos los productos Fortinet. Con personal de soporte en América, Europa, Medio Oriente y Asia, FortiCare ofrece servicios para satisfacer las necesidades de empresas de todos los tamaños.

Para obtener más información, consulte forti.net/fortiguard y forti.net/forticare

ESPECIFICACIONES

	FORTIGATE-VM00	FORTIGATE-VM01/01V	FORTIGATE-VM02/02V	FORTIGATE-VM04/04V
Especificaciones técnicas				
Compatibilidad con vCPU (mínimo/máximo)	1/1	1/1	1/2	1/4
Soporte de interfaz de red (mínimo/máximo)	1/10	1/10	1/10	1/10
Soporte de memoria (mínimo/máximo)	1GB / 2GB*	1GB / 2GB	1GB / 4GB	1GB / 6GB
Soporte de almacenamiento (mínimo/máximo)	32GB / 2TB	32GB / 2TB	32GB / 2TB	32GB / 2TB
Puntos de Acceso Inalámbrico Controlados (Túnel / Global)	32 / 32	32 / 64	256 / 512	256 / 512
Dominios virtuales (predeterminado/máximo) **	2/2	10 / 10	10 / 25	10 / 50
Políticas de firewall (VDOM/Sistema)	5.000	20.000 / 40.000	50.000 / 100.000	50.000 / 100.000
Número máximo de FortiTokens	1.000	1.000	1.000	5.000
Número máximo de puntos finales registrados	200	2.000	2.000	8.000
Licencia de usuario ilimitada	Si	Si	Si	Si
Rendimiento de sistema				
Rendimiento del firewall (paquetes UDP)	12 Gbps	12 Gbps	15 Gbps	28 Gbps
Sesiones simultáneas (TCP)	1,0 millón	1,0 millón	2,6 Millones	4,3 millones
Nuevas sesiones/segundo (TCP)	85.000	85.000	100.000	125.000
Rendimiento de VPN IPsec (AES256+SHA1, 512 bytes)	1 Gbit/	1 Gbit/	1.5 Gbit/s	3 Gbps
Túneles VPN IPsec de puerta de enlace a puerta de enlace	s 2.000	s 2.000	2.000	2.000
Túneles VPN IPsec de cliente a puerta de enlace	6.000	6.000	12.000	20.000
Rendimiento SSL-VPN	800Mbps	800Mbps	830Mbps	2 Gbps
Usuarios simultáneos de SSL-VPN (máximo recomendado)	1.000	1.000	2.000	4.500
Rendimiento de IPS (HTTP/mezcla empresarial) [1]	3.5 Gbps / 1 Gbps 2	3.5 Gbps / 1 Gbps 2	5.5 Gbps / 1.5 Gbps	8 Gbps / 3 Gbps
Rendimiento del control de aplicaciones [2]	Gbps	Gbps	2.6 Gbps	4.5 Gbps
Rendimiento de NGFW [3]	850 Mbps	850 Mbps	1.5 Gbps	2.5 Gbps
Rendimiento de la protección contra amenazas [4]	700 Mbps	700 Mbps	1.2 Gbps	2 Gbps

	FORTIGATE-VM08/08V	FORTIGATE-VM16/16V	FORTIGATE-VM32/32V	FORTIGATE-VMUL/ULV
Especificaciones técnicas				
Compatibilidad con vCPU (mínimo/máximo)	1/8	1 / 16	1 / 32	1 / ilimitado
Soporte de interfaz de red (mínimo/máximo)	1/10	1/10	1/10	1/10
Soporte de memoria (mínimo/máximo)	1GB / 12GB	1GB / 24GB	1GB / 48GB	1 GB / GB ilimitados
Soporte de almacenamiento (mínimo/máximo)	32GB / 2TB	32GB / 2TB	32GB / 2TB	32GB / 2TB
Puntos de Acceso Inalámbrico Controlados (Túnel / Global)	1.024 / 4.096	1.024 / 4.096	1.024 / 4.096	1.024 / 4.096
Dominios virtuales (predeterminado/máximo) **	10 / 500	10 / 500	10 / 500	10 / 500
Políticas de firewall (VDOM/Sistema)	50.000 / 100.000	50.000 / 100.000	50.000 / 100.000	50.000 / 100.000
Número máximo de FortiTokens	5.000	5.000	5.000	5.000
Número máximo de puntos finales registrados	20.000	20.000	20.000	20.000
Licencia de usuario ilimitada	Si	Si	Si	Si
Rendimiento de sistema				
Rendimiento del firewall (paquetes UDP)	33 Gbps	36 Gbps	50 Gbps	
Sesiones simultáneas (TCP)	8,5 millones	18,0 millones	38,0 millones	
Nuevas sesiones/segundo (TCP)	150.000	175.000	200.000	
Rendimiento de VPN IPsec (AES256+SHA1, 512 bytes)	5,5 Gbps	6,5 Gbps	7 Gbps	
Túneles VPN IPsec de puerta de enlace a puerta de enlace	40.000	40.000	40.000	
Túneles VPN IPsec de cliente a puerta de enlace	40.000	50.000	64.000	
Rendimiento SSL-VPN	4,5 Gbps	8,5 Gbps	8,6 Gbps	
Usuarios simultáneos de SSL-VPN (máximo recomendado)	10.000	25.000	40.000	
Rendimiento de IPS (HTTP/mezcla empresarial) [1]	15,5 Gbps / 6 Gbps	25 Gbps / 12 Gbps	29 Gbps / 19 Gbps	
Rendimiento del control de aplicaciones [2]	9 Gbps	17 Gbps	17,5 Gbps	
Rendimiento de NGFW [3]	4,5 Gbps	9 Gbps	16,5 Gbps	
Rendimiento de la protección contra amenazas [4]	3,5 Gbps	7 Gbps	9 Gbps	

El rendimiento real puede variar según la red y la configuración del sistema. Las métricas de rendimiento se observaron utilizando un DELL R740 (CPU Intel Xeon Platinum 8168 2,7 GHz, adaptadores de red Intel X710) ejecutando FOS v5.6.3. Probado con VMware vSphere 6.5 Enterprise Plus. SR-IOV está habilitado. 1. El rendimiento de IPS se mide utilizando HTTP de 1 Mbyte y Enterprise Traffic Mix. 2. El rendimiento del control de aplicaciones se mide con un tráfico HTTP de 64 Kbytes. 3. El rendimiento de NGFW se mide con IPS y control de aplicaciones habilitado, según Enterprise Traffic Mix. 4. El rendimiento de la protección contra amenazas se mide con IPS y control de aplicaciones y protección contra malware habilitados, según Enterprise Traffic Mix.

Aplicable a VM que se ejecuta en 5.6 y superior.

No aplicable a la serie FG-VMxxV ya que no se admiten VDOM. FG-VMxxV 6.0.0 es una excepción, que admite la adición de VDOM con licencias VDOM adquiridas por separado. Consulte INFORMACIÓN DE PEDIDO para conocer la SKU de VDOM.

Hay licencias especiales disponibles para entornos de red fuera de línea para la serie VMxxV (01V a UL V) y tienen las mismas especificaciones que las de VMxxV que se muestran en la tabla anterior. Para adquirir licencias fuera de línea, contacte a los representantes de ventas de Fortinet.

ESPECIFICACIONES

PROVEEDOR
Nubes privadas (hipervisores)
VMware ESXi v5.0 / v5.1 / v5.5 / v6.0 / v6.5
Servidor Microsoft Hyper-V 2008 R2 / 2012 / 2012 R2 / 2016
Citrix Xen XenServer v5.6 sp2, v6.0, v6.2 y posteriores
Xen de código abierto v3.4.3, v4.1 y posteriores
KVM qemu 0.12.1 y libvirt 0.10.2 y posteriores para Red Hat Enterprise Linux/CentOS 6.4 y posteriores/Ubuntu 16.04 LTS (kernel genérico)
KVM qemu 2.3.1 para SuSE Linux Enterprise Server 12 SP1 LTSS

PROVEEDOR
Nubes públicas (mercados)
Amazon AWS (incluidos GovCloud y AWS China)
Nube de VMware en AWS
Microsoft Azure (incluido Azure regional gobierno de EE. UU., Alemania y China)
Google GCP (plataforma en la nube de Google)
OCI de Oracle
Aliyun (Nube de Alibaba)

Nota: El soporte de virtualización/plataforma en la nube varía según el modelo y las compilaciones de FortiOS. Consulte las notas de la versión correspondientes.

La serie FG-VMxV requiere FortiOS 5.4.8+, 5.6.1+ / 6.0.0+.

INFORMACIÓN DEL PEDIDO

Producto	SKU	Descripción
FortiGate-VM00	FG-VM00	FortiGate-VM 'dispositivo virtual', 1x núcleo vCPU, (hasta) 2 GB de RAM. No hay soporte para Extreme DB.
FortiGate-VM01	FG-VM01, FG-VM01V	FortiGate-VM 'dispositivo virtual', 1x núcleo vCPU y (hasta) 2 GB de RAM. Sin VDOM de forma predeterminada para el modelo FG-VM01V.
FortiGate-VM02	FG-VM02, FG-VM02V	FortiGate-VM 'dispositivo virtual', 2 núcleos vCPU y (hasta) 4 GB de RAM. Sin VDOM de forma predeterminada para el modelo FG-VM02V.
FortiGate-VM04	FG-VM04, FG-VM04V	FortiGate-VM 'dispositivo virtual', 4 núcleos vCPU y (hasta) 6 GB de RAM. Sin VDOM de forma predeterminada para el modelo FG-VM04V.
FortiGate-VM08	FG-VM08, FG-VM08V	FortiGate-VM 'dispositivo virtual', 8 núcleos de vCPU y (hasta) 12 GB de RAM. Sin VDOM de forma predeterminada para el modelo FG-VM08V.
FortiGate-VM16	FG-VM16, FG-VM16V	FortiGate-VM 'dispositivo virtual', 16 núcleos de vCPU y (hasta) 24 GB de RAM. Sin VDOM de forma predeterminada para el modelo FG-VM016V.
FortiGate-VM32	FG-VM32, FG-VM32V	FortiGate-VM 'dispositivo virtual', 32 núcleos de vCPU y (hasta) 48 GB de RAM. Sin VDOM de forma predeterminada para el modelo FG-VM032V.
FortiGate-VMUL	FG-VMUL, FG-VMULV	FortiGate-VM 'dispositivo virtual', Núcleos de vCPU y RAM ilimitados. No hay VDOM de forma predeterminada para el modelo FG-VMULV.
Accesorios Opcionales		
Licencia de dominio virtual Agregar 5	FG-VDOM-5-UG	Licencia de actualización para agregar 5 VDOM a FortiOS 5.4 y posteriores, limitada por la capacidad máxima de VDOM de la plataforma.
Licencia de dominio virtual Agregar 15	FG-VDOM-15-UG	Licencia de actualización para agregar 15 VDOM a FortiOS 5.4 y posteriores, limitada por la capacidad máxima de VDOM de la plataforma.
Licencia de dominio virtual Agregar 25	FG-VDOM-25-UG	Licencia de actualización para agregar 25 VDOM a FortiOS 5.4 y posteriores, limitada por la capacidad máxima de VDOM de la plataforma.
Licencia de dominio virtual Agregar 50	FG-VDOM-50-UG	Licencia de actualización para agregar 50 VDOM a FortiOS 5.4 y posteriores, limitada por la capacidad máxima de VDOM de la plataforma.
Licencia de dominio virtual Agregar 240	FG-VDOM-240-UG	Licencia de actualización para agregar 240 VDOM a FortiOS 5.4 y posteriores, limitada por la capacidad máxima de VDOM de la plataforma.

FG-VMxV 5.0 admite VDOM agregando licencias VDOM independientes. La cantidad de VDOM configurables se puede acumular hasta la cantidad máxima de VDOM admitidos por modelo de vCPU. Consulte Dominios virtuales (máximo) en ESPECIFICACIONES.

FORTINET

LA SEDE MUNDIAL
Fortinet Inc.
899 CARRETERA KIFER
Sunnyvale, CA 94086
Estados Unidos
Teléfono: +1.408.235.7700
www.fortinet.com/ventas

OFICINA DE VENTAS EN EMEA
905 calle Albert Einstein
06560 Valbonne
Francia
Teléfono: +33.4.8987.0500

OFICINA DE VENTAS APAC
8 Bulevar Temasek
#12-01 Torre Tres Suntec
Singapur 038988
Teléfono: +65.6395.2788

OFICINA DE VENTAS EN AMÉRICA LATINA
Centro de las Américas Sawgrass
13450 W Sunrise Blvd., Suite 430 Sunrise,
Fl. 33323
Estados Unidos
Teléfono +1.954.368.9990

FICHA DE DATOS

Electrodomésticos FortiManager™

Gestión Centralizada para Redes de Seguridad Fortinet

Tome el control de su infraestructura de seguridad

Los dispositivos de administración centralizada FortiManager brindan las herramientas esenciales necesarias para administrar de manera efectiva su infraestructura de seguridad basada en Fortinet. Ya sea implementando varios o miles de nuevos dispositivos y agentes, distribuyendo actualizaciones o instalando políticas de seguridad en activos administrados, los dispositivos FortiManager reducen drásticamente los costos y gastos generales de administración. El descubrimiento de dispositivos, la administración de grupos, las instalaciones de auditoría y la capacidad de administrar entornos complejos de VPN en malla y en estrella son solo algunas de las características que ahorran tiempo que ofrecen los dispositivos FortiManager. Complementado por el dispositivo centralizado de registro e informes FortiAnalyzer™, FortiManager proporciona una solución de gestión centralizada completa y potente para su organización.

Sea el dueño de su dominio

Los dispositivos FortiManager escalan para administrar miles de dispositivos y agentes Fortinet. Los grupos de dispositivos y agentes, junto con sus administradores, forman el concepto de Dominios de Administración (ADOM) de FortiManager. Dentro de un ADOM, un administrador tiene la capacidad de crear paquetes de políticas, carpetas y objetos que pueden compartirse entre todos los dispositivos FortiGate en el ADOM local. En el ADOM global de FortiManager, las políticas y objetos globales también se pueden asignar y aplicar a sub ADOM. Ya sea que esté administrando uno o mil ADOM, los dispositivos FortiManager siempre brindan una administración efectiva y eficiente de sus activos de Fortinet.

Integrado de Fortinet Solución de gestión

Los dispositivos FortiManager le brindan una interfaz segura basada en web para el comando y control de su infraestructura de seguridad Fortinet. Los dispositivos FortiManager también brindan administración centralizada de aprovisionamiento, configuración y actualización basada en políticas para dispositivos FortiGate, FortiWiFi y FortiMail, así como agentes de seguridad de endpoints FortiClient. Finalmente, FortiManager incluye capacidades de monitoreo en tiempo real para mayor visibilidad.

Para completar su solución de gestión centralizada, FortiManager complementa nuestros dispositivos FortiAnalyzer. Estos dispositivos brindan descubrimiento, análisis, priorización e informes en profundidad de los eventos de seguridad detectados dentro de su entorno. Juntos, los sistemas FortiManager y FortiAnalyzer forman una solución de gestión integral y de clase empresarial.

Características	Beneficios
Modos de gestión combinados	El nuevo modo combinado proporciona un flujo de trabajo unido que es adecuado para usuarios de cualquier modo. Ofrecemos esto combinado Modo de gestión para mayor flexibilidad y escalabilidad.
Base de datos de objetos jerárquicos	Facilita la reutilización de configuraciones comunes en toda la organización, tanto a nivel ADOM local como global.
Centralizado basado en electrodomésticos Gestión	Simplifica la implementación y el mantenimiento asociados con la solución de administración central al eliminar los requisitos de hardware y sistemas operativos de terceros.
Aprovisionamiento automatizado de dispositivos / Configuración de políticas centralizada	Reduce el costo de implementar nuevas instalaciones de FortiGate o FortiClient y mantiene políticas en todos los activos administrados.
Administración basada en roles	Permite la administración distribuida, un requisito importante para organizaciones más grandes.
Auditoria de políticas/dispositivos	Le permite demostrar el cumplimiento y realizar un seguimiento de cualquier desviación de la política de seguridad requerida.
SDK para portales web	La API basada en JSON permite a los MSSP ofrecer portales web administrativos a los clientes.
API XML de FortiManager	La API XML de FortiManager es una interfaz de servicios web que permite a los clientes integrarse con sistemas de aprovisionamiento y automatizar la configuración de los numerosos dispositivos que FortiManager es capaz de gestionar.


FortiManager-200D


FortiManager-400C


FortiManager-1000C


FortiManager-3000C


FortiManager-5001A

Dispositivo virtual FortiManager

Dominios administrativos (ADOM)

Permite que el 'administrador' principal cree grupos de dispositivos para que otros administradores los supervisen y administren:

- Los administradores pueden administrar dispositivos en su ubicación geográfica o división comercial.
- Los dispositivos FortiGate con múltiples VDOM se pueden dividir entre múltiples ADOM
- Los usuarios administrativos solo pueden acceder a los dispositivos o VDOM que se les hayan asignado
- El administrador principal puede acceder a todos los dominios y dispositivos administrativos.

Base de datos de objetos jerárquicos

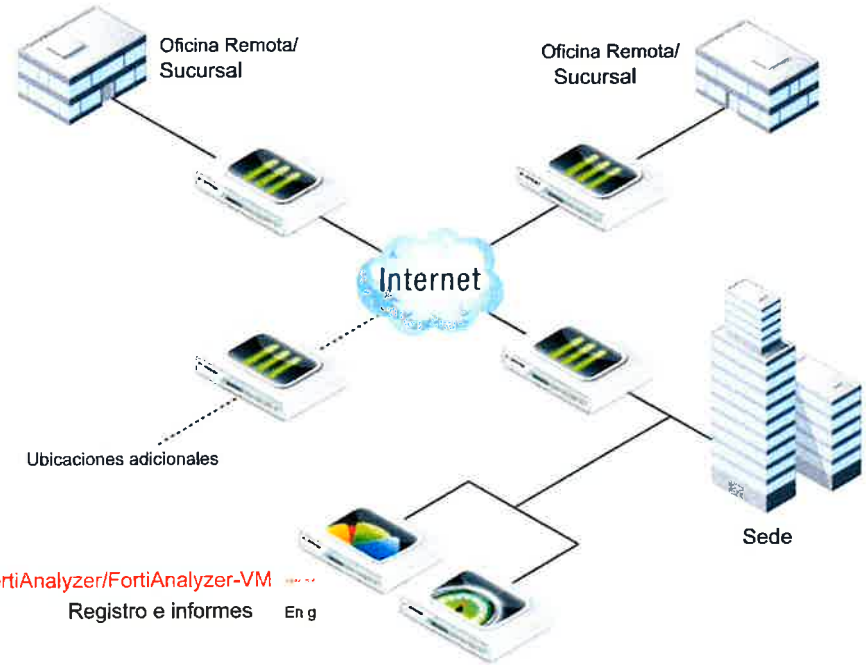
Hay dos niveles de repositorios centralizados dentro de FortiManager que albergan los detalles de configuración de varios activos:

- Crear plantillas de configuración de dispositivos para configurar rápidamente un nuevo dispositivo Fortinet.
- Dentro de cada ADOM, existe una base de datos común de objetos compartidos por todos los dispositivos. y paquetes de políticas que permiten a los usuarios reutilizar configuraciones similares entre un grupo de activos administrados
- Utilizando la función de Política Global incluida, un ADOM global puede tener una política global y una base de datos global común a todos los ADOM en el sistema.

SDK para portales web

Diseñado para aplicaciones multiinquilino dentro de una única plataforma de gestión:

- La API basada en JSON permite a los MSSP ofrecer portales web administrativos a los clientes.
- Proporciona un portal web administrativo para clientes que requieren cierto grado de control sobre la gestión de seguridad de su red
- Permite a los clientes de MSSP administrar su propia lista de usuarios SSL-VPN y filtrado web. Filtros de URL y categorías
- Si están configurados, los clientes también pueden ver las políticas de firewall para su dispositivo FortiGate o VDOM



FortiAnalyzer/FortiAnalyzer-VM
Registro e informes

FortiManager/FortiManager-VM
Gestión Centralizada

Contenido de seguridad alojado localmente

Alojar contenido de seguridad localmente permite al administrador un mayor control sobre las actualizaciones de contenido de seguridad y proporciona un tiempo de respuesta mejorado para las bases de datos de calificación. Incluye soporte para:

- Actualizaciones de definiciones de antivirus
- Actualizaciones de prevención de intrusiones
- Actualizaciones de gestión de vulnerabilidad y cumplimiento
- Filtrado web (sistemas seleccionados)
- Antispam (sistemas seleccionados)

Modelo de Gestión Unificado

El flujo de trabajo único y unido permite la configuración de múltiples componentes de administración por ADOM:

- Objetos y Objetos Dinámicos
- Asistentes de importación y VPN
- Gestión de configuración del dispositivo incluido el resumen y el estado del dispositivo. Sincronización VDOM, basada en GUI Guiones

API XML de FortiManager

La API XML de FortiManager es una web Interfaz de servicios utilizada para facilitar la automatización:

- Los clientes de nube pública/privada pueden integrarse con sistemas de aprovisionamiento.
- Configurar FortiGate administrado dispositivos a través de una interfaz de servicios web.
- Obtener información, crear y ejecutar scripts CLI de FortiOS en la base de datos FortiManager y luego instalar los cambios en las unidades FortiGate.

Política global

Proteja las políticas permitiendo la creación de paquetes de encabezado y pie de página de políticas globales:

- Permite que las políticas se apliquen universalmente a todos los ADOM y VDOM.
- Permite a los administradores de proveedores de servicios soportar instalaciones complejas que requieren que los clientes pasen tráfico a través de la red del proveedor de servicios.

Especificaciones técnicas Electrodomésticos FortiManager	FortiManager-200D	FortiManager-400C	FortiManager-1000C	FortiManager-3000C	FortiManager-5001A
Capacidad					
Dispositivos de red con licencia1 (máx.)	30	300	800	5,000	4,000
Dominios de administración (ADOM)	30	300	800	5,000	4,000
Portales web administrativos	–	–	800	5,000	4,000
Usuarios del portal web (máx.)	–	–	800	5,000	4,000
Política global (incluida)	Sí	Sí	Sí	Sí	Sí
Hardware					
Factor de forma del hardware	Escritorio	Montaje en bastidor (1-RU)	Montaje en bastidor (1-RU)	Montaje en bastidor (2-RU)	Hoja ATCA
Ethernet 10/100/1000 (Base-T)	4	4	4	4	2
Puerto de consola	RJ45	RJ45	DB-9	DB-9	DB-9
Pantalla LCD	No	No	Sí	Sí	No
Capacidad de almacenamiento	1 TB	1 TB	2 TB	4 TB	80GB
Soporte de alta disponibilidad	Sí	Sí	Sí	Sí	Sí
Fuentes de alimentación intercambiables en caliente	–	–	–	Sí	Sí (integrado en el chasis)
Dimensiones					
Altura	4,5 cm (1,75 pulgadas)	4,4 cm (1,7 pulgadas)	4,30 cm (1,69 pulgadas)	3,5 pulgadas (8,9	1,18 pulgadas (3,0 cm)
Ancho	43,3 cm (17,05 pulgadas)	43,5 cm (17,1 pulgadas)	43,4 cm (17,09 pulgadas)	cm) 17,5 pulgadas (44,5	14 pulgadas (35,5 cm)
Longitud	35,2 cm (13,86 pulgadas)	38,4 cm (14,3 pulgadas)	62,71 cm (24,69 pulgadas)	cm) 29,0 pulgadas (73,7	12,2 pulgadas (31,0 cm)
Peso	6,08 kg (13,4 libras)	6,7 kg (14,7 libras)	11 kg (24,2 libras)	cm) 63 libras (28,6 kg)	8 libras (3,63 kg)
Ambiente					
Energía requerida	100 – 240 VCA 50 – 60 Hz, 0,8 amperios (máx.)	100 – 240 VCA 50 – 60 Hz, 4,0 amperios (máx.)	100 – 240 VCA 50 – 60 Hz, 7,0 amperios (máx.)	100 – 240 VCA 50 – 60 Hz, 9,0 amperios (máx.)	Alimentación CC desde el chasis del sistema.
Consumo de energía (AVG)	60 vatios	100W	189W	290 vatios	148 vatios
Disipación de calor	205 BTU/hora	411 BTU/h	644 BTU/hora	988 BTU/hora	505 BTU/h
Temperatura de funcionamiento	32 – 104 grados F (0 – 40 grados C)				
Temperatura de almacenamiento	-13 – 158 grados F (-25 – 70 grados C)				
Humedad	5 a 95% sin condensación				
Certificaciones					
Certificaciones de seguridad	FCC Clase A Parte 15, UL/CB/CUL, C Tick, VCCI, CE				

Especificaciones técnicas Electrodomésticos virtuales FMG	FMG-VM-Base	FMG-VM-10-UG	FMG-VM-100-UG	FMG-VM-1000-UG	FMG-VM-5000-UG	FMG-VM-U-UG
Capacidad						
Dispositivos de red con licencia1,2 (máx.)	10	+10	+100	+1,000	+5,000	Ilimitado2
Dominios de administración (ADOM)	10	+10	+100	+1,000	+5,000	Ilimitado2
Portales web administrativos	10	+10	+100	+1000	+5,000	Ilimitado2
Usuarios del portal web (máx.)	10	+10	+100	+1000	+5,000	Ilimitado2
Restricciones del modelo	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno	Ninguno
Máquina virtual						
Hipervisores compatibles	VMware ESXi/ESX 3.5/4.0/4.1/5.0					
Factor de forma de máquina virtual	Formato de virtualización abierto (OVF)					
vCPU (máx./mín.)	1 Ilimitado					
Soporte de interfaz de red (mín./máx.)	1/4					
Soporte de memoria (mín./máx.)	80GB 2TB					
Memoria de máquina virtual requerida (Mín./Máx.)	1024 MB/4096 MB para 32 bits y 1024 MB/ilimitado para 64 bits					
Soporte de alta disponibilidad	Sí					

1 Cada dominio virtual (VDOM) que opera en un dispositivo físico cuenta como un (1) dispositivo de red con licencia.
2 Limitado en software a 10 000 dispositivos, ADOM, portales web y usuarios de portales web.

Comando y control

- Administrar dispositivos y agentes de punto final individualmente o como grupos lógicos
- Descubre nuevos dispositivos automáticamente
- Crear, implementar y monitorear redes privadas virtuales.
- Delegar el control a otros usuarios con funciones de administración distribuida
- Auditar los cambios de configuración para garantizar el cumplimiento.

Administrar actualizaciones

- Simplifique el mantenimiento continuo de su infraestructura de seguridad basada en Fortinet programando actualizaciones de dispositivos

Monitorear, analizar e informar

- Acceder a estadísticas vitales de seguridad y red.
- Combine con un FortiAnalyzer
  Dispositivo para capacidades adicionales de minería de datos y generación de informes gráficos.

Compatible con FortiManager

Dispositivos y agentes

- FortiGate y FortiCarrier
  Dispositivos de seguridad consolidados
- Software de terminal FortiClient
- Seguridad de mensajería FortiMail
  Accesorios
- Análisis FortiAnalyzer y
  Dispositivos de informes
- Plataformas de conmutación FortiSwitch

Funciones de FortiManager									
	Complemento		Contenido de seguridad alojado localmente					Varios. Características	
	Global Políticas	Portal web SDK	antivirus	Intrusión Prevención	Vulnerabilidad Gestión	Web Filtración	Antispam Bases de datos	Estante Gerente	(Activación de máquina virtual) Modo de red cerrada
FortiManager-200D	Sí	No	Sí	Sí	Sí	Sí	Sí	No	No
FortiManager-400C	Sí	No	Sí	Sí	Sí	Sí	Sí	No	No
FortiManager-1000C	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
FortiManager-3000C	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
FortiManager-5001A	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
FortiManager-VM5K (4.2)	No	No	Sí	Sí	Sí	Sí	Sí	Sí	No
Base FortiManager-VM (4.3)	Sí	Sí	Sí	Sí	Sí	No	No	No	No
FortiManager-VM Base + FMG-VM-10-UG	Sí	Sí	Sí	Sí	Sí	No	No	No	No
FortiManager-VM Base + FMG-VM-100-UG	Sí	Sí	Sí	Sí	Sí	No	No	No	No
FortiManager-VM Base + FMG-VM-1000-UG	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
FortiManager-VM Base + FMG-VM-5000-UG	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
FortiManager-VM Base + FMG-VM-U-UG	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí

Información para realizar pedidos: artículos adicionales de FortiManager	
SKU del producto	Descripción
FMG-WP	Agrega funcionalidad SDK del portal web a FortiManager (válido en FortiManager-1000C, FortiManager-3000C, FortiManager-5001A y FortiManager-VM

Información para realizar pedidos: dispositivos virtuales FortiManager		
SKU del producto	Dispositivos de red con licencia (máx.)	Descripción4
Evaluación incorporada	10	Licencia EVAL incorporada de 15 días, no requiere activación.
Evaluación completa (60 días)	10.000	Licencia EVAL. Se requiere licencia y activación.
G-VM-Base	10	El SKU base admite 10 dispositivos y usuarios de ADOM/WP/WP. Política Global incluida.
FMG-VM-10-UG	+10	Agrega 10 dispositivos y ADOM/WP/WPusers.
FMG-VM-100-UG	+100	Agrega 100 dispositivos y ADOM/WP/WPusers.
FMG-VM-1000-UG	+1000	Agrega 10000 dispositivos y ADOM/WP/WPusers.
FMG-VM-5000-UG	+5,000	Agrega 5000 dispositivos y ADOM/WP/WPusers.
FMG-VM-U-UG	Ilimitado5	Licencia ilimitada.

4 CPU virtuales ilimitadas. La memoria no está restringida hasta el límite del sistema operativo de 4 GB (32 bits)/Ilimitada (64 bits) 5 Limitado en software a 10 000 dispositivos, ADOM, portales web y usuarios de portales web.

Los servicios de suscripción de seguridad FortiGuard® ofrecen actualizaciones dinámicas y automatizadas para los productos Fortinet. El equipo de investigación de seguridad global de Fortinet crea estas actualizaciones para garantizar una protección actualizada contra amenazas sofisticadas. Las suscripciones incluyen antivirus, prevención de intrusiones, filtrado web, antispam, gestión de vulnerabilidades, control de aplicaciones y servicios de seguridad de bases de datos.

Los servicios de soporte FortiCare™ brindan soporte global para todos los productos y servicios de Fortinet. El soporte de FortiCare permite que sus productos Fortinet funcionen de manera óptima. Los planes de soporte comienzan con soporte mejorado 8x5 con reemplazo de hardware de "devolución y reemplazo" o soporte integral 24x7 con reemplazo avanzado. Las opciones incluyen soporte premium, RMA premium y servicios profesionales. Todos los productos de hardware incluyen una garantía limitada de hardware de 1 año y una garantía limitada de software de 90 días.

LA SEDE MUNDIAL
Fortinet Incorporado
1090 Kifer Road, Sunnyvale, CA 94086 EE. UU.
Teléfono +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/ventas

OFICINA DE VENTAS EMEA – FRANCIA
Fortinet Incorporado
120 rue Albert Caquot
06560, Sophia Antipolis, Francia
Teléfono +33.4.8987.0510
Fax +33.4.8987.0501

OFICINA DE VENTAS APAC – SINGAPUR
Fortinet Incorporado
300 Carretera de la Playa #20-01
La explanada, Singapur 199555
Teléfono: +65-6513-3734
Fax: +65-6295-0015

FST-PROD-DS-MG

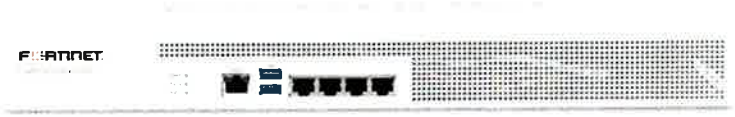
MC-CAT-R12-201

FORTINET

FortiSandbox™

FortiSandbox 500F, 1000F, 2000E, 3000E, VM, alojado en la nube y nube pública

FortiSandbox, el mejor valorado de Fortinet, es el núcleo de la solución Advanced Threat Protection (ATP) que se integra con Security Fabric de Fortinet para abordar las amenazas más específicas y en rápida evolución en una amplia superficie de ataque digital. Específicamente, ofrece inteligencia procesable en tiempo real a través de la automatización de la detección y mitigación avanzadas de malware de día cero.



Amplia cobertura del ataque Superficie con Tela de Seguridad

Defensa eficaz contra ataques dirigidos avanzados a través de una arquitectura cohesiva y extensible que trabaja para proteger redes, correos electrónicos, aplicaciones web y puntos finales desde el campus hasta la nube.

Día cero automatizado, avanzado Detección y mitigación de malware

La integración nativa y las API abiertas automatizan el envío de objetos desde Fortinet y puntos de protección de proveedores externos, y el intercambio de inteligencia sobre amenazas en tiempo real para una respuesta inmediata a las amenazas y una reducción de la dependencia de recursos de seguridad escasos.

Certificado y mejor calificado

Se somete constantemente a pruebas independientes rigurosas y reales y obtiene constantemente las mejores calificaciones al abordar amenazas conocidas y desconocidas.

Modos de implementación

Ser único

Integrado

Seguridad FortiGuard Servicios

www.fortiguard.com

FortiCare en todo el mundo

Soporte 24 horas al día, 7 días a la semana

soporte.fortinet.com

Certificaciones de terceros

NSS LABS RECOMMENDED

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

CARACTERÍSTICAS

Análisis de malware en zona de pruebas

Complemente sus defensas establecidas con un enfoque de zona de pruebas de dos pasos. Los archivos sospechosos y en riesgo se someten a la primera etapa de análisis con el galardonado motor AV de Fortinet, la consulta de inteligencia global FortiGuard* y la emulación de código. El análisis de la segunda etapa se realiza en un entorno contenido para descubrir el ciclo de vida completo del ataque mediante la actividad del sistema y la detección de devolución de llamadas. La Figura 1 muestra nuevas amenazas descubiertas en tiempo real.

Además de admitir el envío de FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (agente ATP) y Fabric-Ready Partner, las ofertas de proveedores de seguridad de terceros son compatibles a través de un conjunto de API abierto bien definido.

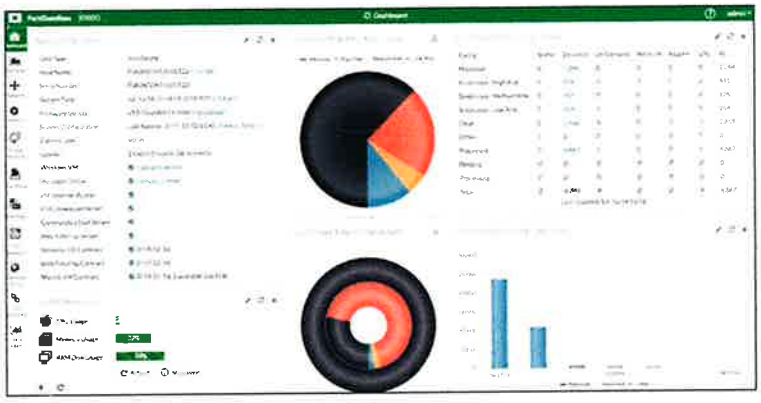


Figura 1: Panel de estado de amenazas en tiempo real basado en widgets

Herramientas de investigación y presentación de informes

Los informes con paquetes capturados, archivos originales, registros de seguimiento y capturas de pantalla proporcionan inteligencia sobre amenazas enriquecida y conocimientos prácticos después de examinar los archivos (consulte la Figura 2). Esto es para acelerar la remediación.

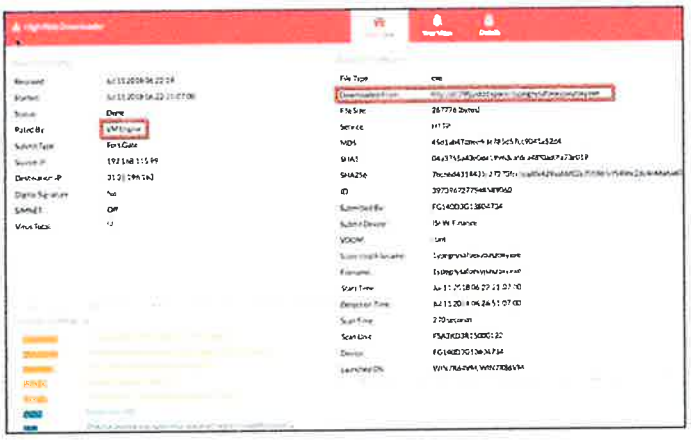


Figura 2: Informe detallado de malware con herramientas integradas

Mitigación de amenazas

La capacidad de Fortinet para integrar de forma única varios productos con FortiSandbox a través de Security Fabric ofrece protección automática con una configuración increíblemente simple. Una vez que se identifica un código malicioso, FortiSandbox devolverá calificaciones de riesgo y la inteligencia local se comparte en tiempo real con Fortinet y dispositivos y clientes registrados por proveedores externos para remediar e inmunizar contra nuevas amenazas avanzadas. La inteligencia local se puede compartir opcionalmente con el equipo de investigación de amenazas de Fortinet, FortiGuard Labs, para ayudar a proteger a las organizaciones a nivel mundial. La Figura 3 muestra el flujo del proceso de mitigación automatizado.

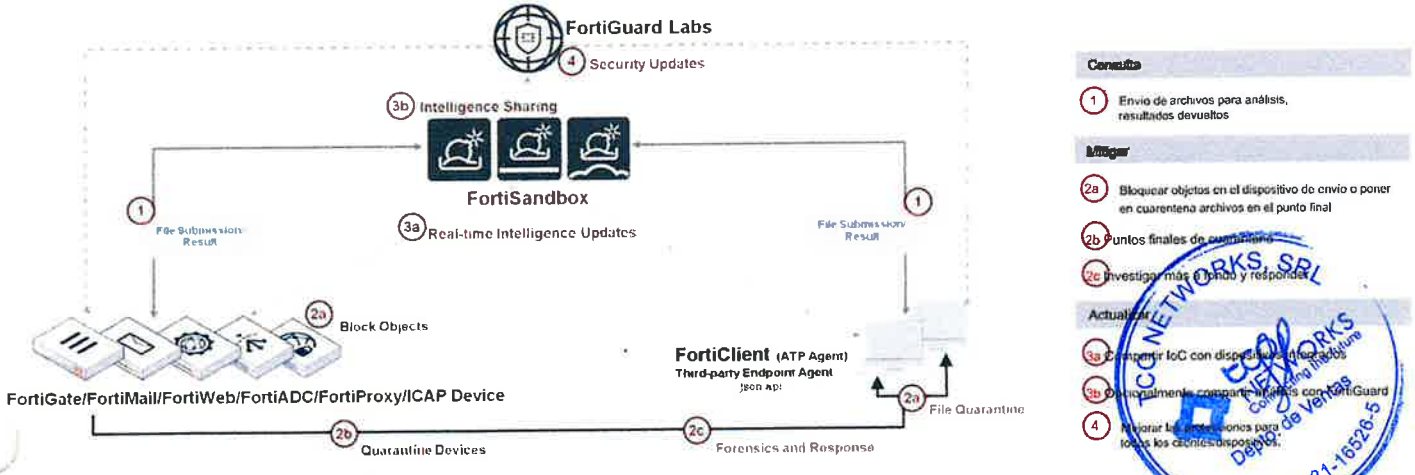


Figura 3. Flujo de trabajo de mitigación de amenazas de FortiSandbox

OPCIONES DE IMPLEMENTACIÓN

Fácil implementación

FortiSandbox admite la inspección de muchos protocolos en una solución unificada, lo que simplifica la infraestructura y las operaciones de la red. Además, se integra dentro de Security Fabric y agrega una capa de protección avanzada contra amenazas a su arquitectura de seguridad existente.

FortiSandbox es el dispositivo de análisis de amenazas más flexible del mercado, ya que ofrece varias opciones de implementación para las configuraciones y requisitos únicos de los clientes. Las organizaciones pueden optar por combinar estas opciones de implementación.

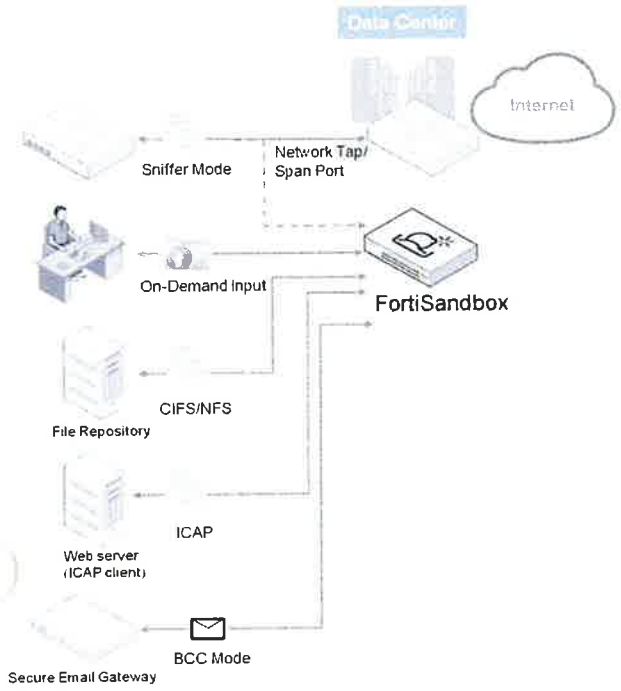


Figura 4: Implementación independiente

Ser único

Este modo de implementación de FortiSandbox acepta entradas como un servidor ICAP o desde puertos de conmutador distribuidos o grifos de red. También puede incluir cargas de archivos bajo demanda por parte de los administradores o escaneo de repositorios de archivos a través de CIF o NFS a través de la GUI. Es la opción ideal para mejorar un enfoque de protección contra amenazas de múltiples proveedores existente.

Integrado

Los productos de Fortinet, como FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy y FortiClient (agente ATP) y los proveedores de seguridad de terceros pueden interceptar y enviar contenido sospechoso a FortiSandbox cuando están configurados para interactuar con FortiSandbox. La integración también proporcionará capacidades oportunas de remediación y generación de informes a esos dispositivos.

Esta integración se extiende a otros FortiSandboxes para permitir el intercambio instantáneo de inteligencia en tiempo real. Esto beneficia a las grandes empresas que implementan múltiples FortiSandboxes en diferentes ubicaciones geográficas. Este modelo automatizado sin intervención es ideal para una protección integral en diferentes fronteras y zonas horarias.

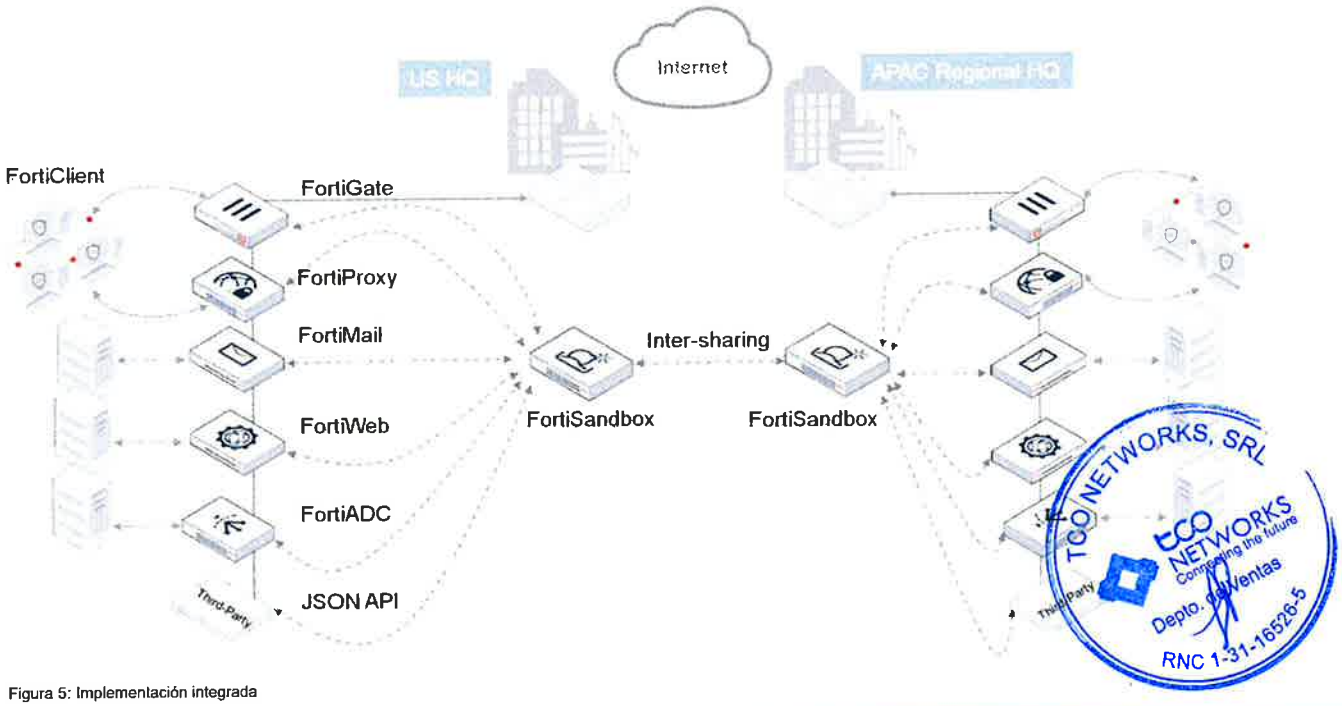


Figura 5: Implementación integrada

RESUMEN DE CARACTERÍSTICAS

ADMINISTRACIÓN

Admite configuraciones WebUI y CLI

Cuentas de usuario de administrador multinivel

Copia de seguridad y restauración del archivo de configuración

Correo electrónico de notificación cuando se detecta un archivo malicioso

Informe semanal a la lista global de correo electrónico y a los administradores de FortiGate

Página de búsqueda centralizada que permite a los administradores crear consultas de búsqueda personalizadas

Actualizaciones automáticas de fines frecuentes

Comprobación automática y descarga de nuevas imágenes de VM

Monitoreo del estado de la máquina virtual

Autenticación Radius para administradores

RED EN SANDBOXING

Soporte de enrutamiento estático

Entrada de archivos: modo sin conexión/fuera de línea, carga de archivos bajo demanda, envío de archivos desde dispositivos integrados

Opción para crear una red simulada para acceder al archivo escaneado en un entorno de red cerrado

Soporte de agrupación en clústeres de alta disponibilidad

Monitoreo de puertos para conmutación por error en un clúster

INTEGRACIÓN DE SISTEMAS

Entrada de archivos desde FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy y FortiClient (agente ATP)

Comentarios e informes sobre el estado del archivo: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy y FortiClient (agente ATP)

Actualización de Dynamic Threat DB: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy y FortiClient (agente ATP)

– Enviar periódicamente bases de datos premium a entidades registradas

– Suma de comprobación de archivos y base de datos de URL maliciosa

Actualizar proxy de base de datos FortiManager

Registro remoto: FortiAnalyzer, servidor syslog

API JSON para automatizar el proceso de carga de muestras y descarga de indicadores de malware personalizados para terceros

Integración certificada de terceros: CarbonBlack, Ziften, SentinelOne

Intercambio de COI entre FortiSandboxes

PROTECCIÓN AVANZADA CONTRA AMENAZAS

Inspección de nuevas amenazas, incluido ransomware y malware protegido con contraseña.

Análisis de código estático que identifica posibles amenazas dentro del código que no se está ejecutando

Análisis heurístico/basado en reputación

Virtual OS Sandbox –

Instancias simultáneas – por tipo de

sistema operativo compatible: Windows XP, Windows 7, Windows 8.1, Windows 10, macOS y Android

– Tiempos ajustados: llamadas de sueño, consultas de proceso y registro.

– Detección y devolución de llamada: visita de URL maliciosa, comunicación C&C de botnet y tráfico de atacantes procedente de malware activado

– Descargar capturas de captura: archivo original, registro de seguimiento y captura de pantalla

– Modo sincrónico: Sniffer

– Compatible con una VM personalizada

Compatibilidad con tipos de archivos: 7z, ace, ace, apk, ar, bat, bz2, cab, cmd, dll, dmg, doc, docm, docx, dot, dotm, dotx, exe, gz, hta, html, jar, lha, lnk, lzh, MacOffice, msi, pdf, pot, potm, potx, ppam, ppa, ppsm, ppsx, ppt, pptm, pptx, rar, rtf, sh, slom, tar, tgz, upa, url, vbs, WEBLink, wsf, xlam, xls, xlsb, xlsm, xlsx, xlt, xltm, xltx, xz, z, zip

Protocolos/aplicaciones admitidos: – Modo

renovador: HTTP, FTP, POP3, IMAP, SMTP, SMB

– Modo BCC: SMTP

– Modo integrado con FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM y sus equivalentes

Versiones cifradas con SSL

– Modo integrado con FortiMail: SMTP, POP3, IMAP

– Modo integrado con FortiWeb: HTTP

– Modo integrado con ClientEndPoint: HTTP

Personalice las máquinas virtuales para admitir varios tipos de archivos

Aislar el tráfico de máquinas de VM del tráfico del sistema

Detección de amenazas de red en modo Sniffer: identifique actividades de Botnet y ataques de red, así como URL maliciosas

Escanee recursos compartidos de red SMB/NFS y cargue en carpetas archivos sospechosos. El escaneo se puede programar

Escanee URL incrustadas dentro de archivos de documentos

Opción de integración con reglas de Yara de terceros

Opción de enviar automáticamente archivos sospechosos a otros equipos para análisis manual y revisión de firmas

Opción de reenviar archivos a un recurso compartido de red para realizar análisis adicionales por parte de hackers

Opción de lista blanca y lista negra de suma de comprobación de archivos

Envío de URL para escaneo y consulta desde correos electrónicos y archivos

INFORMES Y REGISTRO

Widgets de monitoreo en tiempo real (vistas por fuente y opciones de período de tiempo), estadísticas de resultados de escaneos, estadísticas de entrada (a lo largo del tiempo), principales hosts objetivo, principales malware, principales URL maliciosas, principales usuarios de dispositivos finales

Visor de eventos detallado: tabla dinámica con contenido de acciones, nombre de malware, clasificación, tipo, origen, destino, tiempo de detección y ruta de descarga

Registro: GUI, descarga del archivo de registro RAW

Generación de informes para archivos maliciosos: informes detallados sobre las características y comportamientos de los archivos, modificación de archivos comportamientos de procesos, comportamientos de registro, comportamiento en red, estadísticas de VM, cuadro de cronología y de comportamiento

Análisis adicional: archivos descargados, archivos de muestra, registros de seguimiento de sesiones, capturas de PCAP e indicadores en formato STIX

ESPECIFICACIONES

	FSA-500F	FSA-1000F	FSA-2000E	FSA-3000E
Hardware				
Factor de forma	1 RU	1 RU	2U	2RU
Interfaces de red totales	4 puertos GE RJ45	4x puertos GE RJ45, 4x ranuras GE SFP	4 puertos GE RJ45, 2 ranuras 10 GE SFP+	4 puertos GE RJ45, 2 ranuras 10 GE SFP+
[illegible]	1x 1 TB	2x 1 TB	2x 2TB	4x 2 TB
Fuentes de alimentación	[illegible]	[illegible]	[illegible]	[illegible]
Rendimiento de sistema				
Número de máquinas virtuales	6*	14*	24*	56*
Rendimiento del prefiltro de Sandbox (archivos/hora)1	4.500	7.500	12.000	15.000
Rendimiento del espacio aislado de VM (archivos/hora)	120	280	480	1,120
Rendimiento efectivo en el mundo real (archivos/hora)	6002 3603	1,4002 8403	2,4002 1,4403	5,6002 3,3603
Rendimiento del rastreador	500Mbps	1 Gbps	4 Gbps	8 Gbps
Dimensiones				
Alto x Ancho x Largo (pulgadas)	1,73 x 17,24 x 12,63	1,73 x 17,24 x 22,83	3,46 x 17,24 x 20,87	3,5 x 17,2 x 29
Alto x Ancho x Largo (mm)	44x438x320	44x438x580	88x438x530	89x437x738
Peso	18,72 libras (8,5 kg)	25 libras (11,34 kg)	27 libras (12,25 kg)	43 libras (19,52 kg)
Ambiente				
Consumo de energía (promedio/máximo)	30,1 / 76,3W	66,93 / 116,58W	164,7 / 175,8W	538,6 / 548,6W
Corriente máxima	100/8A, 240V/4A	100V/5A, 240V/3A	100V/8A, 240V/4A	100V/9,8A, 240V/5A
Disipación de calor	260,34 BTU/h	397,75 BTU/h	600,1 BTU/hora	1,943,82 BTU/h
[illegible]	100–240 VCA, 60–50 Hz	100–240 VCA, 60–50 Hz	100–240 VCA, 60–50 Hz	100–240 VCA, 60–50 Hz
Humedad	5–90% sin condensación	5–90% sin condensación	5–90% sin condensación	8–90% (sin condensación)
Rango de temperatura de funcionamiento	32 a 104 °F (0 a 40 °C)	32 a 104 °F (0 a 40 °C)	32 a 104 °F (0 a 40 °C)	50–95°F (10–35°C)
Rango de temperatura de almacenamiento	-4 a 158 °F (-20 a 70 °C)	-40 a 158 °F (-40 a 70 °C)	-4 a 158 °F (-20 a 70 °C)	-40 a 158 °F (-40 a 70 °C)
Cumplimiento				
Certificaciones	FCC Parte 15 Clase A, C-Tick, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST			

	FORTISANDBOX-VM	NUBE FORTISANDBOX
Requisitos de hardware		
Soporte de hipervisor	VMware ESXi versión 5.1 o posterior, Linux KVM CentOS 7.2 o posterior, AWS (On-Demand y BYOL)	N / A
CPU virtuales (mínimo/máximo)	4 / Ilimitado (Fortinet recomienda que el número de vCPU coincida con el número de VM de Windows +4)	N / A
Soporte de memoria (mínimo/máximo)	8GB / Ilimitado	N / A
Almacenamiento virtual (mínimo/máximo)	30GB / 16TB	N / A
Total de interfaces de red virtual (mínimo)	6	N / A
Rendimiento de sistema		
Rendimiento del rastreador	1 Gbps	N / A
Rendimiento del prefiltro de Sandbox (archivos/hora)1	Dependiente del hardware	--
[illegible]	[illegible]	VM en la nube
[illegible]	8 máquinas virtuales, todos hasta 99 nodos cluster	[illegible] (hasta 200 máquinas virtuales en la nube de Windows)
Rendimiento del espacio aislado de VM (archivos/hora)	Dependiente del hardware	100 (hasta 1000)
Rendimiento efectivo en el mundo real (archivos/hora)2	Dependiente del hardware	500 (hasta 20,000)2 , 300 (hasta 12,000)3

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

1 El prefiltrado de FortiSandbox funciona con FortiGuard Intelligence.

2 Medido en función del tráfico web y de correo electrónico del mundo real cuando todo el prefiltrado dinámico funcionan correctamente.

3 Medido en función del tráfico de correo electrónico [illegible]

** Consulte la descripción del servicio en la nube FortiSandbox.

Forti Sandbox 500F

FortiSandbox 1000F

Forti Sandbox 2000E

Forti Sandbox 3000

MATRIZ DE INTEGRACIÓN

		FORTIGATE	FORTICLIENT	FORTIMAIL	FORTIWEB	FORTIADC	FORTIPROXY
Envío de archivos de máquina virtual y dispositivo FSA		*FortiOS V5.0.4+	FortiClient para sistema operativo Windows V5.4+	FortiMail OS V5.1+	Sistema operativo FortiWeb V5.5+	Sistema operativo FortiADC V5.0+	Sistema operativo FortiProxy V1.0+
	Consulta sobre identidad de archivo	*FortiOS V5.0.4+	FortiClient para sistema operativo Windows V5.4+	FortiMail OS V5.1+	Sistema operativo FortiWeb V5.4+	Sistema operativo FortiADC V5.0+	Sistema operativo FortiProxy V1.0+
	Presentar informe detallado	*FortiOS V5.4+	FortiClient para sistema operativo Windows V5.4+	FortiMail OS V5.1+	–	Sistema operativo FortiADC V5.0+	Sistema operativo FortiProxy V1.0+
	Actualizar archivo base a prevención	*FortiOS V5.4+	FortiClient para sistema operativo Windows V5.4+	FortiMail OS V5.3+	Sistema operativo FortiWeb 5.4+	Sistema operativo FortiADC V5.0+	Sistema operativo FortiProxy V1.0+
Nube FortiSandbox	Envío de archivos	*FortiOS V5.2.3+	–	Sistema operativo FortiMail V5.3+	Sistema operativo FortiWeb 5.5.3+	–	Sistema operativo FortiProxy V1.0+
	Consulta sobre identidad de archivo	*FortiOS V5.2.3+	–	Sistema operativo FortiMail V5.3+	Sistema operativo FortiWeb 5.5.3+	–	Sistema operativo FortiProxy V1.0+
	Presentar informe detallado	*FortiOS V5.2.3+	–	–	–	–	Sistema operativo FortiProxy V1.0+
	Actualizar archivo base a prevención	*FortiOS V5.4+	–	Sistema operativo FortiMail V5.3+	Sistema operativo FortiWeb 5.5.3+	–	Sistema operativo FortiProxy V1.0+

*Algunos modelos pueden requerir configuración CLI

INFORMACIÓN DEL PEDIDO

Producto	SKU	Descripción
Fort Sandbox 500F	FSA-500F	Sistema avanzado de protección contra amenazas: 4x GE RJ45, 2 máquinas virtuales con licencia con Win7, Win10 y (1) licencia de MS Office incluidas. Actualizable a un máximo de 8 VM.
Fort Sandbox 1000F	FSA-1000F	Sistema avanzado de protección contra amenazas: 4 ranuras GE RJ45, 2 ranuras GE SFP, 2 máquinas virtuales con Win7, Win10 y (1) licencia de MS Office incluidas. Actualizable a un máximo de 14 máquinas virtuales con licencia. Consulte el SKU FSA-1000F-UPG-LIC-6 o FC-10-FS1KF-176-02-DD.
Fort Sandbox 2000E	FSA-2000E	Sistema avanzado de protección contra amenazas: 4 ranuras GE RJ45, 2 ranuras 10 GE SFP+, fuente de alimentación redundante, 4 máquinas virtuales con Win7, Win8 Win10 y (1) licencia de MS Office incluidas. Actualizable a un máximo de 24 máquinas virtuales con licencia.
Fort Sandbox 3000E	FSA-3000E	Sistema avanzado de protección contra amenazas: 4 ranuras GE RJ45, 2 ranuras 10 GE SFP+, fuente de alimentación redundante, 8 máquinas virtuales con Win7, Win8 Win10 y (1) licencia de MS Office incluidas. Actualizable a un máximo de 56 máquinas virtuales con licencia. Cumple con TAA.
Fort Sandbox-VM	FSA-VM-00	Dispositivo virtual FortiSandbox-VM con 0 VM incluidos y expansión máxima limitada a 8 VM en total por nodo, hasta 99 nodos por cluster
Máquina virtual en la nube de Windows FortiSandbox	FC-10-FSA01-195-02-DD	Servicio FortiSandbox Windows Cloud VM para (5) Windows VM y expansión máxima limitada a (200) Windows Cloud VM por FortiSandbox VM.
Máquina virtual en la nube FortiSandbox macOS	FC-10-FSA01-192-02-DD	Servicio macOS Cloud VM para (2) VM macOS X y expansión máxima limitada a (8) VM macOS X por FortiSandbox (Dispositivo/VM).
Servicio en la nube Fort Sandbox	FC-10-XXXXX-123-02-12	Suscripción al servicio de nube FortiSandbox (SKU varía según los modelos FortiGate/FortiMail/FortiProxy/FortiWeb)
Accesorios Opcionales		
1 módulo transceptor GE SFP SX	FG-TRAN-SX	1 módulo transceptor GE SFP SX para todos los sistemas con ranuras SFP y SFP SFP+.
1 módulo transceptor GE SFP LX	FG-TRAN-LX	1 módulo transceptor GE SFP LX para todos los sistemas con ranuras SFP y SFP SFP+.
Módulo transceptor SFP+ de 10 GE, corto alcance	FG-TRAN-SFP+SR	Módulo transceptor SFP+ de 10 GE, de corto alcance para todos los sistemas con ranuras SFP+ y SFP SFP+.
Módulo transceptor SFP+ de 10 GE, largo alcance	FG-TRAN-SFP+LR	Módulo transceptor SFP+ de 10 GE, de largo alcance para todos los sistemas con ranuras SFP+ y SFP SFP+.

FORTINET

LA SEDE MUNDIAL
Fortinet Inc.
899 CARRETERA KIFER
Sunnyvale, CA 94085
Estados Unidos
Teléfono: +1.408.235.7700
www.fortinet.com/ventas

OFICINA DE VENTAS EN EMEA
905 calle Albert Einstein
06560 Valbonne
Francia
Teléfono: +33.4.8987.0500

OFICINA DE VENTAS APAC
8 Bulevar Temasek
#12-01 Torre Tres Suntec
Singapur 038988
Teléfono: +65.6395.2788

OFICINA DE VENTAS PARA AMÉRICA LATINA
Centro de los lagos Sawgrass
13450 W. Sunrise Blvd., Suite 430 Sunrise,
FL 33323
Estados Unidos
Teléfono: +1.954.368.9990