

# FORTIMAIL™ 400

**Plataforma de Seguridad de Correo Electrónico de Alto Rendimiento**



FortiMail ha sido diseñado específicamente como una plataforma de mensajería segura que ofrece protección multinivel contra las amenazas combinadas que se propagan por nuestras redes vía el correo electrónico: spam, virus, gusanos y spyware. Sus elevados rendimientos y ratios de detección, así como la flexibilidad de su despliegue –con MTA integrado– hacen de FortiMail la solución idónea de protección de correo electrónico.

## CARACTERÍSTICAS

- Tres modos de funcionamiento
- Antispam
- Antivirus
- Antispyware
- Filtro de contenidos
- Protección ante denegación de servicio
- Alta disponibilidad
- Actualizaciones automáticas

Fortinet, la compañía pionera y líder del mercado de seguridad integral, ofrece a las empresas una de las plataformas de seguridad integral de correo electrónico líder: FortiMail. Estos sistemas han sido diseñados específicamente como plataformas de mensajería segura que ofrecen protección total antispam, evitando que éste se introduzca en la red corporativa. FortiMail incluye un motor de detección antivirus para la protección frente a virus y spyware y las más completas herramientas de escaneo de correo electrónico. Estos dispositivos se integran sin fisuras con las galardonadas aplicaciones de seguridad FortiGuard Antivirus y Antispam de Fortinet, las cuales ofrecen actualizaciones automáticas tanto a los sistemas FortiMail como FortiGate para detectar el spam en el perímetro de red.

seguridad de correo electrónico FortiMail permite una versatilidad única en la industria para cubrir los más altos requerimientos de seguridad minimizando el impacto de su integración en las redes corporativas.

Este appliance, a diferencia de todos sus competidores, ofrece tres modos de despliegue: transparente, gateway y server.

## MOTORES DE DETECCIÓN

Con el fin de detectar todo tipo de códigos maliciosos, FortiMail dispone de diversos motores de detección a nivel de conexión y a nivel de aplicación, entre los que destacan las técnicas antivirus, que poseen las certificaciones más importantes de la industria, tales como ICSA y VB100. Asimismo, entre las funcionalidades del antivirus cabe destacar el escaneo de virus/spyware en correo SMTP, el soporte de antivirus en archivos comprimidos y anidados, la cuarentena de ficheros infectados, el bloqueo de ficheros por tamaño y

el filtrado de fichero adjuntos por extensión o cabecera MIME.

## TÉCNICAS ANTISPAM

Por otro lado, dentro de las técnicas antispam de la plataforma FortiMail podemos destacar FortiGuard Antispam –existen cinco bases de datos contra las que el correo es chequeado–; Forged IP – comprobación inversa del DNS de la IP del servidor que intenta entregar correo–; Grey List –esta técnica dota a FortiMail de una gran efectividad eliminando conexiones innecesarias–; escaneo Bayesiano y Heurístico –el filtro bayesiano aprende a medida que el spam es reconocido, mientras que el filtro heurístico asigna puntuación a los mensajes dependiendo de varios parámetros, si el correo sobrepasa un umbral es reconocido como spam–; Banned Word –permite definir listas de palabras prohibidas dentro de los mensajes–; escaneo de imágenes –se reconocen los mensajes de spam que están compuestos exclusivamente por

## DESPLIEGUE

La variedad de modos de despliegue de las plataformas de

imágenes y que no son susceptibles de ser analizados por otras técnicas-; técnicas de sesión -determina si el servidor es un spammer, con lo que no se aceptarán mensajes de ese equipo-; Sender Reputation - control sobre los servidores para evitar los equipos spammers-.

categorías diferentes que permiten una minuciosa clasificación de los mensajes de log, con lo que se consigue realizar búsquedas mucho más exhaustivas, utilizando filtros que simplifican la tarea de encontrar un evento en particular. Además, FortiMail también permite la generación y envío automatizado de informes, con lo que estos pueden ser generados y enviados de forma totalmente desatendida.

permite actualizaciones automáticas y programadas, con lo que se consigue que tanto las bases de datos de virus, gusanos y spyware como los motores de escaneo de spam están continuamente actualizados. Estas actualizaciones son distribuidas mediante la red de distribución de contenidos FortiProtect Distribution Network tan pronto como nuevos virus y gusanos son encontrados y difundidos.

### OPCIONES DE REPORTING

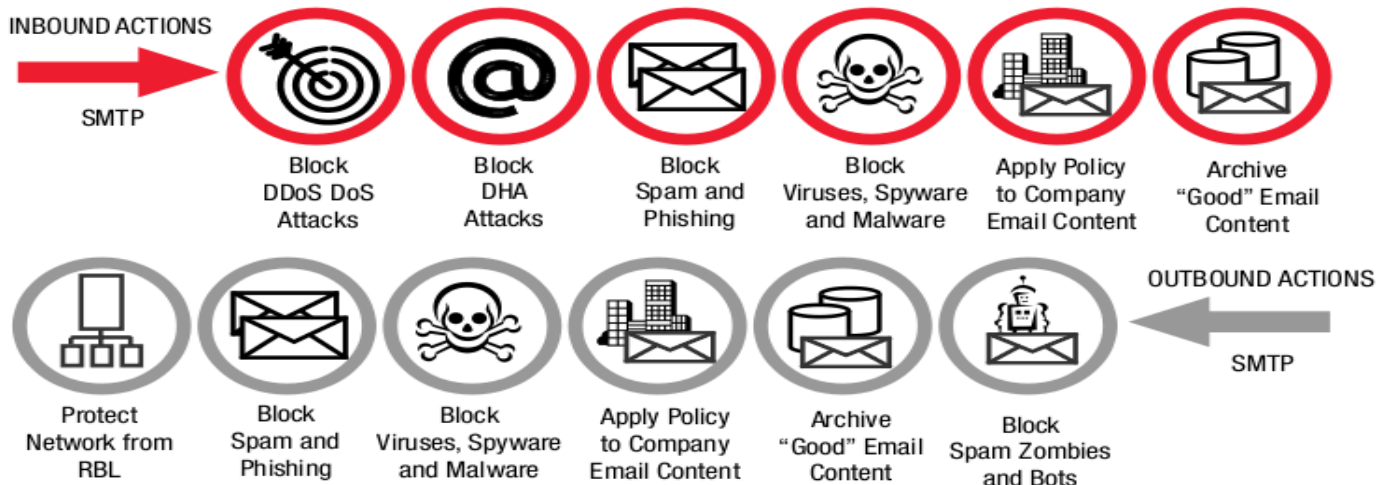
La solución FortiMail incorpora una potente herramienta de gestión de logs que clasifica los eventos generados por el sistema en cuatro

### ACTUALIZACIONES

Por otro lado, esta plataforma

## Aspectos más destacados en Fortimail

- Sistema operativo de alta estabilidad y rendimiento con sistema de almacenamiento RAID
- Altos ratios de precisión y detección
- Las actualizaciones automáticas seguras del antivirus y de su motor de detección garantizan una protección siempre al día de spam, virus, gusanos y otros archivos adjuntos malintencionados.
- Diseño de dispositivo con interfaz web intuitiva para una rápida configuración e instalación
- MTA (Mail Transfer Agent) de alto rendimiento basado en estándar
- Soporta copias de seguridad, lo que permite almacenar de forma remota el correo electrónico archivado para satisfacer las necesidades a largo plazo
- Soporta un amplio grupo de tecnologías multinivel de detección y filtrado de spam, con políticas de spam globales y por usuario dando la máxima flexibilidad de configuración
- El Modo transparente permite una perfecta integración en los entornos de red existentes
- Antivirus y Antispam certificados por ICSA LABS y VB100
- Protección contra ataques DDOS DOS
- Análisis de Spam bidireccional
- No licenciamiento por usuarios
- Soporte para configuración en Alta Disponibilidad
- Reporting & Logs avanzado



## Especificaciones del sistema

### FortiMail 400



### Especificaciones Hardware:

Puertos Ethernet .....	4x 10/100 Ethernet ports 2x 10/100/1000 Ethernet ports
Procesador .....	Single 3.0 GHz CPUs
Memoria .....	1 GB of RAM
Almacenamiento .....	2x / 250GB 3.5" IDE drives
Hardware RAID .....	(0, 1)
Dimensions (H, W, L) .....	4.5 x 42.7 x 25.4 cm
Weight.....	3,3 kg
Rack Mountable .....	Yes
Input Voltage .....	100-240VAC
Input Current .....	4A
Operating Temperature .....	32 to 104 deg F (0 to 40 deg C)
Storage Temperature .....	-13 to 158 deg F (-25 to 70 deg C)
Humidity .....	5 to 95% non-condensing
Regulatory .....	FCC Class A Part 15 / CE Mark

## Características principales

### Modos Transparente y Gateway

- Soporta múltiples dominios de correo electrónico
- Actúa como pasarela de correo SMTP para los servidores de correo existentes
- Despliegue rápido y sencillo mediante un simple cambio de registro MX de DNS (Modo Gateway)
- Enrutamiento y gestión de colas de correo integrados basado en políticas
- Funciona como un relay del correo saliente para mejorar la seguridad del correo
- Políticas de detección granular en niveles que previenen el spam y la propagación de virus
- Notificación mediante mensajes de sustitución antivirus
- Puesta en cuarentena y marcado del spam
- Aceptación, retransmisión, rechazo o eliminación del spam basándose en la dirección de correo electrónico, la dirección IP o el dominio
- Acceso al correo electrónico en cuarentena a través de WebMail, POP3 e IMAP
- Resúmenes diarios de mensajes en cuarentena
- Función de archivo, basado en políticas, de los mensajes de correo electrónico entrantes y salientes, con soporte de copia de seguridad para almacenamiento remoto
- Monitorización, registro e informes completos del correo electrónico
- Soporta cola de correo para mensajes fallidos, diferidos e imposibles de entregar
- Control del tamaño máximo de correos electrónicos
- Soporta autenticación SMTP mediante LDAP, RADIUS, POP3 o IMAP
- Lista Blanca Automática por usuario
- Aceleración de DNS
- Configuración antivirus y antispam por usuario mediante consulta LDAP

### Modo Servidor

Todas las características de los Modos Transparente y Gateway y además, las siguientes:

- Servicios de correo electrónico POP3, SMTP e IMAP
- Soporta SMTP sobre SSL
- Soporta políticas de cuota de disco para cuentas de usuario
- Acceso seguro a cliente de WebMail
- Soporta listas de usuarios, grupos y alias
- Autenticación LDAP y listas locales
- Soporta carpetas bulk para el spam

### Protección antivirus

- Explora en busca de virus los mensajes SMTP
- Soporta exploración de archivos adjuntos

comprimidos y anidados

- Cuarentena de archivos infectados
- Notificación mediante mensaje de sustitución
- Bloqueo por tipo de archivo
- Filtrado de archivos adjuntos

### Protección contra Denegación de Servicio

- Denegación de Servicio (mail bombing)
- Ataques de dirección de destinatario
- Limitación de tasa de correo
- Comprobación inversa de DNS (anti-spoofing)
- Dirección falsa del remitente

### Tecnologías de detección de FortiMail:

- Motor de detección antivirus FortiGate para detección de virus
- Actualización automática de firmas de antivirus y ataques a través de la red global de FortiProtect
- Exploración completa del correo electrónico: asunto, cuerpo, cuerpo básico, URI y meta-información
- Métodos avanzados de detección y filtrado de spam:
  - Filtrado de política de acceso
  - Filtrado de contenidos
  - Filtrado mediante listas blancas/negras globales y de usuario
  - Filtrado en tiempo real mediante listas de blackhole (RBL)
  - spam URI RBL (SURBL)
  - Servicio FortiGuard AntiSpam (tecnología avanzada de listas negras multinivel)
  - Filtrado bayesiano por usuario
  - Filtrado heurístico (más de 900 reglas)
  - Centro de Comprobación Distribuido de Firmas Digitales (DCC)
- Base de datos global de formación bayesiana para una personalización rápida

### Capacidades de registro y generación de informes de FortiMail

- Registro de cambios de configuración y sucesos de administración
- Registro de incidentes de antivirus
- Registro de actividades antispam
- Soporta servidor de conexión al sistema externa o local
- Informes centralizados ampliados gracias al soporte de FortiReporter
- Alertas de sucesos críticos e incidentes de virus
- Completa generación de informes con más de 140 parámetros en siete categorías
- Generación de informes programada