



## **FortiMail 3.0**

# **Seguridad integral de correo electrónico**

En colaboración con **TCN**

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.

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.

### DESPLIEGUE

La variedad de modos de despliegue de las plataformas de 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.

En el modelo transparente, FortiMail actúa como un bridge ofreciendo todas las características de protección disponibles en la plataforma, así como la gestión de cuarentenas o la administración centralizada mediante acceso Web al interfaz de gestión. Además, opera como proxy transparente analizando el tráfico SMTP entrante o saliente, hacia o desde los servidores SMTP corporativos.

Operando en modo Gateway, FortiMail se comporta como un sistema securizado de relay SMTP, llevando a cabo las labores de inspección del correo en busca de ataques dirigidos contra los servidores o relays de correo. Y por último, cuando se emplea el despliegue en modo server, lleva a cabo las labores de servidor de correo integral soportando SMTP, POP3 e IMAP, así como acceso Webmail, todo ello cumpliendo las expectativas propias de securización de una plataforma de mensajería. El modo server está especialmente indicado para entornos PYME en los que se busca un sistema potente y seguro minimizando la gestión administrativa de la plataforma de mensajería global.



### CARACTERÍSTICAS

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

### 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 VBI00. 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 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–.

### OPCIONES DE REPORTING

La solución FortiMail incorpora una potente herramienta de gestión de logs que clasi-

fica los eventos generados por el sistema en cuatro 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.

### ACTUALIZACIONES

Por otro lado, esta plataforma 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 estén 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.

## FortiMail-4000A & IronPort Systems C350

Para medir la eficacia del sistema FortiMail-4000A para bloquear spam y virus en los mensajes de correo, los ingenieros de The Tolly Group realizaron un estudio, comparando este equipo con el sistema IronPort Systems C350, midiendo el porcentaje de spam bloqueado, el número de falsos positivos y falsos negativos, así como los mensajes de virus detectados. Además, también tuvieron en cuenta la seguridad y flexibilidad de despliegue. Estas pruebas se llevaron a cabo en noviembre de 2007.

Category	FortiMail-4000A	IronPort C350
Inbound Messages Tested*	29,187	27,280
Total Spam	28,751	26,581
Spam Blocked Correctly	28,726	26,544
Spam Detection Percentage	99.91%	99.86%
False Negatives (Spam missed)	31 out of 28,751	37 out of 26,581
False Positives (Classified as SPAM but not actually spam)	6 out of 1,984 quarantined messages	0 out of 261 quarantined messages
Legitimate Messages	426 out of 29,187	699 out of 27,280
Virus Messages Detected	4 out of 29,187	0 out of 27,280

## Formación técnica y comercial que ayudará a su implantación

Mambo Technology ofrece formación técnica y comercial continua sobre los productos y soluciones de su catálogo a toda su red de partners y canal de distribución informática: resellers, integradores, consultoras y service providers. Los programas de formación que desarrolla están orientados a cubrir las áreas de networking y comunicaciones,

así como políticas de seguridad, firewalls y VPNs. En el caso concreto de los equipos Fortinet FortiMail, Mambo facilita a su canal de partners e integradores cursos de formación gratuita o a coste reducido. La formación es impartida por personal altamente cualificado técnico y comercial de Mambo Technology o de los propios

fabricantes en salas de formación y en el domicilio del cliente si éste así lo solicitara. Otro de los alicientes que Mambo ofrece a su canal de distribución, es la posibilidad de equipos en préstamo sin coste

alguno ni compromiso de compra, lo que permite ahondar en el conocimiento de estas soluciones. Además, también asesora a sus socios en la integración y configuración de estas soluciones de seguridad y networking, aportando un valor añadido a sus clientes en lo que se refiere a conocimiento y prescripción de nuevas tecnologías.





# XUNTA DE GALICIA Proyecto Antispam

La Xunta de Galicia contaba con soluciones Antivirus y Antispam distribuidas basadas en aplicaciones software instaladas en cada uno de los múltiples servidores de correo, para proteger los más de 20.000 buzones y casi 500.000 mil correos diarios con los que cuenta en la actualidad.

Además de bajos niveles de eficacia de detección y elevados índices de falsos positivos, este tipo de solución les generaba problemas tanto de administración, al tratarse de una solución descentralizada, como de rendimiento, al llegar todo el correo infectado a los servidores finales consumiendo altos niveles de recursos en éstos y afectando en consecuencia a la disponibilidad global de la aplicación de Correo Electrónico. Con este problema de fondo se planteó el proyecto de securización y optimización de la plataforma de correo electrónico, con el que se buscaba dotar de forma centralizada la seguridad necesaria, descargando a los servidores internos de estas labores e impidiendo que el correo infectado, más del 80% del total recibido, llegase a los mismos mermando de forma innecesaria sus recursos.

Tras testar en producción varias soluciones de la industria, la Xunta de Galicia finalmente se decantó por dos equipos appliance Fortinet FortiMail4000A en alta disponibilidad, colocados como relays SMTP, proporcionando funcionalidades de Antivirus SMTP y Antispam. Las razones principales de dicha decisión fueron su facilidad de gestión, los altos niveles de efectividad de detección, los bajos niveles de falsos positivos y el alto rendimiento proporcionado.

## PROYECTO DE NAVEGACIÓN SEGURA

La Xunta de Galicia carecía de solución para proteger la navegación de los más de 50.000 puestos de trabajo de sus distintas redes



### SOLUCIONES

- Correo electrónico
  - FortiMail4000A
- Navegación web
  - FG5050
  - FortiManager3000
  - FortiAnalyzer2000A

internas, entre ellas la Red Corporativa de la Xunta y la Red de Educación de Galicia, que generan por encima de los 500 Mbps de tráfico HTTP. En este marco, y ante la necesidad de garantizar la seguridad en la navegación, así como limitar el acceso a determinadas páginas potencialmente peligrosas o improductivas, se abrió un proceso de evaluación de las distintas herramientas del mercado capaces de proporcionar los altos niveles de seguridad y rendimientos requeridos para proteger semejante caudal de tráfico, siendo uno de los principales requisitos de la Xunta que la solución finalmente elegida no introdujese retardos apreciables en la navegación. Fruto de este proceso de evaluación, en el que se realizaron pruebas en producción con numerosos fabricantes, se eligió finalmente Fortinet

por su gran nivel de eficacia de detección de virus y malware en el tráfico de navegación, por su elevado nivel de eficiencia de categorización de los sites de Internet y por el altísimo rendimiento demostrado durante las pruebas en comparación con el

resto de fabricantes. La solución final, basada en los chasis FG5050 de Fortinet, contempló cuatro blades FG5005FA2 en alta disponibilidad trabajando de forma Activa, proporcionando de forma transparente Antivirus, Antimalware y Filtrado de URLs. La solución se completó con FortiManager3000, para disponer de las bases de datos de categorización y firmas en local, y de FortiAnalyzer2000A, para poder almacenar y explotar toda la información de logs generados por esta potente solución de Navegación Limpia.