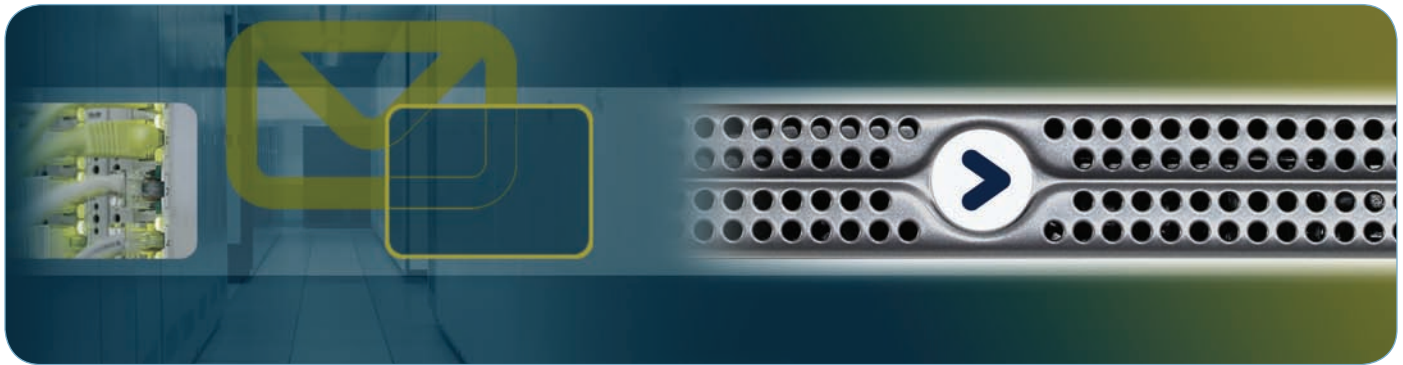


# Proofpoint Messaging Security Gateway Appliances



## Proofpoint on Demand Hosted Service y Proofpoint Protection Server Software



**Proofpoint Messaging Security Gateway™ appliances, Servicio Proofpoint on Demand™ y Proofpoint Protection Server® software protegen en contra de amenazas de mensajería entrante, previenen fugas de información sensible, encriptan mensajes y analizan la infraestructura de su mensajería. Su arquitectura unificada, defensas modulares y su interfaz de administración de políticas protegen las organizaciones contra todo tipo de riesgos de mensajería en la empresa, justo en la entrada.**

### defiende, previene, encripta, analiza

¿Por qué comprar otra solución puntual? La plataforma unificada de Proofpoint para seguridad de correo electrónico y prevención de pérdida de datos brinda protección integral contra riesgos de seguridad que plantean las amenazas entrantes y los contenidos salientes. La arquitectura modular de Proofpoint permite desplegar fácilmente nuevas defensas y adaptarse a nuevas amenazas.

Todas las funciones de Proofpoint, incluyendo antispam, antivirus, seguridad de contenido en múltiples protocolos, reportes y encriptación basados en políticas, se manejan centralmente desde una sola interfaz gráfica de usuario (Graphical User Interface, GUI) administrada. Las funciones pueden ser reportadas en casi cualquier configuración para satisfacer los requisitos específicos de su organización.

Ya sea que su despliegue implique un solo servidor de Proofpoint, múltiples appliances distribuidos globalmente, todas las tareas de manejo y gestión de políticas se controlan a través de la consola de administración basada en Web.

### opciones flexibles

Las soluciones de Proofpoint para seguridad de correo electrónico y prevención de pérdida de datos se ofrecen en diferentes plataformas para acoplarse a las necesidades de cada cliente:

- **Appliance:** Proofpoint Messaging Security Gateway es un dispositivo fácil de implementar, seguro y reforzado que se instala en minutos. Este dispositivo se encuentra disponible en una variedad de modelos para dar asistencia a empresas de cualquier tamaño.
- **Virtual Appliance:** Proofpoint Messaging Security Gateway—Virtual Edition proporciona la mejor protección de su clase con igual calidad que los appliances de Proofpoint; en combinación con los muchos beneficios de la virtualización, tales como la reducción de costos y administración simplificada y fácil de respaldar en caso de desastres. El dispositivo virtual funciona en cualquier computadora de escritorio x86 o servidor estándar que use VMware Server o VMware Infrastructure.
- **Software:** Proofpoint Protection Server brinda la plataforma de seguridad de mensajes de Proofpoint como software para el sistema operativo Red Hat Enterprise Linux.
- **Hosted Services:** Proofpoint on Demand ofrece funciones de seguridad de correo electrónico y de prevención de pérdida de datos como un servicio altamente adaptable, que no requiere de hardware ni software en las instalaciones.

### Seguro. Efectivo. Fácil de desplegar.

Estas son solo algunas maneras de describir la plataforma unificada de seguridad de correo electrónico y la prevención de la pérdida de datos de Proofpoint. Es la solución más poderosa de la industria presentada como un dispositivo, un dispositivo virtual o un software listos para usar para la empresa que ofrece:

- Detección de spam y manejo de las conexiones inigualables
- Protección contra virus y epidemias de nivel internacional
- Prevención de la pérdida de datos en múltiples protocolos y seguridad del contenido integrales
- Encriptación de mensajes de correo electrónico basado en políticas
- Informes y análisis avanzados
- Gestión unificada de políticas
- Rendimiento de nivel empresarial
- Despliegue y habilitación rápidos
- Arquitectura de escalabilidad óptima

**“En Pacific Sunwear, evaluamos una gran cantidad de productos antispam, antivirus y productos de exploración de contenido, y Proofpoint fue la primera compañía en presentar una plataforma que resuelve todos nuestros desafíos relacionados con la mensajería y el correo electrónico mediante una solución sencilla, fácil de desplegar y de manejar. El dispositivo Messaging Security Gateway ha regresado nuestro canal de correo electrónico a su lugar correcto como un canal estratégico para las comunicaciones comerciales, en lugar de ser una puerta giratoria para las amenazas contenidas en los mensajes”.**

**Ron Ehlers**  
VP de Sistemas de Información  
Pacific Sunwear

# Proofpoint Messaging Security Gateway y Proofpoint Protection Server

## completa protección

### Tecnología Proofpoint MLX

#### Aprendizaje automático avanzado

La potencia que alimenta las soluciones de seguridad para mensajería empresarial de Proofpoint, Proofpoint MLX, es un sistema avanzado de aprendizaje automático, con patente pendiente desarrollado por científicos en el Centro de Respuestas a Ataques de Proofpoint. Basado en técnicas estadísticas avanzadas que incluyen la regresión logística y el análisis del incremento de la información, Proofpoint MLX permite la clasificación e identificación precisas de contenido no estructurado, como el contenido en el correo electrónico y en otros documentos.

#### Precisión incomparable

Proofpoint MLX es la base de la precisión antispam sin igual brindada por el módulo Proofpoint Spam Detection. Con el uso de MLX, Proofpoint analiza cientos de miles de atributos de estructura, imágenes, contenido y reputación para diferenciar de manera precisa entre spam y mensajes válidos. Las soluciones antispam tradicionales evalúan únicamente una cantidad de atributos limitada y no son capaces de clasificar el spam de manera decisiva, lo que ocasiona una baja efectividad y un alto índice de resultados falsos positivos.

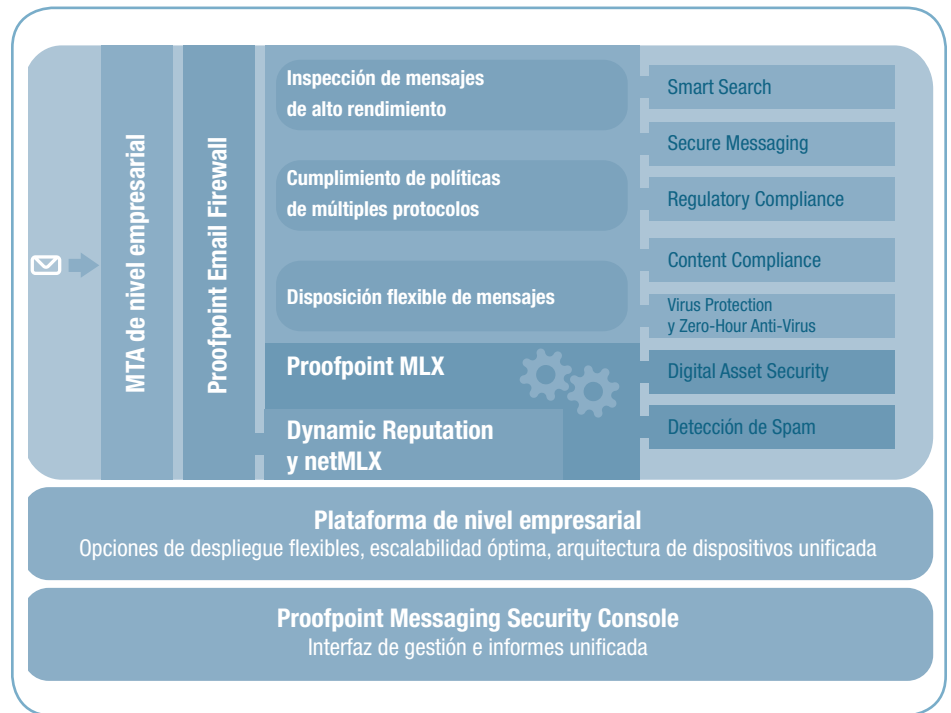
#### Inteligencia a prueba del futuro

La tecnología antispam inteligente de Proofpoint se actualiza continuamente para actuar como defensa contra nuevas formas de spam. El continuo autoaprendizaje y las nuevas técnicas desarrolladas por los científicos de Proofpoint permiten que MLX prediga y se adapte a las nuevas formas de spam a medida que aparecen. Las actualizaciones de MLX se entregan automáticamente a todos los clientes varias veces por día.

Como resultado de ello, Proofpoint MLX ofrece más del 99% de efectividad, incluso contra las formas más difíciles de spam, incluidos imágenes, PDF, archivos adjuntos y spam en idioma extranjero.

A diferencia de otras soluciones antispam, la capacidad de Proofpoint para defender a la empresa contra los ataques de spam no se deteriora con el tiempo, y las actualizaciones del motor antispam MLX se envían automáticamente a su empresa en forma regular. Proofpoint MLX está en continuo desarrollo para contrarrestar las amenazas emergentes y asegura que su infraestructura de mensajería se encuentre segura contra los "spammers" de hoy y también los del mañana.

Proofpoint MLX también acciona las funciones avanzadas de seguridad de contenido del módulo Proofpoint Digital Asset Security y las funciones inteligentes de seguridad del perímetro del servicio Proofpoint Email Firewall y Dynamic Reputation. Proofpoint es el único proveedor que aplica estas poderosas técnicas de aprendizaje automático a la seguridad de los mensajes de correo electrónico y a la prevención de la pérdida de datos.



## protección en contra de amenazas entrantes

### Advanced Spam Detection con tecnología Proofpoint MLX™

Con tecnología de aprendizaje automático Proofpoint MLX, con patente pendiente, el módulo **Proofpoint Spam Detection™** examina cientos de miles de atributos en cada mensaje de correo electrónico, incluidos el título del asunto, la estructura del mensaje, las propiedades de las imágenes, los datos del remitente y el contenido no estructurado en el cuerpo de los mensajes, para bloquear la mayoría del spam, el spam basado en imágenes y los ataques de fraude electrónico, al mismo tiempo que se adapta automáticamente a los nuevos ataques que aparecen. **Proofpoint Dynamic Update Service™** mantiene automáticamente actualizada su protección contra spam y le asegura una máxima efectividad en todo momento. La puntuación con control individual del spam y del contenido adulto le permite hacer cumplir las políticas de tolerancia cero contra el spam pornográfico. Las funciones antifraude electrónico evitan que el fraude electrónico y otros ataques de robo de identidad se propaguen y se apoderen de información personal de los empleados.

Proofpoint Spam Detection es multilingüe y ofrece una exactitud sorprendente contra spam en cualquier idioma, incluidos los idiomas difíciles de analizar o de caracteres multibyte como el japonés y el chino.

Las políticas antispam pueden ser personalizadas a niveles globales, grupales y de usuario final con integración completa al protocolo de acceso ligero a directorio (Lightweight Directory Access Protocol, LDAP) o Directorio Activo, para optimizar la administración continua.

### Protección integrada Email Firewall

**Proofpoint Email Firewall™** proporciona una primera línea de defensa contra spam y conexiones maliciosas, sin modificar el estado de la transacción en curso, a través de la prueba de puntos de datos en diversos niveles de conexión, incluidos DNS, verificación de registro MX, SPF, verificación del receptor, información de Proofpoint Dynamic Reputation y datos netMLX opcionales.

### Manejo innovador de las conexiones

**Proofpoint Dynamic Reputation™** con tecnología de **Proofpoint netMLX™** agrega las funciones de manejo de conexiones más poderosa de la industria al instalar Proofpoint. Es el único servicio de reputación de correo electrónico que utiliza una combinación de datos locales de comportamiento predecible con la reputación observada en forma global, analizada por algoritmos poderosos de aprendizaje automático, para bloquear las conexiones entrantes de las direcciones IP maliciosas.

Todas las implementaciones de appliances y software Proofpoint proporcionan un análisis de comportamiento predecible incorporado del tráfico IP local que responde en tiempo real para eliminar los picos de tráfico de mensajes de correo electrónico ocasionados por ataques a objetivos y para bloquear o restringir las conexiones maliciosas de las botnets.

# Proofpoint Messaging Security Gateway y Proofpoint Protection Server

## protección en contra de amenazas entrantes (continuación)

Los clientes con altos volúmenes de mensajes de correo electrónico pueden agregar la protección optimizada de Proofpoint netMLX a sus despliegues para reducir los volúmenes de conexiones entrantes en un 80% o más. Proofpoint netMLX constituye la base de datos de direcciones IP que envían mensajes de correo electrónico a través de Internet mas exacta y actualizada de la industria. Cada minuto, se analizan en detalle cientos de puntos de datos para todas las direcciones IP con algoritmos avanzados de aprendizaje automático para generar una puntuación que representa la historia del remitente. Después, Proofpoint Dynamic Reputation utiliza estas puntuaciones, en combinación con datos locales de comportamiento, para tomar decisiones inteligentes sobre la aceptación, la restricción o el rechazo de las conexiones de correo electrónico entrantes.

### Virus Protection y Zero Hour Anti-Virus Defenses

Mediante alianzas estratégicas con vendedores líderes de software antivirus, **Proofpoint Virus Protection™** provee funcionalidad completa en la exploración para la detección de virus. Los motores antivirus están totalmente integrados con la plataforma Proofpoint, y brindan una gestión práctica y centralizada de las políticas de antivirus desde la misma interfaz que se utiliza para manejar las políticas de spam y de contenido. Los mensajes se exploran eficientemente en busca de virus, simultáneamente con el análisis de spam y contenidos de mensajes, para proteger a los usuarios finales de virus, gusanos y otros códigos maliciosos. Además, el módulo **Proofpoint Zero-Hour Anti-Virus™** protege contra virus emergentes en las etapas más tempranas de su proliferación y los detiene horas antes de que las soluciones de la competencia comiencen siquiera a reaccionar.

## previenen las filtraciones de información en protocolos múltiples

Las funciones de prevención avanzada de pérdida de datos de Proofpoint pueden proteger los mensajes de correo electrónico salientes, así como los flujos de mensajes adicionales, incluidos los mensajes de correo electrónico basados en el Web, publicaciones en blogs, foros y otras actividades basadas en HTTP o FTP.

### Content Compliance: hace cumplir fácilmente las políticas de uso aceptable

**Proofpoint Content Compliance™** facilita la definición y aplicación de las políticas corporativas de uso aceptable para el contenido de los mensajes y los archivos adjuntos. Una práctica interfaz de señalar y pulsar simplifica el proceso de definición de reglas complejas relacionadas a los tipos de archivos, el tamaño de los mensajes y el contenido de los mensajes. Estas funciones pueden utilizarse para identificar y prevenir una amplia variedad de violaciones entrantes y salientes a la política, incluidos lenguaje ofensivo, acoso, archivos compartidos y violaciones de reglamentaciones externas.

### Regulatory Compliance: mantenga seguros los datos privados

Hoy más que nunca, las empresas necesitan salvaguardar la privacidad y la seguridad de los datos de clientes y empleados. El módulo **Proofpoint Regulatory Compliance™** implementa las mejores prácticas de seguridad de datos privados y protege a su organización de las responsabilidades asociadas con las reglamentaciones de privacidad y seguridad de datos (tales como la Ley de responsabilidad y transferencia de seguros médicos (Health Insurance Portability and Accountability Act, HIPAA), la Ley Gramm-Leach-Bliley (Gramm-Leach-Bliley Act, GLBA), la Interconexión de componentes periféricos (Peripheral Component Interconnect, PCI), las normas de la Comisión de valores (Securities and Exchange Commission, SEC y otras). Se utilizan normas personalizables, diccionarios manejados e "identificadores inteligentes" para explorar automáticamente la información no pública, como información protegida sobre la salud e información financiera personal, y rechazar o encriptar los mensajes según corresponda.

Los identificadores inteligentes de Proofpoint son más sofisticados que las simples expresiones regulares. Buscan la cantidad correcta de dígitos o caracteres, pero también realizan un procesamiento algorítmico complejo para asegurar un alto nivel de precisión en la detección y reducir, a la vez, los resultados falsos positivos.

### Digital Asset Security: protección de documentos confidenciales

Al igual que los mensajes de correo electrónico, el webmail y otros sistemas de mensajería se han convertido en los canales de comunicación más importantes; asimismo, se han convertido en un vehículo que deja expuesta la información delicada o confidencial. El módulo **Proofpoint Digital Asset Security™** evita que los activos corporativos y los datos confidenciales se filtren fuera de su organización a través de mensajes de correo electrónico y otros protocolos de mensajería. La poderosa tecnología de aprendizaje automático MLX analiza y clasifica sus documentos confidenciales y luego controla esa información (o partes de esa información) en el flujo de mensajería saliente y detiene las violaciones a la seguridad del contenido antes de que sucedan.

## Administración centralizada

### Gestión de políticas, administración y controles de usuarios finales basados en el Web

Proofpoint Messaging Security Console™ brinda una interfaz de administración centralizada y basada 100% en Internet para el marco de gestión unificada de políticas de Proofpoint, que asegura la aplicación uniforme de las políticas corporativas de mensajería. La consola facilita el monitoreo y el control de su infraestructura de mensajería y define las políticas de mensajería. Usted puede incluso definir y hacer cumplir diferentes políticas para diferentes grupos de usuarios finales. A medida que se agregan módulos Proofpoint a su despliegue, se utiliza la misma práctica interfaz para la gestión de políticas.

La interfaz basada en Ajax le permite personalizar la función "arrastrar y soltar" para los informes, la información de estado, los alimentadores de sindicación realmente simple (Really Simple Syndication, RSS) y otros componentes que aparezcan. Incluso puede crear "mashups" o mezclas de información de fuentes externas.

La sorprendente facilidad de uso de Proofpoint se extiende también a los usuarios finales. Los informes y controles fáciles de entender, tales como el resumen para el usuario final de Proofpoint, la cuarentena basada en el Web y las listas de seguridad y bloqueo personalizadas otorgan a los usuarios un control total sobre sus propias preferencias de spam.

### Informe completo

La consola también le brinda acceso a más de 60 informes y alertas gráficas en tiempo real que le permiten ver todo el estado del sistema de mensajería de su empresa. Los informes pueden ser enviados fácilmente por correo electrónico o publicados como HTML/XML. Los informes "activos" de Proofpoint envían información clave, pero también permiten que los administradores tomen medidas inmediatas (ej. simplemente hacer un clic en un enlace para bloquear a un remitente abusivo).

## Administración cero

### Protección siempre actualizada, máxima facilidad de administración

La instalación automática y la notificación de los componentes actualizados hacen que la administración continua sea simple. Proofpoint Dynamic Update Service asegura que su red tenga siempre el más alto nivel de protección contra las amenazas contenidas en los mensajes. Brinda actualizaciones continuas para cada componente de su software o despliegue de dispositivo Proofpoint, incluidos el sistema operativo reforzado y el agente de transporte de correo (Mail Transport Agent, MTA), los motores de spam y virus, los léxicos (tales como los diccionarios utilizados por el módulo Proofpoint Regulatory Compliance), los componentes de la aplicación y las revisiones o "hot fixes" personalizadas.

# Proofpoint Messaging Security Gateway y Proofpoint Protection Server

## encripte información sensible

**Proofpoint Secure Messaging™** agrega capacidades potentes de encriptación en función del contenido a su despliegue de Proofpoint y encripta en forma automática los mensajes sobre la base de las políticas de su organización. Aplica sus políticas de encriptación de manera automática y uniforme sin solicitar a los usuarios finales que realicen acción especial alguna. La tecnología de encriptación de la identidad (Identity Based Encryption, IBE) de Voltage provee una poderosa encriptación fácil de usar, sin las molestias del manejo de claves y certificados de otras soluciones. Los dispositivos de hardware y virtuales de Proofpoint también admiten certificados digitales, y permiten la transferencia y recepción de mensajes de correo electrónico seguras de gateway a gateway mediante el uso de Seguridad de la Capa de Transporte (Transport Layer)

## analiza su infraestructura de mensajería

**Proofpoint Smart Search™** mejora las funciones incorporadas de registro e informe de Proofpoint con un rastreo avanzado de mensajes, capacidades de análisis de registros y técnicas forenses y ofrece una sencilla visibilidad en tiempo real en el flujo de mensajes, en toda su infraestructura de mensajería. Busque y analice todos sus registros de mensajes a partir de una única GUI conveniente y fácil de usar, incluso entre despliegues de Proofpoint distribuidos globalmente.

## alto rendimiento, fácil despliegue, óptima escalabilidad

Proofpoint Messaging Security Gateway Proofpoint Protection Server fueron diseñados para satisfacer las necesidades específicas de grandes empresas, proveedores de servicios de Internet (Internet Service Provider, ISP), universidades y organizaciones gubernamentales. Ofrecen todas las funciones de rendimiento, flexibilidad, escalabilidad, personalización y control de usuarios finales necesarias en despliegues a gran escala.

Cada uno de los componentes del sistema Proofpoint está diseñado para cumplir con las demandas rigurosas de rendimiento de una empresa. Desde el sistema operativo de mensajería optimizado y reforzado, utilizado en los dispositivos Proofpoint, hasta la exclusiva arquitectura sin cola de espera de Proofpoint, que permite que todas las funciones de exploración de mensajes se realicen en la memoria, Proofpoint brinda el alto rendimiento requerido, incluso en los despliegues más sofisticados.

La escala de dispositivos y software Proofpoint crece de manera indefinida para admitir millones de mensajes por día. Pueden desplegarse fácilmente en muchas configuraciones maestro/agente de dispositivos múltiples para admitir centros de datos complejos o distribuidos geográficamente, y ofrecen la seguridad del 100% de redundancia combinada con la practicidad de una sola interfaz administrativa. Proofpoint permite tener implementaciones híbridas con los dos dispositivos virtuales y de hardware trabajando simultáneamente.

La arquitectura de escalabilidad óptima de Proofpoint le permite manejar todos los servidores agentes desde una sola consola maestra. La propagación automática de la configuración, una cuarentena centralizada de mensajes y el informe centralizado simplifican el mantenimiento y reducen el costo total de propiedad.

Además, Proofpoint reduce el costo total de propiedad ya que se integra fácilmente con cualquier infraestructura de TI, sin importar cómo esté distribuida. La consola de comando LDAP basada en GUI y el hecho de que admite Microsoft Active Directory® facilitan la integración con los servidores de directorios. Proofpoint también es compatible con soluciones de servidores de correo electrónico recargadas, tales como Microsoft Exchange® y Lotus Notes®, y minimiza la carga que deben procesar.

## versión de prueba gratuita, ¡pruébela hoy mismo!

Pruebe usted mismo el poder de Proofpoint. Visite el sitio Web [www.proofpoint.com/trial](http://www.proofpoint.com/trial) y regístrese para descargar una versión gratuita por 45 días totalmente funcional de Proofpoint Messaging Security Gateway—Virtual Edition, equipada con los módulos de seguridad de correo electrónico entrante de Proofpoint. El dispositivo virtual de Proofpoint puede desplegarse en cuestión de minutos, protegiendo inmediatamente a sus usuarios de mensajes de correo electrónico de todo tipo de amenazas contenidas en los mensajes.

## Versiones de dispositivos

El dispositivo Proofpoint Messaging Security Gateway está disponible en una variedad de configuraciones de hardware para admitir despliegues de cualquier tamaño. Para obtener información actualizada sobre los modelos de dispositivos Proofpoint, visite el sitio Web:

[www.proofpoint.com/products/msg.php](http://www.proofpoint.com/products/msg.php)

## Requisitos de sistema del software

El software Proofpoint Protection Server es compatible con cualquier servidor para descargas de mensajes de correo electrónico y está disponible para plataformas hardware Linux.

### Plataformas Linux

Red Hat Enterprise Linux ES 3.0, 4.0 ó 5.0

Red Hat Enterprise Linux AS 4.0 ó 5.0

## Requisitos de la edición virtual

Proofpoint Messaging Security Gateway—Virtual Edition es una aplicación de seguridad de mensajería empresarial, un agente de transferencia de mensajes y un entorno operativo seguro, preinstalado y preconfigurado en su totalidad que funciona en cualquier computadora de escritorio x86 o servidor estándar que usa productos de virtualización VMware.

Para los despliegues de producción, evaluación o de laboratorio, se requiere VMware Server o VMware Infrastructure (VMware ESX 3.0 o superior).

## Navegadores admitidos

Todas las tareas de configuración y de administración, para el dispositivo hardware, el dispositivo virtual o las versiones de software, se manejan a través de la interfaz de Proofpoint basada 100% en un navegador Web. Los navegadores admitidos incluyen: Microsoft® Internet Explorer 6.0 o superior, Mozilla Firefox 1.2 o superior, y Netscape® 7.0 o superior.

©2008 Proofpoint, Inc. Proofpoint Protection Server es una marca comercial registrada de Proofpoint, Inc. en los Estados Unidos y otros países. Proofpoint, Proofpoint Messaging Security Gateway, Proofpoint Email Firewall, Proofpoint Spam Detection, Proofpoint Virus Protection, Proofpoint Content Compliance, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint Dynamic Update Service, Proofpoint MLX, Proofpoint Dynamic Reputation, Proofpoint netMLX, Proofpoint Smart Search, Proofpoint Messaging Security Console y Proofpoint on Demand son marcas comerciales de Proofpoint, Inc. en los Estados Unidos y otros países. Todas las otras marcas comerciales aquí incluidas son propiedad de sus respectivos titulares. 02/08