

Dispositivos McAfee WebShield

Los dispositivos McAfee® WebShield® son soluciones integradas que combinan excelente software antivirus y de gestión de contenido con hardware avanzado. Los dispositivos WebShield e250, e500 y e1000, diseñados para proporcionar el máximo rendimiento, ofrecen protección antivirus de McAfee para resolver con rapidez los principales problemas de seguridad empresarial que provocan los virus.

Diseñados para ofrecer el máximo rendimiento

Alta escalabilidad

Los dispositivos WebShield se han diseñado para ofrecer el máximo rendimiento y fiabilidad. WebShield e250 está pensado para empresas pequeñas y puede gestionar un volumen de 30.000 mensajes de correo electrónico SMTP por hora, o bien 4Mbps de tráfico HTTP por segundo. Por su parte, McAfee WebShield e500 es capaz de explorar 80.000 mensajes de correo electrónico SMTP por hora o 8 Mbps de tráfico HTTP por segundo, lo que lo convierte en el dispositivo ideal para empresas medianas y grandes. WebShield e1000 dobla prácticamente el rendimiento del dispositivo e500 y puede ser utilizado simultáneamente por un mayor número de usuarios. Además, WebShield e1000 puede emplearse en infraestructuras de red Gigabit de cobre. La tecnología de cargas compartidas que incorpora cada uno de los dispositivos WebShield permite utilizar varios dispositivos en caso de necesitar un mayor rendimiento. Asimismo, si se precisa mayor disponibilidad, es posible configurar los dispositivos mediante soluciones comercializadas por otros fabricantes.

Soporte para múltiples protocolos

Exploración de los principales protocolos de mensajería

Los dispositivos de detección de virus McAfee WebShield pueden utilizarse en los protocolos SMTP, HTTP, FTP y POP3. Al instalarlos detrás de un cortafuegos (el funcionamiento de los dispositivos es independiente al del cortafuegos), detectan y eliminan los virus y programas malignos, sin afectar al rendimiento del cortafuegos o los servidores de correo electrónico. De este modo, se garantiza la máxima protección de la red y los usuarios de la empresa al navegar por Internet, descargar archivos o consultar los buzones de correo electrónico.

Exploración transparente en línea

Fácil de configurar e instalar

Las opciones de exploración transparente que ofrecen los dispositivos WebShield evitan tener que configurar las máquinas clientes o redireccionar los datos desde los servidores de correo electrónico para explorar el tráfico SMTP, HTTP, FTP o POP3. Los dispositivos WebShield proporcionan dos modos de exploración transparente: la creación de puentes o el enrutamiento transparentes. La creación transparente de puentes elimina la necesidad de realizar cambios en la red o el cortafuegos para garantizar que el dispositivo explore el tráfico, siempre que se disponga de una dirección IP que el dispositivo WebShield pueda utilizar. El enrutamiento transparente significa que el dispositivo se instala y actúa como enruta-

dor entre dos puntos de la red. En estos modos transparentes, el tráfico fluye por el dispositivo entrando por una tarjeta NIC y saliendo por la otra, conservando información como las direcciones IP y MAC de origen. Además, estas opciones de exploración transparente permiten

proteger los servidores Web internos, a la vez que facilitan la instalación. Si se desea, ambos dispositivos pueden ejecutarse en un modo de proxy explícito para la exploración. Este método de instalación implica que únicamente el tráfico SMTP, HTTP, FTP y POP3 pasa por el dispositivo WebShield. El tráfico del resto de los protocolos no podrá controlarse mediante este dispositivo.

Gestión de contenido

Supervisión de los elementos que entran y salen de la red

Los dispositivos McAfee WebShield permiten conocer con exactitud la información que entra y sale de la red. Las funciones de filtrado de contenido de WebShield evitan que los usuarios reciban mensajes de correo electrónico con contenido ofensivo o difamatorio, a la vez que protegen la empresa frente a posibles problemas legales al impedir que se envíen mensajes de correo electrónico de este tipo. Para reforzar aún más la protección legal, los dispositivos McAfee WebShield permiten introducir notas de renuncia de responsabilidad en todos los mensajes de correo electrónico que se reciben y se envían. Asimismo, con estos dispositivos podrá conservar el ancho de banda al impedir que los usuarios envíen o reciban mensajes de correo electrónico con determinados archivos adjuntos, mensajes superiores a un tamaño específico o mensajes que contengan muchos archivos adjuntos.

Detección de mensajes no deseados y mecanismo de prohibición de envío

Ahorro del ancho de banda de la red

Al admitir el uso de listas negras basadas en DNS, los dispositivos McAfee WebShield permiten bloquear los mensajes de correo electrónico no deseados con el fin de evitar que los usuarios pierdan tiempo leyéndolos y conservar los valiosos recursos de la red. El mecanismo de prohibición de envío evita que se utilicen los servidores de la empresa para enviar mensajes de correo electrónico no deseados, lo que mejora el control y la seguridad de la red. Además, pueden bloquearse determinadas palabras y frases no deseadas mediante las funciones de filtrado de contenido.

Informes exhaustivos

Integración de ePolicy Orchestrator

Mediante la integración de los dispositivos WebShield con ePolicy Orchestrator™ de McAfee se pueden crear informes gráficos de la actividad de los virus en la pasarela. Asimismo, pueden obtenerse informes detallados sobre las reglas de filtrado de contenido utilizadas y los intentos de acceder a direcciones URL prohibidas. Además, los dispositivos ofrecen completos informes y análisis de tendencia de los virus para que el administrador esté siempre informado de las infecciones.

Dispositivos McAfee WebShield

Dispositivos McAfee WebShield

	WebShield e250	WebShield e500	Webshield e1000
Dispositivo integrado	Sí	Sí	Sí
Archivos desinfectados	Sí	Sí	Sí
Archivos en cuarentena	Sí	Sí	Sí
Archivos eliminados	Sí	Sí	Sí
Hardware y software suministrado	Sí	Sí	Sí
Tipo de caja	Minitorre	Bastidor de 1U	Bastidor de 2U
Tolerancia a fallos	No	Sí—RAID 1	Sí—RAID 1
Sistema operativo reforzado	Sí	Sí	Sí
Interfaces de red Gigabit (NIC)	No	No	Sí—Cobre
Alta escalabilidad	Sí	Sí	Sí
Sólo tráfico SMTP	30.000 mensajes por hora	80.000 mensajes por hora	160.000 mensajes por hora
Sólo tráfico HTTP	4 Mbps	8 Mbps	16 Mbps
Exploración de múltiples protocolos	Sí	Sí	Sí
SMTP, HTTP, FTP y POP3	Sí	Sí	Sí
Fácil de configurar e instalar	Sí	Sí	Sí
Exploración transparente en línea	Sí	Sí	Sí
Modo de exploración de proxy	Sí	Sí	Sí
Gestión de contenido	Sí	Sí	Sí
Línea de asunto y cuerpo de un mensaje de correo electrónico	Sí	Sí	Sí
Nombre, tipo o tamaño del archivo adjunto	Sí	Sí	Sí
Exploración del texto de los archivos adjuntos	Sí	Sí	Sí
Mecanismo contra mensajes no deseados	Sí	Sí	Sí
Soporte para lista negra	Sí	Sí	Sí
Frases definidas por el administrador	Sí	Sí	Sí
Informes empresariales	Sí	Sí	Sí
Uso de ePolicy Orchestrator	Sí	Sí	Sí
Informes gráficos y análisis de tendencias	Sí	Sí	Sí
Alertas y notificaciones	Sí	Sí	Sí
Alertas completas (correo electrónico, SNMP, etc.)	Sí	Sí	Sí
Alertas enviadas automáticamente	Sí	Sí	Sí
Bloqueo de direcciones URL	Sí	Sí	Sí
Estado de descarga de archivos HTTP	Sí	Sí	Sí
Mecanismo de prohibición de envío	Sí	Sí	Sí
Soporte para notas de renuncia de responsabilidad	Sí	Sí	Sí
Capacidad de gestión remota	Sí	Sí	Sí

Todos los productos de Network Associates cuentan con el soporte de Network Associates Laboratories y de nuestro programa PrimeSupport®. El servicio PrimeSupport, personalizado según las necesidades de la empresa, ofrece información básica del producto y soluciones técnicas rápidas y fiables para garantizar el funcionamiento de la empresa. Network Associates Laboratories, líder mundial en seguridad y sistemas de información, garantiza un desarrollo y ajuste continuado de nuestra tecnología.

