

McAfee SpamKiller Appliances

En los variados ambientes de red actuales, es esencial garantizar que el contenido que entra y sale de una empresa siga las políticas internas de seguridad y la legislación sobre privacidad. Las soluciones de Administración Segura de Contenido de McAfee® cuentan con una tecnología integrada y flexible que permite a las empresas de cualquier porte optimizar recursos, aumentar la productividad e impedir el comprometimiento de las políticas de seguridad. Con la mejor combinación de tecnologías antivirus, anti-*spam* y de protección de contenido, las soluciones de Administración Segura de Contenido de McAfee permiten que usted controle, administre y comprenda su tráfico de Internet.

Las *appliances* McAfee SpamKiller® ofrecen la mejor protección anti-*spam* y la mejor filtración de contenido del mercado en una única solución física con hardware y software integrados. SpamKiller ofrece una proporción de detección de *spam* de hasta 95%, sin necesidad de ajustes o configuraciones.

**¿El *spam* es apenas un pequeño inconveniente?
¡No!**

Una amenaza devastadora

Los mensajes indeseables costaron a las empresas norteamericanas más de US\$10 000 millones en 2003, según un informe divulgado en enero de 2003 por Ferris Research. Un estudio reciente del Gartner Group estima que, hasta el final de 2004, más de 50% del tráfico de mensajes será compuesto por *spam*, a menos que las empresas tomen medidas de defensa.* McAfee identifica cuatro principales áreas en las cuales el *spam* puede costar mucho dinero a su empresa.

- **Pérdida de productividad** — la cantidad de tiempo utilizada por los usuarios en la lectura y en la administración de mensajes indeseables. Se calcula que la pérdida de productividad de los usuarios sea el mayor costo asociado al *spam* para las empresas.
- **Contenido inadecuado** — mensajes que, de algún modo, son considerados ofensivos y, muy probablemente, violan la política de RH. Ese tipo de mensaje puede ofender a personas o grupos (por ejemplo, el mensaje puede contener asuntos adultos).
- **Consumo de recursos de TI** — la cantidad de ancho de banda de la red ocupada por el *spam*.

- **Spam como una amenaza a la seguridad** — los *e-mails* de *spam* pueden contener códigos mal intencionados o ataques de DoS; los *e-mails* infectados por virus pueden usar métodos de distribución semejantes a los del *spam* (por ejemplo, Sobig.F y envío de *e-mails* en masa). La protección contra *spam* es un componente esencial de su política de seguridad

*Fuentes: *Spam Control: Problems and Opportunities*, The Ferris Group, enero de 2003, y *Waves of Information Disruption Due in 2003*, The Gartner Group, diciembre de 2002.

Tecnología McAfee SpamKiller

Powered by McAfee SpamAssassin

La tecnología central de la familia de productos McAfee SpamKiller es el *engine* McAfee SpamAssassin™, que opera con un sistema de clasificación, que atribuye puntuaciones a los mensajes de acuerdo con una serie de pruebas. Es altamente preciso en la identificación del *spam*, y captura hasta 95% de todo el *spam* sin ninguna configuración especial, además de proporcionar una tasa muy reducida de identificación de falsos positivos (menos de 0,05%). Las reglas predefinidas de SpamKiller, mantenidas por McAfee, no exigen la definición de ninguna regla adicional y son eficaces en la detección del *spam* sin configuraciones especiales.

Sistema de puntuación

Puntuaciones diferentes para mensajes diferentes

SpamAssassin utiliza un sistema de puntuación basado en un amplio conjunto de reglas, para determinar si un mensaje de *e-mail* es un *spam*. Centenas de reglas son aplicadas a cada *e-mail* y cada regla es asociada con una puntuación negativa o positiva. Las reglas con puntuación negativa indican atributos de *e-mails* legítimos y las reglas con puntuación positiva indican atributos de mensajes no-solicitados. Combinadas, esas puntuaciones individuales atribuyen a cada *e-mail* una "clasificación general de *spam*". Un algoritmo genético optimiza la puntuación, utilizando un archivo de millones de mensajes de *spam* y de mensajes que no son *spam* para determinar las puntuaciones de cada regla. Ahora que el *e-mail* es usado como una parte crítica de la infraestructura de negocios, es vital que todos los fabricantes de anti-*spam* ofrezcan protecciones contra mensajes incorrectamente identificados como *spam*. Los sistemas de puntuación son esenciales en la actual lucha contra el *spam*, pues son más precisos que las técnicas tradicionales de comparación, y permiten la identificación de las áreas "grises" de la detección de *spam*.

DetECCIÓN DE SPAM

Varios métodos para garantizar la detección

Utilizando el proceso subyacente de conjuntos de reglas predefinidas, los *appliances* SpamKiller verifican, mediante cinco métodos diferentes de detección, cada *e-mail* recibido.

- **Análisis de Integridad** — SpamKiller examina el encabezamiento, el *layout* y la organización de cada mensaje de *e-mail* para identificar las características comunes del *spam*.
- **DetECCIÓN Heurística** — Usada para identificar mensajes como *spams* probables. La detección heurística utiliza una serie de exámenes internos para determinar la probabilidad de que un mensaje sea *spam*. Cada prueba atribuye una puntuación para ayudar a reducir los falsos positivos.
- **Filtración de contenido** — Esta función puede ser usada para ayudar a identificar las palabras o expresiones claves presentes en un *e-mail* y que pueden indicar que el mensaje se trata de *spam*.
- **Uso de “blacklists” y “whitelists”** — *Blacklists* definidas por el administrador bloquean los dominios conocidos por ser remitentes de *spam*, mientras que las *whitelists* definidas por el administrador siempre liberan los mensajes provenientes de los dominios especificados.
- **Uso de Listas de Bloqueo por DNS** — Los *appliances* McAfee WebShield® permiten el uso de listas negras por DNS para la identificación de remitentes conocidos de *spam*.
- **Filtración Bayesiana** — McAfee SpamKiller cuenta con tecnología de filtración Bayesiana para permitir que los mensajes de *e-mail* sean evaluados de manera inteligente con base en criterios de lo que es y de lo que no es *spam*. La filtración Bayesiana ofrecida cuenta con un banco de datos predefinido de filtros Bayesianos, además de una tecnología preventiva de aprendizaje automático de los tipos de mensajes que deben ser clasificados como *spam* y *no-spam*, en su empresa.

La filtración avanzada de contenido monitorea lo que entra y sale de su red

¿Qué tal si pudiese protegerse contra la entrada de contenidos inadecuados en su red, además de protegerse contra la salida de informaciones confidenciales? La filtración de contenido puede evitar ambas cosas. Con el barrido lexical de *e-mails* y más de 300 tipos de adjuntos basados en reglas de administración de contenido, además de la identificación del verdadero tipo de los adjuntos para impedir la tan común evasión de reglas, la filtración de contenido protege a sus empleados y sistemas contra daños. Los *e-mails* y adjuntos pueden ser sustituidos por un

mensaje personalizable si contienen palabras o expresiones específicas que violen una regla de contenido.

Control por políticas con el eXtended Policy Support

WebShield ofrece a las empresas controles por políticas para protección contra virus y reglas de filtración de contenido y *spam*. Con WebShield, los administradores pueden establecer reglas específicas de filtración para personas o grupos de usuarios, con varios tipos de barrido, mejorando la exploración y aumentando la flexibilidad de configuración. Al definir reglas y especificar grupos de personas, WebShield da acceso al Microsoft® Active Directory o al LDAP, y permite que los clientes utilicen los directorios de usuarios que ya poseen.

McAfee Dashboard

Al ofrecer análisis pericial y presentar el estado de los sistemas, McAfee Dashboard muestra a los administradores las condiciones de la red y estadísticas sobre el *appliance* instalado, en una pantalla unificada y fácil de entender, detallando estadísticas tales como el número de virus detectados o de mensajes de *spam*. Como parte de la función de panel de control, WebShield permite la recolección de detalles más profundizados de sesiones de SMTP, tales como el número y el tipo de mensajes que pasaron por el *appliance*. Esas informaciones pueden ser usadas como herramienta de depuración, solución de problemas y pericias, además de ayudar a las empresas a cumplir las exigencias de conformidad con las prácticas recomendadas por auditores de información internos.

Informes gráficos detallados

WebShield se integra al McAfee ePolicy Orchestrator® para generar informes gráficos y análisis de tendencias, con lo cual proporciona una visión amplia de la actividad del *gateway* de Internet.

Velocidad de e-mail

La herramienta cierta para su empresa

Los *appliances* McAfee SpamKiller son creados y configurados para operar en alta velocidad y ser confiables. El e250 fue proyectado para empresas de menor tamaño, explora 19 000 mensajes de SMTP por hora con el SpamKiller y la administración de contenido configurada; el e500, para empresas de medio y gran porte, explora 63 000 mensajes de SMTP por hora con el SpamKiller y la administración de contenido configurada; y el e1000, para grandes empresas, empresas con necesidad de alta velocidad o empresas que usan infraestructuras de red de cables de cobre de alta velocidad, explora 95 000 mensajes de SMTP por hora con el SpamKiller y la administración de contenido configurada. La tecnología incorporada de compartición

de carga del *appliance* permite el uso de varios *appliances* si fuese necesaria más velocidad.

Componentes del *appliance* SpamKiller

Los *appliances* McAfee SpamKiller cuentan con:

- Licencia del software SpamKiller para *appliances*, para reducir el impacto del *spam*.
- Licencia del software de Filtración Avanzada de Contenido de McAfee para permitir el monitoreo del tráfico que entra y sale de la red.
- Una licencia de prueba, de seis meses, del premiado software WebShield de McAfee para *appliances*.

McAfee PrimeSupport

McAfee ha seguido una estrategia de proveer la mejor combinación de tecnologías para cada tipo de aplicación de seguridad y administración de desempeño — pero la estrategia Protection-in-Depth™ va mucho más allá de la simple distribución e implementación de la mejor combinación de soluciones, hoy. La prevención es, con toda seguridad, nuestra primera prioridad, aunque, inevitablemente, usted tendrá que reaccionar a algún problema.

El programa McAfee PrimeSupport es esencial para que usted aproveche al máximo sus inversiones en las Soluciones de Protección de Sistemas y Redes de McAfee. El equipo PrimeSupport de McAfee cuenta con todos los recursos necesarios y está listo para ofrecer la solución de servicio que usted precisa. Entre los recursos del PrimeSupport están: autorización de acceso a todas las versiones de mantenimiento y actualizaciones de productos disponibles, acceso a una amplia gama de otros recursos de autoatención por Internet, auxilio telefónico personal accesible 24/7/365, gerentes dedicados de soporte de cuenta a disposición, además de una amplia gama de soluciones de soporte de software y hardware que pueden ser adecuadas a sus necesidades específicas.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

Los productos de McAfee® denotan años de experiencia y compromiso con la satisfacción del usuario. El equipo PrimeSupport® de McAfee, que cuenta con técnicos de soporte atentos y altamente cualificados, ofrece soluciones a la medida y asistencia técnica detallada para administrar el éxito de proyectos esenciales — todo eso con niveles de servicio que atienden a las necesidades de todas las empresas. McAfee Research, líder mundial en investigación de seguridad y sistemas de información, continúa en la vanguardia de la innovación en el desarrollo y en el refinamiento de todas nuestras tecnologías.

McAfee, SpamKiller, powered by SpamAssassin, WebShield, ePolicy Orchestrator, Protection-in-Depth, y PrimeSupport son marcas comerciales, registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo relacionado con la seguridad es marca distintiva de los productos que llevan la marca McAfee®. Todas las otras marcas comerciales, registradas o no, mencionadas aquí pertenecen exclusivamente a sus respectivos titulares. © 2004 Network Associates Technology, Inc. Todos los derechos reservados. 1-sps-spka-003-0804