

# McAfee SpamKiller 3000 Series Appliances

Nos ambientes de rede multifacetados de hoje, é essencial garantir que o conteúdo que entra e sai de uma empresa siga as políticas internas de segurança e a legislação sobre privacidade. As soluções de Gerenciamento Seguro de Conteúdo da McAfee® contam com uma tecnologia integrada e flexível que permite a empresas de qualquer porte otimizar recursos, aumentar a produtividade e impedir o comprometimento das políticas de segurança. Com a melhor combinação de tecnologias antivírus, anti-spam e de proteção de conteúdo; soluções de Gerenciamento Seguro de Conteúdo da McAfee permitem que você controle, gereencie e compreenda o seu tráfego de Internet.

Os appliances McAfee SpamKiller® oferecem a melhor proteção anti-spam e a melhor filtragem de conteúdo do mercado em uma única solução física com hardware e software integrados. O SpamKiller oferece uma proporção de detecção de spam de até 95%, sem a necessidade de ajustes ou configurações.

## O Spam é somente um pequeno inconveniente? Não!

### Uma ameaça devastadora

as mensagens indesejáveis custaram às empresas norte-americanas mais de US\$10 bilhões em 2003, segundo um relatório divulgado em janeiro de 2003 pela Ferris Research. Um recente estudo do Gartner Group estima que, até o final de 2004, mais de 50% do tráfego de mensagens será composto por spam, a menos que as empresas tomem medidas de defesa.\* A McAfee identifica quatro principais áreas nas quais o spam pode custar muito dinheiro à sua empresa.

- **Perda de produtividade** — a quantidade de tempo gasta pelos usuários na leitura e no gerenciamento de mensagens indesejáveis. Estima-se que a perda de produtividade dos usuários seja o maior custo associado ao spam para as empresas.
- **Conteúdo inadequado** — mensagens que, de alguma maneira, são consideradas ofensivas e, muito provavelmente, violam a política de RH. Esse tipo de mensagem pode ofender pessoas ou grupos (por exemplo, quando a mensagem contém assuntos adultos).
- **Consumo de recursos de TI** — a quantidade de largura de banda da rede ocupada pelo spam.

- **Spam como uma ameaça à segurança** — os e-mails de spam podem conter códigos mal-intencionados ou ataques de DDoS. Os e-mails infectados por vírus podem usar métodos de distribuição semelhantes aos do spam (por exemplo, Sobig.F e envio de e-mails em massa). A proteção contra spam é um componente essencial da sua política de segurança

\*Fontes: Spam Control: Problems and Opportunities, The Ferris Group, janeiro de 2003, e Waves of Information Disruption Due in 2003, The Gartner Group, dezembro de 2002.

## A tecnologia McAfee SpamKiller

### Powered by McAfee SpamAssassin

A tecnologia central da família de produtos McAfee SpamKiller é o engine McAfee SpamAssassin™, que opera com um sistema de classificação, atribuindo pontuações às mensagens de acordo com uma série de testes. É altamente preciso na identificação do spam, capturando até 95% de todo o spam sem nenhuma configuração especial, além de proporcionar uma taxa muito reduzida de identificação de falsos positivos (menos de 0,05%). As regras predefinidas do SpamKiller, mantidas pela McAfee, não exigem a definição de nenhuma regra e são eficientes na detecção do spam sem configurações especiais.

## Sistema de pontuação

### Pontuações diferentes para mensagens diferentes

O SpamAssassin utiliza um sistema de pontuação baseado em um amplo conjunto de regras, para determinar se uma mensagem de e-mail é um spam. Centenas de regras são aplicadas a cada e-mail e cada regra é associada a uma pontuação negativa ou positiva. Regras com pontuação negativa indicam atributos de e-mails legítimos e regras com pontuação positiva indicam atributos de mensagens não-solicitadas. Combinadas, essas pontuações individuais atribuem a cada e-mail uma "classificação geral de spam". Um algoritmo genético otimiza a pontuação, utilizando um arquivo de milhões de mensagens de spam e que não são spam para determinar as pontuações de cada regra. Agora que o e-mail é usado como uma parte crítica da infraestrutura de negócios, é vital que todos os fabricantes de anti-spam forneçam proteções contra mensagens incorretamente identificadas como spam. Sistemas de pontuação são essenciais na atual luta contra o spam, pois são mais precisos que as técnicas tradicionais de comparação, permitindo a identificação das áreas "cinzas" da detecção de spam.

## Detecção de spam

### Vários métodos para garantir a detecção

Utilizando o processo subjacente de conjuntos de regras predefinidas, os appliances SpamKiller verificam, por meio de cinco métodos diferentes de detecção, cada e-mail recebido.

- **Análise de Integridade** — O SpamKiller examina o cabeçalho, o layout e a organização de cada mensagem de e-mail para identificar as características comuns do spam.
- **Detecção Heurística** — Usada para identificar mensagens como spams prováveis. A detecção heurística utiliza uma série de testes internos para determinar a probabilidade de que uma mensagem seja spam. Cada teste atribui uma pontuação para ajudar a reduzir falsos positivos.
- **Filtragem de conteúdo** — Esta função pode ser usada para auxiliar na identificação das palavras ou expressões-chaves presentes em um e-mail e que podem indicar que a mensagem se trata de spam.
- **Uso de “blacklists” e “whitelists”** — *Blacklists* definidas pelo administrador bloqueiam domínios conhecidos por serem remetentes de spam, ao passo que as *whitelists* definidas pelo administrador sempre liberam mensagens provenientes de domínios especificados.
- **Uso de Listas de Bloqueio por DNS** — Os appliances McAfee WebShield® permitem o uso de listas negras por DNS para a identificação de remetentes conhecidos de spam.
- **Filtragem Bayesiana** — O McAfee SpamKiller conta com tecnologia de filtragem Bayesiana para permitir que as mensagens de e-mail sejam avaliadas de maneira inteligente com base em critérios do que é e do que não é spam. A filtragem Bayesiana oferecida conta com um banco de dados predefinido de filtros Bayesianos, além de uma tecnologia preventiva de aprendizado automático dos tipos de mensagens que devem ser classificadas como spam e não-spam na sua empresa.

## A filtragem avançada de conteúdo monitora o que entra e sai da sua rede

E se você pudesse se proteger contra a entrada de conteúdos inadequados na sua rede, além de se proteger contra a saída de informações confidenciais? A filtragem de conteúdo pode evitar ambas as coisas. Com a varredura lexical de e-mails e mais de 300 tipos de anexos baseados em regras de gestão de conteúdo, além da identificação do verdadeiro tipo dos anexos para impedir a tão comum evasão de regras, a filtragem de conteúdo protege os seus funcionários e sistemas contra danos. Os e-mails e anexos podem ser substituídos por uma mensagem personalizável

se contiverem palavras ou expressões específicas que violem uma regra de conteúdo.

## Controle por políticas com o eXtended Policy Support

O WebShield oferece às empresas controles por políticas para proteção contra vírus e regras de filtragem de conteúdo e spam. Com o WebShield, os administradores podem estabelecer regras específicas de filtragem para pessoas ou grupos de usuários, com vários tipos de varredura, melhorando a varredura e aumentando a flexibilidade de configuração. Ao definir regras e especificar grupos de pessoas, o WebShield proporciona acesso ao Microsoft® Active Directory ou ao LDAP, permitindo que os clientes utilizem os diretórios de usuários que eles já possuem.

## McAfee Dashboard

Oferecendo análise pericial e apresentando o status dos sistemas, o McAfee Dashboard mostra aos administradores as condições da rede e estatísticas sobre o appliance instalado, em uma tela unificada e fácil de entender, detalhando estatísticas, tais como o número de vírus detectados ou de mensagens de spam. Como parte da função de painel de controle, o WebShield permite a coleta de detalhes mais aprofundados de sessões de SMTP, tais como o número e o tipo de mensagens que passaram pelo appliance. Essas informações podem ser usadas como ferramenta de depuração, solução de problemas e perícias, além de ajudar as empresas a cumprir as exigências de conformidade com as práticas recomendadas por auditores de informação internos.

## Relatórios gráficos detalhados

O WebShield integra-se ao McAfee ePolicy Orchestrator® para gerar relatórios gráficos e análises de tendências, proporcionando uma visão ampla da atividade do gateway de Internet.

## Velocidade de e-mail

### A ferramenta certa para a sua empresa

Os appliances McAfee SpamKiller são criados e configurados para operar em alta velocidade e serem confiáveis. O 3100 foi projetado para empresas de menor porte, varrendo 30 mil mensagens de SMTP por hora com o SpamKiller e a gestão de conteúdo configurada; o 3200, para empresas de médio e grande porte, varre 55 mil mensagens de SMTP por hora com o SpamKiller e a gestão de conteúdo configurada; e o 3300, para grandes empresas,

empresas com necessidade de alta velocidade ou empresas que usam infra-estruturas de rede de cabos de cobre de alta velocidade, varre 110 mil mensagens de SMTP por hora com o SpamKiller e a gestão de conteúdo configurada. A tecnologia incorporada de compartilhamento de carga do appliance permite o uso de vários appliances quando houver necessidade de mais velocidade.

### Componentes do appliance SpamKiller

#### Os appliances McAfee SpamKiller contam com:

- Licença do software SpamKiller para appliances, para reduzir o impacto do spam.
- Licença do software de Filtragem Avançada de Conteúdo da McAfee para permitir o monitoramento do tráfego que entra e sai da rede.
- Uma licença de experiência de seis meses do premiado software WebShield da McAfee para appliances.

### Anti-Phishing

O McAfee SpamKiller inclui regras específicas que ajudam a identificar os “phishing attacks” observando certas características específicas de phishing presentes em e-mail. Uma vez aplicadas, o Spamkiller atribui uma pontuação, que resulta em bloqueio na maioria dos casos. Em conjunto com o Anti-Phishing Working Group (APWG), a McAfee reuniu um considerável Banco de Dados de phishing attacks que é utilizado para criar regras efetivas de filtragem destes ataques.

### McAfee PrimeSupport

A McAfee tem seguido uma estratégia de fornecer a melhor combinação de tecnologias para cada tipo de aplicação de segurança e gestão de desempenho — contudo, a estratégia Protection-in-Depth™ vai além da simples distribuição e implementação da melhor combinação de soluções hoje. Com toda certeza, a prevenção é prioridade para a McAfee, entretanto, inevitavelmente, você precisará reagir a um problema.

O programa McAfee PrimeSupport é essencial para que você aproveite ao máximo seus investimentos nas Soluções de Proteção de Sistemas e Redes da McAfee. A equipe PrimeSupport da McAfee conta com todos os recursos necessários e está pronta para fornecer a solução de serviço do qual você precisa. Entre os recursos do PrimeSupport estão: autorização de acesso a todas as versões de manutenção e atualizações de produtos disponíveis, acesso a uma ampla gama de outros recursos de auto-atendimento pela Internet, suporte telefônico pessoal acessível 24/7/365, gerentes dedicados de suporte de conta à disposição, além de uma ampla diversificação de soluções de suporte de software e hardware que são adequadas às suas necessidades específicas.

**McAfee, Inc.** 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, [www.mcafee.com](http://www.mcafee.com)

Os produtos da McAfee® denotam anos de experiência e compromisso com a satisfação do usuário. A equipe PrimeSupport® da McAfee, que conta com técnicos de suporte atenciosos e altamente qualificados, oferece soluções sob-medida e assistência técnica detalhada para gerenciar o sucesso de projetos essenciais — tudo isso com níveis de serviço que atendem às necessidades de todas as empresas. A McAfee Research, líder mundial em pesquisa de segurança e sistemas de informação, continua na vanguarda da inovação no desenvolvimento e no refinamento de todas as nossas tecnologias.

McAfee, SpamKiller, powered by SpamAssassin, WebShield, ePolicy Orchestrator, Protection-in-Depth, and PrimeSupport são marcas comerciais, registradas ou não, da McAfee, Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. A cor vermelha relacionada com a segurança é marca distintiva dos produtos que levam a marca McAfee®. Todas as outras marcas comerciais, registrada ou não, mencionadas aqui pertencem exclusivamente aos seus respectivos titulares. © 2004 Network Associates Technology, Inc. Todos os direitos reservados.1-sps-spka-003-0804