

# McAfee SpamKiller 3000 Series Appliances

In today's multi-faceted networking environments, it is essential to ensure that content entering and leaving an organization meets the company's security policies and privacy regulations. McAfee® Secure Content Management solutions deliver integrated, flexible technology, allowing businesses of all sizes to optimize resources, increase productivity, and prevent security policy compromises. With best-of-breed anti-virus, anti-spam, and secure content technologies, McAfee Secure Content Management solutions enable you to control, manage, and understand your Internet traffic.

McAfee SpamKiller® appliances provide industry-leading, anti-spam protection and content filtering in one integrated hardware and software appliance solution. SpamKiller offers an out-of-the-box spam detection rate of up to 95 percent.

## Is Spam Just a Nuisance? No!

### A Devastating Threat

Unwanted e-mail will cost U.S. corporations more than \$10 billion in 2003, according to a report released in January 2003 by Ferris Research. A recent study by the Gartner Group estimates that by the end of 2004, more than 50 percent of message traffic will be spam, unless enterprises take defensive action.\* McAfee identifies four key nuisance areas where spam can cost your organization money.

- **Lost Productivity**—The amount of time users waste reading and dealing with unwanted e-mail. Lost productivity for users is estimated to be the largest spam-associated cost for companies
- **Inappropriate Content**—E-mail that is in some way deemed offensive and most likely an HR violation. This type of message could offend an individual or group of people, e.g., the message could contain adult content subject matter
- **Consumption of IT Resources**—The amount of bandwidth used by incoming spam e-mail

- **Spam as a Security Threat**—Spam e-mails can contain malicious code or distributed denial of service (DDoS) attack, and virus-infected e-mails can use spam-like methods of distribution (e.g., Sobig.F and mass-mailing). Spam protection is an essential component of your security policy

\*Sources: *Spam Control: Problems and Opportunities*, The Ferris Group, January 2003, and *Waves of Information Disruption Due in 2003*, The Gartner Group, December 2002.

## McAfee SpamKiller Technology

### Powered by McAfee SpamAssassin

The core technology of the SpamKiller appliances is the McAfee SpamAssassin™ engine. The SpamAssassin engine works on a rating system that scores e-mail based on a series of tests. It is highly accurate in spam identification and catches up to 95 percent of all spam e-mail out-of-the-box, while providing a very low false-positive identification rate of less than 0.5 percent. The default SpamKiller rules, maintained by McAfee, require no rule-setting and are effective at detecting spam *out-of-the-box*.

## Scoring System

### Different Scores for Different Messages

SpamAssassin uses a scoring system based on an extensive rule set, to determine whether a particular e-mail message is spam. Hundreds of rules are run against every e-mail, and each rule has a negative or positive score associated with it. Rules with negative scores indicate attributes of legitimate mail and rules with positive scores indicate attributes of unsolicited mail. When combined, these individual scores give each e-mail an *overall spam rating*. A genetic algorithm optimizes the scoring, using an archive of millions of spam and non-spam messages to determine the scores for the individual rules. Now that e-mail is used as a critical part of the business infrastructure, it is vital for every anti-spam vendor to provide safeguards against erroneously identified spam e-mail. Scoring systems are essential in today's fight against spam, as they are more accurate than traditional matching techniques and allow the *gray areas* in detecting spam to be identified.

## Spam Detection

### Multiple Methods to Ensure Detection

Utilizing the underlying default rule-set process, McAfee SpamKiller appliances check each e-mail message received, using different methods of detection.

- **Integrity Analysis**—SpamKiller examines the header, layout, and organization of each e-mail message, identifying the common characteristics of spam
- **Heuristic Detection**—This is used to identify e-mail as probable spam. Heuristic detection uses a series of internal tests to determine the likelihood that a message might be spam, and each test carries a score to help reduce false positives
- **Content Filtering**—This functionality can be used to help identify key words or phrases that appear in an e-mail that could indicate that the message is spam
- **Blacklist and Whitelist Support**—Administrator-defined blacklists block domains that administrators know to be senders of spam, while administrator-defined whitelists always allow e-mail from administrator-specified domains
- **DNS Blocklist Support**—The McAfee WebShield® appliances support the use of DNS-based black hole lists for identification of known senders of spam e-mail
- **Bayesian Filtering**—SpamKiller provides Bayesian filtering technology to allow e-mail messages to be intelligently assessed for spam and non-spam criteria. The Bayesian filtering provided includes a pre-taught database of Bayesian filters, as well as proactive technology to automatically learn what types of messages should be classed as spam and non-spam in your organization

## Advanced Content Filtering Monitors What Is Entering and Leaving Your Network

What if you could protect against inappropriate content coming into the network, as well as guard against sensitive information leaving the network? Content filtering can prevent both. With lexical scanning of e-mails and more than 300 types of attachments based on content management rules, and true file attachment type identifications to prevent common rule evasion, content filtering protects your employees and your systems from harm. E-mails and attachments can be replaced with a customizable message if they contain specific words or phrases that violate a content rule.

## Policy-Based Control with eXtended Policy Support

WebShield provides organizations with policy controls for virus protection, content, and spam-filtering rules. With WebShield, administrators now have the ability to set specific filtering rules for individuals or groups of users across multiple scan types to ensure greater scanning and configuration flexibility. When defining rules and specifying groups of people, WebShield provides access to Microsoft® Active Directory or LDAP, allowing customers to utilize existing directories of users.

## McAfee Dashboard

Providing forensic analysis and system status, the McAfee Dashboard shows administrators the health and information statistics of the installed appliance in one easy-to-view screen, detailing statistics such as the number of detected viruses or spam messages. As part of the dashboard functionality, WebShield provides the ability to collect more in-depth details on SMTP sessions, such as the number and type of messages that have been seen by the appliance. This information can be used as a tool in debugging, troubleshooting, and forensic activity, as well as helping organizations fulfill company requirements for compliance with security best-practices required by internal information auditors.

## Detailed Graphical Reporting

WebShield integrates with McAfee ePolicy Orchestrator® for graphical reporting and trend analysis, providing a bird's-eye view of Internet gateway activity.

## E-Mail Performance

### The Right Tool for Your Business

McAfee SpamKiller 3000 Series Appliances are built and tuned for performance and reliability. The 3100 is designed for smaller businesses and will scan 30,000 SMTP messages per hour running with SpamKiller and content management configured; the 3200, for medium-to large-size businesses, will scan 55,000 SMTP messages per hour running with SpamKiller and content management configured; and the 3300 for enterprise organizations, businesses with high-performance requirements, or businesses using copper gigabit network infrastructures, will scan 110,000 SMTP messages per hour running with SpamKiller and content management configured. Built-in load sharing technology within the appliance range allows the use of multiple appliances if greater performance is needed.

## SpamKiller Appliance Components

### McAfee SpamKiller Appliances Include:

- Software license for SpamKiller software for appliances, to reduce the impact of spam
- Software license for McAfee Advanced Content Filtering to enable the monitoring of traffic in and out of the network
- A six-month trial license for McAfee's award-winning WebShield anti-virus software for appliances

## Anti-Phishing

SpamKiller includes specific rules that help to identify *phishing* attacks by looking for certain phishing-specific characteristics that can be present in e-mail. Once triggered, these rules are automatically assigned an overall spam rating by SpamKiller, which results, in most cases, with the messages being blocked. Together with the Anti-Phishing Working Group (APWG), McAfee has compiled a thorough database of phishing attacks and uses the knowledge from these attacks to create effective filtering rules.

## McAfee PrimeSupport

McAfee has pursued a strategy of providing best-of-breed technology for each type of security and performance management application—but the Protection-in-Depth™ Strategy is more than just deploying and implementing best-of-breed solutions today. Prevention is certainly our first priority, but inevitably, you will have to react to a problem.

The McAfee PrimeSupport® program is essential for making the most of your investment in McAfee System and Network Protection Solutions. McAfee's PrimeSupport team has all the right resources and is ready to deliver your needed service solution. PrimeSupport resources include: delivering authorization to access all available maintenance releases and product upgrades, access to a comprehensive suite of additional online self-support capabilities, live telephone support accessible 24/7/365, available assigned support account managers, and a range of software and hardware support solutions that can be tailored to meet your needs.

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

McAfee® products denote years of experience and commitment to customer satisfaction. The McAfee PrimeSupport® team of responsive, highly skilled support technicians provides tailored solutions, delivering detailed technical assistance in managing the success of mission-critical projects—all with service levels to meet the needs of every customer organization. McAfee Research, a world leader in information systems and security research, continues to spearhead innovation in the development and refinement of all our technologies.

McAfee, SpamKiller, powered by SpamAssassin, WebShield, ePolicy Orchestrator, Protection-in-Depth, and PrimeSupport are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. The color red in connection with security is distinctive of McAfee® brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2004 Networks Associates Technology, Inc. All Rights Reserved.

1-sps-spka-004-0904