



ANTI SPAM SOLUTIONS TECHNOLOGY REPORT

McAfee Secure Internet Gateway



NOVEMBER 2006

CONTENTS

Secure Internet Gateway



McAfee Corporate Headquarters: 3965 Freedom Circle, Santa Clara, CA 95054, USA
www.mcafee.com

Introduction3

Spam in the WCL Tests4

Test Network5

Test Methodology6

Product Testing Reporting7

Checkmark Certification8

The Product9

Developments in the McAfee Spam Technology10

Test Report11

Test Results16

West Coast Labs Conclusion17

Security Features Buyers Guide18



INTRODUCTION



As the war for corporate inboxes intensifies, and unmonitored emails disrupt effective and secure working practices, Anti-Spam solutions continue to evolve to deal with this menace.

In this, the second Anti-Spam Technology Report, we examine the functionality and performance of the leading products in this market, which are aimed specifically at the SME network environments.

A key objective of the testing is to replicate the installation, configuration and use of the solutions in a real-world business environment to enable readers of the White Paper – prospective buyers – to make a meaningful assessment of the product that is right for protecting their corporate email environment.

Test Engineers have evaluated how the solutions install to ensure timely and effective spam protection. Consideration has also been given to the level of security administrator expertise and technical support required to facilitate both out-of-the-box operation and thereafter product training to ensure maximum effective spam protection.

This reports provides an independent assessment of effectiveness with regard to:

- The features and functionality of the solution.
- Integration into a network infrastructure.
- The level of user administration required to operate the product effectively.
- Spam detection capability and rates of detection.

SPAM IN THE WCL TESTS

As part of the Anti-spam testing, WCL engineers used one of six domains wholly owned and controlled by West Coast Labs. Each of these domains contained several user accounts that were then signed up to a wide range of newsletters and websites with the aim of generating a significant daily spam feed. These sites included those offering free legal and financial advice, sports sites, dating sites, and some offering free adult content. These spam feeds were then left for several months before the beginning of the Technology Report so that email addresses belonging to each of the domains could propagate through an array of spam lists.

In the context of this Technology Report and the specific spam testing, mail received to the 'users' in each of the domains which formed part of the tests was classified into one of three categories: Genuine, Grey, and Spam. By manually classifying each email received, engineers at West Coast Labs could report on statistical figures relating to how many messages were correctly identified as Spam, the number of messages incorrectly identified as Spam (false positives), and finally the number that were missed. Using these figures each product could then receive a percentage representing the catch rate.

GENUINE MAIL

Messages were sent from engineers at West Coast Labs from both internal addresses and external web mail hosts such as Hotmail, ntlworld, and Yahoo!. Also included within this category were some newsletters based upon particular business requirements.

GREY MAIL

Messages classified by West Coast Labs as grey mail may be described as mail where the classification is unclear. For the purposes of this Technology Report, grey mail includes email and newsletters from sites that were known to be visited during the signup process but would otherwise be recorded as Spam, for example some of the free adult newsletters.

SPAM

Incoming mail was classified as Spam dependent upon common rules across the entire range of testing, for example unrequested emails or newsletters containing content such as free pharmaceuticals and or narcotics, Nigerian scam emails, unrequested pornography, weight loss or financial advice. Included within this category are the commonly seen random-text emails containing strings of unconnected words or phrases.

Note : As a test laboratory accredited to ISO 17025:2005, all websites visited and signed up to by West Coast Labs adhered to strict EU legal guidelines. Any messages that may be received as a result of address proliferation that contain content defined by UK law as illegal was immediately forwarded to the Internet Watch Foundation.

More information about the Internet Watch foundation can be found at www.iwf.org.uk.

TEST NETWORK



WCL has a number of domains that collect genuine spam. These domains receive varying levels of spam and are consistent with different email environments.

To reflect the email usage within a corporate environment, within each domain are a number of designated user accounts with a variety of email practices and needs including some that are subscribed to a variety of newsgroups and mailing lists. Some user accounts actively contribute to mailing lists.

The multiple domains designated for testing purposes were those that, between them, receive spam at a level consistent with the defined requirements of testing.

Software solutions included in the test program were installed on servers that meet the minimum specifications required by the vendor. Appliance-based solutions were installed on the network according to the vendor's recommended placing.

For hosted services, WCL tested through identified email domains and changed the MX records to divert the mail stream through the hosted service.

TEST METHODOLOGY

A decorative horizontal bar consisting of a blue segment on the left and a red segment on the right.

WCL initially performed the testing with an “out-of-the-box” configuration, changing only those settings on the solution needed to ensure correct operation in line with the vendor’s recommended installation and configuration procedures.

Further testing was then performed following the vendor's advice for the tuning or training of the solution under test. WCL fine-tuned the solution each day of the test, spending no more than half an hour per day undertaking such work.

Throughout the course of testing, a mixture of email was sent to the test domains from other email addresses and domains controlled by WCL to mirror genuine email activity common in business, for example, requesting meetings, sending notifications to groups and non-business related social emails.

Emails were also sent from web-based accounts such as Hotmail and Google's Gmail in order to simulate external users sending non-business related social emails, and home workers.

Thus, during the testing period the domains received some spam, some list/newsgroup mailings and "genuine" individual emails.

PRODUCT TEST REPORTING



Product evaluation addresses three specific areas* - Management/Administration, Functionality, Performance plus Additional Feature Testing.

1. MANAGEMENT/ADMINISTRATION

- Ease of Setup/Installation
- Ease of Use
- Logging and reporting function
- Rule creation
- Customization
- Content Categories

2. FUNCTIONALITY

- Email Processing Steps
- Allow/Blocking of Email
- Quarantine Area
- Additional functionality reporting

3. PERFORMANCE

- Volume or Percentage of spam detected
- False positive rate
- Spam incorrectly passed through
- Legitimate mail blocked
- Legitimate subscription mail blocked

CHECKMARK CERTIFICATION

Upon completion of the testing, individual product results are analyzed, resulting in accreditation to one of the two Checkmark Certifications for Anti-Spam subject to achieving the following catch rates:-

- Checkmark Anti-Spam Certification - Premium - 97% and over Catch Rate.
- Checkmark Anti-Spam Certification - Standard - 90% and over Catch Rate.



THE PRODUCT

MCAFEE® SECURE INTERNET GATEWAY

McAfee® Secure Internet Gateway is an integrated solution that blocks spyware, spam, inappropriate Web content, phishing attacks, viruses, worms and Trojans. This simple, affordable solution is easy to install and virtually maintenance-free.

www.mcafee.com

MCAFEE SAYS ABOUT THE PRODUCT'S BUSINESS BENEFITS

Increase user productivity - Block spam and other threats so that users can be more productive

Thwart information theft - Prevent information theft by keeping phishing scams at bay.

Conserve precious email server resources - Prevent spam from clogging your email server.

Reduce corporate liability - By filtering obnoxious messages

Reduce staff workload - By allowing end-users to manage their own personal whitelists, blacklists, and access their spam quarantine over the web.

www.mcafee.com/us/smb/products/anti_spam/index.html

MCAFEE SAYS ABOUT THE PRODUCT'S TECHNICAL BENEFITS

- High anti-spam effectiveness, low false positive rate. Spam rules are automatically updated every 10 minutes by McAfee.
- Protect against known and unknown viruses with advanced McAfee scan engine
- End-user quarantine utilizes a centralized, scalable, off-box server to store messages.
- Multiple forms of end-user spam management: daily spam digests, Outlook spam submission tool, Web-based access to quarantine.
- Integration with McAfee's Outlook Spam Submission tool to support blacklists, whitelists and spam/ham submission

DEVELOPMENTS IN THE MCAFEE SPAM TECHNOLOGY

AS STATED BY MCAFEE...

The inclusion of IP Reputation Filtering to identify malicious computers that have recently launched email attacks and block all of their messages. McAfee IP Reputation Filtering monitors over 1 billion SMTP connections for evidence of malicious activity.

At any given time, our database contains threat information for approximately 40,000 suspicious computers. Unlike other reputation systems, senders cannot self-certify their “good” reputation in an attempt to evade this layer of defense.

Through the inclusion of image-based spam detection, multiple proprietary technologies are used to identify spam messages that are based solely or primarily on images.

McAfee's new domain name reputation technology proactively identifies potentially bad URIs even before they are ever used in a spam campaign. This unique detection technique can block up to 40 percent of spam attacks even before they occur.

TEST REPORT



INTRODUCTION

The McAfee product under test in this Technology Report is McAfee Secure Internet Gateway v4.2, specifically the 3100 model based on a Dell Poweredge 750 server. Secure Internet Gateway is designed to monitor and protect a corporate IT network across a range of services including HTTP and FTP. The only service undergoing testing for this Tech Report was SMTP.

The device is fully rackmountable and has connections available on the front of the box for a USB keyboard and mouse along with a standard VGA connection for a monitor. Also included on the front of the appliance are both a CD and floppy disk drive. The rear of the appliance also provides a standard VGA socket, two USB connections, two PS/2 ports, a serial port, and two RJ45 network interfaces.

TEST REPORT

INSTALLATION AND CONFIGURATION

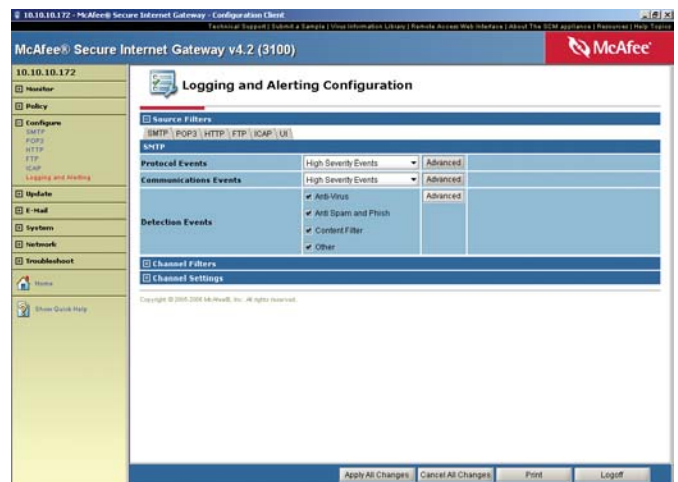
Installation of the appliance is very quick, and with the help of the clear on-screen descriptions and detailed user documentation, very easy. Due to this, minimal configuration is needed before the McAfee Secure Internet Gateway can begin protecting a network. This configuration can be carried out either from a client-side Java application, or a web-based Java applet.

Initial configuration requires some basic networking information. The appliance must be configured with standard details such as the gateway, a nameserver and the IP addresses - the domain name should also be entered along with a network name for the appliance. The final step in configuring the appliance is assigning the internal mail server addresses so that mail scanned by the appliance may be forwarded to the appropriate recipients within an organisation.

The layout of the pages relating to the setup of Secure Internet Gateway is both clear and user friendly. Thanks to the concise descriptions relating to each option the appliance can be configured and begin protecting the host network from Spam in minutes.

After the networking configuration is complete, further customization of the appliance is available from the setup menu. From here the user can access options relating to the various supported protocols including FTP and POP3, along with those relating to logging and reporting. For the purposes of this Technology Report, engineers dealt with those options contained within the SMTP category.

Once expanded, the SMTP category displays six further sub-categories these include Delivery Settings, Anti-Relay Settings, Permit and Deny Settings, Connection Settings, Retriever, and Transparent Exceptions. This gives Secure Internet Gateway a broad range in the number of possible customizations.



TEST REPORT

INTERFACE

Upon loading the Java-based interface, the user is presented with a login screen requesting the address of the server, the username, and password for logging into the device. For remote users McAfee Secure Internet Gateway also provides a web-based interface that can be accessed across a secure Internet connection on a standard port. The interface itself uses the same Java technologies and design as the standalone console, which means an Administrator can easily swap between the two without having to learn a different interface layout.

Throughout the duration of these tests, engineers used the standalone console in line with McAfee's recommendation.

After the login, the interface presented is clear and concise - it has been designed to reduce the learning curve, and hence the time needed before the appliance can be fully utilized in protecting a network. The interface is easily navigated through the use of expanding option menus and hyperlinks where all the information is readily available without the need to dig, a time saver when compared with products that bury information under several levels of links.

The initial screen presented to the user is the Status page. The name and version of the product is displayed at the top, while the menu runs down the left hand side. Above the menu is displayed the IP address of the Secure Internet Gateway appliance. The menu consists of eight options, all of which can be expanded, including Monitor, Policy, Configure, Update, Email, System, Network, and Troubleshoot. Below these options are links for the Help Guide and Home Page, the latter returns the user to the initial login page.

The main area of the Home page displays a full statistical analysis of the information gathered by the appliance. This information includes the number of Phish and Spam messages detected, and hourly throughput of traffic over such protocols as SMTP, FTP, and HTTP. Also contained within these statistics are the numbers of Viruses detected over the common protocols, although this is outside of this Report.

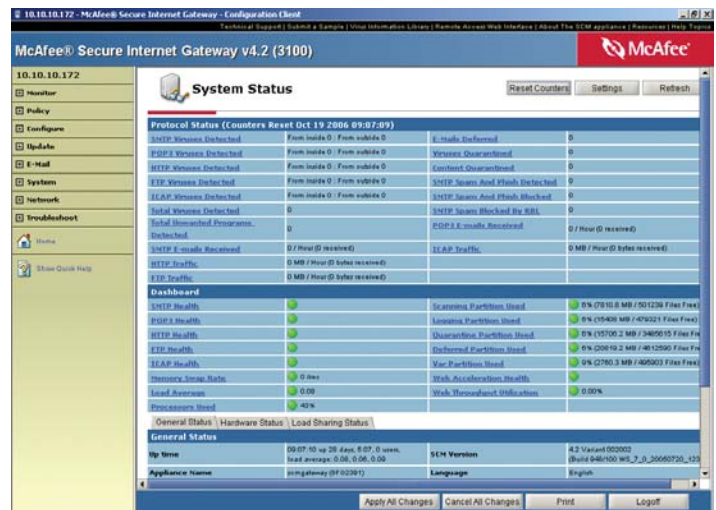
Presenting this information on the initial login page ensures that the Administrator can quickly get an overview on the performance of the appliance. Not being required to dig for such information increases the chance that any potential problems may be detected and remedied before having any significant impact on the network.



TEST REPORT

McAfee Secure Internet Gateway allows the user some scope in customizing how the appliance handles mail identified as Spam. For the purposes of aiding statistical analysis in this Technology Report, engineers set the device to tag all the unsolicited mail identifying the mail as Spam. This tag was prepended to the subject line of the original email. Use of this option quickly allows a user to group and delete batches of unwanted mail while also being able to check for any messages that may be incorrectly identified as spam.

The appliance carries out training of McAfee Secure Internet Gateway automatically, although this training can be further enhanced through the use of McAfee's Customer Submission Tool. This is a freely available download and can be used as a plugin for Microsoft Outlook. Should Secure Internet Gateway engines miss any Spam messages, the user is able to submit the message to McAfee Labs. Engineers at McAfee will then analyze all submissions and, if appropriate, add identifying data to the next Spam definition update.



The screenshot displays the McAfee Secure Internet Gateway v4.2 (3100) System Status dashboard. The interface includes a navigation menu on the left with options like Monitor, Policy, Configure, Update, E-Mail, System, Network, and Troubleshoot. The main content area is titled 'System Status' and features a 'Reset Counters' button, 'Settings', and 'Refresh' options. Below this, there is a 'Protocol Status (Counters Reset Oct 19 2006 09:07:09)' table with columns for protocol, source, destination, and count. A 'Dashboard' section shows various system health indicators with green status icons. At the bottom, a 'General Status' section provides information about the system time, load average, SEM version, appliance name, and language.

Protocol	Source	Destination	Count
SMTP Viruses Detected	From inside 0 / From outside 0	E-Mail Quarantined	0
SMTP Viruses Detected	From inside 0 / From outside 0	Viruses Quarantined	0
HTTP Viruses Detected	From inside 0 / From outside 0	Content Quarantined	0
HTTP Viruses Detected	From inside 0 / From outside 0	SMTP Spam And Phish Detected	0
HTTP Viruses Detected	From inside 0 / From outside 0	SMTP Spam And Phish Blocked	0
SMTP Viruses Detected	0	SMTP Spam Blocked By SBL	0
Spam Quarantined/Approved	0	SMTP E-mails Received	0 / Hour (0 received)
SMTP E-mails Received	0 / Hour (0 received)	HTTP Traffic	0 MB / Hour (0 bytes received)
HTTP Traffic	0 MB / Hour (0 bytes received)	SMTP Traffic	0 MB / Hour (0 bytes received)
FTP Traffic	0 MB / Hour (0 bytes received)		

Component	Status	Value
SMTP Health	OK	6% (7910 MB / 201228 File Freq)
HTTP Health	OK	4% (25406 MB / 47621 File Freq)
HTTP Health	OK	6% (15700.2 MB / 348015 File Freq)
HTTP Health	OK	6% (20616.2 MB / 461260 File Freq)
HTTP Health	OK	6% (2780.3 MB / 48520 File Freq)
Memory Usage	OK	0.0%
Load Average	OK	0.00
Processors	OK	40%
Web Acceleration	OK	Web Acceleration Health
Web Throughput	OK	Web Throughput Utilization

General Status

System Time: 09:07:10 on 28 Aug 2006 5:07:00 AM
 Load Average: 0.06, 0.06, 0.06

SEM Version: 4.2 Update 020002
 (Build 046100 MS_7_0_20060720_12)

Appliance Name: smgateway (8192391)
 Language: English

TEST REPORT

REPORTING

Reporting and monitoring is carried out from a series of links available under the Monitor tab in the user interface. The data gathered by Secure Internet Gateway may be viewed in a variety of different formats including a statistical breakdown, various graphical representations, and detailed log entries. Options are available under the Monitor category in the menu to view data regarding Status, Performance, Logs, Charts, Updates, and Resources.

Using the Status option displays the same data shown on the initial Home page of the interface - a total count of the messages scanned by Secure Internet Gateway including a count of how many were placed into categories including Spam, phishing, and virus infected.

The most detailed and varied reports are available from the Logs page. This provides the Administrator with a range of categories from which to choose including Resource and System, Protocol, Communications, and Detections each containing a further list of Report Types.

Of principle interest to readers of this report will be Spam and Phish, found under the Detections category. When selected, this displays records of all detected Spam and Phish messages laid out in a table format and organised into several fields. These fields include Spam Score, Rules Broken, Sender, Recipient(s), and Source Address.

Also of interest in ensuring that the latest definitions are being used by McAfee's Secure Internet Gateway is the Update section which is part of the Monitor category. This reports upon the various engines used by Secure Internet Gateway and their current update status, along with the date of the last successful update.

The data presented in the log entries is all well formatted and appropriate, and it is useful for troubleshooting purposes to note that there are also reports generated by the device that allow the user to view system events if necessary.



TEST RESULTS

<u>Type of Mail</u>	<u>Detected as Genuine</u>	<u>Detected as Spam</u>
GENUINE	100%	0%
SPAM	2%	98%

McAfee's Secure Internet Gateway performed well during the installation, setup, training and spam detection testing processes, delivering 100% of the genuine mail correctly and correctly classifying 98% of the Spam mail.

It is also worth noting that Secure Internet Gateway delivers a good proportion of grey and list mail as genuine. This gives an organisation the flexibility and opportunity to define policies during a training period without missing mail that could potentially be business critical.

West Coast Labs is pleased to award Secure Internet Gateway the Premium Anti-Spam Checkmark certification.



WEST COAST LABS CONCLUSION



The appliance may be installed and configured very rapidly, and this is coupled with informative monitoring and impressive scalability. The ability of this solution to run many of the tasks as automated processes will make more time available for any hard-pressed administrators or network teams. Further to this, the speed in which basic configuration can be performed along with the design of the hardware, allows the appliance to be rapidly integrated into any corporate network.

Data gathered by the appliance is displayed clearly and provides a high level of Information. This may then be used to inform an Administrator so that they may better protect their network from the effects of unwanted mail.

The ability of the appliance to also protect the host network from viral infestation adds to the level of protection afforded by Secure Internet Gateway. This is further enhanced by plugins and tools designed by McAfee to compliment the product.

West Coast Labs Disclaimer

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is not always possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose.

Therefore, the test results published within any given report should not be taken and accepted in isolation. Potential customers interested in deploying any particular product tested by West Coast Labs are recommended to seek further confirmation that said product will meet their individual requirements, technical infrastructure and specific security considerations.

All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability. When West Coast Labs provide test results for any particular product tested, said results are most relevant at the time of testing and within the context of the specific scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools utilized during that specific test process.

West Coast Labs is unable to directly endorse or certify the overall worthiness and reliability of any particular product tested for any given situation or deployment.

SECURITY FEATURES BUYERS GUIDE

AS STATED BY MCAFEE...

- Integrity analysis examines the header, layout, and organization of each email message and identifies common spam characteristics
- Bayesian filtering intelligently assesses your email messages for spam and non-spam based on criteria specific to your business
- Content filtering uses keywords, phrases, and embedded URLs to identify spam email
- Blacklists and whitelists let your administrator and users ensure that important messages will not be blocked
- Centralized management allows you to configure multiple implementations of McAfee Anti-spam with a single action.

ADVANCED SPAM MANAGEMENT TOOLS

A spam solution should do more than just block spam; it should provide a rich set of management tools. McAfee provides the following:

- Daily digests of quarantined messages list the header of each message and state whether it was blocked because it was spam, phish, or for some other reason such as inappropriate content or forbidden file attachments. Users can click a drop-down box next to each message to release it from the quarantine and/or to add the sender of the message to the user's personal white list.
- On-box quarantine. You can choose to store quarantined messages on the McAfee appliance, ideal for small and mid-size organizations.
- Off-box quarantine. You can choose to store quarantined messages on your own server running McAfee Quarantine Manager. McAfee Quarantine Manager provides easy, centralized management of spam and other forms of quarantined email, which is particularly useful when using multiple McAfee appliances. Users can access the centralized quarantine via a web browser to search for messages and manage their whitelists and blacklists.
- Microsoft® Outlook plug-in allows users to configure their own whitelists and blacklists. It can also be used to send samples of missed spam back to the appliance or to McAfee's labs for purposes of learning and fine-tuning. McAfee's anti-spam appliances have the ability to learn the peculiar characteristics of your organization's messages. Once the appliance has been provided with samples of mail, it uses Bayesian technologies to make better judgments on future messages.

SECURITY FEATURES BUYERS GUIDE

INTEGRATED SECURITY

McAfee Anti-spam integrates with and is a component of other McAfee products, such as GroupShield and Secure Internet Gateway. These integrated security products provide complete protection against messaging threats, both inbound and outbound. Here is a partial feature list:

EMAIL REGULATORY COMPLIANCE

McAfee Email Compliance contains predefined content filters for HIPAA, GLB, and other regulations; it blocks or encrypts messages containing private information.

CONTENT FILTERING

Built-in content filtering lets you guard against sensitive or proprietary information leaving your company or transiting departmental boundaries. Build acceptable use policies using regular expressions, and scan the contents of over 200 file types to detect violations.

BROAD ANTI-VIRUS PROTECTION

McAfee messaging security products block both known and unknown viruses, inbound and outbound traffic using SMTP and POP3 protocols. McAfee messaging security appliances also block viruses through webmail using HTTP and FTP protocols.

ANTI-SPYWARE

McAfee messaging security appliances also block spyware from entering through email or web protocols.

Denial of service attack prevention. Block or tarpit connections based on the arrival of malicious SMTP commands.

Directory Harvest Attack prevention. Block or tarpit connections based on the ratio of valid email recipient addresses to invalid ones.

Encryption. Policy-based encryption allows you to direct messages over an encrypted link using TLS, or to redirect the messages to a separate email encryption server.