

**McAfee  
Secure Messaging  
Gateway**

# Contents



## McAfee Secure Messaging Gateway



Test objectives and scenario .....	3
Test network .....	4
Test methodology .....	5
Product test reporting .....	6
Certification .....	7
The product .....	8
Test report .....	10
Test results .....	17
West Coast Labs conclusion .....	18
Security features buyers guide .....	19



West Coast Labs, William Knox House, Britannic Way, Llandarcy,  
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.  
[www.westcoastlabs.org](http://www.westcoastlabs.org)

## Test objective and scenario

The war for control of corporate inboxes has been raging for some years now as Anti-Spam solution providers seek to protect us from unsolicited, inappropriate and often offensive intrusions into our time.


The originators of these emails are becoming ever more inventive and so more and more companies are coming to rely on automatic solutions with learning engines to protect their users and machines. The emails themselves are getting more sophisticated. Spam is now no longer just advertising material, but is evolving, and often acting as the precursor to identity theft.

This Technology Report examines the functionality and performance of participating Anti-Spam products which are aimed at the small, midsize and corporate network environments. It has been open to both software and appliance-based solutions plus hosted services.

The objective of our overall testing program, which is open to all Anti-Spam Vendors is, through a real-world test environment, to provide an independent validation of Anti-Spam solution effectiveness with particular reference to:

- A detailed view of the features and functions of the solutions
- Spam detection capability and rates of detection of each solution
- Integration into a network infrastructure and level of administration required to operate effectively.

# Test network



Software solutions are installed on servers that exceed the minimum specifications required by the vendor.

Appliance-based solutions are installed on the network according to the vendor's recommended placing.

For hosted services, WCL test through identified email accounts and will change the MX records to divert the mail stream through the hosted service. In order to allow the DNS change to propagate, service providers allow a 2-day settling-in period.

Details of the tuning and vendor customer support will form part of the additional feature testing and reporting.

## Test methodology

WCL has a number of domains available which act as honeypots for spam, receiving genuine, not canned spam. These domains receive varying levels of spam and are intended to mirror different email environments.

Within each domain are designated user accounts with a variety of email practices and needs - some are subscribed to a variety of newsgroups and mailing lists. Some user accounts actively contribute to mailing lists. The domain designated for testing purposes will be that which currently receives spam at a level consistent with the test requirements.

For testing in this Technology Report and for the certification of each of the participating solutions, we used live mail feeds coming in to various extra domains wholly owned and controlled by West Coast Labs. Each domain used contains a number of individual user accounts with established email addresses, along with distribution lists.

To maintain the flow of genuine mail, test engineers used several internal and external accounts, to send emails that simulated real life email transactions 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 to simulate external users sending non business-related emails and home workers. Individual user accounts were subscribed to several mailing lists and daily newsletters for grey mail purposes.

For each solution we configured the device or software to fit in with the test network and placed it into a stream of live mail to see how it would cope in an 'out-of-the-box' configuration with real-world traffic. However, we do recognize that a large part of spam detection relies on an initially intensive learning process. (Hence, we will be placing these devices in the mail feed in coming months for longer periods of time, interactively training them, and updating the performance data included in the online White Papers.)

# Product test reporting

For each product that we test, we will issue a report which will address the following aspects of the product:

### 1. Management/Administration

- Ease of Setup/Installation
- Ease of Use
- Logging and reporting function
- Rule creation
- Customization
- Content Categories
- Technical Support Available
- Program Help Menu

### 2. Functionality

- Email Processing Steps
- Allow/Blocking of Email
- Quarantine Area
- Additional functionality reporting
- Block Email Addresses
- Blacklist/Whitelist
- Allow Email Addresses

### 3. Performance

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

## Certification - Checkmark

Upon successful completion of the catch rate testing, participating solutions will be accredited to Checkmark Certifications for Anti-Spam subject to achieving the following catch rates:-



Checkmark Anti-Spam Certification  
PREMIUM – 97% and over Catch Rate.

[www.check-mark.com](http://www.check-mark.com)



Checkmark Anti-Spam Certification  
STANDARD – 90% and over Catch Rate.

[www.check-mark.com](http://www.check-mark.com)

## The product

McAfee has a broad product portfolio that secures systems and networks from known and unknown threats. McAfee claims that its Secure Messaging Gateway (SMG) product protects against spam, inappropriate content, phishing, worms, viruses and messaging system attacks. McAfee further states that the dedicated appliance provides enterprise-class performance to meet the most demanding requirements.

*[url : http://www.mcafee.com/us/products/mcafee/scm\\_app/smg.htm](http://www.mcafee.com/us/products/mcafee/scm_app/smg.htm)*

McAfee further claims that the Secure Messaging Gateway meets the throughput requirements of large organizations (over 1000 users). A lower-cost version of this product is available for smaller organizations -- McAfee Secure Internet Gateway.

### ***McAfee says...about the Secure Messaging Gateway's Business Benefits.***

- Increase employee productivity and reduce strain on e-mail servers by blocking spam.
- Maintain business continuity by blocking viruses, worms and other malware
- Reduce risk of information theft by blocking phishing messages.
- Reduce staff workload by managing multi-level security – gateway, mail server and desktop – with one centralized application: McAfee ePolicy Orchestrator.
- Reduce liability and improve information security by filtering e-mails, both inbound and outbound.
- Save money with superior price performance

*[http://www.mcafee.com/us/products/mcafee/scm\\_app/smg.htm](http://www.mcafee.com/us/products/mcafee/scm_app/smg.htm)*

## The product (continued)

### ***McAfee says...about the Secure Messaging Gateway'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
- Multiple forms of administrative access, including out-of-band access
- High message throughput
- Flexible policy management based on LDAP directory

*url : [http://www.mcafee.com/us/products/mcafee/scm\\_app/smg.htm](http://www.mcafee.com/us/products/mcafee/scm_app/smg.htm)*

## Test report

### Introduction

The McAfee Secure Messaging Gateway is a 1U rackmountable Dell unit with a CD drive, power switch, NIC indicator lights, a VGA connection, two USB ports and a floppy drive on the front. It also has two power sockets for failover redundancy, a serial connection, a further VGA connection, keyboard and mouse connectors, two USB ports, and two recessed Gb NICs on the rear. A nice feature of the NIC connectors is that they have release catches so that fingers don't get caught when changing network cables.

The documentation came provided in printed form for the hardware, and in PDF format for the McAfee software. The abundance of software included the Secure Messaging Gateway Recovery, Linux Source, and System Diagnostics CDs.

Organisations with deployments of other McAfee security products will doubtless appreciate the ability to use ePolicy Orchestrator, also included on CD, with the Secure Messaging Gateway thus rationalising all their security products into one easy-to-manage system.

The screenshot displays the McAfee Secure Messaging Gateway v4.0 (3300) configuration interface. The main content area is titled "System Status" and includes a "Reset Counters" button, "Settings" link, and "Refresh" button. Below this, there is a "Protocol Status (Counters Reset Sep 14 2005 07:31:14)" table:

Protocol Status	Counters	Reset	
SMTP Viruses Detected	From inside 0 / From outside 3	SMTP Spam And Phish Detected	1002
PDP3 Viruses Detected	From inside 0 / From outside 0	SMTP Spam And Phish Blocked	0
Total Viruses Detected	3	SMTP Spam Blocked By RBL	0
Total Unsanitized Quarantines Detected	0	E-Mail Deferred	123
Viruses Quarantined	2	PDP3 E-mails Received	0 / Hour (0 received)
Content Quarantined	0	SMTP E-mails Received	14573 / Hour (259 received)

Below the protocol status is a "Dashboard" section with various health indicators:

- SMTP Health: ●
- PDP3 Health: ●
- Memory Usage Rate: ● 0.8%
- Load Average: ● 0.05
- Processors Used: ● 22%
- Scanning Partition Used: ● 6% (7230.7 MB / 501044 Files Free)
- Lessons Partition Used: ● 6% (13707.4 MB / 900371 Files Free)
- Quarantine Partition Used: ● 6% (14054 MB / 314887 Files Free)
- Deferred Partition Used: ● 6% (19152.0 MB / 424550 Files Free)

At the bottom, there is a "General Status" table:

General Status	Hardware Status	Load Sharing Status	
Up Time	09:04:12 up 1:33, 0 users, load average: 0.06, 0.06, 0.06	SCN Version	4.0 Variant 002000
Appliance Name	142 (6348776)	License	00000
Anti-Virus DAT	9278	Last DAT Update	Sep 14 2005 07:23:21
Anti-Virus Engine	4.4.0.0	Last Engine Update	Sep 14 2005 07:23:21
Anti-Spam Rules	1.0.2332.2332.2005	Last Rules Update	Sep 14 2005 07:23:21
Anti-Spam Engine	1.0.2332.1.3000	Last Engine Update	Sep 14 2005 07:23:21
		Last Streaming Update	Sep 12 2005 03:46:02

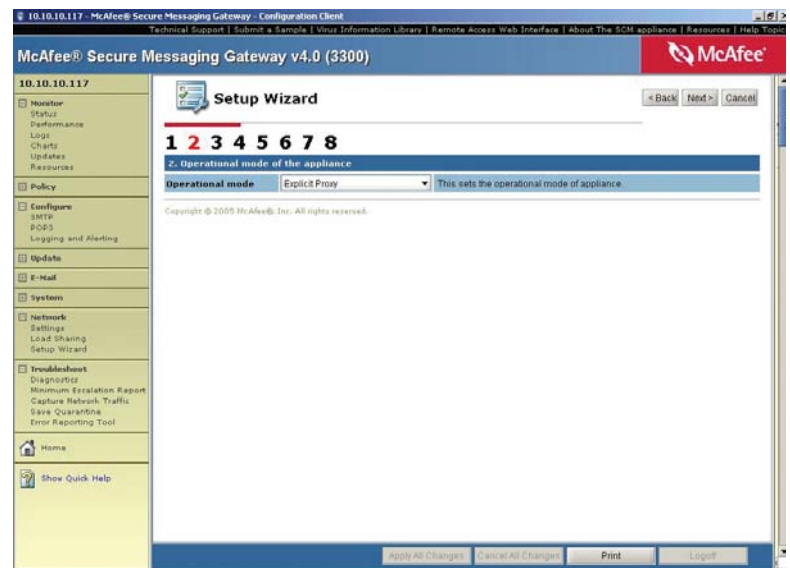
The interface also includes a left-hand navigation menu with options like Monitor, Policy, Configure, Update, E-Mail, System, Network, and Troubleshoot. At the bottom, there are buttons for "Apply All Changes", "Cancel All Changes", "Print", and "Logout".

## Test report

# Installation and Configuration

The initial installation and configuration is performed via a client machine that is assigned to a temporary private subnet for the duration of the process. It is worth noting that there are prerequisites for the client – the Java JRE 1.4.2 is essential and on some versions of Windows the client must be patched with Service Packs before commencing.

Installation is instigated by the user browsing to a secure web address on the McAfee device itself. There is then the opportunity either to download the standalone administration tool or continue via the web. We followed the McAfee recommended procedure and downloaded the standalone tool for administration.



The well written and clear manuals have detailed instructions for standalone installation on both Windows and Linux.

The rest of the initial set up is both rapid and uncomplicated as it guides the user through entering the networking parameters to fit in with the corporate network. The device was configured and ready to accept email within a few minutes.

## Test report

### Installation and Configuration *(continued)*

During the installation, the user must specify various parameters to allow the device to fit into the current corporate network, such as IP addresses for each interface and Fully Qualified Domain Name. The user also specifies the protocols that are to be used, and then internal and external networks.

During this phase of the installation, the appliance can be configured for a load sharing mode if multiple appliances are being used. Once configured in load sharing mode, all the load-sharing appliances can be managed from a single device's interface.

The appliance can be deployed in any of three different modes: Explicit Proxy, Transparent Bridge and Transparent Router. For this test, West Coast Labs used the Explicit Proxy mode.

The Anti-Spam component is integrated within the Secure Messaging Gateway appliance, which only needs to be activated by entering a license code within the interface.

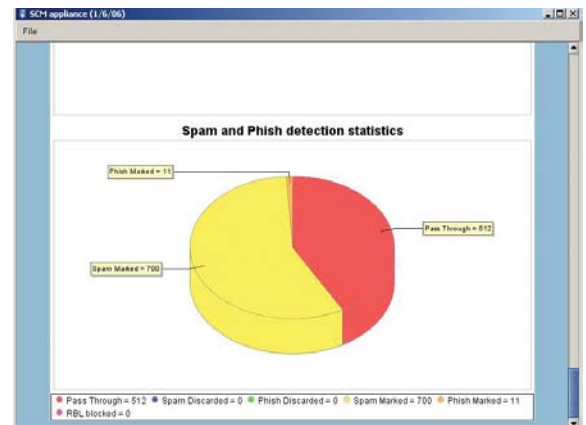
# Test report

## The Interface

The experience of setting up the device provides the user with a good grounding in using the interface. It is easy to navigate around the various options and menus. The initial status screen that shows upon login displays a large amount of useful detail – this includes not only traffic and detection statistics but also data such as the time and date of the most recent updates for the engines and rulesets, allowing the administrator to see at a glance the current state of play.

There are eight main sections within the interface: Monitor, Policy, Configure, Update, E-mail, System, Network, and Troubleshoot. Each of these has many subsections, but all are well marked and simple to locate.

Having successfully completed the initial set up, the manual then walks the user through the options available and gives some background information on how to set them up. The help screens that can be called from within the interface itself have just the right amount of information and are written clearly to ensure that users have the right advice about each option and can make informed decisions.



## Test report

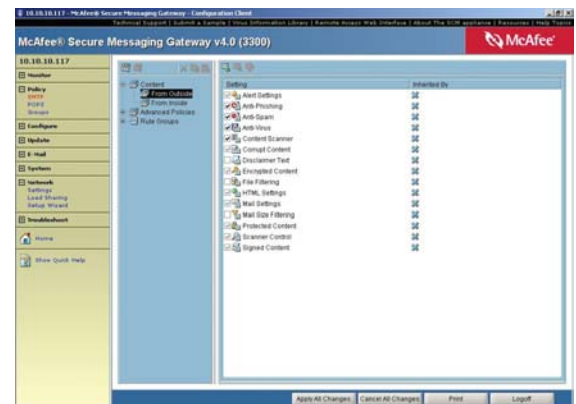
### The Interface (continued)

The Monitor group of options contains a plethora of reporting options that are broken down into logs, charts, performance data, along with the latest update status and a link to the status screen originally displayed upon login. The filtering tools available in the reporting section are well thought out and easy to use – they provide several useful ways of looking at the data.

Of particular interest when considering Spam, the Policy section allows the administrator to look at components that are enabled for each protocol. These fall into different categories such as Anti-Virus, Anti-Spam, Anti-Phishing, and Content Scanner.

Within the Anti-Spam module there is the ability to set blacklists and whitelists of email addresses, alter the dictionaries using words or complex phrases, and to set varying trigger levels at which to quarantine, notify or redirect emails to a specified user. It is also possible to set a subject line alteration if the mail is still to be delivered, and attach the Spam score marking as a header. These tools are aimed at giving the corporate administrator full control over an organisation's mail traffic, however ease of use is not overlooked and the rules are simple to implement.

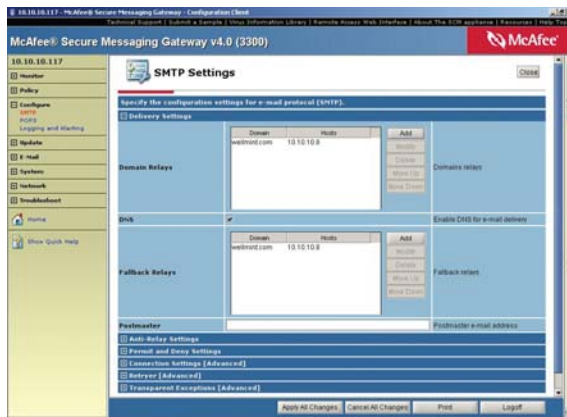
In the Policy section, you can configure different security policies for different groups of users in your organization. For example, the administrator may wish to set a maximum message size of, 10 MB for all users in the organization except users in the marketing department, for whom you will allow messages up to 20 MB. Similarly, an administrator can configure content scanning policies, such as blocking all financial data unless the user is in the finance department.



## Test report

### The Interface (continued)

In addition to stopping viruses, spam and other unwanted messages, the McAfee Secure Messaging Gateway blocks Directory Harvest attacks and other types of Denial of Service attacks against your messaging system. This ensures that your mail servers stay up and running, unaffected by e-mail storms on the Internet.



The Configure menu includes Quarantine Management, Logging and Alerting settings, and allows access to the Spam Learning facility settings – messages can be either queued for manual learning or automatically learned. This is also where the user will find various settings for each protocol that are

available for change or configuration. These include the number of connections allowed at once, listener ports and anti-relay settings, and all are laid out in subsections that are easy to understand. Once again it is worth noting the quality of the online help available in this section.

Update is a small but important section giving data for the last set of updates received for rules and engines for both the Anti-Spam and Anti-Virus functionality. It is also in this section that manual updates can be performed and scheduled updates may be enabled or changed with the option to get updates from McAfee's ftp server.

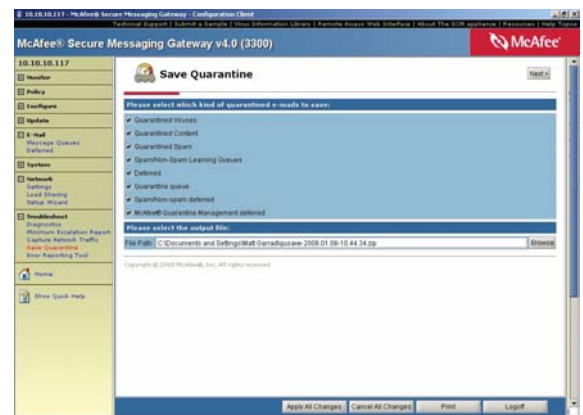
The section labelled Email is where the queue maintenance and management is performed. The McAfee device allows for either manual or automatic maintenance and it is possible to either learn or unlearn messages as spam or genuine. It is also possible here to set the times for the routine daily quarantine maintenance and the maximum time to keep mails in the quarantine. There is also a quick link to look at deferred emails with options available to forward or retry delivery.

## Test report

### The Interface (continued)


The System menus are where the optional components of the solution including ePolicy Orchestrator connection and the Anti-Spam functionality can be enabled. These are simple processes and only take a few seconds to get up and running. The management tools for either the individual appliance or a group of appliances are located in this section as well, and the system may also be backed up, restored or reset to a default status. The ability to export logs and configuration files in zip format from the system to an external client machine completes the line up.

The Network subsection allows the user to alter the way the device views networks as inside or outside, change network settings, enable or disable protocols and change the operational mode. It is also possible to set up load sharing if further units are purchased after the initial set up. Finally, for this section, the user is able to run the initial set up wizard again should the need arise.



The last menu item, and particularly worthy of note due to the features contained within, is the Troubleshoot section – it is possible from here to perform all the tests pertinent to the configuration with just a couple of clicks. There is basic traffic sniffer functionality that can capture everything on the network or be restricted to particular types of mail traffic relevant to the appropriate protocols – this is then exported to a client machine for further analysis. The error reporting tool is capable not only of monitoring the system but also of automatically submitting error events. Also built in to this section is the ability to export the quarantine to a local client machine as an archive file. All this functionality is nicely complimented by the ability to escalate problems to McAfee from within the interface.

## Results



Type of Mail	Delivered as Genuine (%)	Delivered as Spam (%)
GENUINE	100	0
SPAM	3	97

The Secure Messaging Gateway box performed well, delivering 100% of the genuine mail correctly and correctly classifying 97% of the spam mail in a straight out of the box configuration.

It is also worth noting that on default settings, the McAfee device delivers a reasonable proportion of grey and list mail as genuine, thus giving users and administrators within an organisation the flexibility and opportunity to define policies during a training period without missing mail that could be potentially business critical.

## West Coast Labs conclusion

As another valuable tool from McAfee to protect users on corporate networks, the Secure Messaging Gateway solution is very effective.

It boasts an intuitive and well thought out interface, which allows the administrator lots of control. Well structured and easy-to-use, all the options are located in the expected sections and the online help is both relevant and easily accessible.

This is a powerful product that deserves serious consideration from any corporation looking to stop users from getting spam.

The McAfee Secure Messaging Gateway device performed to a consistently high standard in the tests, and therefore West Coast Labs is pleased to award the McAfee Secure Messaging Gateway the PREMIUM level Anti-Spam Checkmark.



Anti-Spam  
PREMIUM



West Coast Labs, William Knox House, Britannic Way, Llandarcy,  
Swansea, SA10 6EL, UK. Tel : +44 1792 324000, Fax : +44 1792 324001.  
[www.westcoastlabs.org](http://www.westcoastlabs.org)

## Security features buyers guide as stated by McAfee

### SPAM MANAGEMENT

A spam solution should do more than just block spam, it should provide the users (and administrators) with a rich set of spam management tools. Here the McAfee device does not disappoint. Administrators have two options for storage of spam: The spam can be stored on the appliance itself, using the appliance's built-in 80 GB hard disks. Or the spam can be stored on a Windows server somewhere on the network that is running McAfee's free McAfee Quarantine Manager software.

McAfee Quarantine Manager may be especially advantageous for large organizations that utilize multiple Secure Messaging Gateway appliances, because having to manage just one spam quarantine is easier than managing multiple quarantines. Also, the McAfee Quarantine Manager represents just one place that users or administrators need to go to search for inappropriately blocked messages, release those messages, and configure blacklists and whitelists. Users can access McAfee Quarantine Manager from a web browser.

Regardless of where spam is stored, the McAfee device can be configured to send users a daily digest of the messages that have been blocked over the past 24 hours. The digest lists the header of each message and states 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 whitelist.

McAfee also provides an Outlook plug-in that can be used to send samples of missed spam back to the appliance or to McAfee's labs for purposes of learning and fine-tuning. The McAfee appliance has 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 as stated by McAfee

### SPAM FEATURES

Does the product block spam out of box or does it require addition or tuning of rules?

*The product blocks spam out of box.*

Is user feedback required over initial stage of deployment? *No*

### FILTERING

Does the product utilise keyword lists? *YES*

Does the product utilise Bayesian filtering? *YES*

Can white-lists/black-lists be set? *YES*

Does product support RBL? *YES*

Does the product support the setting of different confidence levels? *YES*

Can actions be varied at different confidence levels? *YES*

Can subject line of messages be altered? *YES*

Can email headers be set/amended? *YES*

## Security features buyers guide as stated by McAfee

### ADMINISTRATION

Can the product be automatically updated? *YES*

Can filters be automatically updated? *YES*

What are the update methods?

*Updates are delivered over HTTP every 10 minutes*

Can suspected spam be quarantined? *YES*

If so, what type of quarantine (forward to Q mailbox / saved on device / etc.)?

*Two options are available: on-box quarantine, or off-box centralized quarantine utilizing a Windows server.*

### END USER INTERACTION

Can users see reports individual to them and process their messages?  
*YES*

Can users review mail marked as spam? *YES*

Can users free messages from quarantine and set their own white lists/black lists? *YES*

## Security features buyers guide as stated by McAfee

### ADDITIONAL SECURITY FEATURES

- content filtering scans inside more than 300 types of attachments, both inbound and outbound
- message integrity analysis
- heuristic rules to protect against both known and unknown ("day zero") spam and phishing attacks
- global and personal blacklists and whitelists
- DNS blocklist and RBL support
- Bayesian filtering
- streaming rule updates (every 10 minutes) from McAfee
- daily spam digest
- web-based end-user quarantine
- secure, hardened Linux operating system
- auditing and tracking of administrative changes
- high-availability mode with failover configuration
- centralized administration of one or more appliances
- protect against directory harvest attacks
- inbound and outbound malware filtering ensures that your organization does not send viruses, spam or inappropriate content

*url : [http://www.mcafee.com/us/products/mcafee/scm\\_app/msg.htm](http://www.mcafee.com/us/products/mcafee/scm_app/msg.htm)*