



McAfee System Protection Solutions

Secure Scanning for Microsoft Exchange

Table of Contents

Abstract	3
-----------------	----------

GroupShield for Microsoft Exchange and the Microsoft APIs	3
--	----------

The Microsoft Exchange 5.5 and the Anti-Virus API 1.0	3
--	----------

The Microsoft Exchange 2000 and the Virus Scanning API 2.0	4
API 2.0 On-Access Scanning (a.k.a. Microsoft On-Demand Scanning)	4
API 2.0 Proactive Scanning	5
API 2.0 Background Scanning	5
How GroupShield Works with the Microsoft Virus Scanning API 2.0	5
Exchange 2000 Message Routing and the Virus Scanning API 2.0	6
Benefits of Using GroupShield with the Microsoft Virus Scanning API 2.0	6

Microsoft Exchange 2000 and Transport Scanning	7
---	----------

Microsoft Exchange 2000 and Anti-Spam	7
--	----------

Microsoft Exchange 2003 and Virus Scanning API 2.5	7
---	----------

Microsoft Exchange 2003 and Anti-Spam	7
--	----------

Abstract

This paper provides an overview of Microsoft® Virus Scanning API, Transport Scanning, Internet Message Filtering (IMF), Secure Confidence Level (SCL), and other techniques used by McAfee® Security GroupShield® for Microsoft Exchange to protect Microsoft Exchange 5.5, 2000, and 2003 environments from viruses, inappropriate content, and spam.

GroupShield for Microsoft Exchange and the Microsoft APIs

McAfee GroupShield for Microsoft Exchange provides comprehensive threat protection for e-mail and other content entering and leaving your Microsoft Exchange 5.5/2000/2003 environment. Proactive anti-virus scanning and an automatic Outbreak Manager prevent malicious code from disrupting the system, while advanced content filtering allows administrators to set up rules for inappropriate content, sensitive information, and adding disclaimers to messages.

McAfee Security GroupShield for Microsoft Exchange is an industry-leading solution for mail content security. By working closely with Microsoft, GroupShield was the first product released to utilize the Microsoft anti-virus 1.0, 2.0, and 2.5 APIs. 1.0 was introduced as part of the Microsoft Exchange 5.5 Service Pack 3 and was also used in the initial release of Microsoft Exchange 2000. With Service Pack 1 for Exchange 2000, Microsoft updated the API to improve functionality and performance, and in doing so, renamed it from “anti-virus” (AVAPI) to “virus scanning” API (VSAPI) 2.0. With the release of Microsoft Exchange 2003, Microsoft released VSAPI 2.5, building on the previous releases of the API. The following is a list of Microsoft Exchange versions and the API available for them to use:

- Microsoft Exchange 5.5 SP3—AV-API 1.0
- Microsoft Exchange 2000 SP1—VS-API 2.0
- Microsoft Exchange 2003—VS-API 2.5

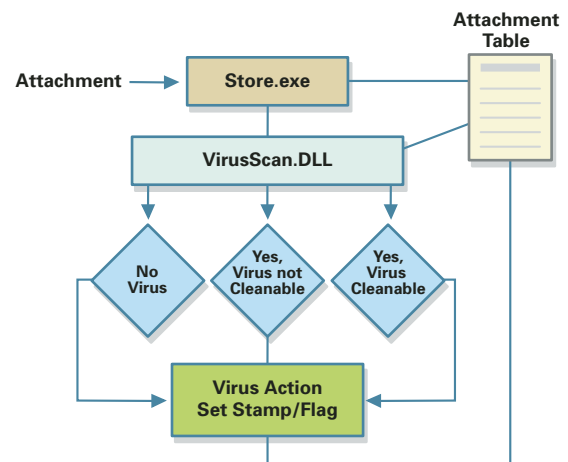
Note: The above APIs are not available for later versions of Exchange; for example Microsoft Exchange 5.5 cannot benefit from VS-API 2.0 or 2.5.

To overcome certain limitations of earlier APIs, GroupShield provides additional support, explained in further detail later in this paper, to increase the security of Microsoft Exchange. Following is a list of GroupShield versions along with support Exchange versions and additional scanning technology employed:

- GroupShield 5.0 SP1 for Microsoft Exchange 5.5
 - Microsoft Exchange 5.5 SP3—AV-API 1.0/MAPI/ESE-API
- GroupShield 6.0 for Microsoft Exchange
 - Microsoft Exchange 2000 SP1—VS-API 2.0/SMTP Transport Scanning
 - Microsoft Exchange 2003—VS-API 2.5

The Microsoft Exchange 5.5 and the Anti-Virus API 1.0

The anti-virus API 1.0 was introduced in Exchange Server 5.5 SP3 to provide high performance scanning of attachments in the Exchange Server information store. While anti-virus scanning solutions had been available using MAPI, due to timing of the scans and periodic server loading, it was possible for attachments to be delivered to users before being scanned. To combat this vulnerability, the anti-virus API provides low-level hooking into the Exchange stores and ensures that all attachments are scanned before a client can access them. In addition to scanning, the anti-virus API also provides the ability to selectively repair, mark as suspicious, or replace any attachment. Any time an attachment is opened, modified, or sent by a user, the anti-virus API ensures that the attachment is completely scanned before allowing it to continue in its delivery or storage.



Server performance is significantly improved over other solutions, such as MAPI-based scanning or other inter-process communication methods, because the API provides a means for the virus scanning to run in process with the information store. By scanning at the store level, attachments need only be scanned once, instead of multiple times as they move from a person’s “sent items” folder to multiple recipients’ “inbox” folders and then to “deleted items” folders.

The Microsoft Exchange 2000 and the Virus Scanning API 2.0

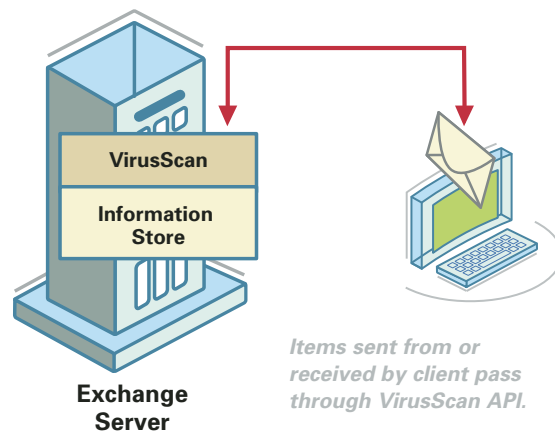
While the anti-virus API 1.0 provided improved scanning of attachments, version 2.0 addressed previous shortcomings and added functionality. The virus scanning API 2.0 was released as an upgrade to Microsoft Exchange 2000 in Service Pack 1 and contained the following enhancements:

- Scanning of all message items, i.e., not just attachments
- Message details including sender and recipient information
- Native MIME/MAPI content scanning
- Proactive scanning
- Priority-based queuing
- Multi-threaded queue processing
- Per-messaging database configuration options
- Enhanced background scanning
- Event logging
- Virus scanning API-specific performance monitor counters

Note: McAfee Security and Microsoft use different terms to describe scanning that takes place when an item is being requested by a user or process. McAfee refers to this real-time scanning as “on-access;” whereas Microsoft uses the term “on-demand.” To maintain consistency with other McAfee Security materials, this document will use the McAfee Security convention.

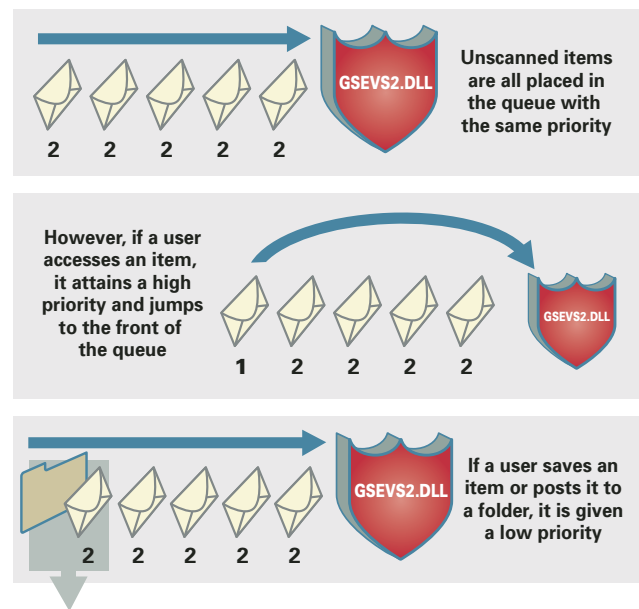
API 2.0 On-Access Scanning (a.k.a. Microsoft On-Demand Scanning)

As in virus scanning API 1.0, virus scanning API 2.0 continues to support on-access scanning. As clients attempt to gain access to Exchange items, either by using an Internet protocol-based client such as Post Office Protocol version 3 (POP3), Outlook Web Access (OWA), Internet Message Access Protocol, Version 4rev1 (IMAP4), or by using a conventional Messaging Application Programming Interface (MAPI) client, a comparison is made to ensure that the message body and attachment (if present) have been scanned by the current virus signature file. If the content has not been scanned by the current vendor or signature file, the corresponding item is submitted to GroupShield for scanning before that item is released to the client.



In virus scanning API 2.0, a single queue processes all of the message body and attachment data. Items that are submitted to this queue as “on-demand” (Microsoft terminology) are submitted as high-priority items. This queue is now serviced by a series of threads (the default number of threads is: two times the number of processors plus one), with high-priority items always taking precedence. This allows multiple items to be submitted to GroupShield simultaneously. In addition, client threads are no longer tied to “time-out” values that are waiting for items to be released. After items are scanned and marked as safe, the client thread is notified that the item is available. By default, the client thread waits up to three minutes for notification of the availability of the requested data before a time-out occurs.

Global Scanning Queue

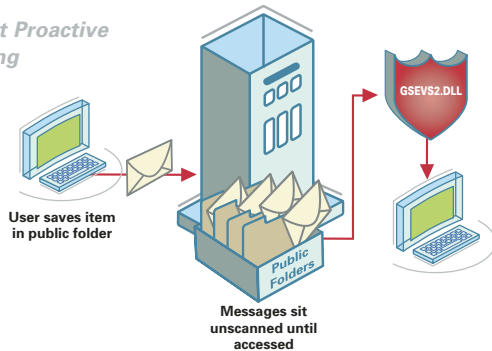


API 2.0 Proactive Scanning

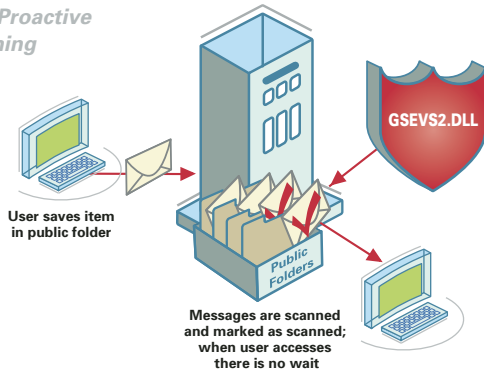
A new feature in virus scanning API 2.0 is proactive-based scanning of messages. In virus scanning API 1.0, message attachment information was only scanned as it was accessed. In virus scanning API 2.0, items are submitted to a common information store queue as they are submitted to the information store. Each of these items receives a low priority in the queue, so that these items do not interfere

with the scanning of the high-priority items. When all of the high-priority items have been scanned, virus scanning API 2.0 begins to scan low-priority items. The priority of the items is dynamically upgraded to high priority if a client attempts to access the item while the item is in the low-priority queue. A maximum of thirty items can exist at one time in the low-priority queue, which is determined on a first in, first out basis.

Without Proactive Scanning



With Proactive Scanning

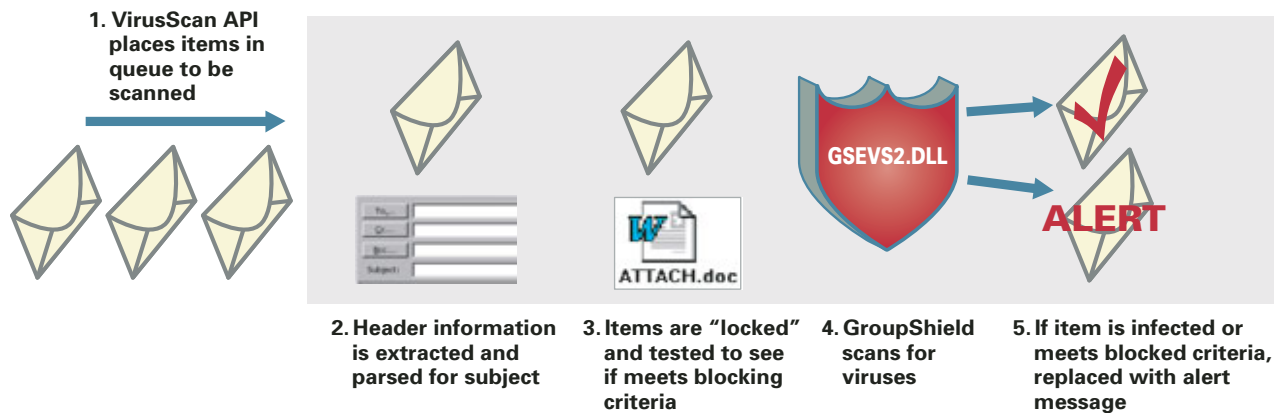


API 2.0 Background Scanning

Background scanning navigates the series of folders that comprise each user’s mailbox and public stores, and as items that have not been scanned by the current virus signature file are encountered, they are submitted to GroupShield. Each Messaging Database (MDB) receives one thread to conduct the background scanning process, and after the thread completes a pass of all the contents, the thread waits for a restart of the information store process before conducting another pass. A background scan can also be initiated by GroupShield after an Engine or DAT update.

How GroupShield Works with the Microsoft Virus Scanning API 2.0

As items are written and read from the Microsoft Exchange stores, the virus scanning API passes them to GroupShield for scanning prior to routing. After scanning, the item is either delivered, cleaned, or quarantined as required, and the results are noted in the information stores.



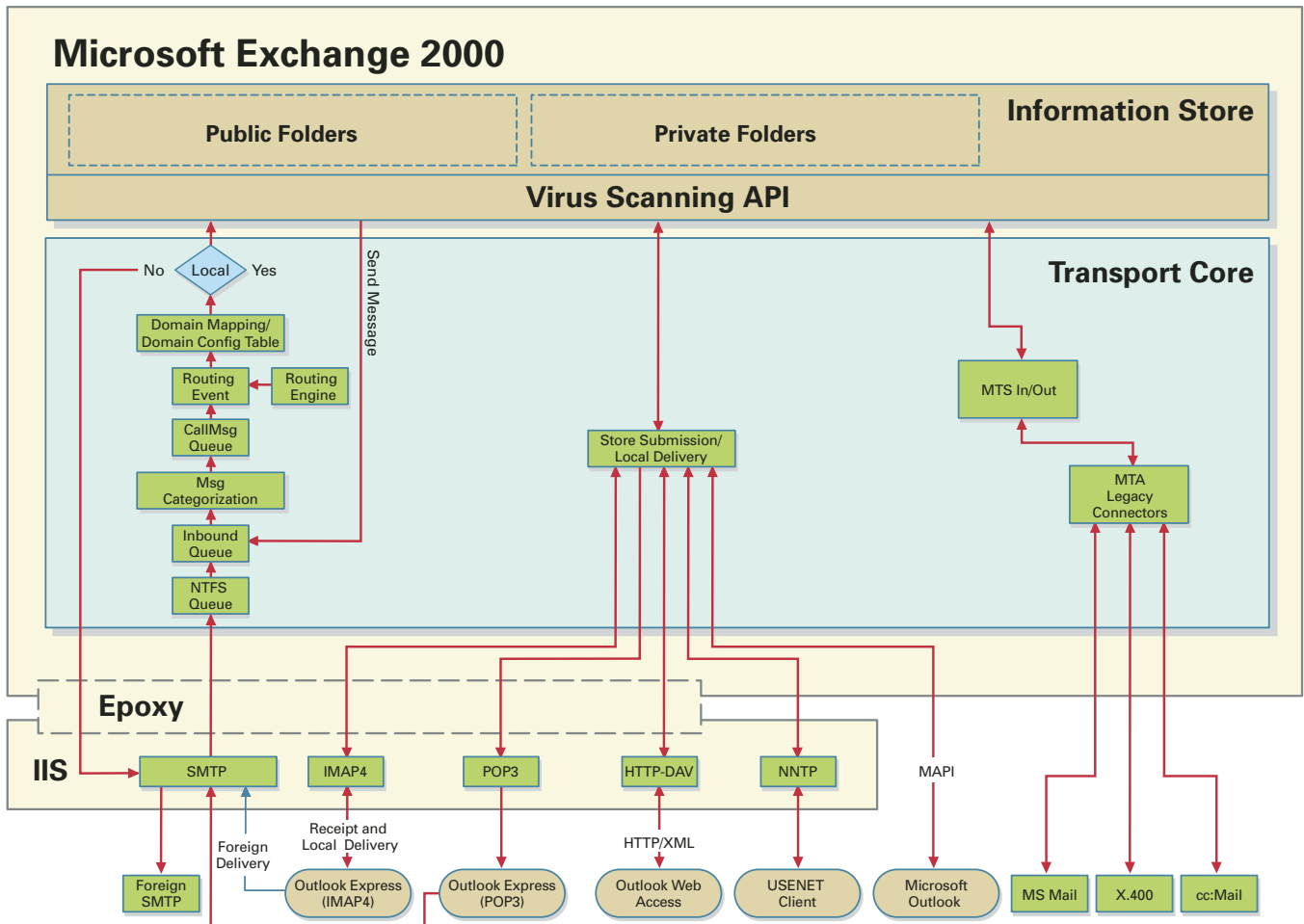
Exchange 2000 Message Routing and the Virus Scanning API 2.0

Below is a diagram that illustrates how messages are routed through Microsoft Exchange 2000 from various e-mail clients and external sources. From this diagram, it can be seen that all messages are routed through the Microsoft Exchange virus scanning API, with the exception of *external SMTP traffic*.

So long as SMTP messages are being delivered to or sent from the local Exchange 2000 server, they will be scanned. However, SMTP messages sent from a POP3 client or from another server to a non-local recipient will not be scanned. Customers with multiple Exchange servers should, for best-practice reasons, use GroupShield on each server. If they are using POP3 clients, they should ensure that VirusScan® is used to provide scanning of outbound messages from those users.

Benefits of Using GroupShield with the Microsoft Virus Scanning API 2.0

- Ensures that all Microsoft Exchange items (messages, attachments, files, etc.) are thoroughly scanned before being delivered to internal users or sent to external recipients
- Single-instance scanning of items, even if one e-mail is sent to multiple recipients
- GroupShield for Microsoft Exchange 2000 can be administrated to provide realtime protection to Exchange 2000 servers without requiring the Exchange services to be stopped and restarted
- Scans all protocols passing to and from the Exchange 2000 server, including: SMTP, MAPI, HTTP, POP3, IMAP4, Installable File System (IFS), X.400, etc.
- Provides the highest level of scanning performance with lowest possible server resource utilization



- Uses the Microsoft approved and preferred method of scanning Exchange stores to provide the best possible scanning while ensuring compliance with other Microsoft APIs, integrity of data, and stability of the Exchange services

Microsoft Exchange 2000 and Transport Scanning

On Exchange 2000, Transport Scanning offers the following functionality that is not available in the VSAPI for Microsoft Exchange 2000:

- (a) Scanning of routed mail (i.e., mail not destined for local server)
- (b) Stopping delivery of messages

An administrator should enable transport if they require the above action. For example, administrators prevent spam by scanning on a bridgehead or gateway-designated server.

Note: *Transport Scanning supports quarantining and message modification (item replacement and cleaning) for MIME messages only.*

Messages are presented as MIME in the following situations:

- (1) They are sent using a non-MAPI client (i.e., not Outlook or Outlook Web Access) from a mailbox on the local server
- (2) They are arriving from outside the organization
- (3) They are about to leave the organization

Options (2) and (3) make Transport Scanning a more appealing option on gateway servers where most, if not all, e-mail will be MIME.

Microsoft Exchange 2000 and Anti-Spam

Microsoft Exchange 2000 does not provide specific anti-spam APIs for third-party solutions to integrate. McAfee GroupShield 6.0 for Microsoft Exchange with McAfee SpamKiller® for Microsoft Exchange add-on and McAfee SpamKiller for Microsoft Exchange detect spam by scanning at the SMTP Transport level. Transport scanning can perform scanning of routed mail—e-mail messages that are not destined for the local server and can stop the delivery of messages.

Microsoft Exchange 2003 and Virus Scanning API 2.5

Microsoft Exchange 2003 includes the new Virus Scanning API 2.5. Building on the Virus Scanning API 2.0, the Virus Scanning API 2.5 includes the following improvements:

- Stopping at the point of entry—VSAPI 2.5 enables GroupShield software to scan e-mail messages as it enters a corporate network, helping to prevent malicious content from reaching the Exchange mailbox servers
- Stopping at the point of exit—All outgoing messages can also be scanned, and infected mails can be prevented from leaving the network
- Allows GroupShield to run on Exchange 2003 servers that do not have resident Exchange mailboxes such as bridgehead servers or gateway servers
- Allows GroupShield to delete messages and send messages to the sender, and additional virus status messages allow clients to better indicate the infection status of a particular message

Virus Scanning API 2.0 and Virus Scanning API 2.5 processes all the message body and attachment data by using a single queue explained earlier in the document. Realtime or on-access (Microsoft-named on-demand) items that are submitted to this queue are marked as high-priority. In Exchange 2003, this queue is now serviced by a series of threads, and high-priority items always take precedence. The default number of threads is two times the number of processors plus one. This makes it possible for multiple items to be submitted to the anti-virus vendor product at the same time. Also, client threads are not tied to time-out values that are waiting for items to be released. After items are scanned and marked safe, the client thread is notified that the item is available. By default, the client thread waits up to three minutes to be notified of the availability of the requested data before a time-out occurs.

Microsoft Exchange 2003 and Anti-Spam

Microsoft provides three levels of anti-spam capabilities primarily focused on connection-based filtering rather than content-based filtering, the following levels are included as part of Microsoft Exchange 2003:

- Allow/Deny List Realtime Blocklist
- Recipient and Send Filter

In addition Microsoft offers Internet Message Filtering (IMF), available with SA support from Microsoft.

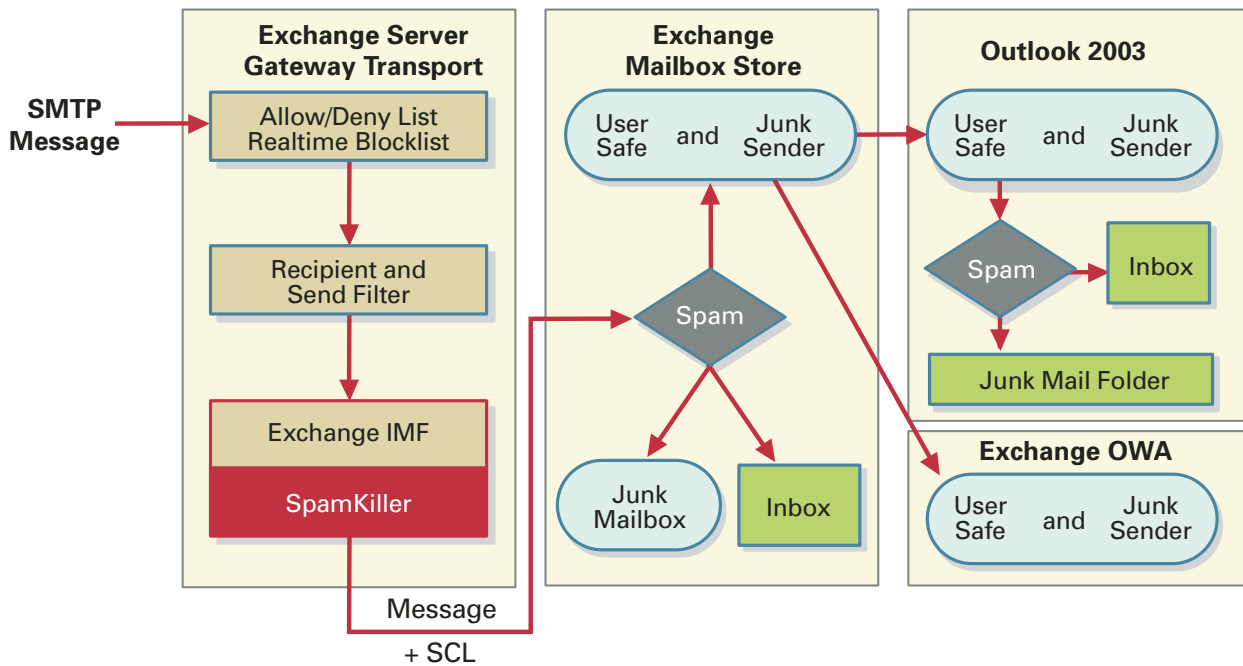
Microsoft's Internet Message Filter (IMF) is based on Microsoft's Smart Screen technology from MSN Hotmail. The Smart Screen technology implemented in IMF from mid-2004 requires regular updates from Microsoft which is updated at about one month to six-week intervals. Administrators are

required to download update files from Microsoft to keep IMF up-to-date. Microsoft's IMF does not offer a complete solution but it does complement ISV solutions such as SpamKiller for Microsoft Exchange.

Microsoft scores all messages with a Spam Confidence Level (SCL) that allow the administrator or users to tailor the level of spam they wish to receive. In conjunction with Exchange 2003 GroupShield with McAfee SpamKiller add-on or McAfee SpamKiller, software scans each incoming message and attaches a numeric score, called the Spam

Confidence Level (SCL), to each message. Based on a threshold set by an administrator, the message will be delivered either to the recipient's inbox or to the junk mail folder.

Note: The anti-spam infrastructure available in Microsoft Exchange 2003 uses a different scoring system from McAfee SpamKiller, however, McAfee SpamKiller translates the scores so that they correlate to each other.



McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054, 888.VIRUSNO (888.847.8766)

Network Associates® products denote years of experience and commitment to customer satisfaction. The 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, continues to spearhead innovation in the development and refinement of all our technologies.

Network Associates, McAfee, GroupShield, VirusScan, SpamKiller, and PrimeSupport are registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. Red in connection with security is distinctive of McAfee®. All other registered and unregistered trademarks herein are the sole property of their respective owners. © 2004 Networks Associates Technology, Inc. All Rights Reserved. 6-sps-gse-001-0504