SPAMfighter Exchange Module

For Microsoft Exchange Server 2000 and 2003.

White Paper

July 2004.

Table of content

Abstract

SPAMfighter Exchange Module is build for Microsoft Exchange 2000 and 2003 running on Microsoft Windows Server 2000 or 2003 operating systems protecting end users from SPAM.

SPAMfighter is a Danish company owned by the founders of Jubii (Now owned by Lycos Europe), Denmark's largest Internet Portal.
Every day SPAMfighter removes 2.5 million spam mails from 4 million screened emails, received by +400.000 users from 160 countries.

SPAMfighter Exchange Module

Introduction

SPAMfighter Exchange Module seamlessly integrates with Microsoft Exchange Server and that makes the solution very fast and stabile. As email arrives and the Exchange Server routes it to its addressees, SEM makes a unique signature for each message and sends it to the SPAMfighter Server for evaluation. If the SPAMfighter Server determines that a message is spam, it notifies SEM and the spam mail is moved to the users spam folder.

SPAMfighter Exchange Module also offers reporting, so administrators can review statistics on how many messages SEM is filtering, how many users are enabled, how much time is saved and more.
In addition, SEM is simple to use for end users, as spam is automatically moved to the Spam folder. While SEM simplifies administration and keeps software and configuration off the employee's desktop, it also provides individual control for end users if the administrators decide they want it.

Intended audience

This document is intended for the technical staff or system administrators.

Reference material

Following is a list of reference material that supplements this white paper.
- Visit http://www.microsoft.com for more information about Microsoft Server family and Microsoft Active Directory.
- Visit http://www.microsoft.com for more information about Microsoft Exchange Server.

- Visit http://www.microsoft.com for more information about Microsoft .NET Framework 1.1.

Contact your SPAMfighter sales agent to obtain further information on these or related documents.

Top 10 network administrator questions

Installing 3rd party software to process the network mail messages can be a fatal decision for a network administrator. During a product validation, there are some natural questions witch needs to be answered.

Q: **Network security**. What impact to my network security does SPAMfighter have?
A: *SEM needs access to the internet, but SEM limits the connection to TCP/2409 and UDP/2409 for backend.spamfighter.com and TCP/80 to ks.spamfighter.com. This allows the network administrator to secure network traffic by disabling all other connection than the ones listed.*

Q: **Data security.** What will SEM send to SPAMfighter and what will SEM receive from the outside?
A: *SEM sends installation details at registration, logon information when running, debug information when failing and email compiled hash values when testing mails.*
SEM never sends information sensitive to the network. Also all information sent and received is validated to avoid tampering.

Q: **Installation.** What happens if the installation fails?
A: *If the SEM installation fails, no interaction with the Exchange Server has been made, hence it has no impact on your configuration.*

Q: **Runtime.** What happens if the application fails?
A: *Since SEM utilizes the Exchange Server interface, no mails are deleted but only moved. If SEM should unexpectedly fail during parsing, processing or redirecting a mail item, the transaction is rolled back and the system is intact.*

Q: **Data security.** How is a mail determined to be spam?
A: *SEM creates a unique irreversible signature of the mail and containing elements and sends the signatures to the SPAMfighter server for processing. The server then returns a score, determining if the message is spam or not. The original mail message never leaves the server during SEM filtering.*

Q: **Data security.** When a message is determined as spam what happens?

A: *If a message is determined as spam, SEM moves the message to a folder named SPAMfighter in the user's mailbox. If the folder does not exist, it will be created. The move process is transactional and will rollback if it fails.*

Q: **Management.** Can you disable filtering on a single mailbox?
A: *Yes using the administration interface, it's possible to disable spam filtering on a single mailbox.*

Q: **Security.** SEM requires IIS as a part of the installation, can this be disabled?
A: *Yes. SEM only uses IIS for the administration interface. The IIS can be disabled when configuration has ended. Likewise the IIS can be enabled if further configuration is needed.*

Q: **Coexistence.** Can SEM work with Antivirus software installed on the Exchange Server?
A: *Yes. SEM works with most common antivirus software. Since SEM is integrated in the Exchange server, it doesn't impact the functionality of antivirus software.*

Q: **Trust.** Is SPAMfighter certified in Microsoft Software?
A: *SPAMfighter is a Microsoft Partner, having the SPAMfighter Pro client certified for the "Designed for Microsoft Windows 98, ME, NT, 2000, XP" logo. SEM is approved for VeriTest®, "Designed for Microsoft Windows 2003 Server" and ".NET Connect" logo certifications.*

Installation

Requirements

SPAMfighter Exchange Module is intended for Microsoft Exchange servers running on a Windows Server family operating system. For more information on Microsoft Exchange installation, visit Microsoft Exchange Server website for requirements and installation instructions.

SEM uses .NET Framework described by Microsoft as:

"The Microsoft® .NET Framework is an important new component of the Microsoft Windows® family of operating systems. It is the foundation of the next generation of Windows-based applications that are easier to build, deploy, and integrate with other networked systems."

Listed below are the minimum and recommended system requirements.

Minimum:

CPU	Intel Pentium or compatible 166-megahertz (MHz) or higher processor.
Memory	256 megabytes.
Hard Disk	500 megabytes on Exchange installation 200 megabytes on system drive 5 megabytes for SEM installation
Operating system	Windows 2000 Server + IIS. Make sure the latest service packs are installed.
Exchange Server	Exchange Server 2000. Make sure the latest service packs are installed.
LDAP	Windows 2000 Active Directory
.NET Framework	.NET Framework 1.1
Data Access	Microsoft Data Access Components 2.6

Recommended:

CPU	Intel Pentium or compatible 1000-megahertz (MHz) or higher processor
Memory	512 megabytes.
Hard Disk	500 megabytes on Exchange installation 200 megabytes on system drive 5 megabytes for SEM installation
Operating system	Windows 2003 Server + IIS. Make sure the latest service packs are installed.
Exchange Server	Exchange Server 2003. Make sure the latest service packs are installed.
LDAP	Windows 2003 Active Directory
.NET Framework	.NET Framework 1.1
Data Access	Microsoft Data Access Components 2.6

Before installation

When you have your Exchange server up and running, there are a few details that need to be checked before installing SPAMfighter Exchange Module.

Connectivity

Ensure the Exchange server has access to the internet. If you use a firewall and/or proxy service within your network, please verify the following requirements are available:

Traffic protocol	Local port	Endpoint port	Endpoint	Direction
UDP	Dynamic	2409	backend.spamfighter.com	Both
TCP	Dynamic	80	sem.licensing.spamfighter.com	Both
TCP	Dynamic	80	sem.errors.spamfighter.com	Both

If just one of the listed ports isn't available SEM will not work properly.

Service account

In order for SEM to receive notifications from the Exchange server, it needs special user rights. Creating a special account with the sole purpose to act as service account for SEM, limits security problems when this account is assigned the required rights.

Please note, the service account must not have the option "Must change password at next login" enabled. If so the installation will fail.

Installation

Download

The first task is to download the latest version of SPAMfighter Exchange Module. Visit the homepage for instructions to download the latest version.

http://www.spamfighter.com/SEM_Installing.asp

Install

Executing the SEM setup will bring up a well known Installshield interface. Follow the on screen instructions to install SEM.

Register

When the installation is almost done, the installation will bring up a custom SPAMfighter installation dialog.
In order to complete the installation, you need to register your copy of SEM and enter company and contact information.

Completing

After registering your SEM copy, the setup dialog will install various components and prepare the installation for first use. When finished, the installation is complete.

Management

SEM provides an intuitive web interface for managing the installation. The installation process will setup a website on the local IIS named fiSPAMfighter Administrationfl.

The management interface can be accessed by navigating to the SPAMfighter program group in the Windows Start Menu. Here you will find a link to fiSPAMfighter Administrationfl. The interface can also be accessed by typing http://localhost:2404 in the Internet Explorer address bar .

When entering a password, dialog appears. The default password is set to fipasswordfl and can be changed after login.

FrontPage

The fiFront-pagefl list installation details that is important if you want to upgrade or get In touch with SPAMfighter customer support.

Mailboxes

The fiMailboxes pagefl allows you to enable or disable filtering on individual mailboxes. When SEM is combined with the SPAMfighter Pro client, you can also show or hide the SPAMfighter toolbar for specific user.

Filters

Using the "Filters page" you can configure SEM filters. This includes the SEM Sender Filter where sender addresses can be black or white-listed based on the sender email or domain.

Product Keys

The "Product keys page", enables you to manage and view the SEM license. Here you can also add new product keys when needed.
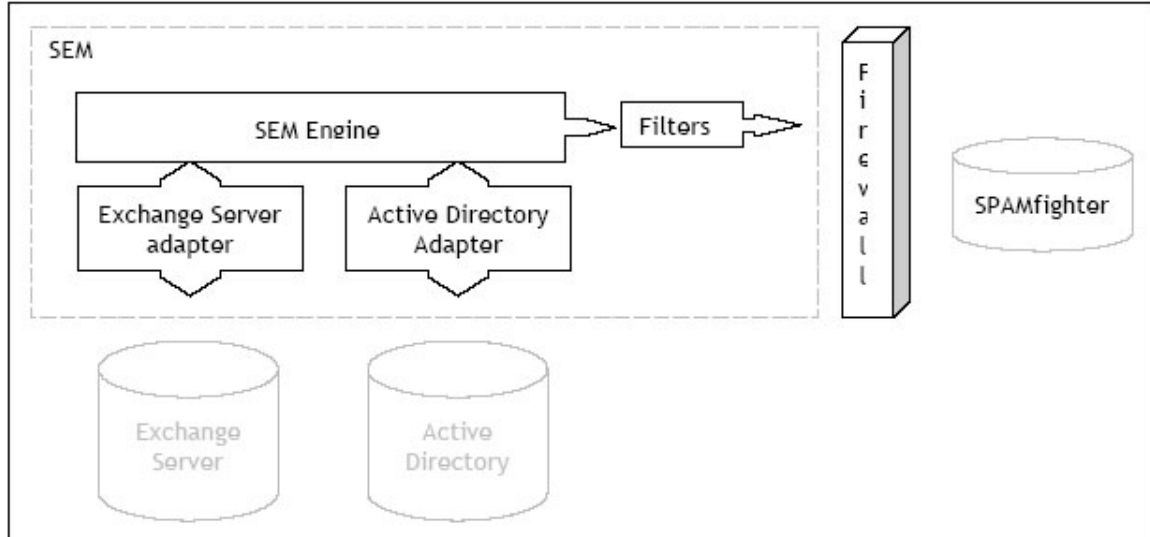
Administration

The "Administration page" allows you to change the SEM administration interface password.

SEM Components

SEM consists of four major components: Exchange Server adapter, Active Directory adapter, SEM engine and filter modules.
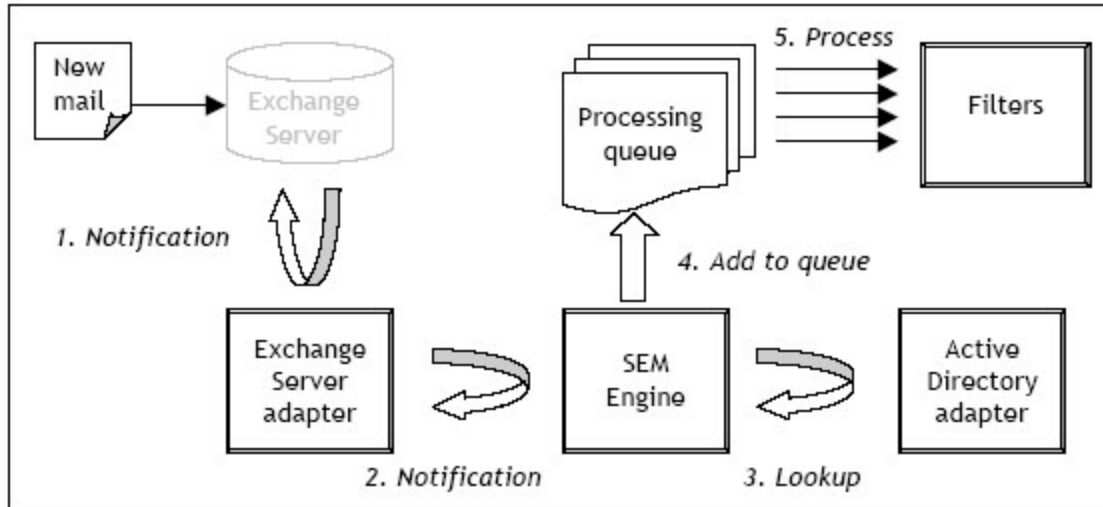
The diagram below illustrates the relation between these components.

New message processing

During the processing of new mail items, all the SEM components are activated to filter the message.

The diagram below illustrates the processing of new mails.

When a new mail arrives on the Exchange Server, the server notifies (1) SEM Exchange Server adapter about the new mail. The SEM engine is notified (2) by the Exchange Server adapter that looks up (3) the recipient by using the Active Directory adapter. If the recipient is filter enabled, the Engine ads the message to a processing queue (4) for further processing. The processing queue process (5) each mail item through the SEM filters, and determines if the message is spam or not.

If a mail item is determined to be spam, the SEM Engine notifies the Exchange Server adapter to move the mail item to the users SPAMfighter folder.