Chapter 7: Configuring ScanMail eManager

Chapter Objectives

After completing this chapter, you should be able to achieve the following objectives:

- Describe the default policy conventions used in the ScanMail eManager
- Configure ScanMail eManager to filter out spam
- Configure ScanMail eManager to filter content

Enabling ScanMail eManager

Before you can create policies and configure the spam filter and the content filter, you must enable ScanMail eManager. Open the ScanMail Management Console and click **Virus Scan** and then **Options**. Then select **Enable eManager** (see Figure 7-1).

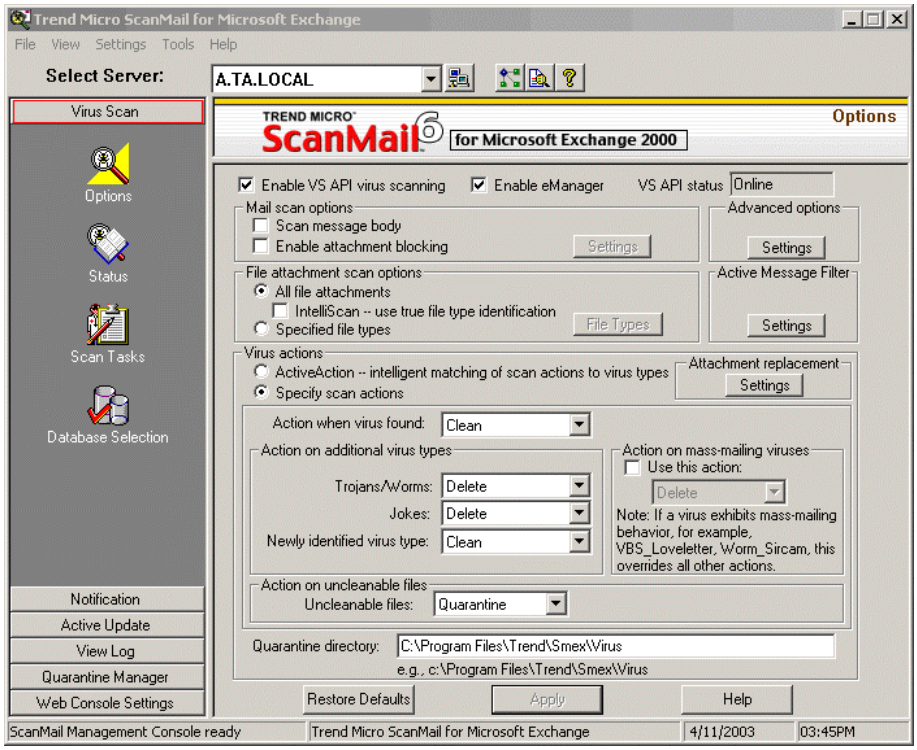

Figure 7-1: Scanning Options screen

You can use the Real-Time Scan Monitor to ensure that ScanMail eManager is loaded and is scanning messages. The *Messages Scanned* section should show that ScanMail eManager is loaded (see Figure 7-2).

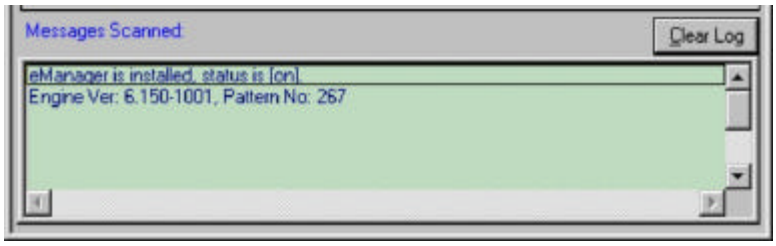

Figure 7-2: Checking to see if ScanMail eManager is loaded

You can also open the Windows NT Task Manager and ensure that the ***Cm_smex.exe*** process is loaded.

Default Policy Conventions

The spam and content filters in ScanMail eManager follow a set of predefined, default conventions. Exceptions to these conventions are noted later in the chapter.

Case Sensitivity

Keyword comparisons are *not* case sensitive. For example, "Free Offer," "Free offer," and "free Offer" are considered matches for "free offer." To specify a case-sensitive comparison, select the **Case-Sensitive Comparison** check box next to the desired field.

Exact Matches

Keywords can match whole or partial words. For example, if "free" is the keyword, an occurrence of "freezer" would register a match. To eliminate partial-word matches, select the **Exact Match** check box next to the desired field.

> ✔ ***Note:*** *Accepting partial-word matches can increase the number of false positives, or legitimate email that eManager blocks.*

Delimiters

Use commas to delimit multiple keywords entered in a single field. If you enter a phrase, it is treated as a single unit.

The comma functions as the AND operator. Messages must contain all of the keywords to register a match. For example, you could enter the following keywords:

```
free offer, music, movie
```

In this case, only messages that contain all keywords are considered a match. The keywords can appear in any order in the message.

Keywords that appear on different lines are implicitly connected by the OR operator. The text can contain any of the words from the various lines. For example, you could enter the following keywords:

```
free offer
music
movie
```

In this case, messages that contain the words *free offer* are a match, messages that contain the word *music* are a match, and messages that contain the word *movie* are a match.

When synonym checking is engaged, a combination of the two operators is applied. For more information, see the "Synonym Checking" section in this chapter.

Wildcards and Punctuation

The eManager **spam filter** supports the asterisk (*) as a wildcard character. You can configure rules that include this wildcard character for the message header fields.

The eManager **content filter** *does not* support wildcard characters such as the asterisk (*) and question mark (?). If you include quotation marks, spaces, and punctuation marks in a content rule, these characters are taken literally. A match is registered only when each word, space, comma, or other punctuation mark in the phrase is found in the message. For example, if you use quotation marks to signify a phrase, the filter will match only those phrases that include quotation marks as entered in the search criteria.

Archive, Delete, Quarantine

eManager can take following actions on messages that match filtering criteria:

Archive	Messages are forwarded to the intended recipient but are also renamed and moved to the archive directory.
Delete	Messages are erased from the system and are not recoverable.
Quarantine	Messages are moved to the quarantine directory.

Spam Filtering

The spam filter uses the header information (including *From:, To:, cc:,* and *Subject:* lines) to evaluate messages. To filter spam, you must create rules using information such as the routing domain that identifies the origin of the spam. You can create an unlimited number of your own anti-spam rules.

Trend Micro provides a rule file that contains hundreds of predefined, anti-spam rule sets. These rules block unsolicited and unwanted email that originates from a number of known spam senders. The rules also block email that contains popular spam subjects. The vendor-provided rule file is typically used in conjunction with the customized list of rules you develop to address specific occurrences of spam.

> ✔ ***Note:*** *Binary attachments encoded using MIME, Unicode, or other encoding schemes are not evaluated. Non-encoded text and Word attachments are included in the evaluation.*

When creating spam rules, you should remember that many spam senders add false header information to their messages to make tracking back to the source difficult. The most prolific bulk emailers will often reuse the same false routing domains and other header information. This makes it easier to create anti-spam rules. You can use these false domains as a signature to identify and safely block entire classes of spam rather than create rules on a one-rule/one-spam basis.

Spam Filter Options

When configuring spam filters, you have the following options:

- View and reorder the list of anti-spam rules
- Add, edit, or delete a rule
- Activate the vendor-provided rule file
- Configure notification messages

To configure these options, click Windows **Start** | **Programs** | **Trend Micro ScanMail for Microsoft Exchange** | **Trend Micro ScanMail eManager** | **ScanMail eManager Configuration**. Click the **Anti-Spam** tab to access the *Anti-Spam Configuration* screen (see Figure 7-3):

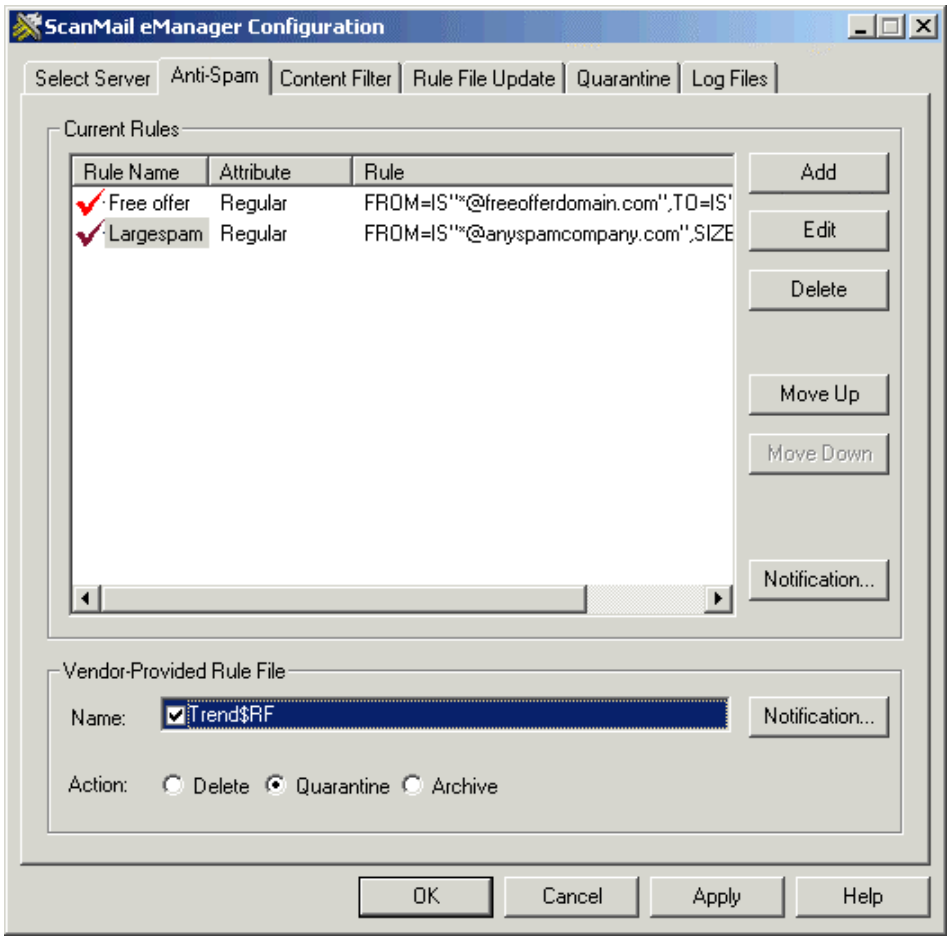

Figure 7-3: Anti-Spam configuration screen

Viewing and Reordering Anti-Spam Rules

The *Current Rules* table on the *Anti-Spam* configuration screen displays a list of customized rules against which inbound and outbound messages are evaluated. ScanMail evaluates Exchange traffic against the rules, starting from the first rule on the list and proceeding down the list in order to the last rule. There is no limit to the number of rules that can be created.

If a message matches the criteria specified in a rule, ScanMail eManager performs the action specified within that rule (such as quarantine, archive, or delete) and notifies the appropriate people, such as the administrator. ScanMail eManager does not perform any more scanning on the message.

You can configure the order in which rules are listed. You should evaluate your Exchange environment before you determine the order of rules. For example, if your company is receiving a large number of messages from a particular spam sender, you may want to list the rule for this spam first.

Adding, Editing, and Deleting Rules

To add a user-defined rule, click **Add** in the *Current Rules* section on the *Anti-Spam* configuration screen. To edit an existing user-defined rule, highlight the rule you want to edit, and click **Edit** in the *Current Rules* section on the *Anti-Spam* configuration screen. To delete a rule, highlight the rule and click **Delete**.

When you click **Add** or **Edit**, the *Add/Edit Rule* screen appears (see Figure 7-4). Use this screen to specify the criteria by which email is evaluated. Each *Add/Edit* page represents a separate rule.

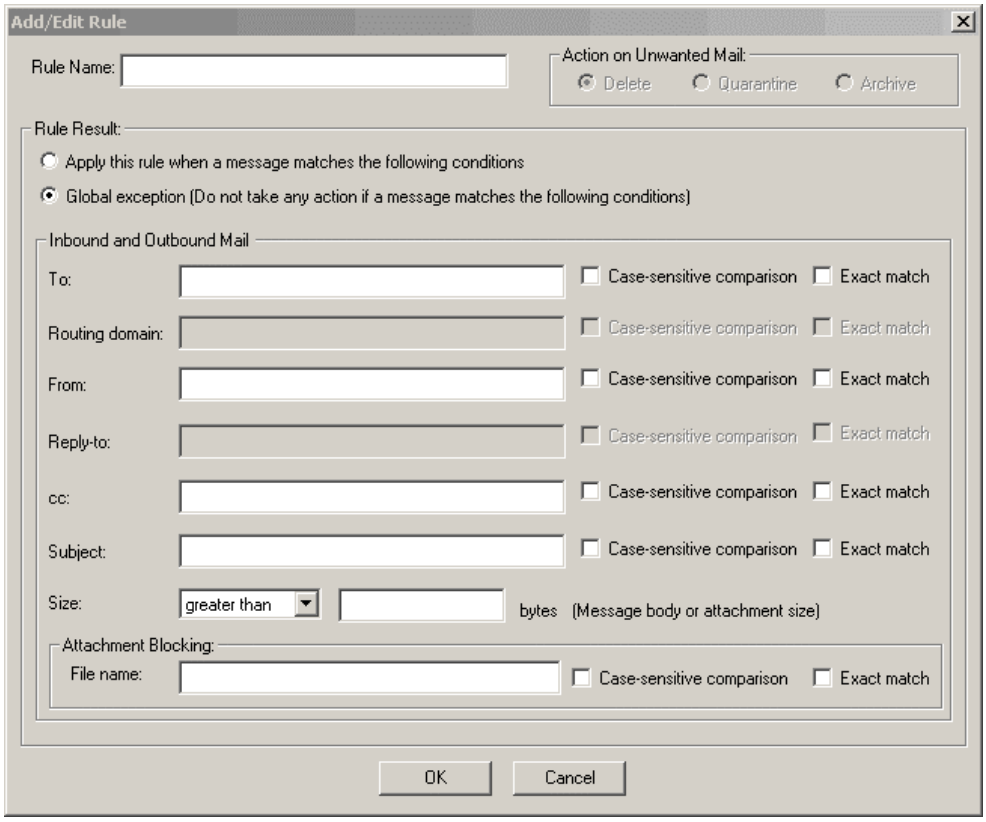

Figure 7-4: Add/Edit Rule configuration screen

You can configure the following for each rule:

Rule Name

Use the *Rule Name* field to create meaningful, descriptive names for the rules you create.

Action on Unwanted Mail

Messages that are found to match the filter rules can be deleted, quarantined, or archived. Messages that are deleted or quarantined are not passed to ScanMail for Exchange for virus scanning. However, messages that are copied to the archive directory are passed to ScanMail for Exchange for virus checking. All of these actions are recorded in the log file.

Trend Micro recommends that you archive messages for the first few weeks after you create or modify your spam filter rules. You can then check your messages to evaluate how effective your rule is.

Rule Result

You can apply the designated action to all messages that match the rule by selecting **Apply this rule when a message matches the following conditions** option. Alternately, you can set the rule as a global exception by selecting **Global exception (Do not take any action if a message matches the following conditions)** option. The Global exception option tells the system to take no action if a message matches the conditions listed.

By default, rules are regular, which means that the rule is applied to any email message that satisfies the specific conditions of the rule.

Global exception rules are applied regardless of any other rules you have configured. For example, if a message matches the global exception conditions, that message is not checked against any other rules. The message is then passed on to ScanMail for Exchange for virus scanning.

Address, Sender, Copies, and Subject Fields

You can configure the spam filter to filter email based on information contained in any of the following fields:

```
To:, From:, cc:, Subject:
```

Blind carbon copies (that is, email addresses appearing in the bcc: field) are not included in the header information and cannot be used as a basis for filtering spam.

> ✔ ***Note:*** *Rules for the message header fields support the asterisk (*) as a wildcard character in the To:, From:, cc:, and Subject: fields.*

Message or Attachment Size

Messages can be filtered according to the size of the message body or the attachment. Using the following conditions, you can filter messages according to the size in bytes:

- Greater than
- Less than
- Equal to
- Not equal to

For example, you can block the body of the message or the attachment if it is greater than 100,000 bytes. To do so, select the condition (greater than) and type the number of bytes (100,000) in the Bytes field.

Attachment Blocking

File-attachment blocking is usually enabled during virus outbreak conditions to temporarily block all attachments that have a particular file name. To use this option, type the attachment file name in the *File Name* field in the *Attachment Blocking* section.

✔ ***Note:*** *You can use the asterisk (*) as a wildcard in the file name.*

You can specify only one attachment file name per rule. You have the option of performing a case-sensitive comparison or an exact match comparison, but Trend Micro recommends that you not select either of these options unless it is absolutely necessary. Spam messages often use the same file name as a previous spam with a few characters added. For example, "TROJ_MTX" in the *File Name* field without exact match enabled would catch files such as the following:

```
TROJ_MTX_II.DLL, TROJ_MTX_IlI.DLL, TROJ_MTX_II2.DLL, etc.
```

Activating Vendor-Provided Rule File

To use the vendor-provided rule file in the analysis of inbound and outbound mail, select the rule-file check box. Rules in the rule file do not appear in the *Current Rules* table.

The vendor-provided rule file, which is encrypted, is stored in the ***\Program Files\Trend\SMCF\spamrule*** directory. The file is named ***Trend$RF.###***, where ### represents the version number of the file.

This file cannot be edited. This rule file is provided by Trend Micro and can be updated automatically.

Configuring Notification Messages

You can configure separate notifications for user-defined rules and the vendor-provided rules. To configure a notification, click the **Notification** button in the section corresponding to the type of rule on the Anti-Spam configuration screen. The *Anti-Spam Notification* dialog box appears (see Figure 7-5).

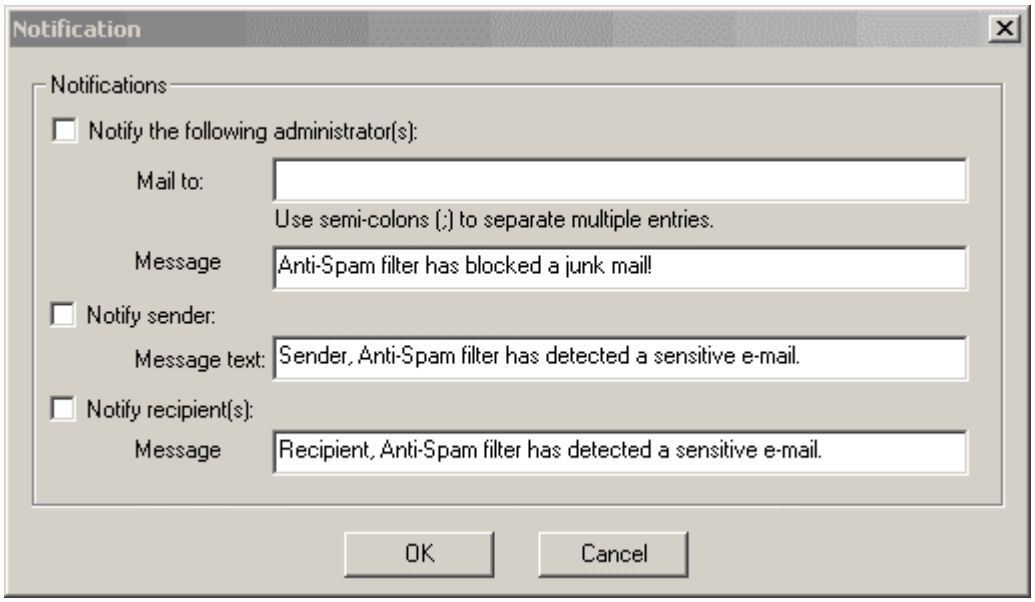

Figure 7-5: Anti-Spam notification

Current Rules Notification

To set notifications for user-defined rules, click **Notification** in the *Current Rules* section and then select any or all of the following:

- Notify the following administrator(s) — To notify administrators, check this option and enter the email addresses of the administrators in the **Mail to:** field. Multiple email addresses should be delimited with semicolons. Enter the message text to send in the *Message* field. For example, you might enter the following:

  ```
  ScanMail eManager spam filter blocked an email.
  ```

- Notify sender — To notify the sender, check this option and enter the message text to send.
- Notify recipient(s) — To notify the recipients, check this option and enter the message text to send.

Vendor-Provided Rule File Notification

To create a notification message to be sent when one of the vendor rules is met, click the **Notification** button in the *Vendor-Provided Rule File* section. Configure the vendor-rule notifications as described in the *Current Rules Notification* section.

✔ ***Note:*** *For the spam filter, only the email header information is compared against the rules defined in the Add/Edit page. Identical information appearing in the message text of a forwarded message will not register a match. To evaluate message text, you should use the content filter.*

Content Filtering

A content-filter policy represents a group of conceptually related words and phrases that will be matched against inbound and outbound messages. ScanMail eManager evaluates the content of the message text, the To field, and the From field against the list of policies. Whenever any policy is found to match the contents of a given email, the action specified in the matching policy is taken. The message can be archived, quarantined, or deleted.

There is no limit to the number or type of content policies that can be created, and policies can be individually enabled or disabled. The content filter also provides a synonym-checking feature, which allows you to extend the reach of your policies.

You can, for example, create policies to check for the following:

- Spam
- Profanity
- Racist language
- Sexually harassing language
- Hoaxes
- Chain mail
- Viruses
- HTML script

Content Filter Options

When configuring content filters, you have the following options (see Figure 7-6):

- View a list of policies
- View summary information for each policy

- Add, edit, or delete a policy
  - Specify which actions to take when a message matches a rule
  - Specify keywords to filter
  - Configure notification messages
- Use the keyword lists that Trend Micro provides
- Configure global policy settings

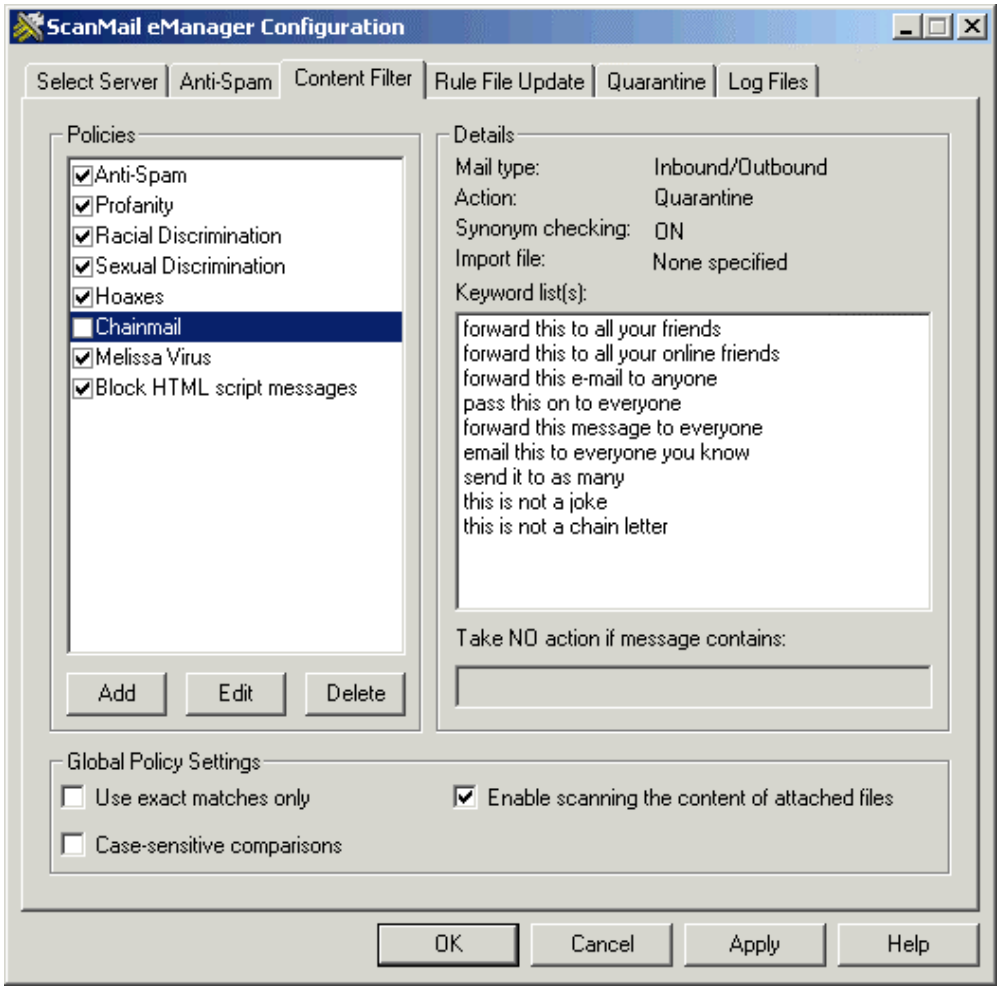

Figure 7-6: Content Filter configuration screen

To configure these options, click the **Content Filter** tab in the *ScanMail eManager Configuration* screen (see Figure 7-6):

Viewing a List of Policies

The Policies list displays the individual rules by which inbound and outbound messages are evaluated. ScanMail eManager evaluates the contents of the message text in addition to the header data. The evaluation of mail traffic against the policies starts from the first, or top, rule and proceeds down the list to the last, or bottom, rule. You should order policies with the broadest reach at the top of the list and those that are more narrowly defined at the bottom.

Viewing a Policy Summary

The *Details* section on the *Content Filter* screen provides a detailed summary of the highlighted policy. The summary shows data from the *Add/Edit Policy* screen and offers more information on the makeup of a given policy.

To change the values that appear in the *Details* section, click the **Edit** button below the Policies list to access the *Add/Edit Policy* screen. Make your edits, and then click **OK**. (See *Add/Edit Policy Options* for more information.)

Available fields are listed below:

Mail type	Inbound, outbound, or both
Action	Delete, quarantine, or archive
Synonym checking	On or off
Import file	None specified or the file name
Keyword list(s)	Keywords that have been configured to match content
Take NO action if message contains	Text that, if found in the message, prevents the above-named action from being taken

Adding, Editing, and Deleting Policies

To add a policy, click **Add** in the *Policies* section on the *Content Filter* screen. To edit an existing user-defined rule, highlight the policy you want to edit, and click **Edit**. To delete a rule, highlight the policy and click **Delete**.

When you click **Add** or **Edit**, the *Add/Edit Policy* screen appears (see Figure 7-7). Use this screen to specify the criteria by which email is evaluated. Each *Add/Edit Policy* page represents a separate policy. Each of the options is explained below.

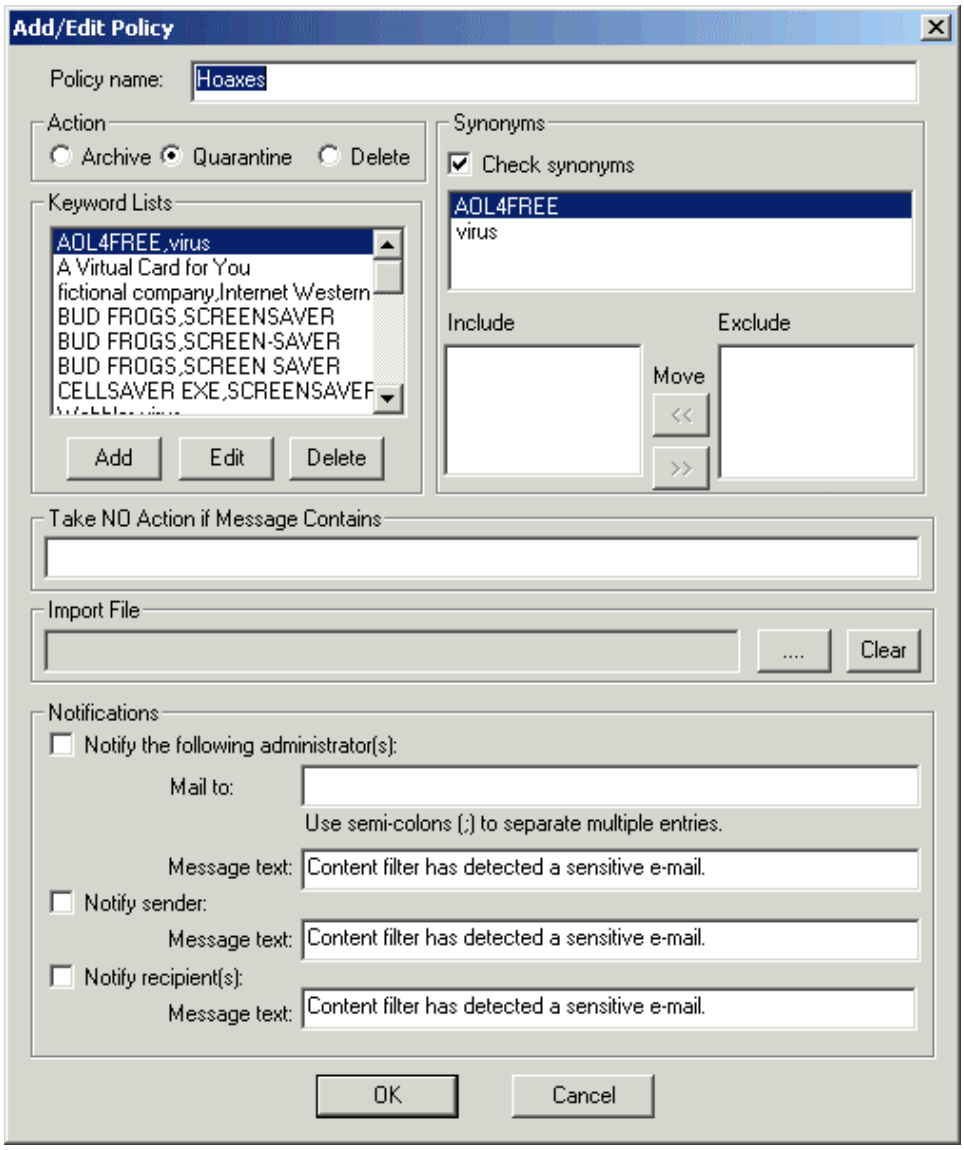

Figure 7-7: Add-Edit Policy configuration screen

Policy Name

Use the *Policy Name* field to create meaningful, descriptive names for the policies you create. The name, which appears in the Policies list, will not be used as a keyword in the content filter.

Action

Messages found to match the criteria specified in a given content-filter policy can be archived, quarantined, or deleted.

Trend Micros recommends that you archive messages for the first few weeks after you create or modify your content-filter policies. You can then check these messages to evaluate the efficacy of your policy.

For example, if you inadvertently created a policy with "the" as its sole keyword, nearly every email message passing through the Exchange server would match. If the action for this policy were set to **Delete**, each one of these messages would be deleted and would not be recoverable. If the action were set to **Archive**, however, the messages would be delivered even when they matched. After discovering the error, you could easily modify or delete the errant policy.

Keyword Lists

The content filter uses keywords and phrases to check email message content. When multiple keywords are included on the same line of a policy, a match is made only when the message being evaluated contains all of the keywords on that line. For example, you can add the following keywords to the list (perform four separate adds).

Example 1

sex, bare
sex, nude
sex, naked
sex, buff

Notice that in this example, four related words are used instead of just one. Basing the policy solely upon the word *sex* would probably not produce reliable results because *sex* is often used in place of the word *gender*. To minimize the chance of registering false positives, it is a good idea to qualify the primary word, *sex*, with additional words typically associated with it in a spam sex message: *buff*, *bare*, *nude*, and *naked*. Including several keyword groups will increase the reach of the filter. If the keyword list is configured like the example, messages that contain any of the keyword pairs are considered a match.

Example 2

Alternatively, you could have the filter trigger an action only when all five words are encountered in a single message. To create this filter, you would include all the keywords on a single line (perform a single add).

sex, bare, nude, naked, buff

Obviously, the likelihood of detecting every sex message on the basis of this filter is much less than for a policy that contains several rule sets bases upon the word *sex*, as shown in Example 1 above.

Example 3

In the following example, a policy is constructed wherein the occurrence of any one of the related words in Example 2 triggers a match.

nude
sex
buff
bare
naked

This technique can be used to filter out other offensive content—not every expletive in the dictionary need appear in a message to qualify as a match. Instead, you might deem the occurrence of any one of the words on your offensive list to be sufficient to warrant tracking (archive option), further investigation (quarantine option), or immediate deletion.

The words listed in these examples would probably not qualify for exclusion on their own. You will need to decide which words might be offensive enough individually to warrant exclusion.

The criteria you specify for content-filter policies are evaluated exactly as they are entered, including any quotes, spaces, and punctuation. Phrases are treated as a single unit. A match is registered only when each word, space, character, and so on in the phrase is found in the message.

✔ ***Note:*** *Do not use quotes to signify a phrase. Use commas to delimit multiple words entered in a single field or create separate rules. Wildcards such as the asterisk (*) and question mark (?) are not supported in the content filter. If included in a rule, these characters are taken literally.*

Synonym Checking

Synonyms are an extension of the content filter's Keyword list and can be used to broaden the reach of a keyword to include conceptually related topics. You must add synonym suggestions for a given word or phrase to the Include list.

✔ ***Note:*** *Global property settings for case-sensitive comparisons and exact matches (enabled on the Content Filter tab) are also applied to synonyms.*

In general, keywords linked on the same line should not include more than four or five values, or they risk being overly restrictive. On the other hand, if only one keyword is included on any given line, the policy risks being too permissive—few email messages will be found to match. Of course, a lot depends upon what you want to filter out.

The criteria you specify are evaluated exactly as they are entered, including any quotes, spaces, and punctuation. Phrases, delimited by commas, are treated as a single unit. A match will be triggered only when each word, space, etc. in the phrase is found in the message and it appears in the order entered.

The following examples show how the content filter will interpret keyword lists without synonym checking and with synonym checking:

Example

Case 1. All three keywords appear on the same line:

apple juice, pear, orange

Case 2. Each keyword appears on its own line:

apple juice
pear
orange

Case 3. All three keywords appear on the same line, and synonym checking is enabled for the word *orange*:

apple juice, pear, orange
orangish
red
yellow

The words *orangish*, *red,* and *yellow* are on the synonyms list for *orange*.

- In Case 1, only messages containing all items, *apple juice*, *pear,* and *orange* (in any order, anywhere in the message text) are considered a match.
- In Case 2, all messages containing the phrase *apple juice* are considered a match, all messages that contain the word *pear* are considered a match, and all messages that contain the word *orange* are considered a match.
- In Case 3, with synonym checking enabled, messages that contain the phrase *apple juice* and the word *pear* and also contain any of the words *orange*, *orangish*, *red,* or *yellow* are considered a match.

> ✔ ***Notes***: Apple juice *is a phrase because the words* apple *and* juice *are not delimited with a comma; even if the words* apple *and* juice *both appear somewhere in the message, no match will be registered unless they occur together, as* apple juice.

The capitalization and exact-match properties of synonyms are consistent with those defined on the *Content Filter* screen. In other words, if the word *red* appears in the synonyms list, it will register a match with the word ***red****undant* only if Exact Match is *not* enabled. Likewise, the word *red* will trigger a match with the word *Red* in the message text only if **Case-Sensitive Comparison** is *not* enabled.

Take No Action If Message Contains

You can define exceptions or "anti-keywords" that will apply to all rule sets and override the designated action for those rules. Enter the words you want to trigger and override in the *Use the Take NO Action If Message Contains* field on the *Add/Edit Policy* configuration screen to define

For example, if you want the Human Resources (HR) manager to see all inbound messages that contain her name, you enter her name in the *Take NO Action If Message Contains* field. Inbound messages that contain the HR manager's name will be forwarded to her regardless of the other content of the message. Even if all the values specified in a keyword list are detected in a message, no action will be taken if any of the words or phrases that appear in the exclusion field are also found.

> ✔ ***Note:*** *You can designate only one exclusion for each policy. You cannot create multiple exclusion lists for a single policy.*

Example

If your policy is to block *Free Offer* email but you do not want to block email that includes the option for users to take themselves off the mailing list, you could include a phrase such as "To remove yourself from this list," in the *Take NO Action If Message Contains* field. Use a comma as a delimiter if you would like to enter multiple phrases.

For example, you can create a new policy and add keywords such as the following to cover a wide range of "remove" phrases:

remove in the subject line
"remove" in the "SUBJECT"
"remove" in the subject line
remove in the "subject" line
remove list

Disable case-sensitive comparisons in the *Content Filter* screen so that the filter will register a match for *remove, REMOVE, ReMove*, and so on.

Import Files

You can develop import files to augment an existing content filter policy. These files might include an existing list of keywords exported from a database or spreadsheet program from the U.S. Federal Trade Commission's "dirty-dozen" list of the worst spam scams or from keyword lists solicited from department heads and other concerned individuals in your organization.

Import Files must contain only ASCII characters. To edit an import list, you use an ASCII editor (such as Notepad) and disable any Word Wrap feature. Quotation marks should not be used. Use a comma to delimit individual words and phrases within a policy.

Notifications

Whenever the content filter acts upon an email message, ScanMail eManager can notify the email administrator and others. Content-filter notifications are policy-based to allow different people to be notified depending on which policy registers the rule violation. For example, you might want to notify your HR department whenever the Sexual Harassment or Racial Harassment policy triggers a match.

Using the Keyword Lists That Trend Micro Provides

Trend Micro provides special keyword lists that are designed to efficiently filter certain types of spam and other unwanted email based on message content. These keyword lists go beyond the quick header checking that the spam filter performs. Instead, they filter messages based on an analysis of the actual message content. Import files, like the rule file, are updated monthly by Trend Micro and can be downloaded on demand or scheduled for automatic downloads.

Editing Profanity and Discrimination Lists

The Profanity list includes keywords such as "four-letter words" and other keywords that could be used in offensive ways. You can edit this list to suit your needs.

The Racial Discrimination list is used to store words that are considered to be racist and offensive. This list contains words that are commonly considered offensive and do not have alternate meanings that are not offensive. You can add as many terms to this list as you want.

The Sexual Discrimination list includes words that are considered to be sexually harassing or inappropriate. This list is intentionally brief. The keywords listed are words that generally do not have alternate meanings that are not offensive.

Editing Hoaxes and Chain Mail Policies

The Hoax list contains keywords that in combination can be used to identify some of the most common hoaxes on the Internet. These warning messages often describe fantastical or impossible virus or Trojan program characteristics but appear to be real. Forwarding these hoax warnings to friends and co-workers only perpetuates the problem. Other hoaxes offer bogus free gifts or other items not appropriate for a corporate environment.

The Chain Mail list contains several keyword phrases that can be used to identify chain letters. Chain letters are sometimes "get rich quick" schemes. A typical chain letter includes names and addresses of several individuals whom you may or may not know. You are instructed to send a certain amount of money to the person at the top of the list, and then eliminate that name and add yours to the bottom of the list. You are then instructed to mail copies of the letter to a few more individuals.

Chain letters have several problems. Even when delivered on the Internet, chain letters are illegal if they request money or other items of value and promise a substantial return to the participants. Chain mail that does not request money can bog down networks and contribute to a spam mail problem. Chain mail can also be offensive and might contain threats that if you do not forward them, you will experience bad luck. You can edit the Chain mail list to add chain letter phrases that are prevalent at your organization.

Editing the HTML Script Message List

The HTML Script Message list contains several entries that are generally found in all HTML scripts. Some HTML scripts have been known to contain code that executes destructive commands on user computers. If HTML scripting is an important part of your company's business, be careful when using this option.

Configuring Global Policy Settings

Three options on the *Content Filter* screen are global, which means they apply to all policies:

- Use exact matches only
- Case-sensitive comparisons
- Enable scanning the content of attached files

> ✔ ***Note:*** *When enabled, the global options are applied to the keyword list and any included synonyms that are defined in the Add/Edit page of every policy.*

Exact Matches

For content filtering, the **Use Exact Matches Only** option applies to all policies in the Policies list. If you do not select exact matches, every keyword or phrase used in every list for every policy will be used for partial-word matches. Accepting partial-word matches can significantly increase the incidence of false positives. Trend Micro therefore recommends that you enable Use Exact Matches Only for content filtering.

Case-sensitive comparisons

By default, keyword comparisons are *not* case sensitive. To specify a case-sensitive comparison, select the **Case-Sensitive Comparison** check box next to the desired field.

Enable Scanning the Content of Attached Files

You can select **Enable Scanning the Content of Attached Files** to scan the text of attachments for content violations. ScanMail eManager can scan the content of non-encoded text files and Microsoft Word documents.

> ✔ ***Note:*** *Scanning the content of attached files takes longer than scanning only the message subject and message body.*

Chapter 7 Summary and Review Questions

Summary

ScanMail eManager allows administrators to create innumerable filters to block spam and objectionable content. Rules can be created to filter messages based on case, exact- or partial-word matches, wildcards, *To: From: cc:* and *Subject:* lines, attachment or message size, attachment type, specific words or phrases, and HTML script. For the content filter, keyword lists can be configured to filter out words or groups of words and their synonyms using proximity or frequency of use as filtering criteria.

Review Questions

1. Which is NOT a default setting of the spam and content filters?
   a. Case sensitivity
   b. Partial-word matches
   c. No wildcard characters
   d. Messages that match filtering criteria can be quarantined, archived, or deleted.
2. For the spam filter, which information is compared against the rules defined on the Add/Edit page?
   a. Email header
   b. Message body
   c. Attachment information
   d. All of the above
3. When defining attachment-blocking rules, you can use the asterisk wildcard.
   a. True
   b. False
4. When keywords are on a single line, delimited by a comma, what is the relationship between the words?
   a. They are joined by AND.
   b. They are joined by OR.
   c. They are synonyms of the same word.
   d. They are part of the global policy.
5. Given the keywords *cat, rat, dog, howling werewolf* on the same line, which of the following would score a match?
   a. A message that contains the words *cat, rat, dog, howling,* and *werewolf*
   b. A message that contains *cat*, *rat*, *dog,* and *howling werewolf*
   c. A message that contains either *cat, rat, dog,* or *howling werewolf*
   d. Only a message that contains *cat, rat, dog,* and *howling werewolf* in that order