Trend Micro
InterScan™ eManager™

TREND MICRO

Getting Started Guide

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes and the latest version of the Getting Started Guide, which are available from the Trend Micro Web site at:

http://www.trendmicro.com/download/documentation/

NOTE: A license to the Trend Micro Software includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Thereafter, you must renew Maintenance on an annual basis by paying Trend Micro's then-current Maintenance fees to have the right to continue receiving product updates, pattern updates and basic technical support.

To order renewal Maintenance, you may download and complete the Trend Micro Maintenance Agreement at the following site:

http://www.trendmicro.com/license

Document Part No. IMEM31514/30529

The Getting Started Guide for Trend Micro™ InterScan eManager is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available online Solution Bank at Trend Micro's Web site.

At Trend Micro, we are always seeking to improve our documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Table of Contents

Chapter 1

Installing InterScan eManager

Trend Micro InterScan eManager is a part of the InterScan suite of products. Used in conjunction with InterScan VirusWall, eManager provides additional security and management features to an Internet gateway security solution. InterScan E-mail VirusWall scans SMTP traffic passing between the corporate network and the Internet. eManager adds the ability to filter out spam mail and inappropriate content.

In this chapter we will cover the following:

- Overview of eManager
- Installing eManager
- How to get started using eManager

Content Management

The Content Management component includes spam and content filters.

InterScan eManager allows you to filter out spam mail and check user messages for content considered to be sensitive, offensive, or against company policy. eManager is easily configured to fit the needs of different businesses.

Spam Filtering

Content Management's spam filter quickly evaluates the header fields of messages en route to the SMTP server(s). In particular, it checks the origin of messages to assess whether they are spam (unsolicited commercial email, or UCE) by comparing the header information to a set of user-defined rules. Messages that are found to be spam can be **deleted, archived** or **quarantined**. They are not passed to the SMTP server for delivery.

Spam rules are completely user-definable and there is no limit to the number of rules you can employ. Trend Micro also provides a comprehensive list (called the Rules File list) of spammers, identified by subject, routing domain, or sender. This list is available for download from:

http://www.trendmicro.com

Content Filtering

Another function of **Content Management** is content filtering. The content filter performs an analysis of the message and header text. Like the spam filter, the content filter evaluates messages on the basis of user-defined rules. These rule sets, or *policies*, can be created to check for the use of inappropriate language, to guard against the loss of proprietary information, to scan for resumes, etc. In fact, you can screen for any content.

Policies can be created to check inbound and/or outbound mail for any type of content. Examples include:

- Sensitive, or restricted business information
- Inappropriate language (four letter words, etc.)
- Racial slurs
- Indications of job hunting
- Pornography traffickers

Processing Order

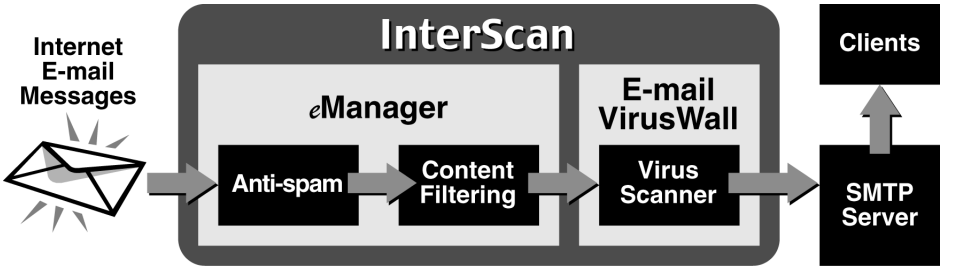

FIGURE 1-1. A graphic overview of the processing order of an incoming email.

On a network with an SMTP server, InterScan E-mail VirusWall, and one or more instances of Content Management installed, the processing order is as follows:

1. InterScan E-mail VirusWall receives inbound and/or outbound mail, and directs it to the content filter. This action occurs before virus scanning, and before the SMTP server receives the message for processing.
2. In a quick operation, a spam/not-spam evaluation is performed. Message header information is compared to the user-defined list of current rules. Mail that violates a policy is **Deleted, Archived**, or **Quarantined**, as defined in the policy. The message is not compared further, nor is it forwarded to the E-mail VirusWall or SMTP server.
3. Next, the message text of all mail found not to be spam is evaluated against the active user-defined policies in the filter. Encoded attachments are not evaluated.
4. Mail that has not matched any of the content filter policies or spam filter rule-sets is forwarded. If another plug-in is installed, E-mail Management, for example, the mail is passed to it. Otherwise the message is passed to E-mail VirusWall where it will be checked for viruses.
5. Infected email attachments are either **Cleaned**, **Quarantined**, **Deleted**, or **Passed** (infected files are not blocked), according to what is specified in the E-mail VirusWall configuration. Cleaned and uninfected messages are passed to the SMTP server for processing, as usual.
6. The SMTP server delivers the email to the intended recipient(s).

System Requirements

To run InterScan eManager:

- InterScan E-mail VirusWall 3.5 or above must be installed
- To enable "Specialized Filtering", InterScan for Unix 3.6 or above must be installed
- Install InterScan eManager on a system with at least the configuration indicated below.

Solaris Version

- Solaris 2.6 or later on Sun SPARC platform
- 256MB main memory (DRAM)
- swap space should be 2~3 times the main memory
- 50MB disk space for InterScan and eManager plug-in installation
- Minimum 9GB disk space for processing email messages during operation

HP-UX Version

- HP-UX 10.20 or later, see note below
- 256MB main memory (DRAM)
- Swap space should be 2 to 3 times the main memory
- 50MB disk space for program files (including InterScan)
- 9GB of disk space for operation (processing email messages)
  If you are using HP-UX 10.20, the DCEProg package is required. Follow the instructions below to install DCEProg.
  1) Put 10.20 Core OS CD in cdrom and mount
  2) Run /usr/sbin/swinstall
  3) Choose the package "DCEProg" for install

  To use HP-UX 11.0, you need to apply three patches:
  1) PHNE_21767 -- s700_800 11.00 Cumulative ARPA Transport Patch
  2) PHNE_20316 -- s700_800 11.00 Cumulative STREAMS Patch

Linux Version

To run InterScan eManager version 3.7 for Linux, you must install to a computer that has InterScan(r) E-mail VirusWall 3.7 or above. In addition, you need the following minimum configuration:

- IBM/AT compatible PC with Intel Pentium 133MHz or faster
- Memory: 128MB or more
- Swap space should be 2 to 3 times the main memory
- 20MB disk space for InterScan
- At least 9GB disk space for operation (processing email messages)
- OS: Linux kernel 2.2.12 or above, glibc 2.1.2 or above
- We have tested on these Linux distributions.
    - - RedHat Linux 6.1
    - - RedHat Linux 6.2
    - - TurboLinux Server 6.1 Japanese version (*3)
- *3: C++ standard shared library (libstdc++) package needs to be installed. For more details about its installation, please refer to the manuals of your OS.
- Package name: libstdc++-compat

Installing InterScan eManager

InterScan eManager is a plug-in to InterScan E-mail VirusWall and it must be installed on the same machine as E-mail VirusWall. The current version works with the *Standard Edition* of InterScan. It does not work with the *CVP (Content Vectoring Protocol) Edition*.

Before Installing InterScan eManager

Important: Before Installing eManager, you must have InterScan E-mail VirusWall installed on the same machine. The following InterScan VirusWall components must be installed: the SMTP, ISADMIN, and ISBASE packages. If you do not have these packages installed, please install them before continuing with the eManager installation.

Installing eManager

The eManager setup includes scripts requiring superuser permission—log on as **root** before installing eManager.

From the directory containing the eManager installation files, type **`./install.sh`** and press ENTER.

1. The **Main Menu** appears, displaying the installation options.
2. By default, eManager will scan the file system and install under the directory where InterScan was installed. If InterScan was installed into the default `/opt/trend` directory, eManager will install into the `/opt/trend/Plug-Ins/EM` directory.
3. Choose **Option 1** to start the installation.
4. Once eManager systems is installed, you are prompted to type a serial number.

   Press **Enter** without typing in a serial number to install the 30-day trial version. This version of eManager is fully functional but will expire after 30 days, at which time it should be upgraded or removed. For information on how to buy, please refer to the following URL:

   `http://www.trendmicro.com/buy`

Note: Serial numbers can be found on the front cover of the InterScan eManager manual and on the product registration card.

5. Continue to follow the screen prompts to complete the installation.
6. Once you have completed the installation, select **Exit**.

Start eManager

After installing eManager, you need to configure InterScan to recognize and enable eManager. The following tasks must be done in the sequence shown to enable eManager.

1. Using a Web browser, open the InterScan configuration menu (user name and password are **`default)`** .
2. Click **Configuration** on the navigation bar.
3. Click **Configuration: E-mail Scan**. (Make sure the box is checked and email scan is active.)
4. Scroll down to the bottom of the page and select the check box **Enable Plug-In**.
5. Click **Apply.**
6. Go to the **Turn On/Off** page. Turn the **Mail** button **Off**, then back **On** by clicking on the image.

InterScan eManager is now enabled and active.

Opening the Web Console

After installing eManager, a hyperlink to the eManager configuration menu is added to the InterScan configuration menu. You can access the eManager configuration menu by clicking on the link in the InterScan Web configuration menu, or type the URL directly in the browser as shown below.

1. Open a Web browser, then type the eManager URL followed by the port (**:1812)**. The URL can be either the domain name or IP address of the eManager machine. The port used for the Web Console is also user-configured. For example,

```
http://domain:port/eManager/eManager.html
http://isvw.widget.com:1812/eManager/eManager.html
http://123.12.123.123:1812/eManager/eManager.html
```

2. The eManager console is password-protected. By default, both the user name and password are **`default.`** The eManager password is the same as the InterScan VirusWall password. If you change the password in InterScan, the eManager password will change accordingly.

Outbound Filtering

The **Enable Outbound Mail Processing** option in E-mail VirusWall must be enabled for outbound content and spam filtering to occur.

Note: Outbound mail processing is a separate operation from outbound mail scanning. Be sure to also check **Enable outbound mail virus scanning** to turn outbound virus scanning on.

To enable outbound mail processing,

1. Start the InterScan configuration program.
2. Make the **Configuration > E-mail Scan** page active.
3. Click the **Additional Email Options** link.
4. Click **Enable outbound mail blocking and disclaimer processing**.
5. Specify your local domain (required).
6. Click **Apply.**

Removing eManager

eManager's uninstall scripts require superuser privileges. You must be logged on as **root** to uninstall eManager.

1. To remove eManager, type `./install.sh` from the directory where your eManager files are located.
2. Choose **Option 2** and follow the on-screen prompts to remove eManager.

Note: During uninstall, you will be asked if you want to keep the eManager rule files. If you choose **yes**, the rule files will be saved. The current rule files will then be available if you reinstall eManager.

Upgrading from the Trial Version

Upgrading from the trial version is very simple. Open the Web configuration and go to the **Register Software** page. Type the serial number in the provided field and click **Save**.

Trial version users who want to remove the time limit can contact Trend Micro via email at

`support@trendmicro.com or sales@trendmicro.com`

Chapter 2

Using the Spam Filter

Overview

In this chapter we will present a number of tasks that take you through the basic processes and functions of the Spam Filter. The tasks presented in this chapter should give you a comprehensive understanding of how the Spam Filter works. For detailed information on each of the functions in eManager, please refer to the online help.

In this chapter we will cover the following:

- Using the rule file to stop spam
- Creating a spam filter based on problem spam mail

Spam Contact Info

You can send your spam to Trend Micro at the following address:

spam@trendmicro.com

Spam received at this address is included in the anti-spam data file used by eManager.

Using the Rule File to Stop Spam

InterScan eManager includes both Rule Files and Log Files for the Content Management filter. Rule Files are supplied by Trend Micro. They contain predefined anti-spam rules created by Trend Micro's engineering staff.

Log Files are kept for all policy violations. Once you have established anti-spam and content management policies, it is a good idea to review the log files to ensure the effectiveness of the policies.

Rule Files

As new spam is written and released onto the public, and as spammers jump from routing domain to routing domain to cover their tracks, Trend Micro monitors and collects telltale blocking information and incorporates it into new **Rule** and **Import** files.

- The **Rule file** is used by the spam filter and contains numerous predefined anti-spam rule-sets.
- **Import files** are used by the content filter and can augment existing policies.

Clearly, it is very important to keep these files up-to-date. New Rule and Import files are typically published monthly by Trend Micro, and you should not wait much longer to update the files.

Updates are available free to registered InterScan eManager customers. They can be scheduled for automatic download over the Internet, or updated "on demand" (in **Content Management**, make the **Rule File Update/Update Rule File** page active and click the **Update Now** button).

Note: Registration uses HTTP to register. If you use a HTTP proxy, you need to know the host name (or IP address) and port. If the proxy requires a user name and password, you need to type them before updating the rule file.

The rule file is kept in the following directory:

/EM/spamrule

Rule-files are named according to the following convention:

```
Trend$RF.1
```

where **.1** represents the rule file version. When multiple rule files exist in the directory, only the one with the highest number is read.

Rule File Information

The following information is available on the *Rule File Update* page:

- **Version of last rule file:** Used by the spam filter, represents the current rule file version.
- **Version of last imported Anti-spam policy:** Used by the content filter, represents the currently imported file version.

Click **Refresh** after adding a new rule file to display the most current settings.

Enabling the Rule File

You can enable the rule file from the **Anti-Spam/Set Global Options** page.

1. Check the box next to **Enable vendor-provided rule file: "Trend$RF"**.
2. Click **Save**.

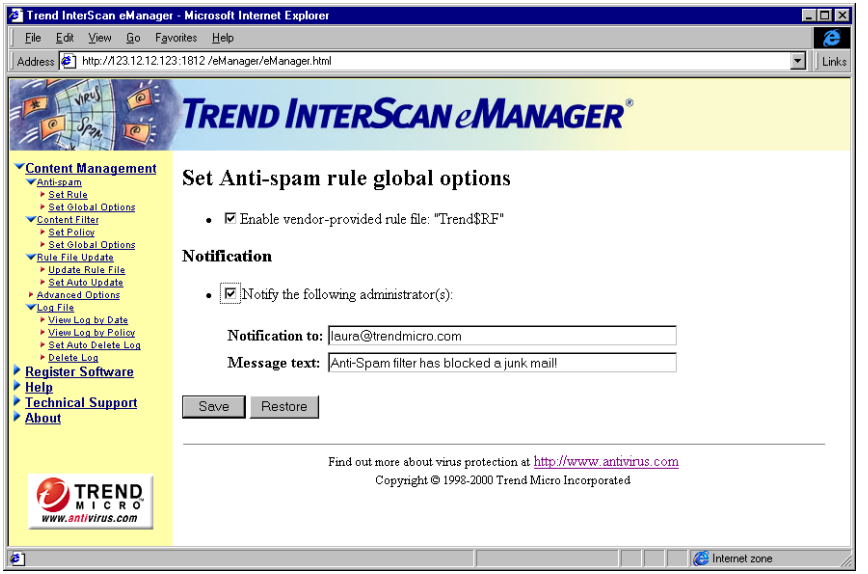

FIGURE 2-1. The Anti-Spam/Set Global Options page shows both the rule file and notification enabled.

Using A Proxy Server

If you use an HTTP proxy server on the network (i.e., InterScan eManager does not have direct Internet access),

1. Go to the **Rule File Update/Update Rule File** page on the configuration menu.
2. Type the IP address (number) and port of this HTTP proxy in the fields provided.
3. Type the appropriate logon credentials in the fields provided.

Note: If you just installed InterScan Web VirusWall, your proxy information may have changed. Be sure to type the correct IP address and port.

---

4. Click **Update Now** to test the proxy connection and update the rule file.

If the current Rule and/or Import file on your server is already up-to-date, you will receive a message such as "your rule file is already up-to-date." Otherwise, you may see a progress bar informing you of the download progress. Rule and Import file downloads are usually completed within a few seconds.

After the files have been downloaded, a status confirmation message appears. There is nothing more that you need to do; the new files are automatically installed and take effect immediately.

Note: You must register eManager before you can download new rule files.

Automatic Update

When **Automatic Update** is enabled on the **Set Automatic Update** page, the content filter will automatically update the Rule and Import files from Trend Micro at the interval specified.

New files are typically published monthly by Trend Micro, but special releases are occasionally made to address new spam issues that are likely to pose an immediate problem for customers. We recommend that you schedule automatic Rule and Import file updates at least monthly.

Updating the Rule File Automatically

To schedule automatic updates of the Rule file,

1. On the Web configuration menu, make the **Rule File Update/Set Auto Update** page active.
2. Choose one of the following:
   - **Update Daily** schedules InterScan to automatically update the files each day
   - **Update Weekly** to schedules InterScan to automatically update the files each week
   - **Update Monthly** and select a suitable date from the corresponding pop-up list

   If you do not want InterScan to automatically update the pattern file, choose the **Do not update automatically** radio button.

3. Type the IP address and port of your HTTP proxy server if one is required on the **Rule File Update/Update Rule File** page.

   Test your proxy information by clicking **Rule File Update** to start an immediate download of the pattern files.

4. Click **OK** to keep your settings, or **Restore** to bring back the last saved configuration setting.

Creating a Spam Filter Policy

When creating spam rules, it is important to bear in mind that many spammers add false header information to their messages in an effort to make tracking back to the source difficult (see detailed information on spam in the online help). Bulk emailers will often reuse the same false routing domains and other header information because it is too much work to create a unique fake for each spam-blast. This is actually good news when it comes to creating anti-spam rules, because you can use these false domains like a "signature," to identify and safely block many spam messages rather than creating rules on a one-policy-one-spam basis.

Additionally, some ISPs do not have adequate anti-spam rules. They can easily become unwitting hosts to spammers. Identifying these domains and adding them to your rules can have a significant impact on the amount of spam your organization receives.

Viewing Email Headers

The header information from known spam is an excellent source of data for defining anti-spam rules. Many mail clients support viewing the header information of email messages. Header information can usually be seen through a **Properties** item on the menus, an **Options** tab on the open message, or by saving the entire message as ASCII text.

Header information of the original message is usually not available on forwarded messages. To preserve the header information of forwarded messages, have users copy the message (as a file) and include it as an attachment in the email they are sending you. Check the online help that came with the mail client for instructions on reading message header data.

Spammers' Email Lists

Lists of email addresses are generated in a variety of ways, including culling the addresses from postings to UseNet, using special Web-crawlers to harvest them from Web sites, and collecting them from false contests, drawings, surveys, and other Internet gimmicks. Lists are also put together by legitimate marketing outfits and businesses, then sold and resold countless times.

Lists of email names are easily available for purchase over the Internet and through other channels, with prices as low as $50.00 for 100,000 "verified" names. The following UCE example shows a current price list.

An Example of Unsolicited Commercial Email

Return-Path: <ked@andinet.com>
Received: from kepler.andinet.com (kepler.andinet.com [123.221.129.28])
by ihot.com (8.8.5/8.8.5) with ESMTP id AAA12130
for <DSWENSON@IHOT.COM>; Mon, 12 Apr 2000 00:09:52 -0700
Message-Id: <199910120709.AAA12130@ihot.com>
Received: from kepler.andinet.com ([123.37.75.162]) by kepler.andinet.com
(Post.Office MTA v3.1.2 release (PO203-101c)
ID# 629-49361U15000L15000S0) with SMTP id ACJ2386;
Mon, 12 Apr 2000 00:12:00 +0500
To: jtt@geo.au.com
Date: Sun, 11 Apr 00 21:54:54 EST
From: ked@ihot.com
Subject: Hi
Reply-To: jtt@geo.au.com
X-UIDL: 440bb61acc12ec0536991b3a41132b1f
Status: RD

Do you know what the number one factor is, (sic) that will determine whether your business is a success or not? ADVERTISING! Effective conventional advertising is quite expensive. So what do you do? Direct email is one of, if not thee(sic) most effective method of advertising in the 90's. You can get your ad out to hundreds of thousands, even millions, for only a fraction of the cost of traditional advertising. The wave of future advertising is here, (sic) don't miss it. We will send your advert for you. We have gone through painstaking methods to insure(sic) that we have the the(sic) most (sic) quality lists on the Internet. We send your ad for your (sic), all you have to do is create it.

250,000 addresses - $199
350,000 addresses - $250
500,000 addresses - $350

Anti-Spam Rules

Generally speaking, it is best to create spam-filtering rules by defining only one or two criteria on the **Add/Edit Rule** page.

For example, if you are defining spam-filtering rules that are based on actual spam mail, define the policy using only the mail's **Subject** field, or only the **Sender** field. The more criteria you specify for any given policy, the less chance there is of stopping similar violations.

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

Do not use quotes to signify a phrase, or commas to delimit multiple words entered in a single field. Instead, create separate rules.

Step-by-Step: Creating the Policy

In this example, we will create a policy for the spam filter designed to block all email messages originating from a fictitious organization that sends advertisements soliciting business for their bulk emailing service.

1. Open eManager configuration menu and make the **Anti-spam/Set Rule** page active.

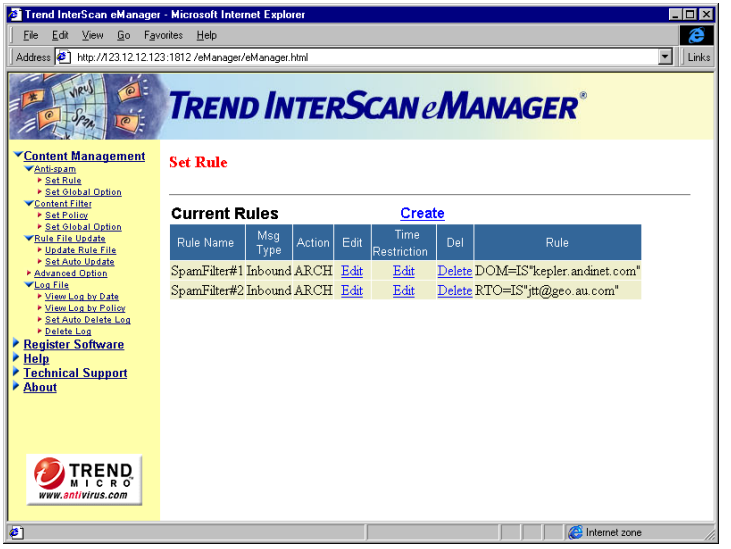

FIGURE 2-2. The Set Rule page shows the currently available policies. All policies shown on this page are active.

2. Click **Create** or **Edit** to open the **Add/Edit Rule** page.

   a. Type a name for the spam policy in the **Rule Name** field, for example, *Bulk Mail Solicitation, 05-01-00.*

   b. Check **Inbound**, as the SMTP flow direction (this type of spam mail will not be outbound).

   c. In the **Action on unwanted mail** field, select **Delete, Quarantine,** or **Archive**.

   - Deleted mail is not processed by E-mail VirusWall or the SMTP server
   - Quarantined mail is not sent to the recipient. It is renamed and moved to the `/EM/Quarantine` directory of the local machine

- Archived mail is delivered to the intended recipient, but a copy of the message, including header information, is also placed in the `/EM/Archive` directory. You can change the destination directory using the **Advanced Options** page.

Because this is a new policy, select **Archive** to save rather than delete matching messages, at least for the first week. This way, recipients will still get email while you fine tune the policies.

d. Check the header of the spam message to identify the criteria by which you can best block this and similar messages.

Because the Subject line is, simply, "Hi," it is too broad and would not make a good filter. Perhaps the spammer knew this. The routing domain, however, is pretty clear: *kepler.andinet.com* and there is no evidence of forgery (as may be indicated by numerous routing domains). Other possible candidates for the filter are the **To** field, which has been forged, and the **Reply to** field, which also appears to be forged (it does not match the domain of origin).

3. In this case, let's create a second anti-spam policy and cover two filtering criteria.

a. In the **Edit Rule** page, type only *kepler.andinet.com* in the **Routing domain** field.

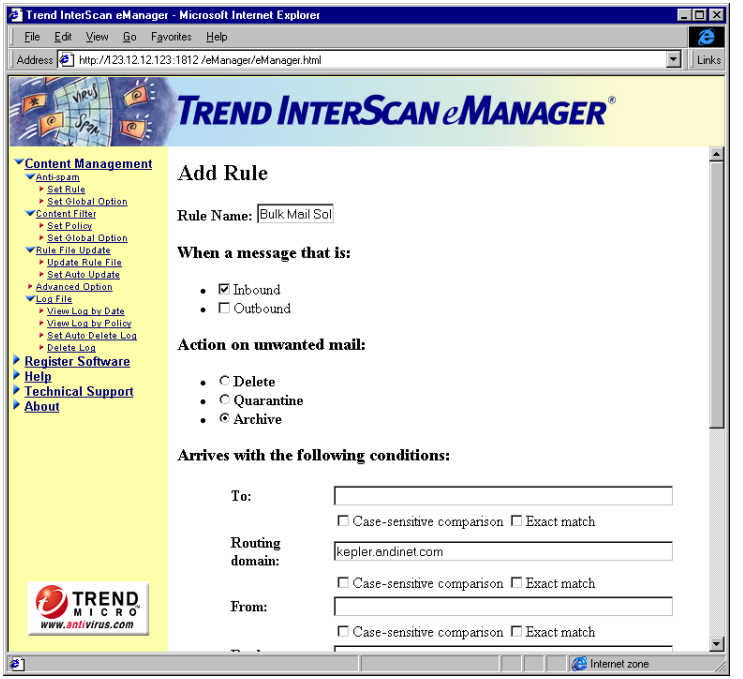

FIGURE 2-3. The Add Rule page showing the routing domain used to block spam.

b. Next, click **Edit** in the **Time Restrictions** field and select the times when you want the policy to be in effect. In this case, select the morning hours from 12:00 A.M. to 7:00 A.M. and the evening hours from 7:00 P.M. until 12:00 A.M.

Red time cells indicate the times when the policy is in effect. If no time selection is made, the policy is applied 24 hours a day.

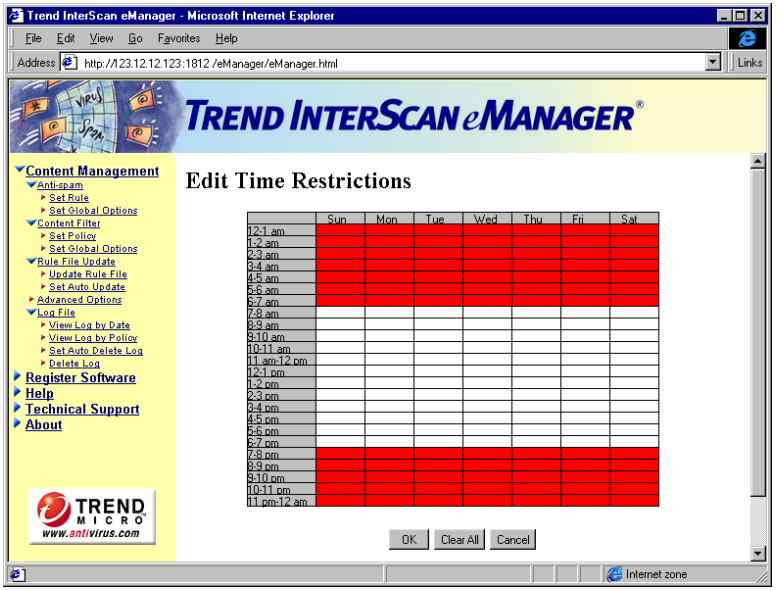

FIGURE 2-4. The dark squares show the times when the policy will be in effect.

c. Click **OK** and return to the **Set Rule** page.

4. Create another policy. This time Type *jtt@geo.au.com* in the **Reply to** field.

Of course, you could use both criteria to create a single policy. The decision as to whether to create one policy with multiple criteria or several rules, each with a single criteria, depends on whether you trust the routing domain. If the routing domain were AOL.COM, or HOTMAIL.COM, for example, you would probably want to narrow the scope of the policy by including an email address in the **From** or **Reply to** fields.

Click **Save** to save the policy. A new screen will appear with the message that the policy has been saved. Clicking **Back** will bring you back to the **Set Rule** page.

5. Back on the **Anti-spam/Set Global Options** page, type the email address of the person(s) you want eManager to automatically notify whenever one of your Current Rules matches a message. Include a brief message in the **Message text** field. For example,

   Anti-spam filter has blocked a junk mail.

   If you type multiple email addresses in the **Notifications** field, delimit them with commas.

6. Click **Save**.

   Notifications are global. The same notification will be sent out regardless of which policy actually triggers the match.

Testing Your Spam Rules

You can use Telnet or any mail client to test your spam filter rules and content filter policies. You just need to make sure that you are sending to the SMTP server that InterScan is scanning.

To create test email messages using Telnet,

1. From the command line, telnet to the SMTP server using the host name and port.
2. At the "ready" prompt from the SMTP server, type the following:

   MAIL FROM:*(true From address)*
   RCPT TO:*(true To address)*

   DATA
   From:*(type false email address here)*
   To:*(type false email address)*
   Subject:*(type test subject)*
   Message text:*(type the message text that you want the content filter to check here)*

   Note: *The* ***spam filter*** *checks only message header information, i.e., that which appears above* ***Message text*** *and below* ***DATA****. The* ***content filter*** *checks data appearing in both the message text and header areas.*

   The information entered in the first two lines, **MAIL FROM** and **RCPT TO**, should be genuine (Content Management does not check these two fields).

3. If you have configured the notification to go to your mailbox, you will receive a notification. To see the log files, see *Viewing Log Files*.

Current Rules Strategy

When specifying multiple rules in the Current Rules list, we recommend that you employ an inverted pyramid model, where you put rules with the broadest reach, or highest probability of matching, at the top of the list. Those that are more narrowly defined (less likely to trigger a match) should be placed towards the bottom of the list. This is the most efficient arrangement because in this way the filter will eliminate the greatest proportion of traffic with the fewest number of evaluations.

Policy Strategy Example

The following example further explains the inverted pyramid policy strategy. Let's say that you have created the five spam filter rules shown below:

1. Delete any mail originating from the domain SPAM.COM.
2. Delete any mail sent from SpamKing.
3. Quarantine any mail being sent to *SpamLover@company.com*
4. Delete any mail containing the phrase "Free Offer" in the subject line.
5. Quarantine any mail containing the term "SeXXX" in the subject line.

Let's further say that you have analyzed your incoming messages and know that for every 10,000 messages processed by the SMTP server, 42 are sent by SpamKing, 150 originate from the SPAM.COM domain, 500 contain the phrase "Free Offer" in the subject line, 18 are sent to *SpamLover@company.com*, and 196 contain the term "SeXXX" in the subject line.

In this case, the optimal ordering of the rules appearing in the Current Rules list is as follows:

1. Free Offer (500 instances)
2. SeXXX (196 instances)
3. SPAM.COM (150 instances)
4. SpamKing (42 instances)

5. *SpamLover@company.com* (18 instances)

When ordered as above, 500 of every 10,000 incoming messages can be eliminated in the first round of evaluation because they match the "Free Offer" policy. If, on the other hand, the order was reversed and "SpamLover" was the first policy and a "Free Offer" message arrived, the message would be evaluated five times (1. check for "SpamLover@company.com," 2. check for "SpamKing," 3. check for "Spam.com," 4. check for "Sexxx", 5. check for "Free Offer") before finally matching on "Free Offer" and being rejected.

Chapter 3

Using the Content Filter

Overview

In this chapter we will present a number of tasks using the Content Filter. The tasks presented in this chapter should give you a comprehensive understanding of how the Content Filter is used to create security policies. For detailed information on each of the functions in eManager, please refer to the online help.

In this chapter we will cover the following:

- Using the content filter to stop spam
- Using the content filter to block a specific type of file
- Using the content filter to block greeting cards

Creating Content Filter Policies

The content filter provides a means for the administrator to evaluate and control the delivery of email on the basis of the message text itself.

It can be used to monitor both inbound and outbound messages to check for the existence of sensitive, offensive, or otherwise objectionable message contents being sent to customers, competitors, or others. 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.

Any number of policies can be created, regarding any subject.

Depending on how you have InterScan E-mail VirusWall set up on the network, only messages crossing the Internet gateway are checked against the content filter. Internal email is not necessarily scanned.

Note: The content filter supports scanning double-byte messages, such as messages in Chinese and Japanese.

Content Filter Policies

A content filter **Policy** represents a group of conceptually related words and phrases that will be matched against inbound messages, outbound messages, or both.

The message text, or body, of email (including the header) is compared against the list of policies and 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**.

Only the email message text (and any non-encoded ASCII attachments) are included in content filter comparisons; binary email attachments are not considered.

Messages are checked first for the keywords specified in the first policy on the list, then the second policy, third, and so on.

Policies can be individually enabled by selecting the check boxes proceeding the policy name in the Policies list. There is no limit to the total number of policies that can be engaged by the content filter. One rule of thumb, however, is that the more active policies there are, the longer it takes to evaluate a given email message.

Keyword Lists

The **Keyword List** for a given **Policy** contains the words and phrases that the content filter uses 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 **Add**s).

Example 1:

resume, position
resume, job
resume, experience
resume, enclosed

Notice that in this example, four related words are used instead of just one. Basing the policy solely upon the word *resume* would not likely produce reliable results because *resume,* i.e., curriculum vitae, shares the same spelling as *resume*, i.e., to start again. To minimize the chance of such false matches, it is a good idea to qualify the primary word, *resume*, with additional words typically associated with it in a job seeking letter: *enclosed*, *position, job*, and *experience*. Including several keyword groups will increase the reach of the filter.

As configured in the example, messages that contain any of the keyword pairs are considered a match. Alternatively, you could have the filter trigger the configured action only when all five words are encountered in a single outbound message. Do this by including all the keywords on a single line (perform a single **Add**).

Example 2:

Resume, position, job, experience, enclosed

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

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

Example 3:

job
resume
enclosed
position
experience

Although not applicable to the case of a resume filter, this technique is appropriate, for example, when filtering for offensive content—not every four-letter word in the dictionary need appear in a message to qualify as a match. Instead, you may decide that 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.

Generally speaking, keywords linked by the **AND** operator should not include more than four or five words or they risk being overly restrictive. On the other hand, if only one keyword is included on any given line, (**OR** operator) the policy risks being too permissive—too many email messages will be found to match. Of course, as shown above, a lot depends upon what you are filtering.

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. Only when each word, space, etc. in the phrase is found to appear in the message, and it appears in the order entered, will a match be triggered.

Note: Do not use quotes to signify a phrase. Use commas to delimit multiple words entered in a single Keyword field.

More on Keyword Lists

Case 1. Keywords appear on a single line

```
Apple Juice, [and] Pear, [and] Orange
```

Case 2. Keywords each appear on their own individual lines

```
Apple Juice [or]
Pear   [or]
Orange [or]
```

Case 3. Keywords appear on a single line and synonym checking is enabled for the word Orange,

```
Apple Juice, [and] Pear [and] Orange
[or] orangish
[or] red
[or] yellow
```

where the words *orangish*, *red*, and *yellow* are included from the synonyms list.

- 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 on, messages that contain the phrase *Apple Juice*, and the word *Pear*, and also contain any of the word(s) *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 triggered unless they occur together, as *Apple Juice*.

The capitalization and exact-match properties of synonyms are consistent with those defined on the Content Filter tab. In other words, if the word *red* appears in the synonyms list, it will only trigger a match with the word ***red****undant* if **Exact Match** is not checked; likewise, the word *red* will only trigger a match with the word *Red* in the message text if **Case-sensitive comparison** is not checked.

Step-by-Step: Creating the Policy

In this example we create a policy to check outbound email messages for resumes.

Since we are creating a new policy, the **Action** will be set to **Archive** at first as a safeguard against errors. Neither the **Sender** or **Recipient** will be informed of the message evaluation; Edna Brokaw, a fictitious human resources manager, will be automatically notified. Additionally, if the message being sent contains Edna's name

(as appears in her signature at the end of her email), the message will be ignored even if a match is made.

1. From the Web configuration menu, click the **Content Filter/Set Policy** page. The **Set Policy** page shows all the current policies.

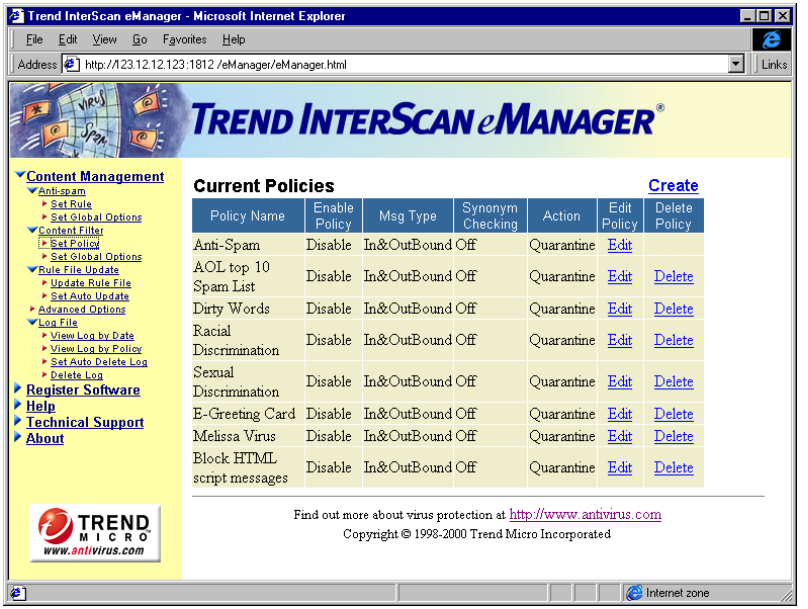

FIGURE 3-1. The Current Policies page shows some of the default policies that ship with eManager.

2. Click the **Create** link located above the Policies list. When you click the **Create** link, eManager will assign the policy a number and provide two links, **Options** and **Add Keyword**, that will allow you to create the new policy.
3. Go to the **Add Keyword** page.
   a. Type the word or phrase you want to scan for. **Add** (i.e., create) a new keyword for each word or phrase that you want the content filter to check for. In our example, we will add *resume*.

b. Click the synonym field to create a synonym for resume. A new screen will give list the synonyms for resume. By default, the words are excluded (not scanned).

c. Click **Edit**.

d. In the **Synonyms** list box, highlight the keyword for which you want to check synonyms, and click the word or words in the **Exclude** list to move them to the **Include** list.

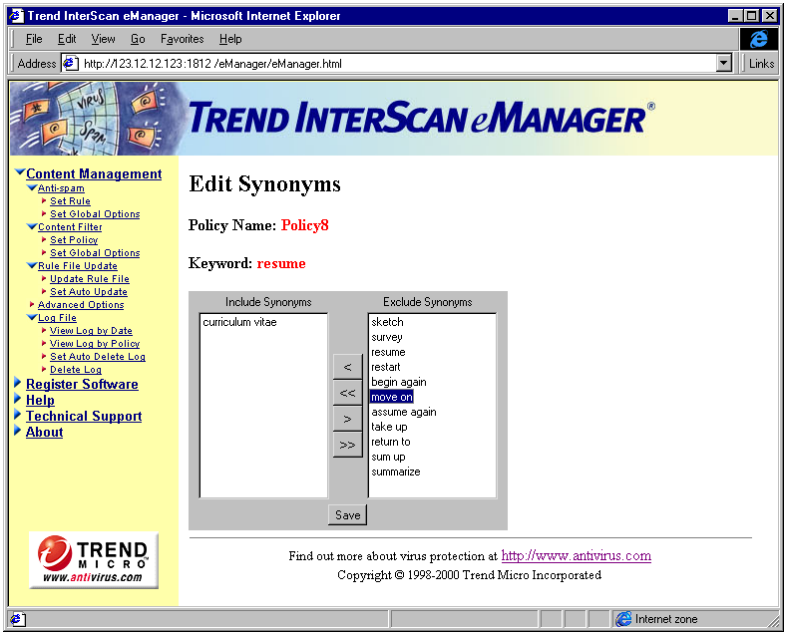

FIGURE 3-2. Use this page to add synonyms to keyword searches.

e. Click the << or >> button to move the word from one column to another. For this example, select *Curriculum Vitae* and move it to the **Include** list. None of the other synonyms apply.

f. Click **Save.**

4. Return to the **Content Filter/Set Policy** page.

a. Click the **Edit** field of the policy you are creating.

b. Click **Edit Options** to name the policy and set the scanning parameters. The **Edit Options** page will allow you to complete the policy once you have defined the keyword list and the synonyms that will be scanned.

c. In the **Policy name** field, type a name for the policy, in this example, **Outbound Resumes**.

Select whether to monitor **Inbound** mail, **Outbound** mail, or Both.

d. Define the **Action** to take whenever a match is detected. In this case, choose **Archive** to save a copy of the email, but also deliver the original to the intended recipient.

e. In the **Take NO Action If Message Contains** field, type the name of Edna Brokow, the HR manager, to exempt her email from the policy. (Do this to allow Edna to reply to any inbound messages that contain resumes sent to the HR department.)

f. Configure the **Notifications** so that Edna is automatically sent an email whenever a violation of the Resume policy is detected. Put a check in the **Send To user(s)** check box and type Edna's email address (use Internet email format, for example, *edna@company.com*, and delimit multiple email addresses with a comma). The message sent is as follows:

> *Edna: I am forwarding an email to you for review. Please determine whether this individual is sending out resumes.*

Because of the sensitive nature of this policy, neither the message sender or intended recipient are informed of the action. Alternatively, you could have a mild warning automatically sent to the **Sender**:

> *A message you sent appears to be an application for a job outside the company. We do not condone the use of company time and equipment to solicit employment.*

g. Put a check next to **Enable policy** and **Check synonyms**.

h. Click **Save** to add the policy to the **Policy list**.

5. Finally, go to the **Set Global Options** page and check the **Use exact matches only** option.

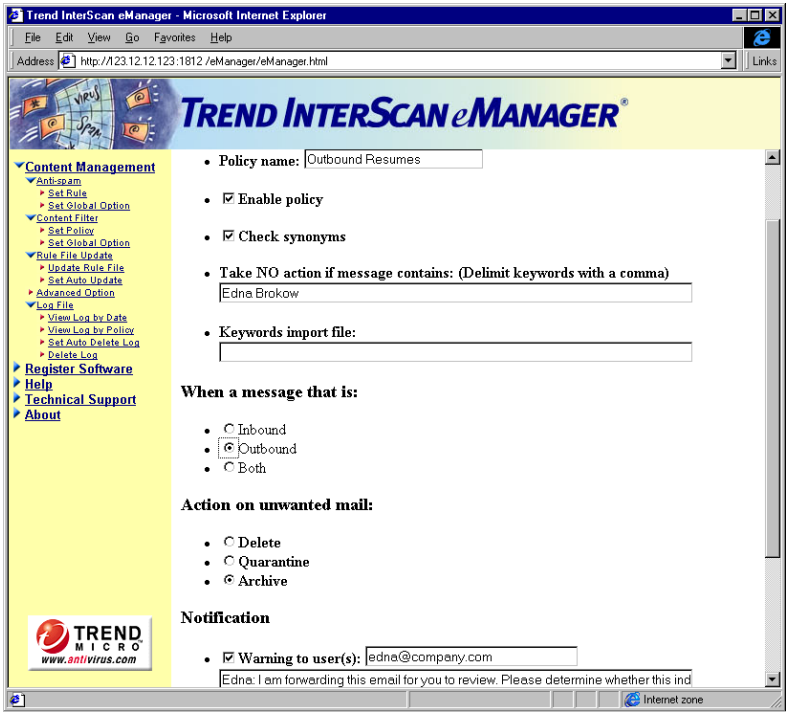

FIGURE 3-3. The Edit Options page shows many of the important scanning parameters.

6. Click **Save**.

Using The Content Filter to Block Spam

You can use the content filter to block spam, especially the type of spam that complies, or attempts to comply, with legislation requiring that bulk emailers provide a means of removal from the spam list.

For example, create a new Policy and add keywords such as the following to cover a wide range of "remove" phrasings:

remove in the subject line
"remove" in the "SUBJECT"
"remove" in the subject line
remove in the "subject" line
remove list
Per Section 301, Paragraph (a)(2)(C) of S. 1618

Disable **Case sensitive comparisons** in the **Set Global Options** page to have the filter trigger a match for *remove, REMOVE, ReMove*, etc.

You can create additional policies like the one above according to actual samples taken from your own spam (or that of your users).

Blocking Attachments with the Spam Filter

The Internet is offering more and more material to promote the music and film industry. Audio and video files are easily downloaded. Unfortunately, they are usually big files. They take up a large amount of bandwidth during the download process and can slow down the delivery of business communications. MP3 files are songs that can be downloaded from the Internet and are becoming popular downloads. Then, once they are downloaded they are shared through email. In this example we are going to show how you can block these types of audio files transferred through email during normal business hours.

Step-by-Step: Creating the Policy

In this example, we will create a rule for the spam filter designed to block all email messages containing *.mp3* audio file attachments coming from outside the company.

1. Open eManager configuration menu and make the **Anti-spam/Set Rule** page active.
2. Click the **Create** link to open the **Add/Edit Rule** page.
   a. Type a name for the spam rule in the **Rule Name** field, for example, *Audio_Files*.
   b. Check **Inbound** for the SMTP flow direction.

c. In the **Action on unwanted mail field**, select **Delete, Quarantine,** or **Archive**.

Because this is a new rule, select **Archive** to save rather than delete matching messages at least for the first week.

d. Scroll to the bottom of the screen and type *mp3* in the **Extension type** field.

To block only *.mp3* files, you do not need to fill in any of the other information on the screen.

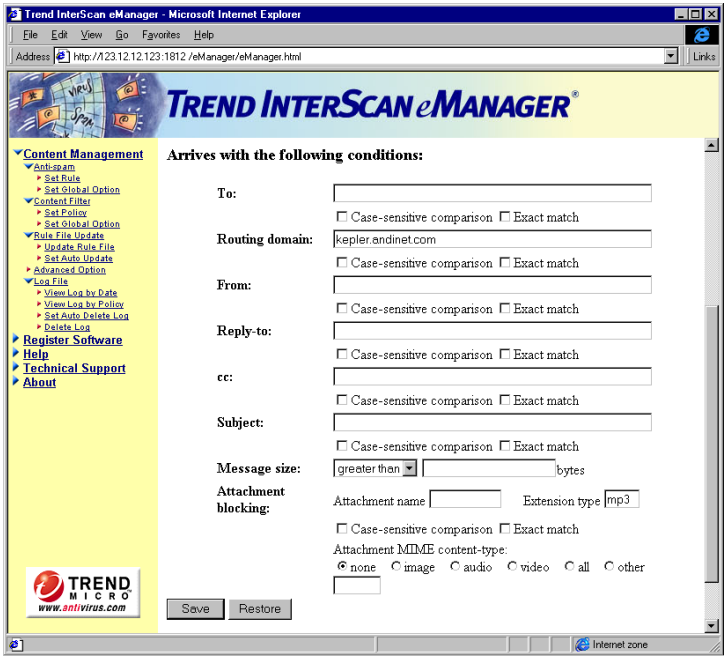

FIGURE 3-4. Do not put a wildcard character in the Attachment type field. The Attachment Blocking rule does not support wildcards.

e. Click **Save**. A message page will notify you that the rule has been save. Click **Back** to return to the **Current Rule** page.

3. Next, click **Edit** in the **Time Restrictions** field of the *Audio_Files* rule and select the times when you want the rule to be in effect. In this case, select the standard work hours for your company: from 8:00 A.M. to 5:00 P.M.

   Red time cells indicate the times when the rule is in effect. If no time selection is made, the rule is applied 24 hours a day.

4. Click **OK** to save the Rule.

Testing the Rule

After creating the rule, you will need to test the rule. Simply configure an email client to send an email with an *.mp3* attachment to the InterScan SMTP server. You can use any email client to send the message.

1. Set the **Outgoing mail (SMTP):** field in the server properties of your email client to point to InterScan.
2. Send an email to any address that includes an *.mp3* file as an attachment.
3. *See* Chapter 4 for instructions on how to view the log files.

Blocking Greeting Cards with Content Filter

Electronic greeting cards are very popular and can absorb valuable network resources. During the Christmas season, network traffic can be especially heavy because of the volume of business being conducted over the Internet. Blocking greeting cards, along with spam and unwanted attachment types, can save you money and help your network run smoothly during the holidays.

Trend Micro provides a preset Content filter policy for electronic greeting card messages. However, if you want to add additional rules, you can enhance the existing policy by adding your own policy as we will in this example.

Step-by-Step: Creating the Policy

In this example we create a policy to check inbound email messages for greeting card notifications.

Since we are creating a new policy, the **Action** will be set to **Archive** at first as a safeguard against errors. Neither the **Sender** or **Recipient** will be informed of the message evaluation.

1. In the eManager configuration menu, click the **Content Filter/Set Policy** page, then the **Create** link above the Policies list.
2. Click the **Add Keyword** link.
   a. We will add two keyword phrases to this policy. Type *free greeting card* and click **Apply**.
   b. Click the **Add Keyword** again and type *electronic greeting card*. Click **Apply**.

      Since each of the phrases are on their own line, eManager will scan for *free greeting card* or *electronic greeting card*.

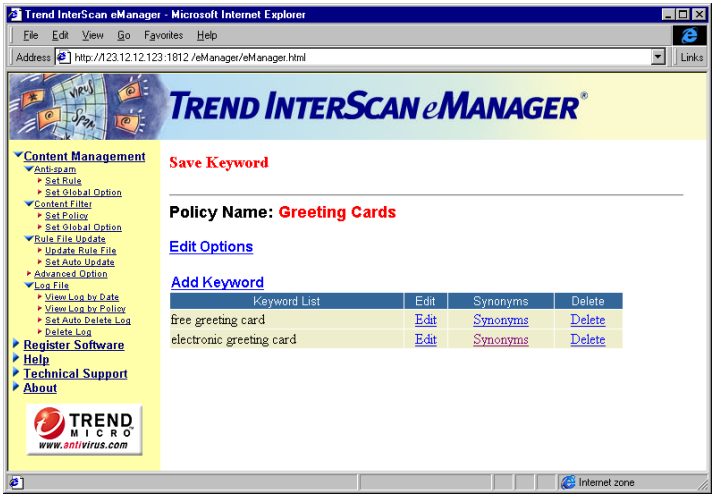

FIGURE 3-5. Each time a keyword is created for a policy, it appears in a list under the policy name.

3. Click the **Options** link.
   a. In the **Policy name** field, type a name for the policy, in this example, **E-Greeting Card II**.

b. Select **Enable policy**.

c. In the **When a message that is** field, select **Inbound**.

d. Define the **Action** to take whenever a match is detected.

- Choose **Archive** to save a copy of the email, but also deliver the original to the intended recipient.
- Choose **Quarantine** to move, without delivering, the message to the quarantine directory.
- Choose **Delete** to remove the message from the server without saving or delivering it.

e. Leave the **Check Synonyms** box blank.

f. Leave the **Take NO Action If Message Contains** field blank.

g. Configure the **Notifications** so that the person(s) you determine will be notified of the blocked email (use Internet email format, for example, *edna@company.com*, and delimit multiple email addresses with a comma).

Note: When initially creating and testing policies, always include your email address for testing purposes. That way, when you send a text email, you are notified, when the message is detected.

---

4. Click **Save** to finish.

Chapter 4

Maintaining InterScan eManager

The tasks presented in this chapter focus on common eManager maintenance tasks. These task show you how to ensure that eManager files are up-to-date and the program is functioning properly. For detailed information on each of the functions in eManager, please refer to the online help.

In this chapter we will cover the following:

- Viewing the log files
- Troubleshooting Tips
- Technical Support
- SolutionBank

Viewing Log Files

Logs are kept whenever eManager takes action on an email message. View log files, for example, to evaluate new Rules and Policies created for the spam and content filter, to determine the file name of a quarantined email message, or to identify the sending party of a deleted message.

By default, the plug-ins write their logs to the `/Plug-Ins/EM` directory.

eManager logs are named in the following manner:

```
iscan.log.2002.05.13
```

which can be read as InterScan Log for May 13, 2002.

Logs include the following details:

Message Date & Time stamp
Message From:
Message To:
Message filename, if quarantined
Action (quarantined, archived, deleted)
Filter that performed the action
Policy/Rule that triggered the match

***Date & Time stamp** of the log entry
***Service** (Content Management, Email Management, etc.)
***Process ID number**
***Action/Message**
***Service** (Email, Web, etc.)
***Error messages**

*Not seen in the **Log Reports** dialog box; open each log file individually with a text editor instead.

Error messages are also logged.

Step-by-Step: Viewing Logs

Log files can be viewed by either the name of the individual policy or by all the policies grouped together. You can select a date range for either type of log report. In the following example, we are going to view a log report based on a specific policy. The same process applies to viewing all logs according to date.

To view eManager log files for a specific policy,

1. Start the eManager configuration menu and make the **Log File/View Log by Policy** page active.
2. Select the **Mail Type** of the logs you want to view: **Inbound**, **Outbound**, or **Both**.

3. In the **Time Period** group, check the radio button for the log dates you want to view:

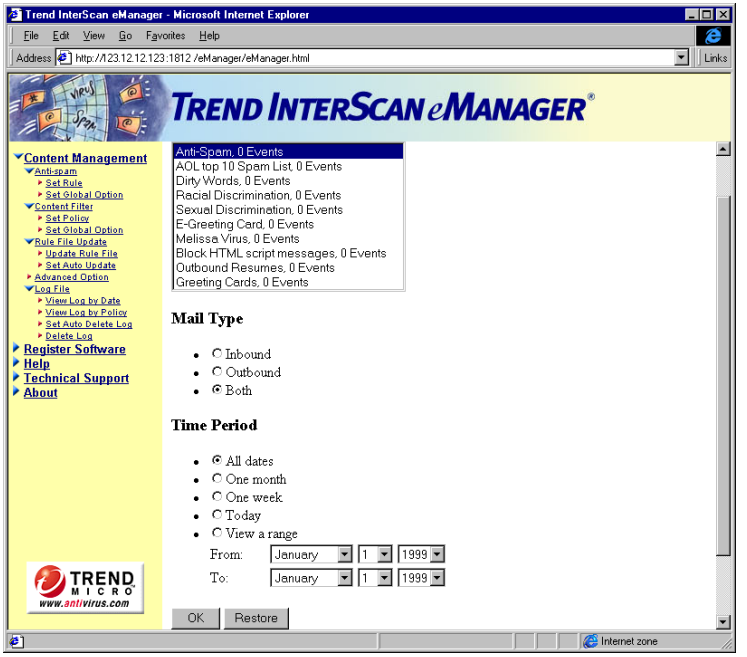

FIGURE 4-1. The View Logs by Policy page generates logs for individual policies.

In this example, check the **Range** radio button to select for viewing a range of dates, and specify the start and end dates for the log files.

4. Click **OK**. eManager will display all the logs that fit the criteria you specified in the **Log Reports** dialog box.

Troubleshooting Tips

1. How do I know that eManager is enabled after I install it?

   Go to the InterScan Web configuration menu and click **Configuration: Email Scan**. Scroll down to the bottom of the page. Select **Enable Plug-Ins**. Click **Apply**. then go to the **TurnOn/Off** page. Turn off the mail service and then turn it on again.

2. How can I check if eManager loaded successfully?

   You can view the plug-in value in the intscan.ini file. Make sure that it is set to **Yes**. The log file will also contain the following entry:

   "Returning from Initialize() of plug-in: eManager".

3. Why can't I update the rule file from the Internet?

   Prior to updating the rule file, you need to register eManager. Also, check the proxy settings to make sure they are correct.

4. When using the spam filter to block message size, eManager lets some files pass that are bigger than the size limit.

   Message sizes vary from platform to platform. The message may have been sent on a platform that creates a smaller file.

5. Question: After using Back or Reload on the browser, I get an error or unusual behavior.

   Back and **Reload** may affect the CGI program and cause it to rerun or lose the values you have entered. Always click **Apply**, **Save**, or **OK** after making changes using the Web configuration program before moving to another page.

6. eManager has been running for a long time, but it doesn't work consistently.

   Check to see if you are running a trial version. If so, you need to upgrade to a regular version.

7. eManager is running, but it does not block spam.

   Please check free space of /opt or the inode number of /opt/trend/Plug-Ins/EM/Quarantine(Archive)

8. I can't install eManager

You must install InterScan VirusWall Standard Edition before installing eManager. If you have InterScan VirusWall installed, you need to make sure there is enough free space in the /opt directory for eManager to install.

9. How can you move the quarantine/archive folder to another folder (/tmp or /var), when space of /opt is full?

   From the command line, type the following:

   ```
   mkdir /var/quarantine [Enter]
   cd/opt/trend/Plug-Ins/EM [Enter]
   mv quarantine  quarantine.orig [Enter]
   ln -s /var/quararntine  /opt/trend/Plug-Ins/EM/quarantine
   [Enter]
   ```

   This will create the new directory and move the files to the new directory.

10. How do I change the password for the eManager Web configuration program?

    In the InterScan Web configuration console, click **Configuration/Change Password**. The eManager password is the same as the one used by InterScan VirusWall and defined using the InterScan configuration.

Technical Support

The best way to receive support is to send an email to our highly trained Technical Support staff or visit our Web site.

http://kb.trendmicro.com/solutions

or send an email to:

support@trendmicro.com

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

http://www.trendmicro.com/en/about/contact/overview.htm

To speed up your problem resolution, when you contact our staff please provide as much of the following information as you can:

- Product serial number
- Wireless Protection program, scan engine, pattern file, version number

- OS name and version and Internet connection type
- Exact text of any error message given
- Steps to reproduce the problem

Additional resources available over the Internet

The Trend Micro Virus Information Center provides many features to access virus information and security alerts. Visit HouseCall for a virus check-up. If you want to have regular virus alerts sent to you via email, sign up here.

Comprehensive security information is available over the Internet at our antivirus center

http://www.trendmicro.com/vinfo

Use the Virus Information Center to find out about:

- • Which viruses and malicious mobile code are currently "in the wild," or active and
- a list of computer virus trigger dates
- • Computer virus hoaxes and how to determine whether a detection is actually a
- false alarm
- • Trend Micro's Virus Encyclopedia, which includes a comprehensive list of names
- and symptoms for known viruses and malicious mobile code
- • A basic guide to computer viruses
- • A safe computing guide
- • Product details and white papers

In addition, you can sign up to receive

- • A weekly virus alert, listing the virus outbreaks that occurred during the current week

TrendLabs

TrendLabs is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world. (These centers are called "global antivirus eDoctor centers" in Japan and other Asian markets.)

Staffed by a team of more than 250 engineers and skilled support personnel, TrendLabs' dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA. ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

TrendLabs' modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited.

Support Database

Trend Micro provides SolutionBank, an online database filled with answers to technicalproduct questions. Use SolutionBank, for example, if you are getting an error messageand want to find out what to do to.

http://kb.trendmicro.com/solutions/

New solutions are added daily. However, if you don't find the answer you seek, you can submit your question on-line, where the experts at TrendLabs will provide you with an answer or contact you for more information.

Index

U