Content Filtering
With MDaemon 6.0

Alt-N Technologies, Ltd
1179 Corporate Drive West, #103
Arlington, TX 76006
Tel: (817) 652-0204

Contents

Abstract...3

Email: The Good and The Bad...4

Filtering Email...5

Designing Filters...6

How Server-Side Filtering Operates...7

MDaemon Content Filtering...7

- Content Filters...8
  - Condition and Action Rules...8
  - Filter Rule Setup...9
  - Example Rule...10
- Restricted Attachments...11
- Notification...12
- File Compression...13
- Macros for Messages...14

Other Blocking Options...15

Conclusion...15

Abstract

With the rapid increase in the volume of email comes the need to manage messages, both incoming and outgoing. The primary challenges are security violations, bandwidth waste and user information overload. While most email software clients enable users to create rules for screening sent and received messages, a well managed server-side filtering system provides many additional benefits. Among the positives of server-side filtering are uniform enforcement of company email policies, diminished threats from viruses, reduction of spam, easy routing of single emails to multiple users, the rejection of unwanted messages and better use of bandwidth. The bottom line is more effective deployment of the enterprise or service provider email server.

Email: The Good and The Bad

The good of email is self-evident to its users. It is an efficient and quick means to send and receive written communications among people worldwide.

Enterprises and individuals use email to inform, persuade, motivate, entertain and greet each other. Emails contain comments, discussions, questions and answers. Memos and meeting announcements also come and go through electronic mail. Attachments to email, which typically must be opened with programs external to the email client, include forms, surveys, pictures and word processing files. Because of its ease of use, email has developed into a very popular tool for both personal and business communications. Email is perhaps more versatile, useful and economical than the telephone.

Overall, email is:

- Easy to use for reaching individuals or audiences; responses are also easy, so email senders normally gets more results than from regular "snail" mail.
- Almost as fast as the "send" command, thereby saving time.
- Economical by using nearly free electrons rather than expensive paper; email is also less costly than postage.
- Good for keeping records of communications and discussions since users can easily and permanently keep email conversations.
- Inexpensive. Some of the best email software clients are free. Even the most costly programs are low-priced and come with many free upgrades.
- Casual. While personal and professional etiquette still apply, email is generally less formal than other types of written communications.
- Flexible. Emails can be formatted as simple text, rich text or HTML.

However, because it is widespread, flexible and easy to use, email is a great source of abuse. On the negative side email can:

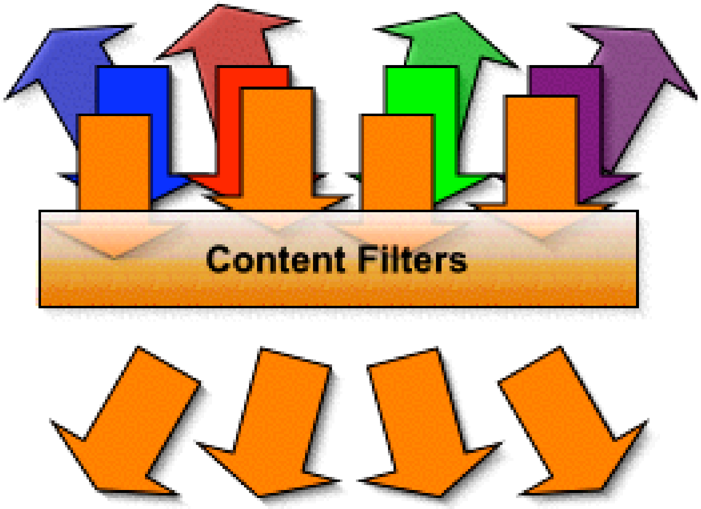
- Distract people from their main job by generating dozens to hundreds of emails daily.
- Reduce workplace efficiency because of too many personal emails sent and received on the job.
- Provide an open door for advertisers to "spam" users with promotional emails; including many offensive messages.
- Help malicious users spread computer viruses.
- Waste bandwidth because of huge attachments.
- Create confusion when senders unknowingly omit recipients from a list.
- Aid corporate theft by enabling unethical employees to send company information to competitors.

If left unmanaged, the negatives of email communications can overcome many of its benefits.

Filtering Email

Email filtering operates as a sieve and re-distribution system. It is one way to regulate the flow of messages in, through, and out of email boxes.

In some aspects, filtering email is similar to filtering air or water, at least in theory. Physical filters screen out pollutants and pass only pure content. In many cases, a well designed water or air filter can be 98 percent effective or better. Since email is neither air nor water, the analogy to filtering gases and liquids is imperfect. For one thing, with email, filtering out the bad and letting in the good is more difficult. In fact, sometimes an email filter can accidentally eliminate the positive along with the negative. Because of this, email filtering often requires fine tuning plus balancing the benefits against the risks for any filter.



Consider the example of virus-infected HTML, the web's Hypertext Markup Language. This type of security nuisance could arrive as HTML-formatted email or as a simple text message with an HTML attachment. HTML can potentially carry damaging scripts that can automatically execute when opened. One sure and effective way to abolish such a security threat is to filter out all HTML mail. But this would also obliterate the many legitimate emails formatted with HTML. A more subtle approach might block HTML messages and attachments only if they contain scripts. Or the filter could reject scripted HTML only from sources outside the company. Each refinement lets more HTML mail pass, but also may increase potential security risks . The same type of balancing could be applied to blocking unsolicited advertising, also known as spam. A filter can block and pass email by many different criteria.

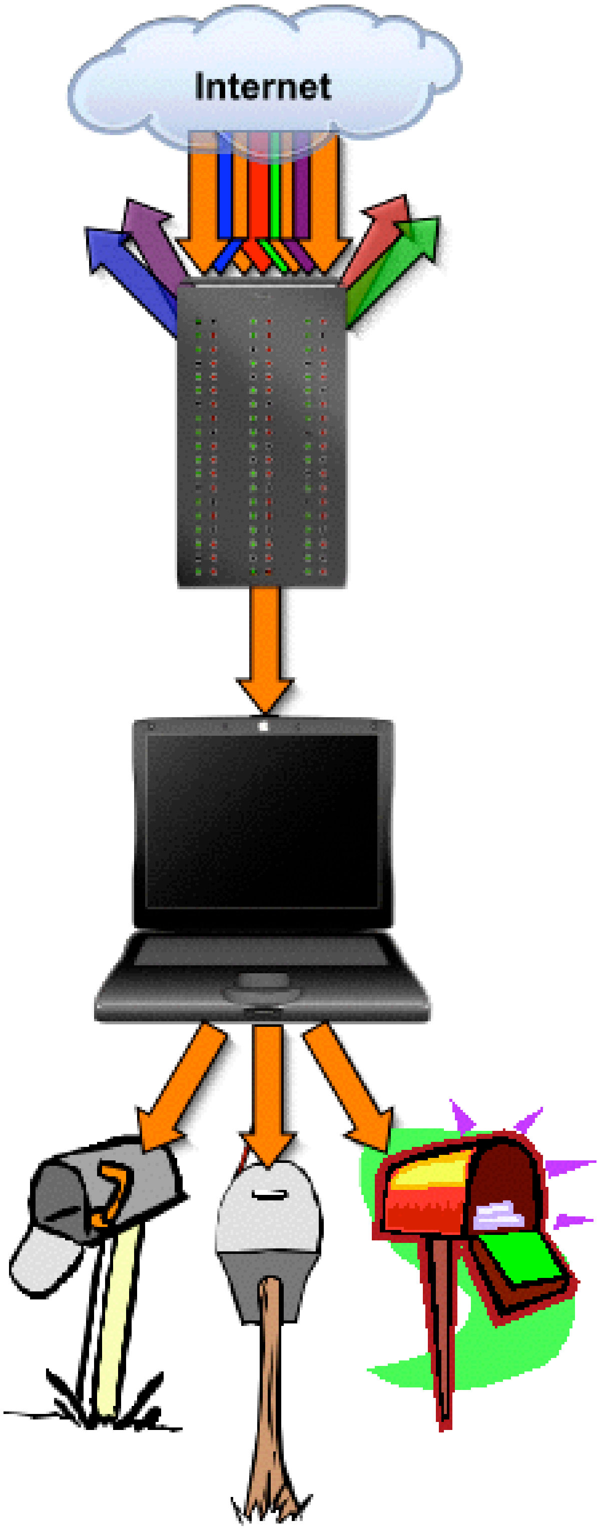
Filtering, however, does much more than protect against viruses and other pollutants. It can also:

- Redirect email from one address to another.
- Automatically reply to specific types of mail.
- Re-distribute a single email to multiple addresses.
- Attach notes to the bottom of an email.
- Remove and add attachments.
- Notify email administrators about Internet email servers that host spam content providers.
- Any combination of these and more.

The illustration shows blue, red, green and purple messages being filter out and orange messages being passed through.

Designing Filters

Many email clients come with filtering capabilities. The power of the filtering varies with the client. Some filtering tools enable simple distribution to mail folders on the user's machine, determined by the email sender, subject or content, for example. Other implementations add more complex content-based responses such as redirection to one or more recipient, auto replying, bouncing mail to the sender, attachment stripping, virus blocking, appending words to the subject and adding notes to the message text, to name a few.



However, surveys show most users seldom apply any filters beyond distribution to mail folders. This happens because mail folder distribution is easy to understand and use. The benefit is immediately obvious. On the other hand, filters such as redirecting, bouncing, auto replying and other advanced functions are beyond the interest or abilities of typical users. Therefore, most never benefit from these sophisticated features.

Server-side filtering places filter design and implementation where it belongs, in the hands of information technology professionals. These people can better understand the subtleties of content pattern matching, filtering actions and filter sequence hierarchies, for example. Pattern matching determines if an email gets processed by a filter. Actions control what a filter does. Hierarchies set the deployment sequence when running multiple filters against one message.

Applying filters on the server-side also enables the implementation of consistent email policies at the level of the enterprise or service provider. Server-side filtering passes and blocks specified types of mail before it arrives in user mailboxes or goes out to the Internet. It helps eliminate extraneous, nuisance and infectious messages, both incoming and out going. Filtering also reduces bandwidth usage by cutting down on extraneous emails.

The illustration shows both server-side and client-side filtering.

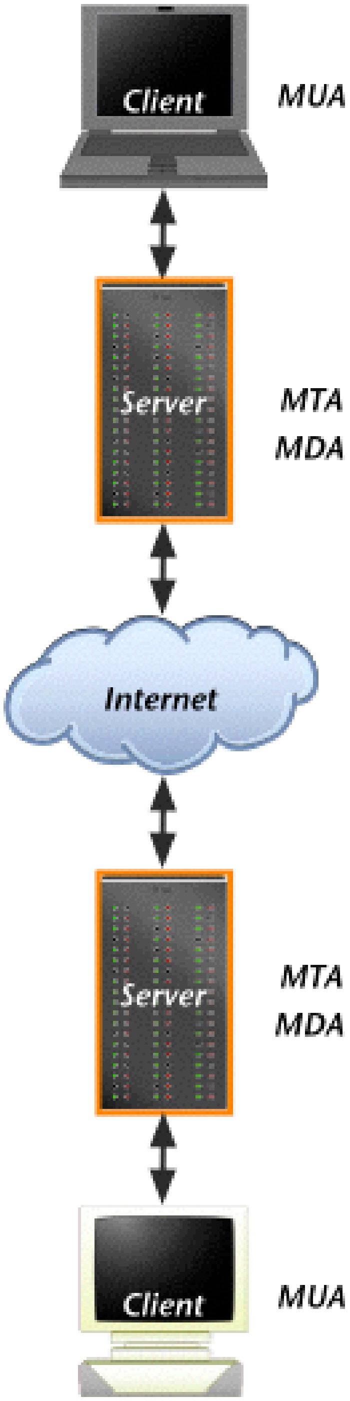
How Server-Side Filtering Operates

Server-side filtering operates as a layer added to normal Internet email processing. Internet email uses three basic types of software:

- Mail User Agent (MUA), more commonly referred to as the email client. This software runs on the users' machines and enables the creating, sending and receiving of emails from the desktop.
- Mail Transport Agent (MTA), better known as the SMTP server because it uses the Simple Mail Transfer Protocol. This software runs on server machines and transports email between MUA's. An email typically goes through two MTA's -- one local to the sender and the other local to the receiver -- when sent from one email client (MUA) to another.
- Mail Delivery Agent (MDA), also known as the email server. This software runs on a server, along with the MTA. It is local to the recipient's MTA and delivers email to local mailboxes, when called by the MTA.

Filtering takes place in the MDA after the mail is queued for delivery and prior to it being sent to individual mailboxes.

The illustration shows email connectivity with filtering occurring in the orange-outlined servers.



MDaemon Content Filtering

There are four parts to MDaemon's content filtering. A fifth part deploys a virus protection program. Virus protection is the topic of a different whitepaper. From an administrator's point of view, the four parts of filtering consist of defining and setting up:

- Content filters.
- Filename matching for restricted attachments.
- Notification messages about attachment removal for the sender, receiver and system administrator.
- Attachment compression rules for saving outgoing and incoming bandwidth.

The Setup Content Filter command provides access to all of these functions.

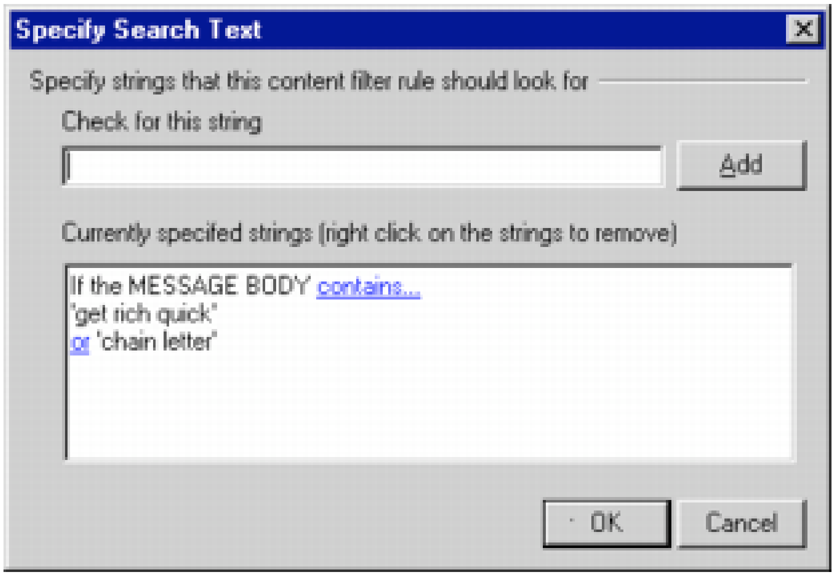
Content Filters

Condition and Action Rules

Content filtering operates with rules comprised of conditions and actions. When an email meets one or more conditions of a rule, one or more of the rule's actions take place. Each rule can include multiple conditions and actions.

Conditions consist of content tests made against an email. Examples of the tests are:

- Header content, such as the name of the sender or the subject of the email
- Message content, such as "join us at the races " or "get rich quick"
- Message size
- Attachment names


Specify Search Text
Specify strings that this content filter rule should look for
Check for this string
Add
Currently specifed strings (right click on the strings to remove)
OK
Cancel

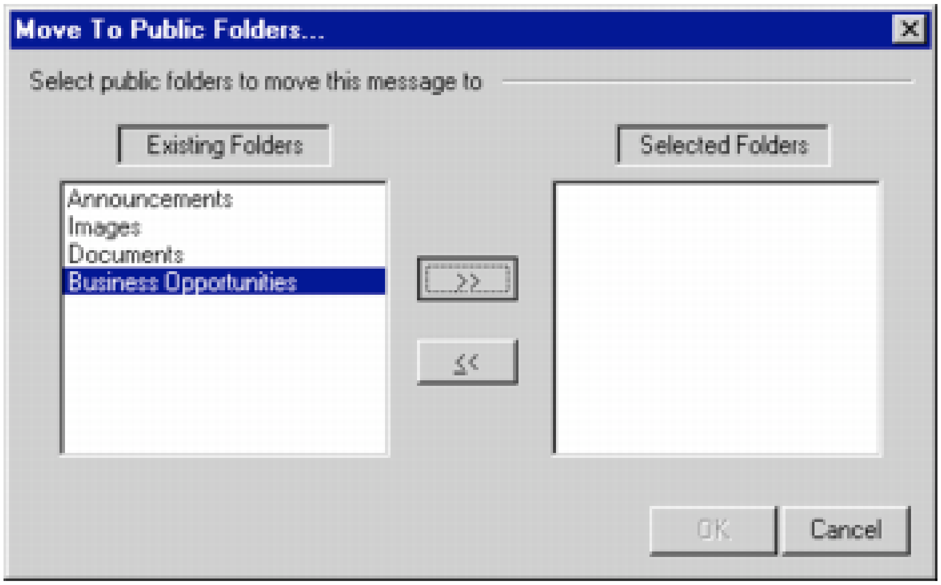
If the MESSAGE BODY contains...
'get rich quick'
or 'chain letter'

Actions are the things MDaemon does with a message when the message matches one or more conditional tests. Examples of actions are:

- Delete the message
- Remove the attachments
- Append a disclaimer to the message

The grouping of conditions and actions within a rule is very flexible. Multiple conditions and actions in one rule can be:

- grouped together for nested testing
- separated for individual testing.

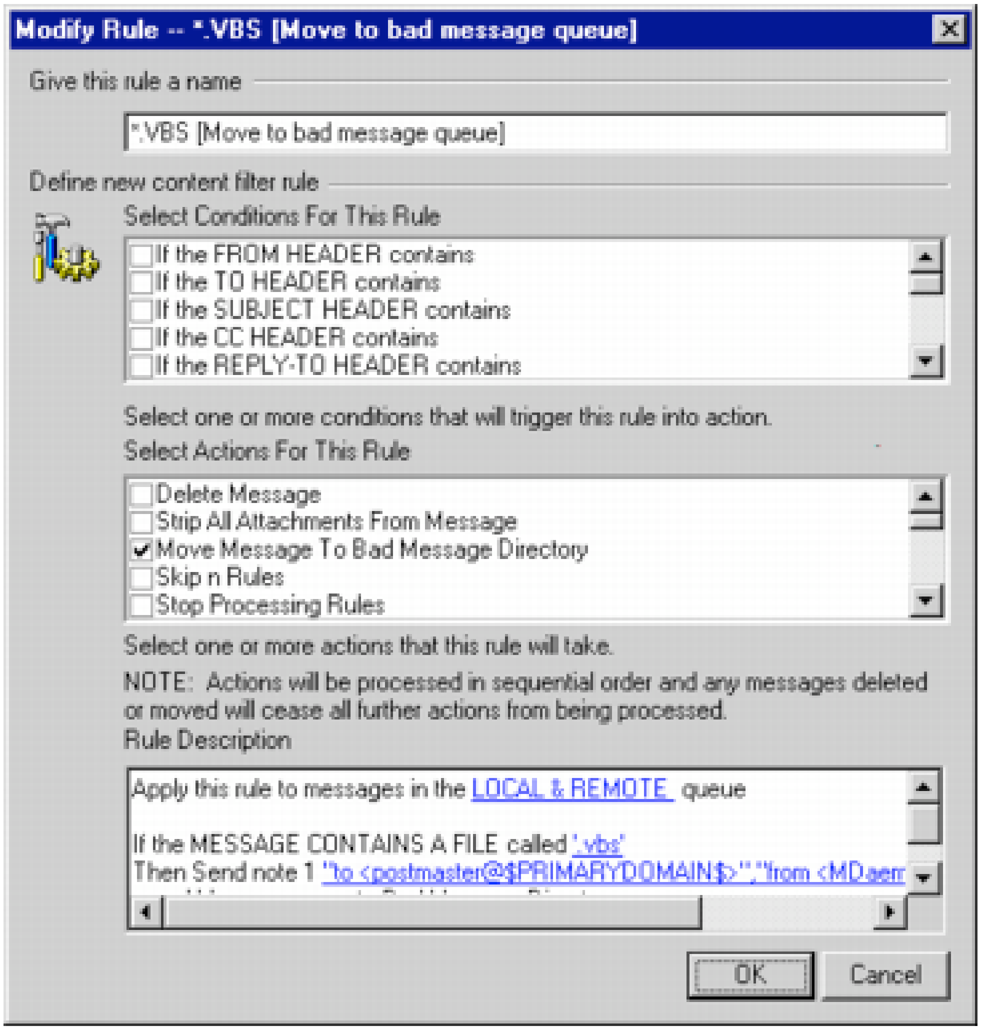

Move To Public Folders...
Select public folders to move this message to
Existing Folders
Selected Folders
>>
<<
OK
Cancel

Announcements
Images
Documents
Business Opportunities

Conditional tests occur in sequence, followed by their actions. Actions, however, can alter the testing sequence by skipping or jumping to tests, for example.

Filter Rule Setup

Setting up rules within a filter is mostly a matter of pointing, clicking and typing some content. The interface to the rule language prevents syntax errors. But the person setting up the rules should understand if-then logic.



Modify Rule -- *.VBS [Move to bad message queue]

Give this rule a name

*.VBS [Move to bad message queue]

Define new content filter rule

Select Conditions For This Rule

- □ If the FROM HEADER contains
- □ If the TO HEADER contains
- □ If the SUBJECT HEADER contains
- □ If the CC HEADER contains
- □ If the REPLY-TO HEADER contains

Select one or more conditions that will trigger this rule into action.

Select Actions For This Rule

- □ Delete Message
- □ Strip All Attachments From Message
- ☑ Move Message To Bad Message Directory
- □ Skip n Rules
- □ Stop Processing Rules

Select one or more actions that this rule will take.

NOTE: Actions will be processed in sequential order and any messages deleted or moved will cease all further actions from being processed.

Rule Description

Apply this rule to messages in the LOCAL & REMOTE queue

If the MESSAGE CONTAINS A FILE called '.vbs'
Then Send note 1 "to <postmaster@$PRIMARYDOMAIN$>","from <MDaem

The rule dialog box controls rule editing. The dialog has four sections:

- A text box for naming the rule. The user creates the name.
- A list box for selecting conditional tests. You select a condition by clicking on its check box.
- A list box for choosing actions. You select an action by clicking on its check box.
- A read-only text box showing the content of the rule. The content of this text box changes as the user adds, changes and deletes conditions and actions. While you cannot type directly in this text box, you can edit any underlined item by clicking on it.

Conditions and actions occur in the sequence the user chooses them from the list boxes.

Example Rule

These instructions show the process of rule setup. The example rule may or may not be suited for a particular purpose. If you use this rule in production, you're on your own.

The example instructions start on the Create Rule dialog.

1. Type **No Outside Scripts** in the *Give this rule a name* text box.
2. Scroll down in the *Select Conditions for this Rule* list box and activate the check box next to **If the MESSAGE HAS A FILE called**.
3. Notice the entry in the read only *Rule Description* text box at the bottom of the dialog. This text box contains the content of the rule.
4. Click on **specific file name** in the *Rule Description* text box. This displays a dialog for entering a filename specification.
5. Type ***.vbs** to test for visual basic script attachments and press **Enter**. File naming wild cards, such as "?" and "*" are permitted in the filename specification.
6. Scroll down in the *Select Conditions for this Rule* list box and activate the check box next to **If the FROM HEADER contains**.
7. Notice the entry in the *Rule Description* text box now shows two tests: the first test AND the second test.
8. Click on **contains specific string** in the *Rule Description* text box. This displays a dialog for editing the FROM HEADER test.
9. Click on **contains** following FROM HEADER. This displays a dialog for changing the contains option.
10. Select **Does Not Contain** from the drop down list box and press **Enter**.
11. Type **company.mail** in the **Check for this string** list box and click on the **Add** command button.
12. Click on the **OK** command button.

    So far the rule says, roughly: "If you receive an email from outside the company and the email has a visual basic script attached....

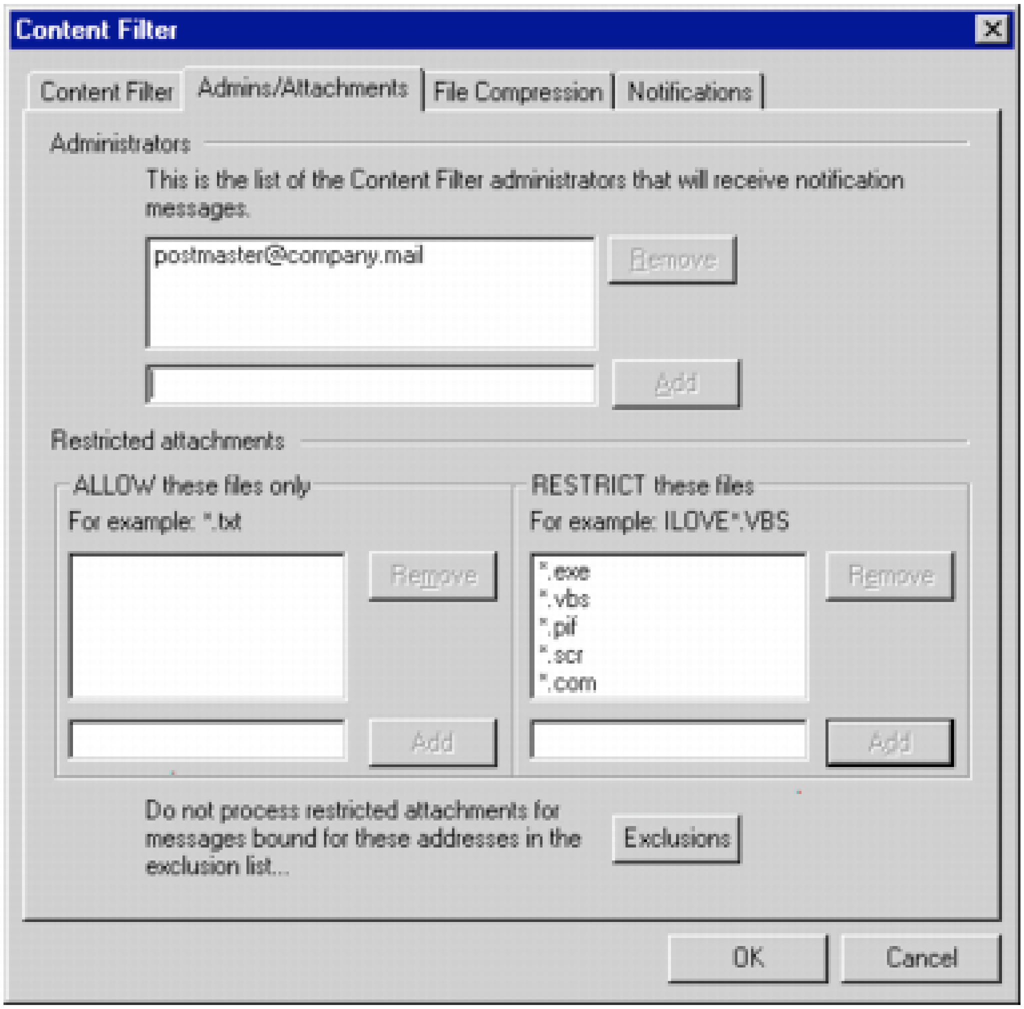
    Next the rule will delete the attachment. No questions asked.
13. Scroll down in the *Select Actions for this Rule* list box and activate the check box next to **Strip All Attachments From Message**.
14. Notice the change in the *Rule Description* text box.
15. Click on **specify information**, select **Yes** from the dialog and press **Enter**.
16. Click on the **OK** command button.

While it would be polite to notify the sender and receiver of the deletion, this example rule does not do that.

When setting up rules you can edit any item underlined in the *Rule Description* text box.

Restricted Attachments

Filtering out attachments is the best single way to avoid viruses, cut down on wasted bandwidth and keep employees focused on work rather than cute multimedia presentations, for example.



This is the list of the Content Filter administrators that will receive notification messages.

postmaster@company.mail

ALLOW these files only

For example: *.txt

RESTRICT these files

For example: ILOVE*.VBS

*.exe
*.vbs
*.pif
*.scr
*.com

Do not process restricted attachments for messages bound for these addresses in the exclusion list...

Content Filtering's Admins/Attachments tab allows you to delete incoming attachments without setting up specific rules.

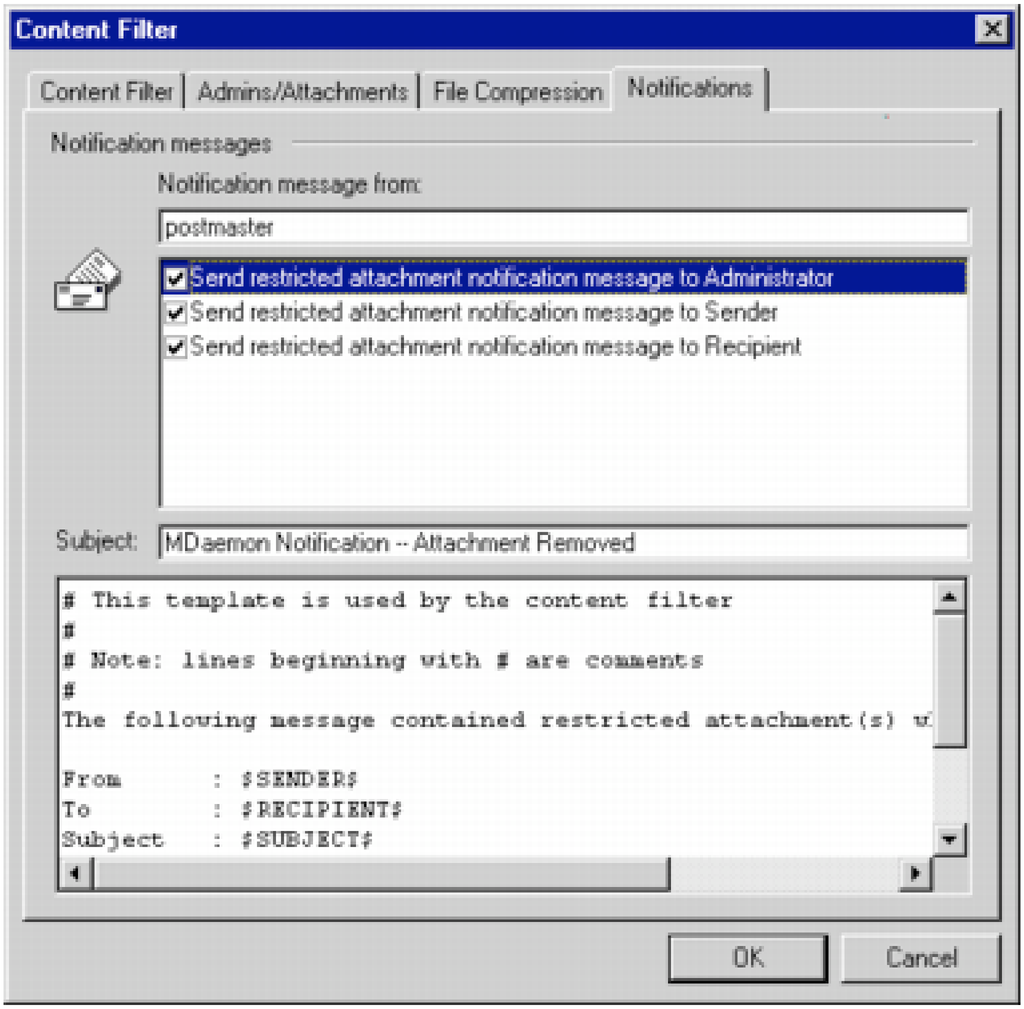
This tab allows the administrator to specify:

- Filename matching patterns for attachments to block.
  Note: Entering *.exe, *.com, *.pif, *.scr and *.vbs, to block all attachments ending with these extensions, would go a long way toward eliminating the spread of viruses.
- Email address to notify when an attachment is blocked. These are administrator addresses only.
- Filtering exclusions. For example, if you want to allow the emailing of scripts from IT to the internal users, you might allow script attachments from support@company.mail.

Notification

Education helps eliminate unwanted email attachments within an enterprise or service provider environment. While Content Filtering can strip attachments and say nothing of it, it can also be set up to send notifications of the event to the sender, receiver and mail server administrator. The Notification tab in the **Content Filtering** dialog has options for specifying who receives a explanatory message and what the message contains. Items on the tab are:

- A text box for entering the name of the account sending the notification message. This account name appears in the *From* section of the email.
- A list of check boxes for selecting who receives the email. The options are the sender, the receiver and the administrator.
  Note: This part of the tab can also include options for notifying the sender, receiver and administrator of blocked viruses. These options appears only if the DVAK virus protection software is installed and enabled.
- A text box for entering the subject of the message sent. For example: **MDaemon Notification -- Attachment Removed**. This subject can be unique for each enabled message.
- A text box for setting up the content of the notification email. This content can include specific details taken from the blocked email.



Notification message from: postmaster

☑ Send restricted attachment notification message to Administrator
☑ Send restricted attachment notification message to Sender
☑ Send restricted attachment notification message to Recipient

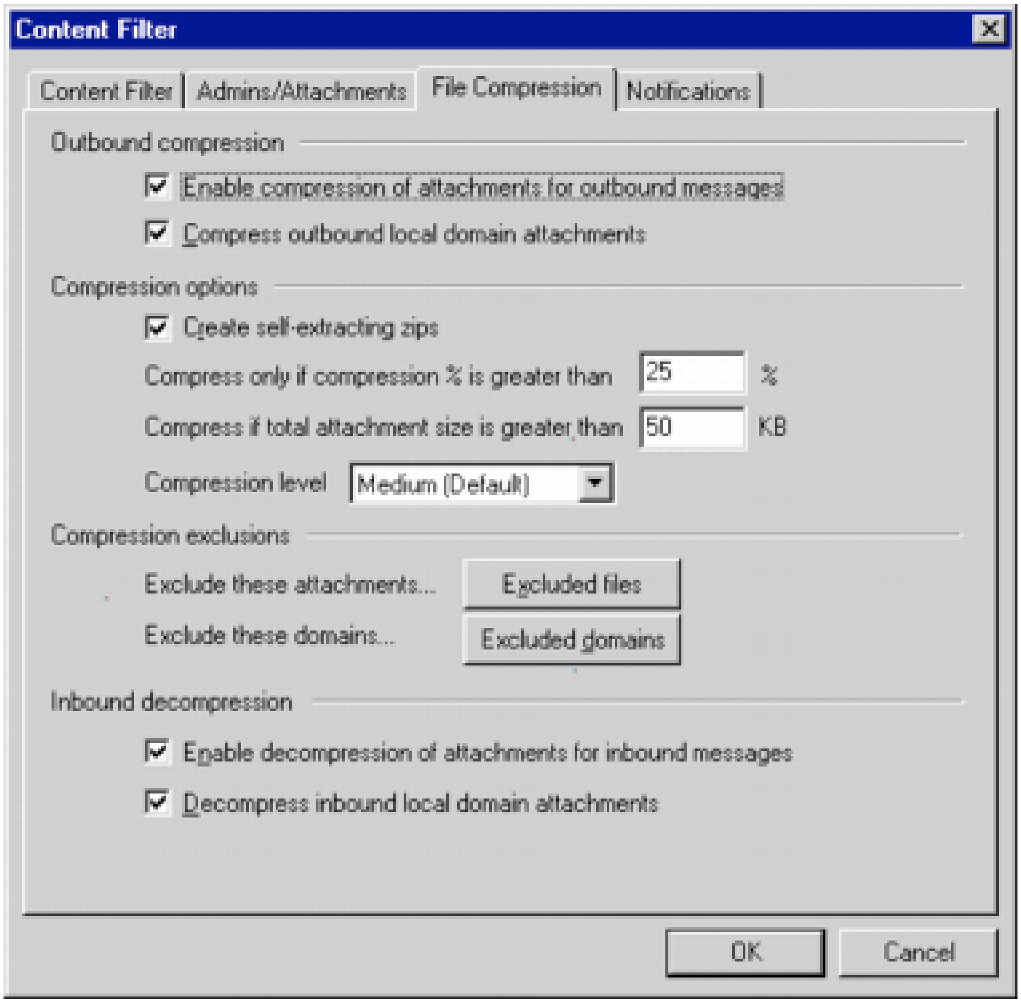
Subject: MDaemon Notification -- Attachment Removed

```
# This template is used by the content filter
#
# Note: lines beginning with # are comments
#
The following message contained restricted attachment(s) w

From       : $SENDER$
To         : $RECIPIENT$
Subject    : $SUBJECT$
```

File Compression

Compressing attachments saves bandwidth, both when sending and receiving emails. However, compressing also uses the processing resources of the email server. MDaemon Filtering can optionally compress attachments depending on their source, destination, size and compressibility. If an administrator decides to use file compression, these options help balance processing time consumed and bandwidth saved.



Outbound compression

☑ Enable compression of attachments for outbound messages

☑ Compress outbound local domain attachments

Compression options

☑ Create self-extracting zips

Compress only if compression % is greater than 25 %

Compress if total attachment size is greater than 50 KB

Compression level Medium (Default)

Compression exclusions

Exclude these attachments...

Exclude these domains...

Inbound decompression

☑ Enable decompression of attachments for inbound messages

☑ Decompress inbound local domain attachments

The File Compression tab built into the Content Filter dialog contains controls for determining what, if anything, to compress. The compression options are:

- Outbound Compression. These check boxes turn compression on or off for the local domain and for outside destinations.
- Compression Options. These options include:
  - > A check box for choosing to create auto-extracting compression files. These files automatically decompress when the receiver opens them.
  - > A text box for entering a compression percentage threshold. If compressing will reduce the file size by less than the specified amount, MDaemon skips the attachment and sends it uncompressed. This is useful, for example, if the user is sending graphics files, which are

normally compressed already. The time spent compressing the file would likely use more resources than the bandwidth consumed in sending the file uncompressed.

> A text box for entering the minimum size file to compress. Compressing a small file is another case where processing consumption may cost more than bandwidth savings. This option allows the administrator to skip small files.

> A drop down list box for setting the level of compression to minimum, medium or maximum. Maximum compression creates smaller files, but consumes more processing power and time.

Compression Exclusions. The administrator can set compression exceptions by file type and domain. As a file type example, entering *.jpg, *.png and *.tiff, would cause file compression to always skip these type of graphics attachments. Entering *theartgroup.com* as a domain exception would turn off compression for all attachments from this domain.

Macros for Messages

Content Filtering contains a tool for sending personalized and detailed messages from within any content filtering rule. This feature adds a nice touch of humanity to rules processing. It allows the administrator to notify the sender, receiver and anyone else about filtering actions, including details of what happened and why. These additional messages can be sent separately or appended to a filtered message.

Including the details of the filtering action is possible because of processing "macros" built into MDaemon. These macros take content from the filtering action, change it into text and place it in a new message.

Consider the example of an email received from an external source. It contains an attachment, as is normal from this source. Rather than sending this to dozens of people in the company, the external source uses the email address: publictechgroup@company.mail. Filtering on the "to" and "from" sections of the external message, MDaemon routes the message and attachment to a public email folder and sends this notification to selected users:

> You have received a message from $SENDER$. The subject of the message is $SUBJECT$. It contains one or more attachments. You will find the message and attachments in your #TechGroup public folder. The message was place in the public folder at $CURRENTTIME$. For you geeky types the filename of the message is $MESSAGEFILENAME$. This message was brought to you by the MDaemon Content Filter $FILTERRULENAME$. Goodbye.

$SENDER$ and $SUBJECT$ in the message are replaced by the "From" and "Subject" content of the original message. $CURRENTTIME$ shows the processing time of the filtering action. The filename of the message stored in the public folder is $MESSAGEFILENAME$. $FILTERRULENAME$ tells which filtering rule sent the message.

These and other macros enable the generation of detailed and personalized messages from an automated process. When carefully employed, the macros can help improve email within an enterprise or service provider.

Other Blocking Options

Beyond the scope of content filtering, MDaemon has tools for blocking messages by user name, IP address and domain. These features are described in the Spam Blocking white paper.

Conclusion

Content filtering on the server side makes sure filtering gets done. Generally speaking, technical people understand filtering rules better than everyday users. The filtering facilities of MDaemon are diverse, fluid and easy to learn. Senders, receivers and administrators can be notified of filtering actions by using personalized and detailed messages. Filtering can reduce email delivery costs by eliminating undesirable messages and cutting down on bandwidth usage.