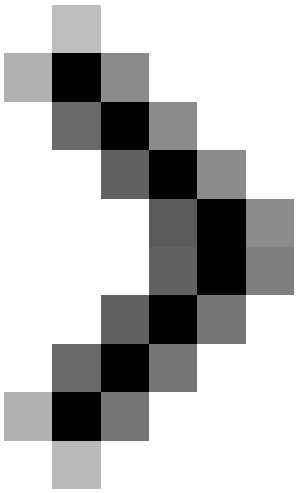
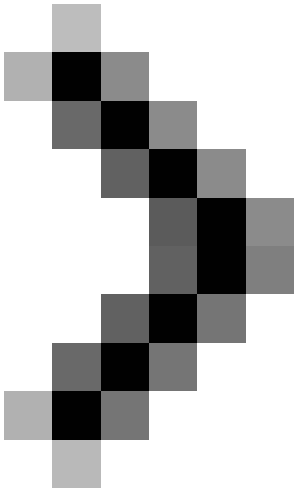
Install and configure email handling solutions on TMG 2010 Firewall - Part 4

In Part 4 of this series, I will show you the virus and content filtering features on TMG 2010 Firewall.

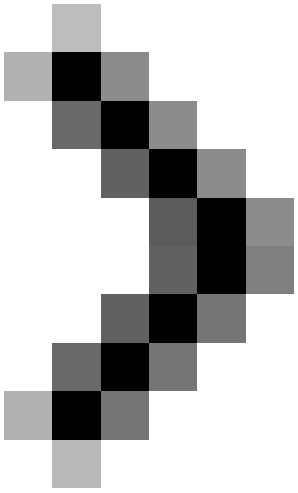
Network Administration **- In Part 4 of this series, I will show you the virus and content filtering features on TMG 2010 Firewall.**



Install and configure the solution to handle email on TMG 2010 Firewall - Part 1: Installation



Install and configure email handling solutions on TMG 2010 Firewall - Part 2: E-Mail Policy



Install and configure email handling solutions on TMG 2010 Firewall - Part 3: Anti-spam
In Part 3 of this series, I showed you how to configure the anti-spam feature on the TMG email handling solution. This part 4 will continue with the introduction of content and virus filtering features.

Content filtering and virus

In the TMG firewall console, click **Email Policy** on the left pane. In the middle pane of the interface, click the **Virus and Content Filtering** tab. You will then see three options for content filtering to protect TMG's email. That is:

- **File Filtering:** This option allows you to control attachments, which attachments are allowed to enter and exit the email system in your network.
- **Virus Filtering** : This option allows locking, preventing malware from entering and leaving the email system.
- **Message Body Filtering** : This option allows you to control incoming and outgoing email based on their content.

In the image below, you can see two links indicating that Content Filtering and Virus Filtering features are enabled.

Figure 1

Filter files

Let's start with the File Filtering option. Click the **File Filtering** link in the middle pane. In the **File Filtering** dialog box, you will see the **File Filters** tab. Here you can configure file filters to block incoming and outgoing attachments. Click the **Add** button, as shown in Figure 2 below.

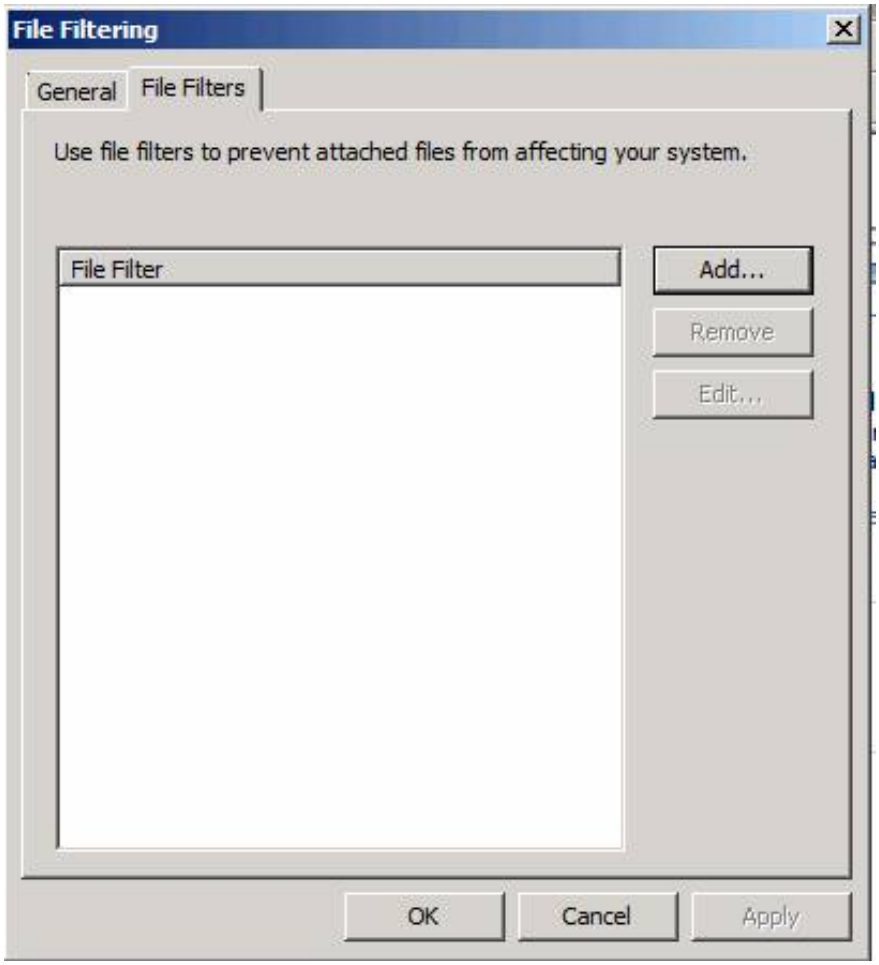


Figure 2

You will see the **File Filter** dialog box. On the **General** tab, you can choose the following options:

- **Enable this filter** : This option works to enable or disable the filter.
- **Filter name** : This option allows you to enter the name of the filter you are creating.
- **Hành** ??ng **cho thông báo h?p l? này này:** This option allows you to choose between the following actions: **Skip, Identify, Delete** and **Purge** . The **Skip** option checks the message and writes an entry if it is valid for the filtering criteria, but then forwards the message to the next destination. The **Identify** option attaches to the subject line a custom word, which can be used for inbox filtering. The **Delete** option will delete the message and **Purge** will remove the message from the system.
- **Scan inbound messages** : When you enable this option, TMG will inspect incoming messages in the organization.
- **Scan outbound messages:** When this option is enabled, TMG will inspect messages sent from the organization.

The options in the General tab are shown in Figure 3 below.

Figure 3

Click the **File Types** tab. Here you can control the type of file to be inspected. When the system detects a certain file type selected for inspection, the action you configure on the **General** tab will be executed. Note that this is a feature of Forefront Protection for Exchange (FPE), so the detection for file types is real, not just file extensions. That's a pretty interesting thing because the files can be renamed to indicate that the extension is different from what it really is. You can see the File Types tab in Figure 4 below.

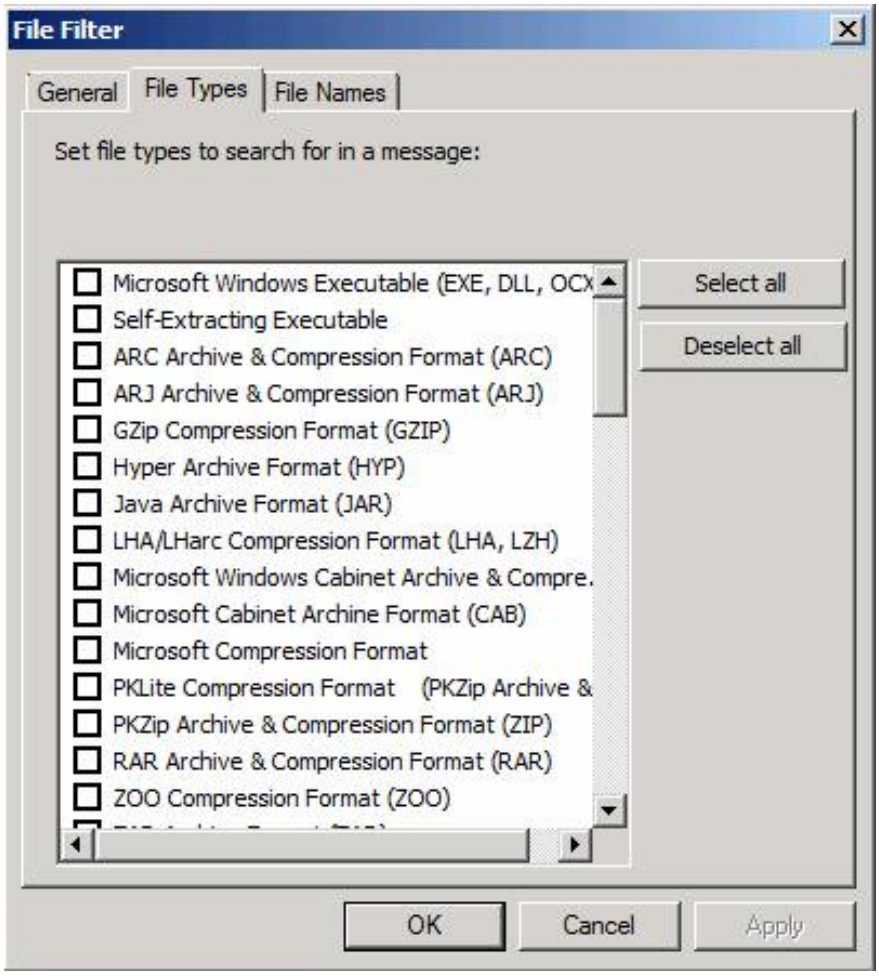


Figure 4

Next, click the **File Names** tab. Here you can configure the file name so that the system will search in email attachments. You can enter the full file name, or you can use wildcards like '?' and '*'. '?' This is used to replace a certain character in a string, and '*' is used to replace certain unknown characters. The File Names tab is shown in Figure 5.

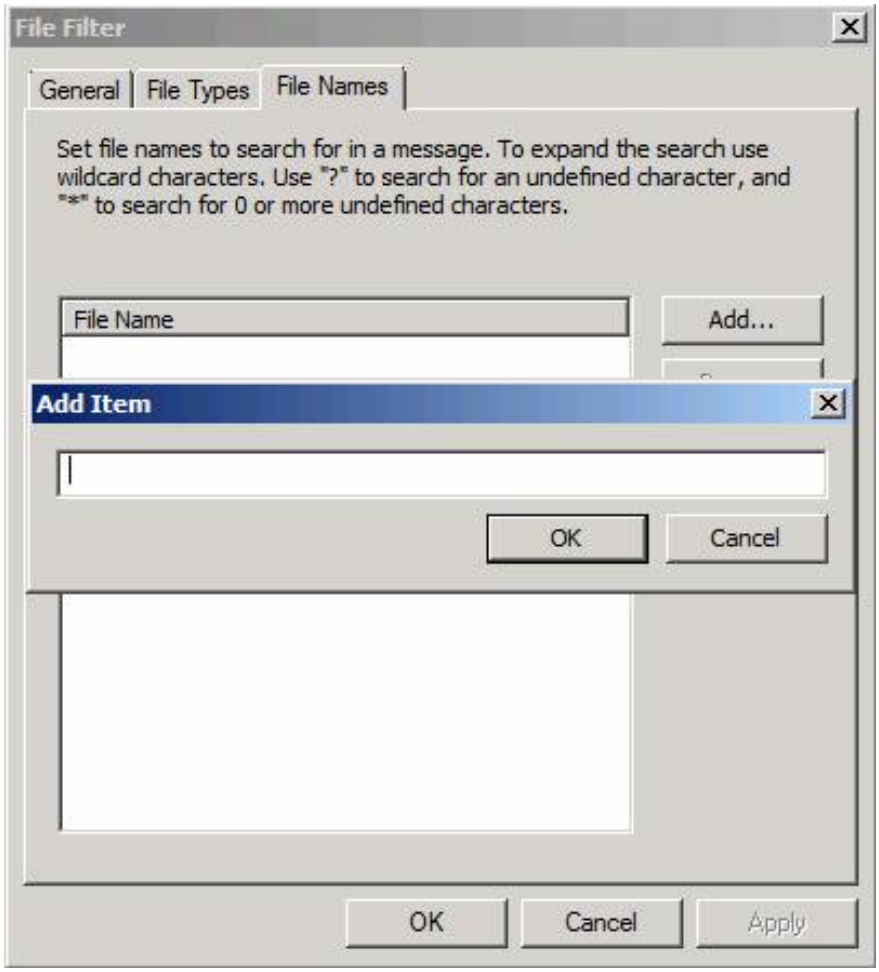


Figure 5

See page 2 **: Antivirus configuration**

Antivirus configuration

Let's take a look at the email Antivirus configuration on the TMG firewall. Click the **Virus Filtering** link in the middle pane of the console. There are many benefits to using many antivirus engines: increasing the ability to catch new threats even without all the machines being updated to this emergency threat, and providing caution in in case a machine has trouble or is not updated promptly, other machines can still add work to it. You can activate up to 5 different machines. Note that the more machines you have, the better, but you'll pay for performance.

The first tab we will work with is **Engines** . In this tab we have the following options:

- **Use automatic engine management:** When choosing this option, FPE will decide which antivirus engine to use and how they are used.

- **Manually enable up to 5 engines:** Select this option if you want to control which machines are used and control the policy of choice used for machines. When selecting this option, you must select one or more antivirus engines from the list.
- **Always scan with all selected engines:** When choosing the desired antivirus engine, you need to define a smart choice policy (Intelligent Engine Selection Policy). When selecting **Always scan with all selected engines,** FPE will scan messages with all selected machines.
- **Scan with a subset of engines that are available:** A machine available (available) is a machine that is not in an upgrade state. When a machine is being upgraded, it will be marked as unavailable, so when this option is selected, the system will not wait for all available machines before completing the mail check. . All available machines will be used when you select this option.
- **Scan with a selected** selection **of engines:** this option uses evaluation methods based on recent results and statistical projects to select which machines are used to scan mail.
- **Scan with only one of the selected engines:** This option also uses evaluation methods based on recent results or statistical projects to select *a* machine used for scanning.

You can see all of these options in Figure 6:

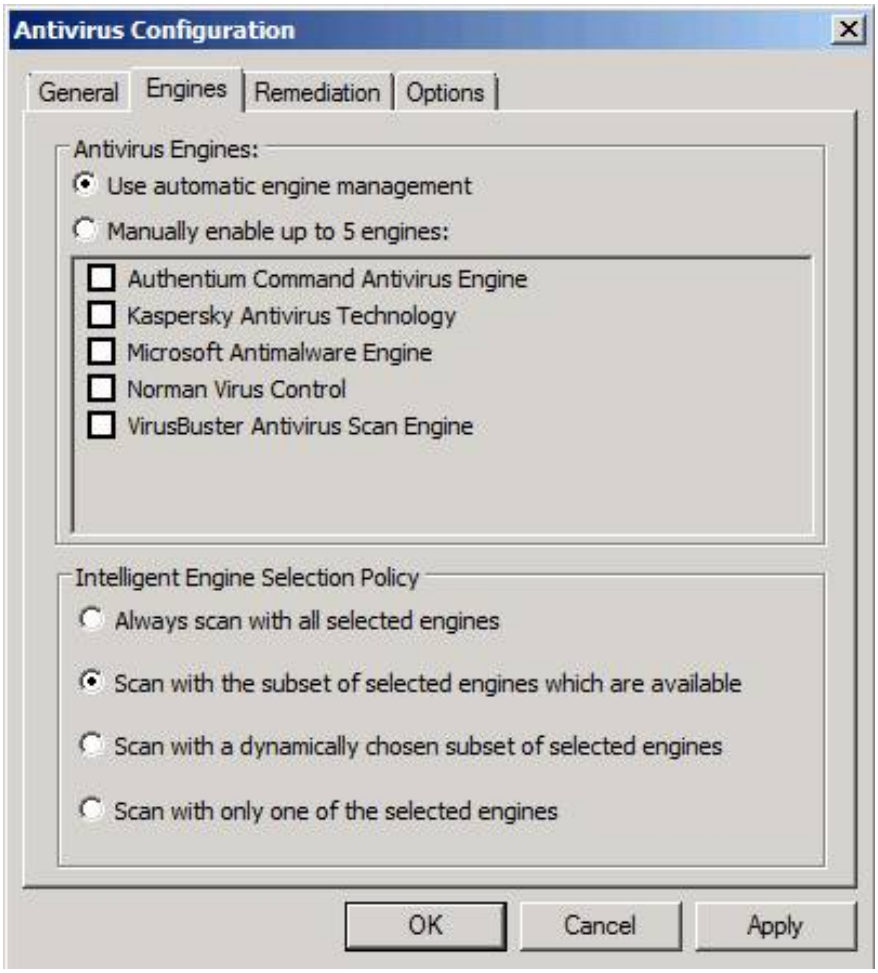


Figure 6

Click on the **Remediation** tab. On this tab we have the following options:

- **Skip (detect only):** This option detects and reports a virus, but it still forwards the message, with malware, to the next door. This is clearly not a beneficial option.
- **Clean (repair attachment):** This option will try to clean the attachments and then distribute this cleaned attachment to its next destination. If TMG cannot clean certain attachments, it will be removed and another attachment marked with deletion will be integrated into the message.
- **Delete:** This option will delete an infected attachment and a deleted file will replace the infected attachment.
- **Enable:** This option allows the file to be deleted, which is a .txt file containing the delete confirmation text you entered earlier.
- **Deletion Text:** This is information that is integrated into the deleted text file. The% File% entry will be replaced by the name of the deleted file.

You can see this dialog in Figure 7.

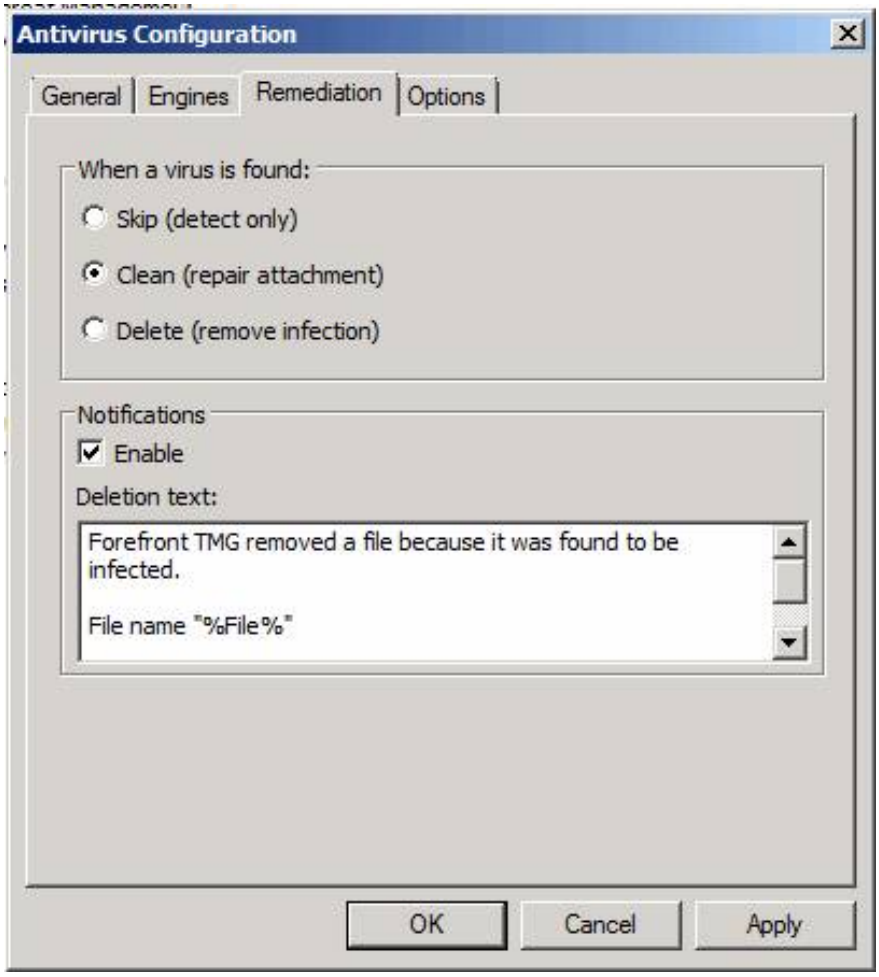


Figure 7

Finally, click the **Options** tab. This is a tab with the following options:

- **Scan doc files as containers:** You can set this option to scan .doc files that use OLE embedded data as a container file so that embedded files are also scanned.
- **Container scanning timeout (seconds):** The default timeout time is 120 seconds for a file scan, but you can change this value here.
- **Hành** ??ng ?? th?c hi?n khi th?c hi?n **th?i gian t?o Scanner:** Here you can choose the action to take when you reach the timeout limit.
- **Action to perform for illegal MIME headers:** Here you can choose what action to take if you find a title that seems to be invalid (for example, filtering or deleting).
- **Transport sender information:** This setting determines how to transmit the **sender's information** .
- **Purge message if body is deleted:** By default, messages will be purified if a virus is detected in their body.
- **Optimize for performance (not rescan message):** By default, mail will not need to be re-scanned after filtering. This helps increase performance but you can change it here.

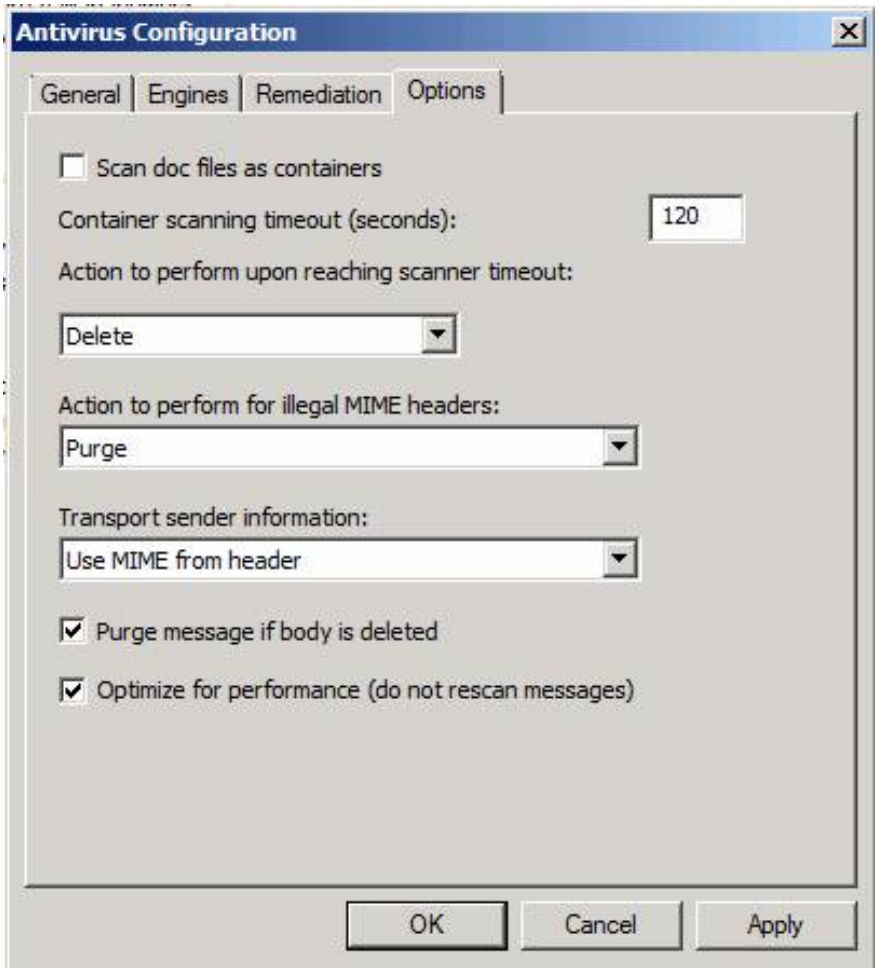


Figure 8

See page 3: **Filter content in the body (Body) email**

Filter content in the body (Body) email

Click the **Message Body Filtering link** in the middle pane of the console. In the **Message Body Filtering** dialog box, click the **Message Body Filters** tab. Click the **Add** button. You will now see the **Message Body Filter** dialog box shown in Figure 8 below. On the **General** tab, you have the following options:

- **Enable this filter:** This option will activate the filter you are creating
- **Filter Name:** Allows you to name to distinguish filters.
- **Hành** ??ng **cho thông báo h?p l? này này:** Allows you to select **Skip** actions, **Identify** , **Delete** and **Purge** . **Skip** will check the message and write whether it is valid or not, but then it will forward it to the next destination. **Identify** will append the subject line a custom word used for inbox filtering. And **Delete** will delete the message, **Purge** will remove the message from the system.
- **Scan inbound messages** : When enabled, this option will configure FPE to scan messages sent to your organization.
- **Scan outbound messages:** When enabled, this option will configure FPE to scan messages sent out of your organization.

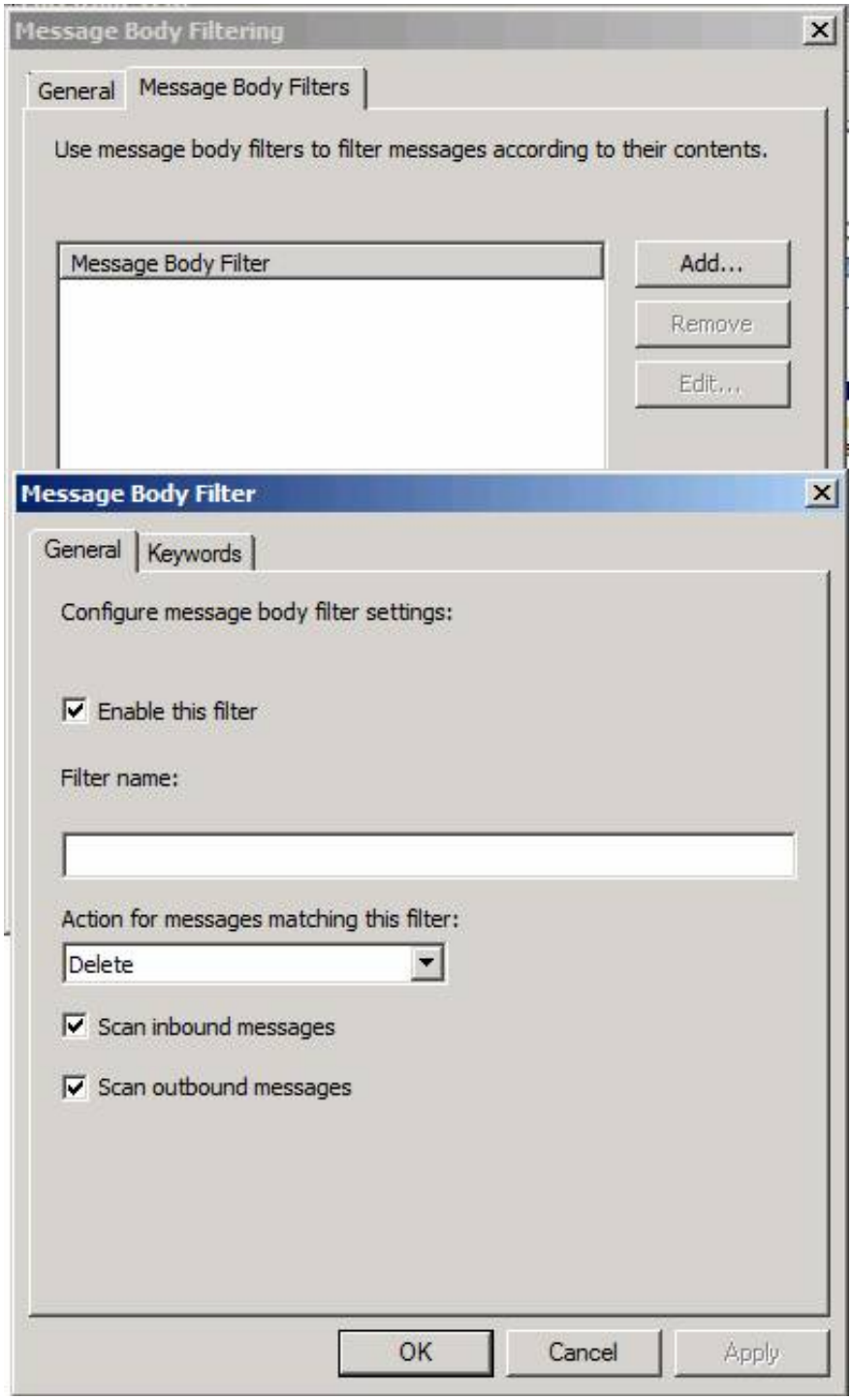


Figure 9

Click the **Keywords** tab in the **Message Body Filters** dialog box, as shown in Figure 10. Here you can define keywords for checking within the body of the message. Can use discrete words or can take advantage of the keyword list syntax rules, acting as the content queries of the message. The query syntax is quite complicated, but the TMG firewall team did a good job in detailing how to build these queries, completely through examples. You can check their instructions here.

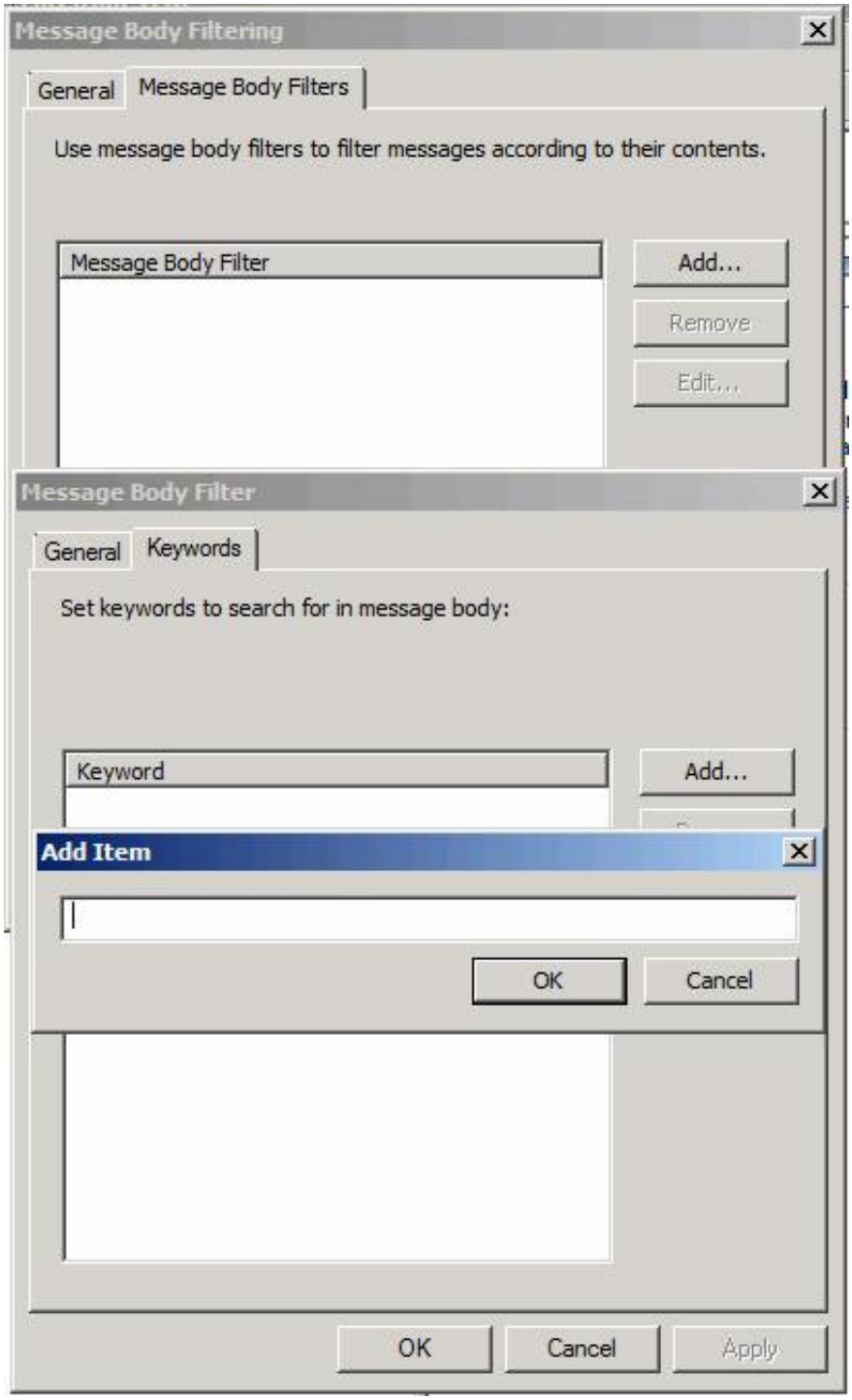


Figure 10

Conclude

In this section, I have explained the Virus Filtering and Content Filtering options. Using TMG, you can lock incoming and outgoing mail containing malware; or messages that contain content within the subject or body of the message that you deem unacceptable. In the next part of this series, we will introduce the procedure used to create the Edge Subscription with the back-end Exchange Server. This is a valuable feature because it allows you

to perform recipient filtering so that it can block certain messages to certain addresses in your organization.