Owner of the content within this article is www.isaserver.org
Written by Marc Grote – www.it-training-grote.de

Configuring and using the E-Mail protection feature in Microsoft Forefront Threat Management Gateway Beta 2 - Part 2

Abstract

In this two part article series, I will show you how to configure the Anti-spam and Anti-Virus protection features in Microsoft Forefront Threat Management Gateway Beta 2.

Let's begin

First, keep in mind that the information in this article are based on a beta version of Microsoft Forefront TMG and are subject to change.

A few month ago, Microsoft released Beta 2 from Microsoft Forefront TMG (Threat Management Gateway), which has a lot of new exiting features.

In this second article, I will show you how Microsoft Forefront TMG acts as Anti-virus and file filtering gateway.

Let's begin

Microsoft Forefront TMG is the first Microsoft Firewall with integrated SMTP proxy functionality and own Anti-virus and Anti-spam functionality. TMG integrates the Exchange Server 2007 Edge Server component which provides most of the Anti-Spam functionality. In addition to the Anti-Spam functionality, TMG also scans e-mail traffic for viruses with a multi-engine antivirus solution where message content is scanned with up to 5 different engines based on Microsoft Forefront Security solutions.

Microsoft Forefront TMG has a new policy node called e-mail policy where all Anti-Spam, Anti-Virus and SMTP route settings are configured as you can see in the following screenshot.

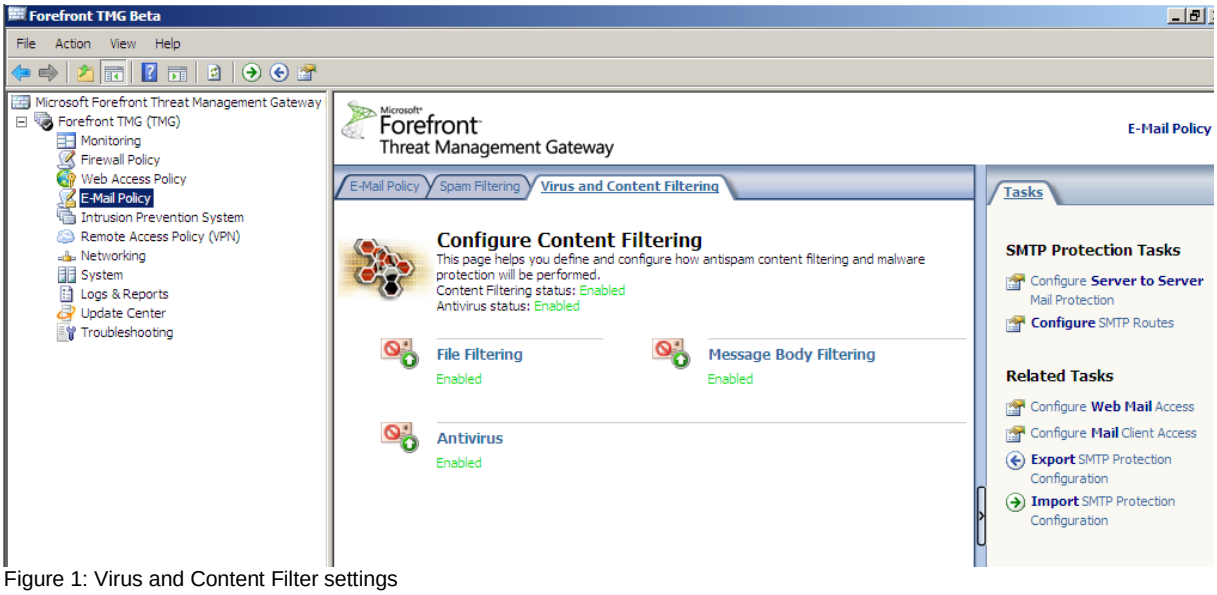

Figure 1: Virus and Content Filter settings

File filtering

Let us start with the File Filtering settings in Microsoft Forefront TMG. With TMG it is much more easier to filter files based on file extension, MIME type and entire file name. It is possible to globally enable or disable File Filtering in Forefront TMG as you can see in the following picture.

Figure 2: Enable file filtering

As a first step you have to give a name to the Filter and to configure the action if a filter matches your policy.

It is also possible to specify if you want to scan inbound and/or outbound messages.

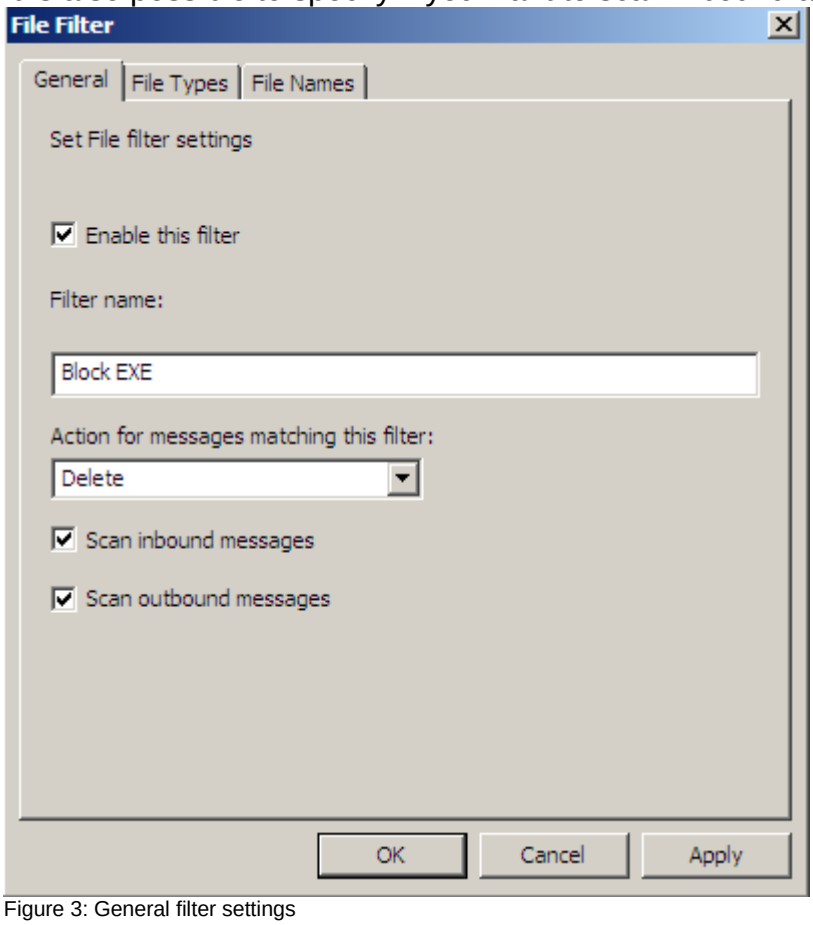

Figure 3: General filter settings

Actions for messages matching this filter:

Delete

Deletes the file attachment. The detected file attachment is removed from the message.

Identify

Tags the subject line or message header of the detected message with a customizable word or phrase so that it can be identified later for processing into folders by user inboxes.

Purge

Deletes the message from your mail system.

Skip

Records the number of messages that meet the filter criteria, but enables messages to route normally.
After the action for message filtering has been selected, you must select the file types you want to filter in messages.

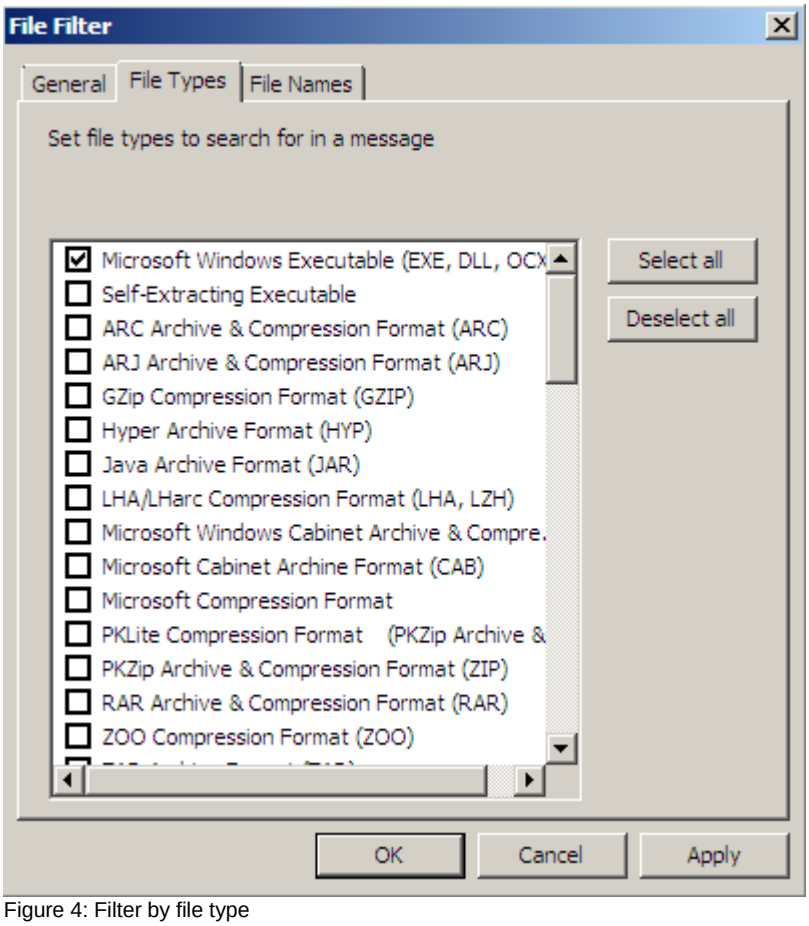

Figure 4: Filter by file type

It is also possible to filter by custom file names. in the following screenshot, I filtered for a file name called dangerous.exe.

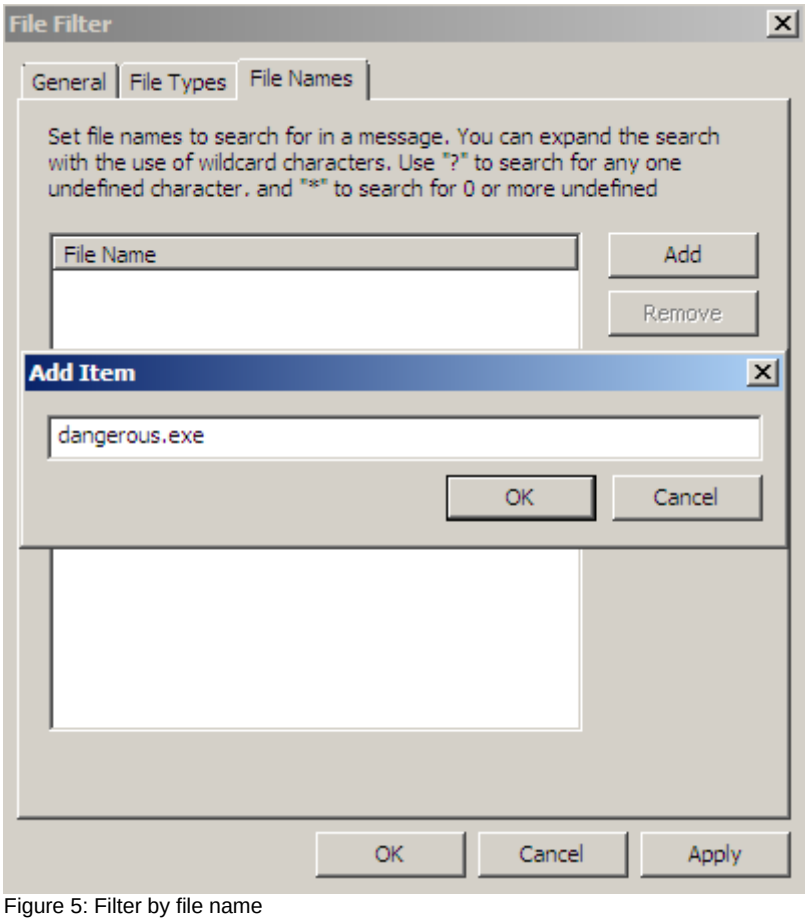

Figure 5: Filter by file name

Message Body Filter

on other option in Microsoft Forefront TMG is to filter content of messages based on keywords in the message body. It is possible to enable and to disable this feature. The filter actions are the same as for the file filter setting feature.

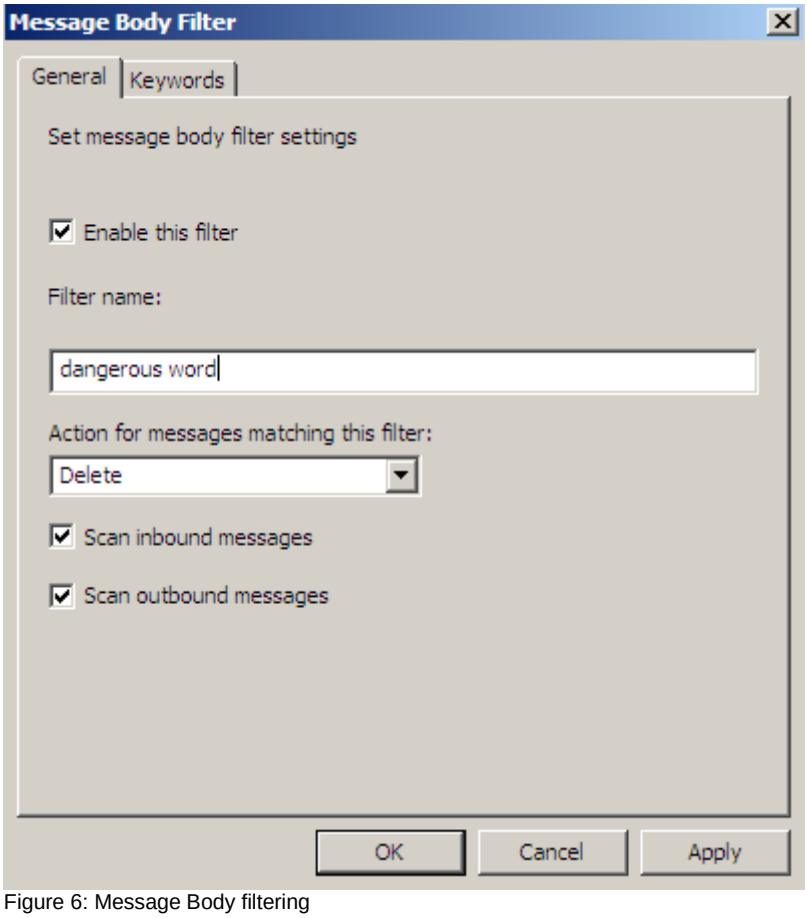

Figure 6: Message Body filtering

As a next step you have to specify keywords that you want to filter if TMG found this keywords in the message body.

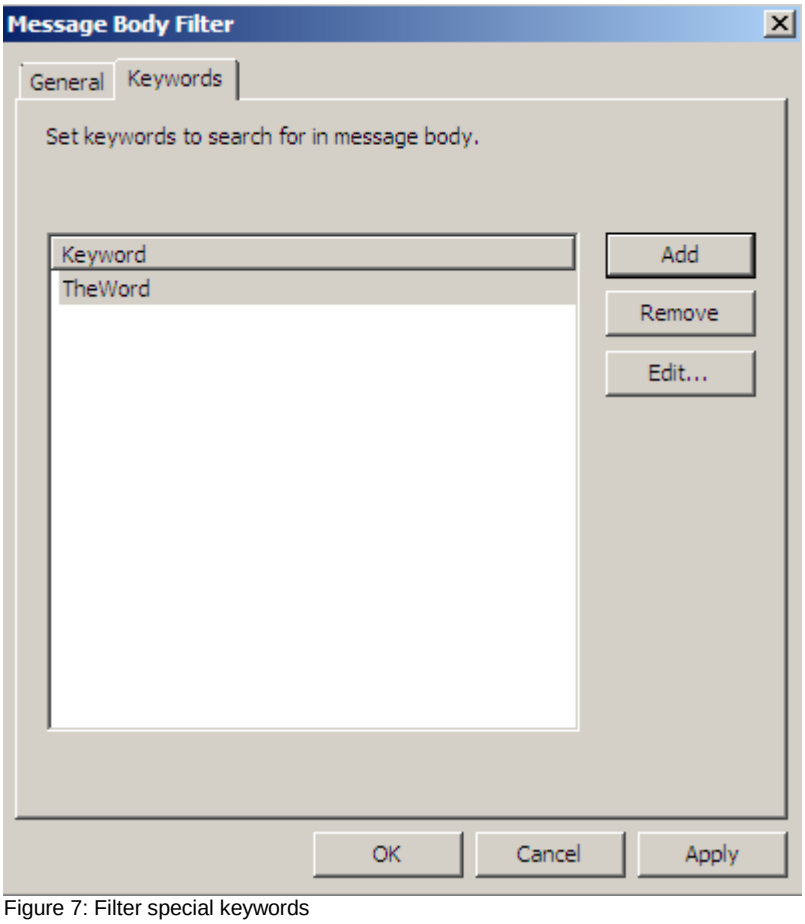

Figure 7: Filter special keywords

Antivirus configuration

Antivirus settings can also be enabled or disabled globally in Microsoft Forefront TMG and it is possible to select up to five Anti Virus scan engines. The Anti Virus scan engines and the technique behind this feature is based on Microsoft forefront Security products.

For a good scanning result you should select at least two Anti Virus scan engines. The more scan engines you select, the scan results will be better, but if you select more Anti Virus scan engines, the Server performance could be negative effected.

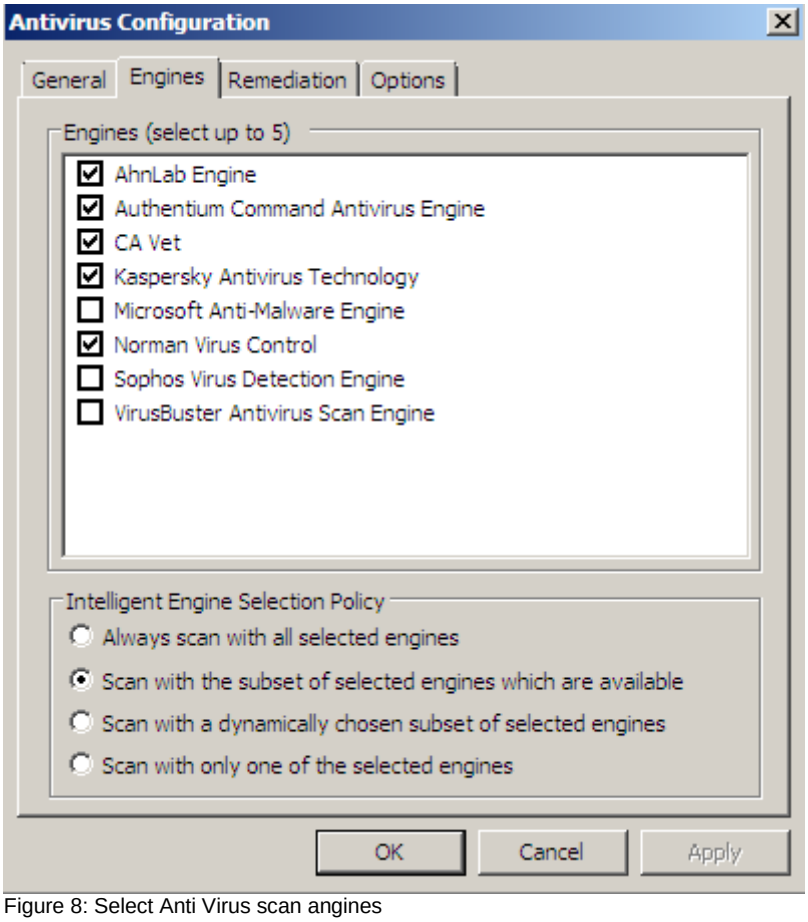

Figure 8: Select Anti Virus scan angines

It is possible to let TMG select the Anti Virus scan engines based on an Intelligent Engine Selection Policy. The default setting is to scan with a subset of selected engines which are available.

When a virus was found, TMG Administrators can select if the process should skip the scanned message, try to clean the attachment or to remove (delete) the infection. to inform the message recipient, it is possible to send a customized notification message to the recipient.

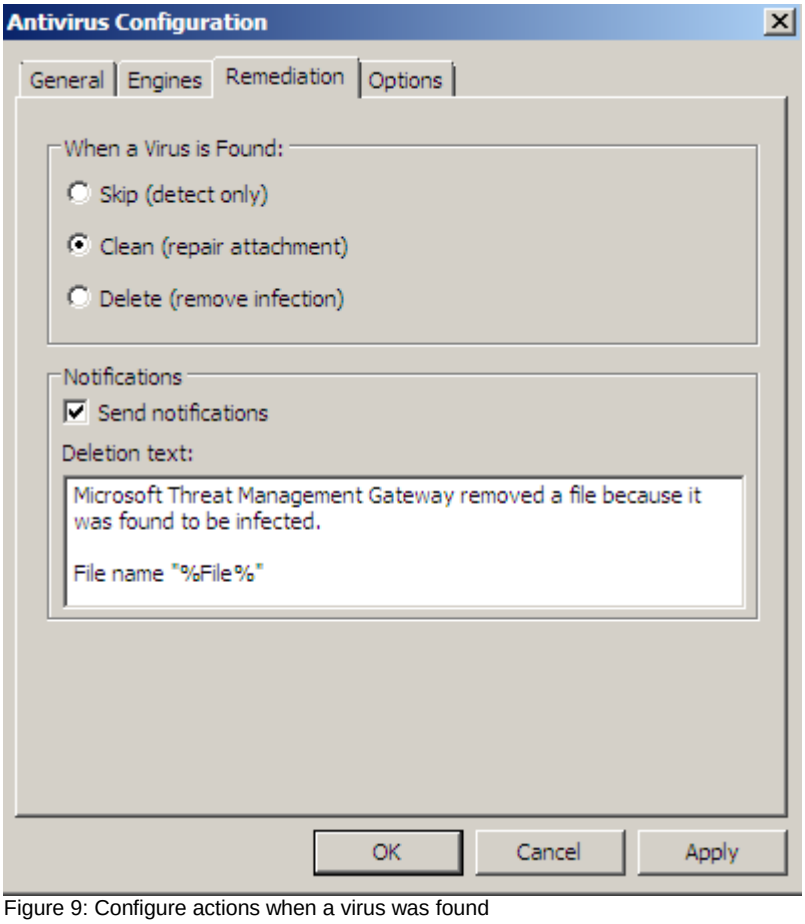

Figure 9: Configure actions when a virus was found

Antivirus options

It is possible to configure several Antivirus scanning options. One of the important one is to select if doc files should be scanned as containers. This option configures the Antivirus scan to scan .doc files and any other files that use structured data and the OLE embedded data format (for example, .xls, .ppt, or .shs) as container files. This ensures that any embedded files are scanned as potential virus carriers. This setting is disabled by default.

It is also possible to configure a scanning and a container scanning download timeout which is by default 300 seconds for the scanning timeout and 120 seconds for the container scanning timeout.

For security reasons it is possible to configure a action to delete messages if the scanning process runs into a timeout.

If TMG found illegal MIME headers you can specify additional actions.

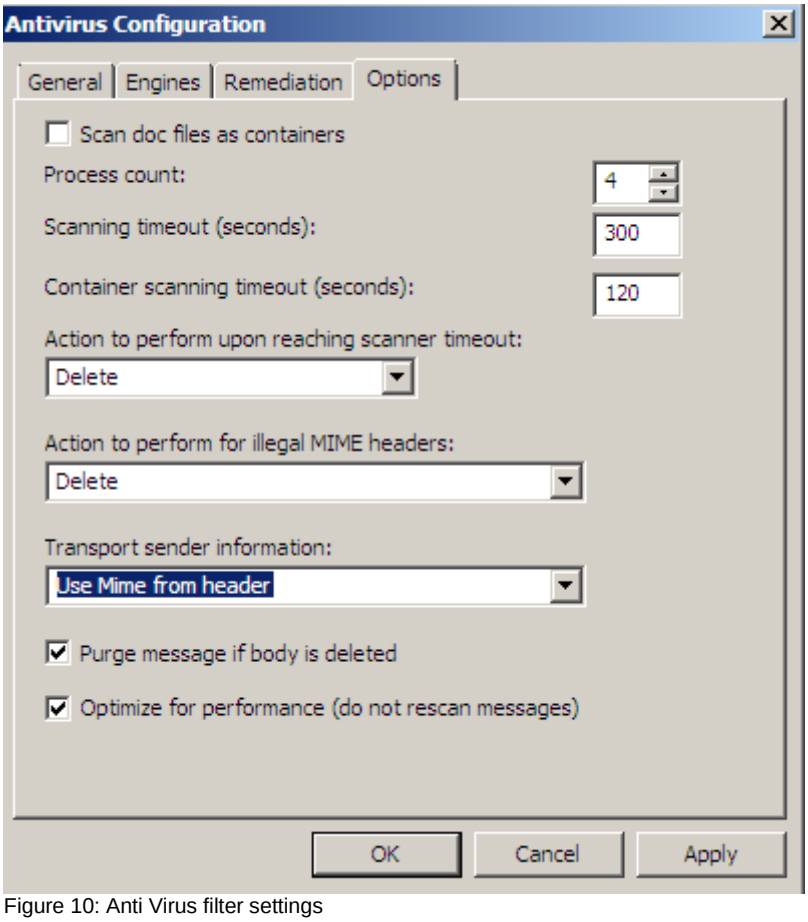

Figure 10: Anti Virus filter settings

Messages are always purged by default if the message body is deleted. for performance reasons, TMG doesn't rescan messages after filtering actions are applied.

Conclusion

In this second part of this article series, I gave you an overview about how Microsoft Forefront Threat Management Gateway uses its Antivirus capabilities some content features. With these new features of Microsoft Forefront TMG and the other robust ISA Server 2006 capabilities, TMG is more powerful than ISA Server 2006 and is wll prepared for modern threats.

Related links

Forefront Threat Management Gateway Beta 2
http://www.microsoft.com/downloads/details.aspx?FamilyID=e05aecbc-d0eb-4e0f-a5db-8f236995bccd&DisplayLang=en
Forefront TMG Beta 2 is Released
http://blogs.technet.com/isablog/archive/2009/02/06/forefront-tmg-beta-2-is-released.aspx
Configuring E-mail policy
http://technet.microsoft.com/en-us/library/dd441084.aspx
Forefront TMG MBE Frequently Asked Questions
http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/tmg-mbe-faq.aspx
How to install the Forefront Threat Management Gateway (Forefront TMG) Beta 1

http://www.isaserver.org/tutorials/Installing-Forefront-Threat-Management-Gateway-Forefront-TMG-Beta1.html