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

Configuring the AntiMalware functionality in Microsoft Forefront TMG

Abstract

In this article, I will show you how to configure the AntiMalware functions 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.

Definition of Malware

Wikipedia (http://en.wikipedia.org/wiki/Malware) defines Malware as follows:
Malware, a portmanteau from the words malicious and software, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software

Let's begin

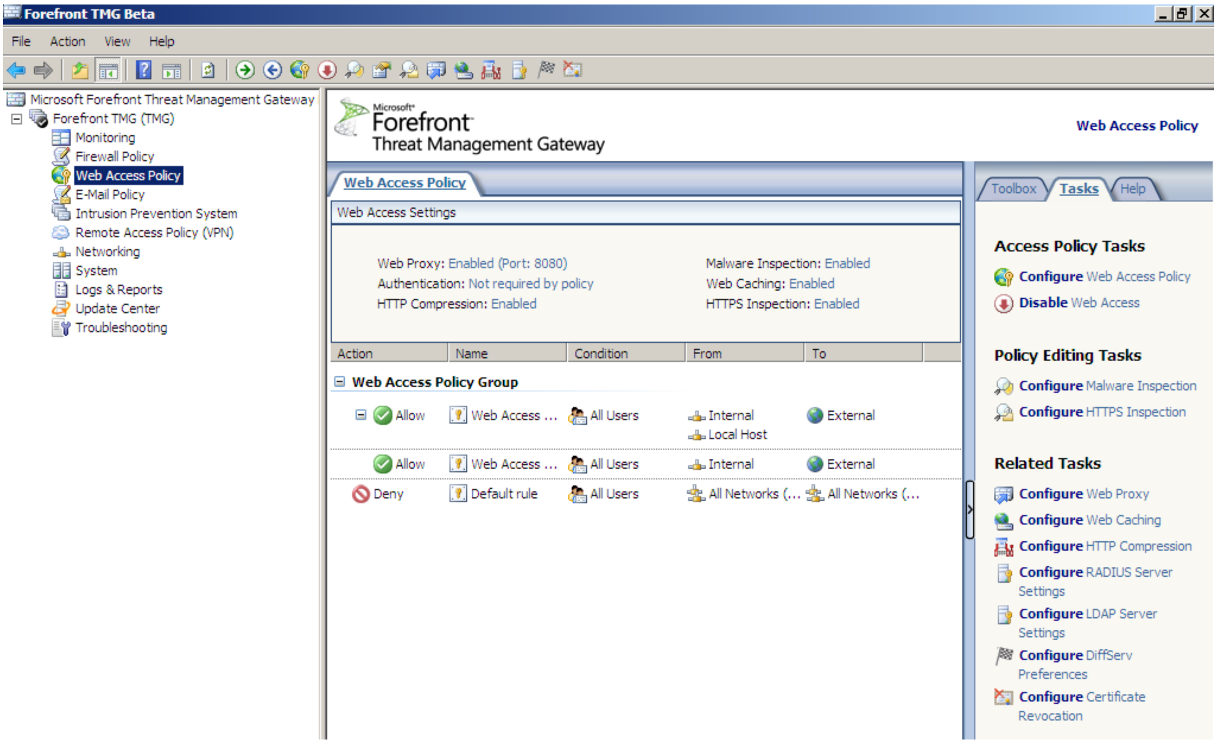
With Microsoft Forefront TMG it is possible to protect your network against Malware, before Malware content can reach your internal network, because TMG scans all related HTTP traffic for malicious content.

The Malware protection feature in Microsoft Forefront TMG uses the same Malware Protection Engine which is also used in Microsoft Forefront Client Security (FCS), Live One Care and Windows Defender.

Some of the Malware features are configured globally, but it is also possible top configure some settings on a rule base. It is also possible to enable or disable the Malware inspection feature per Firewall policy rule.

General settings

The global Malware settings are configured in the new ISA TMG node called Web Access Policy.


Forefront TMG Beta
File Action View Help
Microsoft Forefront Threat Management Gateway
Forefront TMG (TMG)
Monitoring
Firewall Policy
Web Access Policy
E-Mail Policy
Intrusion Prevention System
Remote Access Policy (VPN)
Networking
System
Logs & Reports
Update Center
Troubleshooting
Microsoft Forefront Threat Management Gateway
Web Access Policy
Toolbox Tasks Help
Access Policy Tasks
Configure Web Access Policy
Disable Web Access
Policy Editing Tasks
Configure Malware Inspection
Configure HTTPS Inspection
Related Tasks
Configure Web Proxy
Configure Web Caching
Configure HTTP Compression
Configure RADIUS Server Settings
Configure LDAP Server Settings
Configure DiffServ Preferences
Configure Certificate Revocation

Web Access Settings

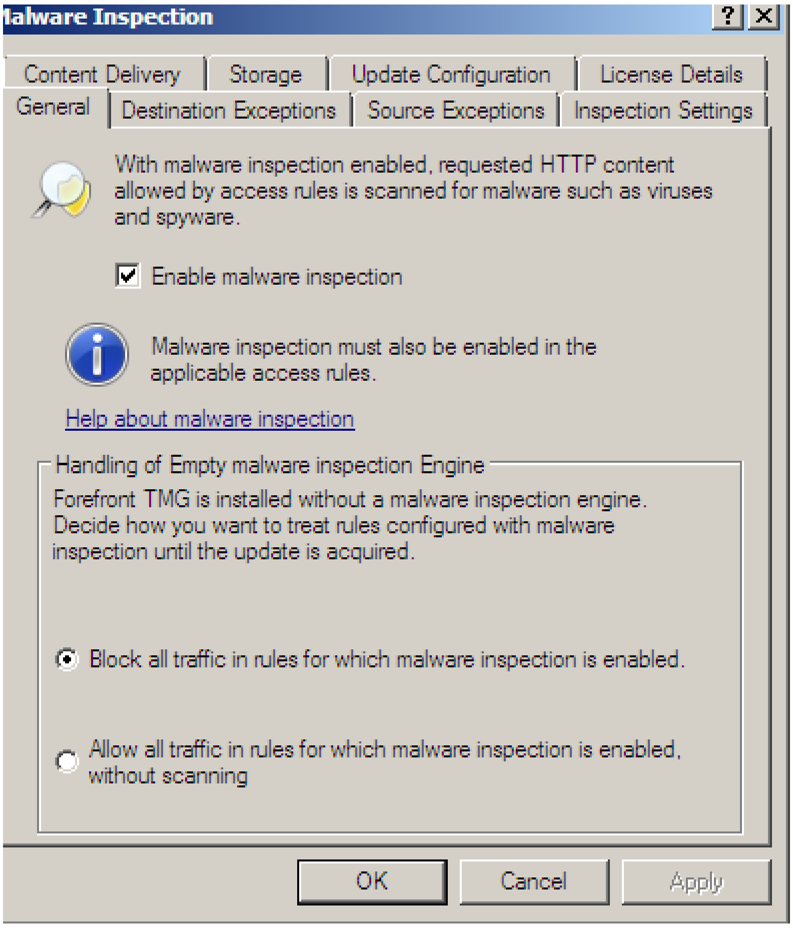
Web Proxy: Enabled (Port: 8080)
Authentication: Not required by policy
HTTP Compression: Enabled

Malware Inspection: Enabled
Web Caching: Enabled
HTTPS Inspection: Enabled

Action	Name	Condition	From	To
Web Access Policy Group				
Allow	Web Access ...	All Users	Internal Local Host	External
Allow	Web Access ...	All Users	Internal	External
Deny	Default rule	All Users	All Networks (...	All Networks (...

Figure 1: Web Access Policy node

Click *Configure Malware Inspection* in the right task pane to configure the global settings. The settings in the first register card allows you to enable or disable the Malware Inspection filter. Malware must also be enabled in the Firewall policy rule where you want to use the Malware feature.



With malware inspection enabled, requested HTTP content allowed by access rules is scanned for malware such as viruses and spyware.

☑ Enable malware inspection

Malware inspection must also be enabled in the applicable access rules.

Handling of Empty malware inspection Engine

Forefront TMG is installed without a malware inspection engine. Decide how you want to treat rules configured with malware inspection until the update is acquired.

● Block all traffic in rules for which malware inspection is enabled.

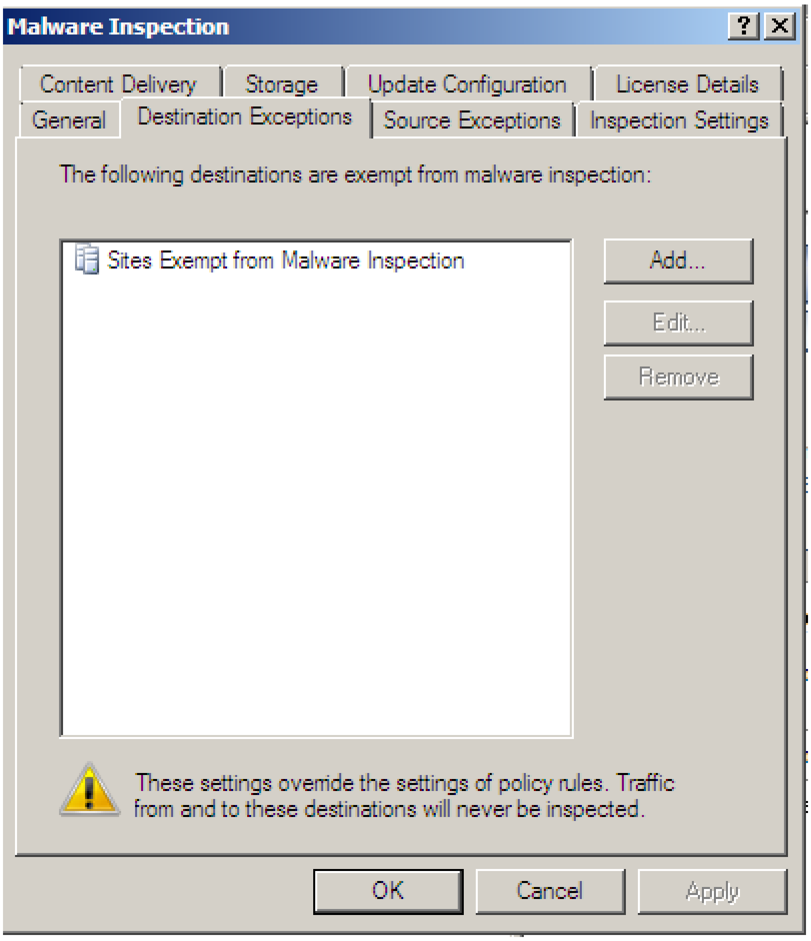
○ Allow all traffic in rules for which malware inspection is enabled, without scanning

Figure 2: Enabling Malware inspection

The standard settings blocks all network traffic when Malware inspection is activated but TMG doesn't find a Malware Inspection engine update.
It is possible to change this behavior, but it reduces the overall security.

Destination exceptions

It is possible to exclude some websites from Malware filtering. Some websites like Microsoft websites are automatically excluded from Malware checking. It is possible to extend the list with your own websites.



The following destinations are exempt from malware inspection:

Sites Exempt from Malware Inspection

These settings override the settings of policy rules. Traffic from and to these destinations will never be inspected.

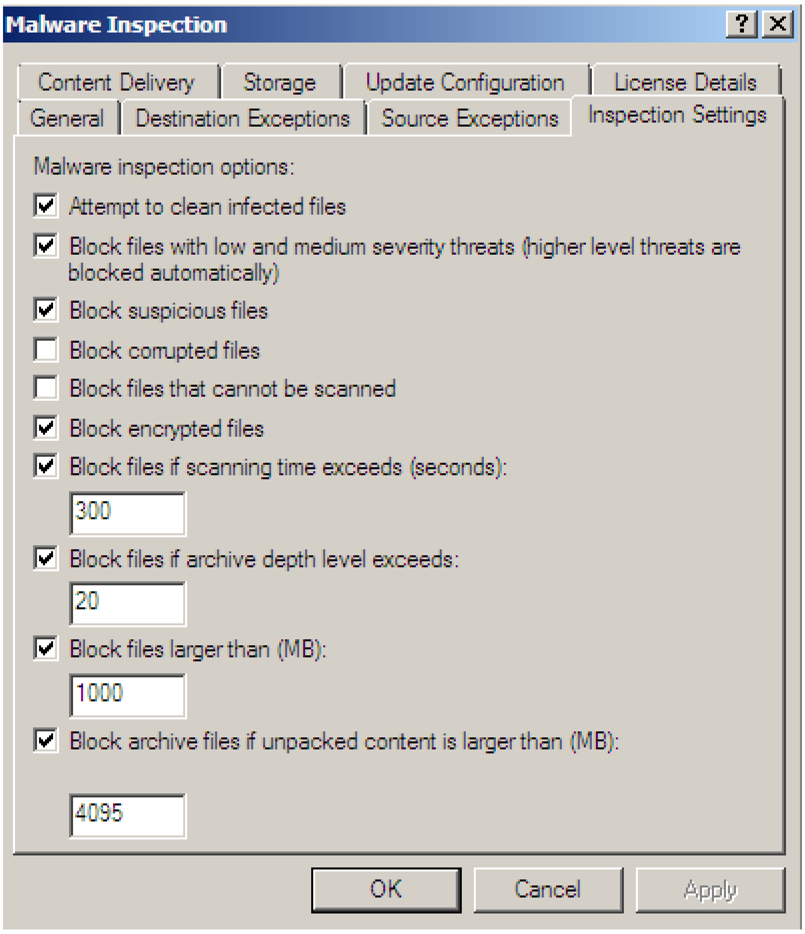
Figure 3: Destination exceptions

Source exceptions

Like destination exceptions, Source exeptions exludes some internal clients and Servers from Malware scanning when they open websites.

Inspection settings

The Inspection settings in the Malware protection feature allows the configuration and fine tuning of several settings.
It is possible to configure different block settings when the Malware inspection should block infected or suspicious files, or files that cannot be scanned. TMG by default blocks encrypted files.



Malware inspection options:

☑ Attempt to clean infected files

☑ Block files with low and medium severity threats (higher level threats are blocked automatically)

☑ Block suspicious files

□ Block corrupted files

□ Block files that cannot be scanned

☑ Block encrypted files

☑ Block files if scanning time exceeds (seconds):

300

☑ Block files if archive depth level exceeds:

20

☑ Block files larger than (MB):

1000

☑ Block archive files if unpacked content is larger than (MB):

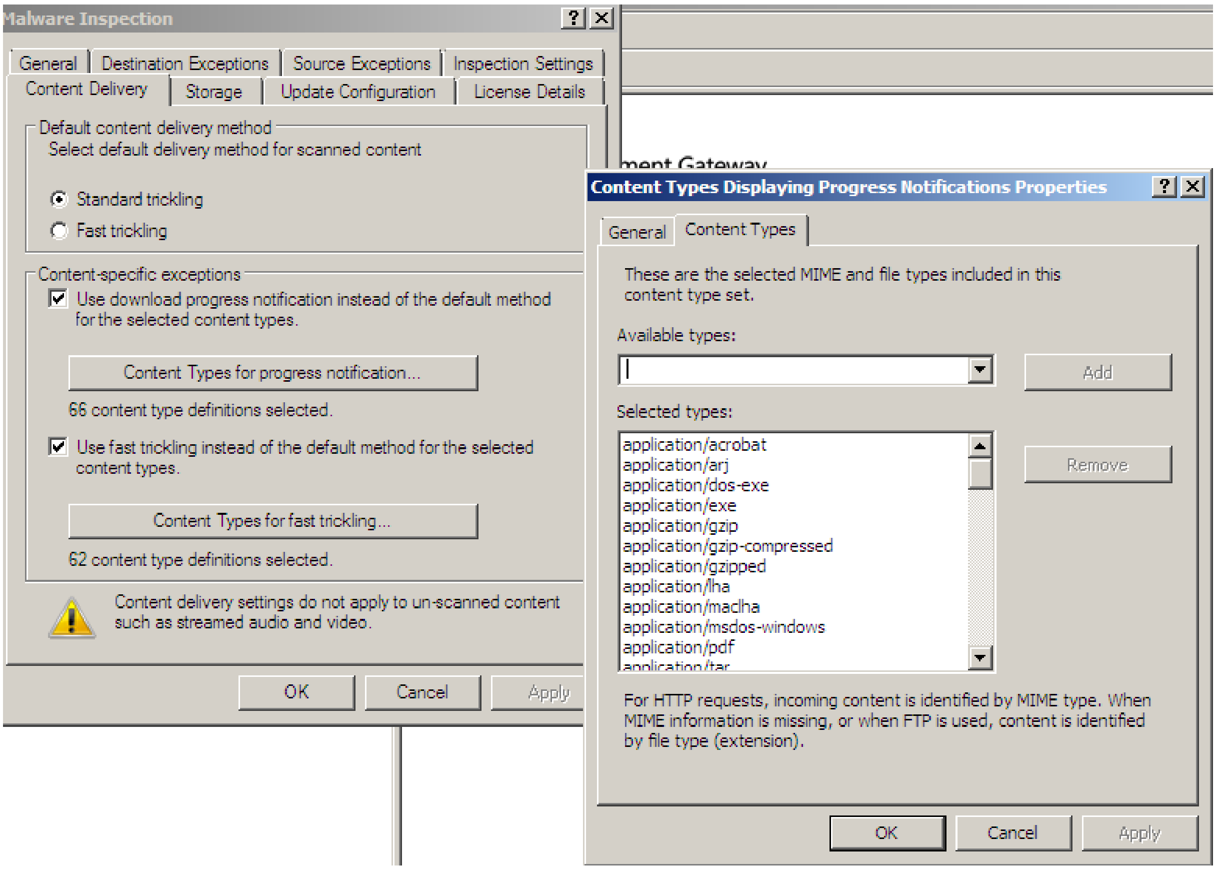
4095

Figure 4: Inspection settings

It is also possible to configure the Malware inspection to block files when the scanning time exceeds a configured limit or if files to download are larger than the specified size in Megabyte and something more.

Content Delivery

The Content Delivery tab allows TMG Administrator to configure the user experience while the Malware inspection of TMG scans the network traffic. Because downloading larger files can take a relative long time and the user will normally get no status message about the download and downloads could run into timeouts, it is possible to configure how the Malware inspection feature displays a progress notification to users. Forefront TMG sends an HTML page to the client. This HTML page informs users that the requested content is being inspected and displays an indicator of the download and Malware inspection progress.



Malware Inspection

General | Destination Exceptions | Source Exceptions | Inspection Settings
Content Delivery | Storage | Update Configuration | License Details

Default content delivery method

Select default delivery method for scanned content

● Standard trickling

○ Fast trickling

Content-specific exceptions

☑ Use download progress notification instead of the default method for the selected content types.

Content Types for progress notification...

66 content type definitions selected.

☑ Use fast trickling instead of the default method for the selected content types.

62 content type definitions selected.

Content delivery settings do not apply to un-scanned content such as streamed audio and video.

Content Types Displaying Progress Notifications Properties

These are the selected MIME and file types included in this content type set.

Available types:

Selected types:

application/acrobat
application/arj
application/dos-exe
application/exe
application/gzip
application/gzip-compressed
application/gzipped
application/lha
application/maclha
application/msdos-windows
application/pdf
application/tar

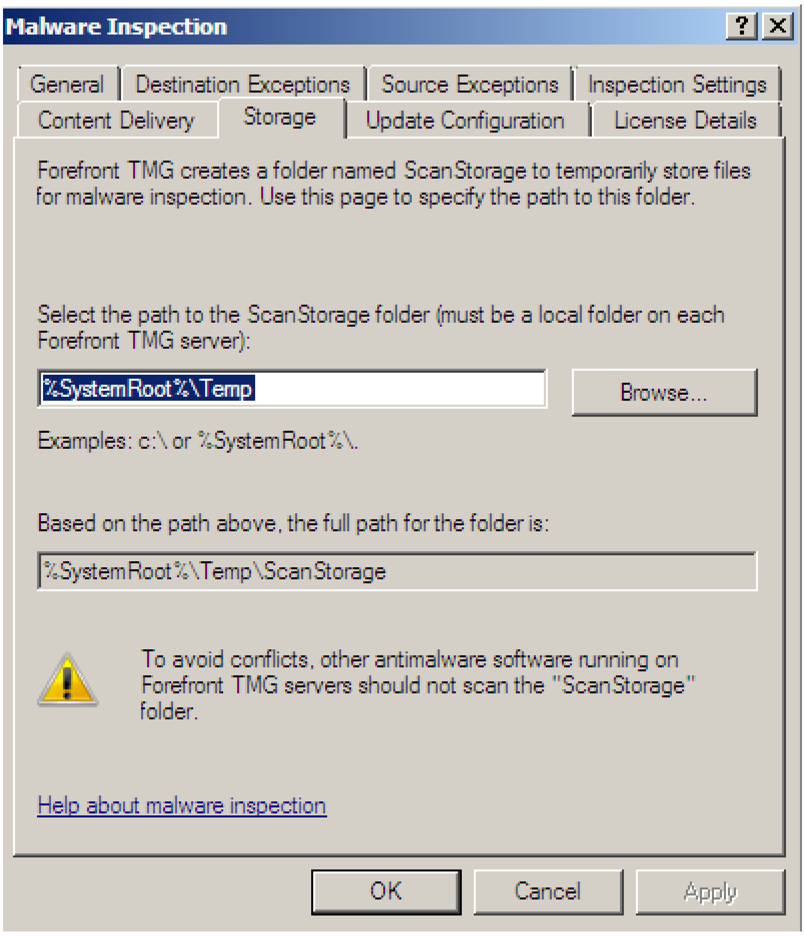
For HTTP requests, incoming content is identified by MIME type. When MIME information is missing, or when FTP is used, content is identified by file type (extension).

Figure 5: Content delivery settings

Standard trickling is used to send the requested content at a slow rate to the client which requested the content. The content will be cached on TMG during Malware inspection.
Fast trickling is used to find the balance between the end user experience during downloading files and the wish of the TMG Administrator for less file buffering on TMG and more scans. If an infection is found in the file that is trickled to the user, Microsoft Forefront TMG resets the connection and the download is not delivered to the client.

Storage

The Storage setting allows TMG Administrator to specify the location for the local temporary storage where the Malware engine temporary places downloaded content which should be scanned for Malware. If TMG Server is heavily loaded, you should specify another directory for the temporary Malware Storage location.



Forefront TMG creates a folder named ScanStorage to temporarily store files for malware inspection. Use this page to specify the path to this folder.

Select the path to the ScanStorage folder (must be a local folder on each Forefront TMG server):

%SystemRoot%\Temp

Examples: c:\ or %SystemRoot%\.

Based on the path above, the full path for the folder is:

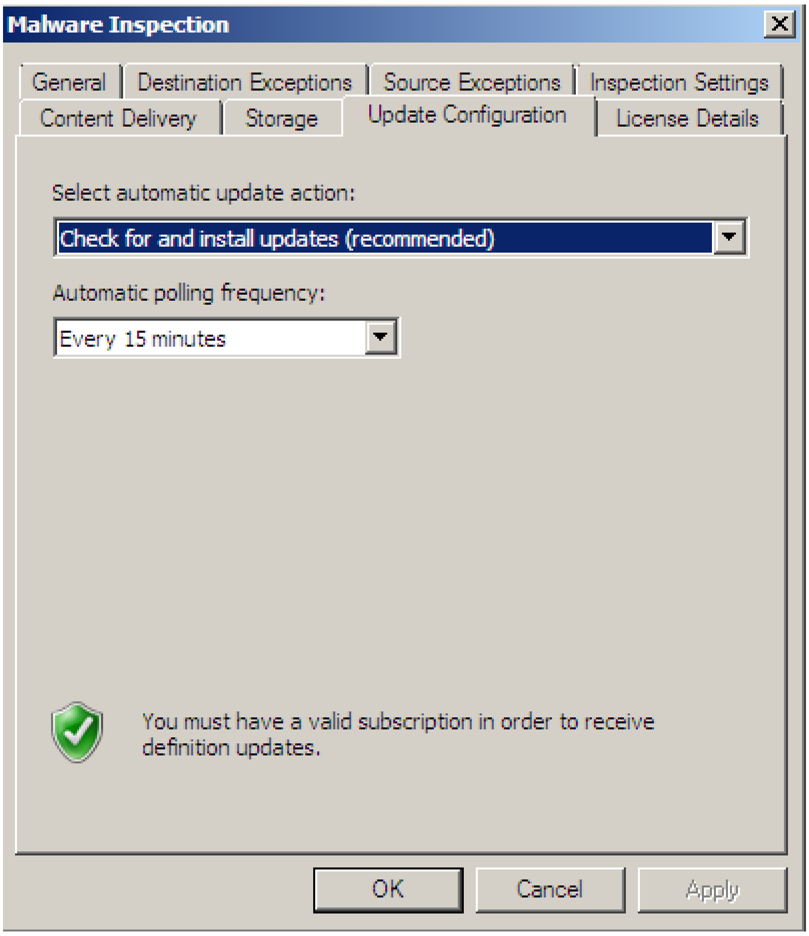
%SystemRoot%\Temp\ScanStorage

To avoid conflicts, other antimalware software running on Forefront TMG servers should not scan the "ScanStorage" folder.

Figure 6: Storage for temporary scanned files during Malware inspection

Update configuration

The Malware inspection feature in TMG is only effective, if there are permanent updates for this feature to protect against new Malware. By default, the Malware inspection feature in TMG scans every 15 minutes for updates against the Microsoft servers. You need a valid subscription to use this feature.



Select automatic update action: Check for and install updates (recommended)

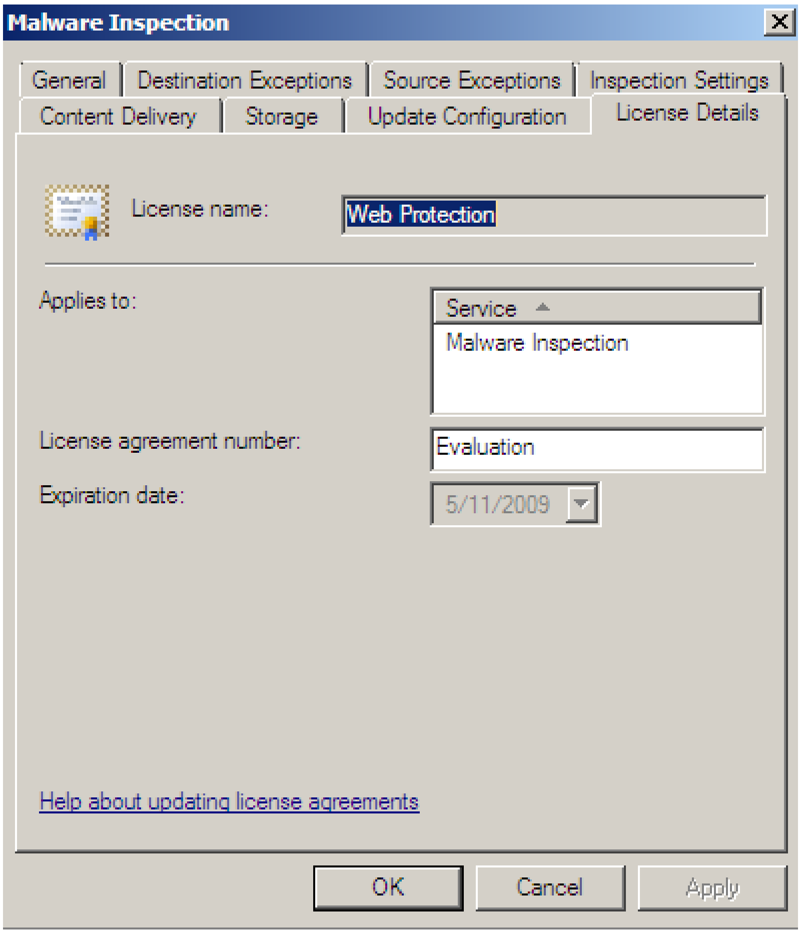
Automatic polling frequency: Every 15 minutes

You must have a valid subscription in order to receive definition updates.

Figure 7: Update configuration settings

License Details

The Malware protection feature is licensed for a period of time. It is possible to see the license details in this configuration window.



License name: Web Protection

Applies to:

Service
Malware Inspection

License agreement number: Evaluation

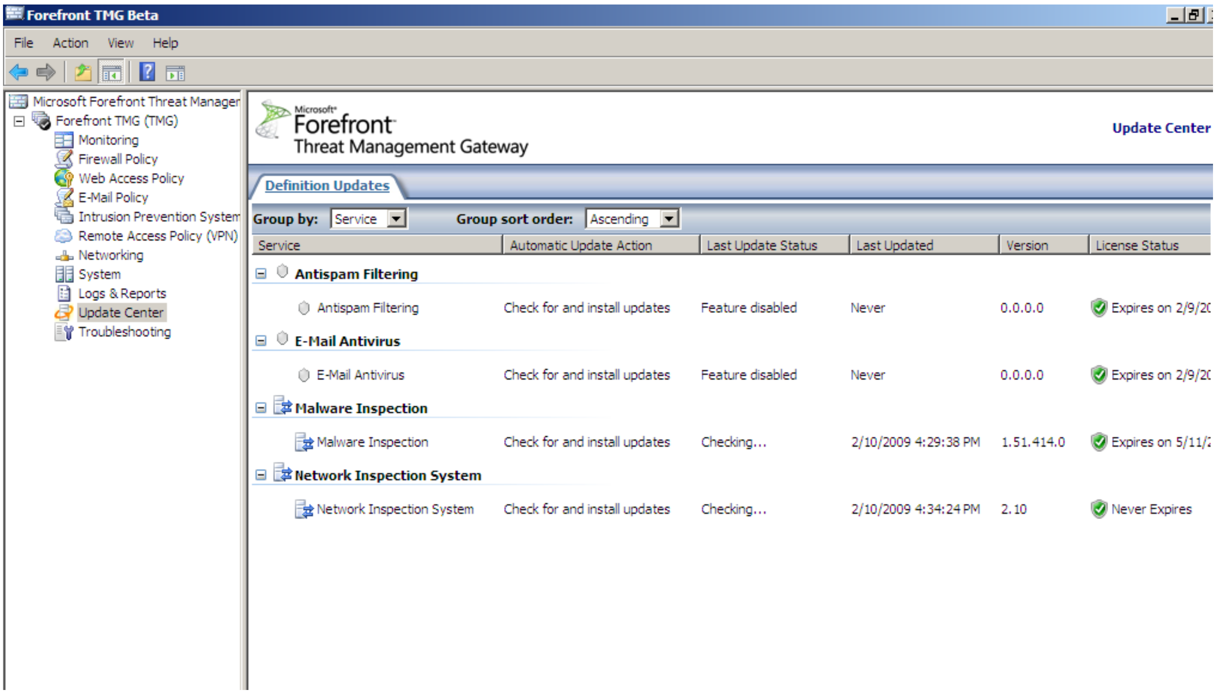
Expiration date: 5/11/2009

Help about updating license agreements

Figure 8: License details

Update Center

A permanent update of the Malware Inspection filter definitions is absolute necessary if want to be protected against the newest tricks of Malware producers. The Update Center allows you to configure updates for several components in Microsoft Forefront TMG.

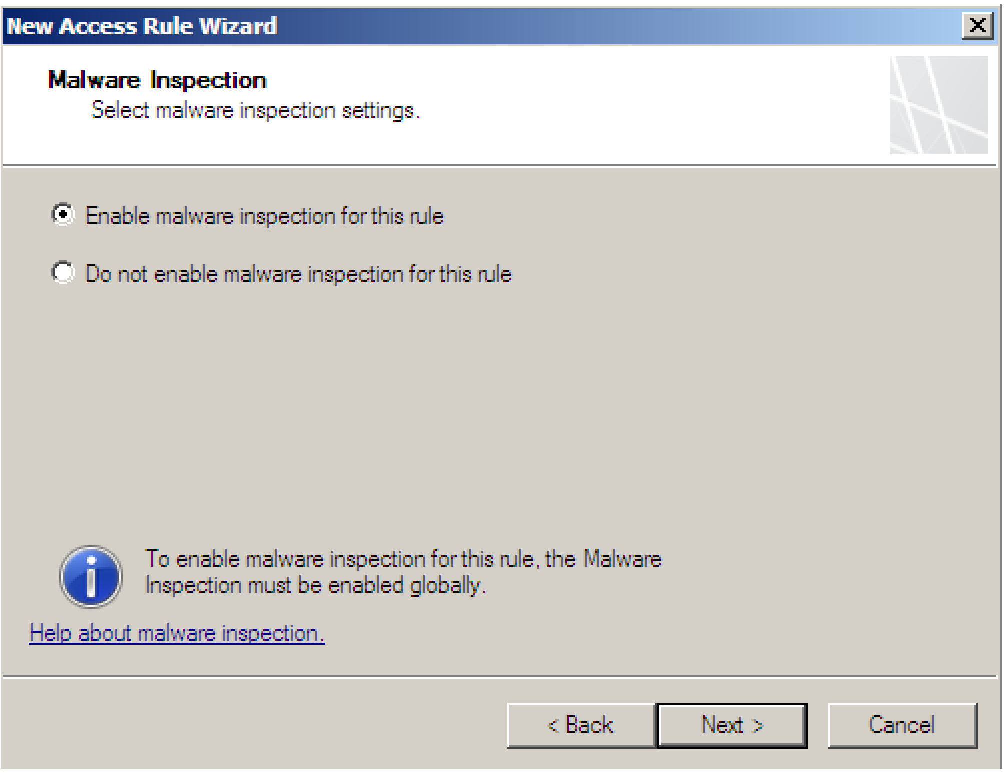


Group by: Service Group sort order: Ascending

Service	Automatic Update Action	Last Update Status	Last Updated	Version	License Status
Antispam Filtering					
Antispam Filtering	Check for and install updates	Feature disabled	Never	0.0.0.0	Expires on 2/9/20
E-Mail Antivirus					
E-Mail Antivirus	Check for and install updates	Feature disabled	Never	0.0.0.0	Expires on 2/9/20
Malware Inspection					
Malware Inspection	Check for and install updates	Checking...	2/10/2009 4:29:38 PM	1.51.414.0	Expires on 5/11/2
Network Inspection System					
Network Inspection System	Check for and install updates	Checking...	2/10/2009 4:34:24 PM	2.10	Never Expires

Figure 9: Update Center

Malware Inspection is configured globally, but can be enabled or disabled for every Firewall rule.


New Access Rule Wizard

Malware Inspection

Select malware inspection settings.

● Enable malware inspection for this rule

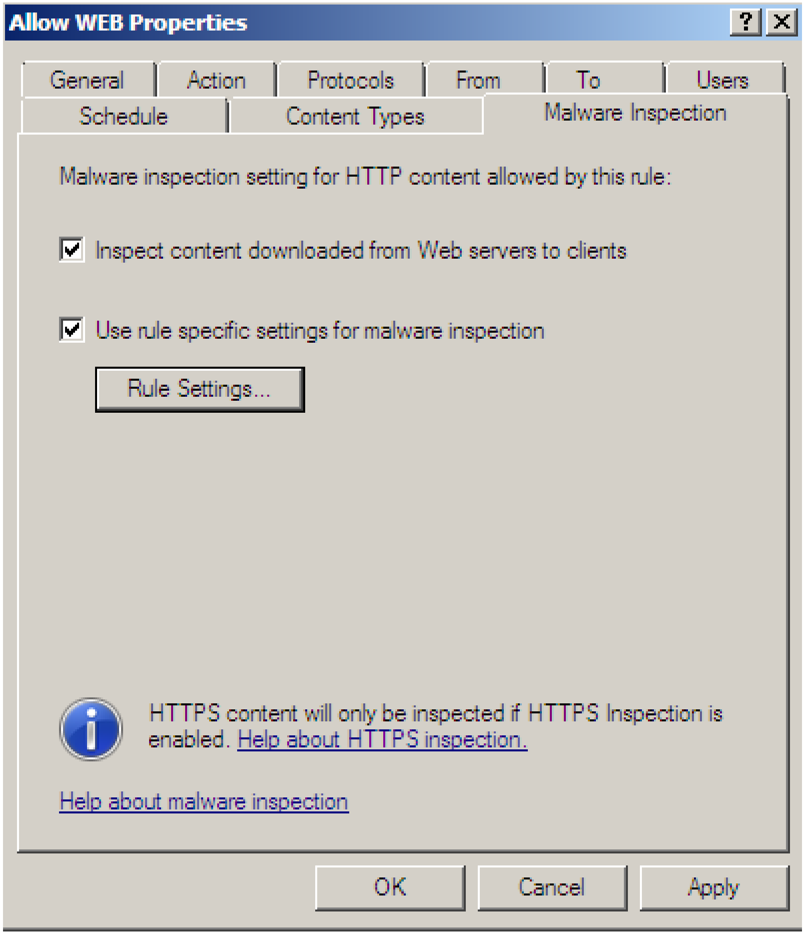
○ Do not enable malware inspection for this rule

To enable malware inspection for this rule, the Malware Inspection must be enabled globally.

Help about malware inspection.

Figure 10: Enable or disable Malware settings

It is also possible to configure rule specific settings for Malware inspection.



Malware inspection setting for HTTP content allowed by this rule:

☑ Inspect content downloaded from Web servers to clients

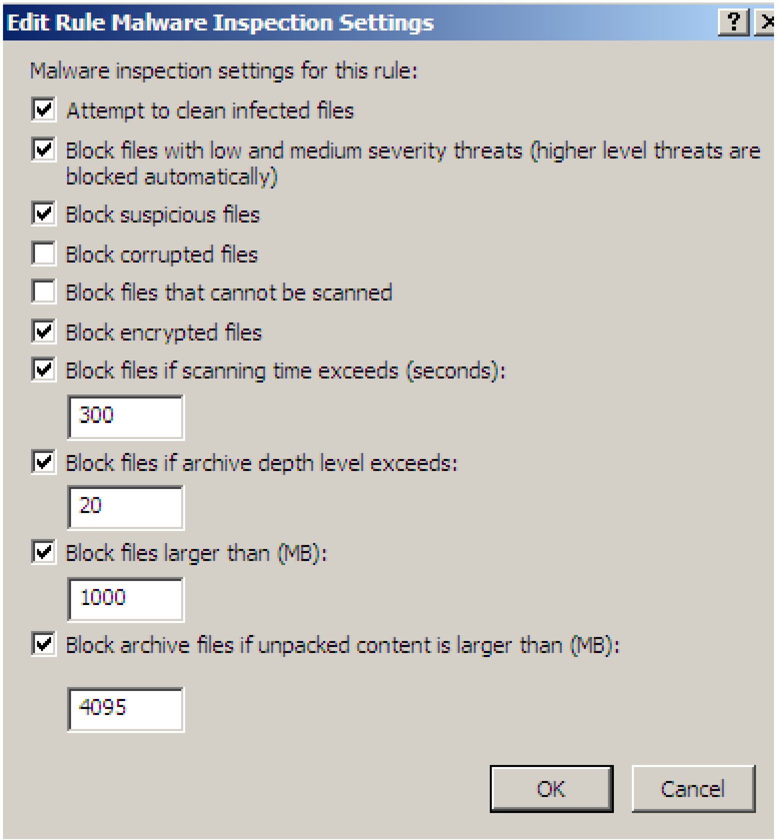
☑ Use rule specific settings for malware inspection

HTTPS content will only be inspected if HTTPS Inspection is enabled. Help about HTTPS inspection.

Help about malware inspection

Figure 11: Firewall policy rule specific Malware inspection settings

The rule specific settings are the same as the global settings.



Malware inspection settings for this rule:

☑ Attempt to clean infected files

☑ Block files with low and medium severity threats (higher level threats are blocked automatically)

☑ Block suspicious files

☐ Block corrupted files

☐ Block files that cannot be scanned

☑ Block encrypted files

☑ Block files if scanning time exceeds (seconds):

300

☑ Block files if archive depth level exceeds:

20

☑ Block files larger than (MB):

1000

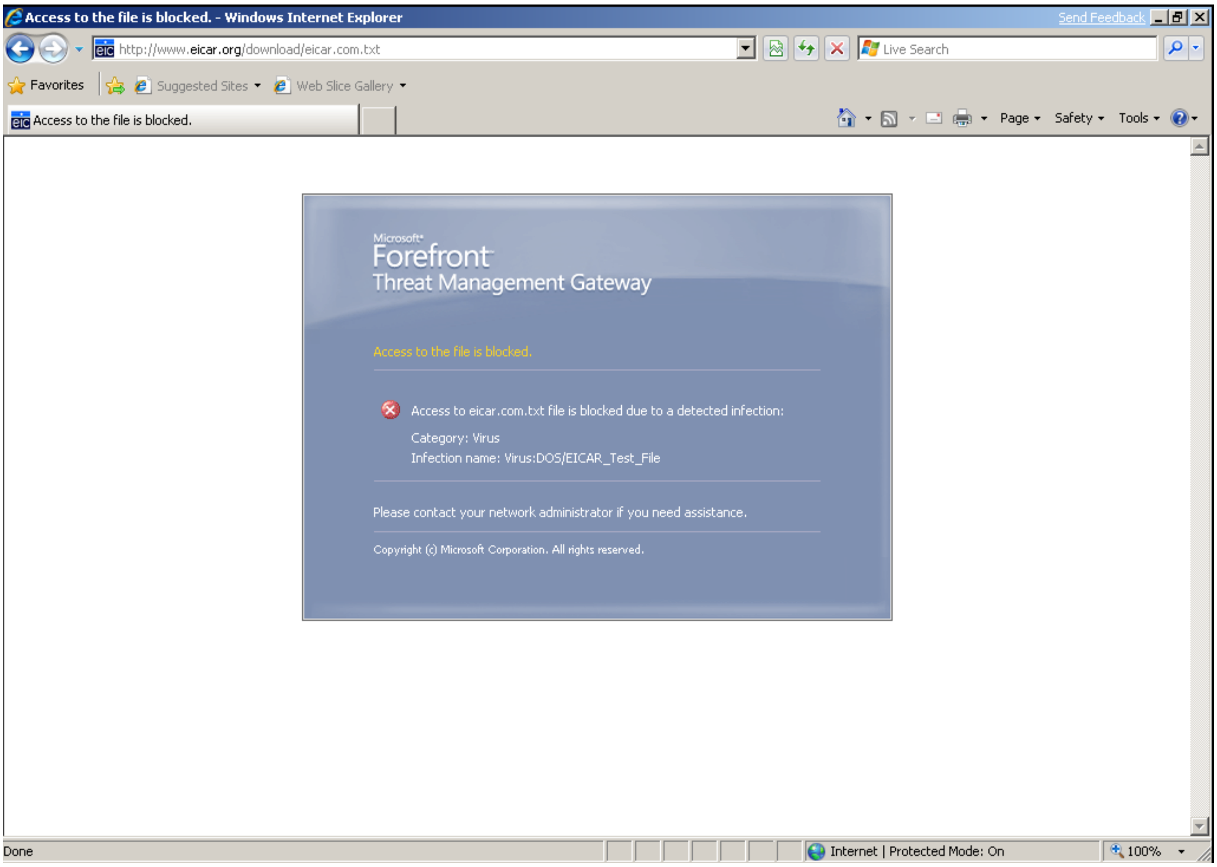
☑ Block archive files if unpacked content is larger than (MB):

4095

Figure 12: Rule specific Malware Inspection settings

User experience

If the Malware inspection finds suspicious content and the content will be blocked, the user gets notified as you can see in the following figure.


Access to the file is blocked. - Windows Internet Explorer
Send Feedback
http://www.eicar.org/download/eicar.com.txt
Live Search
Favorites
Suggested Sites
Web Slice Gallery
Access to the file is blocked.
Page
Safety
Tools
Microsoft
Forefront
Threat Management Gateway
Done
Internet | Protected Mode: On
100%

Access to the file is blocked.

Access to eicar.com.txt file is blocked due to a detected infection:

Category: Virus
Infection name: Virus:DOS/EICAR_Test_File

Please contact your network administrator if you need assistance.

Copyright (c) Microsoft Corporation. All rights reserved.

Figure 13 User notification if Malware was found

Conclusion

In this article, I gave you an overview about the Microsoft Forefront Threat Management Gateway Antimalware features. I also tried to show you the configuration of the Antimalware functionality and who Administrators can protect its networks. The Antimalware functionality is a great weapon for TMG Administrators to fight against Malware.

Related links

Overview of Malware inspection
http://technet.microsoft.com/en-us/library/dd182018.aspx
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
Security Watch Malware Inspection at the Perimeter
http://technet.microsoft.com/en-us/magazine/2009.02.securitywatch.aspx

What’s new in Forefront TMG Beta 2 (Part 1)
http://www.isaserver.org/tutorials/Whats-new-Forefront-TMG-Beta-2-Part1.html
Installing and configuring Microsoft Forefront TMG Beta 2
http://www.isaserver.org/tutorials/Installing-configuring-Microsoft-Forefront-TMG-Beta2.html