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

What's new in Forefront TMG Beta 2 – Part 1

Abstract

In this two part article series, I will show you the new and extended features of 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 days ago, Microsoft released Beta 2 from Microsoft Forefront TMG (Threat Management Gateway), which has a lot of new exiting features.

In this first article, I will show you some of the new features and how they work. Part two of this article series will show you other changes in Microsoft Forefront TMG. Both articles should only give you some basic information about new and changed features in Microsoft Forefront TMG, so we would not go into details in this both articles.

System requirements

One of the most important changes in Microsoft Forefront TMG is that it must be installed on Windows Server 2008 with 64 Bit. Other changes:

- 2 gigabytes (GB) or more of memory
- 2.5 GB of available hard disk space. This is exclusive of hard disk space that you want to use for caching or for temporarily storing files during malware inspection.
- One network adapter that is compatible with the computer's operating system, for communication with the Internal network.
- An additional network adapter for each network connected to the Forefront TMG server.
- One local hard disk partition that is formatted with the NTFS file system.

Microsoft has divided the new feature into six sections:

- Control network policy access at the edge (Firewall)
- Protect users from web browsing threats (Web Client Protection)
- Protect users from E-mail threats (Email Protection)
- Protect desktops and servers from intrusion attempts (NIS)
- Enable users to remotely access corporate resources (VPN, Secure Web Publishing)
- Simplified management (Deployment)

After a successful installation of Microsoft Forefront TMG the Getting Started Wizard will start when you open the Microsoft Forefront TMG console the first time. The Getting Started Wizard will help TMG Administrators to initial configure TMG for their business needs.

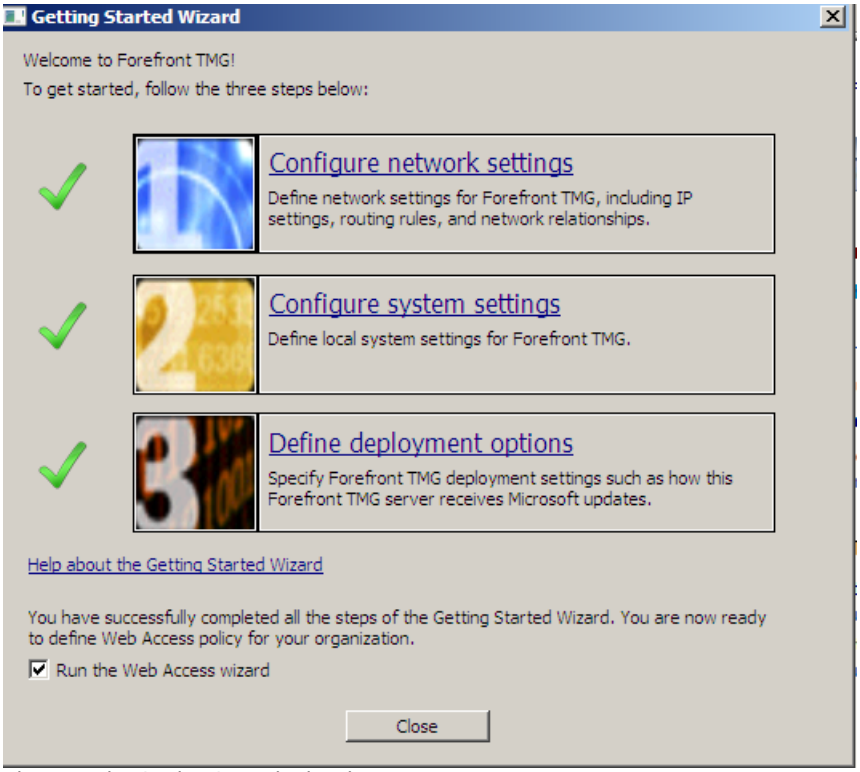

Figure 1: The Getting Started Wizard

The first step of the wizard configures the Internal and external Networks for TMG. The second wizard configures local settings as domain membership settings. The third wizard configures basic settings like Windows Update settings and Microsoft Telemetry settings.

The Microsoft Forefront TMG console is not very different from the ISA Server 2006 Management console. The console is very similar to the ISA Server 2006 Management console. There are only some new nodes in the console on the left side but these nodes allow very powerful settings. Several settings have been unchanged in Microsoft Forefront TMG and some familiar settings have new configuration buttons and configuration tabs.

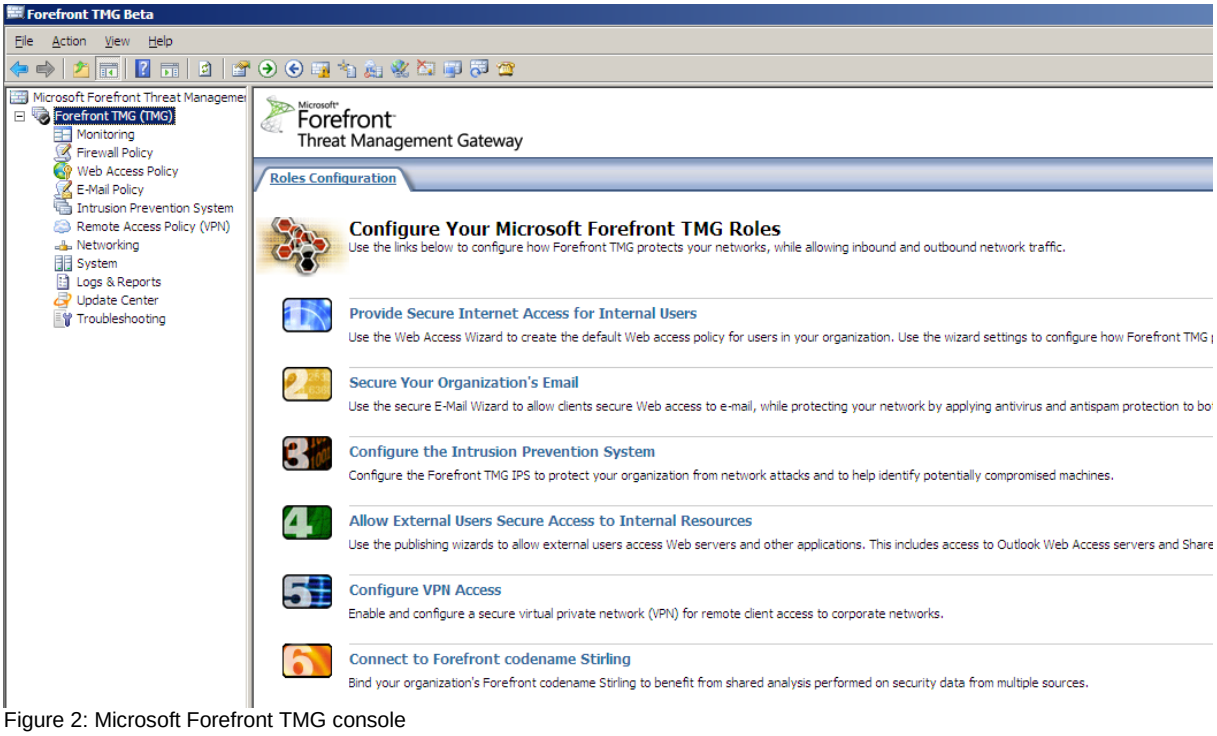

Figure 2: Microsoft Forefront TMG console

In the Monitoring node under the Services tab, Microsoft Forefront TMG services are now grouped and there is a new Reporting engine – the SQL Server 2005 Reporting service engine. There is also a new configuration tab which someone of you knows from ISA Server 2006 Enterprise which displays the configuration state of all ISA Server / TMG Server Enterprise array members.

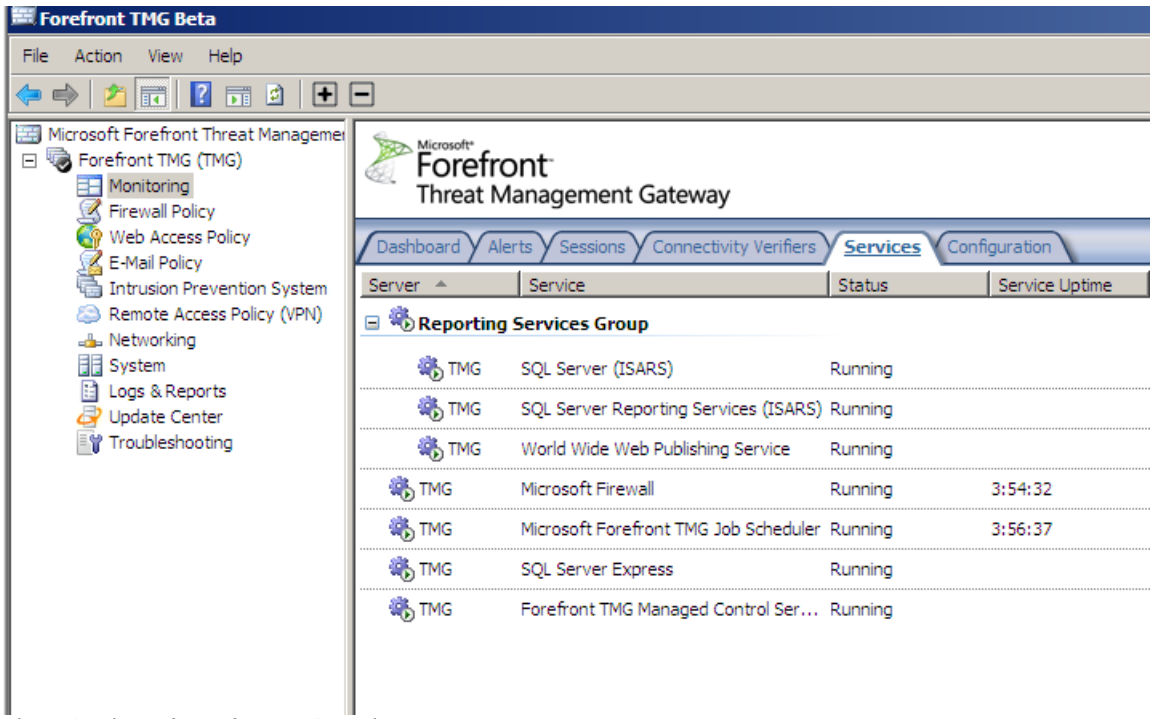

Figure 3: Microsoft Forefront TMG services

In Microsoft Forefront TMG, it is now possible to configure related Firewall policy settings from one point in the console which automatically navigates to the appropriate settings in the TMG MMC.

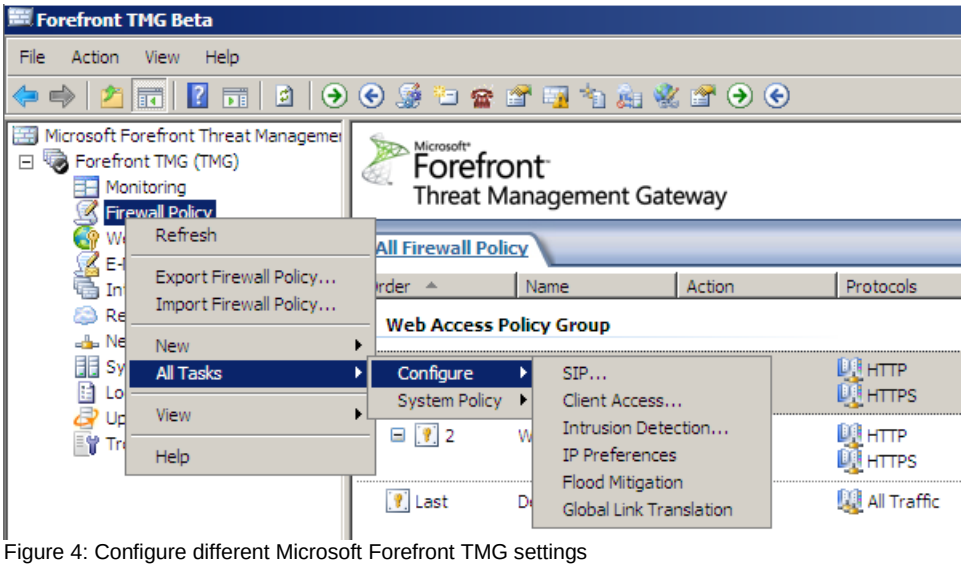

Figure 4: Configure different Microsoft Forefront TMG settings

In the right pane of the TMG console it is possible to configure many related Firewall tasks. New in TMG is the support for several VOIP (VoiceOverIP) scenarios. Microsoft Forefront TMG comes with a native SIP filter.

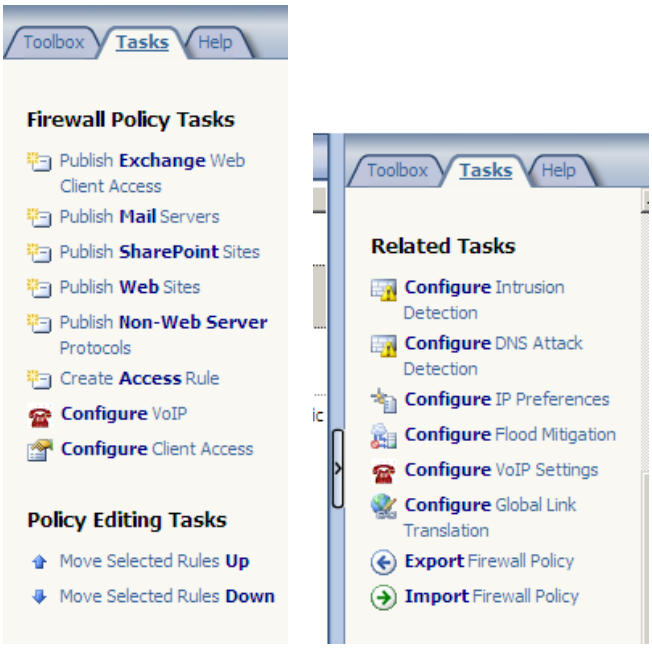

Figure 5: TMG Firewall Policy Tasks

Malware protection

Microsoft Forefront TMG is the first Microsoft Enterprise Firewall which enables you to protect your network from malicious attacks in form from Malware. The Malware protection feature is the first line of defense against several types of Zero Day exploits.

Definition of Malware (Source: http://en.wikipedia.org/wiki/Malware)

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. 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. Malware is not the same as defective software, that is, software which has a legitimate purpose but contains harmful bugs.

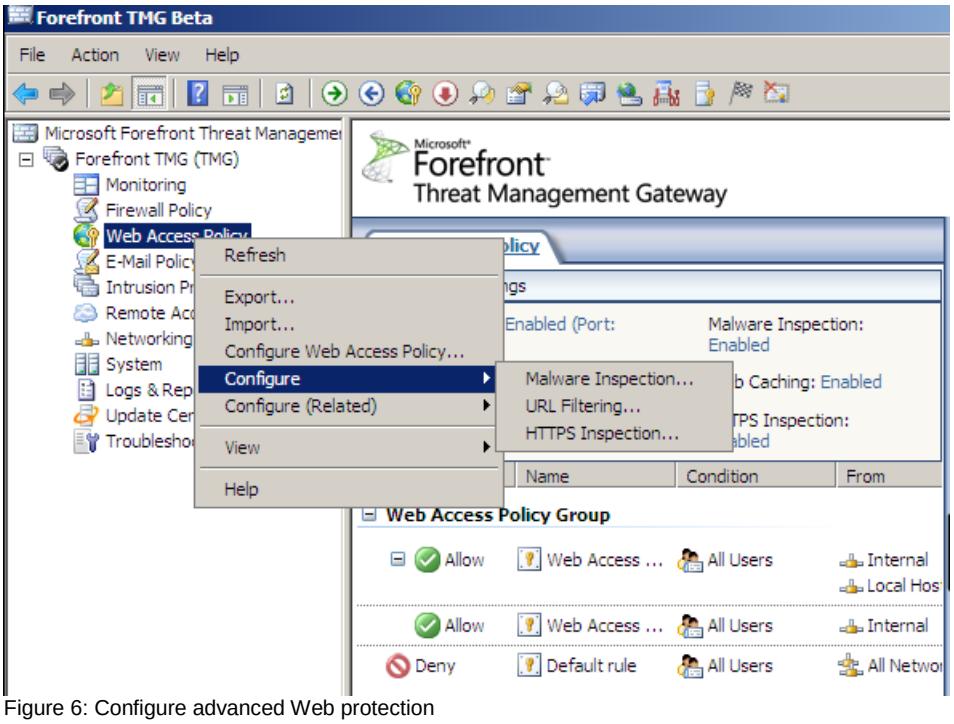

Figure 6: Configure advanced Web protection

The Malware inspection feature can be enabled globally and in the applicable Firewall access rule.

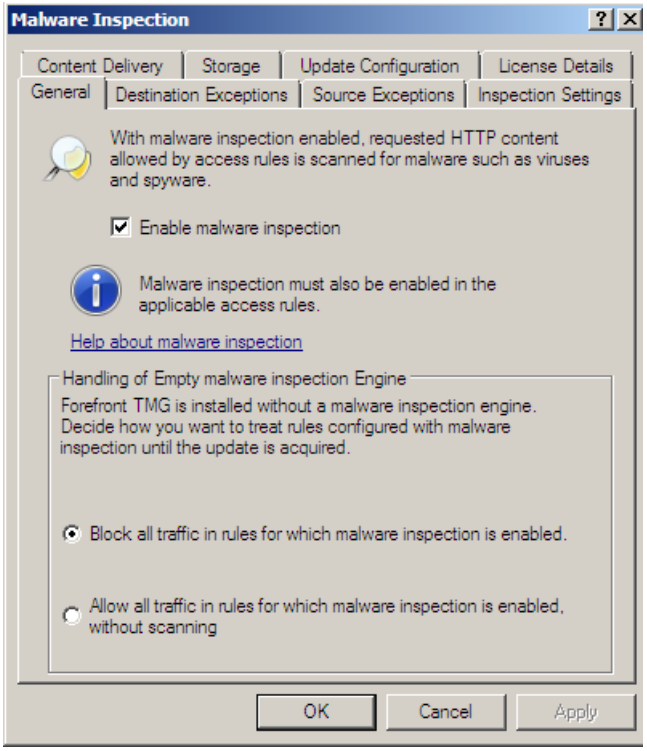

Figure 7: Configure global Malware inspection settings

In the Inspection settings tab it is possible to configure advanced Malware inspection settings like when to scan content for Malware and when to block files which are larger than the configured size.

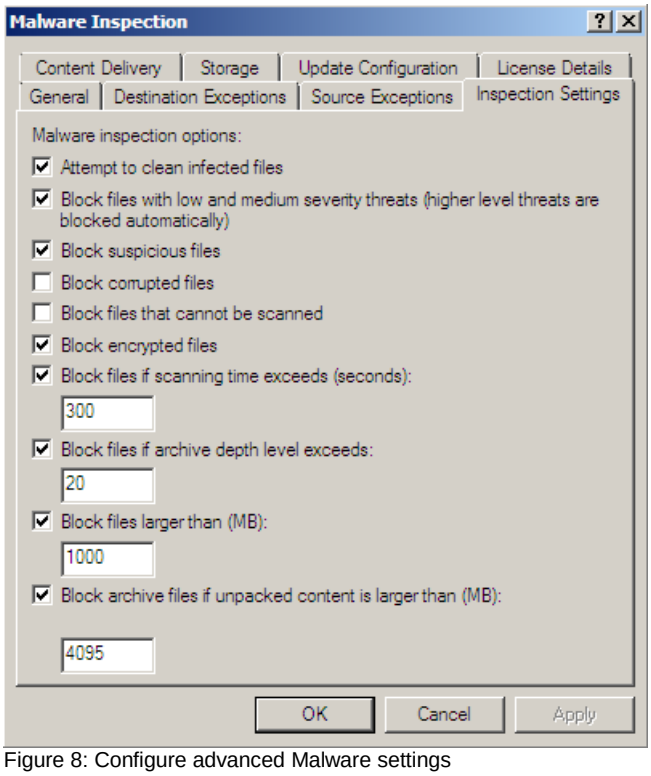

Figure 8: Configure advanced Malware settings

HTTPS outbound inspection

Microsoft ISA Server 2006 supports incoming HTTPS inspection in HTTPS bridging scenarios and Microsoft Forefront TMG extends this feature for outgoing HTTPS inspection.

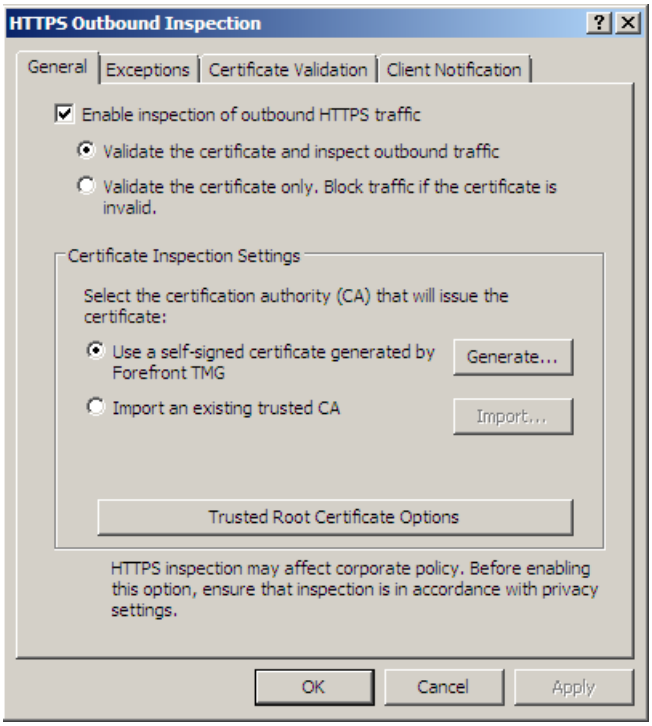

Figure 9: Configure HTTPS inspection settings

It is possible to configure several required certificate settings which are required for HTTPS inspection.

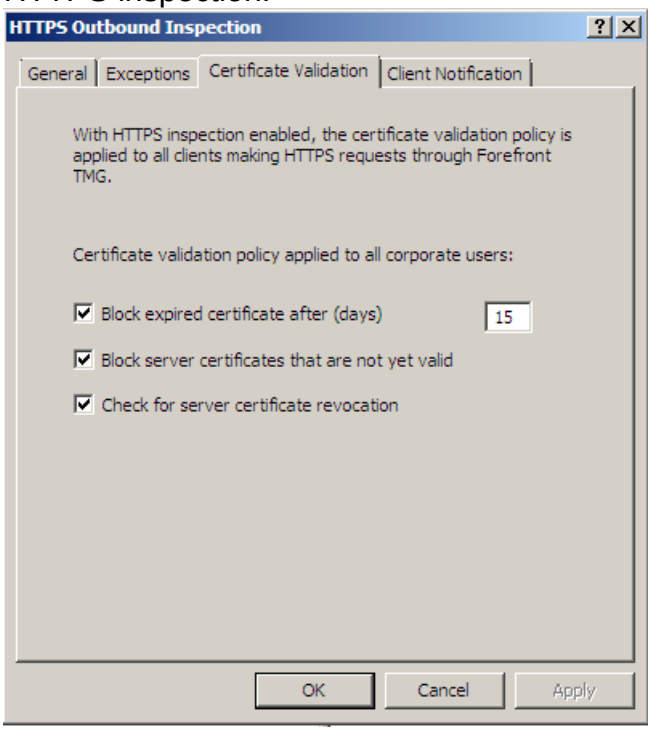

Figure 10: HTTPS inspection certificate settings

Clients can be notified when HTTPS Inspection is used.

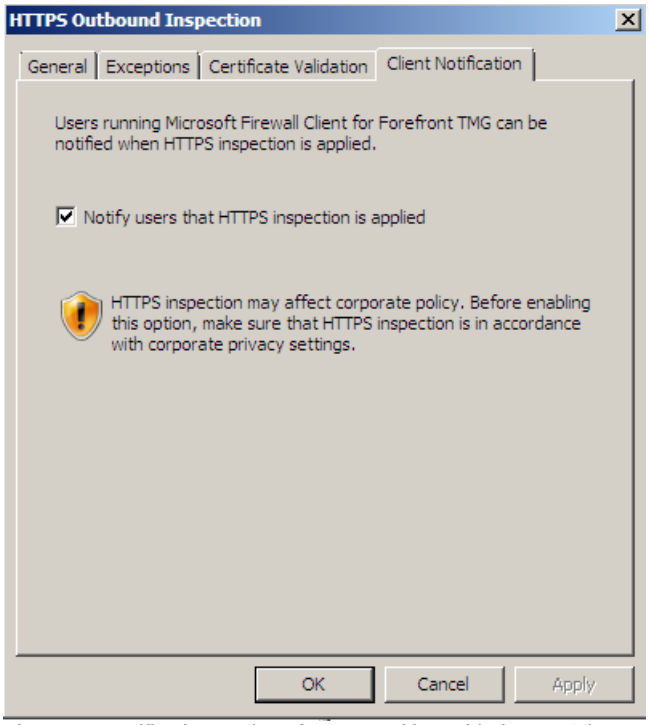

Figure 11: Notification settings for users with enabled HTTPS inspection

Antivirus and Antispam

Microsoft Forefront TMG dramatically extends its functionality in this way, that TMG can act as a SMTP inspection gateway and an antivirus server. The Antispam functionality is based on the Microsoft Exchange Server 2007 edge functionality and the Antivirus functionality on Microsoft Forefront Security. In Microsoft Forefront TMG there is a new Node called E-Mail Policy.

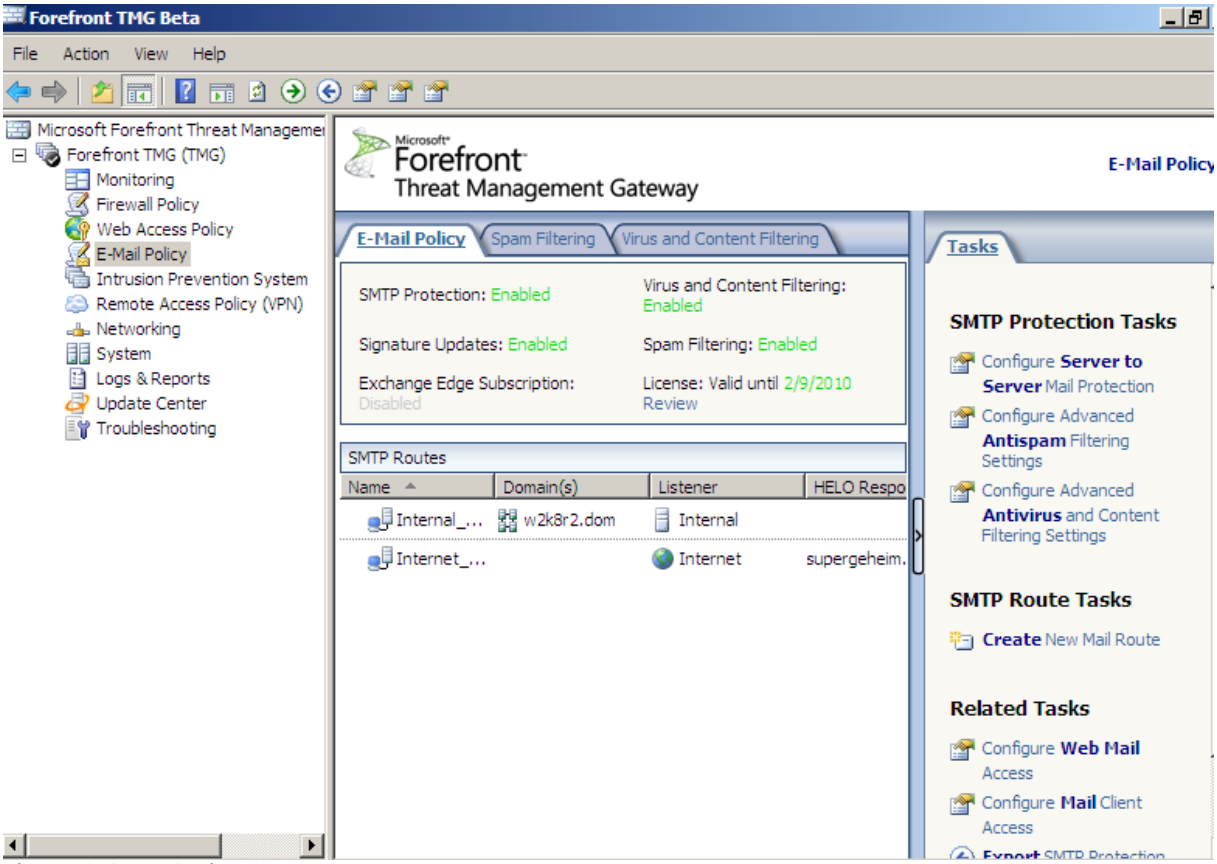

Figure 12: SMTP Settings

It is possible to configure mail flow settings and Antivrus and Antispam settings. All SMTP protection features can be enabled and disabled on a granular base.

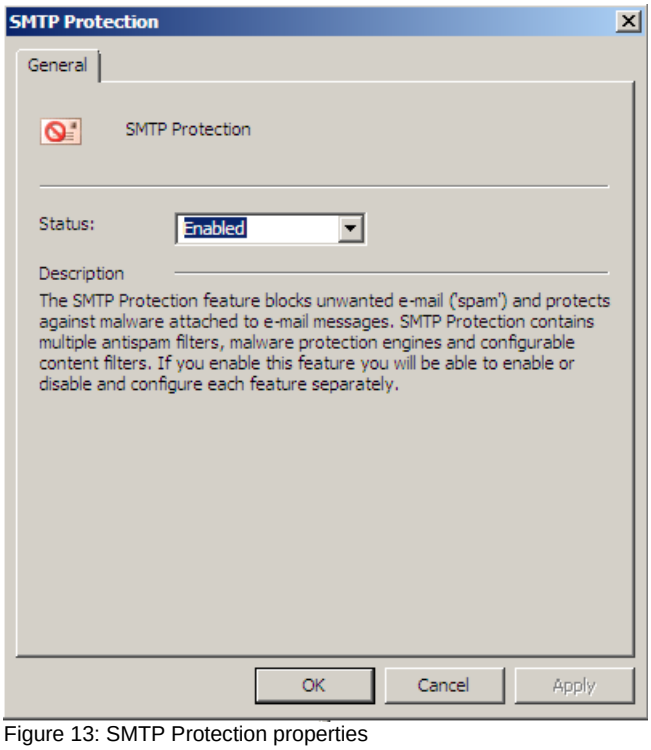

Figure 13: SMTP Protection properties

There are several spam filtering settings which are all based on the protection settings on Microsoft Exchange Server 2007 Edge Server.

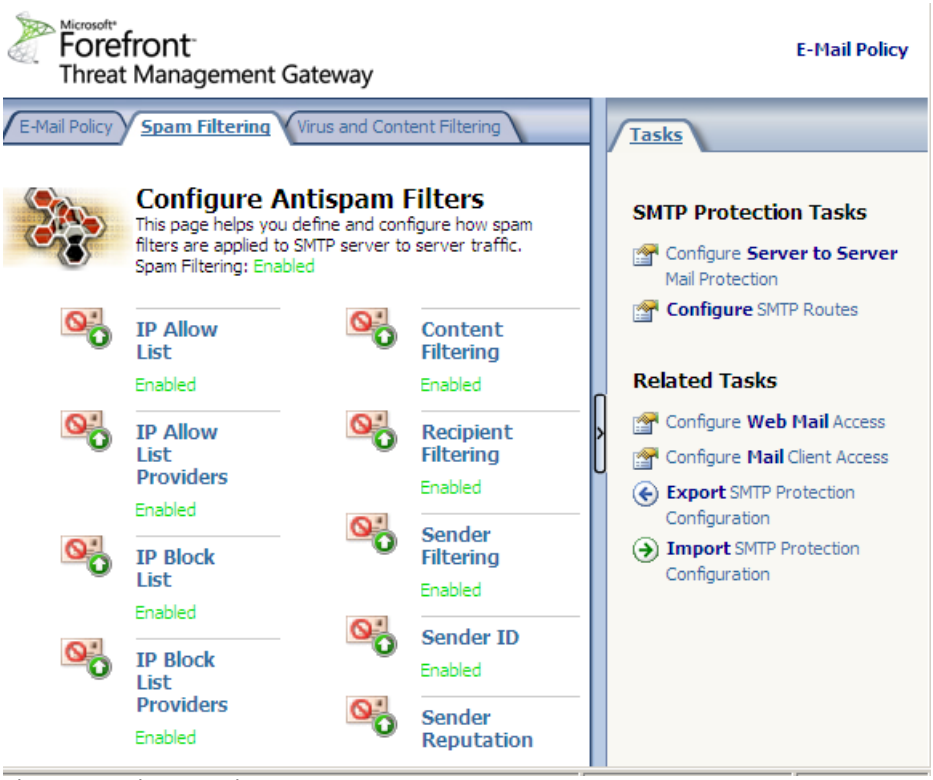

Figure 14: Antispam settings

Like in Exchange Server 2007 Edge, it is possible to configure Content Filtering settings and many more other approved Antispam settings.

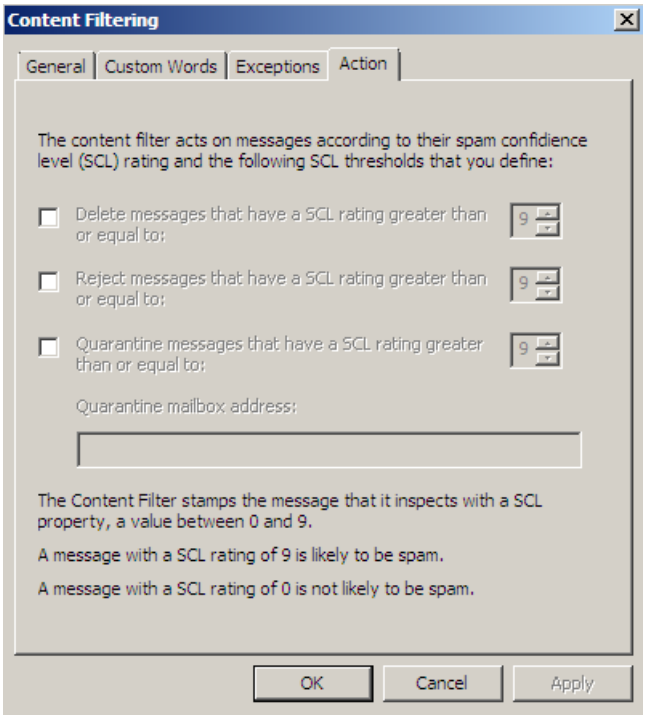

Figure 15: Content Filtering

Forefront TMG comes also with Antivirus components based on the Microsoft Forefront Security family.

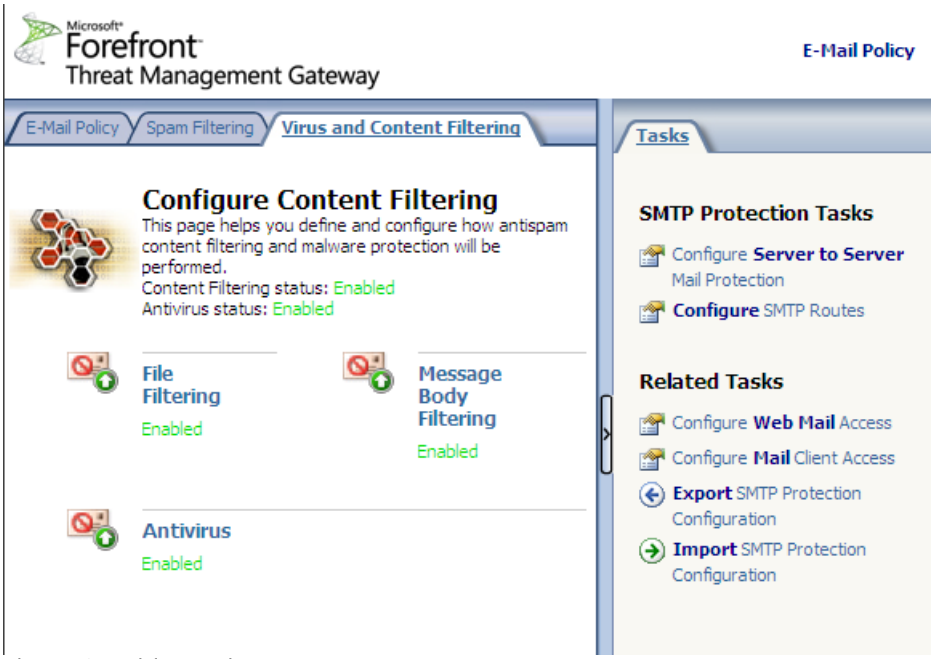

Figure 16: Antivirus settings

You can choose between several Antivirus engines. A maximum of five engines can be used at the same time (like in the original Microsoft Forefront Security products).

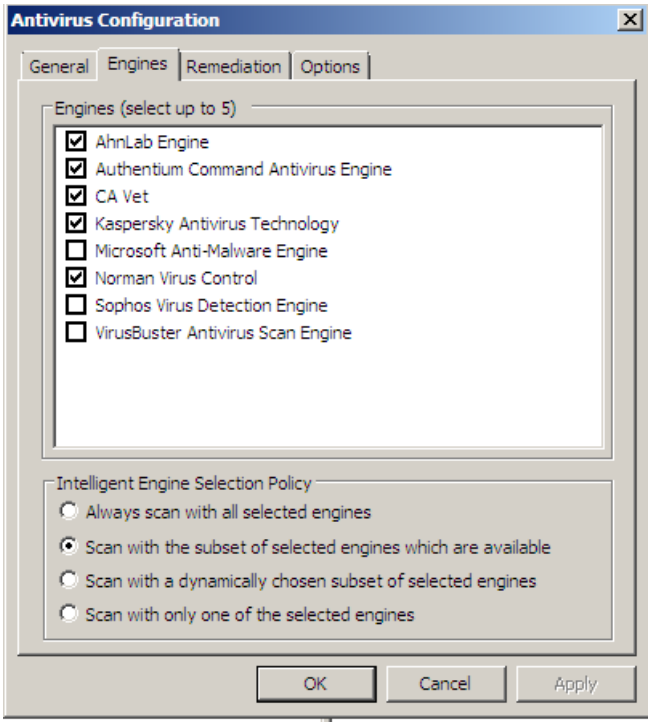

Figure 17: Antivirus engines

If a virus is detected it is possible to configure the actions to perform.

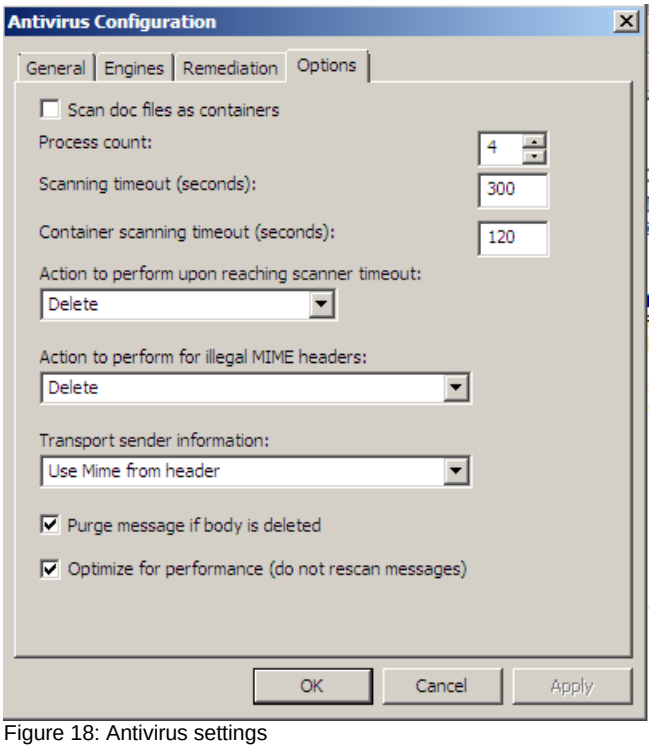

Figure 18: Antivirus settings

Conclusion

In this article, I tried to give you a high level overview about the new features and functionalities in Microsoft Forefront TMG. There are a l lot of new funny things and some functionality has been extended but there are also many not changed feature, so it should be possible to get familiar with the new Microsoft Firewall without learning from the beginning.

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
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
How to configure the Microsoft Forefront TMG Firewall Lockdown Mode and the new TMG Log queue feature (LLQ).
http://www.isaserver.org/tutorials/Explaining-Microsoft-Forefront-TMG-Firewall-Lockdown-Mode.html
Keeping High Availability with Forefront TMG's ISP Redundancy Feature
http://blogs.technet.com/isablog/archive/2009/02/16/keeping-high-availability-with-forefront-tmg-s-isp-redundancy-feature.aspx