Configuring and using the E-Mail protection feature in Microsoft Forefront Threat Management Gateway Beta 2 - Part 1

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 weeks 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 how Microsoft Forefront TMG acts as secure SMTP relay server and how TMG protects you mail servers with Anti-spam features. Part two of this article series will end with explaining some Anti-spam features and will show you the Anti-virus features in Microsoft Forefront TMG.

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. Other enhancements are:

- Frequent AV/AS signature and Block List updates
- Content and attachment filtering
- Automatic synchronization of Safe Sender List (Exchange 2007 only)

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. The screenshot shows the Anti-Spam configuration options in Microsoft Forefront TMG and these options are already known to Microsoft Exchange Server 2007 administrators because they are the same as in the Exchange Server 2007 Management console.

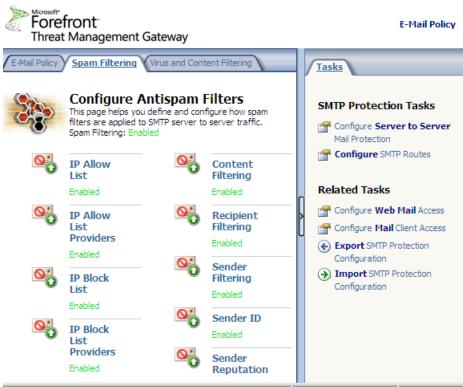


Figure 1: SPAM Filtering

The entire configuration of all related Anti-Spam, Anti-Virus and content filtering settings and the E-Mail policy settings (SMTP routing) are configured through the E-Mail Policy node in the TMG console.

Forefront TMG 8eta	_ 8 ×
File Action View Help	
Microsoft Forefront Threat Microsoft Forefront Threat Microsoft Forefront Forefront Threat Management Gateway Threat Management Gateway	E-Mail Policy
Web Access Policy E-Mail Policy Spam Filtering Virus and Content Filtering	Tasks
Intrusion Preventic SMTP Protection: Disabled Virus and Content Filtering: Disabled	
Remote Access Po Signature Updates: Enabled Spam Filtering: Disabled	SMTP Protection Tasks
System Exchange Edge Subscription: Disabled License: Valid until 2/27/2010 Review	Configure Server to Server
Undate Center V Troubleshooting SMTP Routes	Mail Protection
Name A Domain(s) Listener HELO Response	Related Tasks
	Configure Web Mail Access
	Configure Mail Client Access
	Configuration
	Import SMTP Protection Configuration

Figure 2: E-Mail Policy

The first step in configuring Microsoft Forefront Threat Management Gateway as a SMTP router you have to configure a Server to Server Mail Protection. This settings configures TMG to route E-Mail from your internal E-Mail servers to the Internet. When you create an SMTP route, you must specify a mail listener on your Forefront TMG server, the mail listener responds to requests from your internal SMTP servers and from external SMTP servers. If you enable spam and virus protection, Forefront TMG inspects mail traffic according to your configuration settings.

When you configure the e-mail policy, all configuration settings are stored for the entire TMG array. You need to configure the e-mail policy only once, and all TMG

array members receive the configuration when they synchronize with the Configuration Storage server.

In the following picture, I opened the Exchange Management console (EMC) to show people who are unfamiliar with Exchange Server 2007 how similar the settings in the Exchange Management console and the settings in the Microsoft Forefront TMG console are.

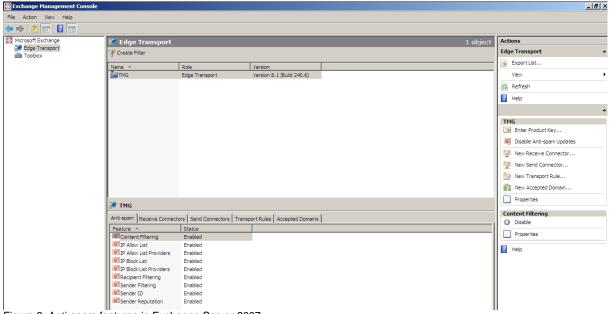


Figure 3: Anti-spam features in Exchange Server 2007

Microsoft Forefront Threat Management Gateway allows the configuration of the following Anti-Spam filters:

- Configuring spam filters
- Configuring the IP Allow List
- Configuring IP Allow List Providers
- Configuring the IP Block List
- Configuring IP Block List Providers
- Configuring Content Filtering
- Configuring Recipient Filtering
- Configuring Sender Filtering
- Configuring Sender ID
- Configuring Sender Reputation

Configure E-Mail protection

Let us start the configuration of the TMG e-mail services. Start the E-mail protection service wizard from the E-mail node, which will guide you through the entire process of configuring TMG as an SMTP relay server and a Anti-Spam, Anti-Virus solution.

E-mail Protection Configurat	ion Wizard	×
	Welcome to the E-mail Protection Wizard	
	This wizard helps you configure the mail protection features of Forefront TMG.	
	To continue, click Next.	
	Help about E-mail protection	
	< Back Next > Cano	el

Figure 4: E-Mail Protection Configuration Wizard

As a first step we have to specify our internal mail servers and the address space associated with these servers. Enter the Computer name and the IP address of your e-mail server and the accepted Mail server domains.

-mail Protection Configuration Wizard				×
Internal Mail Servers Configuration Specify internal mail servers and address spaces associated with them				\mathcal{H}
Please configure your internal servers:				
Computer name	Address			Add
EX07	10.10.10.5			Remove
				Remove
Accepted domains:				
it-training-grote.de				Add
				Remove
		< Back	Next >	Cancel

Figure 5: Internal Mail Servers Configuration

Specify the listener on which TMG should listen for outgoing e-mail requests. Typically, this should be the external network and there the IP address which is used for outgoing e-mail traffic which is important for reverse DNS lookups. Reverse DNS lookups are often used by several Anti-Spam technologies.

E-mail Protection Configuration Wizard Internal Listeners Configuration Specify properties of listener the internal servers	will use to send mail out	×
Listen for incoming requests on these networks:	Selected IPs <all addresses="" ip=""> <all addresses="" ip=""></all></all></all></all></all></all></all></all>	
,	Select Address	Cancel

Figure 6: Internal Listeners Configuration

With TMG it is possible to specify the FQDN (Fully Qualified Domain Name) where the listener is associated with the server to provide a response to HELO or EHLO requests. It is also possible to enable TLS (Transport Layer Security) which will be used to encrypt traffic with other mail servers which requires additional configuration.

E-mail Protection Configuration Wizard		×			
External Mail Routing Configuration Specify settings for route used for e-mail to and from the internet					
Specify FQDN the listener associated with the server will provide in response to HELO or EHLO:					
it-training-grote.de					
, Please configure how your organization will receive mail	from internet:				
Name	Selected IPs				
External	<all addresses="" ip=""></all>				
🗖 🛁 Internal	<all addresses="" ip=""></all>				
🗖 🛁 Local Host	<all addresses="" ip=""></all>				
Quarantined VPN Clients	<all addresses="" ip=""></all>				
🗖 😂 VPN Clients	<all addresses="" ip=""></all>				
🗖 🔹 All Networks (and Local Host)	<all addresses="" ip=""></all>				
🗖 🔹 All Protected Networks	<all addresses="" ip=""></all>				
Forefront codename Stirling Monitored Net	<all addresses="" ip=""></all>				
	Select Addresses				
TLS enabled					
	< Back Next >	Cancel			

Figure 7: External Mail Routing Configuration

If you want to use Anti-Malware and Anti-Spam functions, it is possible to activate these features.

E-mail Protection Configuration Wizard	×
Mail Protection Configuration Specify which protection methods to enable during e-mail processing	
Select protection features to enable, Terms of Use for subscription services (evaluation for now, pay later)	
✓ Enable Anti-Spam Features	
Enable Anti-Virus Features	
< Back Next > Cancel	

Figure 8: Mail Protection Configuration – Enable Anti-Spam and Anti-Virus Features

TMG must activate a system policy rule which allows TMG to receive and forward SMTP traffic and pass it to the Anti-Spam, Anti-Malware and content filter engines.

Microsoft	Forefront Threat Management Gateway Beta	×
?	For SMTP Protection feature, the system policy rules for SMTP Protection should be enabled. These rules will allow the Forefront TMG computer to receive and forward SMTP traffic and pass it through a set of antispam filters, content filters and malware protection engines. For more information, click the Help button. Do you want these system policy rules to be enabled?	
	Yes No Help	

Figure 9: A System Policy rule must be activated for SMTP traffic

The SMTP E-Mail protection wizard has finished its work. You can see the results of the wizard in the TMG Management console.

Forefront Threat Management Gateway						
E-Mail Policy Spam Filte	ering Virus and Conter	nt Filtering				
SMTP Protection: Enabled				Virus and Content Filtering: Enabled		
Signature Updates: Enabled	i			Spam Filtering: Enabled		
Exchange Edge Subscription	1: Disabled			License: Valid until 2/27/2010 Review		
SMTP Routes						
Name 🔺	Domain(s)	Listener	HELO Response			
Internal_Mail_Servers	🚦 it-training-grote.de	📑 Internal				
Internet_Mail_Servers		🎯 Internet	it-training-grote.de			

Figure 10: Established SMTP route

Microsoft Forefront TMG changes the configuration of the underlying Exchange Server 2007 Edge role. In the following screenshot you can see the Microsoft Exchange Server Management Console (EMC) and the receive connectors.

🔀 Exchange Management Console				
File Action View Help				
🗇 🔿 🙋 🖬				
🔀 Microsoft Exchange	🗊 Edge	Transport		
📝 Edge Transport 🖮 Toolbox	Vreate Filter			
	Name 🔺		Role	Version
	TMG		Edge Transport	Version 8.1 (Build 240.6)
	🔝 тмд			
	Anti-spam	Receive Connecto		port Rules Accepted Domains
	Name 🔺		Status	
	Interna	al_Mail_Servers	Enabled	
	📗 🚰 Interne	et_Mail_Servers	Enabled	

Figure 11: Exchange Server 2007 Edge Receive Connector configuration through EMC

The next screenshot shows the SMTP send connectors.

🔀 Exchange Management Console					
File Action View Help					
🗇 🔿 🖄 📊 🛛 🖬					
🔀 Microsoft Exchange	Create Filter				
🗊 Edge Transport 🕋 Toolbox					
	Name 🔺	Role	Version		
	ТМС	Edge Transport	Version 8.1 (Build 240.6)		
	🗊 тмg				
	Anti-spam Receive Connect	ors Send Connectors Transp	oort Rules Accepted Domains		
	Name 🔺	Status			
	Internal_Mail_Servers	Enabled			
	Internet_Mail_Servers	Enabled			

Figure 12: Exchange Server 2007 Edge Send Connector configuration through EMC

The following screenshots shows the accepted E-Mail domains which we previously created in the Forefront TMG console.

🔀 Exchange Management Console				
File Action View Help				
🗇 🔿 🙋 📧 🚺 🗊				
Microsoft Exchange	🗊 Edge Transport			
🗊 Edge Transport 🕋 Toolbox	🌱 Create Filter			
	Name 🔺	Role	Version	
	ТМG	Edge Transport	Version 8.1 (Build 240.6)	
	📝 тмд			
	Anti-spam Receive Connecto	ors Send Connectors Transp	ort Rules Accepted Domains	
	Name 🔺	Accepted Domain	Туре	Default
	🕺 it-training-grote.de	it-training-grote.de	Authoritative	True

Figure 13: Exchange Server 2007 Edge Accepted Domain configuration through EMC

If you configure some settings in the Microsoft Forefront Threat Management console, in this example a new content filter word, you can see the custom word after changes are committed to the TMG configuration in the Exchange Management console.

	front ^a t Management Gateway		
E-Mail Policy	Spam Filtering Virus and Content Filtering		
2	Configure Antispam Filters This page helps you define and configure how spam filters are applied to SMTP ser Spam Filtering: Enabled	rver to server t	traffic.
<u>8</u>	Content Filtering	<u>©</u>	Content Filtering Enabled Recipient Filtering
<u> </u>	Add Remove	<u> </u>	Enabled Sender Filtering Enabled
<u>©</u>		0	Sender ID Enabled
	Messages containing these words or phrases will be blocked, unless the message contains a word or phrase from the list above:	°°	Sender Reputation Enabled
	OK Cancel Apply		

Figure 14: Content filtering through Microsoft Forefront TMG configuration

The custom word in the Exchange Management console.

Content Filtering Properties	×
General Custom Words Exceptions Action	
Messages containing these words or phrases will not be blocked:	
🖞 Add 🗙	
Cisco PIX	
Messages containing these words or phrases will be blocked, unless the message contains a word or phrase from the list above:	
🖶 Add 📉	
OK Cancel Apply Help	

Figure 15: Filter custom words

It is possible to activate or to deactivate the SMTP protection feature in the TMG console.

SMTP Prot	ection			×		
General						
<u>O</u> :	SMTP Protection					
Status:	Enabled	_				
Description The SMTP Protection feature blocks unwanted e-mail ('spam') and protects against malware attached to e-mail messages. SMTP Protection contains multiple antispam filters, malware protection engines and configurable						
content	filters. If you enable and configure each fe	this feature yo	ou will be able to e			
		OK	Cancel	Apply		

Figure 16: Enable or disable the SMTP protection feature in TMG

It is possible to activate or to deactivate the Anti-Spam protection feature in the TMG console.

Anti-spam Configuration	x
General	
Anti-spam Configuration	
Status:	
Description The Anti-spam feature passes each message through a set of filters that decide whether or not it is considered 'spam'. You can enable each filtering feature constraints and curtering it to fit your constraints passed	
feature separately and customize it to fit your organization's needs.	
OK Cancel Apply	

Figure 17: Enable or disable the Anti-spam configuration in TMG

An Anti-Spam and Anti-Virus solution is only effective, when there are permanent updates to ensure the full functionality of the TMG capabilities. In the current Beta 2 release you will use an evaluation license.

Update Service State Properties	×				
Update Configuration License Details					
License name: E-Mail Pro	stection				
Applies to:	Service Antispam Filtering E-Mail Antivirus				
License agreement number:	Evaluation				
Expiration date:	2/27/2010				
Note: this feature downloads and installs updates from Microsoft by default. <u>Help about updating license agreements</u>					
ОК	Cancel Apply				

Figure 18: Configuring Update Service settings in TMG

Conclusion

In this first part of this article series, I gave you an overview about how Microsoft Forefront Threat Management Gateway protects your internal e-mail servers against SPAM and how TMG acts as an SMTP proxy for e-mail relaying. In the second part of this article series, I will show you the Antivirus capabilities of Microsoft Forefront Threat Management Gateway and some content features.

Related links

Forefront Threat Management Gateway Beta 2 http://www.microsoft.com/downloads/details.aspx?FamilyID=e05aecbc-d0eb-4e0fa5db-8f236995bccd&DisplayLang=en Forefront TMG Beta 2 is Released http://blogs.technet.com/isablog/archive/2009/02/06/forefront-tmg-beta-2-isreleased.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