# Contents

**Introduction**

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Planning Forefront Protection for Exchange Server</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding Forefront Protection for Exchange Server</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Architecture</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Software and Hardware Requirements</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Performance Considerations</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Edge Transport Role Considerations</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Hub Transport Role Considerations</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Mailbox Role Considerations</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Administrator’s Punch List</td>
<td>12</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 2</th>
<th>Installing and Configuring Forefront Protection for Exchange Server</th>
<th>13</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing Forefront Protection for Exchange Server</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Opening the Console</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Configuring Forefront Protection for Exchange Server</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Anti-Malware</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Anti-Spam</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>Filters</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td>Online Protection</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>Global Settings</td>
<td>52</td>
<td></td>
</tr>
<tr>
<td>Administrator’s Punch List</td>
<td>58</td>
<td></td>
</tr>
</tbody>
</table>

---

*What do you think of this book? We want to hear from you!*
### Chapter 3  Protecting your Mail System on the Edge with Forefront TMG Email Protection  

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding the Forefront TMG Email Protection</td>
<td>59</td>
</tr>
<tr>
<td>Software and Hardware Requirements</td>
<td>63</td>
</tr>
<tr>
<td>Installing and Configuring Email Protection</td>
<td>64</td>
</tr>
<tr>
<td>Installing Exchange 2010 Edge Transport Role</td>
<td>65</td>
</tr>
<tr>
<td>Installing Forefront Protection for Exchange Server</td>
<td>69</td>
</tr>
<tr>
<td>Email Protection Configuration</td>
<td>70</td>
</tr>
<tr>
<td>Administrator’s Punch List</td>
<td>77</td>
</tr>
</tbody>
</table>

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit: [www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)
Acknowledgments

This Microsoft Forefront project took almost a year to write and resulted in three separate books about deploying Forefront products. Although the authors get lots of credit, there can be little doubt that we could not have even begun, much less completed, this book without the cooperation (not to mention the permission) of an incredibly large number of people.

It’s here that we’d like to take a few moments to express our gratitude to the folks who made it all possible.

With thanks...

To the folks at Microsoft Press, who made the process as smooth as they possibly could: Karen Szall, Devon Musgrave, and their crew.

To the Forefront Protection for Exchange CSS Team who helped us so much in shaping this book; with special thanks to: Ryan McGrath, Alexandre Hollanda, Dan Takata, Craig Wiand, and Neil Carpenter. Your rich contributions are highly appreciated.

From Yuri

First and foremost to God, for blessing my life, leading my way, and giving me the strength to take on the challenges as just another step in life. To my eternal supporter in all moments of my life: my wife Aleksandra. To my daughters who, although very young, understand when I close the office door and say, “I’m really busy.” Thanks for understanding. I love you, Yanne and Ysis.

To my friend Thomas Shinder, whom I was fortunate enough to meet three years ago. Thanks for shaping my writing skills and also contributing to my personal growth with your thoughts, advice, and guidance. Without a doubt, these long months working on this project were worth it, because of our amazing partnership. I can’t forget to thank the two other friends who wrote the Microsoft Forefront Threat Management Gateway Administrator’s Companion with me: Jim Harrison and Mohit Saxena. They were, without a doubt, the pillars of this writing career in which I’m now fully engaged. Thanks, guys. I also want to thank, as Jim says, “da Boyz”: Tim “Thor” Mullen, Steve Moffat, and Greg Mulholland. You guys are amazing. Thanks for sharing all the tales.

To all the folks from CSS Security who support Forefront Protection for Exchange on a daily basis, especially Andrew Davis, Jess Huber, John Moracho, and
Bob Payton. You guys rock! Also, to my friends from the Exchange Team for their outstanding partnership, especially Vandy Rodrigues, Tim Heeney, Charlene Weber, Will Duff, Austin McCollum, Julio Vieira, and Mohammad Nadeem.

**From Tom**

As Yuri does, I acknowledge the blessings from God, who took “a fool like me” and guided me on a path that I never would have chosen on my own. The second most important acknowledgement I must make is to my beautiful wife, Deb Shin-der, whom I consider my hand of God. Without her, I don’t know where I would be today, except that I know that the place wouldn’t be anywhere near as good as the place I am now.

I also want to acknowledge my good friend Yuri Diogenes, my co-writer on this project. Yuri really held this project together. I had just started working for Microsoft and was learning about the ins and outs of the Microsoft system, and I was also taking on a lot of detailed and complex projects alongside the writing of this book. Yuri helped keep me focused, spent a lot of time pointing me in the right direction, and essentially is responsible for enabling me to get done what I needed to get done. I have no doubt that, without Yuri guiding this effort, it probably never would have been completed.

Props go out to Jim Harrison, “the King of TMG,” as well as to Greg Mulholland, Steve Moffat, and Tim Mullen. You guys were the moral authority that drove us to completion. I also want to thank Mike Chan for giving me the opportunity to work as a Technical Account Manager (TAM) for the Business Productivity Online Suite (BPOS) prior to my working for Microsoft.
Introduction

When we began this project, our intent was to create a real-world scenario that would guide IT professionals in using Microsoft best practices to deploy Microsoft Forefront Protection for Exchange Server (FPE) 2010. We hope you find that we have achieved that goal. We’ve also included a thorough explanation of the architectural side of the product, which we consider an advantage for you, because the explanation of the technical details was reviewed by engineers who work directly on the FPE team at Microsoft Customer Service and Support (CSS).

This book provides administrative procedures, tested design examples, quick answers, and tips. In addition, it covers some of the most common deployment scenarios and describes ways to take full advantage of the product’s capabilities. It covers pre-deployment tasks, software and hardware requirements, performance considerations, and installation and configuration, using best practice recommendations.

Who Is This Book For?

*Deploying Microsoft Forefront Protection for Exchange Server 2010* covers FPE in an Exchange Server 2010 environment. This book is designed for:

- Administrators who are deploying FPE
- Administrators who are experienced with Windows Server 2008 and Exchange Server 2010
- Current Forefront Security for Exchange administrators
- Administrators who are new to FPE
- Technology specialists, such as messaging administrators and security administrators

Because this book is limited in size and we want to provide you with the maximum value, we assume a basic knowledge of Windows Server 2008, Active Directory, and Exchange Server. These technologies are not discussed in detail, but this book contains material on all of these topics as they relate to Forefront Protection for Exchange’s administrative tasks.
How Is This Book Organized?

Deploying Microsoft Forefront Protection for Exchange Server 2010 is written to be a deployment guide and to serve as a source of architectural information related to the product. The book is organized in such a way that you can follow the steps to plan and deploy the product. The steps are based on a deployment scenario for the company Contoso. As you go through the steps, you will also notice tips for best practices implementation. At the end of each chapter, you will see an “Administrator's Punch List,” in which you will find a summary of the main administrative tasks that were covered throughout the chapter. This is a quick checklist to help you review the main deployment tasks.

The book is organized into three chapters to cover three deployment topics: planning, installation and configuration, and using the Microsoft Forefront Threat Management Gateway (TMG) for email protection.

We really hope you find the Deploying Microsoft Forefront Protection for Exchange Server 2010 useful and accurate. We have an open door policy for email at mspress.fpebook@tacteam.net, and you can contact us through our personal blogs and Twitter accounts:


Support for This Book

Every effort has been made to ensure the accuracy of this book. As corrections or changes are collected, they will be added to the O’Reilly Media website. To find Microsoft Press book and media corrections:

2. In the Search box, type the ISBN for the book, and click Search.
3. Select the book from the search results, which will take you to the book’s catalog page.

If you have questions regarding the book or the companion content that are not answered by visiting the book’s catalog page, please send them to Microsoft Press by sending an email message to mspinput@microsoft.com.
We Want to Hear from You

We welcome your feedback about this book. Please share your comments and ideas through the following short survey:

http://www.microsoft.com/learning/booksurvey

Your participation helps Microsoft Press create books that better meet your needs and your standards.

NOTE  We hope that you will give us detailed feedback in our survey. If you have questions about our publishing program, upcoming titles, or Microsoft Press in general, we encourage you to interact with us using Twitter at http://twitter.com/MicrosoftPress. For support issues, use only the email address shown earlier.
CHAPTER 3

Protecting your Mail System on the Edge with Forefront TMG Email Protection

- Understanding the Forefront TMG Email Protection Feature 59
- Software and Hardware Requirements 63
- Installing and Configuring Email Protection 64

While maintaining a secure messaging infrastructure within your network is important, having a central repository for the configuration for your Edge role also has value. With Microsoft Forefront Threat Management Gateway (TMG) 2010, a new concept of email protection was introduced that combines the three main products that can help protect the network and the messaging infrastructure in a single management console. In this chapter you will learn how the email protection feature works and how to configure it on Forefront TMG.

NOTE You can find detailed information about Forefront TMG in Microsoft Forefront Threat Management Gateway (TMG) Administrator’s Companion (Microsoft Press, 2010).

Understanding the Forefront TMG Email Protection Feature

Forefront TMG comes with a new feature called email protection. This feature allows the integration of three major components of Microsoft’s protection and messaging solution, which are: the Edge Transport role of Microsoft Exchange 2010, Microsoft Forefront Protection for Exchange Server (FPE), and Forefront TMG. Figure 3-1 shows the main components of this solution.
The TMG Filter driver (FWENG) is the first component to receive email traffic (in a bottom to top approach). FWENG runs in kernel mode, and it performs the initial inspection of a packet. Once this inspection is done, and assuming that the traffic is allowed, the packet is identified as belonging to the Email Protection component because it is an email. At this point, the Exchange Edge components take over and process the request via the Exchange Edge Receive Connector.

A series of inspections are done on the Exchange side, according to the system configuration, and then the traffic is handed over to the FPE component. This component determines whether or not the message is spam, and it scans the message using other tests. Assuming that the inspection completes successfully and the traffic is allowed, the Send connector of the Exchange Edge Transport role is used to send the message through the TMG Filter driver again, for the final outbound inspection, before it goes to the destination. Table 3-1 shows the core components of the protection and indicates the product or products that handle each component.

**TABLE 3-1** Component breakdown

<table>
<thead>
<tr>
<th>FEATURES</th>
<th>EXCHANGE EDGE ROLE</th>
<th>FOREFRONT PROTECTION FOR EXCHANGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Allow/Block Lists</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>IP Allow/Block List Providers</td>
<td>X (Custom)</td>
<td>X (DNS Block List or DNSBL)</td>
</tr>
<tr>
<td>Sender/Recipient Filtering, Sender ID</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sender Reputation</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Basic Content Filtering (SmartScreen)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Premium Anti-spam (Cloudmark)</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>File Filtering</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Message Body Filtering</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Antivirus and Antispyware</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

After installing Forefront TMG, a new service called Microsoft Forefront TMG Managed Control Services is created. This service is responsible for handling the managed code portion of TMG, which is used for Exchange configuration and other managed code. This service monitors the state of the configuration to make sure that what is configured on the TMG interface and what is present on Exchange Edge and FPE are in sync.

TMG will poll the Exchange configuration periodically and compare it to its own configuration. If there is a mismatch, TMG will reconfigure Exchange to match its own configuration. TMG checks only those Exchange configuration elements of which it is aware; it ignores settings that are not set up through the TMG console. If a configuration can’t be set, TMG alerts the administrator. In the case of the Edge Subscription, the polling takes into account the fact that only part of the configuration is controlled by Forefront TMG, and the part not controlled by Forefront TMG will not be polled.

In summary, the default behavior of the Forefront TMG is as follows:

- Changes of email policy are done only through the Forefront TMG console.
- The TMG Managed Control Service will identify those changes and replicate them with the other components (Exchange Edge and Forefront Protection for Exchange).
- If the administrator makes changes directly on Exchange Edge through the Exchange management console, those changes will be overwritten by the settings on the Forefront TMG Console.
- An alert will appear on Forefront TMG, warning that the email policy changed and that the configuration will be reapplied.

**NOTE** When Exchange 2010 SP1 was released, some cmdlets were removed, causing TMG Managed Control Service to fail to start. For more information on this behavior, see [http://blogs.technet.com/b/isablog/archive/2010/09/01/problems-when-installing-exchange-2010-service-pack-1-on-a-tmg-configured-for-mail-protection.aspx](http://blogs.technet.com/b/isablog/archive/2010/09/01/problems-when-installing-exchange-2010-service-pack-1-on-a-tmg-configured-for-mail-protection.aspx).

- Changes that are processed through Exchange PowerShell cmdlet can cause the TMG Managed Control Service to fail to start, with the error 0x80070057. The workaround for this is to undo those changes using Windows PowerShell cmdlet.

**NOTE** It is expected that this behavior will be changed on Forefront TMG SP1 Update 1. With Update 1, the changes made via Exchange Edge console or Windows PowerShell will be merged and the TMG Managed Control service shouldn’t fail in such circumstances.
Each of the three products that comprise the email protection solution on Forefront TMG requires its own license. In other words, you will need a license for Exchange Edge and a license for Forefront Protection for Exchange, in addition to the license that you should already have for Forefront TMG. The solution is vendor-independent in the sense that it can protect any SMTP server that is behind TMG. You can have a non-Microsoft messaging solution in the internal organization and use the Forefront TMG email protection feature on the Edge to protect the messaging environment. The only feature that will not work in this case is the Exchange Edge Subscription because it requires Exchange on the back end to work. Figure 3-2 shows a network that has two email solutions and is using Email Protection on the Edge to filter the traffic.

**NOTE** The most common questions and answers about this solution can be found in “Understanding E-Mail Protection on Forefront TMG,” at http://technet.microsoft.com/en-us/library/ee338733.aspx.
Software and Hardware Requirements

There are software and hardware prerequisites that must be met to enable the Email Protection feature on Forefront TMG. For hardware, you should start by assessing your environment’s needs and traffic profile. Once you have all the information related to those two main elements you can use the Forefront TMG Capacity Planning tool. Figure 3-3 shows the Capacity Planning tool and the feature list in which you can indicate that the Mail Protection feature is going to be enabled in this deployment.


![Capacity Planning Tool v1.0](image)

**FIGURE 3-3**

The software requirements are a bit more diverse and need to be carefully planned. Table 3-2 shows the software needed and supported for the Email Protection feature to work on Forefront TMG.
TABLE 3-2 Software requirements for the Enable Email Protection feature

<table>
<thead>
<tr>
<th>SOFTWARE</th>
<th>VERSION</th>
<th>SUPPORTABILITY</th>
<th>SUPPORTED PLATFORM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Edge Role</td>
<td>2007 RTM</td>
<td>Not supported</td>
<td>NA</td>
</tr>
<tr>
<td>Exchange Edge Role</td>
<td>SP2</td>
<td>Supported</td>
<td>Windows Server 2008 SP2* or R2</td>
</tr>
<tr>
<td>Exchange Edge Role</td>
<td>2010</td>
<td>Supported</td>
<td>Windows Server 2008 SP2 or R2</td>
</tr>
<tr>
<td>Forefront Protection for Exchange Server</td>
<td>2010</td>
<td>Supported</td>
<td>Windows Server 2008 SP2 or R2</td>
</tr>
<tr>
<td>Forefront TMG</td>
<td>MBE</td>
<td>Not supported</td>
<td>NA</td>
</tr>
<tr>
<td>Forefront TMG</td>
<td>2010</td>
<td>Supported</td>
<td>Windows Server 2008 SP2 or R2</td>
</tr>
</tbody>
</table>


It is important to emphasize that each piece of software that is listed in Table 3-2 has its own prerequisites list that you will need in order to install that software. If you don’t have Forefront TMG installed yet and want to build the complete solution, the steps below are necessary to enable the Email Protection capability:

1. Install Active Directory Lightweight Directory Services (AD LDS).
2. Install the Exchange Server Edge Transport role.
3. Install Forefront Protection for Exchange Server.
4. Install Forefront TMG.


**Installing and Configuring Email Protection**

For the purpose of this instruction, the topology shown in Figure 3-4 will be used to perform the installation of the Exchange Edge role and Forefront Protection for Exchange Server. This scenario assumes that Forefront TMG is already installed.
NOTE If you are installing Forefront TMG on a standalone server in a workgroup, it will be necessary to configure the DNS suffix for the server under the computer’s Properties, Advanced System Settings.

Installing Exchange 2010 Edge Transport Role

Complete the following steps to install the Exchange Edge Transport role on an existing Forefront TMG installation:

1. Insert the Exchange 2010 DVD and run the setup.msi. The Welcome page, shown in Figure 3-5, appears.
2. Steps 1 and 2 are grayed and no longer available, because those prerequisites are already met. Click Step 3: Choose Exchange Language Option, and then choose Install Only Languages From The DVD.


4. On the License Agreement page, read the license terms, click I Accept The Terms In The License Agreement, and then click Next to proceed.

5. On the Error Reporting page, you can either enable or disable Error Reporting. Click Yes (Recommended) to enable Error Reporting, and then click Next to continue.

6. On the Exchange Server 2010 Setup page, shown in Figure 3-6, select the Installation Type. Click Custom Exchange Server Installation, and then click Next.
7. On the Server Role Selection page, click Edge Transport Role, as shown in Figure 3-7, and then click Next.

8. The Customer Experience Improvement Program page, which appears next, lets you indicate whether you want to participate in this program. Make a selection, and then click Next.
9. The Exchange Server 2010 Setup Wizard starts the Readiness Checks, which verify that all the prerequisites have been met for the selected role, in this case, Edge Transport. If all prerequisites are in place, the Readiness Checks page appears as shown in Figure 3-8. Click Install to proceed.

![FIGURE 3-8]

10. Once the installation is finished, the Exchange Server 2010 Setup Wizard displays the Completion page, shown in Figure 3-9. Clear the Finalize This Installation Using The Exchange Management Console checkbox, and then click Finish.

![FIGURE 3-9]
11. On the Welcome page, shown in Figure 3-5, click Step 5: Get Critical Updates For Microsoft Exchange.

12. After installing the updates, click Close.

**Installing Forefront Protection for Exchange Server**

The steps to install Forefront Protection for Exchange Server are described in Chapter 2, “Installing and Configuring Forefront Protection for Exchange Server.” The only difference here is that you will launch the FPE installation directly from the Forefront TMG setup screen. Once you insert the Forefront TMG DVD, autorun launches the setup. Choose Install Microsoft Forefront Protection 2010 For Exchange Server, as shown in Figure 3-10.

![Forefront TMG](image)

**FIGURE 3-10**

Then follow the steps detailed in Chapter 2.

**NOTE** Installing FPE from this window—that is, downloading from the Web site—is not required, although it is an option. You can install FPE directly from the installation CD.
Email Protection Configuration
When configuring Email Protection on Forefront TMG, the first step after the installation of all prerequisites is to configure SMTP Routes. These routes will be responsible for creating the Exchange inbound and outbound connectors. After the routes are configured, you can enable spam filtering and virus and content filtering.

Email Policy
To configure the Email Policy, you will need:
- The name/IP address of the Exchange Hub Transport Server.
- The name of the MX record that will be use for the SMTP server.

You will also need to define:
- The TMG network interface that will communicate with this Exchange Hub Transport Server.
- The TMG network interface that will communicate with the Internet, as well as the IP address that will be used to publish the SMTP to the outside world.

When you have this information, you are ready to start the Email Policy configuration:

1. Open the Forefront TMG Management Console, click Email Policy, and, in the Tasks pane on the right side of the console, click Configure Email Policy.
2. On the Welcome To The Email Policy Wizard page, click Next.
3. The Internal Mail Server Configuration step allows you to define two options: the internal mail server to which TMG will send emails, and the domain from which TMG will accept messages.
   a. Click Add beside Internal Mail Servers, and add the Computer Name and IP Address for the Exchange 2007 Hub Transport Server; for this scenario (shown earlier in Figure 3-4), type 10.20.20.11.
4. Beside Accepted Authoritative Domains, click Add, and add the name of the domain that will accept messages; for this scenario type *.contoso.com, as shown in Figure 3-11. If you have multiple domains within your organization, you can enter the names of all of those domains in this box.
   a. Click Next to proceed.
5. On the Internal Email Listener Configuration page, you define the network interface that TMG will use to communicate with the Exchange Hub Transport Server. For this example, select Internal, as shown in Figure 3-12, and then click Next.

6. On the External Email Listener Configuration page, select the interface that will connect with the Internet; in this case, select External. If you have multiple IP addresses on the External interface, you can click Select Addresses and specify an individual IP address that will be used to listen on port 25. In the FDQN Or IP Address box, enter the FQDN that will appear as the response to a HELO or EHLO SMTP command; in this case, type mail.contoso.com, as shown in Figure 3-13.
7. On the Email Policy Configuration page, leave Enable Spam Filtering and Enable Virus And Content Filtering enabled. (These options are discussed in more detail in the “Virus and Content Filtering” section later in this chapter.) Click Next, and then click Finish to conclude the wizard.

8. An informational window appears asking if you want to enable the System policy to allow the SMTP traffic. Click Yes to continue. The Email Policy tab (Figure 3-14) should now show the two SMTP Routes that were created.

9. Click Apply, type a description of this change, click Apply, and then click OK. Forefront TMG will update the Exchange Edge Transport configuration and will create receive and send connectors based on the settings that were selected in the Email Policy
Wizard. For a better management experience between Edge and Hub Transport, enable Edge Sync traffic by following these steps:

1. In the Tasks pane on the right, select the Enable Connectivity For EdgeSync Traffic option. A window appears informing you that system policies will be enabled to allow this communication. TMG does this automatically by enabling system policy 47 (Allow LDAP/LDAPS traffic to the local host for the Exchange Server EdgeSync synchronization process). Click OK to continue.

2. In the Tasks pane, click Generate Edge Subscription Files, choose the location to which you will save this file, and then click OK.

3. When the file is successfully exported, an informational window appears saying that the Edge Subscription was created in the location that you chose. Click OK to continue.

4. Right-click Internal_Mail_Servers in the Email Policy pane, and then click Properties.

5. Click the Listener tab, and then click Advanced.

6. Make sure to configure an authentication method that matches the method used by Exchange Hub Transport. The most common authentication method combines Transport Security Layer (TLS) and Exchange Server Authentication, as shown in Figure 3-15.

![Advanced settings for Edge subscription](image)

**FIGURE 3-15**

7. Click OK twice, click Apply, type a description of this change, click Apply, and then click OK.

8. Copy the Edge subscription file created in Step 2 to the Exchange Hub Transport Server. Then, on that server, open the Exchange Management Console, expand Organization Configuration, and then click Hub Transport.

9. On the Hub Transport actions pane, click New Edge Subscription. Next to the Active Directory Site box, click Browse, and then select Default-First-Site-Name. Next to the Subscription File box, click Browse, and then choose the file generated by Forefront TMG, as shown in Figure 3-16. Click New to conclude.
10. On the Completion page, review the results, and then click Finish.
11. Click the Send Connectors tab, right-click EdgeSync – Inbound To Default-First-Site-Name, and then choose Properties.
12. Click the Network tab, and then click Change.
13. Make sure that the authentication method selected here matches at least one authentication method that was selected in Step 6. Exchange Server Authentication is selected by default. Click OK twice to conclude.
14. To force the synchronization, open the Exchange Management Shell prompt, type **Start-EdgeSynchronization**, and click Enter.


**Spam Filtering**

The Spam Filtering options on Forefront TMG, as shown in Figure 3-17, are the same spam filtering options that are available on the Exchange Edge role, as shown in Figure 3-18.
The anti-spam options that are available on the Edge role and configured by TMG are:

- **Content Filtering** Filters emails based on the settings that you define for the content inspection.

- **IP Allow List** Lets you specify one or more IP addresses that are considered to be trusted and should always be allowed to send email.

- **IP Allow List Providers** Lets you maintain a list of IP addresses that are known not to be associated with any type of spam activity.

- **IP Block List** Lets you to specify one or more IP addresses that should never be allowed to establish an SMTP connection with TMG.

- **IP Block List Providers** Lets you specify providers that are known to send (or are suspected of sending) spam.

- **Recipient Filtering** Lets you specify a list of email addresses or a distribution list that would like to receive emails from outside your organization.
- **Sender Filtering**  Lets you block a source address from sending messages to your organization.
- **Sender ID**  Verifies the source of a message to determine whether the organization is what it claims to be.
- **Sender Reputation**  Relies on persistent data about the sender to determine what action, if any, to take when an inbound message arrives.

**NOTE**  You can find more information about the Spam Filtering option in *Microsoft Forefront Threat Management Gateway (TMG) Administrator’s Companion* (Microsoft Press, 2010), Chapter 19, “Enhancing E-Mail Protection.”

### Virus and Content Filtering

The Virus and Content Filtering options in TMG, shown in Figure 3-19, are the same as the options that were described in Chapter 2, “Installing and Configuring Forefront Protection for Exchange Server.”

![Figure 3-19: Configure Virus and Content Filtering](image)

**NOTE**  Refer to Chapter 2, “Installing and Configuring Forefront Protection for Exchange Server,” for more information about the File Filtering, Virus Filtering, and Message Body Filtering options.
Administrator’s Punch List

In this chapter, you learned about the way the Email Protection feature works, and the way Forefront TMG integrates with the Exchange Edge role and with Forefront Protection for Exchange Server to improve your administrative experience. When deploying Email Protection on Forefront TMG, keep the following points in mind:

- Although there is a single point of configuration for Email Protection, it is important that you understand the boundaries of each product in order to better configure the protection and troubleshoot any problems.
- Planning before deployment is always the best practice to follow. Be sure to use the Forefront TMG Capacity Planning tool to correctly size your Email Protection solution.
- Keep in mind that you will need a license for Exchange Edge and a license for Forefront Protection for Exchange, in addition to the license for Forefront TMG, to enable the Email Protection feature on the Edge.
- If you are deploying Forefront TMG or SP1, do not use Exchange PowerShell cmdlets to make changes, so that you are sure to avoid problems on the Forefront TMG Managed Control Service.
- The installation process for the Exchange Edge Transport role and Forefront Protection for Exchange Server is the same as the process specified in the product documentation.
- To allow a better experience while administering Exchange Hub Transport and Exchange Edge, be sure to enable the EdgeSync subscription.