Microsoft

Deploying Microsoft® Forefront® Threat Management Gateway 2010

Yuri Diogenes and Dr. Thomas W. Shinder

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2010936127

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. For further information about international editions, contact your local Microsoft Corporation office or contact Microsoft Press International directly at fax (425) 936-7329. Visit our Web site at www.microsoft.com/mspress. Send comments to mspinput@microsoft.com.

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions Editor: Devon Musgrave
Developmental Editor: Karen Szall
Project Editor: Karen Szall
Editorial Production: nSight, Inc.
Technical Reviewer: Mitch Tulloch; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Cover: Tom Draper Design

Body Part No. X17-15053

Contents

Acknowledgments

This 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 of your time 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 TMG Product Team folks, especially to Ori Yosefi and David Strausberg, for helping us by reviewing the Service Pack 1 chapter. To all our friends from CSS Security, especially to Bala Natarajan for reviewing content.

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 Alexsandra. 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 grown 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 for this writing career in which I'm now fully engaged. Thanks, guys. To, as Jim says, "da Boyz": Tim "Thor" Mullen, Steve Moffat, and Greg Mulholland. You guys are amazing. Thanks for sharing all the tales.

To my friend Thomas Detzner and all ISA/TMG EMEA engineers (including the great folks from PFE), thanks for sharing your knowledge and all the partnerships that we have had over these years. I would also like to say thanks to all my friends from Microsoft CSS Security (in Texas, North Carolina, and Washington) for sharing experiences every day, with a special thanks to all the great engineers from CSS India—you guys are the pillars of this team. Thanks for pushing me with tough questions and concerns. To all the readers of my articles and blogs, thanks for all the feedback that you guys share with me. If I keep writing in my spare time, it is because I know you are reading it. To all the Forefront MVPs, keep up the amazing job that you guys do. Last, but not least, to my buddies Mohit Kumar, Alexandre Hollanda, Daniel Mauser, and Alejandro Leal, for your consistent support throughout the years.

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 Shinder, 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 give a special "shout out" to Mohit Saxena. His TMG chops and sense of humor also helped us over the finish line.

Finally, I want to thank the operators of ISAserver.org and all the members of the ISAserver.org community. You guys were the spark that started a flaming hot career for me with ISA Server and then TMG. You guys are a never-ending inspiration and a demonstration of the power of community and ways communities can work together to solve hard problems and share solutions.

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 Threat Management Gateway (TMG) 2010. We hope you find that we have achieved that goal. We've also included the main deployment scenarios for Forefront TMG, and we take a deep dive into the installation process from the RTM version to the Service Pack 1 version.

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. This book covers pre-deployment tasks, use of Forefront TMG in a Secure Web Gateway Scenario, software and hardware requirements, and installation and configuration, using best practice recommendations.

Who Is This Book For?

Deploying Microsoft Forefront Threat Management Gateway 2010 covers the planning and deployment phases for this product. This book is designed for:

- Administrators who are deploying Forefront TMG
- Administrators who are experienced with Windows Server 2008 in general and with Windows networking in particular
- Current ISA Server administrators
- Administrators who are new to Forefront TMG
- Technology specialists, such as security administrators and network administrators

Because this book is limited in size and we want to provide you the maximum value, we assume a basic knowledge of Windows Server 2008 and Windows networking. These technologies are not discussed in detail, but this book contains material on both of these topics that relates to Forefront TMG administrative tasks.

How Is This Book Organized?

Deploying Microsoft Forefront Threat Management Gateway 2010 is written to be a deployment guide and also to be 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: Chapter 1, "Understanding Forefront Threat Management Gateway 2010," introduces you to the core concepts of firewalls, perimeter protection, and proxies and guides you through the use of Forefront TMG as a secure web gateway. Chapter 2, "Installing and Configuring Forefront Threat Management Gateway 2010," guides you through the product's installation and configuration. Chapter 3, "Deploying Forefront 2010 Service Pack 1," covers the new features of Service Pack 1 and describes how to install and configure those features.

We really hope you find *Deploying Microsoft Threat Management Gateway 2010* useful and accurate. We have an open door policy for email at *mspress.tmgbook@tacteam.net*, and you can contact us through our personal blogs and Twitter accounts:

- *http://blogs.technet.com/yuridiogenes* and *http://blogs.technet.com/tomshinder*
- *http://twitter.com/yuridiogenes* and *http://twitter.com/tshinder*

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:

1. Go to *http://microsoftpress.oreilly.com*.
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.
4. On the book's catalog page, under the picture of the book cover, click View/Submit Errata.

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

Deploying Forefront TMG 2010 Service Pack 1

In the summer of 2010, Microsoft released a major product update: Forefront TMG 2010 Service Pack 1 (SP1) for Microsoft Forefront Threat Management Gateway (TMG) 2010. This service pack is intended to not only fix some issues that were detected after Forefront TMG was released, but also add new capabilities to the product. This chapter describes the new features, the way to install Forefront TMG 2010 SP1, the way to deploy the core features available in this service pack, and what's coming next.

New Features in Service Pack 1

Forefront TMG 2010 SP1 provides improvements to Forefront TMG in four core areas:

- **Reporting** Forefront TMG 2010 SP1 changes the look and feel of Forefront TMG reports and adds a new user activity report that can show more detailed information about the pages a user browsed and the URL categories that were requested by the user.
- **Secure Web Access** One of the main uses for Forefront TMG is as a Secure Web Gateway (SWG). One of TMG's core features, called URL Filtering, is a key component of SWG. Forefront TMG 2010 SP1 brings a new capability, called *URL Filtering User Override,* to this feature. URL Filtering User Override allows users to override the access restrictions put in place by the URL Filtering feature implemented by the TMG administrator.

- **Branch Office Support** Forefront TMG 2010 SP1 takes advantage of the BranchCache feature that is available in Windows Server 2008 R2. This feature provides branch office users with an improved browsing experience while reducing bandwidth utilization between the branch and main offices.
- **Publishing** A new publishing wizard supports SharePoint 2010 deployments through Forefront TMG.

These features will be covered in detail in this chapter. However, before we discuss new features, it is important to get more details on Forefront TMG 2010 SP1 deployment.

Planning Service Pack 1 Deployment

Before installing Forefront TMG 2010 SP1 on Forefront TMG, it is necessary to plan the deployment to ensure that it goes smoothly. The installation sequence and prerequisites will vary according to your TMG setup. The overall installation process is shown in Figure 3-1:

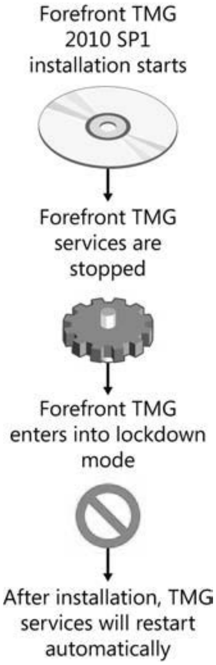

Forefront TMG 2010 SP1 installation starts
Forefront TMG services are stopped
Forefront TMG enters into lockdown mode
After installation, TMG services will restart automatically

FIGURE 3-1

In order to carry out the Forefront TMG 2010 SP1 installation procedures correctly, you will need to answer the following questions:

- Which Forefront TMG version (Enterprise or Standard) are you using?
- Are the Forefront TMG firewalls deployed as array members or as stand-alone servers?
- What Forefront TMG role (EMS or Firewall) is the machine providing?

When you have this information, you can determine the installation sequence from Table 3-1.

NOTE **Before you apply Forefront TMG 2010 SP1, create a full backup of your current Forefront TMG configuration. You should also have the latest Windows updates installed on the computer on which TMG is installed.**

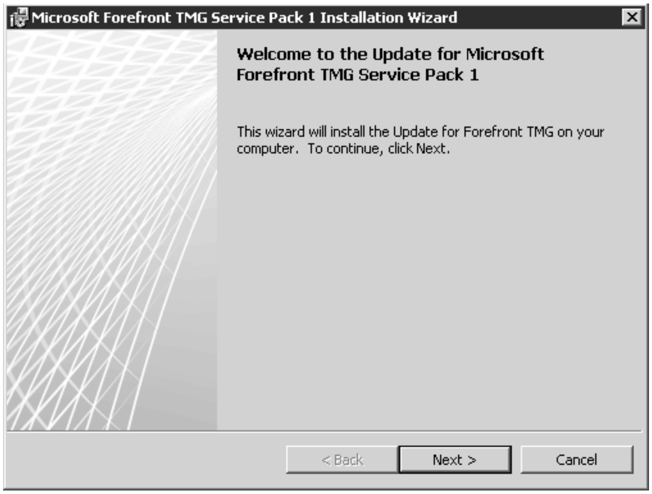
TABLE 3-1 Installation based on the Forefront TMG setup

TMG SETUP	INSTALLATION ORDER	GENERAL NOTES
Single Server	**1.** Single server installation point	Regardless of the Forefront TMG setup, always run the setup with an elevated administrative level.
Array	**1.** Enterprise Management Servers (master and replicas) **2.** Array managers **3.** Array members	Before you install Forefront TMG 2010 SP1 on Forefront TMG Enterprise Edition, you must log on to EMS using the credentials that were used to install EMS during the initial setup process. If you try to install the update using a different administrator account, the installation might fail.

Installing Forefront TMG 2010 Service Pack 1

Assuming that you downloaded Forefront TMG 2010 SP1 in English—from the Microsoft Download Center (*http://www.microsoft.com/downloads/details.aspx?FamilyID=f0fd5770-7360-4916-a5be-a88a0fd76c7c&displaylang=en)* to a temporary folder, such as C:\temp—start the installation by following these steps:

1. Click Start, right-click Command Prompt, and choose the Run As Administrator option.
2. Type **cd c:\temp** to switch to the temporary folder.
3. Type **TMG-KB981324-AMD64-ENU.msp**, and press Enter.
4. On the Open File – Security Warning page, click Open.
5. When the Welcome To The Update For Microsoft Forefront TMG Service Pack 1 page appears, as shown in Figure 3-2, click Next to continue.



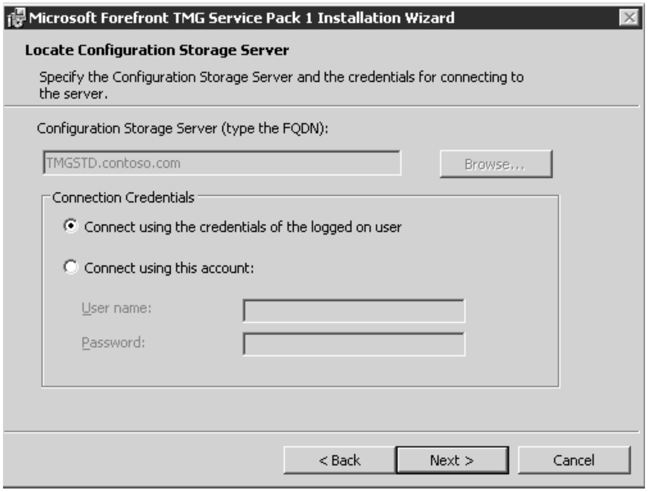
Microsoft Forefront TMG Service Pack 1 Installation Wizard

Welcome to the Update for Microsoft Forefront TMG Service Pack 1

This wizard will install the Update for Forefront TMG on your computer. To continue, click Next.

FIGURE 3-2

6. When the License Agreement page appears, read the license agreement and select the I Accept The Terms In The License Agreement checkbox, and then click Next to proceed.
7. The Locate Configuration Storage Server page appears. Because this is the first Forefront TMG to which we are applying Forefront TMG 2010 SP1, the option to specify the configuration storage server is unavailable (grayed out), as shown in Figure 3-3. When you are applying Forefront TMG 2010 SP1 on array members, this option will be available so that you can specify the configuration storage server. Click Next to continue.



Microsoft Forefront TMG Service Pack 1 Installation Wizard

Locate Configuration Storage Server

Specify the Configuration Storage Server and the credentials for connecting to the server.

Configuration Storage Server (type the FQDN): TMGSTD.contoso.com

Connection Credentials

● Connect using the credentials of the logged on user

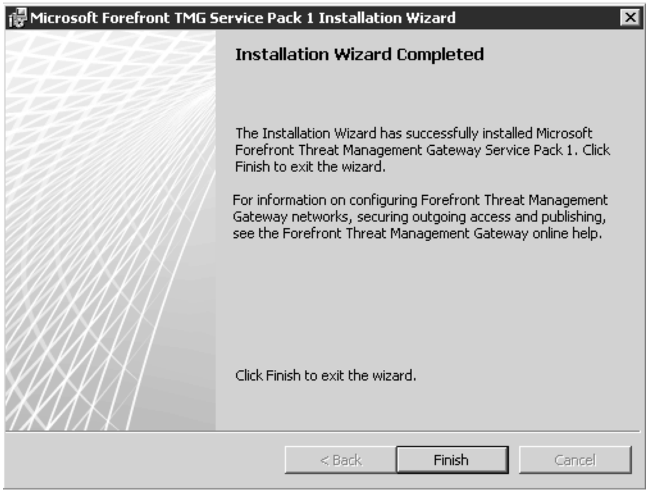
○ Connect using this account:

User name:

Password:

FIGURE 3-3

8. When the Ready To Install The Program page appears, click Install.
9. After the installation is finished, the Installation Wizard Completed page appears, as shown in Figure 3-4. Click Finish to conclude the installation.



Installation Wizard Completed

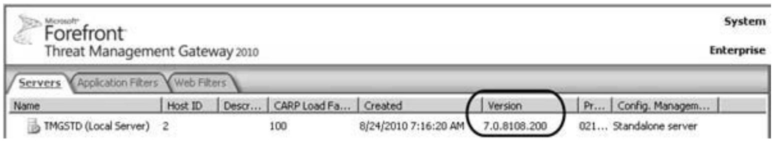
The Installation Wizard has successfully installed Microsoft Forefront Threat Management Gateway Service Pack 1. Click Finish to exit the wizard.

For information on configuring Forefront Threat Management Gateway networks, securing outgoing access and publishing, see the Forefront Threat Management Gateway online help.

Click Finish to exit the wizard.

FIGURE 3-4

10. To confirm that the Forefront TMG 2010 SP1 installation is in place, you can open the Forefront TMG Management console, click System, and verify the Forefront TMG version, which should be 7.0.8108.200, as shown in Figure 3-5.



Name	Host ID	Descr...	CARP Load Fa...	Created	Version	Pr...	Config. Managem...
TMGSTD (Local Server)	2		100	8/24/2010 7:16:20 AM	7.0.8108.200	021...	Standalone server

FIGURE 3-5

Administrator's Insight: Troubleshooting an Installation

There are several issues that you might encounter when installing Forefront TMG 2010 SP1, some of which are documented in the Forefront TMG 2010 SP1 release notes at (*http://technet.microsoft.com/en-us/library/ff717843.aspx#troubleshooting)*. There may be other problems with the installation that will require troubleshooting. The general rule of thumb is to start troubleshooting the installation by reviewing the error messages presented in the UI, and then go to the Forefront TMG setup logs to track the root causes of the issues. The Forefront TMG Setup Installation logs are located at %windir%\temp, and the ADAM Setup log files are located at %windir%\debug.

There are two articles on the TMG Team Blog and one on my blog that describe a general approach to troubleshooting installation issues:

- **"Troubleshooting ERROR: Setup failed to install ADAM.\r\n (0x80074e46) and 0x80070643 while trying to install TMG 2010" can be found at *http://blogs.technet.com/b/isablog/archive/2010/07/07/troubleshooting-error-setup-failed-to-install-adam-r-n-0x80074e46-and-0x80070643-while-trying-to-install-tmg-2010.aspx*.**
- **“Another TMG 2010 Installation failure with error 0x80070643” can be found at *http://blogs.technet.com/b/isablog/archive/2010/07/13/another-tmg-2010-installation-failure-with-error-0x80070643.aspx*.**
- **“Unable to install Forefront TMG 2010 – Error 0x80074e46” can be found at *http://blogs.technet.com/b/yuridiogenes/archive/2010/08/16/unable-to-install-forefront-tmg-2010-error-0x80074e46.aspx*.**

Although these articles are not specifically related to Forefront TMG 2010 SP1, they can be used as troubleshooting methodology for your installation process on Forefront TMG.

Configuring User Override for URL Filtering

In a world in which compliance and security policy enforcement are growing trends, having a secure Web gateway that reflects your IT business requirements is a real advantage. One of the pillars for the Forefront TMG Secure Web Gateway scenario is URL Filtering, which directly affects user productivity by filtering traffic to unwanted destinations. A new enhancement to the URL Filtering feature, introduced with Forefront TMG 2010 SP1, allows users to override restricted Web access and proceed on a per-request basis. This can provide a more flexible Web access policy by allowing users to decide whether to access a site that was initially denied to them. This can help reduce help desk calls, especially for Web sites that have been incorrectly categorized.

While this might sound too flexible when the subject is policy enforcement, the fact of the matter is that the user will receive a warning that a Web site being entered is prohibited and that entering the Web site will be logged. This can help to reveal user Internet usage behavior when accessing prohibited Web sites. This feature uses the logic illustrated in Figure 3-6.

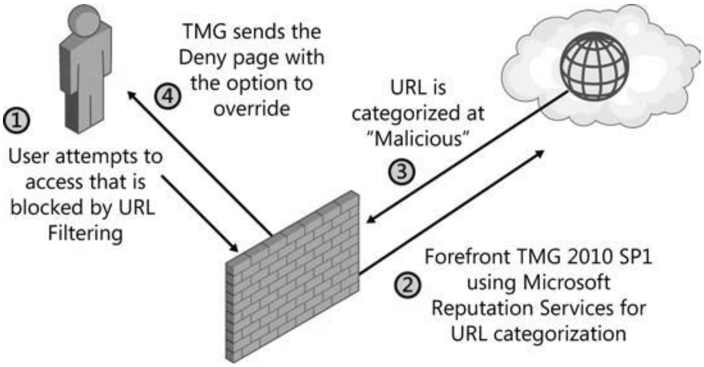

TMG sends the Deny page with the option to override
4
URL is categorized at "Malicious"
3
1
User attempts to access that is blocked by URL Filtering
2
Forefront TMG 2010 SP1 using Microsoft Reputation Services for URL categorization

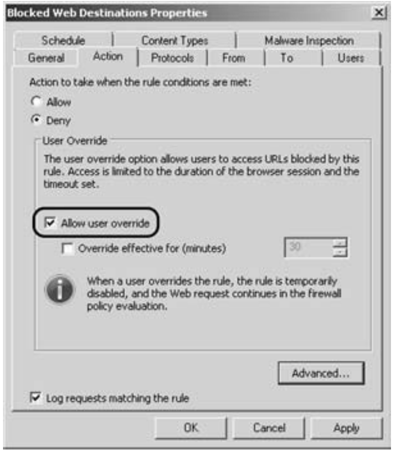
FIGURE 3-6

When Forefront TMG sends the Deny page, as illustrated by Step 4, if the user clicks Override Access Restriction, Forefront TMG will allocate to the user's browser a cookie that will accompany all subsequent Web requests to this domain, and the browser is triggered to reload the URL. Once Forefront TMG receives the Web request with the cookie, it will effectively disable the blocking rule for this particular Web request. It is important to understand that the cookie will remain valid only for the length of the browser session or until the configured time-out period expires. The other important notes about this feature are:

- In order for the user override feature to work, one of the subsequent firewall policy rules must allow access to the requested destination.
- User override configuration requires that you create Deny rules; you cannot enable Allow rules with category exceptions and then enable a user override.
- The user override option only works for the HTTP protocol.
- User override is not supported for HTTPS traffic.
- You can't customize the content type for the user override feature; the rule must apply to all types of HTTP content.

Now that you know how the core functionality of this feature works, the next step is to implement it by following these steps:

1. Open the Forefront TMG Management console.
2. Click Web Access Policy, right-click the rule that denies the traffic to a set of destinations (for this example we will use the default Deny rule created by the Web Access Policy Wizard), and choose Properties.
3. Click the Action tab, and then select the Allow User Override option, as shown in Figure 3-7.



Action to take when the rule conditions are met:

○ Allow

● Deny

User Override

The user override option allows users to access URLs blocked by this rule. Access is limited to the duration of the browser session and the timeout set.

☑ Allow user override

□ Override effective for (minutes) 30

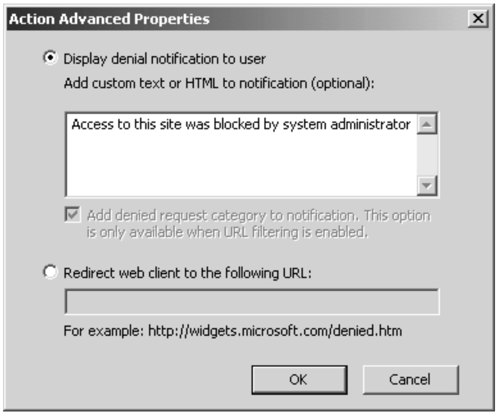
When a user overrides the rule, the rule is temporarily disabled, and the Web request continues in the firewall policy evaluation.

☑ Log requests matching the rule

FIGURE 3-7

NOTE **You can also specify a range of time during which the user can stay on the blocked URL. This is the time that the assigned cookie will be valid for the user.**

4. To customize the error message that the user will receive when attempting to browse a blocked URL, click Advanced. The Action Advanced Properties dialog box appears, as shown in Figure 3-8.



● Display denial notification to user

Add custom text or HTML to notification (optional):

Access to this site was blocked by system administrator

☑ Add denied request category to notification. This option is only available when URL filtering is enabled.

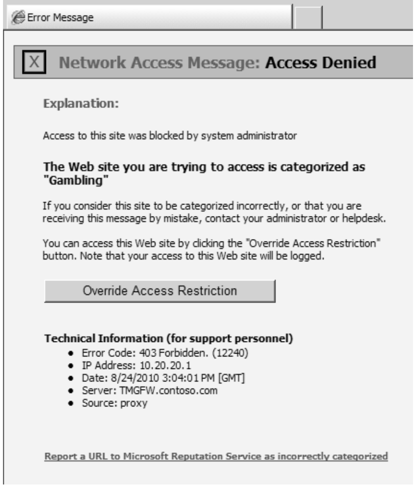
○ Redirect web client to the following URL:

For example: http://widgets.microsoft.com/denied.htm

FIGURE 3-8

5. Type your custom message, as shown in Figure 3-8, click OK, click OK again, and click Apply to commit the changes.

Now that you've implemented this feature, you can perform a test using a client who is trying to browse a Web site that matches one of the categories specified on the Deny rule on which the user override feature is enabled. The user will receive an error message, and the Override Access Restriction button will be available, as shown in Figure 3-9.



X Network Access Message: Access Denied

Explanation:

Access to this site was blocked by system administrator

The Web site you are trying to access is categorized as "Gambling"

If you consider this site to be categorized incorrectly, or that you are receiving this message by mistake, contact your administrator or helpdesk.

You can access this Web site by clicking the "Override Access Restriction" button. Note that your access to this Web site will be logged.

Technical Information (for support personnel)

- Error Code: 403 Forbidden. (12240)
- IP Address: 10.20.20.1
- Date: 8/24/2010 3:04:01 PM [GMT]
- Server: TMGFW.contoso.com
- Source: proxy

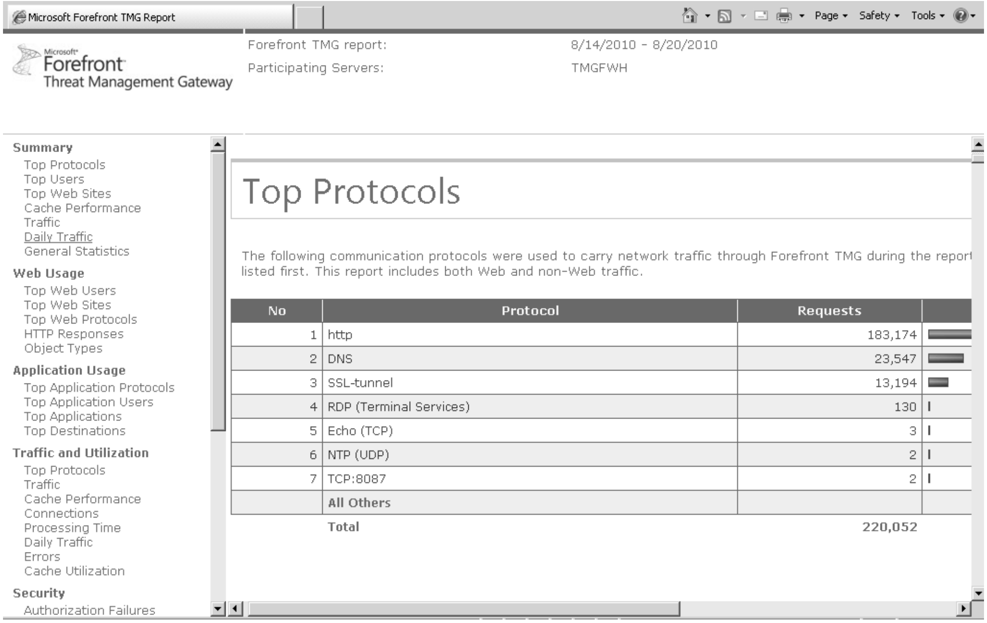
Report a URL to Microsoft Reputation Service as incorrectly categorized

FIGURE 3-9

IMPORTANT **If you don't have an Allow rule for this destination, the user won't be able to access this Web site even by clicking Override Access Restriction.**

Reporting Enhancements

One of the most highly anticipated changes in Forefront TMG 2010 SP1 is the enhancement to the reporting feature. The new report design changes the look and feel of Forefront TMG reports, and the new format provides clearer information. Figure 3-10 shows an example of the new report main page.



Forefront TMG report: 8/14/2010 - 8/20/2010
Participating Servers: TMGFWH

Top Protocols

The following communication protocols were used to carry network traffic through Forefront TMG during the report listed first. This report includes both Web and non-Web traffic.

No	Protocol	Requests	
1	http	183,174	
2	DNS	23,547	
3	SSL-tunnel	13,194	
4	RDP (Terminal Services)	130	
5	Echo (TCP)	3	
6	NTP (UDP)	2	
7	TCP:8087	2	
	All Others		
	Total	220,052	

FIGURE 3-10

NOTE **More sample reports can be found in "Reporting Improvements in Forefront TMG SP1," at *http://blogs.technet.com/b/isablog/archive/2010/08/15/reporting-improvements-in-forefront-tmg-sp1.aspx*.**

The user activity report will contain more granular information about the Web sites that the user visited, including the URL category for each site.

NOTE **While writing this book, a Reporting issue was detected after installing TMG SP1. To view the problem and the solution for this problem, review Yuri Diogenes's answer on the following forum thread: *http://social.technet.microsoft.com/Forums/en-US/ForefrontedgeMLR/thread/543b0ef3-68fa-442c-bb3d-a42177809016*.**

Branch Office Support

The new Branch Office integration functionality uses a new wizard to help you take advantage of the Windows Server 2008 R2 BranchCache role. This option enables Forefront TMG to act as Hosted Cache Server in a branch office scenario. The Forefront TMG UI dashboard for branch and Web cache utilization can be used for monitoring. To illustrate this feature and the capability to use a Read-Only Domain Controller (RODC) on Forefront TMG, we are going to use the topology shown in Figure 3-11.

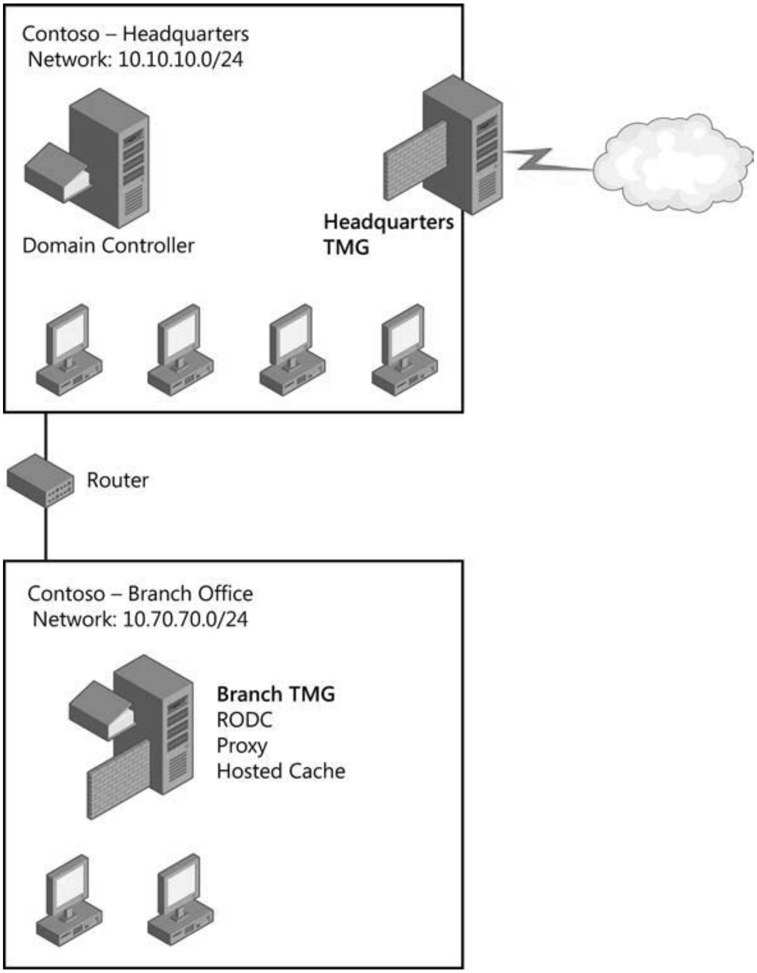
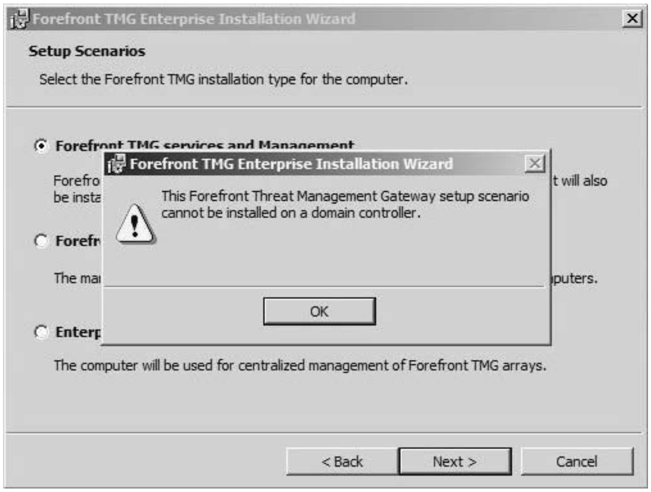


FIGURE 3-11

In order to prepare the RODC you will need to:

- Verify that you have network connectivity to the Headquarters Domain Controller (HQ DC) and that you set the branch server's DNS to the HQ DC.
- If the RODC role is already installed on the server located in the branch office, create a slipstream version of Forefront TMG with Forefront TMG 2010 SP1 to install on top of the RODC. If you try to prepare the RODC without the slipstream version, you will receive the error message shown in Figure 3-12.


Forefront TMG Enterprise Installation Wizard
Setup Scenarios
Forefront TMG Enterprise Installation Wizard
OK
< Back
Next >
Cancel

Select the Forefront TMG installation type for the computer.

● Forefront TMG services and Management

Forefro… be insta… t will also

○ Forefr…

The mai… puters.

○ Enterp…

The computer will be used for centralized management of Forefront TMG arrays.

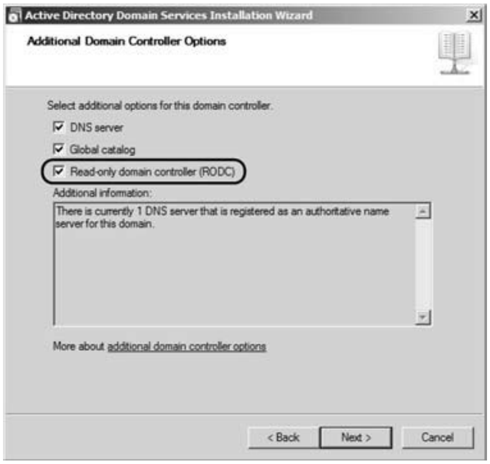
This Forefront Threat Management Gateway setup scenario cannot be installed on a domain controller.

FIGURE 3-12

- Verify that the server located in the branch office is already a member of the domain (in this case it is a member of contoso.com).
- Verify that the server located in the branch office uses the domain controller at headquarters as its DNS server.
- Verify that the certificate that will be used by the BranchCache feature is already installed on Forefront TMG under Personal Store, which is under Certificates (Local Computer). Remember that the certificate must be trusted by the clients that are behind Forefront TMG in the branch office.

With these elements in place, the first step is to enable the RODC role on the server on which Forefront TMG is installed to prepare the forest for RODC. To do that, the forest must be at a Windows Server 2003, Windows Server 2008, or Windows Server 2008 R2 functional level. You must run the **adprep /rodcprep** command on the current domain controller for the domain.

After preparing the forest, you will run the **dcpromo** command on the server on which Forefront TMG will be installed, and then follow the wizard. On the Additional Domain Controller Options page, be sure to select the Read-Only Domain Controller (RODC) option, as shown in Figure 3-13.


Active Directory Domain Services Installation Wizard

Additional Domain Controller Options

Select additional options for this domain controller.

☑ DNS server

☑ Global catalog

☑ Read-only domain controller (RODC)

Additional information:

There is currently 1 DNS server that is registered as an authoritative name server for this domain.

More about additional domain controller options

FIGURE 3-13

Continue to follow the wizard to complete the promotion of this server to a read-only domain controller.

NOTE **For the complete planning and deployment guide for Active Directory RODC, review the article "Deploying RODCs in Branch Offices" at** ***http://technet.microsoft.com/en-us/library/dd735411(WS.10).aspx.***

The next step is to install Forefront TMG 2010 SP1 on the server on which the RODC is installed:

1. Run the following command from an elevated command prompt:

   ```
   ServerManagerCmd.exe -inputpath <DVD_path>\FPC\PreRequisiteInstallerFiles
   \WinRolesInstallSA_Win7.xml -logPath C:\Windows\TEMP\TMG-Prerequisites.log
   ```

2. Prepare a Forefront TMG 2010 SP1 slipstream DVD by following these steps:
   - Copy the Forefront TMG DVD and the Forefront TMG 2010 SP1 MSP file to a local drive on the target computer. For the purposes of this example, let’s assume this is c:\temp\TMG. At a command prompt, type the following command and press Enter.

     ```
     msiexec /a c:\temp\TMG\FPC\MS_FPC_SERVER.msi /p TMG-KB981324-amd64-ENU.msp /qb
     /L*v c:\tmg\log.txt
     ```

   - Run the upgraded setup program by typing **c:\temp\TMG\FPC\setup.exe** at a command prompt and pressing Enter. Follow the wizard for the Forefront TMG installation. For more information on Forefront TMG installation, review Chapter 2, “Installing and Configuring Forefront Threat Management Gateway 2010.”

NOTE During the installation process, be sure to define the internal network to include the branch subnets and complete the installation.

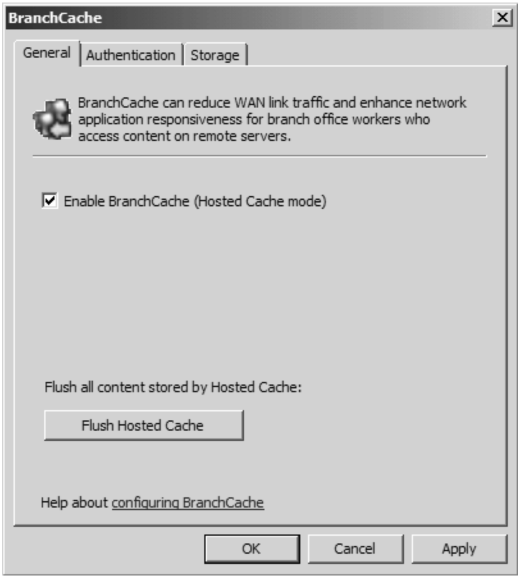
The Forefront TMG installation automatically identifies that it is running on a domain controller and enables the system policy that allows DC traffic from the internal network to the Forefront TMG server as well as from the HQ DCs (if they are outside the internal network).

Every branch account (user or computer) that is joined to the domain needs to have its password replicated to the RODC for authentication. To replicate the password, complete the following steps on the HQ DC:

1. In the Active Directory Users and Computers console, select the Domain Controllers branch, right-click on the RODC, and select Properties.
2. Click the Password Replication Policy tab, and then click Add.
3. Select Allow Passwords For The Account To Replicate To This RODC, select all relevant local users for this branch, and then click OK.
4. On the RODC's Properties page, click Advanced, and verify that the user accounts you added appear in the list of Accounts for which the passwords are stored on this Read-only Domain Controller.
5. Active Directory must complete replicating the user information to the RODC before you can log on with these accounts.

The next step to configure the branch office Forefront TMG is to enable BranchCache support. To perform this operation:

1. Open the Forefront TMG Management console.
2. Click Firewall Policy, and on the Task Pane, click Configure BranchCache.
3. In the BranchCache window, select Enable BranchCache (Hosted Cache Mode), as shown in Figure 3-14.



BranchCache can reduce WAN link traffic and enhance network application responsiveness for branch office workers who access content on remote servers.

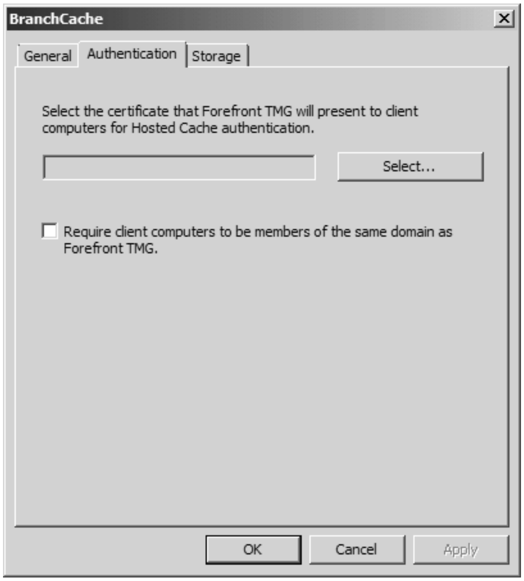
☑ Enable BranchCache (Hosted Cache mode)

Flush all content stored by Hosted Cache:

Help about configuring BranchCache

FIGURE 3-14

4. Click the Authentication tab; click Select, as shown in Figure 3-15; and then choose the certificate that will be presented to the client computers for authentication.



Select the certificate that Forefront TMG will present to client computers for Hosted Cache authentication.

☐ Require client computers to be members of the same domain as Forefront TMG.

FIGURE 3-15

5. Optionally, you can select the Require Client Computers To Be Members Of The Same Domain As Forefront TMG option if you want to restrict the access to this feature. If Forefront TMG is in a workgroup, you should not use this option.
6. Click OK to continue, and then click Apply to commit the changes.

What's Next?

At the time we were writing this chapter, the Forefront TMG product team was finalizing the next update (post-SP1) for Forefront TMG; it is called Update 1. Update 1 will include some additions to the product, such as:

- **SafeSearch** This is a feature that acts as an automated adult-oriented-content filter in Web search engines, such as Bing and Yahoo. SafeSearch is activated by the end user from a search Web page. Forefront TMG can be used for SafeSearch enforcement when organizational policy requires that all or some of its personnel perform SafeSearch only.

> **NOTE** **For more information about the SafeSearch feature, read *http://blogs.technet.com/b/isablog/archive/2010/09/21/new-in-forefront-tmg-update-1-safesearch-enforcement.aspx*.**

- **Multiple Categories for URL Filter** This capability provides a way of categorizing multiple categories in a single URL. With this feature, a Forefront TMG Administrator will be able to create access rules that consider all categories returned by Microsoft Reputation Services. An example of usability of this option is: a site can be categorized as primarily a "general business" site, but also as a "Web mail" site. In this case, the "general business" category is ranked higher than the "Web mail" category. So, for example, if a Forefront TMG Administrator wanted to block Web mail, but couldn't with Forefront TMG 2010 SP1 because a site's primary category was general business, the multiple categories feature of Update 1 will allow the Web mail to be blocked.

> **NOTE** **For more information about the Multiple URL Categories feature, read *http://blogs.technet.com/b/isablog/archive/2010/09/21/new-in-forefront-tmg-update-1-multiple-url-categories.aspx*.**

- **Improve Support of User Account Control in Patch Installation and Uninstallation** Update 1 will include improvements in the installation and uninstallation processes to provide a better product experience in scenarios in which User Account Control (UAC) is enabled.

Beyond these core changes, other minor changes will be included in Update 1.

Administrator's Punch List

In this chapter, you learned about the new features of Forefront TMG 2010 SP1 and how to configure those features, you learned about the enhancements included in Forefront TMG 2010 SP1, and you heard about what's coming next with Update 1. When preparing to deploy Forefront TMG 2010 SP1, keep in mind the following points:

- Review your current environment before deploying Forefront TMG 2010 SP1. Knowing the current role of each Forefront TMG can assist you in installing this service pack in the correct order.
- In an enterprise scenario, before you install Forefront TMG 2010 SP1, you must log on to the EMS using the same credentials that were used to install EMS during the setup process.
- You will need to use administrative elevated privileges in order to install Forefront TMG 2010 SP1.
- If you have installation problems, review the Forefront TMG installation logs under %windir%\temp.
- When using the URL Filtering User Override option, be sure to review the reports and logs to identify the users who are using sites that were initially blocked by URL Filtering.
- After installing Forefront TMG 2010 SP1, review the new report design, and create new reports based on user activity.
- Be sure to plan the BranchCache deployment before enabling it.
- If the RODC role is already installed on the server on which Forefront TMG 2010 SP1 will be installed, it will not work with the Forefront TMG RTM version. You will need to create a slipstream version of Forefront TMG.
- To prepare for the RODC installation, you must run the adprep /rodcprep command on the current controller for the domain.