Microsoft Forefront TMG – installing and configuring the Forefront TMG client

Abstract

In this article, I will show you how to install and configure the updated Microsoft Firewall Client, now called the Forefront TMG client in Microsoft Forefront TMG.

Let's begin

One of the features of Forefront TMG is the support for several clients which are used to connect to the Forefront TMG Firewall. One of the client types is the Microsoft Forefront TMG client, which is also known as a Winsock client for Windows operating systems. Using the TMG client has several enhancements compared to the other clients (Web proxy and Secure NAT). Forefront TMG client can be installed on several Windows client and server operating systems (which I don't recommend, except Terminal Servers), which are protected by Forefront TMG 2010. Forefront TMG Client provides HTTPS inspection notifications (used with TMG 2010), automatic discovery, enhanced security, application support, and access control for client computers. When a client computer running Forefront TMG Client makes a Firewall request, the request is directed to the Forefront TMG 2010 computer for further processing. No specific routing infrastructure is required because of the Winsock process. Forefront TMG Client sends user information transparently with each request, enabling you to create a firewall policy on the Forefront TMG 2010 computer with rules that use the authentication credentials forwarded by the client, but only based on TCP and UDP traffic. For all other protocols you must use a Secure NAT client connection. For a list of reasons for using the TMG client read Tom Shinders article on www.isaserver.org:

In addition to the following standard features of previous Firewall clients, the TMG client supports:

- HTTPS inspection notification
- AD Marker support

Standard features of the TMG client

- User or group based Firewall policies for Web- and non-Web proxy based TCP and UDP traffic (and only for theses protocols)
- Support for complex protocols without the requirement to use a TMG application filter
- Simplify routing configuration for large organizations
- Auto Discovery for TMG information based on DNS and DHCP Server settings.

System Requirements

The TMG client has some system requirements:

Supported operating systems

- Windows 7
- Windows Server 2003
- Windows Server 2008
- Windows Vista
- Windows XP

Supported ISA Server Versions and Forefront TMG Versions

• ISA Server 2004 Standard Edition
• ISA Server 2004 Enterprise Edition
• ISA Server 2006 Standard Edition
• ISA Server 2006 Enterprise Edition
• Forefront TMG MBE (Medium Business Edition)
• Forefront TMG 2010 Standard Edition
• Forefront TMG 2010 Enterprise Edition

Operating system support

Operating system	Forefront TMG Client	Firewall Client 2006 (including Vista hotfix)	Firewall Client 2004
Windows® 7/Windows Server 2008 R2	Supported	Supported	Not supported
Windows Vista Service Pack 2	Supported	Supported	Not supported
Windows Server 2003 R2	Supported	Not supported	Not supported
Windows Server 2003 with Service Pack 2	Supported	Supported	Supported
Windows XP Service Pack 3	Supported	Supported	Supported

Table 1: Source: http://technet.microsoft.com/en-us/library/dd897009.aspx

Client/Server compatibility

	Forefront TMG server	ISA Server 2006	ISA Server 2004	ISA Server 2000
Forefront TMG Client	Supported	Supported	Supported	Not supported
Firewall Client 2006	Supported	Supported	Supported	Supported
Firewall Client 2004	Supported	Supported	Supported	Supported
Firewall Client 2000	Not supported	Supported	Supported	Supported

Table 2: Source: http://technet.microsoft.com/en-us/library/dd897009.aspx

TMG client settings on the TMG server

There are only a few settings on the Forefront TMG server which are responsible for configuring the behavior of the Forefront TMG client. First of all it is possible to enable the TMG client support for the internal network definition on the TMG Server as you can see in the following screenshot.

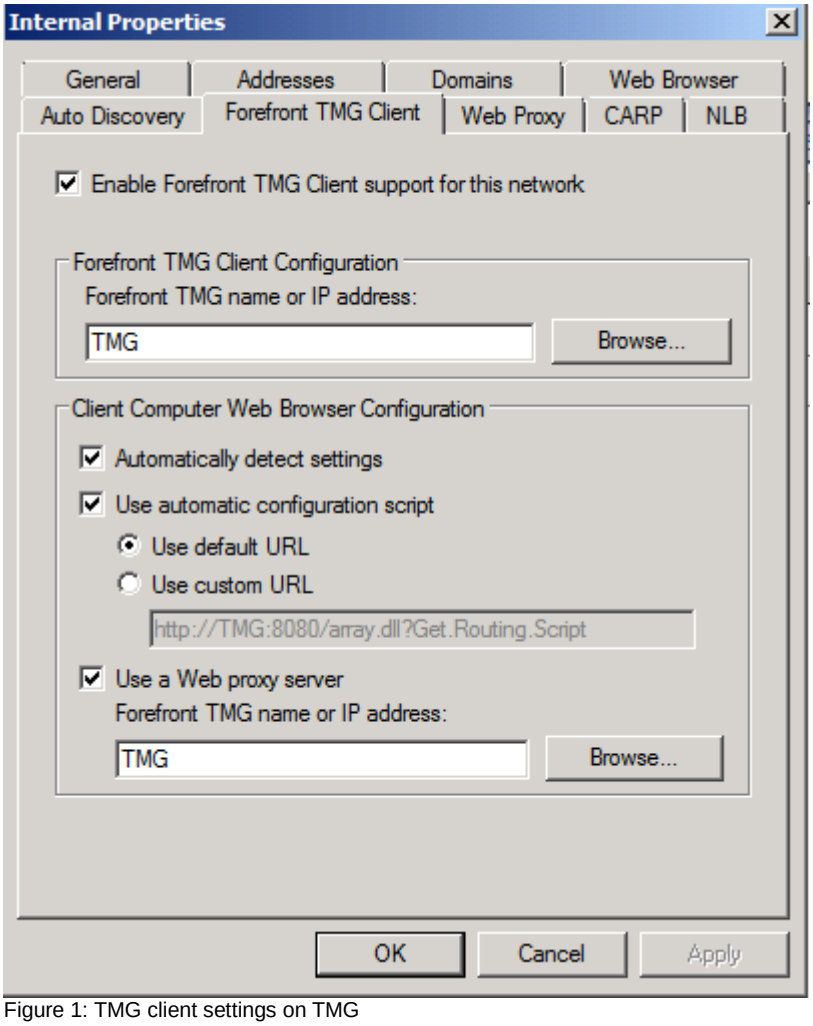

Figure 1: TMG client settings on TMG

After TMG client support is enabled (default after a normal TMG installation), it is also possible to automate the client computers Web Browser configuration. During the normal update intervals of the TMG client or during service startup, the Browser gets the settings configured in the TMG management console.

In the Application settings for the TMG client in the TMG console it is possible to enable or disable some application depended settings.

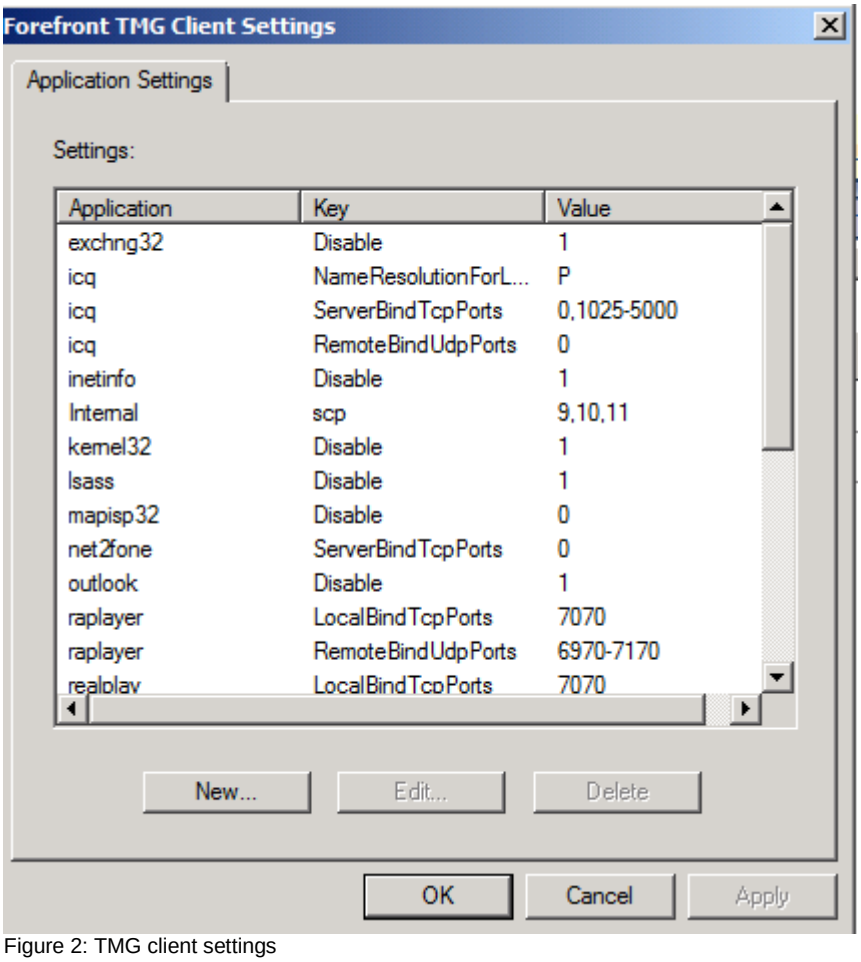

Figure 2: TMG client settings

AD Marker

Microsoft Forefront TMG provides a new functionality for automatic detection of the TMG Server for the TMG client. Unlike previous Firewall client versions, the Forefront TMG client can now use a marker in Active Directory to find the corresponding TMG Server. TMG client uses LDAP to find the required information in Active Directory.

Please note:

If the TMG client didn't find the AD marker it won't failover to classical automatic detection concepts through DHCP and DNS for security reasons to reduce the risk that an attacker might try to force a failback to the less secure method. If a connection to the Active Directory can be established but an AD Marker couldn't be found, the TMG client wills failover to DHCP and DNS.

TMGADConfig Tool

To create the AD Marker configuration in Active Directory, you can download the TMG AD Config Tool from Microsoft Download Center (look for the AdConfigPack.EXE). After the tool has been downloaded and installed on TMG you can execute the following command line in order to register the AD marker key:

Tmgadconfig add –default –type winsock –url http://nameoftmgserver.domain.tld:8080/wspad.dat

It is also possible to remove the AD marker with the tmgadconfig tool if you decide to not use the AD Marker support.

Installation of the TMG client

The newest version of the TMG client can be downloaded from the Microsoft website. I provided you with the download link at the end of this article.

Start the installation process and follow the instructions of the wizard.

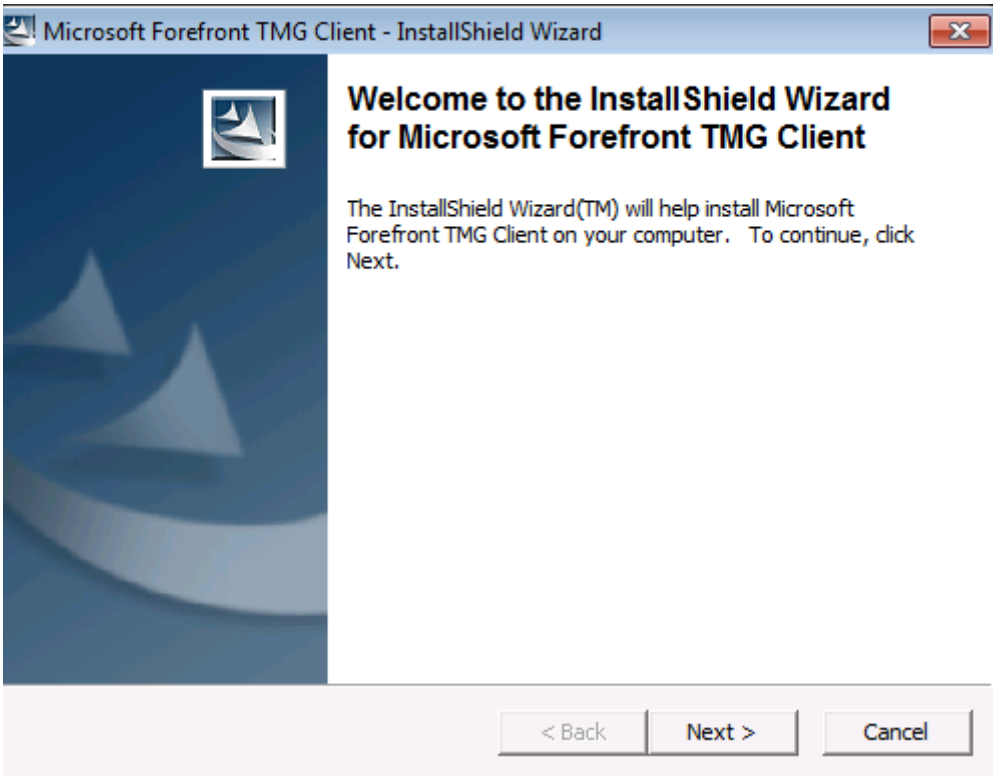

Figure 3: Installation of the TMG client

It is possible to specify the location of the TMG Server manual or automatically during the installation process of the TMG client and after the installation it is possible to reconfigure the settings of the TMG client detection mechanisms with the TMG client configuration tool which you will find in the taskpane of your client.

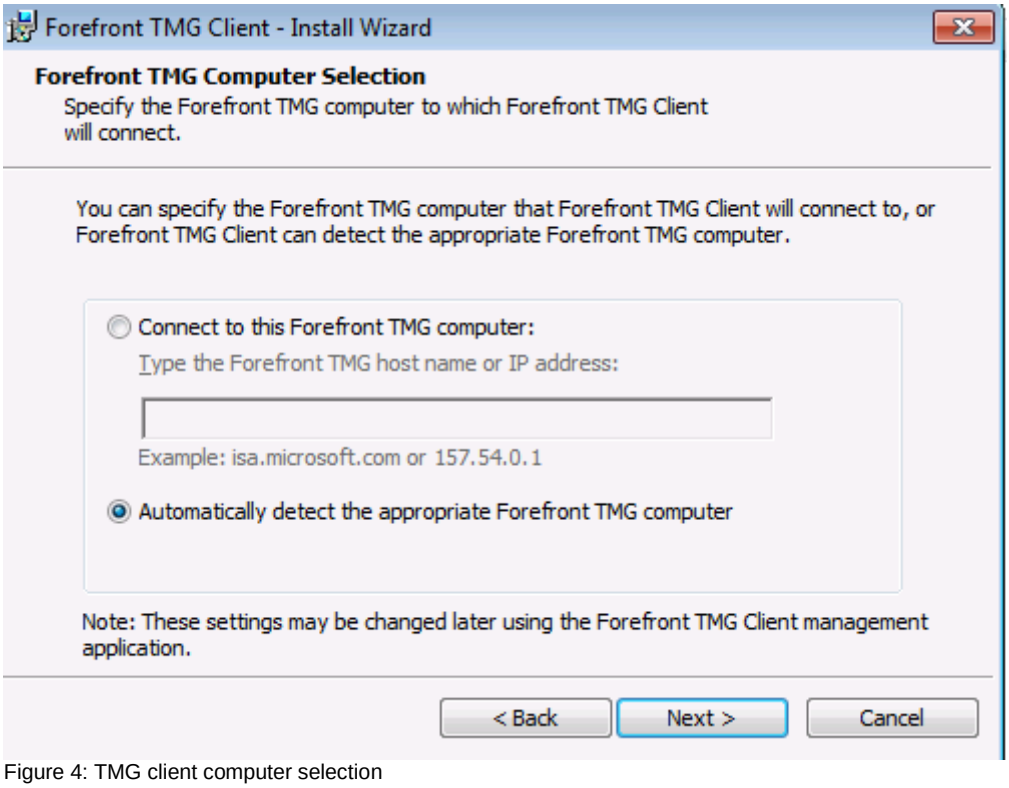

Figure 4: TMG client computer selection

Advanced Automatic Detection

If you want to modify the behaviour of the automatic detection process, the TMG client has now a new options to define the method used for automatic detection.

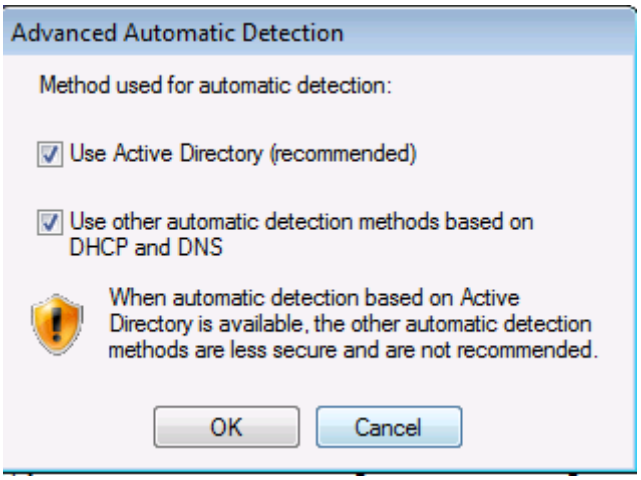

Figure 5: Advanced Automatic Detection

HTTPS inspection notification

Microsoft Forefront TMG has a new functionality to inspect HTTPS traffic for outoing client connections. To inform users about these sensitive process, the new TMG client can be used to inform users that the outgoing HTTPS connection is getting inspected, if you want to do this. TMG Administrators also have the option to deactivate the notification process centrally on the TMG Server or manually on every Forefront TMG client. For more infotmation about outgoing HTTPS inspection settings, read the following article from Tom Shinder on www.isaserver.org.

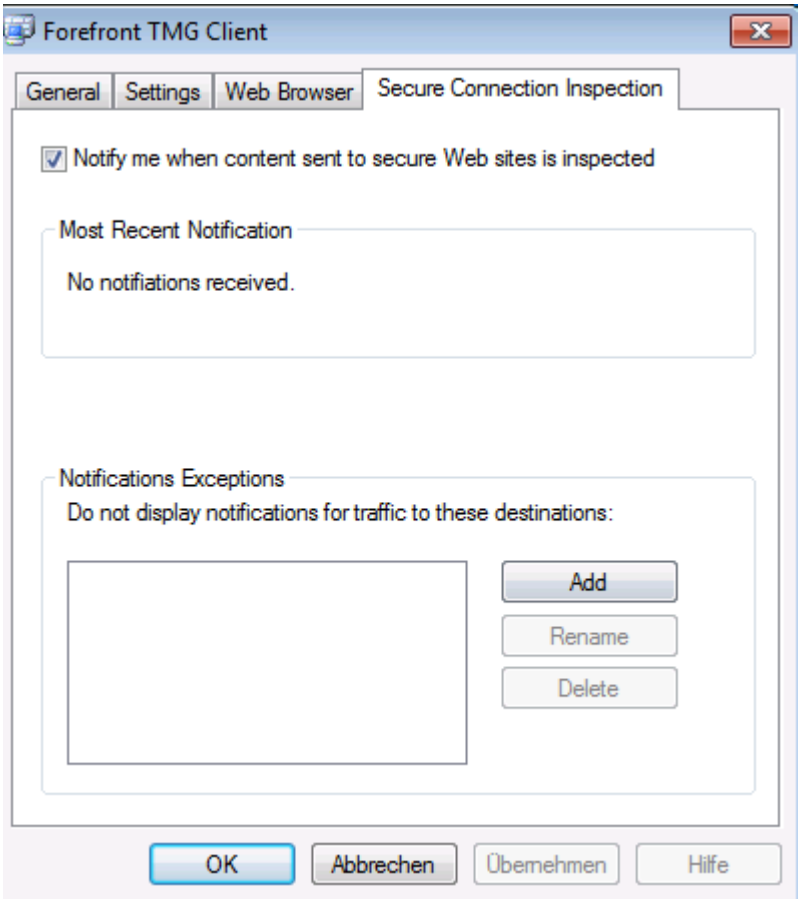

Figure 6: Secure connection inspection

If outgoing HTTPS inspection is enabled and the setting to inform users if HTTPS inspection is used is also enabled, users with an installed Forefront TMG client will get a message like in the following screenshot.

Figure 7: Secure Connection Inspection message

Conclusion

In this article, I gave you an overview about the installation and configuration process of the new Microsoft Forefront TMG client. I also showed you some of the new features of the Forefront TMG client. In my opinion you should use the TMG client wherever it is possible in your environment, because of the additional security features. I explicitly didn't covered some advanced configuration settings of the TMG client because these settings remained unchanged compared to the previous Firewall client, so if you want to get more information about these settings, read the following article on www.isaserver.org.

Related links

Firewall Client Basics: Introduction to the ISA Server Firewall Client and Forefront TMG Client
http://technet.microsoft.com/en-us/library/ee291341.aspx
How to automatically deploy the Microsoft Firewall client
http://www.isaserver.org/tutorials/Automatically-deploy-Microsoft-Firewall-client.html
Forefront Threat Management Gateway (TMG)-Client
http://www.microsoft.com/downloads/details.aspx?displaylang=de&FamilyID=53010a09-3c5c-4d5d-9ae1-692e7447c5bd
ISA Server Firewall client configuration
http://www.isaserver.org/tutorials/Understanding-ISA-Firewall-Client-Part1.html
About firewall client computers
http://technet.microsoft.com/en-us/library/dd897009.aspx
Forefront TMG Client
http://blogs.technet.com/isablog/archive/2009/11/03/forefront-tmg-client.aspx
Installing Forefront TMG Client software
http://technet.microsoft.com/en-us/library/cc441520.aspx
TMG Client introduces automatic detection using Active Directory
http://blogs.technet.com/isablog/archive/2009/10/23/tmg-client-introduces-automatic-detection-using-active-directory.aspx
Why the ISA Firewall Client Rocks: Lessons on the ISA Stateful Application Layer Inspection Firewall
http://www.isaserver.org/articles/2004firewallclient.html
Outbound SSL Inspection with TMG Firewalls (Part 1)
http://www.isaserver.org/tutorials/Outbound-SSL-Inspection-TMG-Firewalls-Part1.html