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

Microsoft Forefront TMG – Explaining the Forefront TMG SDK

Abstract

In this article I will show you how the Forefront TMG SDK tools extends the functionality of Forefront TMG and how the SDK will give you some additional information about how Forefront TMG works under the hood.

Let's begin

The Forefront TMG 2010 SDK contains libraries, tools, samples and documentation to enable developers and system administrators to deploy, configure, customize, and extend their Forefront TMG environment. You can download the Forefront TMG SDK for free here.

There are a lot of tools which are separately available for download and we will have a briefly look into the most important tools. Let us start with the ADAM Sites tool for Forefront TMG Enterprise.

ADAM Sites Tool for Forefront TMG Enterprise Edition

The ADAM Sites tool is used to define AD-LDS (Active Directory Lightweight Directory Service) sites to control the traffic between Forefront TMG Enterprise Management Servers (EMS). The Enterprise Management Server is a server which is used to manage a TMG Enterprise Array or even possibly, a standalone server. Every Forefront TMG nodes which uses this EMS, gets the configuration from this EMS Server. By default, an EMS Server is not site aware, so if you have multiple EMS Servers in different locations there is no way to control the replication interval and the costs used by this link. ADAM Sites tool allows you to define AD-LDS site links and associate costs and a replication interval between this links. Before you can use the ADAM Sites tool copy the ADAMSITES.EXE file to the Forefront TMG installation directory. The following screenshot shows the command line options of ADAM Sites.

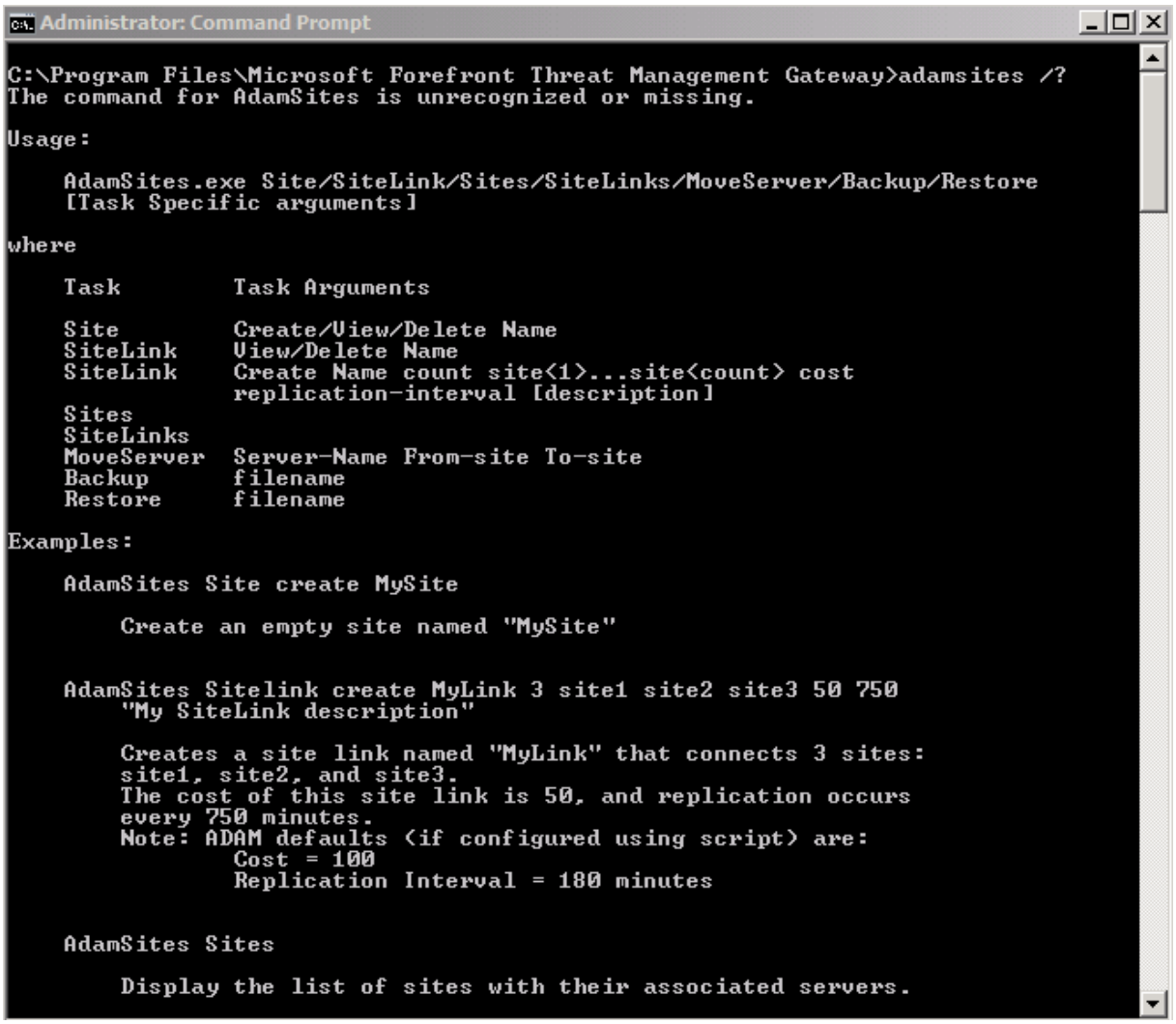

Figure 1: ADAMSITES Tool

Auto Discovery Configuration Tool for Forefront TMG

The Auto-Discovery Configuration Tool can be used to configure Active Directory with a marker key that points to your Forefront TMG server. This key is used by the TMG (formerly Firewall client) client to locate the Forefront TMG server and connect to it. This is an alternative and more secure method as DHCP/DNS to find the Forefront TMG Server. If no Active Directory Marker is found, the Forefront TMG client falls back to DHCP/DNS to find its Forefront TMG Server.

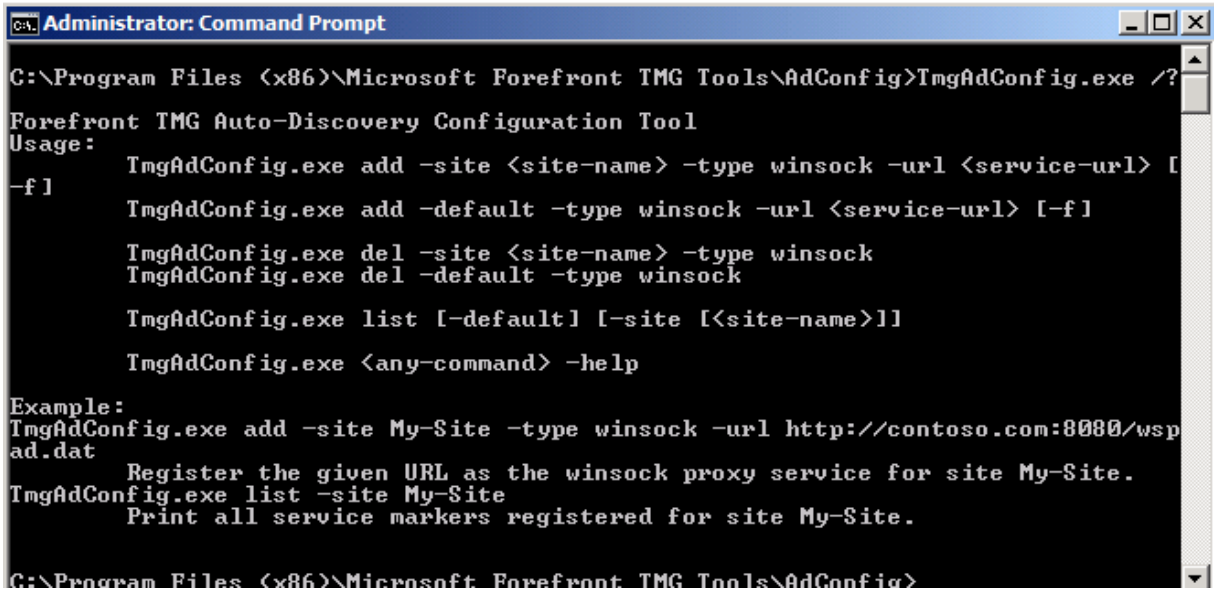

Figure 2: TMG Auto-Discover Tool

Cache Directory Tool for Forefront TMG

Use the Cache Directory Tool to view real-time cache contents, save information about the current cache contents to a file, and mark obsolete items that should not be served from the cache. The Cachedir utility is in my opinion the most wanted utility from the Forefront TMG SDK and was also available in previous ISA Server version. Before you can use the Cachedir tool copy the CACHEDIR.EXE file to the Forefront TMG installation directory.

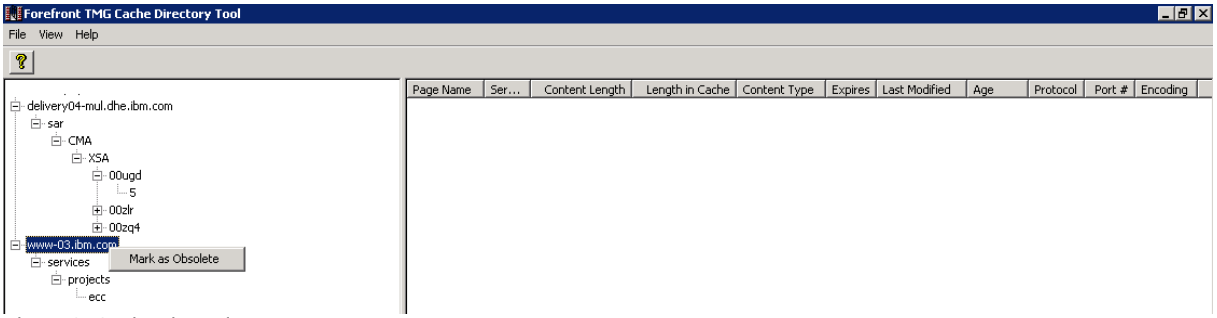

Figure 3: CacheDir Tool

CertTool for TMG

The Certtool for TMG is only required when you use Forefront TMG Enterprise in a workgroup environment. In a TMG workgroup environment certificates are used to communicate between the TMG servers. The Certtool helps you to ease the process of installing or substituting certificates in Forefront TMG. Before you can use the Certtool for TMG copy the ISACERTTOOL.EXE file to the Forefront TMG installation directory.

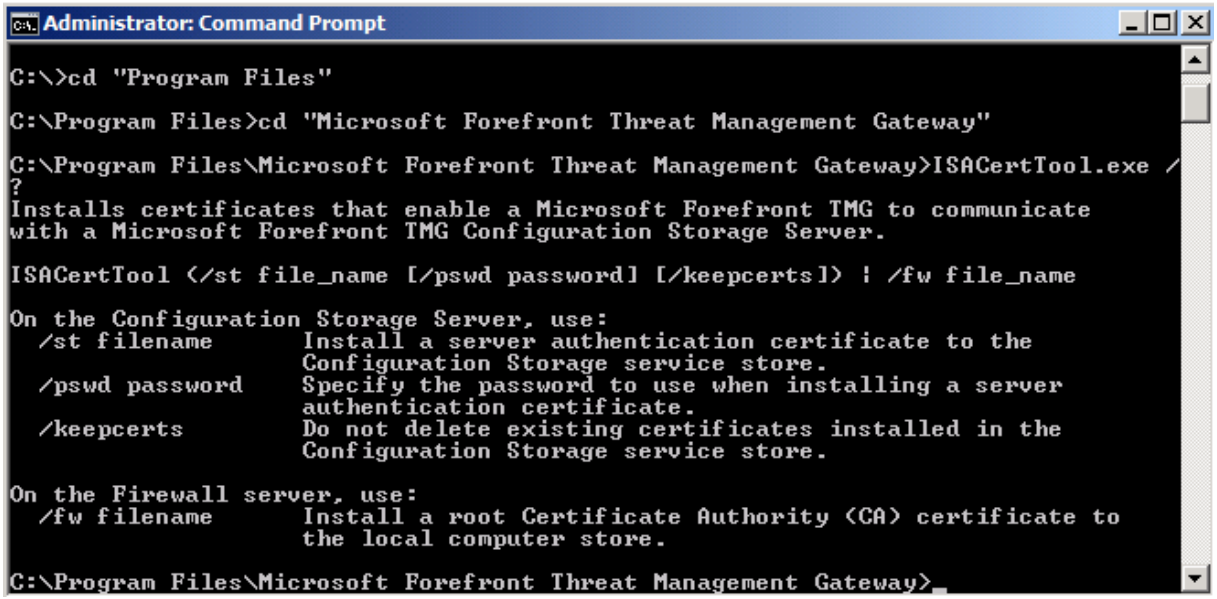

Figure 4: ISACerttool

DNS Cache Tool for Forefront TMG

Use the DNS Cache Tool on a Forefront TMG server to display the contents of the Domain Name System (DNS) cache and to delete entries in the DNS cache. For example, the Forefront TMG clients uses the Forefront TMG DNS settings for name resolution, the Secure NAT client uses the local DNS settings for name resolution. In some circumstances it might be necessary to delete the DNS Cache settings on Forefront TMG.

Please note: Clearing the DNS cache on the TMG server with the well-known IPCONFIG /FLUSHDNS command will only delete the DNS Cache from the local DNS client resolver.

Before you can use the DNS Cache tool, copy the DNSTOOLS.EXE to the Forefront TMG installation directory.

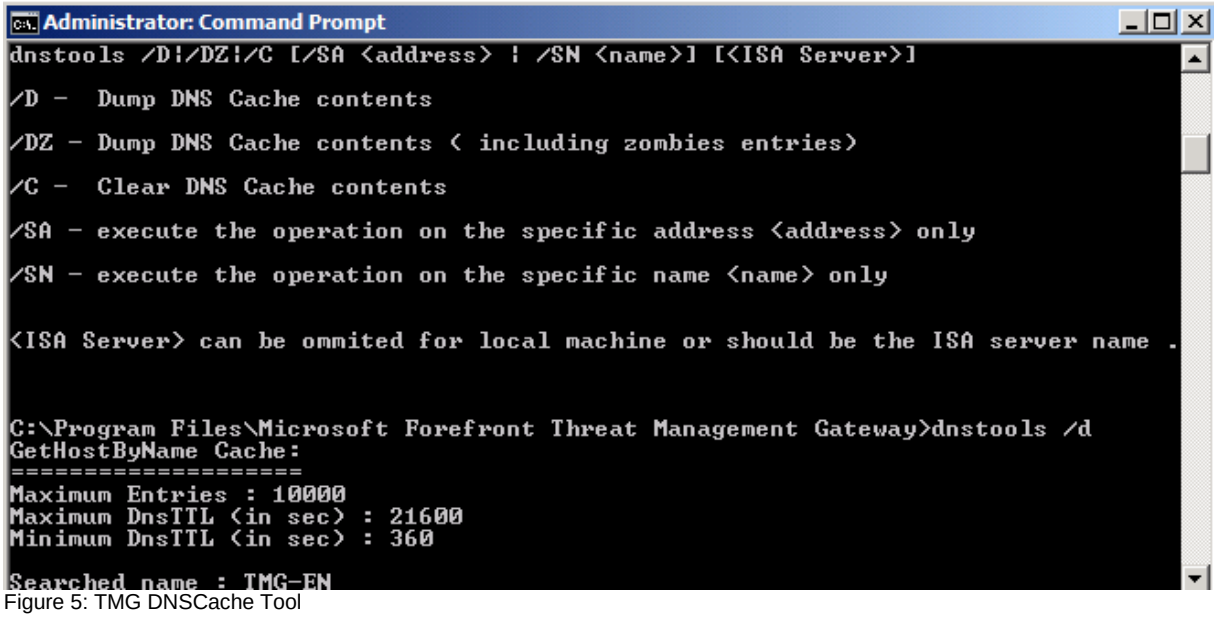

Figure 5: TMG DNSCache Tool

EE Single Server Conversion tool for Forefront TMG

Use this tool (EESingleServerConversion.exe) to help you migrate a standalone server running either ISA Server 2004 Enterprise Edition or ISA Server 2006 Enterprise Edition to Forefront TMG in standalone mode.Before you import the ISA Server Enterprise configuration into Forefront TMG Enterprise in Standalone Mode, you have to convert the different XML settings from the ISA Server export format to a readable format to import the configuration into Forefront TMG Enterprise. After installing the conversion tool and copying the ISA Enterprise configuration file to the Forefront TMG server, open a command prompt and enter the command with the source and target XML file as shown in the following screenshot.

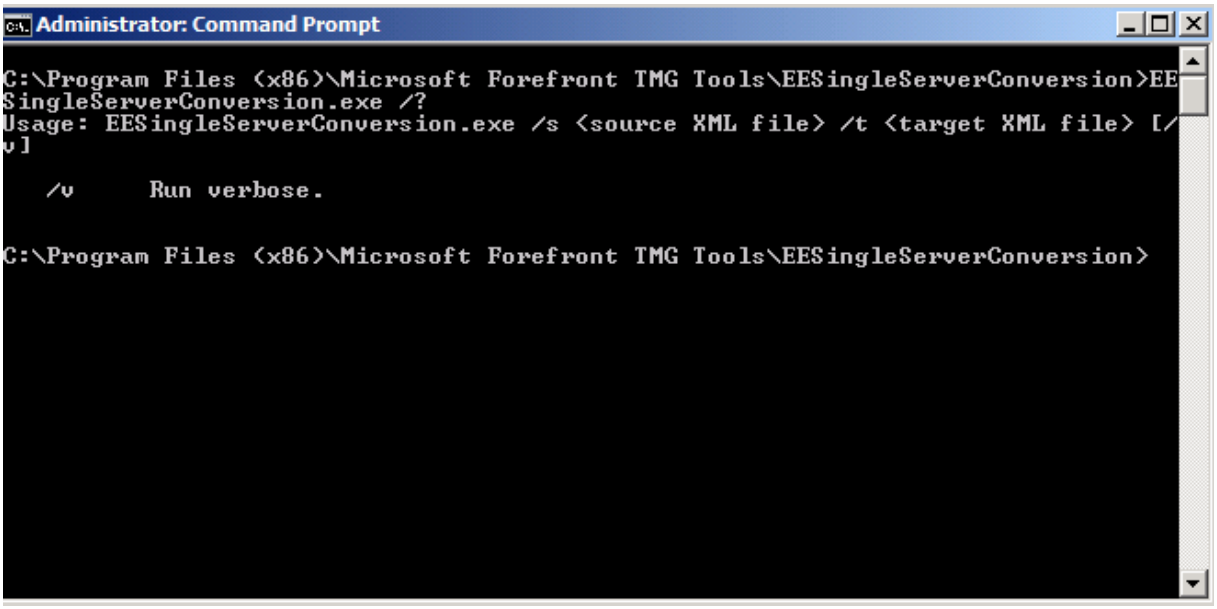

Figure 6: ISA to TMG Single Server conversion tool

This command will convert the ISA Server Enterprise configuration file to a format supported on Forefront TMG Enterprise standalone.

MSDEToText Tool for Forefront TMG

The MSDEtoText tool can be used to convert Forefront TMG SQL Express Server logs into a text file, or to display their contents on the screen. You can use the MSDEtoText utility with ISA Server 200x and Forefront TMG. The following screenshot shows the syntax of the MSDEtoText tool.

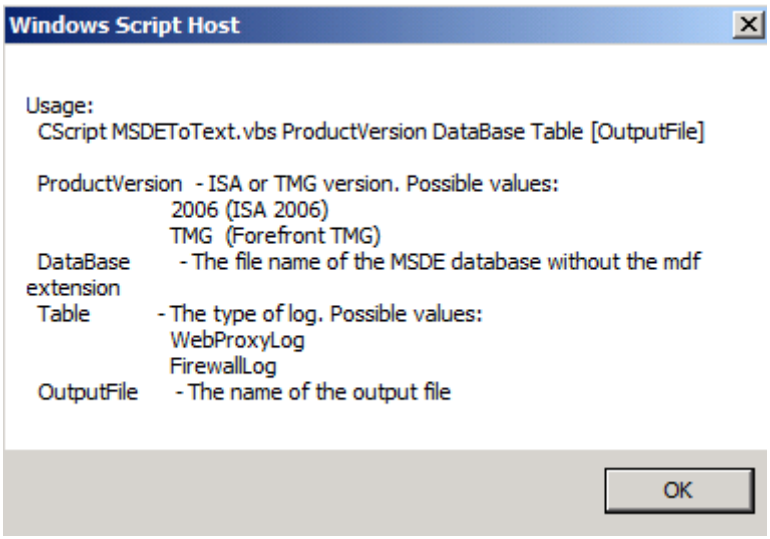

Figure 7: MSDE to Text conversion tool

The following screenshot shows an example for exporting a Firewall log file.

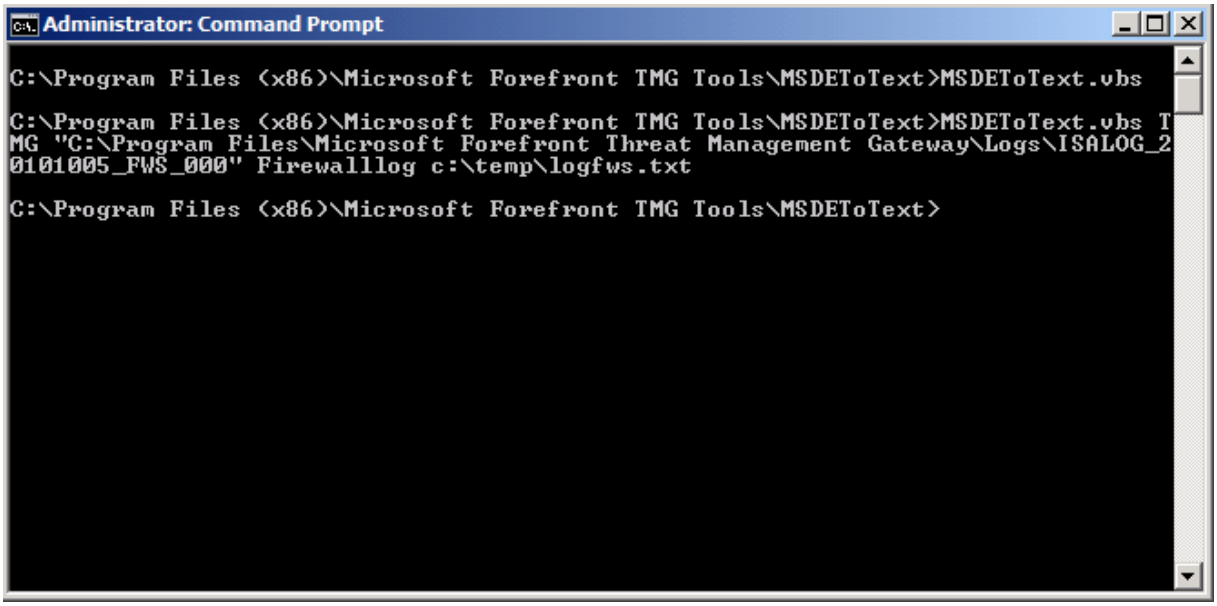

Figure 8: MSDE to Text conversion tool example

Remote Access Quarantine Tool for Forefront TMG

Forefront TMG also supports the legacy Remote Access Quarantine service which must be used in ISA Server 200x to enforce quarantine for VPN clients which connects to ISA Server. I recommend using NAP (Network Access Protection) from Windows Server 2008 in combination with Forefront TMG, which is a much easier and more flexible to configure as the RQS-components from the TMG SDK.

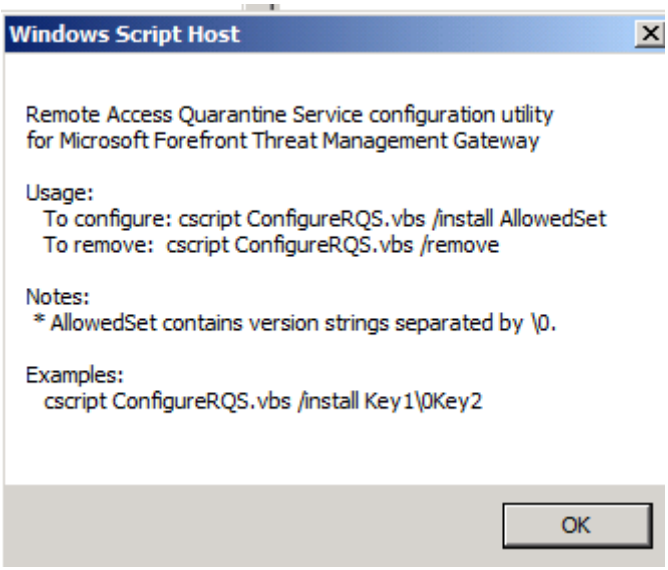

Figure 9: RQS tools

RSA Test Authentication Utility for Forefront TMG

The RSA Test Authentication Utility can be used to verify that a computer running Forefront TMG can authenticate to a computer running RSA Authentication Manager. Before you can use the RSA Test Authentication utility copy the SDTEST.EXE and SDUI.DLL files to the Forefront TMG installation directory.

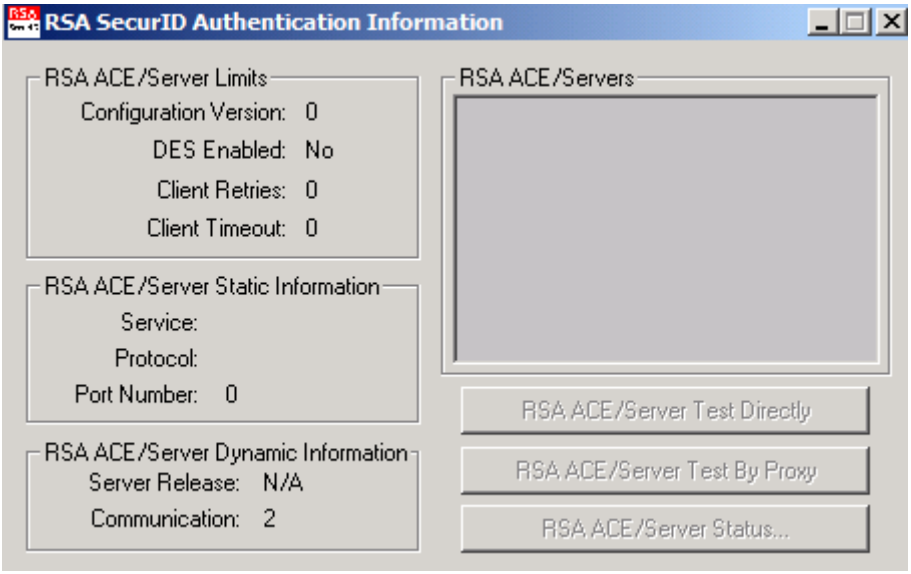

Figure 10: RSA SecurID Authentication tool

Security Configuration Wizard (SCW) Update for Forefront TMG Standard Edition and Enterprise Edition

Windows Server 2008 and Windows Server 2008R2 include a tool called the Security Configuration Wizard (SCW). This tool can be used to simplify the task of hardening the underlying operating system in preparation for deploying Forefront TMG. The SCW will create a policy that configures services, registry settings, Audit policies and more based on the roles and features installed. By default, the SCW doesn't know that Forefront TMG is installed. The Forefront TMG SDK comes with an extension to the SCW.

There are two files which must be copied to the Windows\Security\Msscw\kbs directory:

- SCW_TMG_W2K8R2_SP0.XML
- SCW_TMGEMS_W2K8R2_SP0.XML

After that open an elevated command prompt and enter the following command:
scwcmd register /kbname:TMG /kbfile:SCW_TMG_W2K8R2_SP0.xml

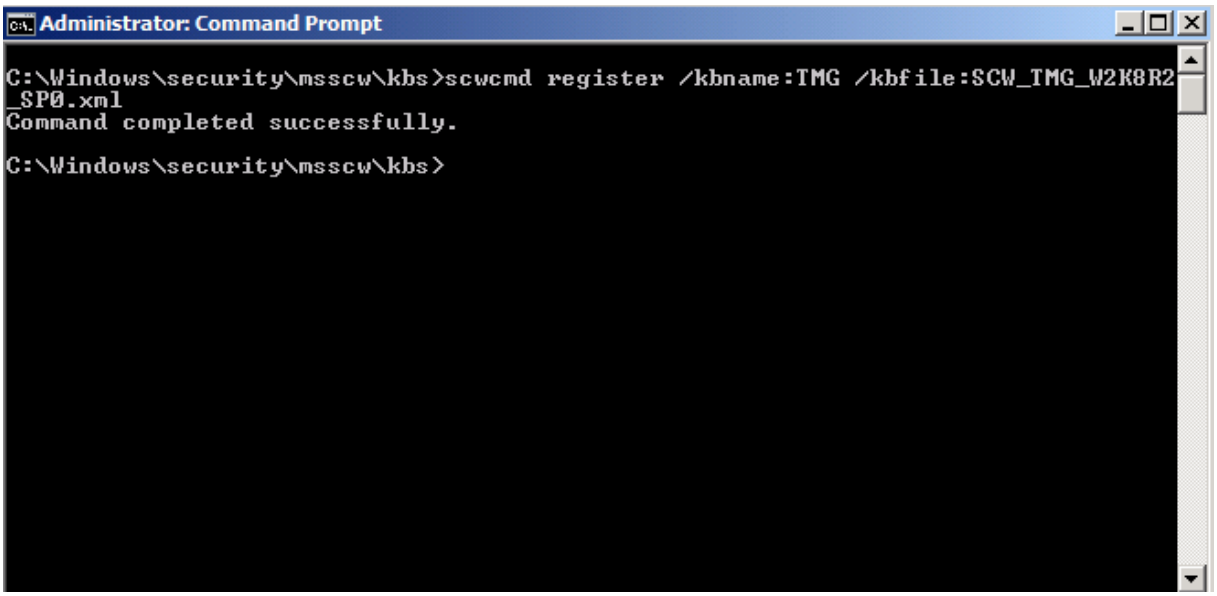

Figure 11: TMG SCW tool

After that create a new Security policy and the SCW will see the roles installed on the Forefront TMG server.

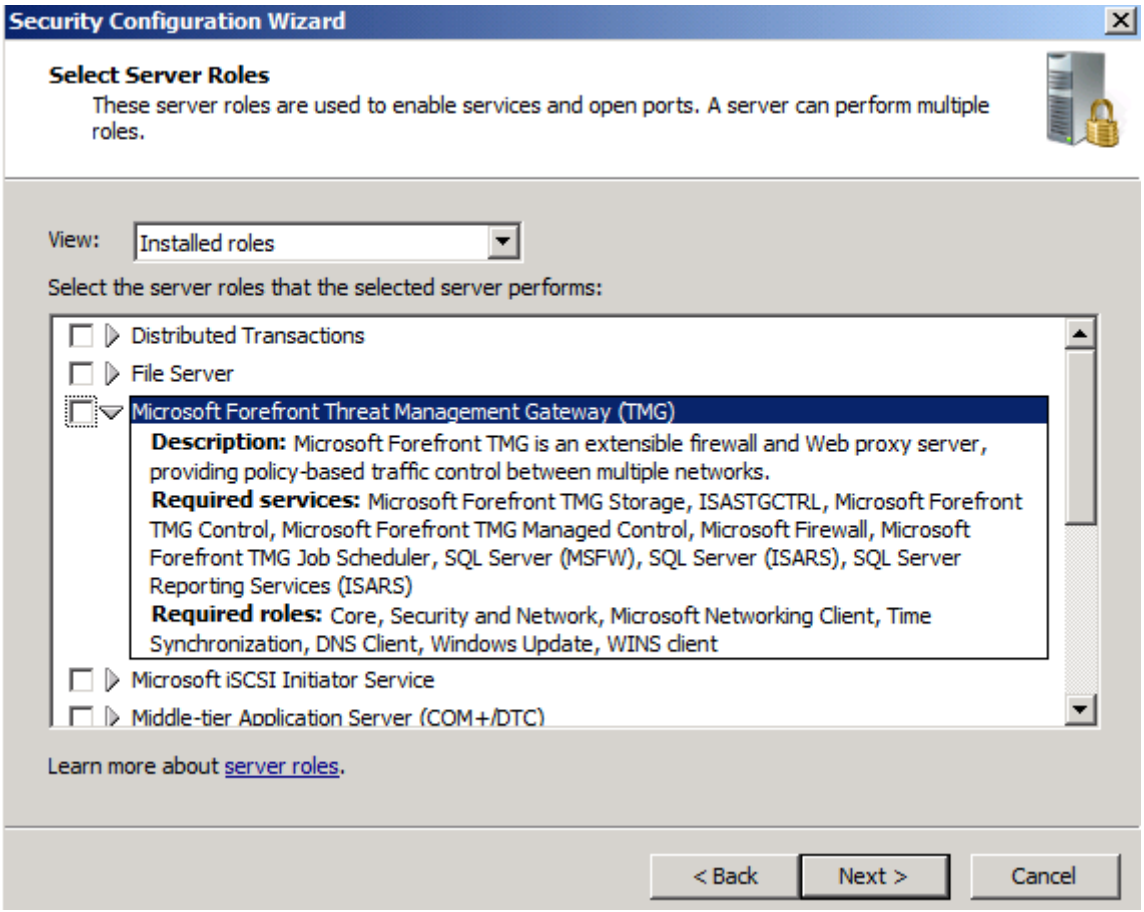

Figure 12: SCW with TMG role

For more information about the SCW and Forefront TMG I recommend reading the article of Richard Hicks.

Forefront TMG 2010 SDK

The Forefront TMG SDK comes with a very helpful ISASDK.CHM file which contains a lot of deep technical information about Forefront TMG and some examples for developing Application and Web filters in Forefront TMG.

ISASDK.CHM

The ISASADK.CHM file contains information about the Forefront TMG architecture and its subsystems and some code samples to configure or extend Forefront TMG programmatically.

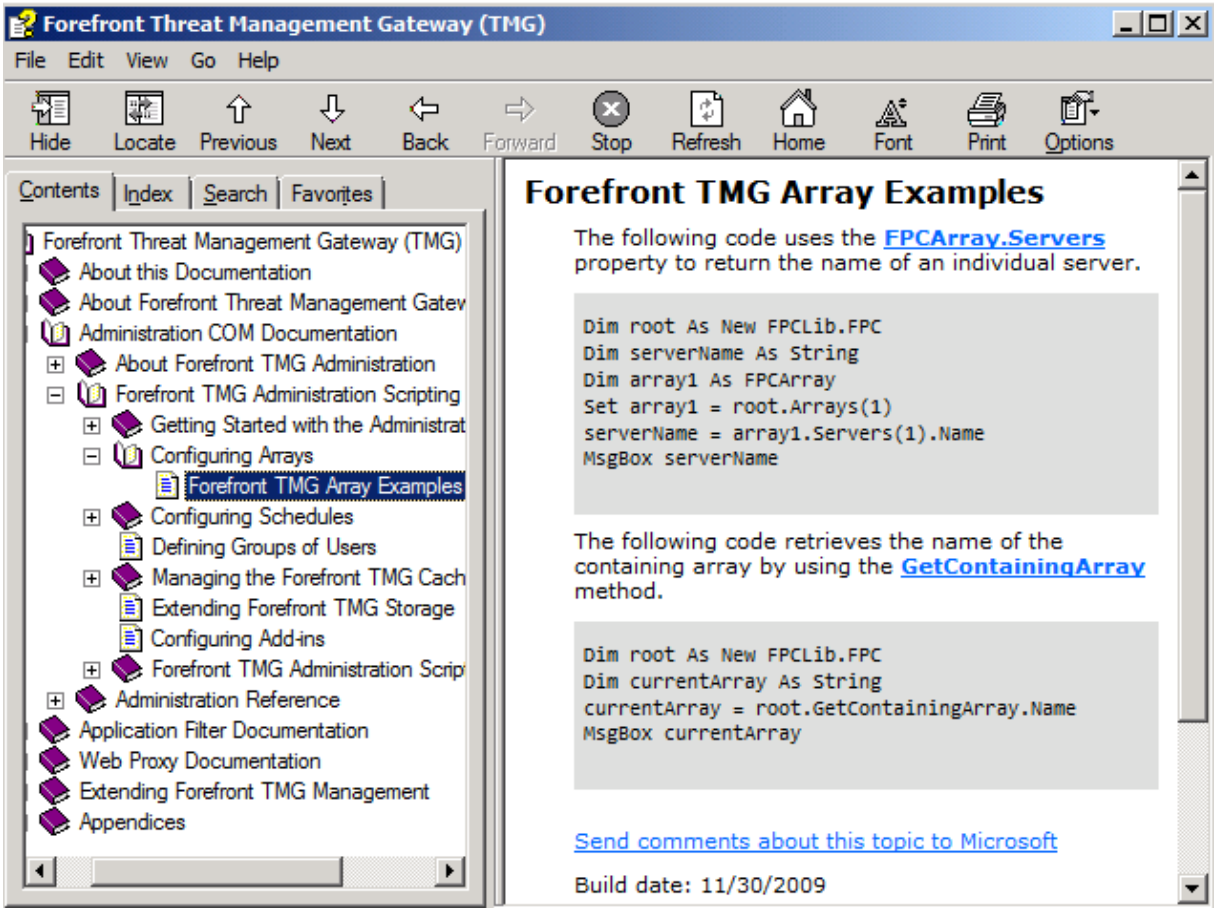

Figure 13: TMG SDK documentation

Samples/Admin directory

There are some very helpful VBS scripts in the samples/Admin directory installed by the Forefront TMG SDK setup routine. For this article I will show you two examples. The first script is the HTTPFilteconfig.vbs which can be used to import or export the HTTP filter settings from a specific firewall policy rule.

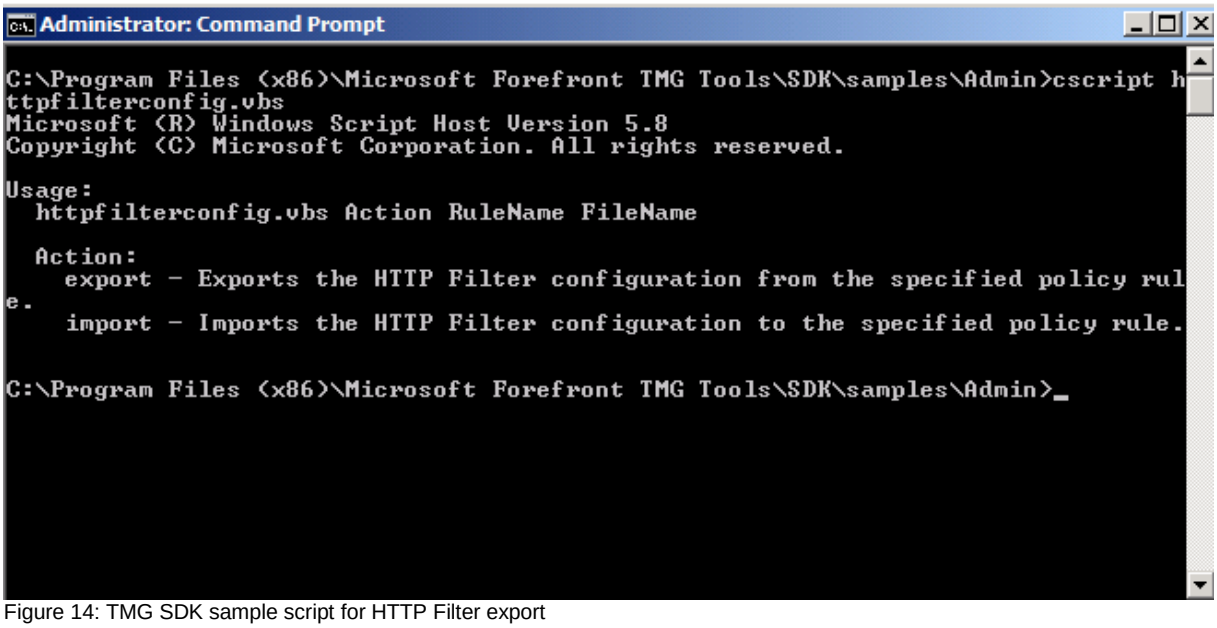

Figure 14: TMG SDK sample script for HTTP Filter export

There is another very helpful script called ActiveSession.vbs which will give you a quick overview about the current connected sessions on Forefront TMG.

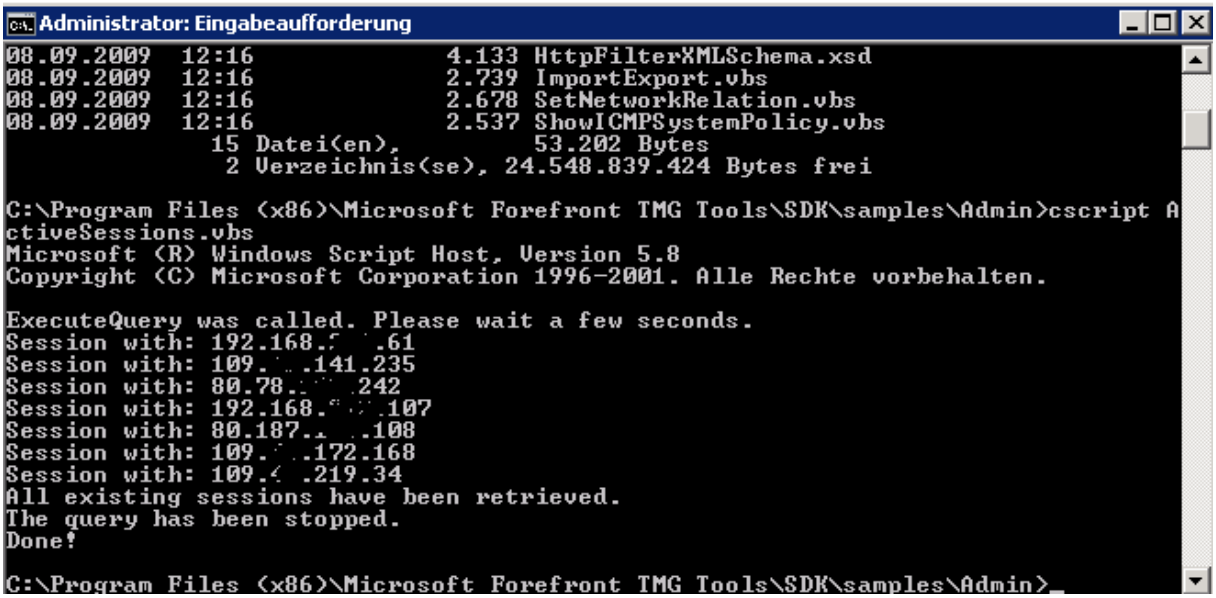

Figure 15: TMG SDK sample script to display Active Sessions

Conclusion

In this article I gave you an overview about the Forefront TMG SDK utilities and the SDK documentation itself. I recommend also spending some time to read the Forefront TMG SDK documentation because they contain a lot of additional information about the internal architecture of Forefront TMG.

Related links

Forefront TMG SDK
http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8809CFDA-2EE1-4E67-B993-6F9A20E08607
ISA Server 2006 SDK
http://www.microsoft.com/downloads/en/details.aspx?familyid=16682c4f-7645-4279-97e4-9a0c73c5162e&displaylang=en
SCW on German Forefront TMG servers
http://www.it-training-grote.de/download/TMG-SCW.pdf
Microsoft Forefront TMG – TMG Storage 101
http://www.isaserver.org/tutorials/Microsoft-Forefront-TMG-Storage-101.html
Using the Security Configuration Wizard with Microsoft Forefront Threat Management Gateway 2010
http://www.isaserver.org/tutorials/Using-Security-Configuration-Wizard-Microsoft-Forefront-Threat-Management-Gateway-2010.html