
Microsoft Forefront TMG – Remote Administration concepts

Abstract

In this article I will show you the different concepts to access a Forefront TMG Server from your workstations with Microsoft RDP or the TMG MMC installed on the local client. We will also talk about the required Firewall policies to access the TMG Server from remote via WMI.

Let's begin

In larger environments with different Forefront TMG Administrators it may be helpful to let the Administrator access the Forefront TMG Management Console remotely via RDP or the TMG MMC installed locally on the client machine.

RDP access to the TMG Server

If you want to remotely access the Forefront TMG Server with the Remote Desktop protocol (RDP) we must first enable RDP on the Forefront TMG Server and specify the encryption level and for security reasons we should also enable NLA (Network Level Authentication). Ideally we should use a certificate issued from an internal Certification Authority to avoid certificate name and trust warnings as shown in the following screenshot.

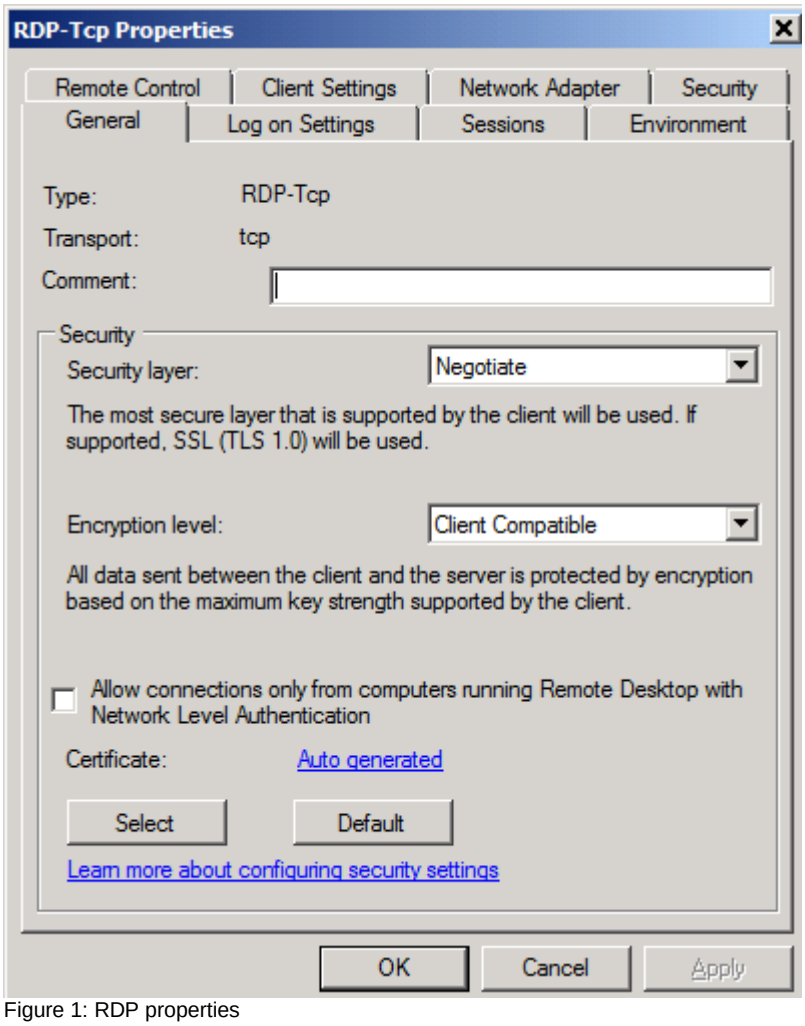

Figure 1: RDP properties

RDP publishing issues

Some Administrators want to publish an internal RDP Server with a Server publishing rule on the TMG Server. If you want to do this you must reconfigure the RDP connection to listen only on the internal network adapter of the TMG Server because the Listener created by the Server publishing rule will listen on the external adapter and if you don't change the RDP settings you will get a socket pooling conflict. To change the settings navigate to the Network adapter settings in the RDP-TCP properties and change the RDP listener to the internal network adapter.

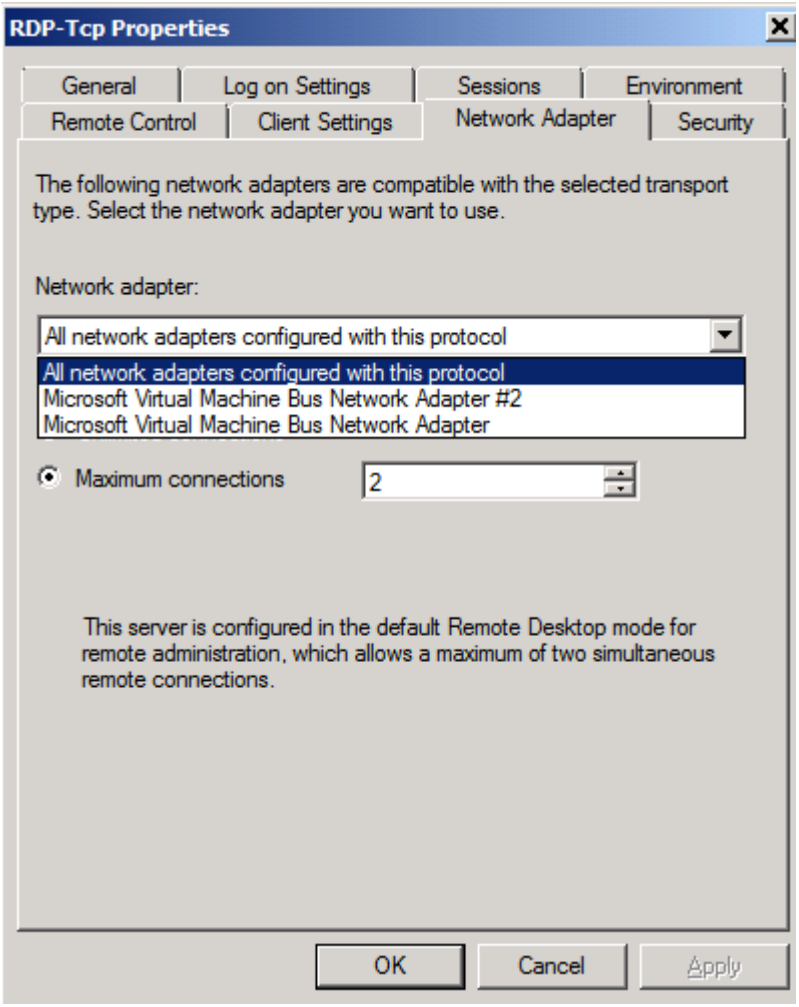

Figure 2: RDP properties – Network adapter

Next we must allow the Administrator or required users to access the TMG Server via RDP. The best way is to put the users / user groups into the local Remote Desktop users group in the local account database on the TMG Server.

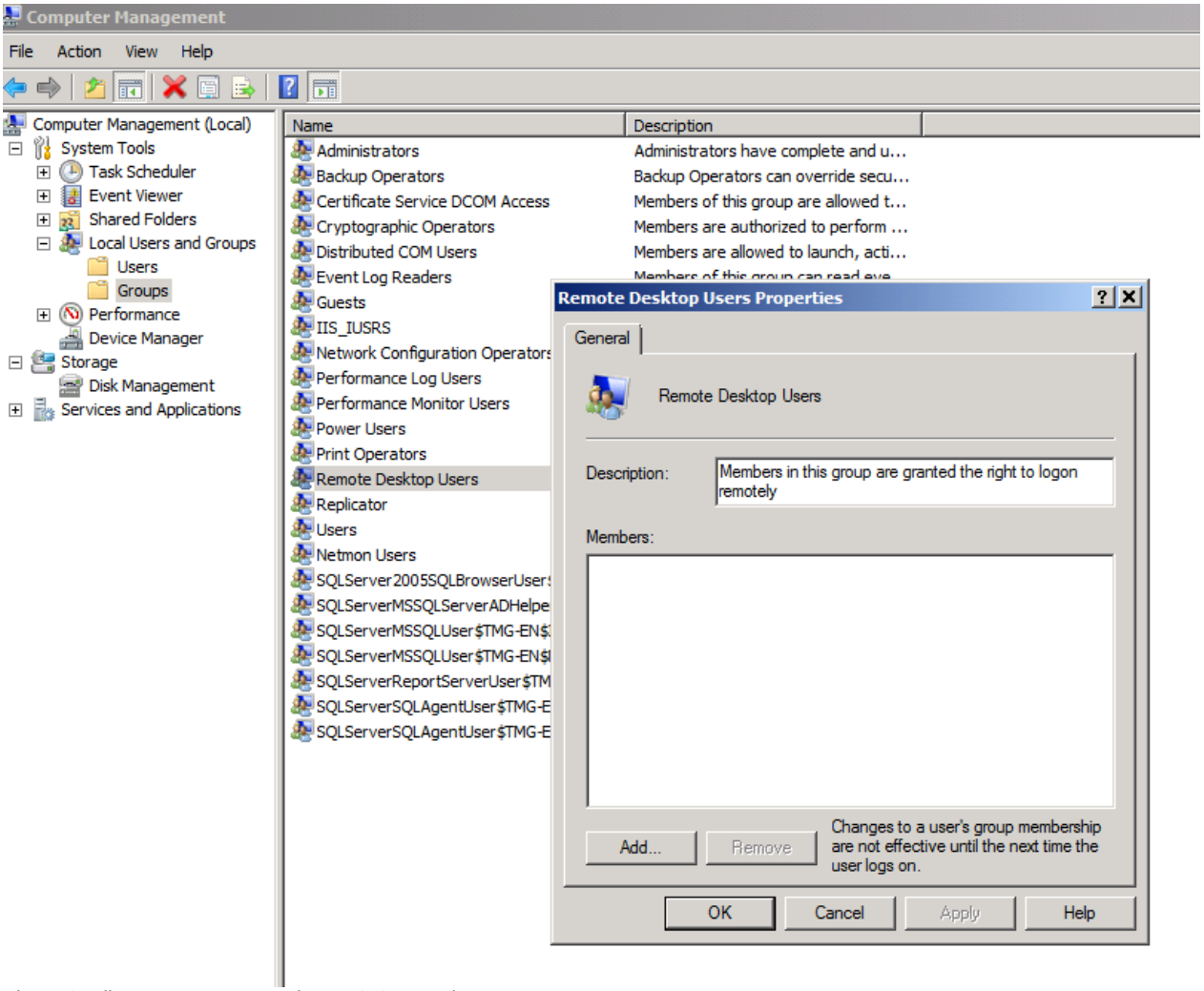

Figure 3: Allow users to access the TMG Server via RDP

Now the users have access to the TMG Server computer we must give the users the necessary rights for TMG Server administration. Forefront TMG Standard and Enterprise comes with a simple role concept which grants users different rights to the Forefront TMG configuration as shown in the following screenshot.

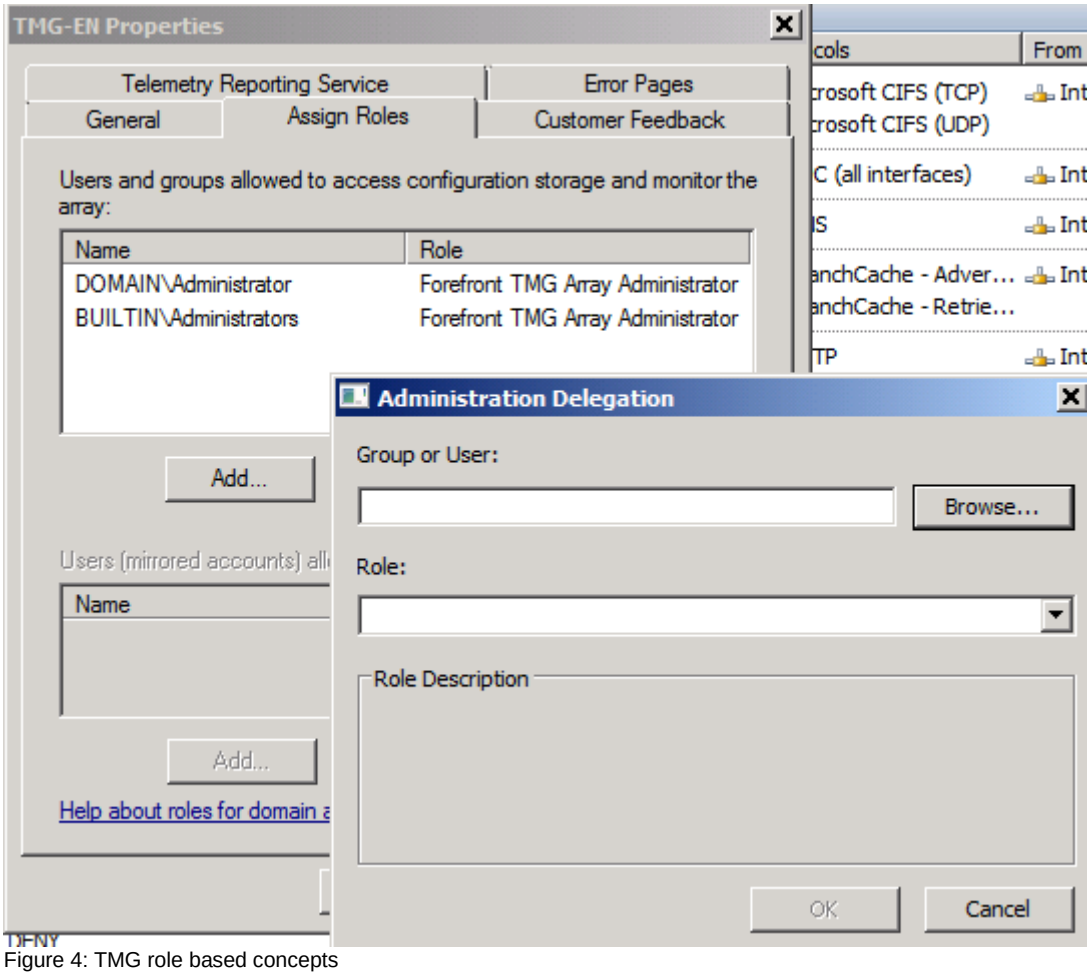

Figure 4: TMG role based concepts

The last step is to change the System Policy rule settings to allow the computers to access the Forefront TMG Server. Forefront TMG Server protects the system for accessing from the internal network. To allow the computers to access the TMG Server start the TMG server and navigate to the Firewall Policy node – All Tasks – System Policy – Edit System Policy and put the computers to the Remote Management Computers set.

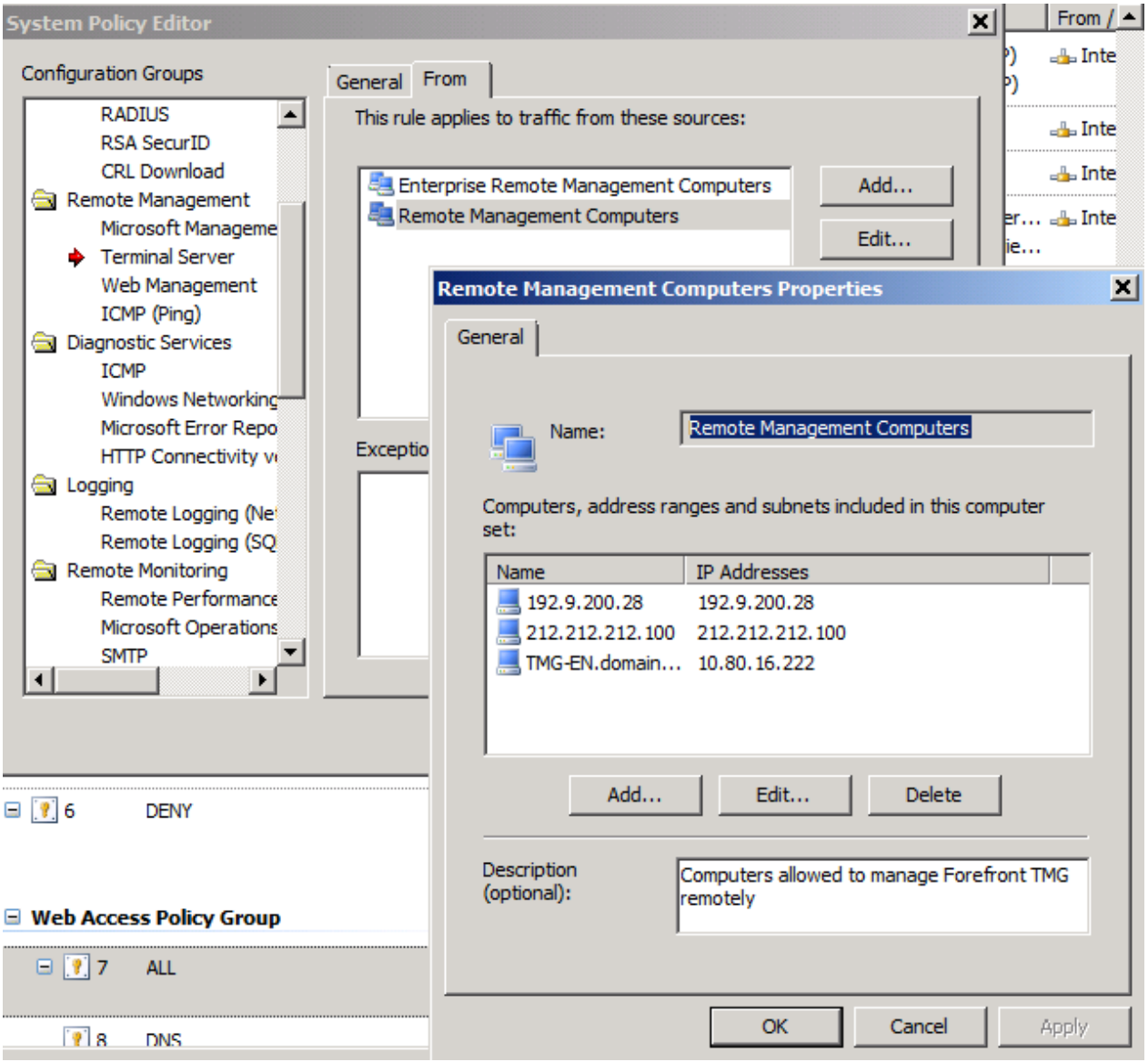

Figure 5: System policy rules

WMI access

If you want to access the Forefront TMG Server remotely via WMI (Windows Management Instrumentation), you must configure some additional settings on the Forefront TMG Server. First we must disable the “Enforce Strict RPC compliance” setting in the System Policy rule set for Active Directory access or if you created a dedicated Firewall Policy rule set which allows the RPC protocol from the client machines to the LocalHost you must disable the “Enforce Strict RPC compliance” in the Firewall Policy rule. To do so right click the Firewall Policy rule and select the RPC setting.

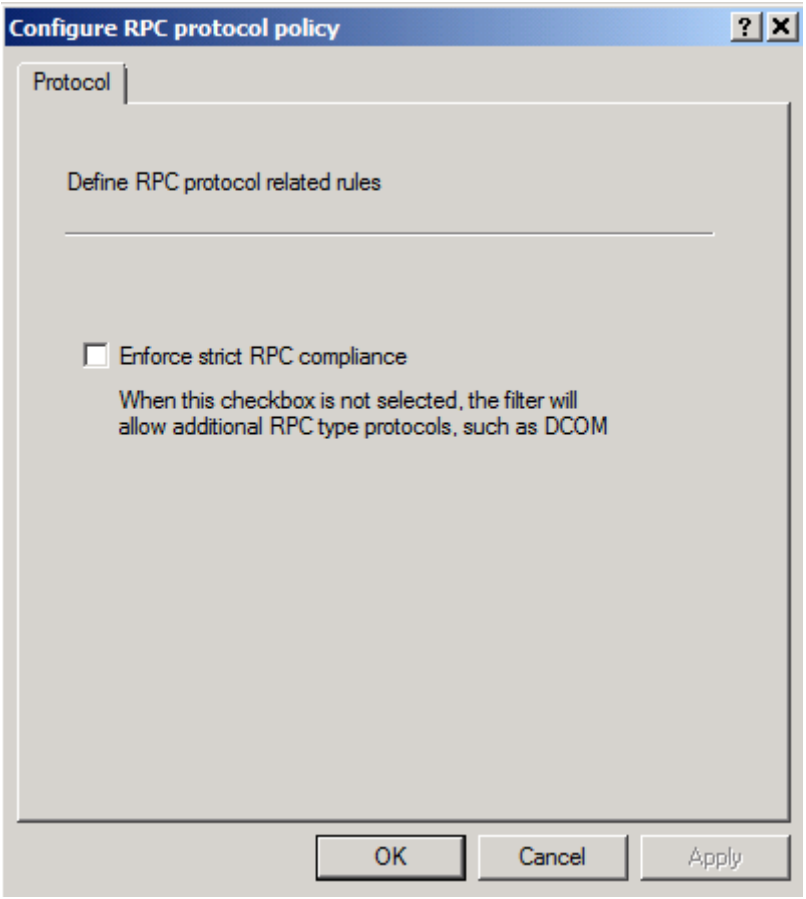

Figure 6: Disable strict RPC compliance

In many scenarios disabling the Strict RPC compliance is not sufficient. In the following screenshot I created a Firewall Policy rule for WMI access with port 10002 to access the TMG Server with a remote WMI tool called PRTG with a special implementation from the Paessler company.

Please note: For different applications accessing the Forefront TMG Server via WMI it might ne necessary to create Firewall Policy rules with different Ports or Port ranges.

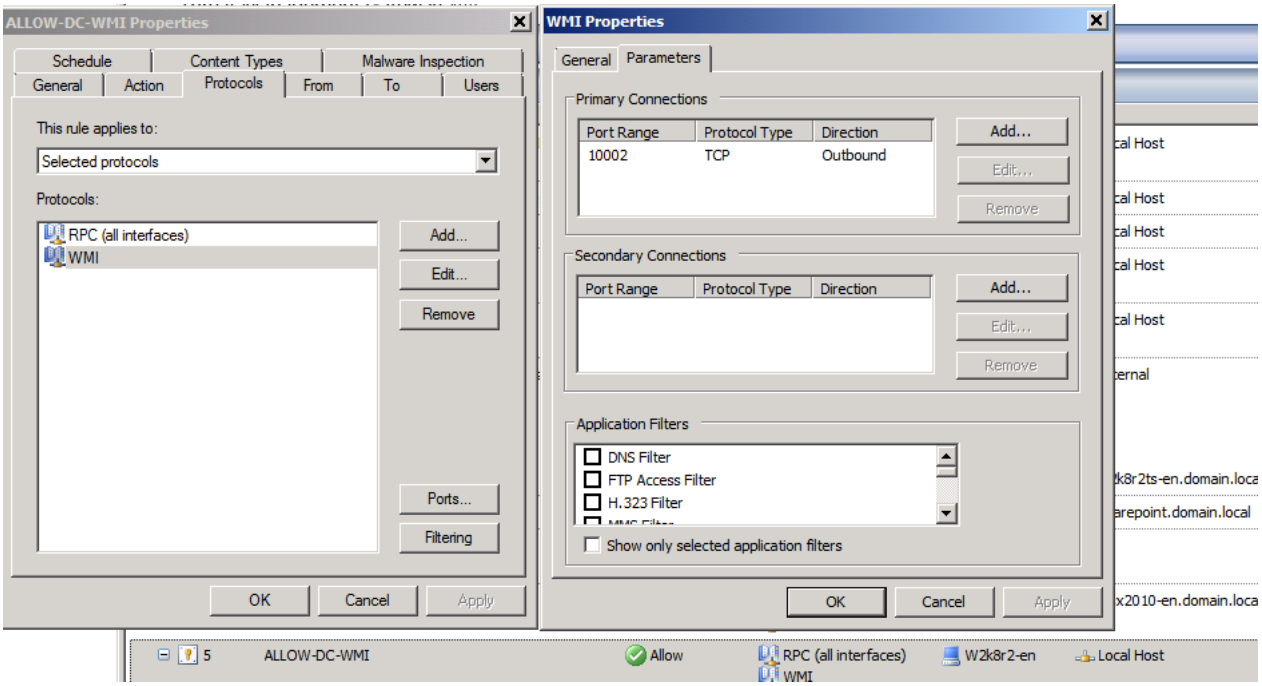

Figure 7: Allow WMI access

Remote TMG MMC installation

It is possible to install the TMG MMC on a local Windows client machine to access the TMG Server remotely.
Insert the TMG DVD on the local machine and install only the Forefront TMG Management console component.

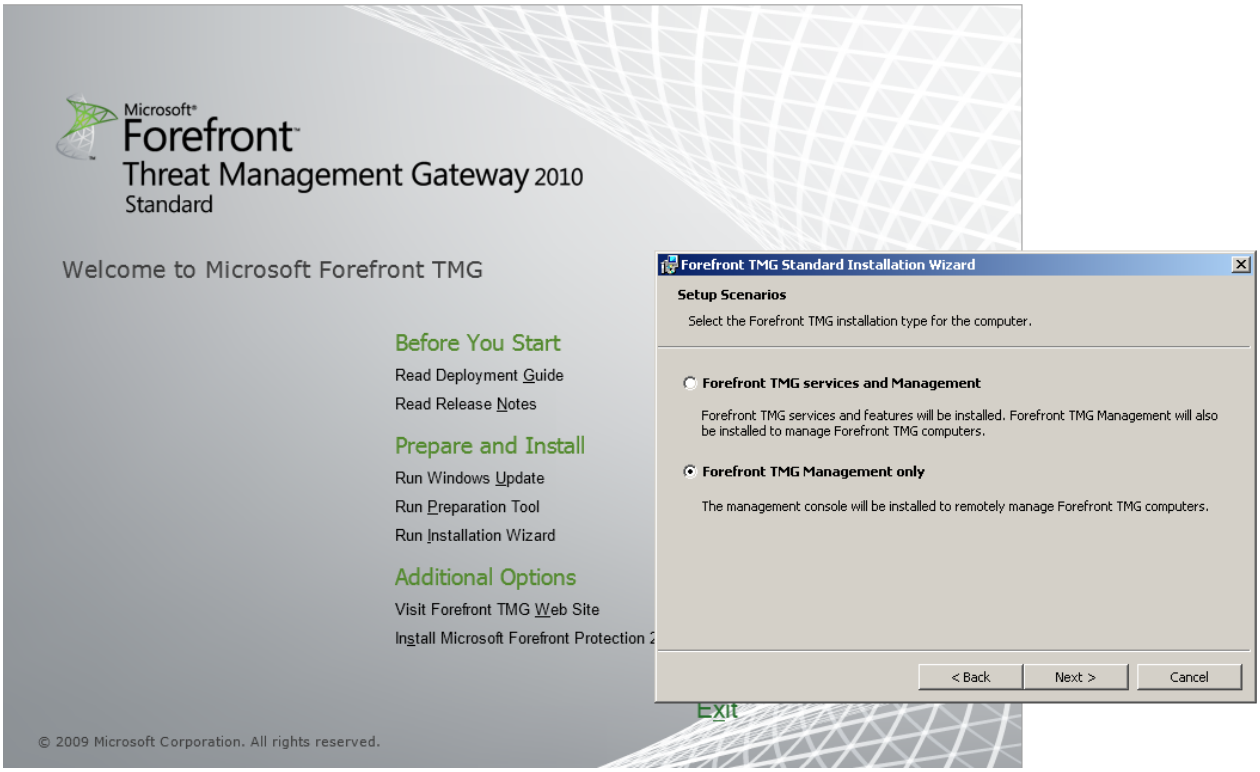

Figure 8: Local TMG MMC installation

Please keep in mind that you must apply the same TMG Service Packs and Rollups on the clients which are installed on the Forefront TMG Server.

Conclusion

In this article we talked about the different concepts to access a Forefront TMG Server from a remote workstation via a Remote Desktop connection or a local installed Microsoft Forefront TMG Management console.

Related links

Strict RPC compliance
http://blogs.technet.com/b/isablog/archive/2007/05/16/rpc-filter-and-enable-strict-rpc-compliance.aspx
TMG WMI access (German)
http://www.it-training-grote.de/download/TMG-WMI.pdf
Remote Management Concepts in ISA Server 2006
http://technet.microsoft.com/en-us/library/bb794770.aspx
About Forefront TMG roles and permissions
http://technet.microsoft.com/en-us/library/dd897006.aspx