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.

RDP-Tcp Properties			×	
Remote Control C General Log o	ient Settings   n Settings	Network Adapter Sessions	Security Environment	
Type: RDF	P-Tcp			
Transport: tcp				
Comment:				
Security				
Security layer:		Negotiate	•	
The most secure layer supported, SSL (TLS 1	that is supported .0) will be used.	by the client will be	used. If	
Encryption level:	[	Client Compatible	•	
All data sent between the client and the server is protected by encryption based on the maximum key strength supported by the client.				
Allow connections only from computers running Remote Desktop with Network Level Authentication				
Certificate:	Auto generated	l		
Select	Default			
Learn more about configuring security settings				
·	ОК	Cancel	Apply	

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.

RDP-Tcp Properties		×
General Log on Settings Remote Control Client Settings	Sessions Env Network Adapter	vironment Security
The following network adapters are com type. Select the network adapter you wa	patible with the selected to ant to use.	ransport
Network adapter:		
All network adapters configured with th	is protocol	<u> </u>
All network adapters configured with the Microsoft Virtual Machine Bus Network Microsoft Virtual Machine Bus Network	s protocol Adapter #2 Adapter	
Maximum connections 2		
This server is configured in the defa remote administration, which allows remote connections.	ault Remote Desktop mod a maximum of two simulta	e for ineous
ОК	Cancel	Apply

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.

1G-EN Properties			×		
		r.	cols		From
Telemetry Reporting General Ass	Service ign Roles	Error Pages Customer Feedback	roso	oft CIFS (TCP) oft CIFS (UDP)	👍 Int
Users and groups allowed to array:	access configu	ration storage and monitor the	C (a	ll interfaces)	👍 Int
Name	Role		s		📥 Int
DOMAIN\Administrator BUILTIN\Administrators	Forefr Forefr	ont TMG Array Administrator ont TMG Array Administrator	anch anch	Cache - Adver. Cache - Retrie	👍 Int
			TP		📥 Int
	Administ	tration Delegation			×
Add Users (mirrored accounts) a Name	Group or Us	er:		Brow	se
Add Help about roles for domain	Role Descr	iption			
KTO			OK	Car	ncel

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.

Configure RPC protocol policy	<u>?</u> X
Protocol	
Define RPC protocol related rules	
Enforce strict RPC compliance When this checkbox is not selected, the filter will allow additional RPC type protocols, such as DCOM	
	1
OK Cancel	Apply

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.

ALLOW-DC-WMI Properties	WMI Properties	د
Schedule Content Types Malware Inspection General Action Protocols From To Users	General Parameters	1
This add papeling to:	Primary Connections	
Selected protocole	Port Range Protocol Type Direction Add 10002 TCP Outbound	cal Host
	Edit	
Protocols:	Remove	Lal Host
RPC (all interfaces) Add	Secondary Connections	Lal Host
Edit	Port Range Protocol Type Direction Add	cal Host
Remove	Edit,,,,	cal Host
	Remove	
		ternal
	Application Filters	
	DNS Filter	
Ports	FTP Access Filter	k8r2ts-en.domain.loca
Filtering		arepoint.domain.local
	Show only selected application filters	
OK Cancel Apply	OK Cancel Apply	x2010-en.domain.loca
G 💽 5 ALLOW-DC-WMI	🖉 Allow 🔍 RPC (all interfaces) 📑 W2k8r2-en 👍	Local Host

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-rpccompliance.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