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

Microsoft Forefront TMG – Publishing RD Web Access with RD Gateway – Part II

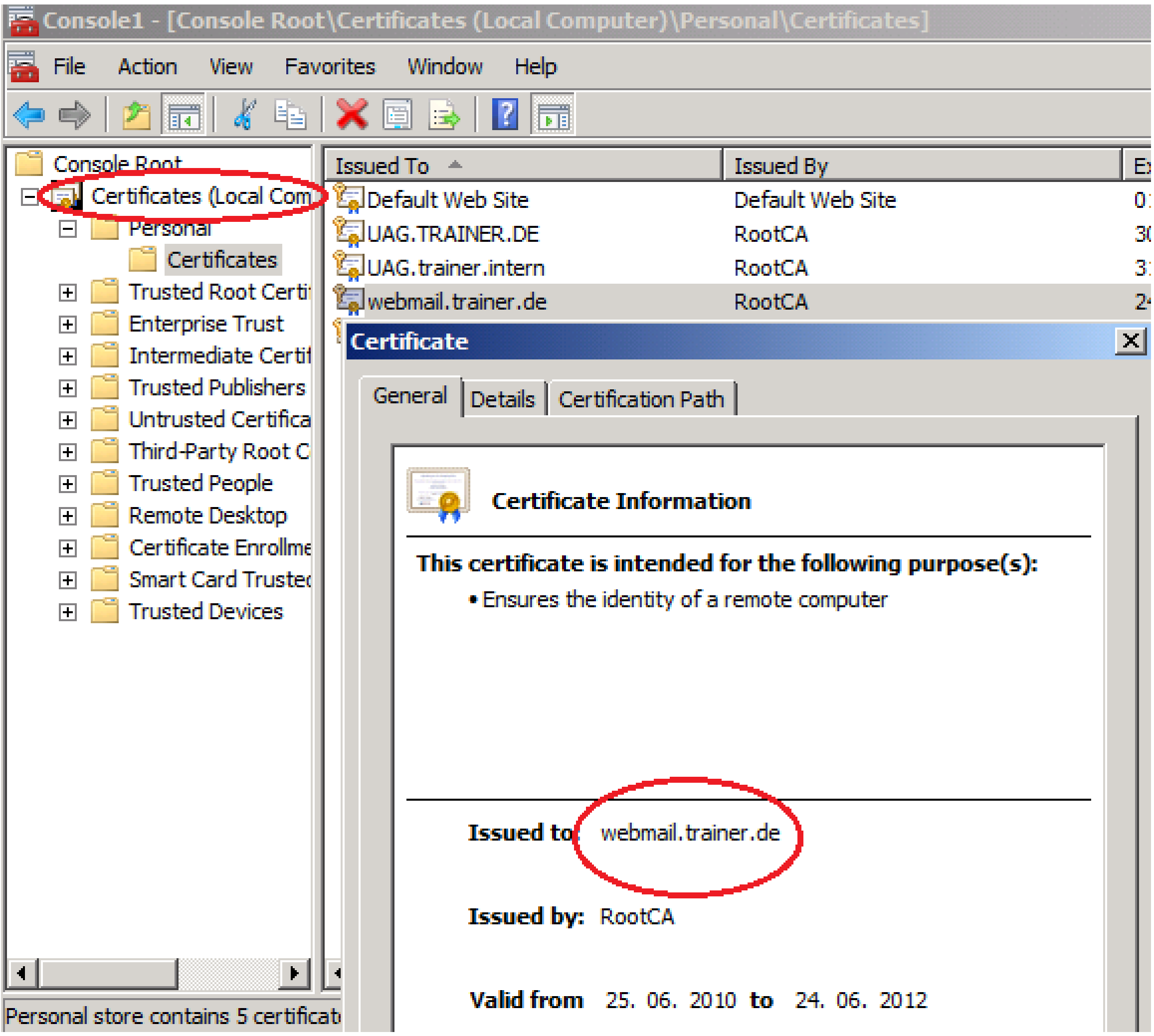
Abstract

In this short article series I will show you how to publish Remote Desktop Web Access with Remote Desktop Gateway over Microsoft Forefront TMG. In Part I of this article I showed you the configuration of the RD Web Access and RD Desktop Gateway service. In this article I will show you how to publish RD Web Access with Forefront TMG and how to access RD Web Access with a Windows 7 client.

Let’s begin

This article assumes that the Remote desktop Session Host feature is correctly installed and configured, so only the Remote Desktop Web Access and Remote Desktop Gateway components has to be installed and configured.

As a first step we have to issue a certificate with the Common Name (CN) webmail.trainer.de. This name is used by clients in the Internet to access the RD Web Access or RD Gateway service.



Issued To	Issued By	Ex
Default Web Site	Default Web Site	0
UAG.TRAINER.DE	RootCA	3(
UAG.trainer.intern	RootCA	3
webmail.trainer.de	RootCA	2

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer

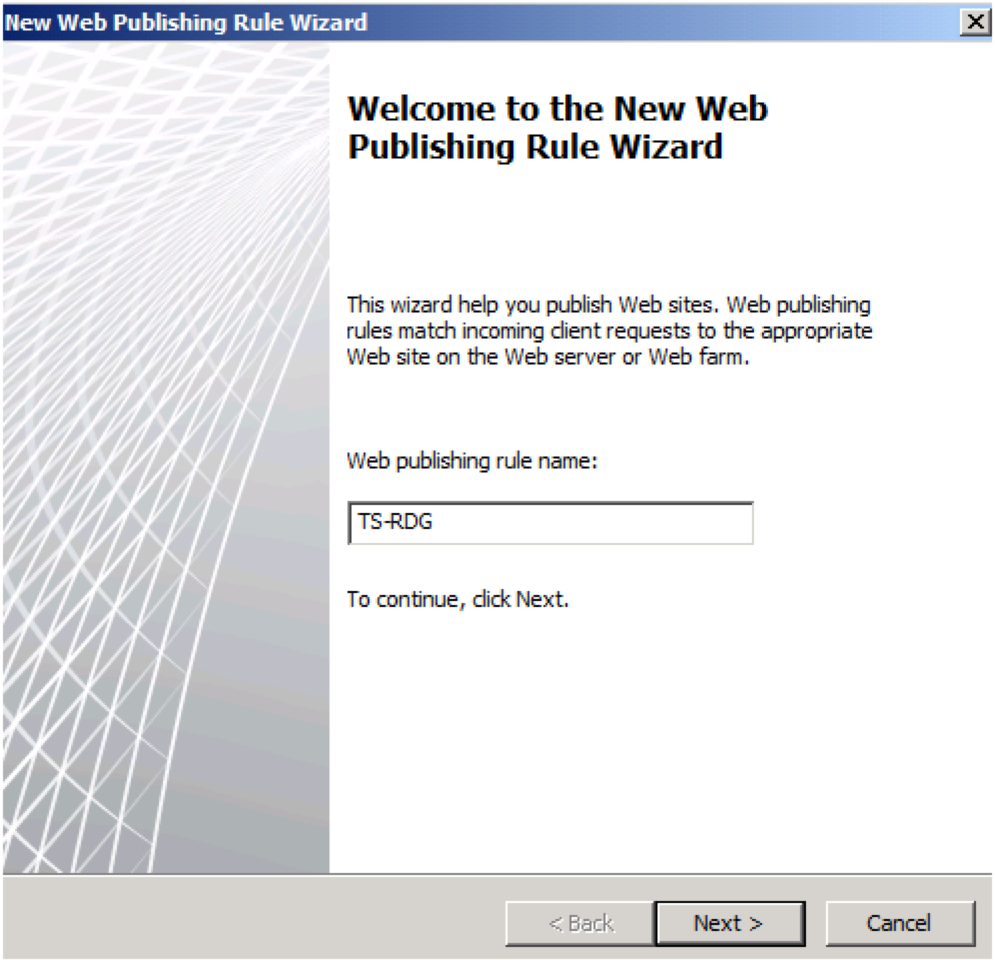
Issued to: webmail.trainer.de

Issued by: RootCA

Valid from 25. 06. 2010 to 24. 06. 2012

Figure 1: Import the Webserver certificate for TMG publishing

As a next step we have to create a Webserver or Exchange Web client publishing rule. You can use booth publishing rules.



Welcome to the New Web Publishing Rule Wizard

This wizard help you publish Web sites. Web publishing rules match incoming client requests to the appropriate Web site on the Web server or Web farm.

Web publishing rule name:

TS-RDG

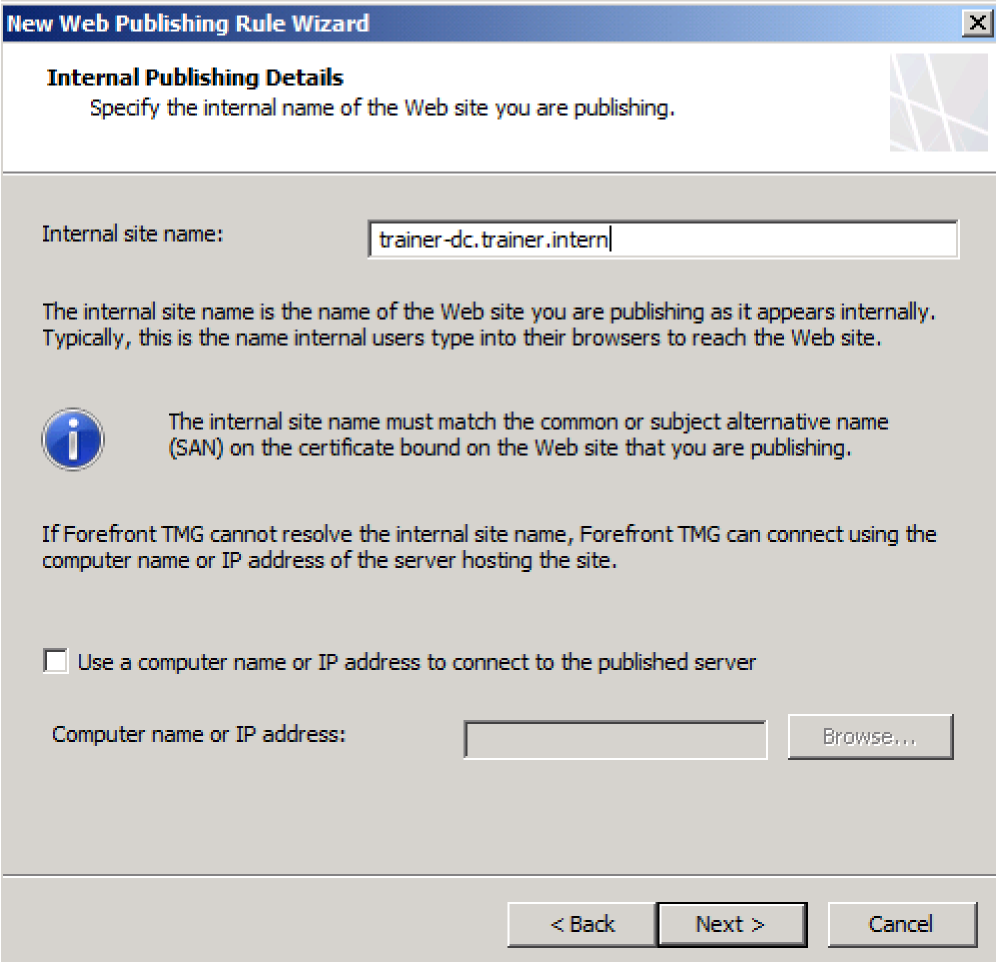
To continue, click Next.

Figure 2: Create new Web publishing rule

Select *Allow* as the rule action.

Select *Publish a single Website or Load Balancer*

Use SSL to connect to the Published Web server and enter the internal Hostname of the Server you want to publish.



Internal Publishing Details

Specify the internal name of the Web site you are publishing.

Internal site name: trainer-dc.trainer.intern

The internal site name is the name of the Web site you are publishing as it appears internally. Typically, this is the name internal users type into their browsers to reach the Web site.

The internal site name must match the common or subject alternative name (SAN) on the certificate bound on the Web site that you are publishing.

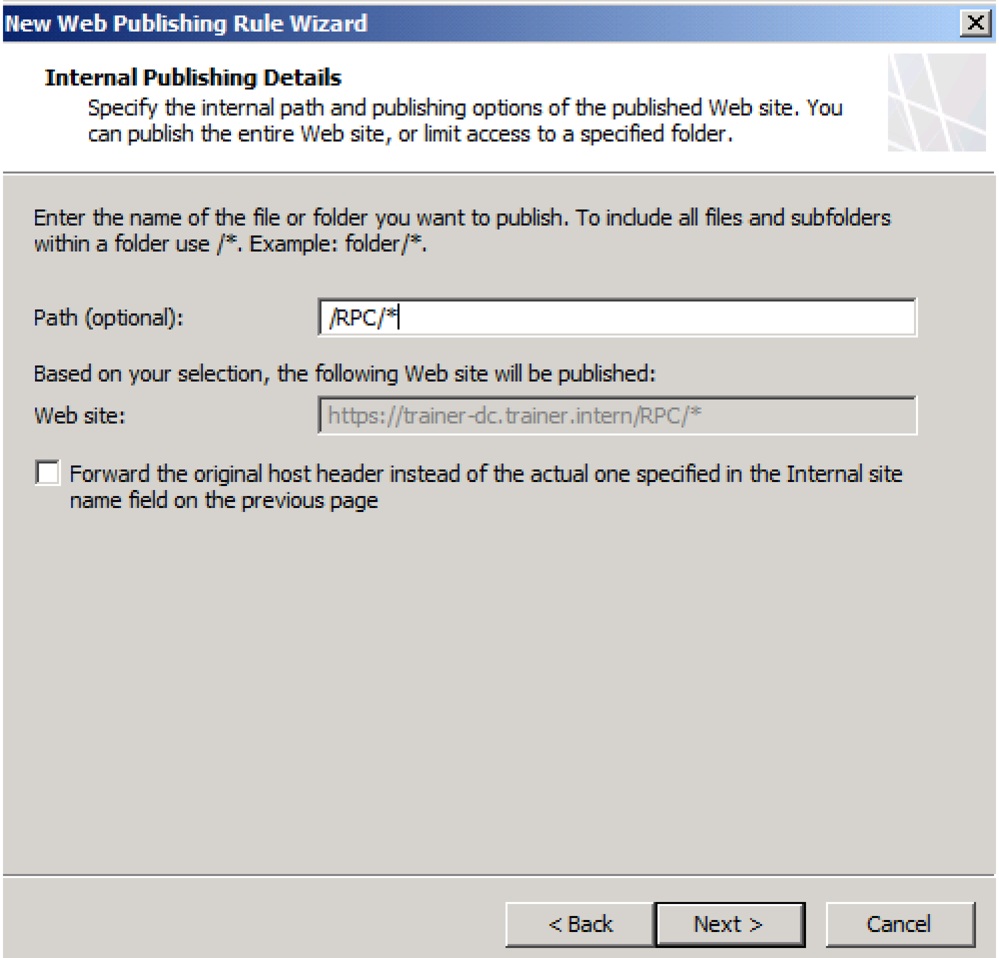
If Forefront TMG cannot resolve the internal site name, Forefront TMG can connect using the computer name or IP address of the server hosting the site.

□ Use a computer name or IP address to connect to the published server

Computer name or IP address:

Figure 3: Enter internal site name

It is possible to restrict the access from clients to specific paths, for RD Gateway access you need to allow the /RPC/* path, which is used by the RPC over HTTPS proxy service. After the wizard has finished we must modify the publishing rule to allow access to /RDWEB/* path too, which is used by the RD Web Access feature.



New Web Publishing Rule Wizard

Internal Publishing Details

Specify the internal path and publishing options of the published Web site. You can publish the entire Web site, or limit access to a specified folder.

Enter the name of the file or folder you want to publish. To include all files and subfolders within a folder use /*. Example: folder/*.

Path (optional): /RPC/*

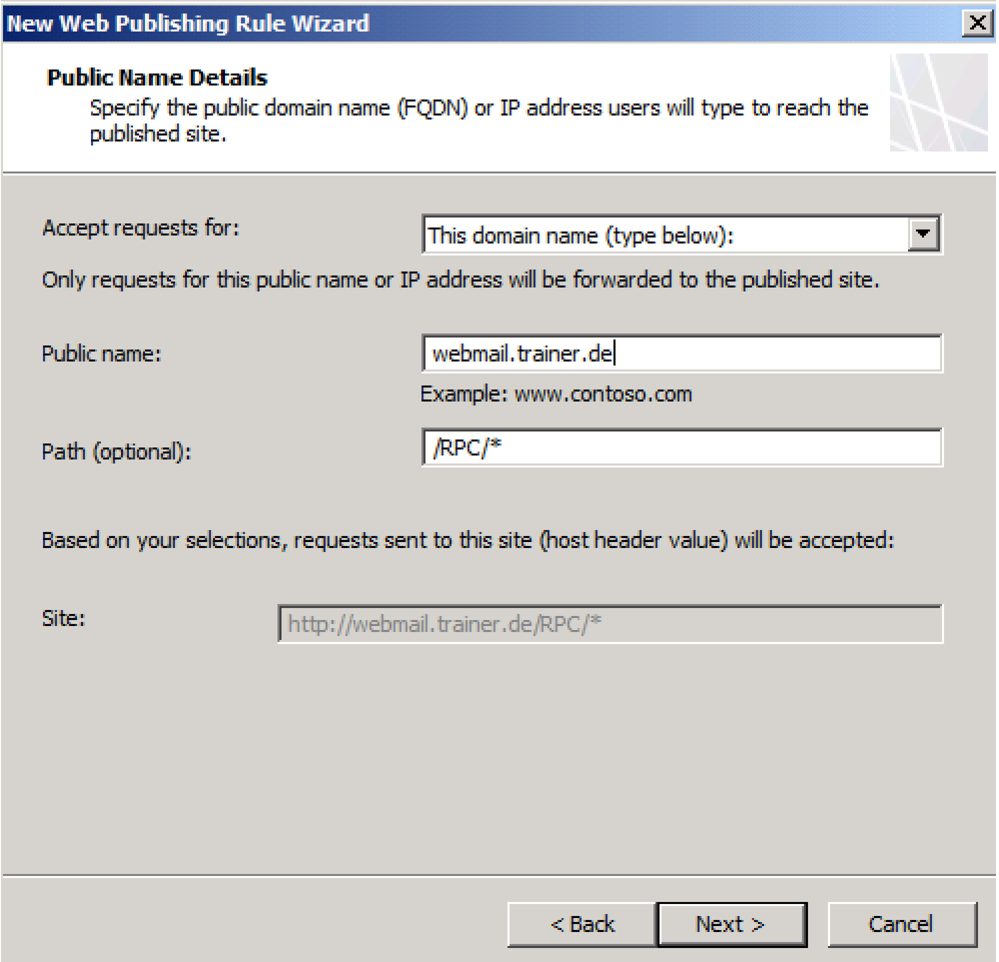
Based on your selection, the following Web site will be published:

Web site: https://trainer-dc.trainer.intern/RPC/*

□ Forward the original host header instead of the actual one specified in the Internal site name field on the previous page

Figure 4: Select the /RPC path to publish

Now we have to enter the public Hostname which we be used to access the published server from the Internet.


New Web Publishing Rule Wizard

Public Name Details

Specify the public domain name (FQDN) or IP address users will type to reach the published site.

Accept requests for: This domain name (type below):

Only requests for this public name or IP address will be forwarded to the published site.

Public name: webmail.trainer.de

Example: www.contoso.com

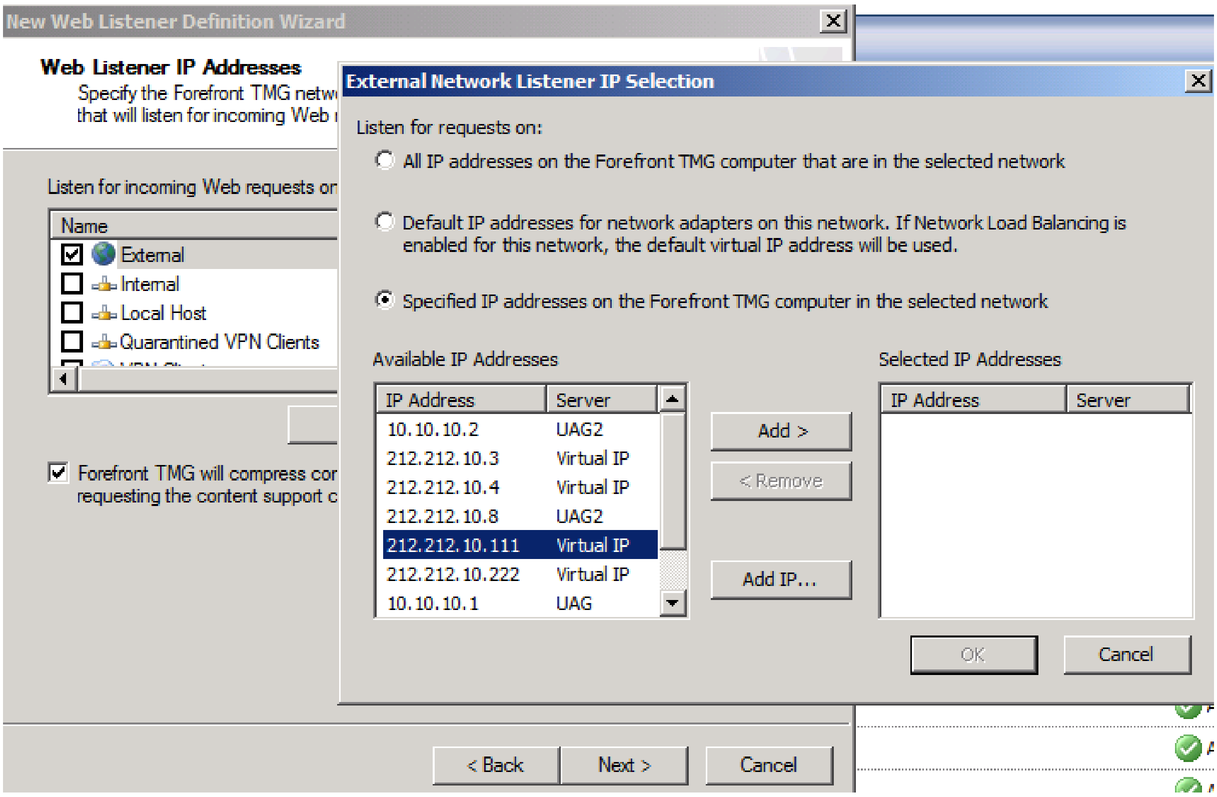
Path (optional): /RPC/*

Based on your selections, requests sent to this site (host header value) will be accepted:

Site: http://webmail.trainer.de/RPC/*

Figure 5: Enter the public Hostname

Next we have to create a new Web listener for RD access. Because we want to use SSL Bridging, select *Require SSL secured connections with clients*. If you only have one IP address bound to the external interface on Forefront TMG you doesn't need to change the Listener IP address. If you have more than one IP address bound to the external NIC interface of Forefront TMG, it is possible to select the IP address which we want to use to publish the RD server.



New Web Listener Definition Wizard

Web Listener IP Addresses

Specify the Forefront TMG netw
that will listen for incoming Web r

Listen for incoming Web requests or

Name
☑ External
□ Internal
□ Local Host
□ Quarantined VPN Clients

☑ Forefront TMG will compress cor
requesting the content support c

External Network Listener IP Selection

Listen for requests on:

○ All IP addresses on the Forefront TMG computer that are in the selected network

○ Default IP addresses for network adapters on this network. If Network Load Balancing is enabled for this network, the default virtual IP address will be used.

● Specified IP addresses on the Forefront TMG computer in the selected network

Available IP Addresses

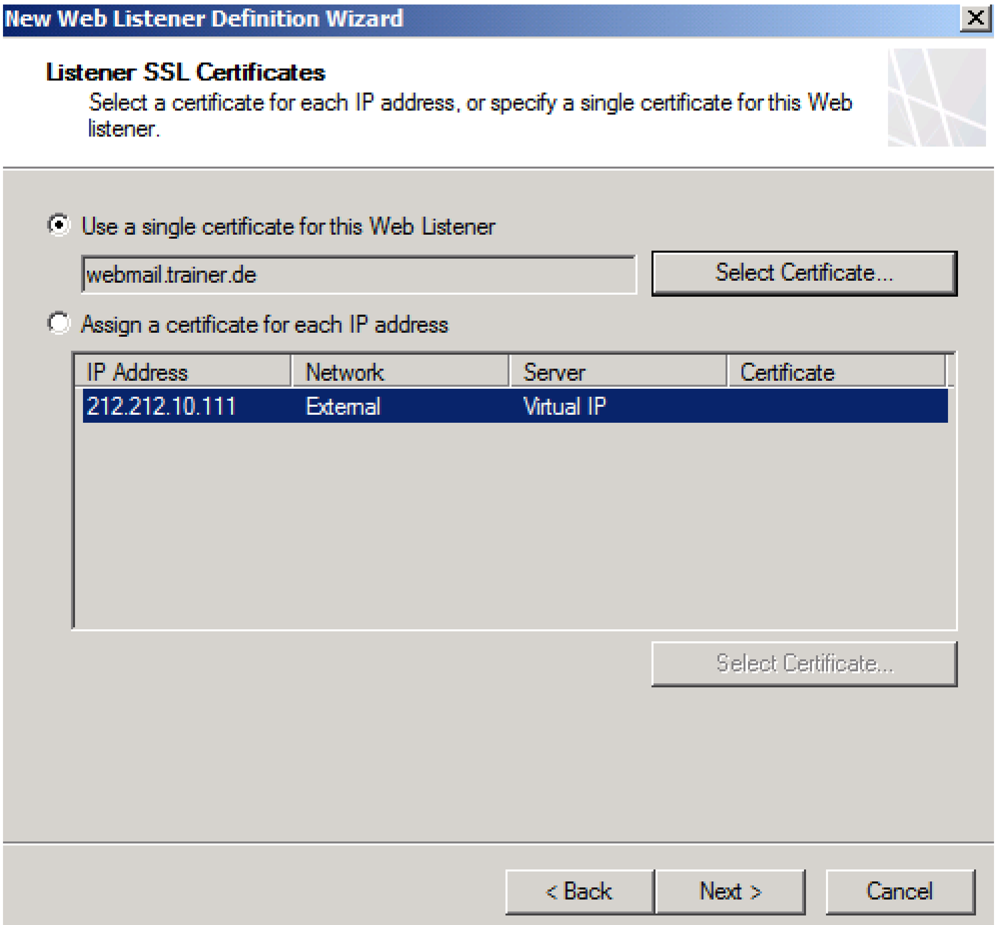
IP Address	Server
10.10.10.2	UAG2
212.212.10.3	Virtual IP
212.212.10.4	Virtual IP
212.212.10.8	UAG2
212.212.10.111	Virtual IP
212.212.10.222	Virtual IP
10.10.10.1	UAG

Selected IP Addresses

IP Address	Server

Figure 6: Select the Web listener

Now it is time to select the Certificate which will be bound to the Web listener. Select the webmail.trainer.de certificate.



New Web Listener Definition Wizard

Listener SSL Certificates

Select a certificate for each IP address, or specify a single certificate for this Web listener.

● Use a single certificate for this Web Listener

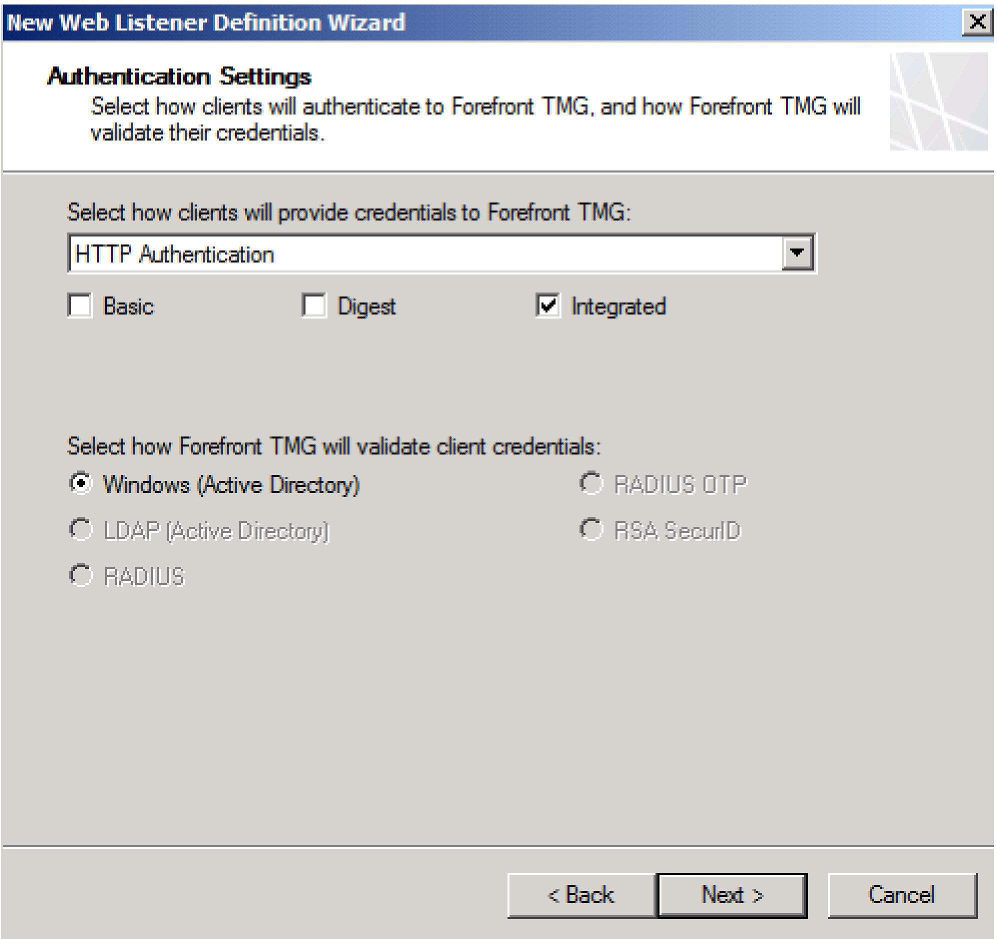
webmail.trainer.de

○ Assign a certificate for each IP address

IP Address	Network	Server	Certificate
212.212.10.111	External	Virtual IP	

Figure 7: Use the Webmail.trainer.de certificate

The Authentication method is HTTP Integrated Authentication with Active Directory.



New Web Listener Definition Wizard

Authentication Settings

Select how clients will authenticate to Forefront TMG, and how Forefront TMG will validate their credentials.

Select how clients will provide credentials to Forefront TMG:

HTTP Authentication

□ Basic □ Digest ☑ Integrated

Select how Forefront TMG will validate client credentials:

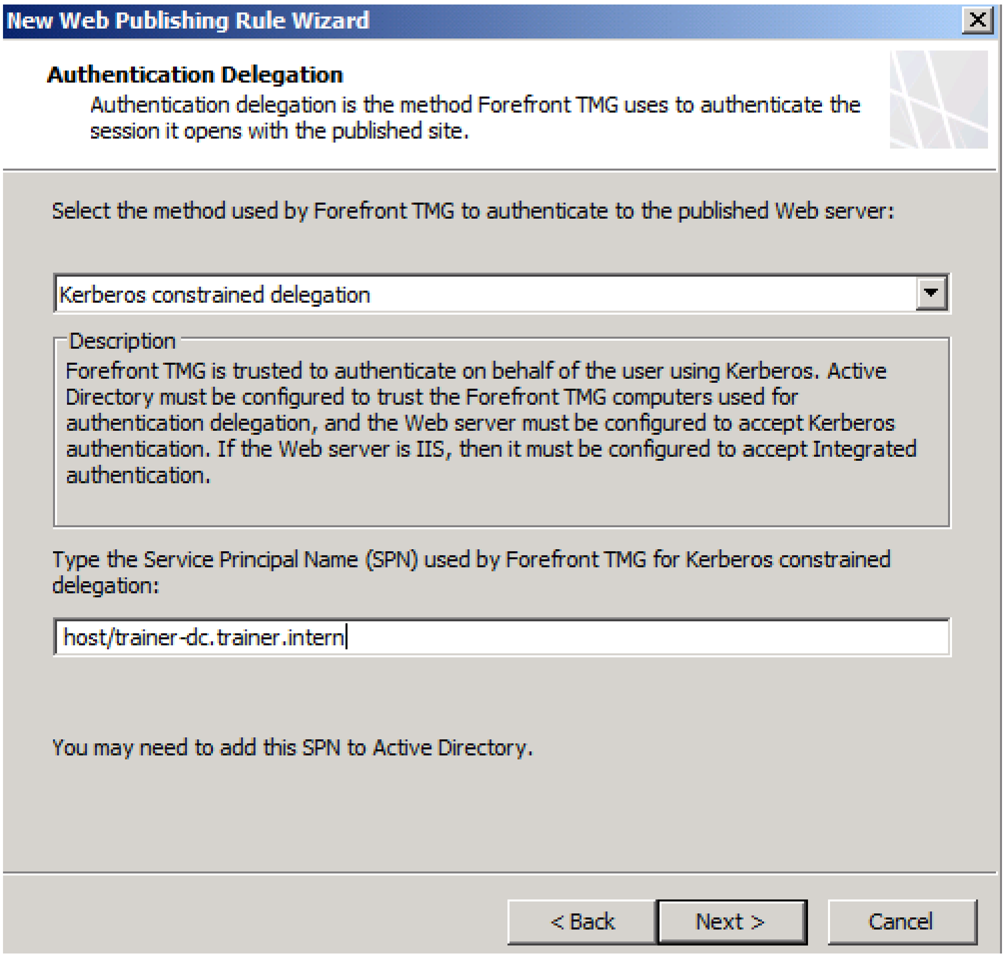
● Windows (Active Directory) ○ RADIUS OTP

○ LDAP (Active Directory) ○ RSA SecurID

○ RADIUS

Figure 8: Select HTTP as the authentication method

The Authentication delegation method is Kerberos constrained delegation (KCD). We also have to enter the correct Service Principal Name (SPN). The SPN for this lab environment is HOST/trainer-dc.trainer.intern.



Authentication Delegation

Authentication delegation is the method Forefront TMG uses to authenticate the session it opens with the published site.

Select the method used by Forefront TMG to authenticate to the published Web server:

Kerberos constrained delegation

Description

Forefront TMG is trusted to authenticate on behalf of the user using Kerberos. Active Directory must be configured to trust the Forefront TMG computers used for authentication delegation, and the Web server must be configured to accept Kerberos authentication. If the Web server is IIS, then it must be configured to accept Integrated authentication.

Type the Service Principal Name (SPN) used by Forefront TMG for Kerberos constrained delegation:

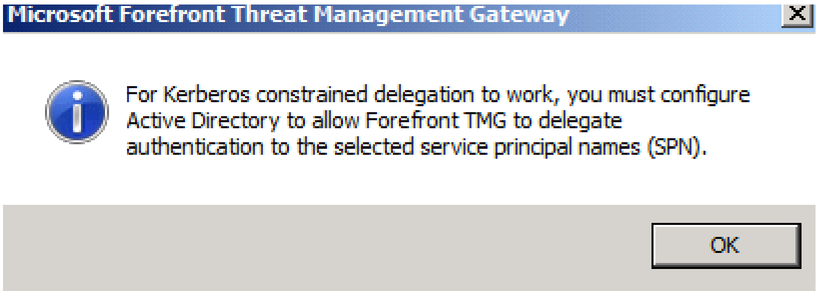
host/trainer-dc.trainer.intern

You may need to add this SPN to Active Directory.

Figure 9: Select KCD and enter the SPN

The rule applies to *All authenticated users.*

Click *Finish*. You will see an additional information message that you have to configure the TMG Server to allow for delegation against the RD server.



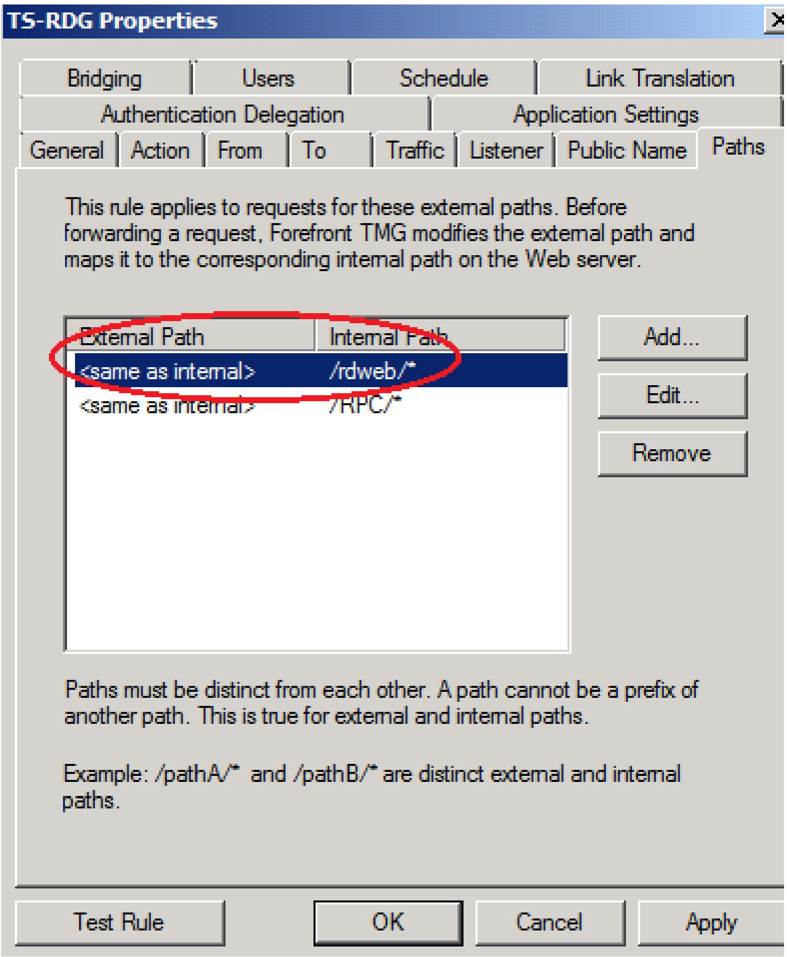
For Kerberos constrained delegation to work, you must configure Active Directory to allow Forefront TMG to delegate authentication to the selected service principal names (SPN).

^

Figure 10: Information message for additional KCD configuration

Click *Apply.*

After the configuration changes has been applied, we have to modify the publishing rule to allow access to the additional /RDWEB/* path which is used by the RD Web Access feature.



This rule applies to requests for these external paths. Before forwarding a request, Forefront TMG modifies the external path and maps it to the corresponding internal path on the Web server.

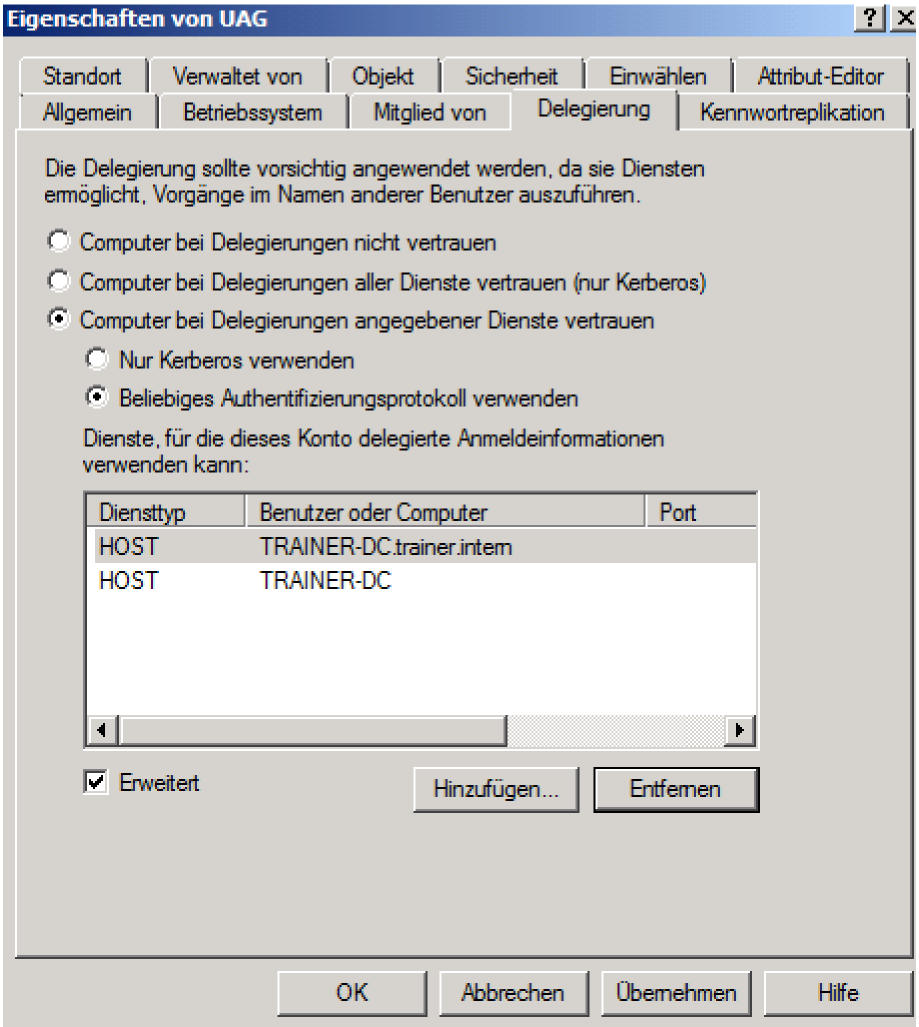
External Path	Internal Path
<same as internal>	/rdweb/*
<same as internal>	/RPC/*

Paths must be distinct from each other. A path cannot be a prefix of another path. This is true for external and internal paths.

Example: /pathA/* and /pathB/* are distinct external and internal paths.

Figure 11: Add the /RDWEB path as an additional allowed path

As a final step we must configure the Trust for Delegation settings. Open the Active Directory Computer and Users Snap In on a Domain Controller and navigate to the Computer account of the Forefront TMG Server, and select the delegation tab, select Advanced and choose the Server with the RD services and select Host as the service type.



Die Delegierung sollte vorsichtig angewendet werden, da sie Diensten ermöglicht, Vorgänge im Namen anderer Benutzer auszuführen.

○ Computer bei Delegierungen nicht vertrauen

○ Computer bei Delegierungen aller Dienste vertrauen (nur Kerberos)

● Computer bei Delegierungen angegebener Dienste vertrauen

○ Nur Kerberos verwenden

● Beliebiges Authentifizierungsprotokoll verwenden

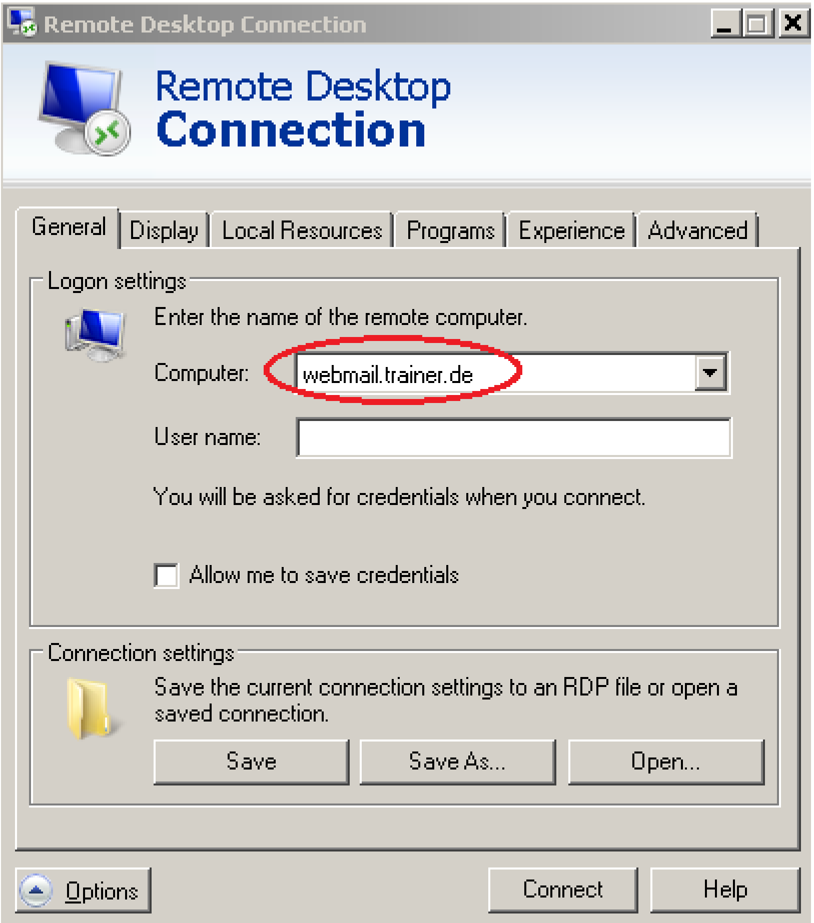
Dienste, für die dieses Konto delegierte Anmeldeinformationen verwenden kann:

Diensttyp	Benutzer oder Computer	Port
HOST	TRAINER-DC.trainer.intern	
HOST	TRAINER-DC	

☑ Erweitert

Figure 12: Trust the RD Gateway for Kerberos Delegation

The configuration of Forefront TMG has been finished so we can now configure the Windows 7 client in the Internet to get RD Gateway and RD Web Access.
Start the Remote Desktop connection utility (MSTSC.EXE) and enter the published public host name as the name of the computer where you want to connect to.



Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: webmail.trainer.de

User name:

You will be asked for credentials when you connect.

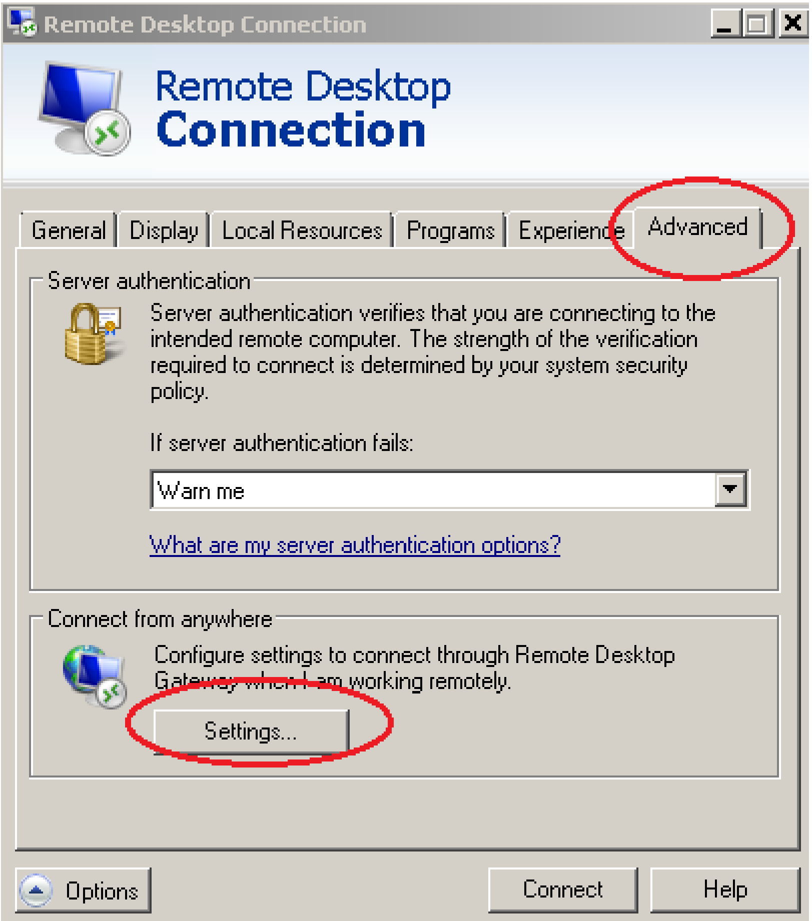
□ Allow me to save credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

Figure 13: Connect to the public hostname

Next click *Advanced* and *settings* in the connect from anywhere section.



Server authentication verifies that you are connecting to the intended remote computer. The strength of the verification required to connect is determined by your system security policy.

If server authentication fails:

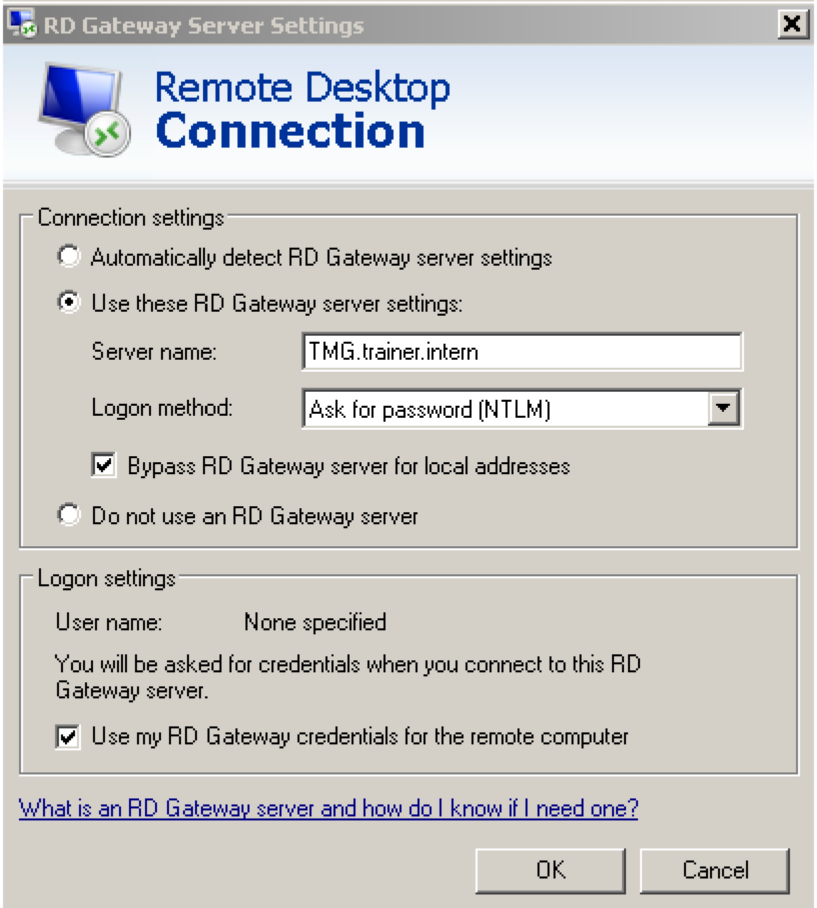
Warn me

What are my server authentication options?

Configure settings to connect through Remote Desktop Gateway when I am working remotely.

Figure 14: Connect from anywhere

Manually specify the RD Gateway settings and as the RD Gateway Server enter the name of the internal Server with the RD Gateway role installed. Be sure that the checkbox *Bypass RD Gateway Server for local access* is checked.



Connection settings

○ Automatically detect RD Gateway server settings

● Use these RD Gateway server settings:

Server name: TMG.trainer.intern

Logon method: Ask for password (NTLM)

☑ Bypass RD Gateway server for local addresses

○ Do not use an RD Gateway server

Logon settings

User name: None specified

You will be asked for credentials when you connect to this RD Gateway server.

☑ Use my RD Gateway credentials for the remote computer

What is an RD Gateway server and how do I know if I need one?

Figure 15: Enter the RD Gateway INTERNAL Server name

Now try to make a connection to the RD Gateway Server. If your connection is successful you should see an additional icon in the Remote Desktop console which indicates that you are connect through the RD Gateway service.

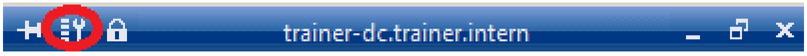
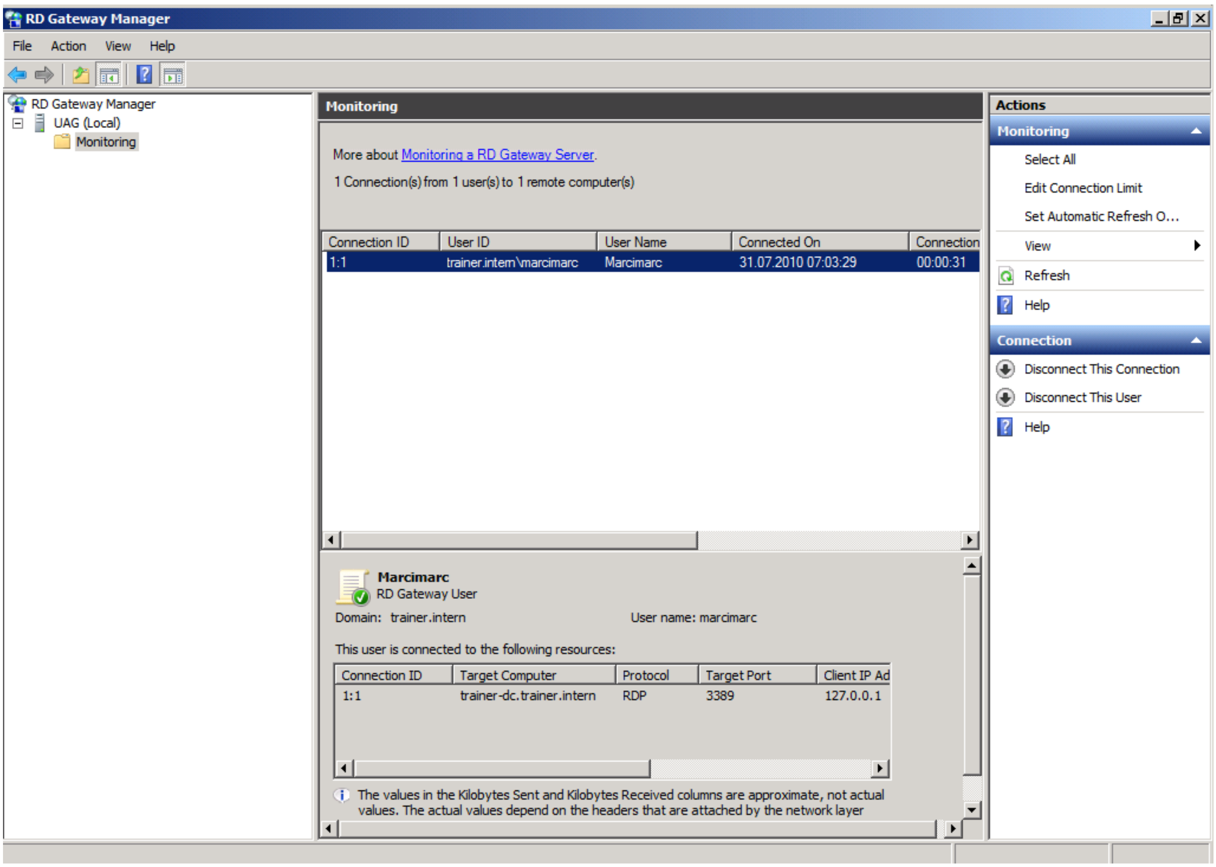


Figure 15: Connected via HTTPS with the RD Gateway service

If you are the Administrator of the RD Gateway server you can also monitor the connections from clients to the RD Gateway with the RD Gateway Manager console under the Monitoring node as you can see in the following picture.



Monitoring

More about Monitoring a RD Gateway Server.

1 Connection(s) from 1 user(s) to 1 remote computer(s)

Connection ID	User ID	User Name	Connected On	Connection
1:1	trainer.intern\marcimarc	Marcimarc	31.07.2010 07:03:29	00:00:31

Marcimarc
RD Gateway User

Domain: trainer.intern User name: marcimarc

This user is connected to the following resources:

Connection ID	Target Computer	Protocol	Target Port	Client IP Ad
1:1	trainer-dc.trainer.intern	RDP	3389	127.0.0.1

The values in the Kilobytes Sent and Kilobytes Received columns are approximate, not actual values. The actual values depend on the headers that are attached by the network layer

Figure 16: Monitoring the connection with the RD Gateway manager

Now try to open the Website https://webmail.trainer.de/rdweb from the Windows 7 client and you should also get access to the RD Web Access feature after a successful authentication. Depending on the RD Web Access and RD RemoteApp settings you can now access application over the web interface which will be tunneled through the RD Gateway service.

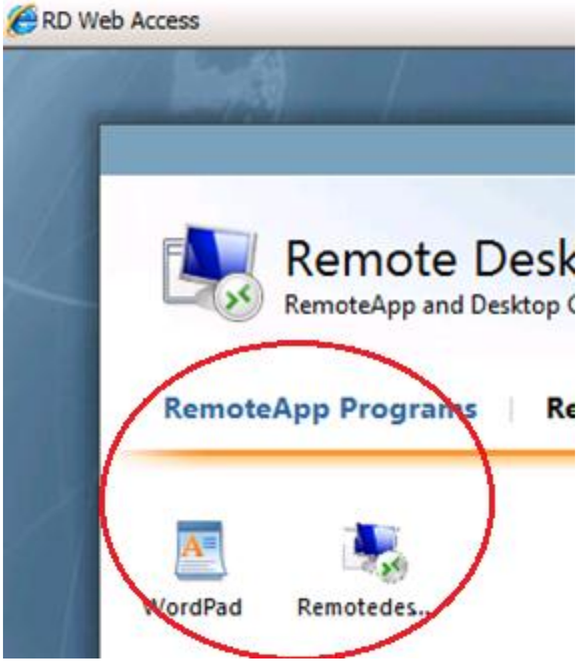


Figure 17: RD Web Access over the Internet

Conclusion

In this article I showed you how to publish the RD Gateway service and the RD Web Access feature with the help of Microsoft Forefront TMG and I also showed you how to access the RD Gateway service with the Remote Desktop client connection and how to access the RD Web Access feature with the client web browser.

Related links

Deploying Remote Desktop Gateway Step-by-Step Guide
http://www.microsoft.com/downloads/details.aspx?FamilyID=6d146124-e850-4cec-9efa-33a5225e155d&DisplayLang=en
Microsoft Forefront UAG – Overview of Microsoft Forefront UAG
http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html
Remote Desktop Web Access (RD Web Access)
http://technet.microsoft.com/en-us/library/cc731923.aspx
Enhance TS Gateway Security with ISA Server 2006
http://technet.microsoft.com/en-us/magazine/2008.09.tsg.aspx
W2K8-R2-Remotedesktopgateway + Web Access Publish (German article)
http://blog.forefront-tmg.de/?p=248