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

Configuring a PPTP Site to Site VPN with Microsoft Forefront TMG

Abstract

In this article, I will show you how to create a PPTP Site to Site VPN between two Microsoft Forefront TMG servers.

Let's begin

First, keep in mind that the information in this article are based on a beta version of Microsoft Forefront TMG and are subject to change.

A few weeks ago, Microsoft released Beta 3 of Microsoft Forefront TMG (Threat Management Gateway), which has a lot of new exiting features.

Microsoft Forefront TMG, like ISA Server 2006 has built-in Client and Site to Site VPN capabilities. Site to Site VPN can be established with the following protocols:

- IPSEC
- L2TP over IPSEC
- PPTP

The configuration of these Site to Site VPN configurations remains nearly unchanged in TMG comparing with ISA Server 2006. One of the new VPN client functionalities in TMG is support for SSTP (Secure Socket Tunneling Protocol) VPN but this new functionality is out of the scope of this article.

Let's start with the Site to Site VPN configuration. Start the TMG Management console and navigate to the Remote Access Policy (VPN) node and in the task pane click Create VPN Site-to-Site connection. This will start the wizard to create a VPN Remote Site.

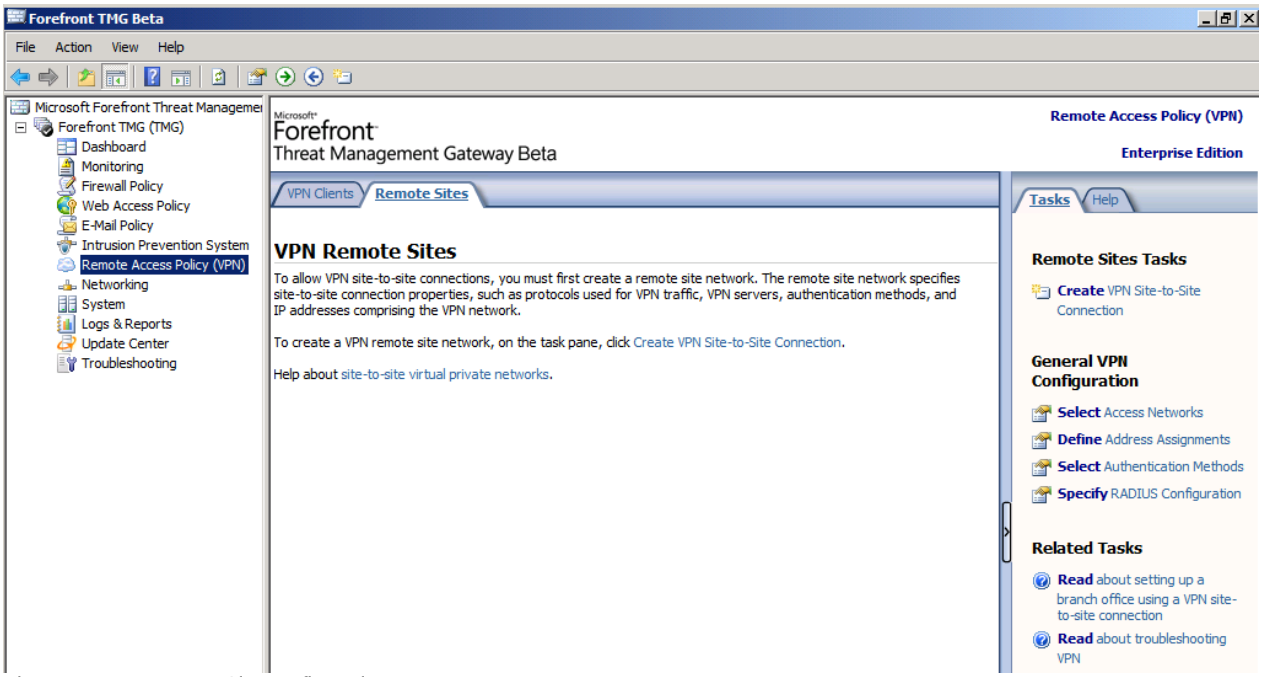

Figure 1: VPN Remote Site configuration

Follow the instructions of the VPN Site-to-Site Connection Wizard and specify the Site-to-Site network name.

Figure 2: Site-to-Site network name

Select the VPN Protocol. For the example in this article we will use the Point-to-Point Tunneling Protocol (PPTP).

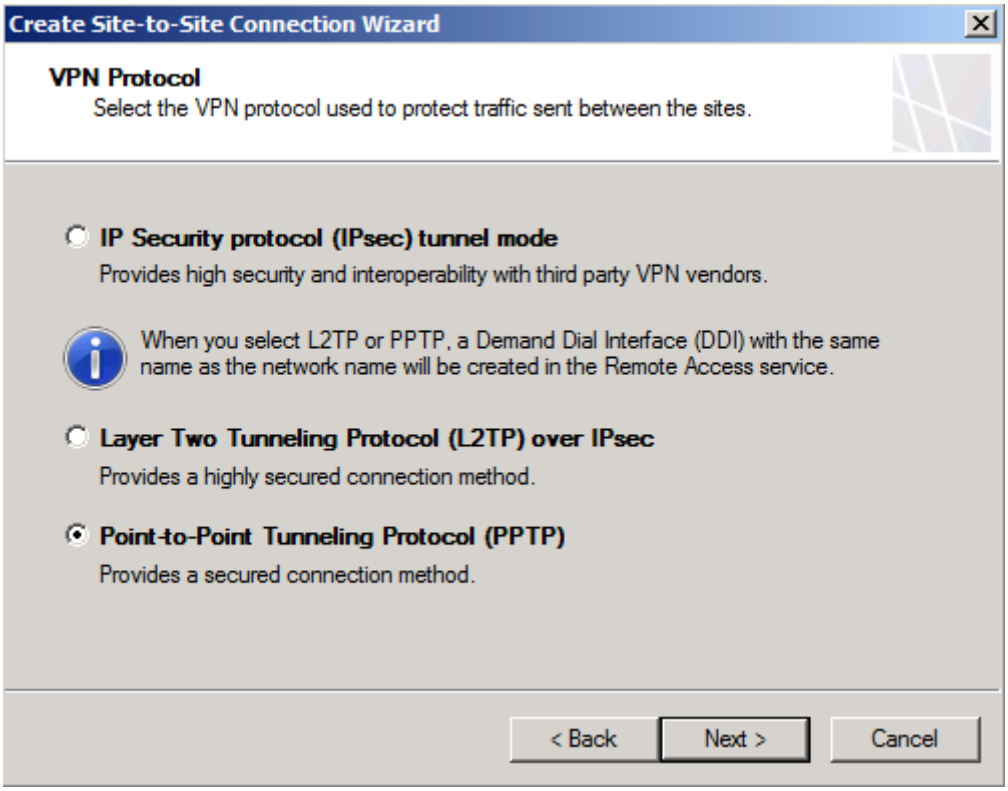

Figure 3: Select VPN-Protocol

After selecting the PPTP protocol, a reminder opens and displays a warning, that you must create a user account for the Site-to-Site VPN that must match the name of the Site-to-Site VPN network. If this user account name doesn't match the name of the Site-to-Site VPN network name, a missconfiguration occurs or only a client VPN connection will be established.

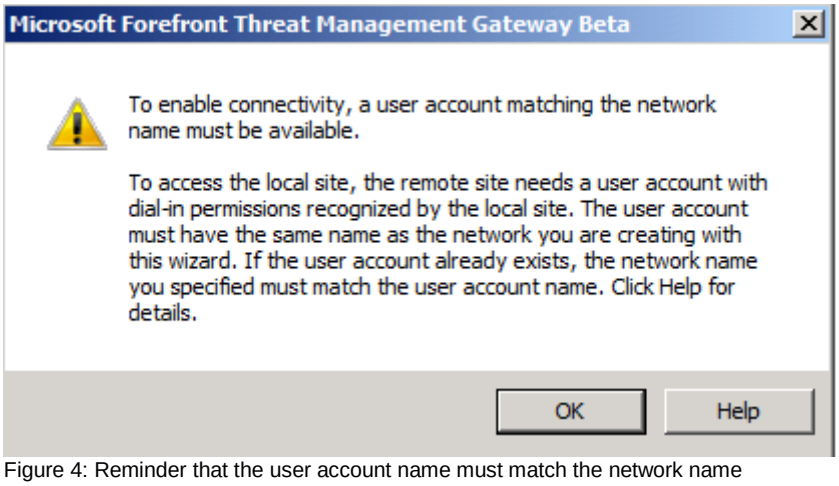

Figure 4: Reminder that the user account name must match the network name

Let us now create the user account used for the Site-to-Site VPN on the other TMG server. We will name the user account Hannover, like the Site-to-Site VPN network name. Activate the checkboxes that the password never expires and the user cannot change the password. You should assign a strong password for this user account.

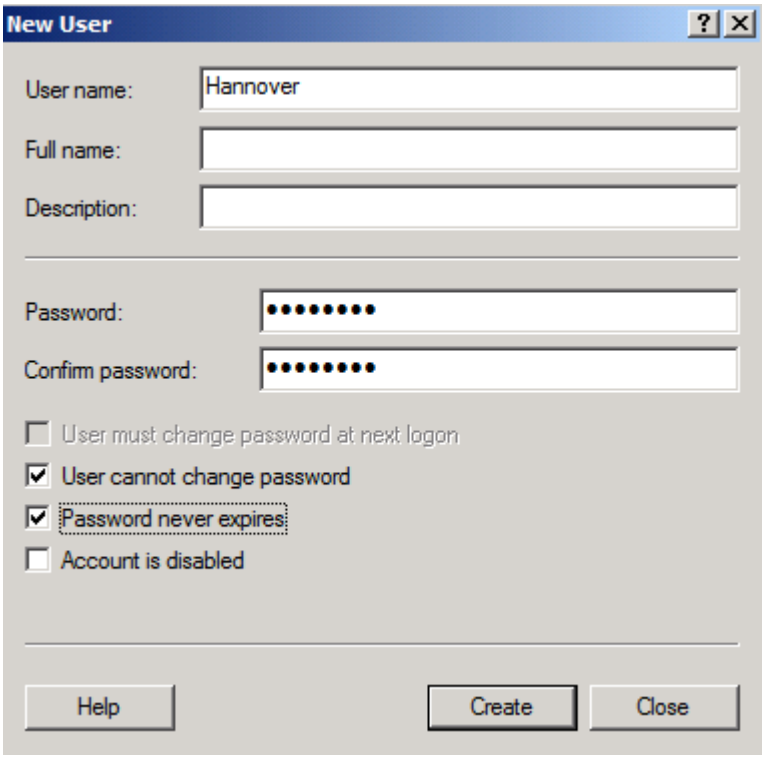

Figure 5: Remote VPN account

Next, you must allow Network access permissons for the Site-to-Site VPN account.

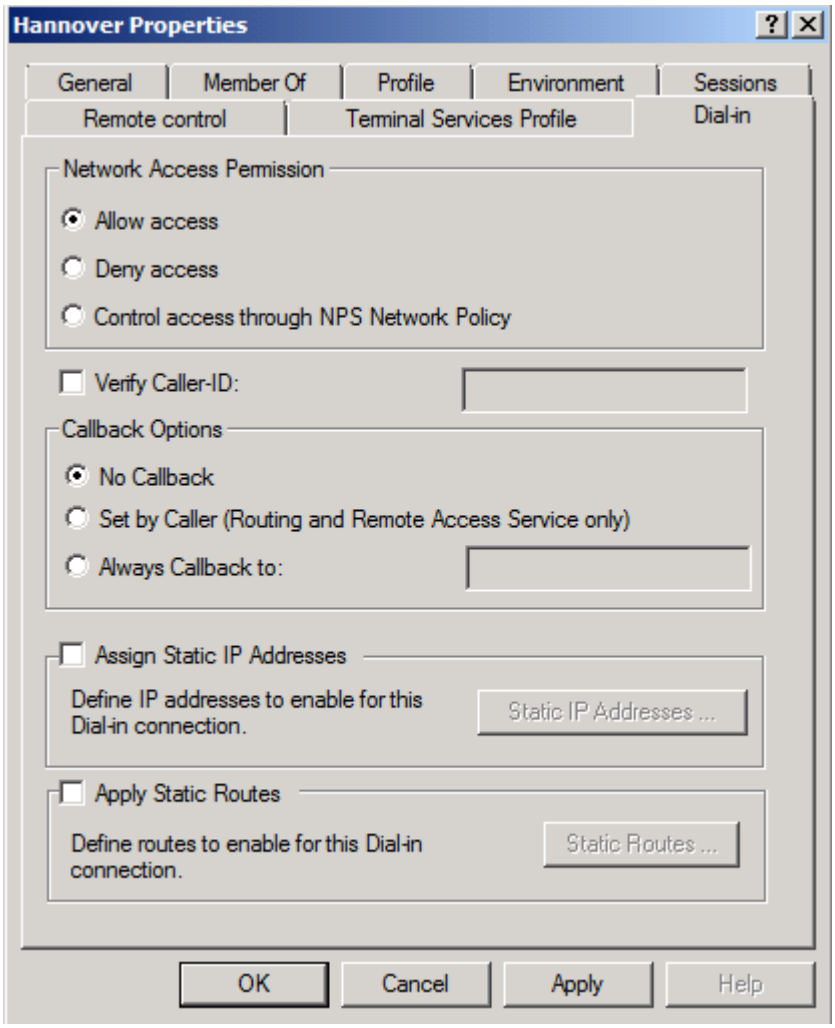

Figure 6: Allow network access permission

As a next configuration step we have to selct the IP address assignment method for the remote VPN client connection from the other site of the Site-to-Site VPN. It is possible to use DHCP or IP addreses from a static IP address pool.

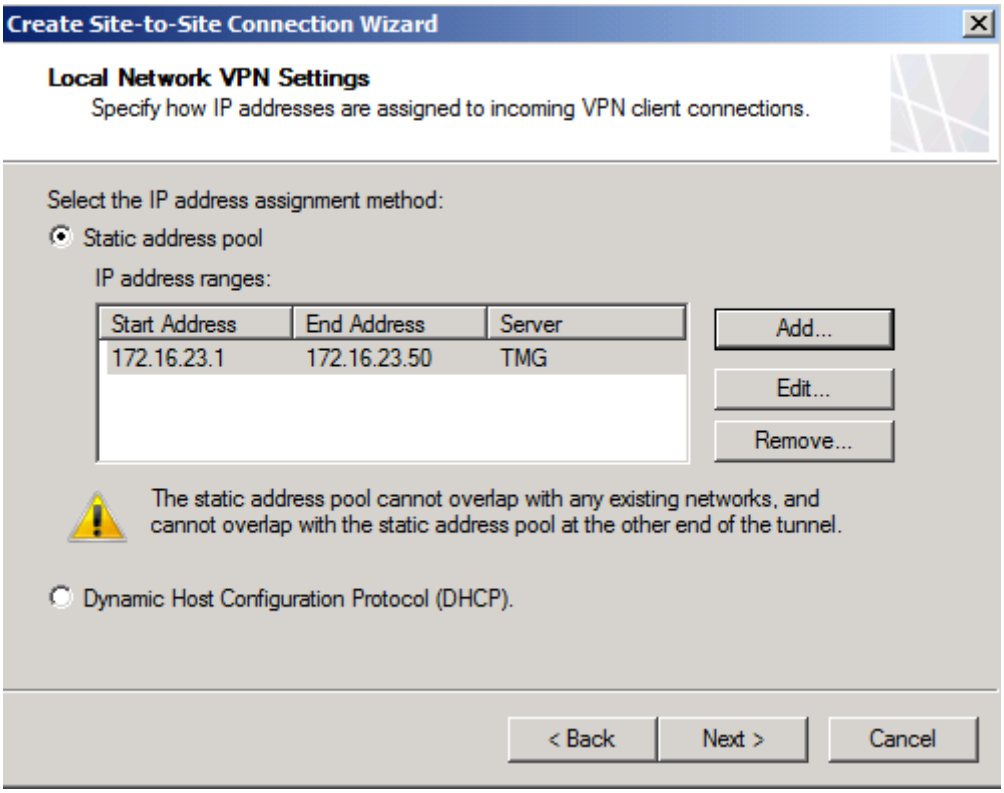

Figure 7: Specify IP address range

If you are using Microsoft Forefront TMG Enterprise, you have to specify the connection owner when Network Load Balancing is not used – which is true in our example. If NLB is used, the connection owner will be automatically assigned.

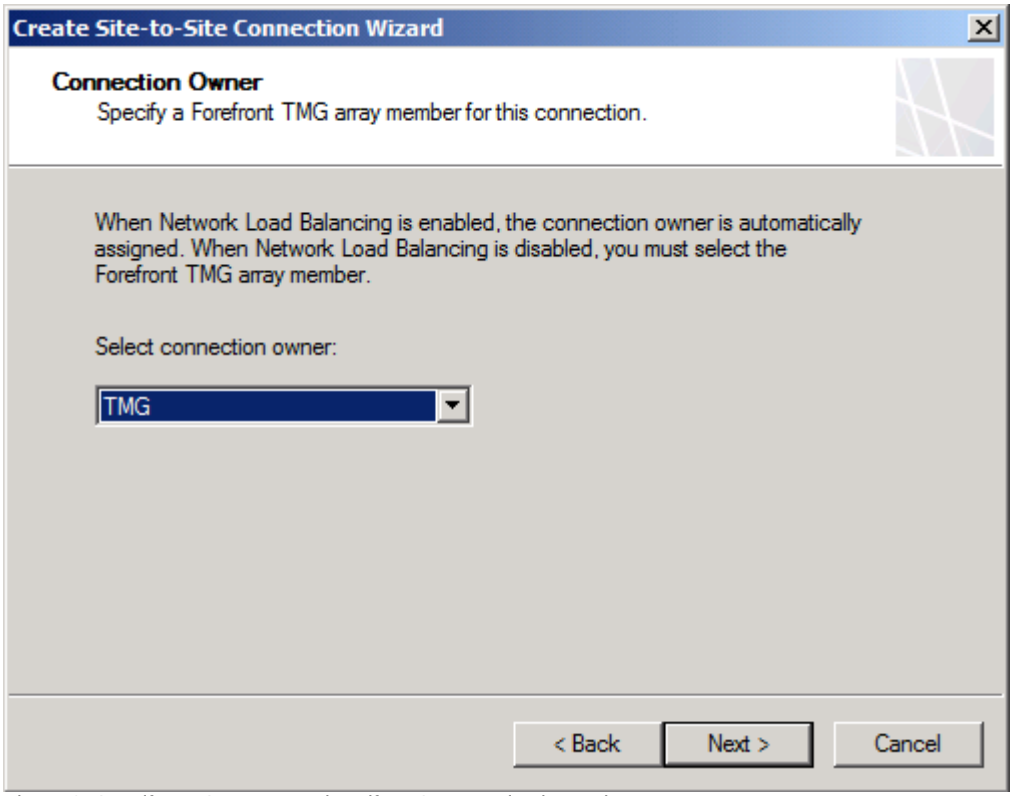

Figure 8: Specify TMG array member, if TMG Enterprise is used

Specify the IP address or FQDN (Fully Qualified Domain Name) of the remote site VPN Server.

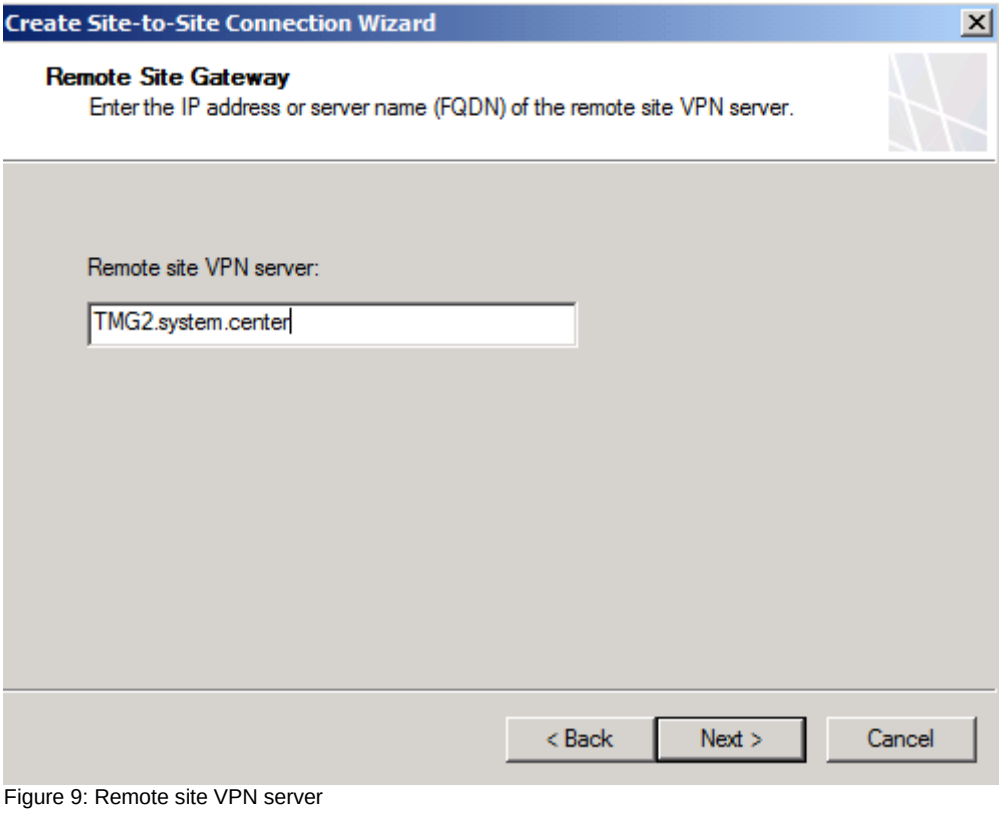

Figure 9: Remote site VPN server

Specify the remote site user account which is used for the Site-to-Site connection. This account is used to establish a connection to the remote site.

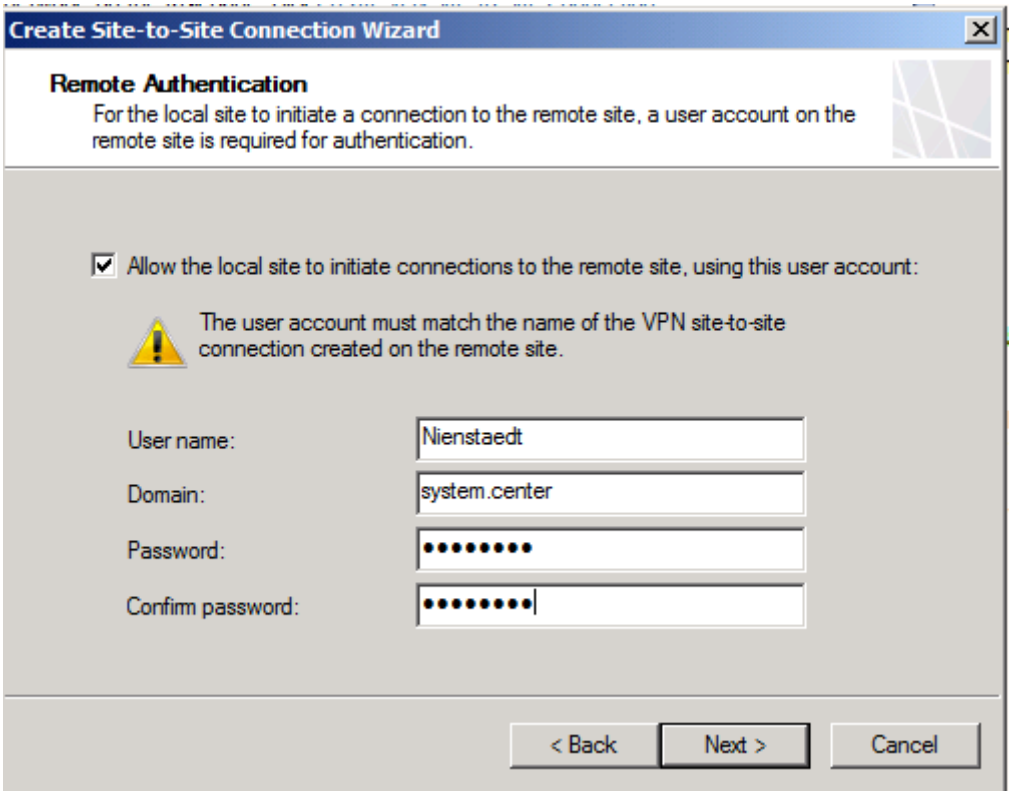

Figure 10: Remote Authentication

TMG Server must know the IP address ranges of the remote site networks to which TMG will connect. You have to specify all IP address ranges of the remote sites.

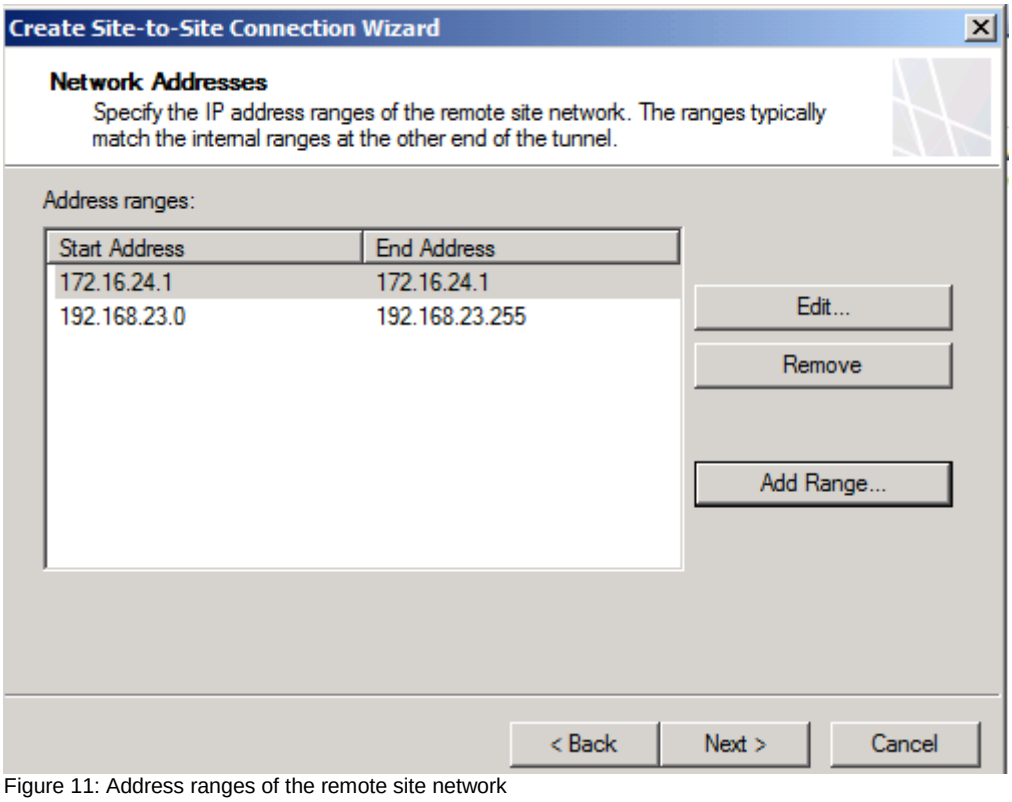

Figure 11: Address ranges of the remote site network

If you are using NLB for connecting the remote Sites, you have to specify the DIP (Dedicated IP address) of the remote site Gateway. In our example, we doesn't use NLB, so the option remains unchecked.

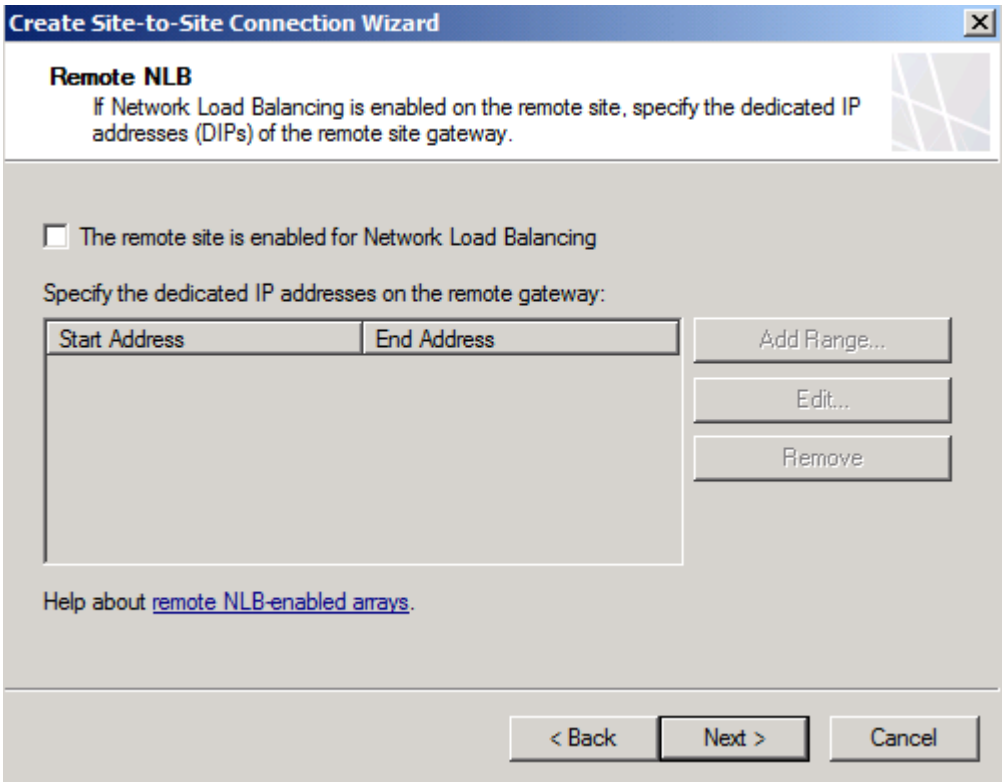

Figure 12: Configuration of Remote site NLB, when used

A Site-to-Site VPN connection requires a network rule which connects both sites of the Site-to-Site VPN. The wizard automatically creates a Network rule with a Route relationship. It is possible to change the network rule after the wizard has finished.

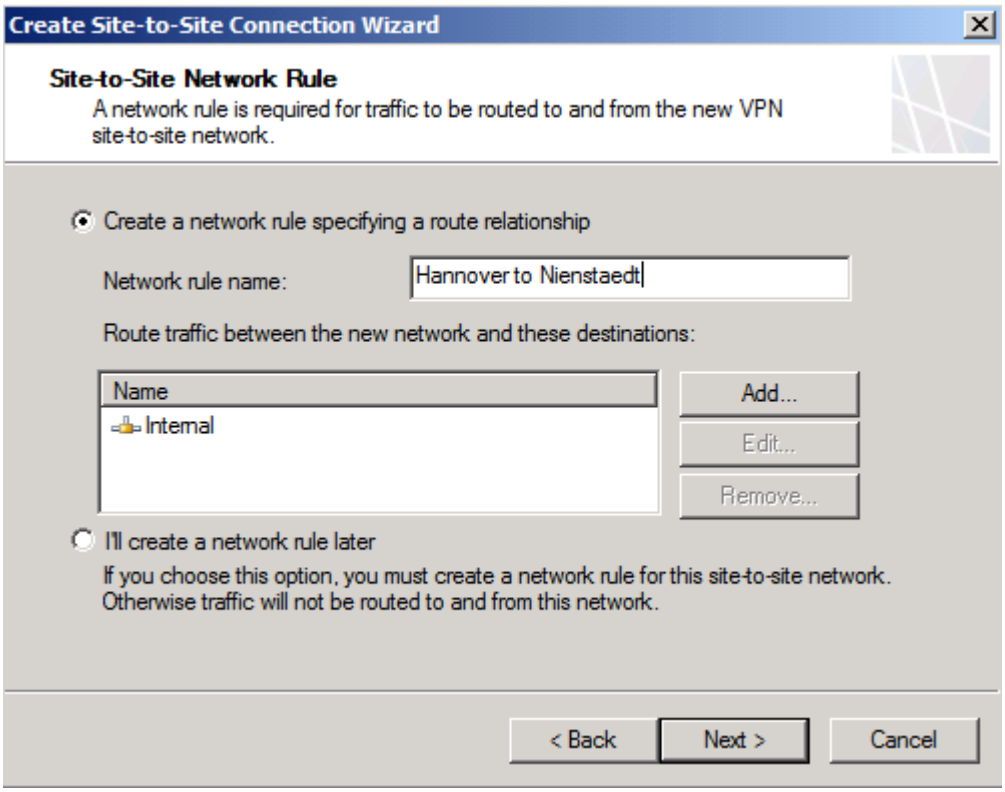

Figure 13: Site-to-Site network rule

The Site-to-Site VPN Wizard also automatically creates a network access rule between the two sites. You have to specify the allowed protocols through the Site-to-

Site network. As a best practice you should only allow a mimimum of required protocols.

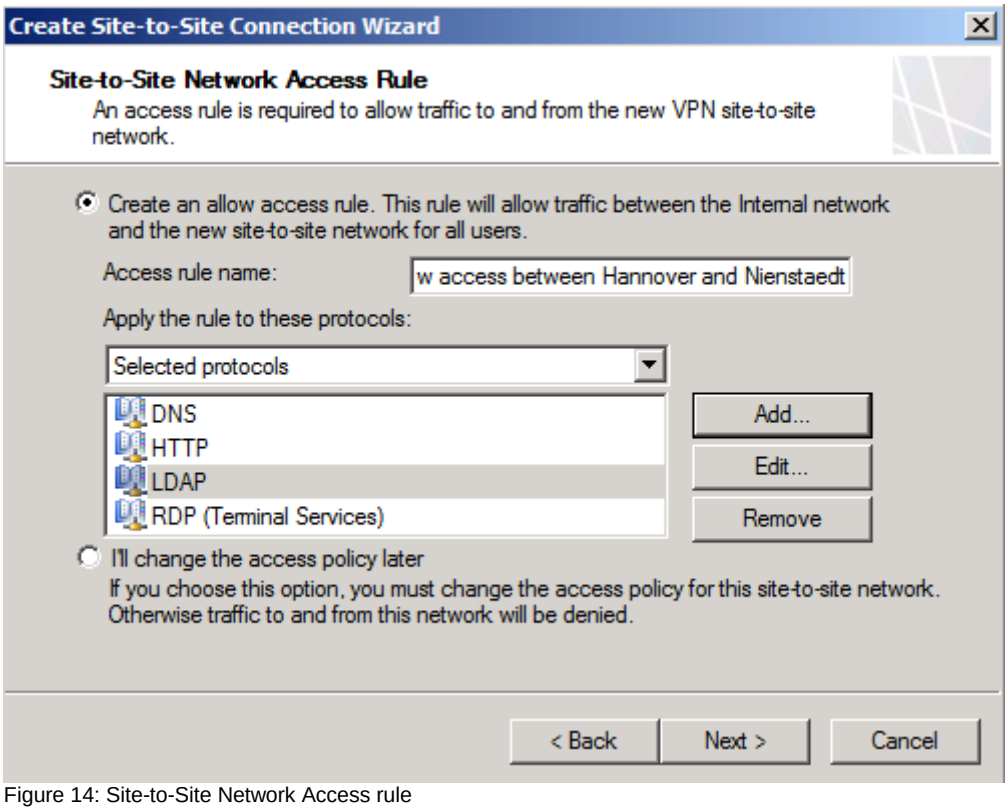

Figure 14: Site-to-Site Network Access rule

The wizard has collected all necessary informations for creating the Site-to-Site VPN. Give the configuration a review and after that click Finish.

Figure 15: Completing the new VPN Site-to-Site Network Wizard

A reminder opens that you must create a local user account for the Site-to-Site VPN connection, so that the other site of the VPN connection can use the Site-to-Site VPN.

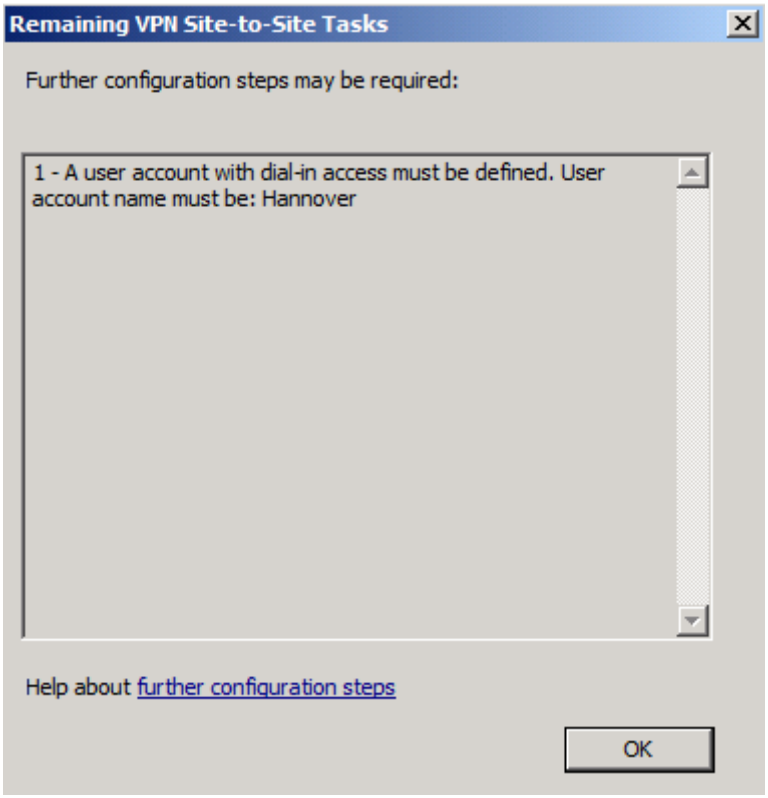

Figure 16: Reminder for more necessary configuration steps

Click Apply.

The Site-to-Site VPN has now sucessfully created. It is possible to change the Site-to-Site VPN properties. Rightclick the VPN connection and click properties. One of the things you should pay attention is the connection timeout for inactive connections on the Connection tab.

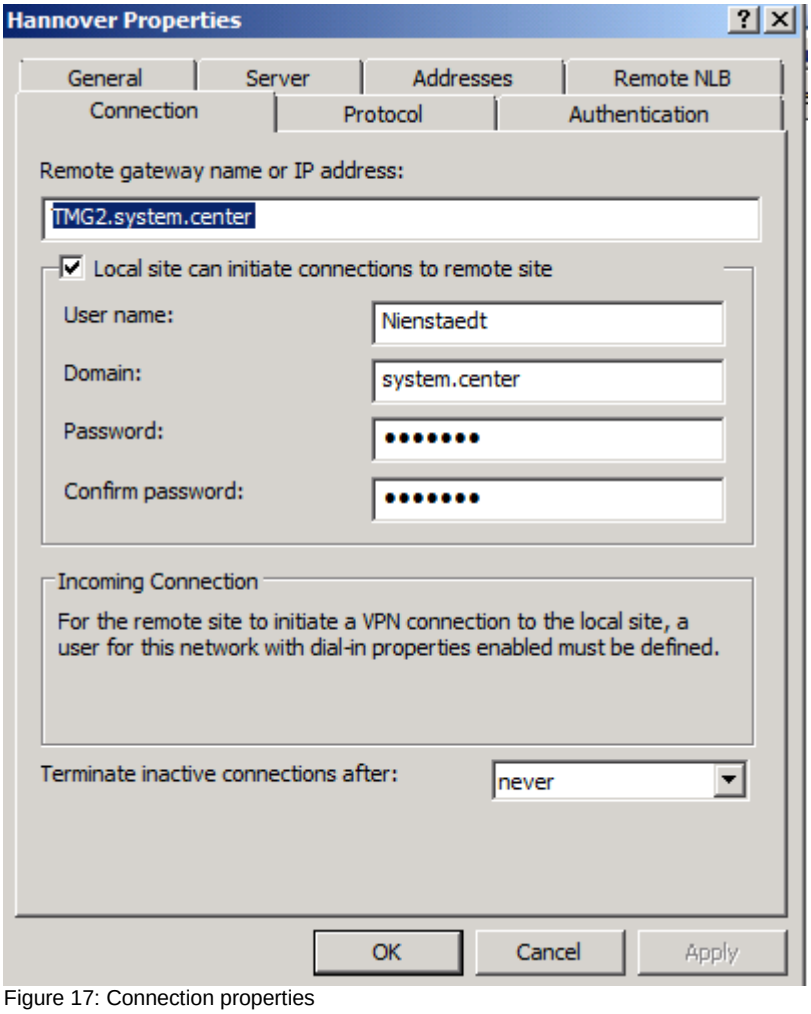

Figure 17: Connection properties

The Authentication tab allows you to select the authentication protocols. MS-CHAP v2 is the default authentication protocol and you should only change the protocol if it is absolutly necessary (and it shouldn't be necessary), because all other protocols are not so secure as the MS-CHAP v2 protocol.

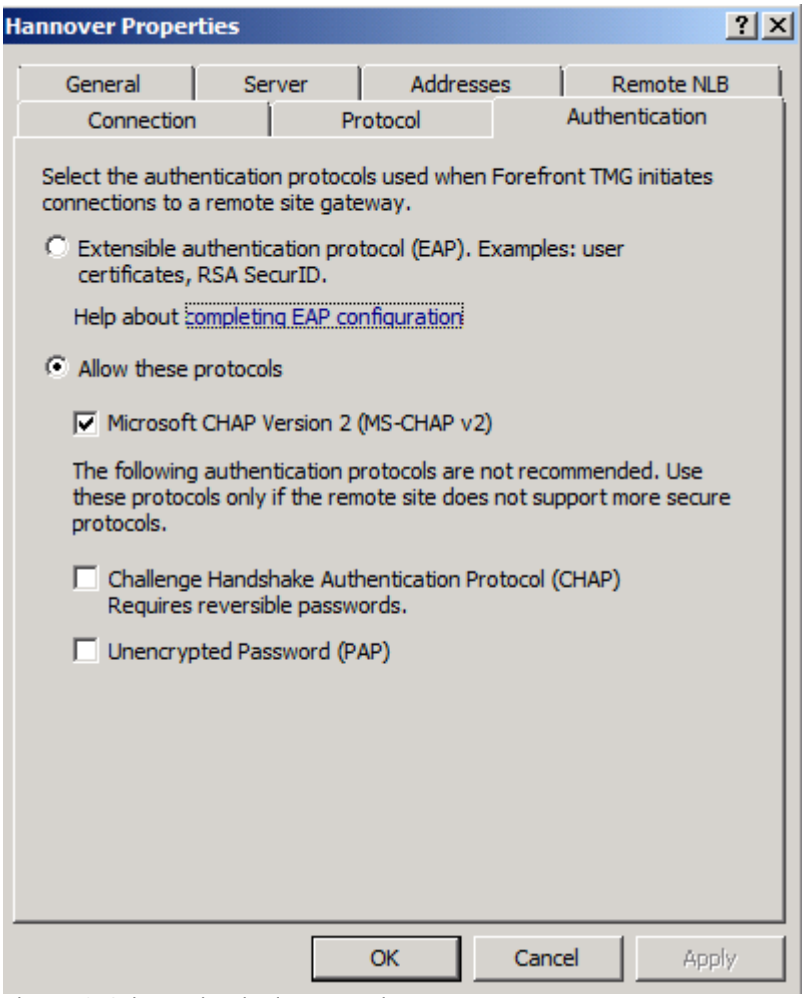

Figure 18: Select authentication protocols

If you would like to have an overview about the Site-to-Site VPN configuration, right click the Site-to-Site rule and click Site-to-Site Summary as you can see in the following screenshot.

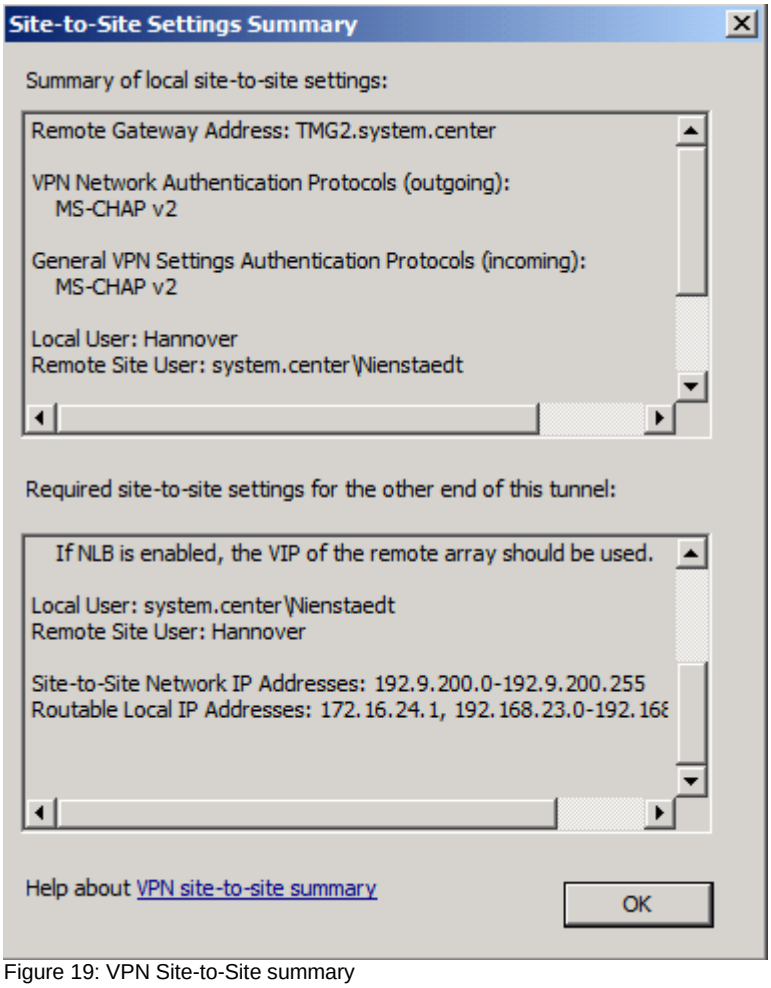

Figure 19: VPN Site-to-Site summary

Next, you should review the Firewall rule, created by the Site-to-Site VPN wizard. Because I used the HTTP protocol in the Site-to-Site VPN firewall rule, you will find the rule under the Web Access Policy node.

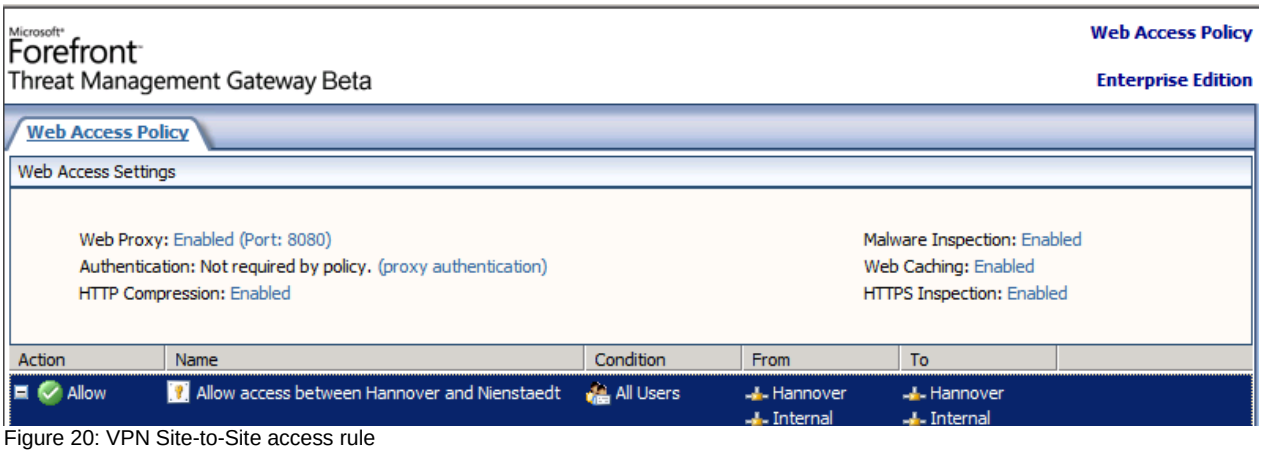

Figure 20: VPN Site-to-Site access rule

As a last step, you should check the network rule, created by the Site-to-Site VPN wizard. You will find the network rule in the TMG Management console under the Networking node in the network rule tab.

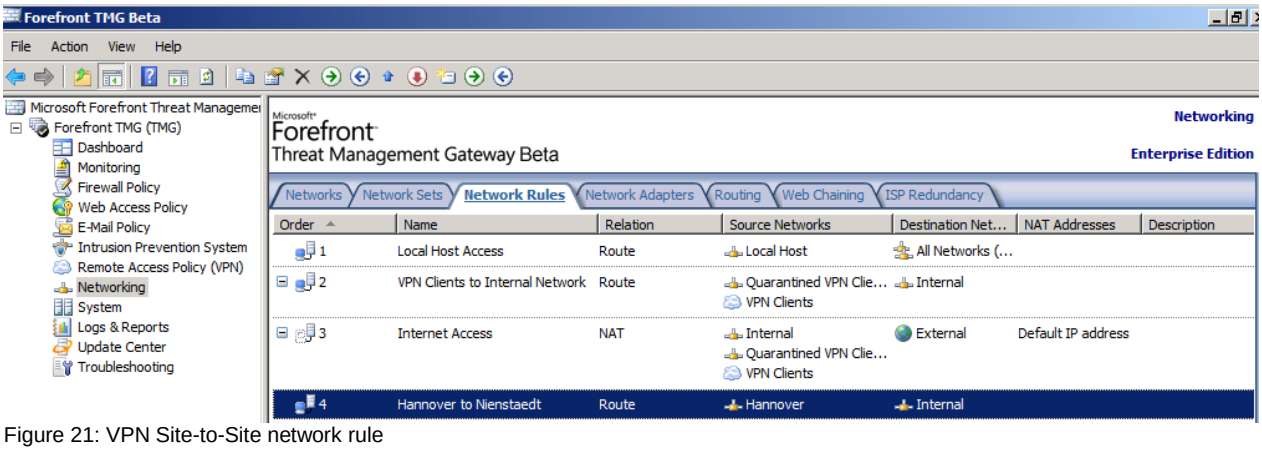

Figure 21: VPN Site-to-Site network rule

We have successfully configured the Site-to-Site VPN configuration on one TMG site. You now have to configure the TMG Server on the other site of the Site-to-Site VPN.

Conclusion

In this article, I gave you an overview about how to create a PPTP Site to Site VPN with Microsoft Forefront Threat Management Gateway. The process is nearly the same as in ISA Server 2006, so it should be easy for you, to create a Site to Site VPN with Microsoft Forefront TMG.

Related links

Forefront Threat Management Gateway Beta 3
http://www.microsoft.com/DOWNLOADS/details.aspx?FamilyID=e05aecbc-d0eb-4e0f-a5db-8f236995bccd&displaylang=en
Forefront TMG Beta 3 is Released
http://blogs.technet.com/isablog/archive/2009/06/09/forefront-tmg-beta-3-is-released.aspx
What's new in Forefront TMG Beta 2 (Part 1)
http://www.isaserver.org/tutorials/Whats-new-Forefront-TMG-Beta-2-Part1.html
Installing and configuring Microsoft Forefront TMG Beta 2
http://www.isaserver.org/tutorials/Installing-configuring-Microsoft-Forefront-TMG-Beta2.html