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.

Create Site-to-Site Connection Wizard		
	Welcome to the Create VPN Site-to-Site Connection Wizard	
	This wizard helps you create a VPN site-to-site network, and configure local VPN settings and rules that enable the VPN connection with a remote site.	
	Help about <u>VPN site-to-site networks</u>	
	Site-to-site network name: Hannover	
	To continue, click Next.	
	< Back Next > Cancel	

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.

New User				? ×
User name:	Hann	over		
Full name:				
Description:				
Password:		•••••		
Confirm password	ł:	•••••		
🔲 User must ch	ange pa	assword at ne:	xt logon	
🔽 User cannot d	change	password		
Password nev	ver expi	res		
Account is dis	sabled			
Help			Create	Close

Figure 5: Remote VPN account

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

Hannover Properties	? ×
General Member Of Profile Environment Remote control Terminal Services Profile	Sessions Dial-in
Network Access Permission Allow access Deny access C Control access through NPS Network Policy	
Verify Caller-ID: Callback Options No Callback Set by Caller (Routing and Remote Access Service only) Always Callback to:)
Assign Static IP Addresses Define IP addresses to enable for this Dial-in connection.	dresses
Define routes to enable for this Dial-in Static	Routes
OK Cancel Apply	Help

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 address from a static IP address pool.

Create Site-to-Site Connection Wizard	×
Local Network VPN Settings Specify how IP addresses are assigned to incoming VPN client connections.	\mathbb{A}
Select the IP address assignment method: Static address pool IP address ranges:	
Start Address End Address Server Add 172.16.23.1 172.16.23.50 TMG Edit Remove. The static address pool cannot overlap with any existing networks, and cannot overlap with the static address pool at the other end of the tunnel. O Dynamic Host Configuration Protocol (DHCP).	
< Back Next >	Cancel

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.

Create Site-to-Site Connection Wizard	×
Connection Owner Specify a Forefront TMG array member for this connection.	\mathbb{A}
When Network Load Balancing is enabled, the connection owner is automatically assigned. When Network Load Balancing is disabled, you must select the Forefront TMG array member.	
Select connection owner:	
< Back Next > 0	Cancel

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.

Create Site-to-Site Connection Wizard		×
Remote Site Gateway Enter the IP address or server name (FQDN	l) of the remote site VPN server.	\mathcal{A}
Remote site VPN server:		
TMG2.system.center		
	< Back Next >	Cancel

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.

Create Site-to-Site Connection V	Vizard	×	
Remote Authentication For the local site to initiate a connection to the remote site, a user account on the remote site is required for authentication.			
Allow the local site to initia	te connections to the remote site, using this user account: must match the name of the VPN site-to-site d on the remote site.		
User name:	Nienstaedt		
Domain:	system.center		
Password:	•••••		
Confirm password:	••••••		
	< Back Next > Canc	el	

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.

Create Site-to-Site Conn	rection Wizard	×
Network Addresses Specify the IP addre match the internal ra	ess ranges of the remote site network. Th anges at the other end of the tunnel.	he ranges typically
Address ranges:		
Start Address	End Address	
172.16.24.1	172.16.24.1	
192.168.23.0	192.168.23.255	EOR
		Remove
		Add Range
	< Back	Next > Cancel

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.

Create Site-to-Site Connection	Wizard	×		
Remote NLB If Network Load Balancing is enabled on the remote site, specify the dedicated IP addresses (DIPs) of the remote site gateway.				
The remote site is enabled for Specify the dedicated IP addresse	Network Load Balancing es on the remote gateway:			
Start Address	End Address	Add Range		
		E dit		
		Remove		
I Help about <u>remote NLB-enabled a</u>	irrays.			
	< Back	Next > Cancel		

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.

Create Site-to-Site Connection Wizard	×
Site-to-Site Network Rule A network rule is required for traffic to be routed to and from the new VPN site-to-site network.	\mathcal{H}
Create a network rule specifying a route relationship Network rule name: Hannover to Nienstaedt Route traffic between the new network and these destinations:	
Name Add Internal Edit Edit Remove. Ill create a network rule later If you choose this option, you must create a network rule for this site-to-site Otherwise traffic will not be routed to and from this network.	network.
< Back Next >	Cancel

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.

Create Site-to-Site Connection Wizard
Site-to-Site Network Access Rule An access rule is required to allow traffic to and from the new VPN site-to-site network.
Create an allow access rule. This rule will allow traffic between the Internal network and the new site-to-site network for all users.
Access rule name: w access between Hannover and Nienstaedt
Apply the rule to these protocols:
Selected protocols
UNS Add
Remove Remove
 I'll change the access policy later If you choose this option, you must change the access policy for this site-to-site network. Otherwise traffic to and from this network will be denied.
< Back Next > Cancel

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.

Create Site-to-Site Connection Wizard		
HH /	Completing the New VPN Site-to-Site Network Wizard	
	You have successfully completed the New VPN Site-to-Site Network Wizard. The new network will have the following configuration:	
	Name: Hannover Protocol: PPTP Connection Owner: TMG	
94KAXV1151	۲. Example 2 and	
	Further configuration steps may be required for VPN connectivity. Help about <u>configuration steps</u>	
ØKN H	To close this wizard, click Finish.	
	< Back Finish Cancel	

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.

Remaining VPN Site-to-Site Tasks	×
Further configuration steps may be required:	
1 - A user account with dial-in access must be defined. User account name must be: Hannover	
, Help about <u>further configuration steps</u> OK	

Figure 16: Reminder for more necessary configuration steps

Click Apply.

The Site-to-Site VPN has now successfully created. It is possible to change the Siteto-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.

Hannover Properties			? ×		
General Server Connection Pro	Address	es R Authe	emote NLB		
Remote gateway name or IP addre	ess:				
TMG2.system.center	tions to remo	te site			
User name:	User name: Nienstaedt				
Domain:	system.cen	ter			
Password:	•••••				
Confirm password:	•••••				
Incoming Connection For the remote site to initiate a VPN connection to the local site, a user for this network with dial-in properties enabled must be defined.					
Terminate inactive connections after:					
	ОК	Cancel	Apply		

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.

Hannover Proper	ties			? ×			
General	Server	Address	es I	Remote NLB			
Connection	I P	rotocol	Autre	entication			
Select the authentication protocols used when Forefront TMG initiates connections to a remote site gateway.							
C Extensible authentication protocol (EAP). Examples: user certificates, RSA SecurID.							
Help about	ompleting EAP co	onfiguration					
Allow these	protocols						
Microsoft	CHAP Version 2	(MS-CHAP v2)					
The following authentication protocols are not recommended. Use these protocols only if the remote site does not support more secure protocols.							
Challenge Handshake Authentication Protocol (CHAP) Requires reversible passwords.							
Unencrypted Password (PAP)							
		ОК	Cancel	Apply			

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.

Site-to-Site Settings Summary	×						
Summary of local site-to-site settings:							
Remote Gateway Address: TMG2.system.center							
VPN Network Authentication Protocols (outgoing): MS-CHAP v2							
General VPN Settings Authentication Protocols (incoming): MS-CHAP v2							
Local User: Hannover Remote Site User: system.center\Nienstaedt							
Required site-to-site settings for the other end of this tunnel:							
Local User: system.center/Nienstaedt Remote Site User: Hannover							
Site-to-Site Network IP Addresses: 192.9.200.0-192.9.200.255 Routable Local IP Addresses: 172.16.24.1, 192.168.23.0-192.168							
▼ ▼							
Help about <u>VPN site-to-site summary</u> OK							

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.

Forefront Threat Manage	ement Gateway Beta				Web Access Policy Enterprise Edition
Web Access Pol	js				
Web Proxy Authentica HTTP Comp	Web Proxy: Enabled (Port: 8080) Malware Inspection: Enabled Authentication: Not required by policy. (proxy authentication) Web Caching: Enabled HTTP Compression: Enabled HTTPS Inspection: Enabled			1	
Action	Name	Condition	From	То	
🗖 🥝 Allow	🟋 Allow access between Hannover and Nienstaedt	🖀 All Users	Hannover Internal	👍 Hannover	

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.

Forefront TMG Beta							_ 8 >
File Action View Help							
(= =) 2 🗊 2 🖬 🔹 🖀 X Ə 😌 🔹 9 🗁 S							
Microsoft Forefront Threat Managemer	Microsoft*						Networking
Forefront TMG (TMG)	Forefront						-
Dashboard	Threat Manage	ement Gateway Beta				E	nterprise Edition
Firewall Policy Networks V Network Sets Network Adapters Routing Web Chaining ISP Redundancy							
E-Mail Policy	Order 🔺	Name	Relation	Source Networks	Destination Net	NAT Addresses	Description
	_1	Local Host Access	Route	👍 Local Host	🚖 All Networks (
Remote Access Policy (VPN)				a a lumu di			
📥 Networking	🗏 🥶 2	VPN Clients to Internal Network	Route	Quarantined VPN Clie	👍 Internal		
System				S VPN Clients			
Logs & Reports	😑 🖂 3	Internet Access	NAT	👍 Internal	🎯 External	Default IP address	
2 Update Center	·			👍 Quarantined VPN Clie			
Troubleshooting				VPN Clients			
	e 4	Hannover to Nienstaedt	Route	Hannover	-1- Internal		

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-isreleased.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