Implementing Windows Server 2012 DirectAccess behind Forefront TMG Part II

Abstract

This is a two part article series. I will show you how to configure Windows Server 2012 as a DirectAccess Server and how to configure Firewall policy rules on the Forefront TMG Server to allow DirectAccess clients to access the Windows Server 2012 DirectAccess Server. Part I talked about some basics DirectAccess technologies and how to configure the DirectAccess feature of Windows Server 2012. This part of the article series explains how to configure Forefront TMG to allow DirectAccess clients to access the DirectAccess Server and how to connect DirectAccess clients.

Let's begin

To publish the Windows Server 2012 DirectAccess Server we must use a non-Webserver Protocol publishing rule. You cannot use a Webserver publishing rule with HTTPS to HTTPS bridging because the communication channel between the DirectAccess client and the DirectAccess server must be unchanged.

Create a publishing rule on the Forefront TMG Server

Start the new Non-Webserver Protocol Publishing Rule wizard. Name the publishing rule *DirectAccess* and specify the IP address of the Windows Server 2012 DirectAccess Server.

New Server Publishing Rule Wizard	×					
Select Server Specify the network IP address of the server you are publishing.						
<u>S</u> erver IP address:						
10 . 80 . 16 . 158 Browse						
< <u>B</u> ack <u>N</u> ext > (Cancel					

Figure 1: Select the Server to publish

As the protocol select the predefined protocol HTTPS-Server

New Server Publishing Rule Wizard	×
Select Protocol Select the protocol used by the published server.	A
Selected protocol:	
HTTPS Server	Properties
	Ports
	New
< Back Nex	d > Cancel

Figure 2: Protocol is HTTPS-Server

Forefront TMG must listen on the external network. If the Forefront TMG Server has only one assigned IP address on the external network adapter select only the External network. If there are mutliple IP addresses bound on the external interface select the specific address for DirectAccess.

New Server Publishing Rule Wizard		×			
Network Listener IP Addresses Select the network IP addresses on the Forefront TMG that will listen for requests intended for the published server.					
Listen for requests from these networks:					
Name	Selected IPs	▲			
🗹 🌑 External	<all addresses="" ip=""></all>				
🗖 🛶 Internal	<all addresses="" ip=""></all>				
🗖 📥 Local Host	<all addresses="" ip=""></all>				
Quarantined VPN Clients	<all addresses="" ip=""></all>				
VPN Clients	<all addresses="" ip=""></all>	_			
<u> </u>					
	Add	ress			
	< Back Next >	Cancel			

Figure 3: Select the External network

If the Windows Server 2012 DirectAccess Server is not a Secure NAT client change the request in the publishing rule on the *To* tab to *Requests appear to come from the Forefront TMG computer*.

DirectAccess Properties	×
General Action Traffic From To Networks Schedule	
Specify the network address of the server to publish:	
10 . 80 . 16 . 158 Browse	
Requests for the published server Specify how Forefront TMG forwards requests to the published server:	
Requests appear to come from the Forefront TMG computer	
C Requests appear to come from the original client	
OK Cancel Apply	,

Figure 4: Change the requests for the published Server if the Server's Default Gateway doesn't point to the Forefront TMG Server

Additonal ports

Depending on the configuration in the DirectAcess wizard it may be necessary to create additional Firewall Policy rules on the Forefront TMG Server. The <u>article</u> explains which additonal ports mut be opened for full DirectAccess connectity at the Edge Firewall if Teredo or 6t04 protocols should be used.

For full DirectAccess connectivity you must open UDP port 3544 in- and outbound for the Teredo protocol and IP level 41 protocol

Teredo Inbound

Teredo-Inbound Properties						
General Parameters						
- Driver and Comparison						
Primary Connectio	ns					
Port Range	Protocol Type	Direction	Add			
3544	UDP	Receive	Edit			
			Remove			
Secondary Connec	tions					
Port Range	Protocol Type	Direction	Add			
			Edit			
			Remove			
Application Filters						
	ilter		3			
H.323 Filter						
			I			
Show only selected application filters						
		ОК С	Apply Apply			

Figure 5: Additional ports for the Teredo protocol

Teredo Outbound

Teredo-Outbound P	roperties			×	
General Parameter	s				
Primary Connectio	ns				
Port Range	Protocol Type	Direction		Add	
3544	UDP	Send		Edit	
				Remove	
Secondary Connec	tions				
Port Range	Protocol Type	Direction		Add	
				Edit	
				Remove	
Application Filters					
DNS Filter			-		
FTP Access F	ilter				
H.323 Filter			-		
Show only se	ected application	filters			
		ОК	Cancel	Apply	

Figure 6: Additional ports for the Teredo protocol

IP Protocol 50 Inbound – Outbound

General Parameters	Properties s			
Primary Connection	ns			
Protocol Num	Protocol Type	Direction		Add
41	IP-level	Send Receive		Edit,
				Remove
				Remove
Application Filters				
DNS Filter	lter			
H.323 Filter				
			<u> </u>	
Show only sel	ected application	filters		
		ок	Cancel	Apply

Figure 7: Additional ports for the IP level 41 protocol

With these new protocol definitons create two new Firewall policy rules. One Firewall policy rule which allows the IP level 41 protocol and the Teredo protocol from EXTERNAL to the Windows Server 2012 DirectAccess Server.

🗖 📝 3	DirectAccess Teredo - IP41	🥝 Allow	ill IPProtocol41-InOut	🌍 External	E WS2012-MEM1	🖀 All Users
🥂 3	DirectAccess Teredo out	🥝 Allow	🛄 Teredo-Outbound	E WS2012-MEM1	🏐 External	澹 All Users
Figure 8: Final F	irewall Policy rules					

The next required Firewall policy rule allows the Teredo protocol from the DirectAccess server to EXTERNAL.

Attention: This setting requires that the network relationship on the Forefront TMG Server from the INTERNAL to EXTERNAL network is ROUTE instead of NAT (the default).

Apply Group Policy to the client

After the Firewall policy rules and the publishing rule has been configured on the Forefront TMG Server apply the group policy to the DirectAccess client. To do this put the computer account of the client computer to the Windows group for DirectAccess, reboot the client machine and see if the group policy settings has been applied. If this is not the case update the group policy manually (Gpupdate /force)

and restart the client and check after the reboot if the group policy has been applied to the client (use Gpresult.exe /v | more for example).

If the group policy has been applied successfully your client computer should now be a DirectAccess client. Check DirectAccess connectivity with a simple Ping to one of your internal clients or servers and you should get an IPv6 address back.

Administrator: Command Prompt		-		×
C:\Users\administrator>ping ws2012-dc.win2012.server Pinging ws2012-dc.win2012.server [fd93:21c7:fb97:7777::a50:105a] data: Reply from fd93:21c7:fb97:7777::a50:105a: time=1ms Reply from fd93:21c7:fb97:7777::a50:105a: time=2ms Reply from fd93:21c7:fb97:7777::a50:105a: time=1ms Reply from fd93:21c7:fb97:7777::a50:105a: time=1ms	with	32	bytes	•
Ping statistics for fd93:21c7:fb97:7777::a50:105a: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 1ms, Maximum = 2ms, Average = 1ms C:\Usens\administraton\				
				~

Figure 9: Check DirectAccess connectivity

Windows 8 has a build in network connectivity assistant (NCA) which gives you more information about the DirectAccess state as shown in the following screenshot. Depending on your DirectAccess configuration on the Windows Server 2012 DirectAccess Server you will see a different name for the DirectAccess connection.

DirectAccess Properties	Networks Connections
General Status Action required No Internet access. Multisite Your computer is correctly configured for single-site DirectAccess.	Workplace Connection
Logs Collect logs for advanced troubleshooting. Collect Logs View logs OK Cancel Apply	

Figure 10: Network Connectivity Assistant

Please note: This screenshot comes from my test environment where the client has no real Internet connectivity. So don't wonder why the status indicator tells us that there is not Internet connectivity.

For troubleshooting purposes users are able to collect log files for advanced troubleshooting and if you specified a e-mail address in the DirectAccess configuration on the Windows Server 2012 users can send these log files to your support personal.

The new DirectAccess component in Windows Server 2012 has Remote Access Dashboard which gives you a quick overview about the state of every DirectAccess component.



Figure 11: A DirectAccess client is connected

The Remote Client Status dashboard gives you more details about connected clients. You can see the clients connected to the DirectAccess server, the communication protocol used and the amount of traffic used by the DirectAccess client.

8	Remote Access N	lanagement Console	_ 0 ×
CONFIGURATION CONFIGURATION CONFIGURATION CONFIGURATIONS STATUS	Remote Access Clients Statu	S	Tasks Monitoring Refresh Configure Refresh Interval
REMOTE CLIENT STATUS			Disconnect VPN Clients
REPORTING	Search P p S	earch (iii) 🕶 📵 🕶 🕟	Learn About
US2012-MEM1	User Name Host Name IS WIN2012\Administrator WIN2012\WIN8CL2\$ -	P Address Protocol/Tunnel Duration IPHttps 00:01:21	Learn About Remote Access
	Access Details 📀	Connection Details 📀	
	Protocol Port IP Addre 17 123 10.80.16.90	Connect Using DirectAccess Total Bytes In 15656 Total Bytes Out 19104 Connection start 16.03.2013 11:20:45 Authentication Machine Kerberos & User Kei ISP Address - K III >	

Figure 12: detailed connection information about the DirectAccess client

For detailed reports about DirectAccess connections you are able to configure a more enhanced reporting in the DirectAccess Management console.

Conclusion

In this second article I showed you how to create Firewall policy rules on the Forefront TMG Server and how to configure Windows 8 clients as DirectAccess clients.

Related links

Windows Server 2012 Direct Access – Part 1 What's New <u>http://blogs.technet.com/b/meamcs/archive/2012/05/03/windows-server-2012-direct-access-part-1-what-s-new.aspx</u> 'Real World' Direct Access installation using Windows Server 2012 <u>http://blogs.msdn.com/b/canberrapfe/archive/2012/07/12/simple-direct-access-setup-with-windows-server-2012-rp.aspx</u> Packet Filters for Your Internet Firewall <u>http://technet.microsoft.com/en-us/library/ee382268(v=ws.10).aspx</u> Publishing non-Web servers <u>http://technet.microsoft.com/en-us/library/cc995316.aspx</u>