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

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.

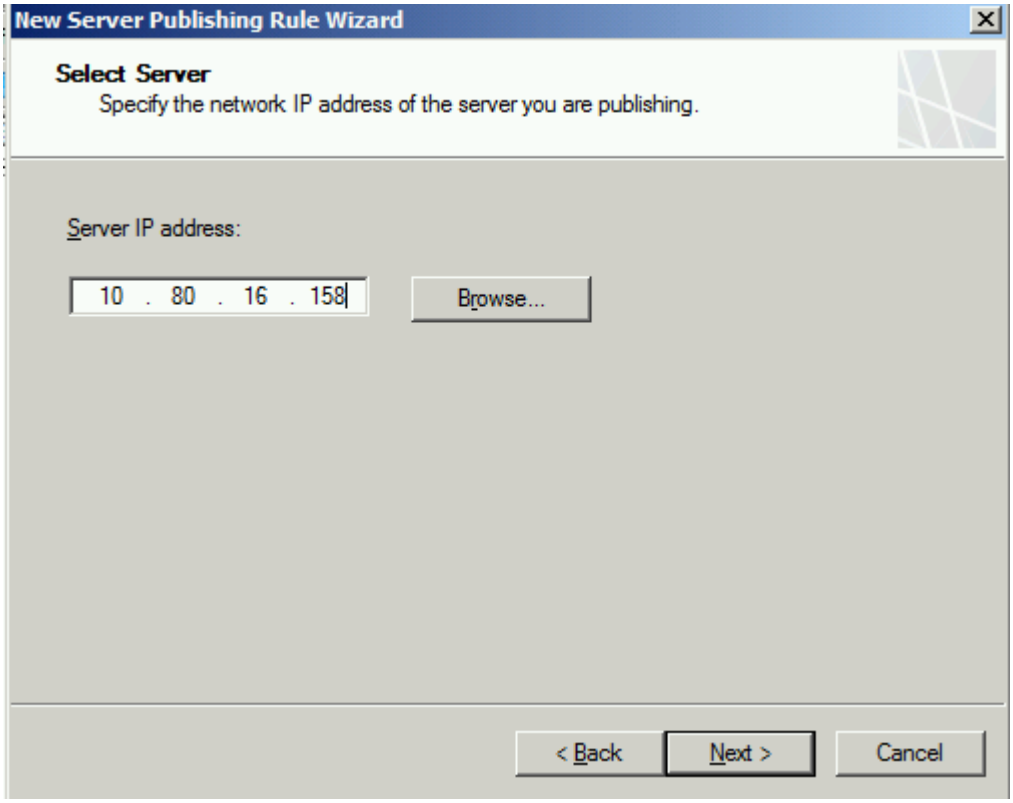

Figure 1: Select the Server to publish

As the protocol select the predefined protocol *HTTPS-Server*

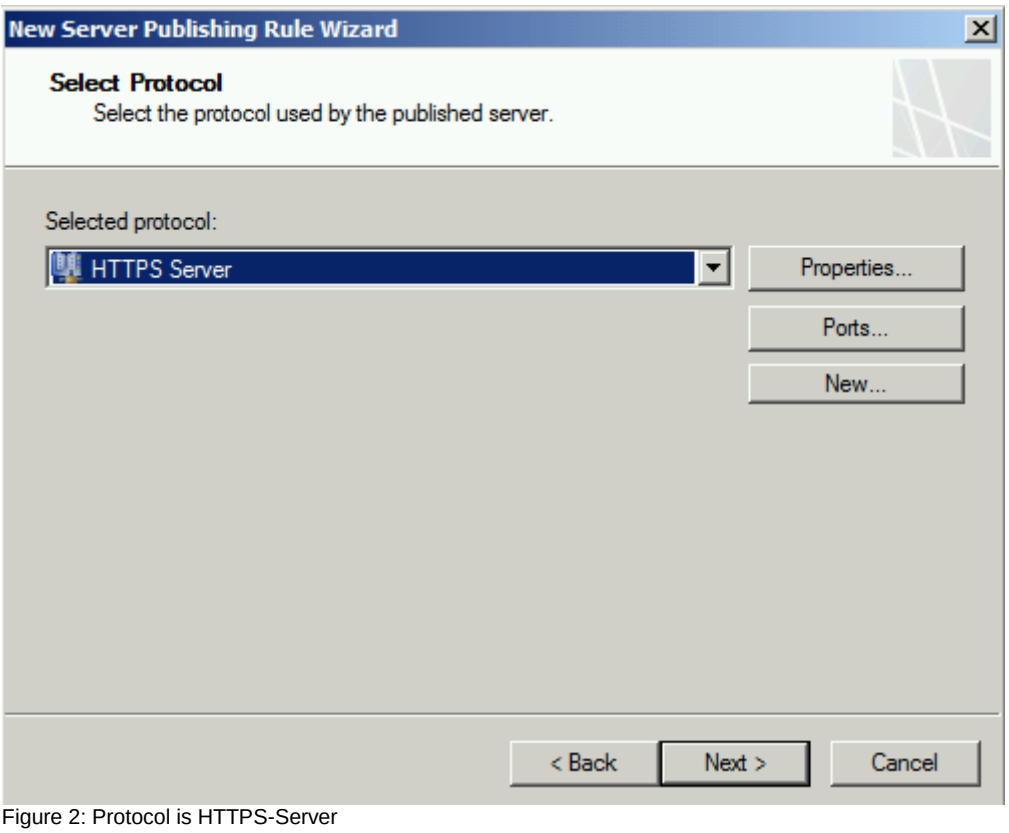

Figure 2: Protocol is HTTPS-Server

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.

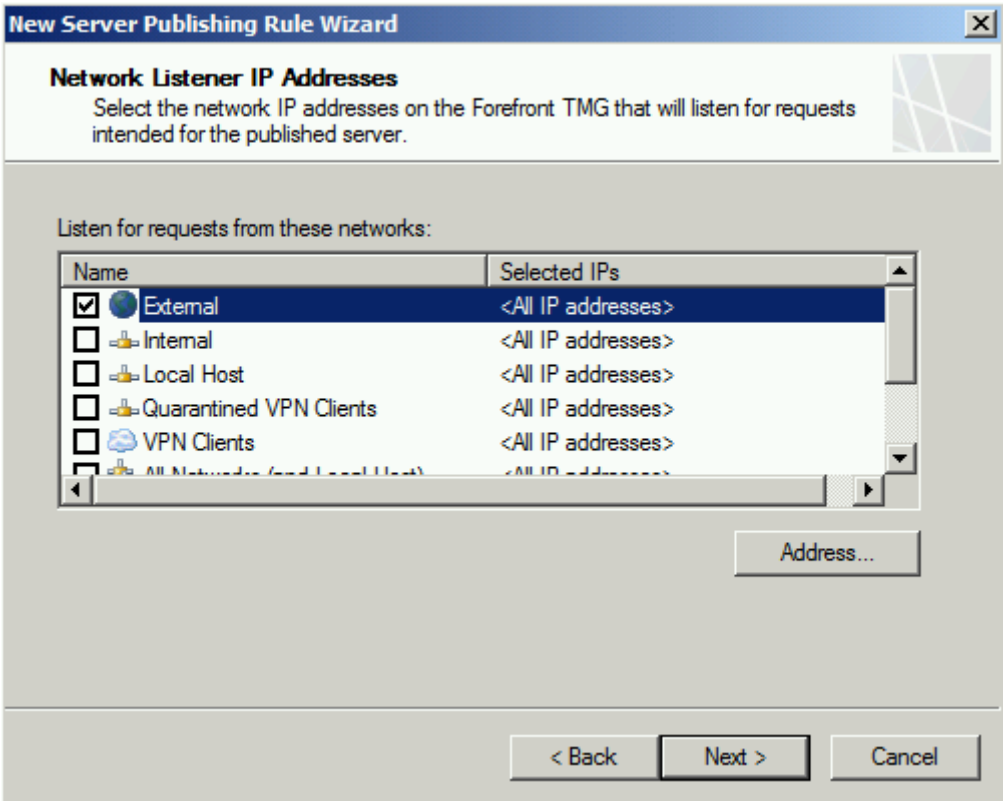

Figure 3: Select the External network

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*.

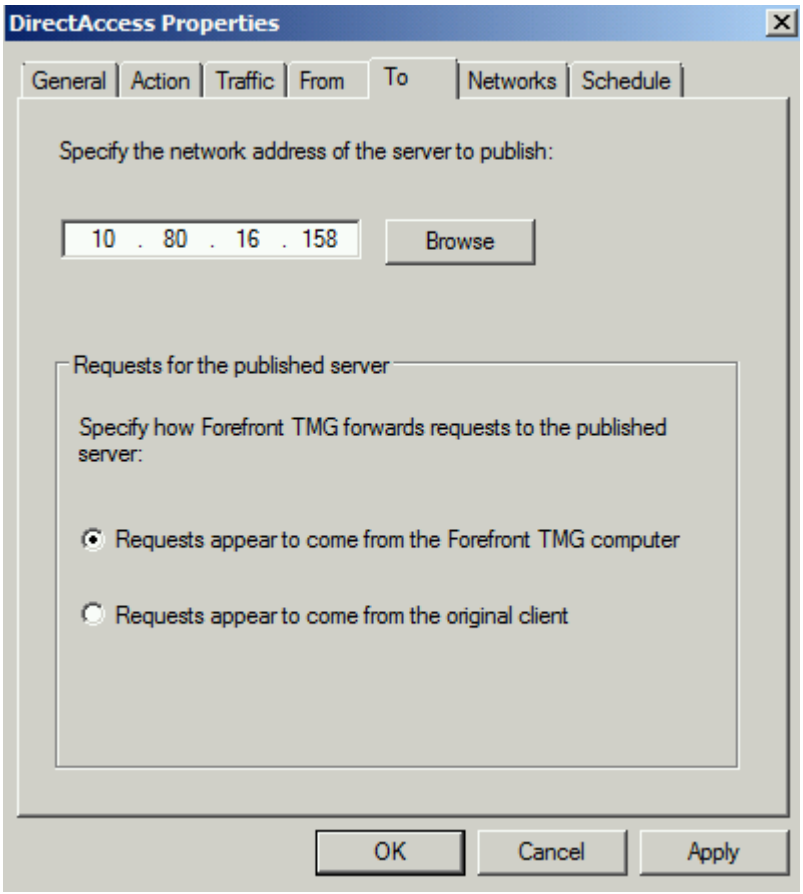

Figure 4: Change the requests for the published Server if the Server's Default Gateway doesn't point to the Forefront TMG Server

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 article 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 connectivty you must open UDP port 3544 in- and outbound for the Teredo protocol and IP level 41 protocol

Teredo Inbound

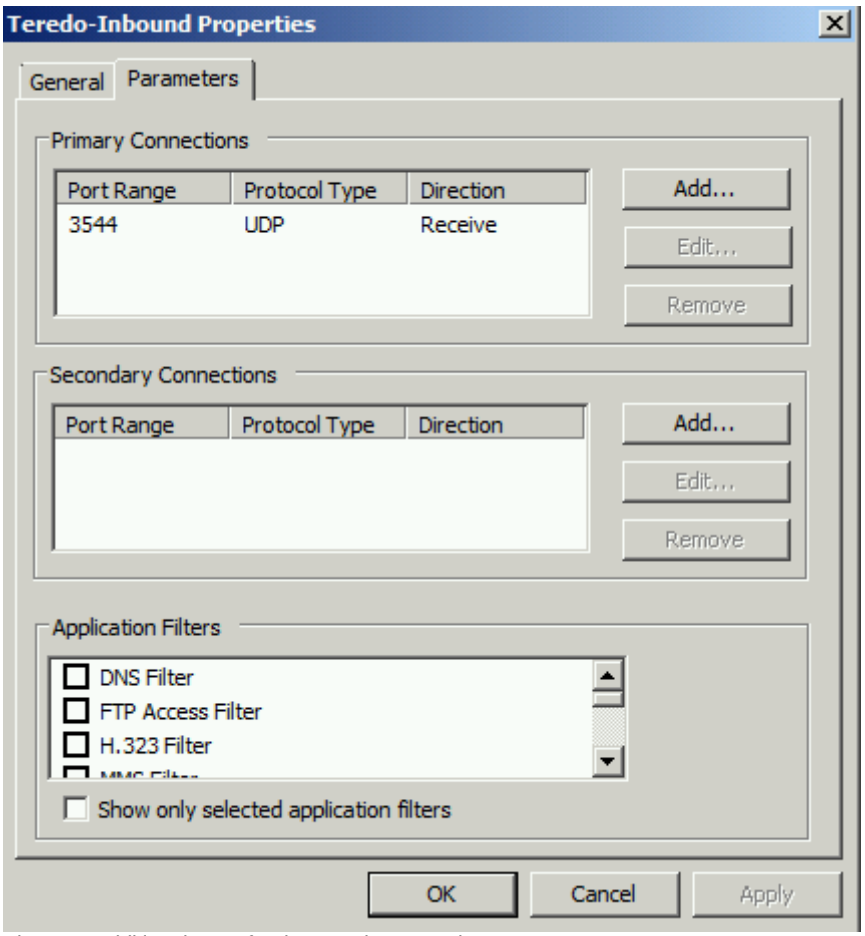

Figure 5: Additional ports for the Teredo protocol

Teredo Outbound

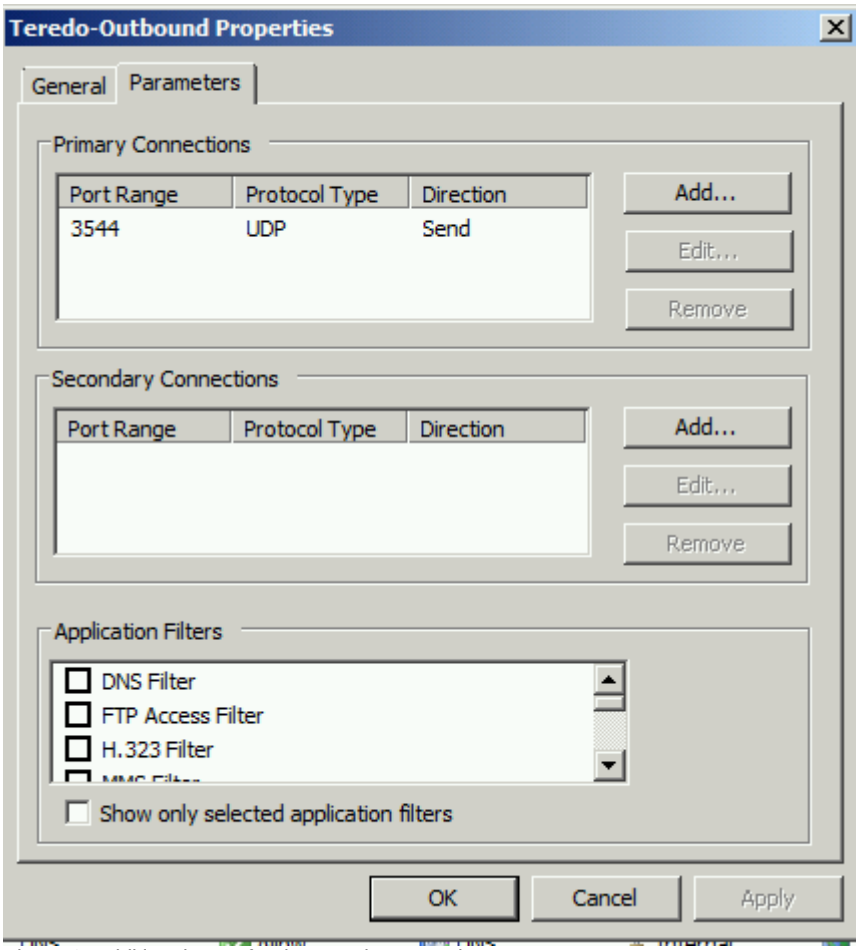

Figure 6: Additional ports for the Teredo protocol

IP Protocol 50 Inbound – Outbound

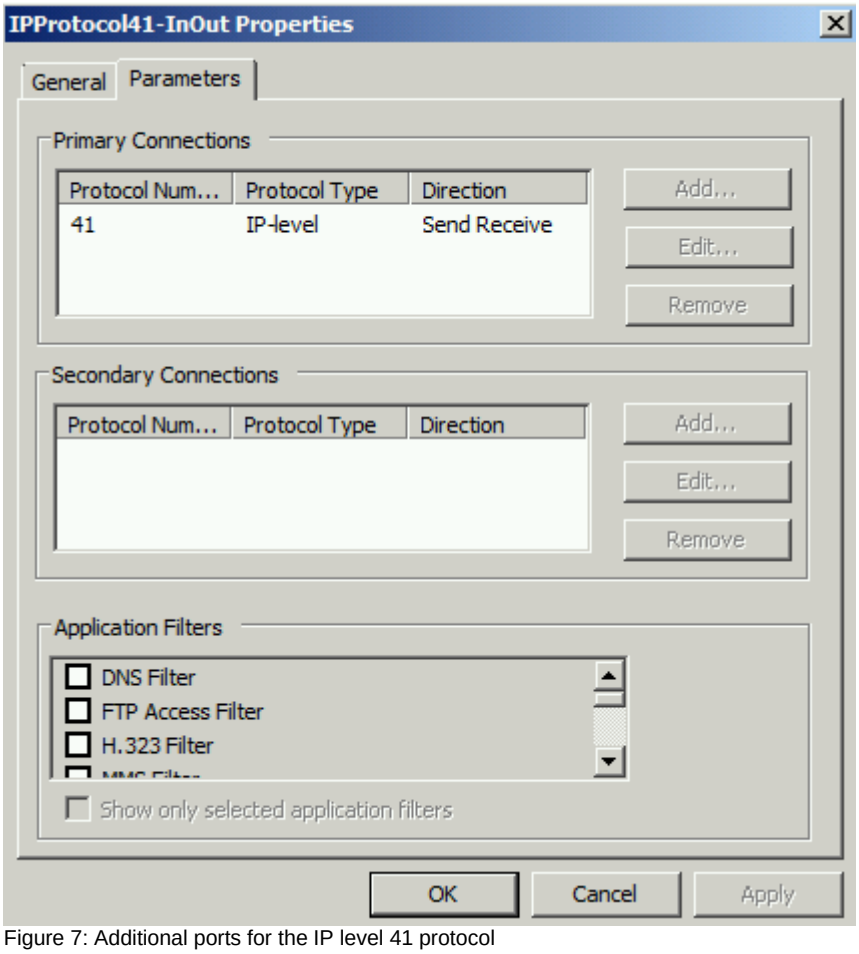

Figure 7: Additional ports for the IP level 41 protocol

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.

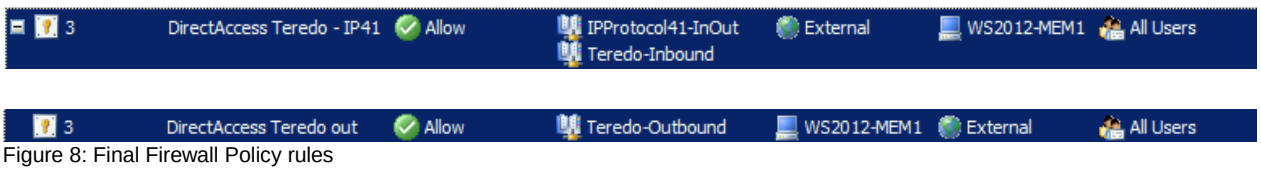

Figure 8: Final Firewall Policy rules

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 sucessfully 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.

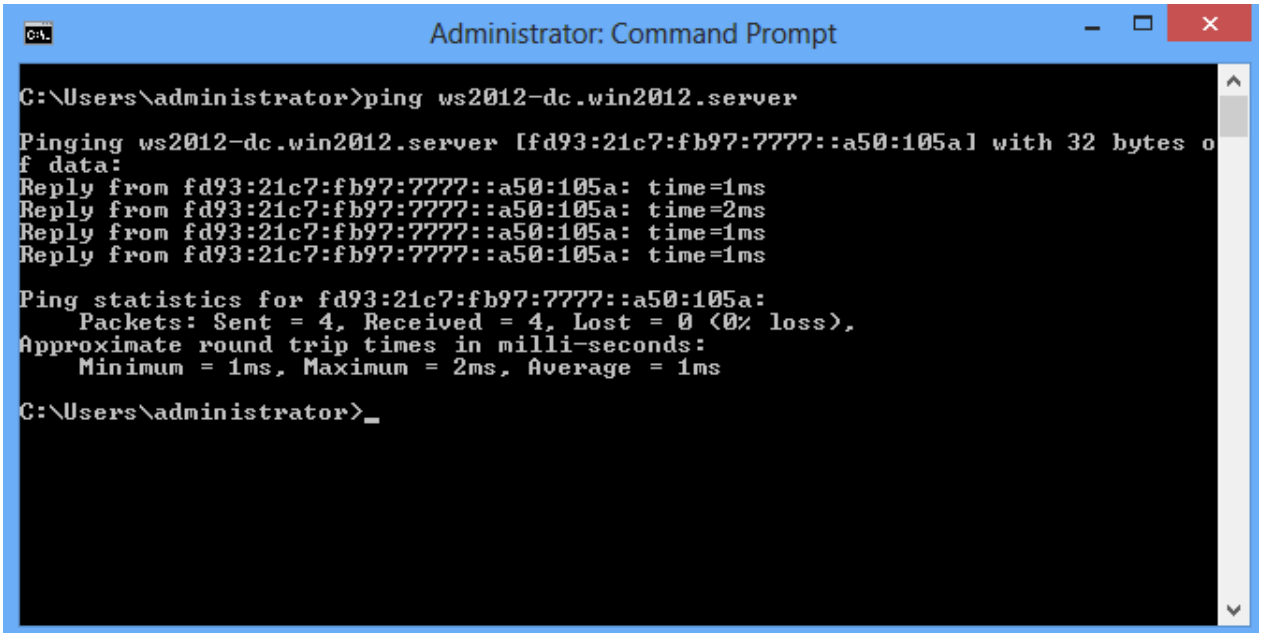

Figure 9: Check DirectAccess connectivity

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.

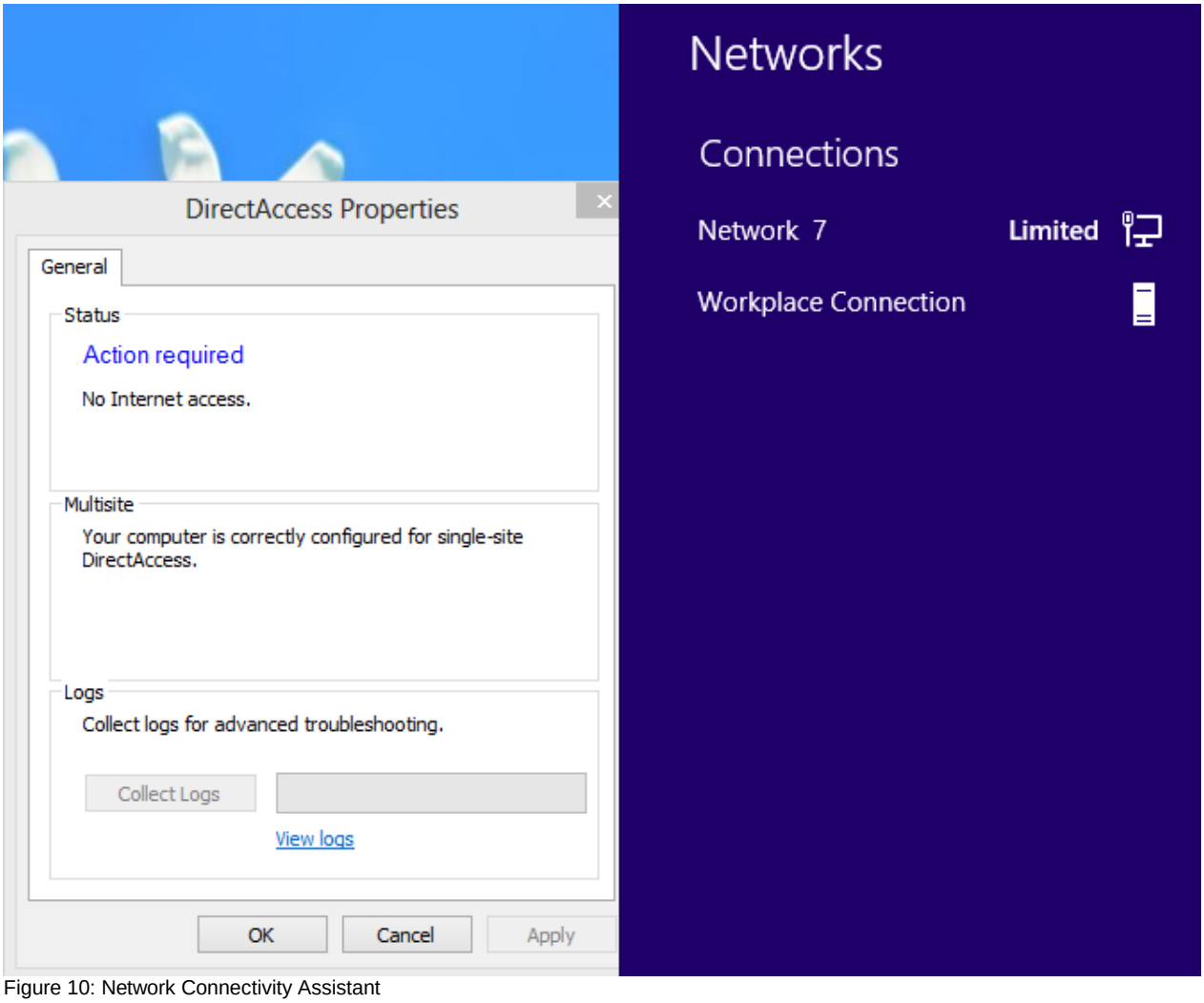

Figure 10: Network Connectivity Assistant

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.

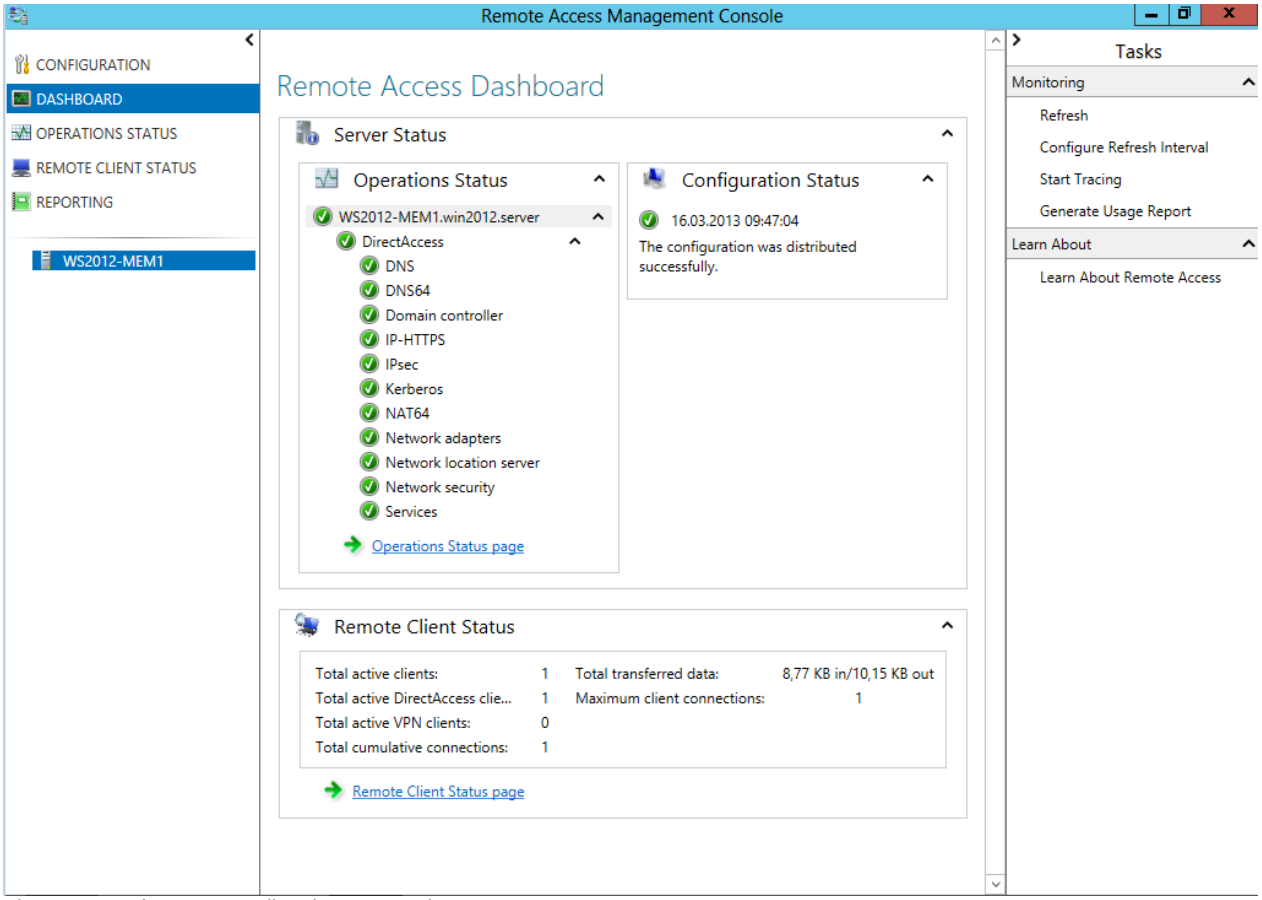

Figure 11: A DirectAccess client is connected

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.

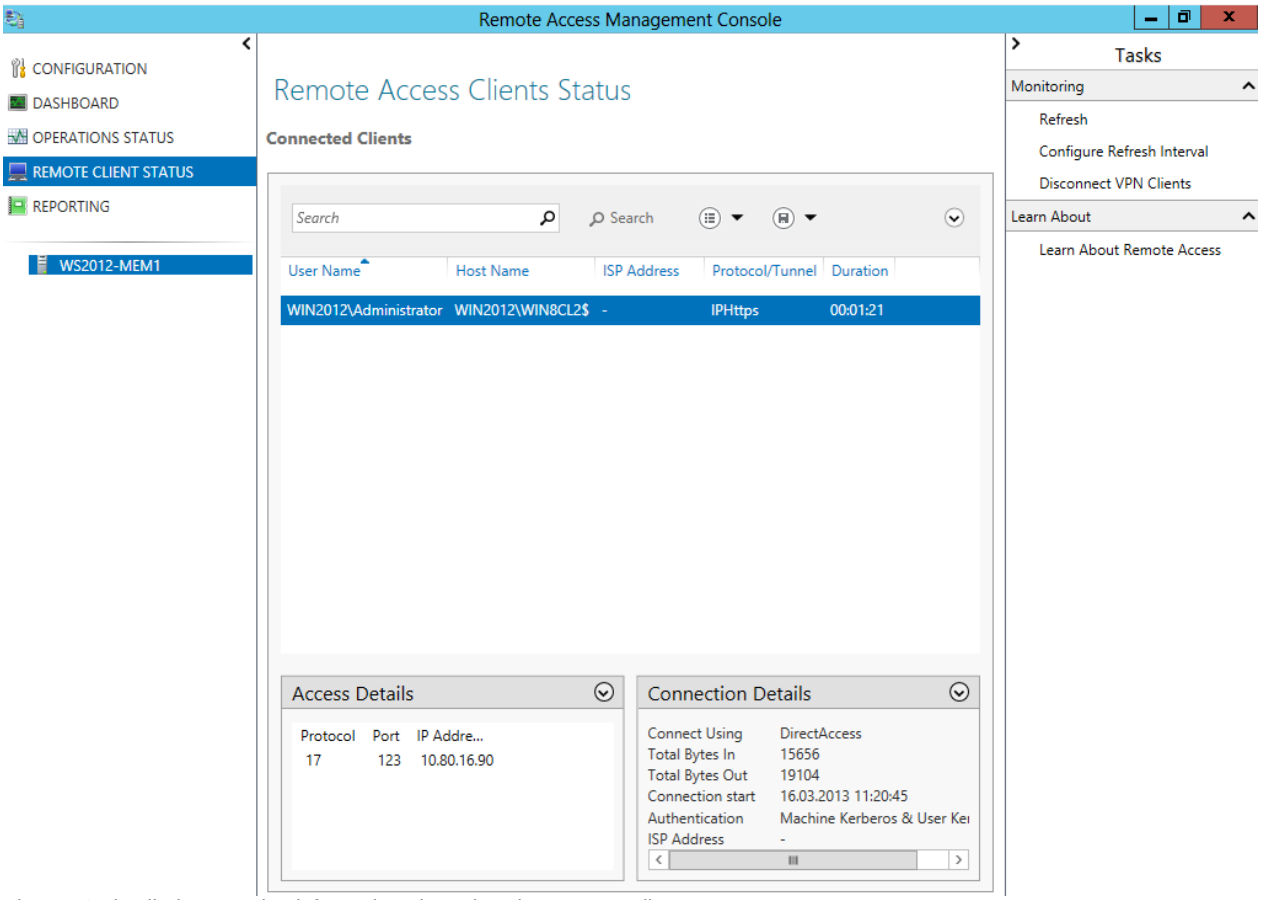

Figure 12: detailed connection information about the DirectAccess client

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