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 I

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 starts with some basics about DirectAccess technologies and how to configure the DirectAccess feature of Windows Server 2012. Part II explains how to configure Forefront TMG to allow DirectAccess clients to access the DirectAccess Server and how to connect DirectAccess clients.

Let's begin

DirectAccess is a new feature which is built into Windows Server 2008 R2 and Windows 7 Ultimate and Enterprise. DirectAccess has been enhance in Windows Server 2012 and Windows 8 and is now cllaed URA (Unified Remote Access). DirectAccess provides a technology called “always on” which means the client is permanently connected with the corporate network if he has an Internet connection. With DirectAccess, users are able to access all corporate resources.
This seamless connectivity provided by DirectAccess also enables Administrators to manage its mobile computers outside the internal network. Notebooks are able to update Group Policy settings, receive software updates, Windows updates, and report security events anytime they have Internet connectivity, even if the user is not logged on. DirectAccess uses Internet Protocol Security (IPsec) to ensure data integrity and encryption. DirectAccess performs both computer and user authentication, and can be configured to require two-factor user authentication for corporate network access using smart cards and OTP.

DirectAccess infrastructure requirements

For a successful DirectAccess implementation you must configure several components in your internal IT infrastructure:

DirectAccess client

A domain-joined computer running Windows 7/8 Enterprise or Windows 7 Ultimate, DirectAccess clients communicate with the corporate network using Internet Protocol version 6 (IPv6) and IPsec, encapsulated over IPv4 transition technologies (6to4, Teredo, or IP-HTTPS).
Attention: IP-HTTPS is the default protocol of the “simple” DirectAccess wizard in Windows Server 2012 if you choose the topology “behind an edge device”.

DirectAccess server

A domain-joined computer running Windows Server 2012 that accepts connections from DirectAccess clients and establishes communication with intranet resources.

The DirectAccess server authenticates DirectAccess clients and acts as the IPsec tunnel router/gateway for the external traffic, while also acting as an IPv6/DNS64/NAT64 router forwarding the network traffic between the clients connected to the Internet and clients and servers in the internal network.

Internal clients and Server

Internal servers and clients are also joined to the IPv6 network and communicate with DirectAccess clients through the DirectAccess server.
For legacy applications and non-Windows servers that have no IPv6 support, Windows Server 2012 translates the incoming IPv6 traffic to IPv4 using NAT64/DNS64.

NAP Server

You can use Network Access Protection (NAP) as an optional component for DirectAccess clients which connect to the internal network through Windows Server 2012.

Network Location Server (NLS)

The NLS Server is a Web server with a HTTPS binding which is located on the internal network. The DirectAccess client tries to connect to the NLS Server. If the client is able to access the DirectAccess Server, the client doesn't use DirectAccess. If the client cannot reach the NLS server, the DirectAccess client will be enabled. The NLS Server can be located on the Windows Server 2012 DirectAccess Server and this is the default behaviour if you use the simple DirectAccess wizard.

Network Access Protection (NAP)

NAP is an optional component in Windows Server 2012 to enhance the security. The Health Registration Authority (HRA) server obtains health certificates on behalf of NAP clients determined as compliant with network health requirements. These health certificates are later used to authenticate NAP clients for IPsec-protected communications with other NAP clients on an intranet.

OTP and Smartcard authentication

Also an optional configuration option it is possible to configure Windows Server 2012 DirectAccess with two-factor authentication using a one-time password (OTP).

Public Key Infrastructure (PKI)

If you use the simple DirectAccess wizard in Windows Server 2012, a PKI is not required. The wizard creates self-signed certificates and make sure that the self-signed certificate is copied to into the local computer certificate store of the Trusted Root Certificate Authorities on the DirectAccess clients. The wizard makes also sure that CRL checking for IP-HTTPS will be disabled. For enhanced URA configuration like Multi Site support and access for Windows 7 clients you will need to deploy a PKI.

What's new in DirectAccess in Windows Server 2012

Windows Server 2012 DirectAccess has some new and enhanced functionality compared with DirectAccess in Windows Server 2008 R2 and Forefront UAG. Here is a brief list of new functionalities:

- Direct Access and RRAS coexistence
- Simplified Direct Access management for small and medium organization administrators
- Built-in NAT64 and DNS64 support for accessing IPv4-only resources
- Support for Direct Access server behind a NAT device
- Load balancing support
- Support for multiple domains
- Support for OTP (token based authentication)
- Automated support for force tunnelling
- Multisite support
- Windows Server Core support
- Windows PowerShell support
- User and server health monitoring
- No PKI required for basic DirectAccess

Installation

The default installation of the DirectAccess functionality in Windows Server 2012 is designed for small and medium size companies and overcomes some limitations of classic DirectAccess deployments and requires fewer infrastructure components like a Public Key Infrastructure, separate Network Location Server (NLS) and the need to publish the Certificate Revocation List (CRL) against the Internet.
Attention: For an advanced DirectAccess configuration in Windows Server 2012 you must configure most settings manually and a manual configuration may require a Public Key Infrastructure and some more components like a DirectAccess Deployment in Forefront UAG.

First we need to install the Remote Access role on the Windows Server 2012.

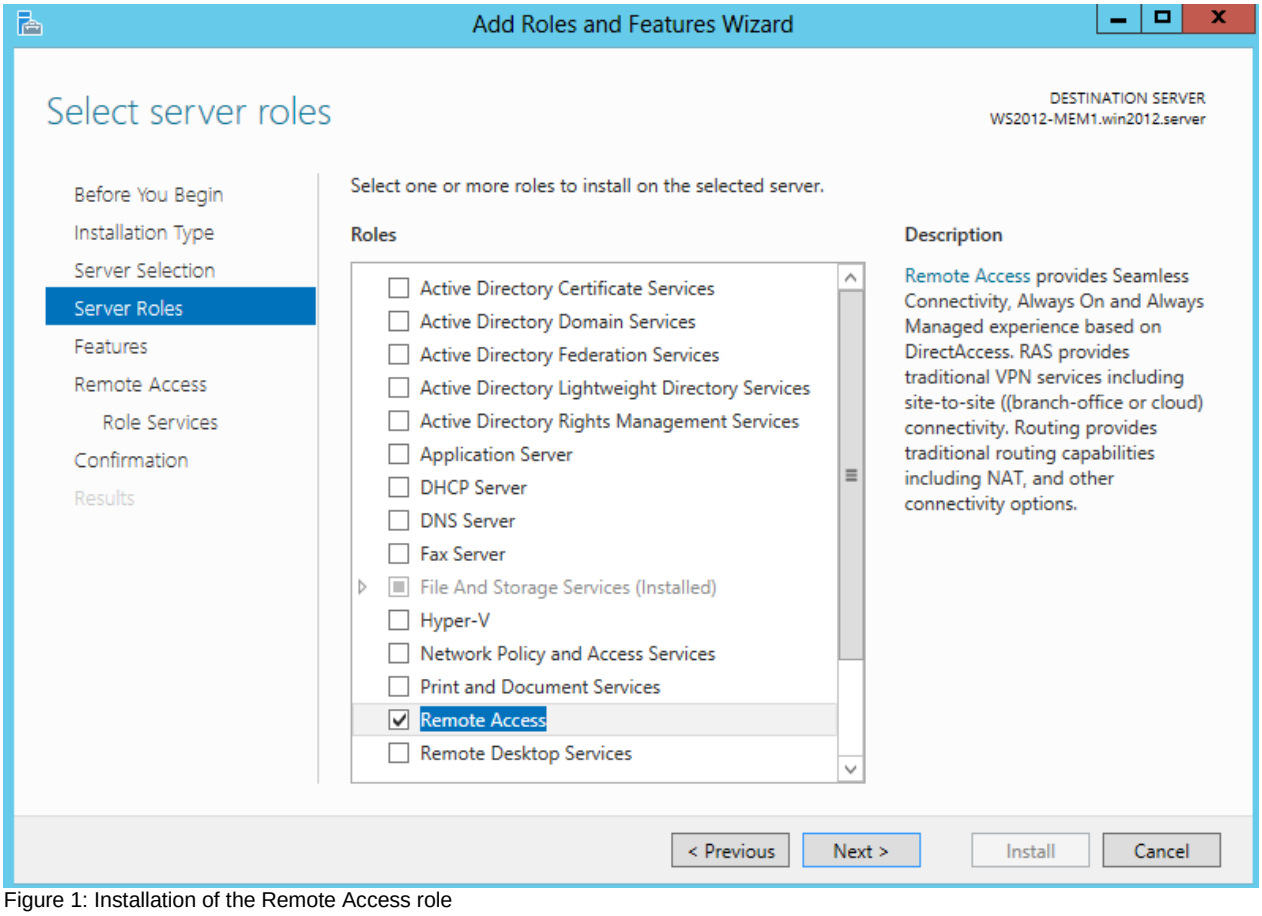

Figure 1: Installation of the Remote Access role

As a role service we select the checkbox DirectAccess and VPN(RAS)

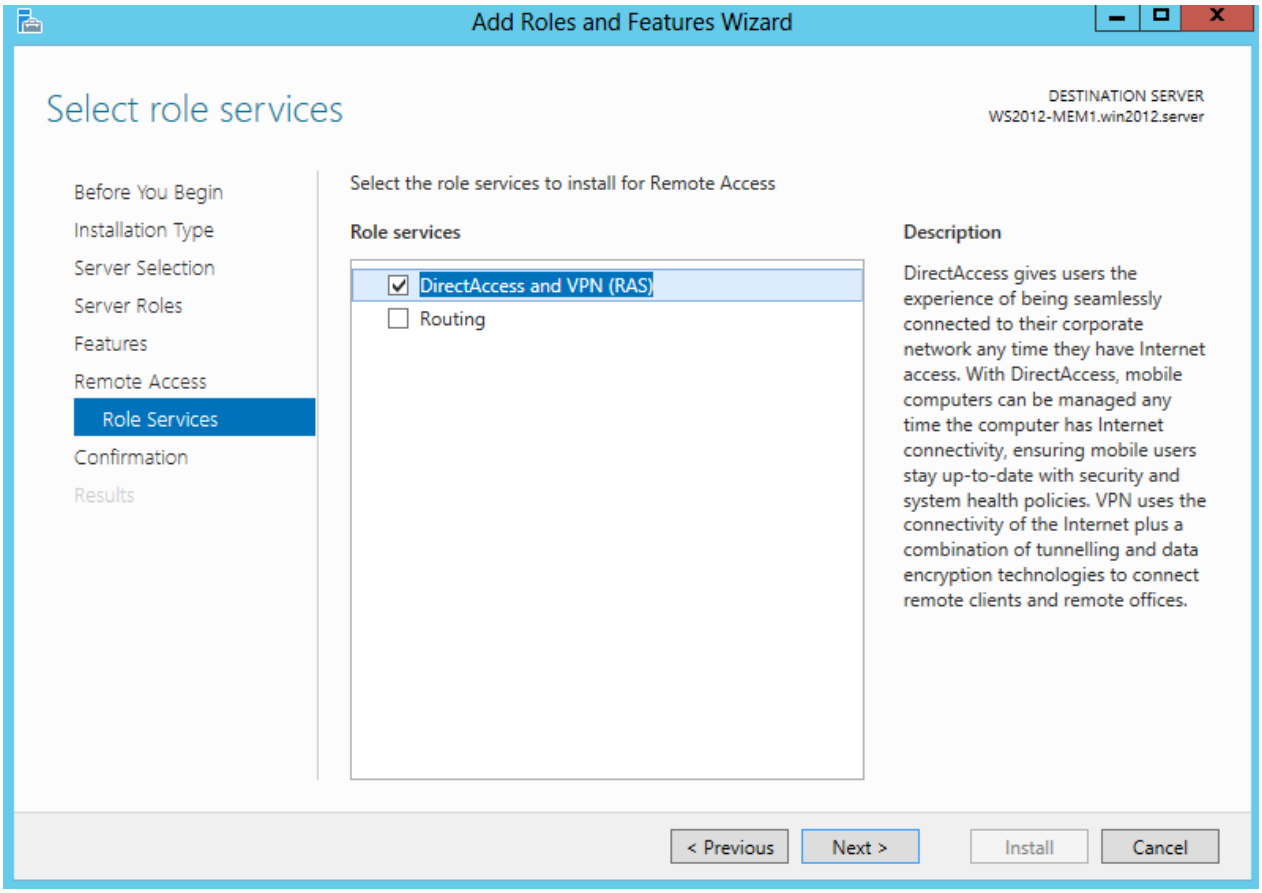

Figure 2: Select required role services

The installation takes a few minutes.

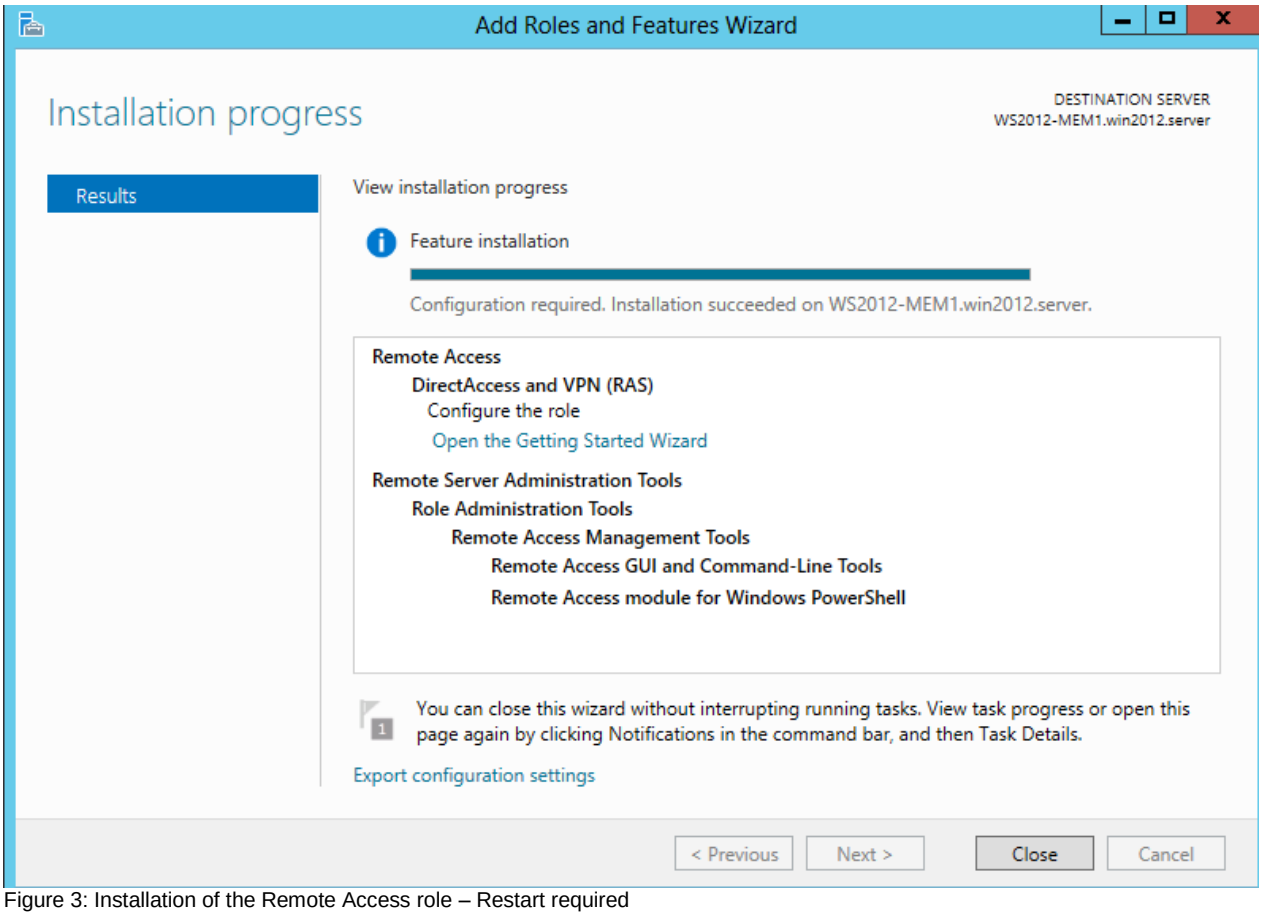

Figure 3: Installation of the Remote Access role – Restart required

Start the getting started wizard and select “Deploy DirectAccess only” if you do not want to configure the DirectAcess Server as a VPN Server.

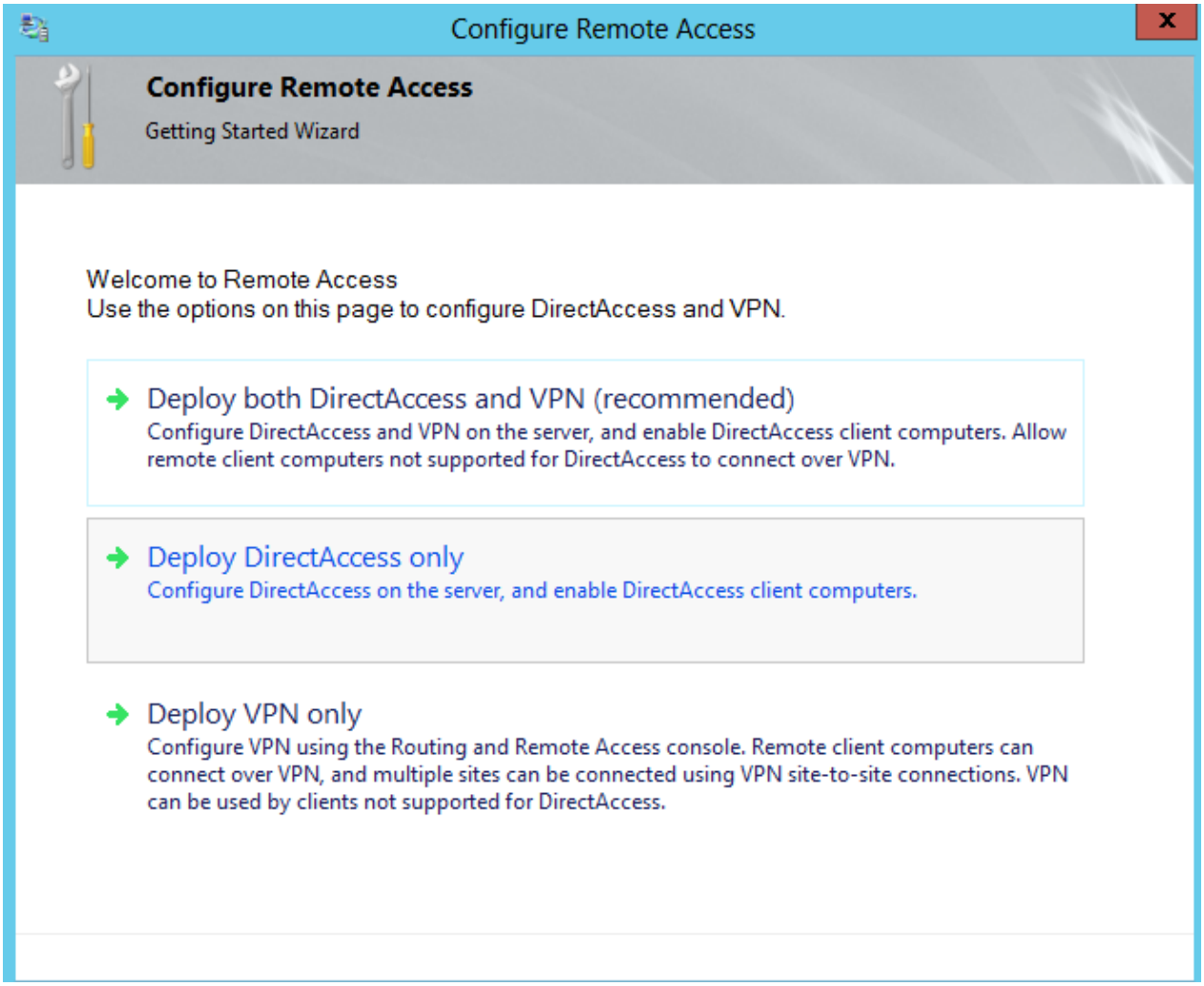

Figure 4: Configure DirectAccess

The DirectAccess Server has only one connected network adapter and will be placed behind the Forefront TMG Server.

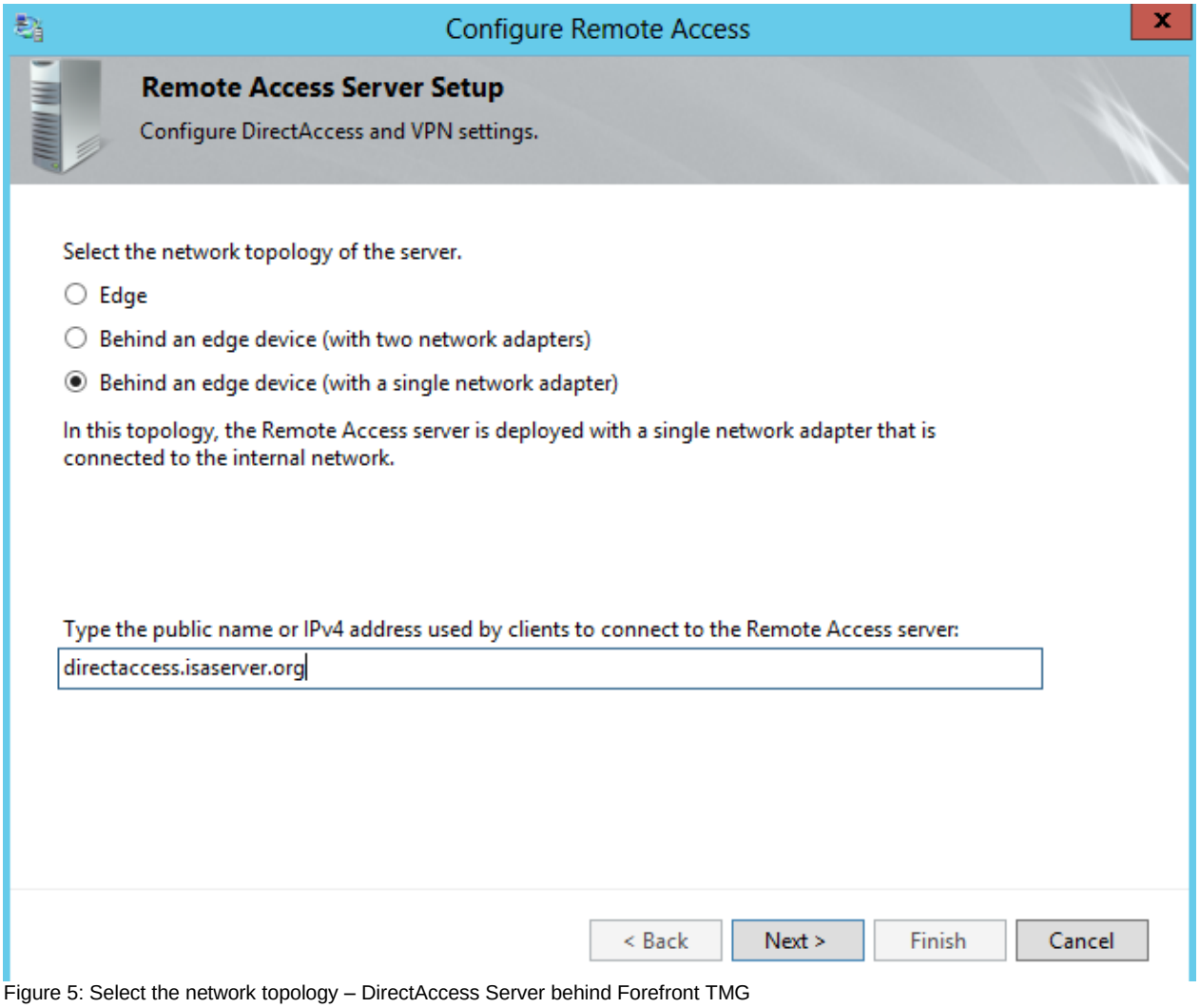

Figure 5: Select the network topology – DirectAccess Server behind Forefront TMG

The public name is used by the DirectAccess clients to connect to the DirectAccess Server.

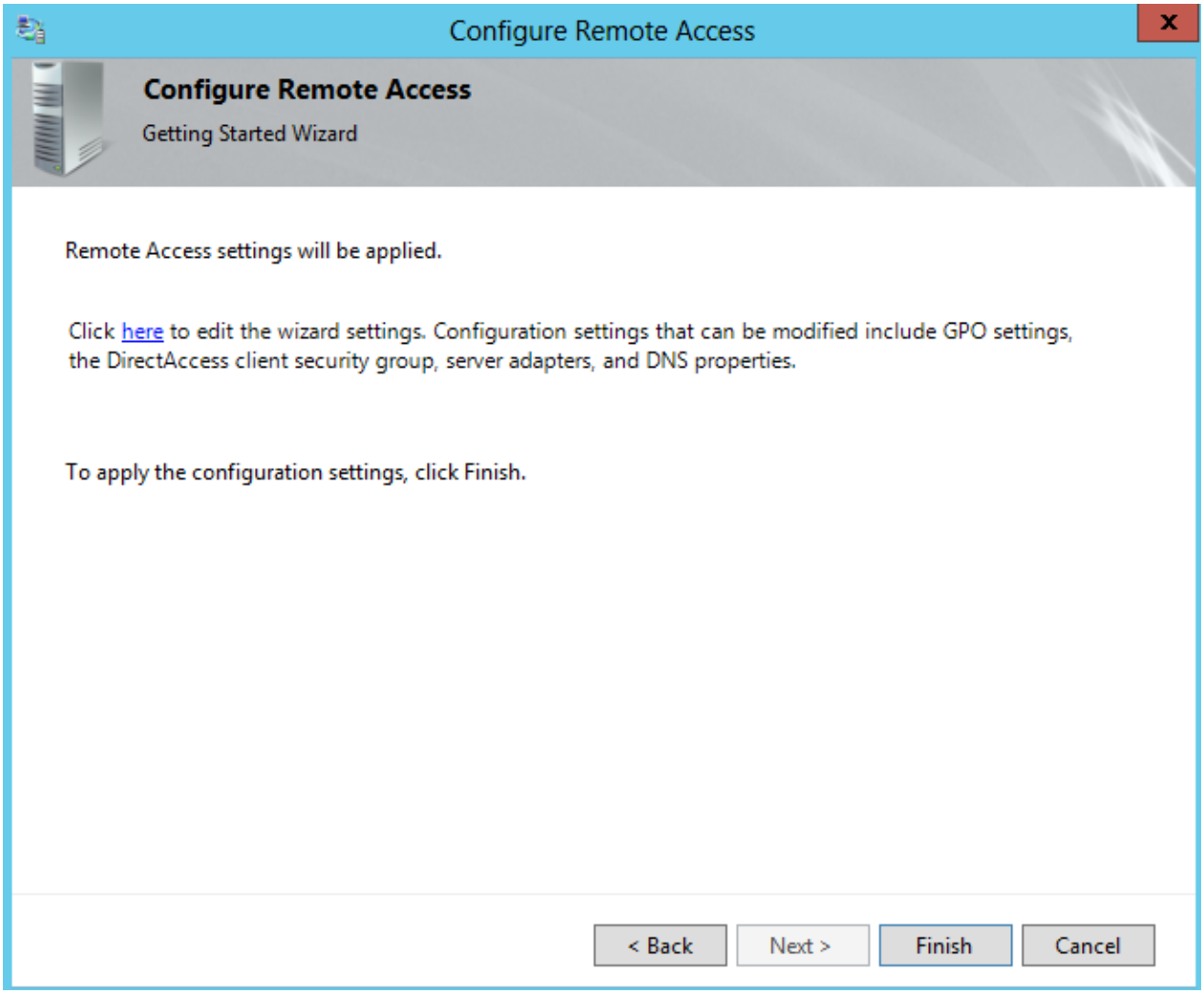

Figure 6: Edit the settings of the DirectAccess wizard

The getting started wizard has collected all required information for a successful DirectAccess deployment but I recommend to change some settings before we apply the configuration.
Leave the GPO settings unchanged.
By default Windows Server 2012 applies the DirectAccess client group policy with security filtering to the predefined user group Domain computers and makes sure that the policy only applies to mobile computers. The DirectAccess wizard creates a WMI filter to filter the scope of the DirectAccess client group policy.

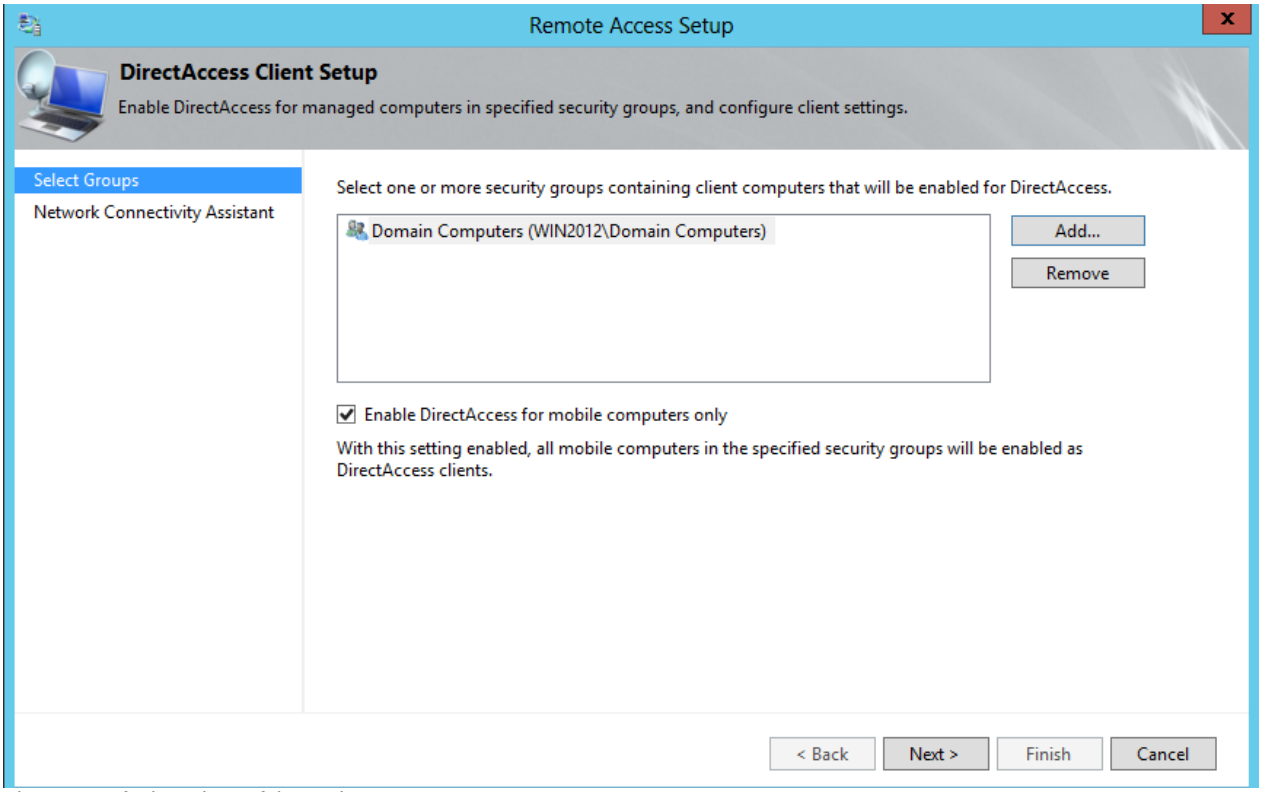

Figure 7: Default settings of the assistant

I recommend to use a special Windows group with all computer accounts which should be configured as DirectAccess clients.

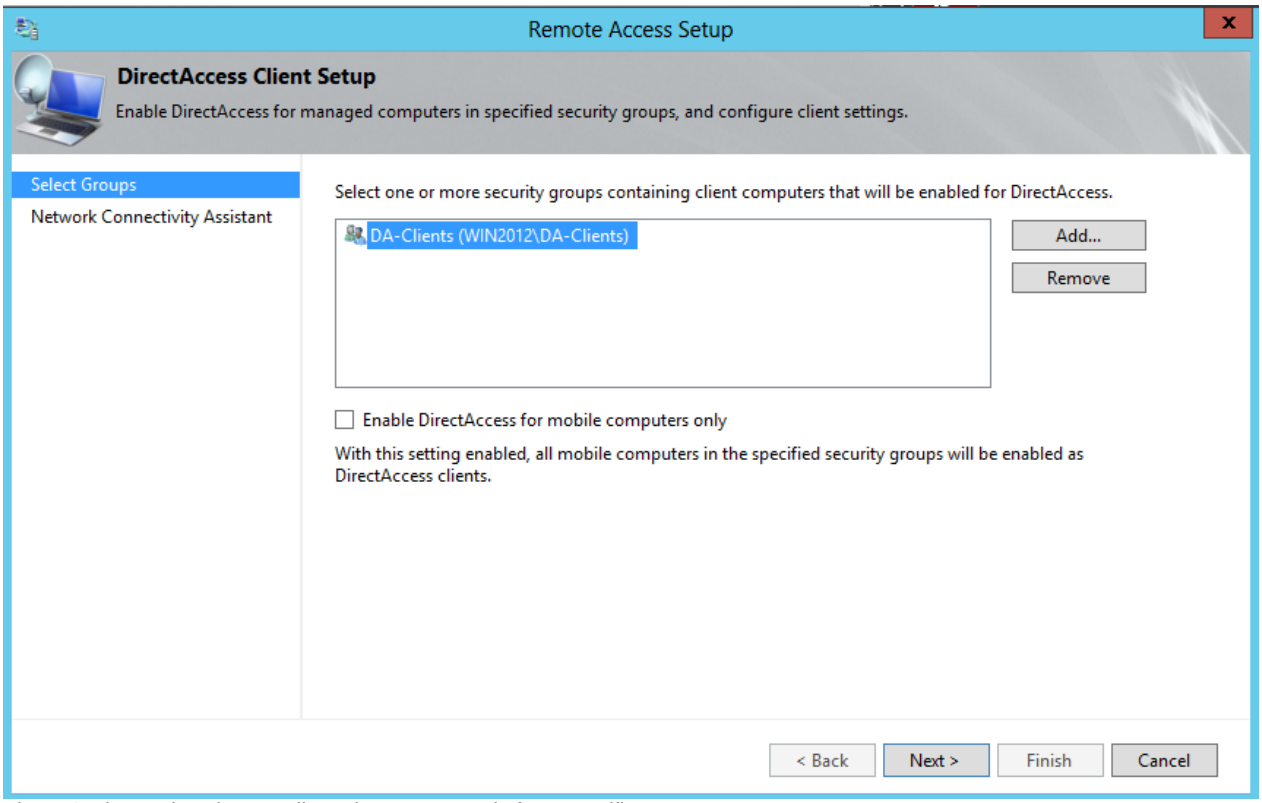

Figure 8: changed settings to allow DirectAccess only for a specific computer group

You can leave the Remote Access Server configuration unchanged. Please only note that a self signed certificate will be created.

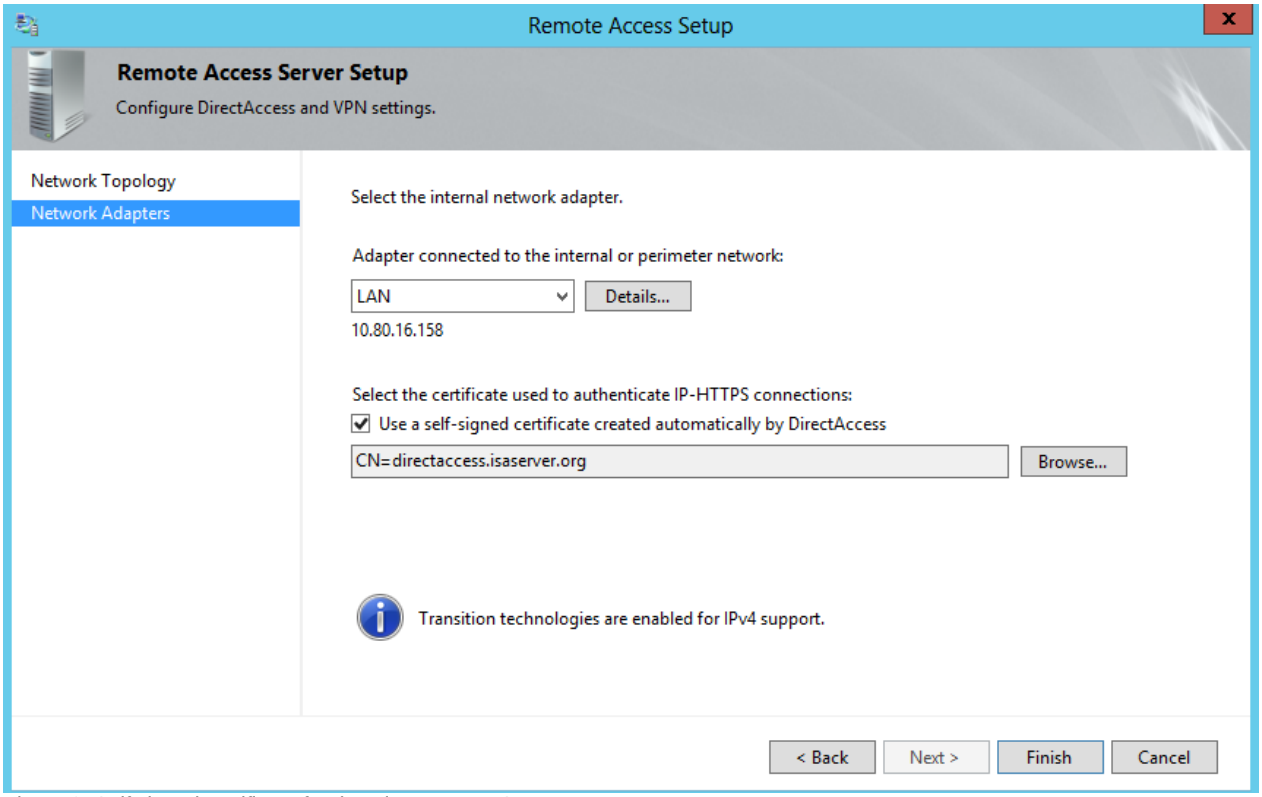

Figure 9: Self signed certificate for the DirectAccess Server

Click *Finish*.

The Windows Server 2012 DirectAccess wizard will created the required settings, group policies and certificates.

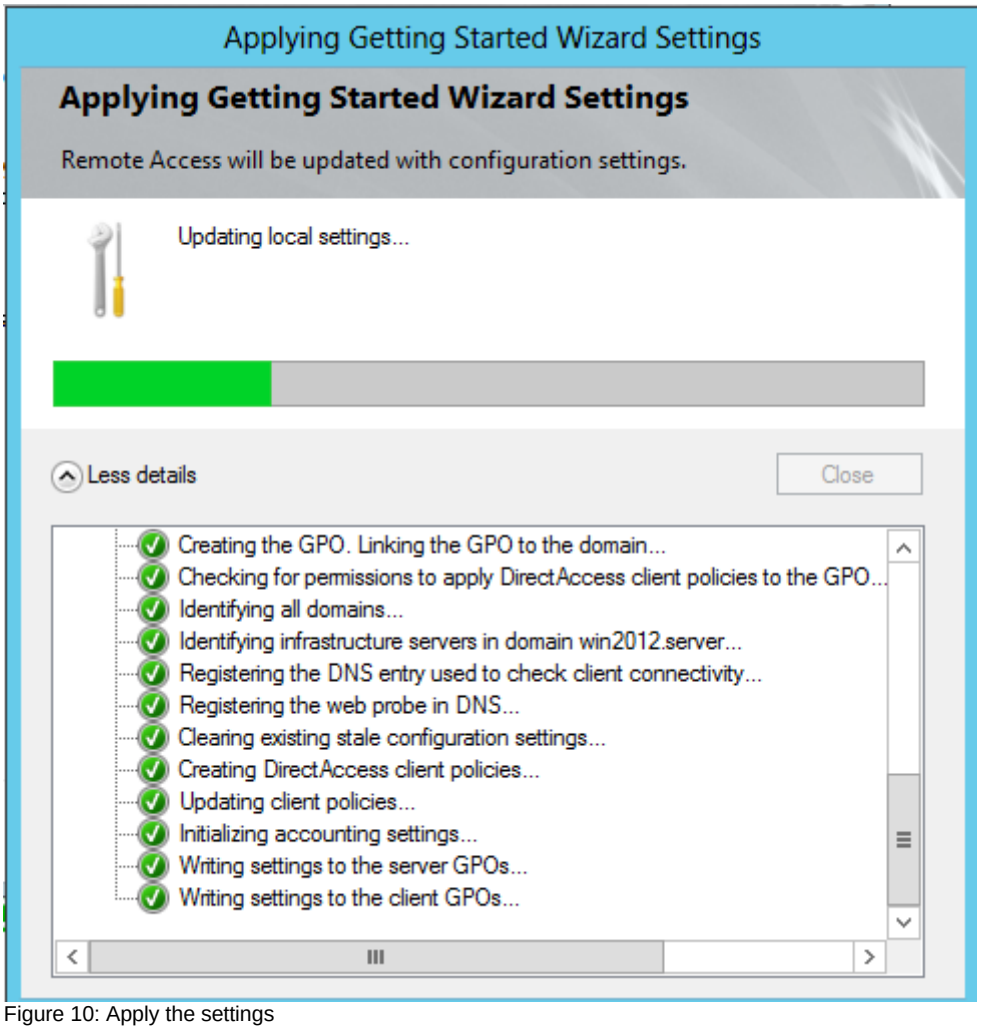

Figure 10: Apply the settings

After the configuration has been sucessfulyl created it is possible to monitor the DirectAccess configuration in the Remote Access Dashboard

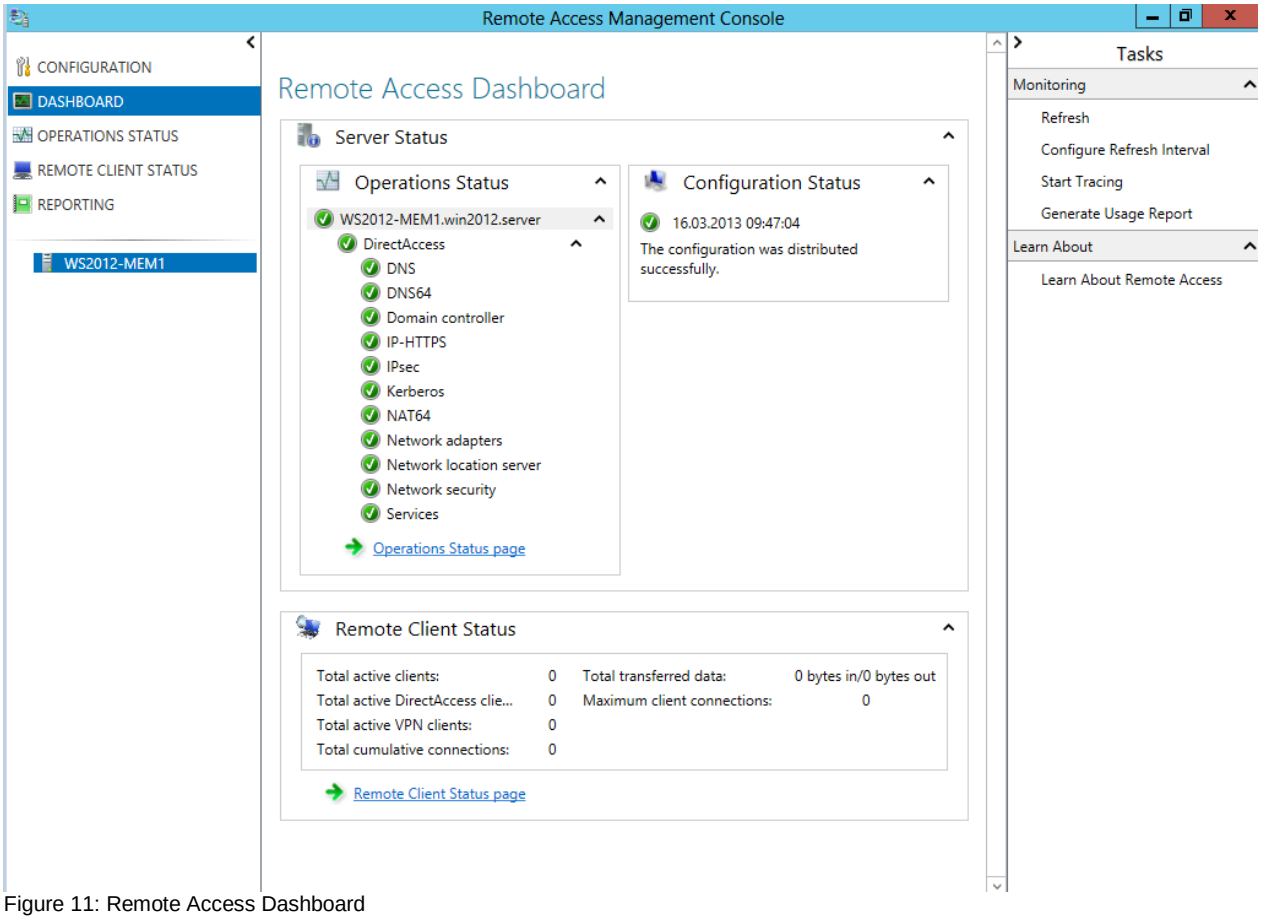

Figure 11: Remote Access Dashboard

Conclusion

In this first article we talked about the prerequisites before we are able to implement DirectAccess with Windows Server 2012 and how to configure basic DirectAccess settings with the Windows Server 2012 DirectAccess assistant. In the second article I will show 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