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

Microsoft Forefront UAG – Configuring Forefront UAG as a DirectAccess Server – Part II

Abstract

This is a three part article series.
In part I I showed you how to configure the prerequisites for using Forefront UAG as a DirectAccess Server
This article will show you how to configure Forefront UAG as a DirectAccess Server
Part III of this article series will show you how to troubleshoot DirectAccess client connections and how to monitor DirectAccess clients with Forefront UAG

Let's begin

In part I of this article series we finished installing all prerequisites for a successful Forefront UAG DirectAccess implementation. It is now time to use the Forefront UAG Management Console to enable DirectAccess for your organization.
We start with Step 1.

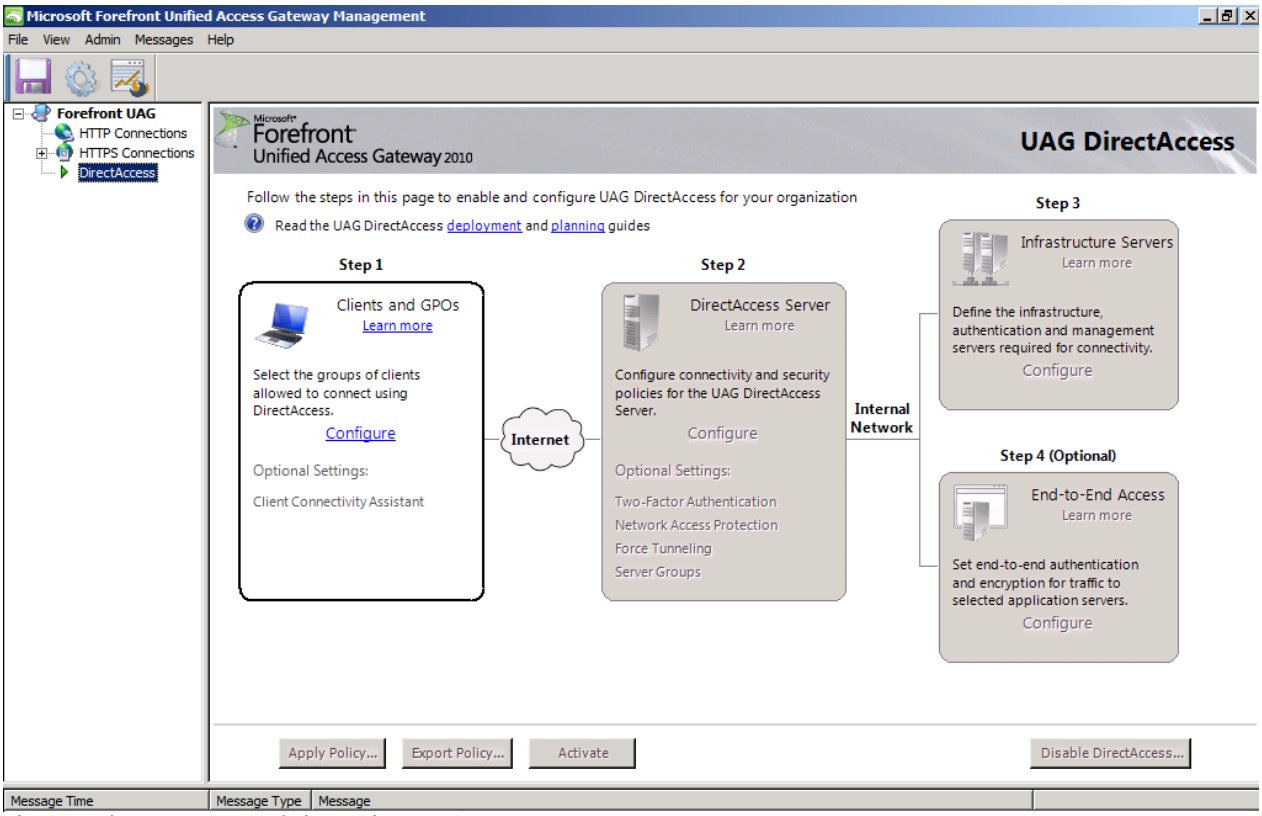

Figure 1: DirectAccess console in Forefront UAG

We want to allow DirectAccess clients to connect to corporate resources and we want to enable Remote Management of DirectAccess computers as shown in the following screenshot. As an optional step it is also possible to enable the DCA (DirectAccess Client Connectivity Assistant). The DCA installs a small software package (MSI package) on the DirectAccess client and the DCA will create a

program symbol in the task pane of the clients. The DCA reports DirectAccess client activity for the enduser and offers some additional troubleshooting steps when DirectAccess is not working as expected.

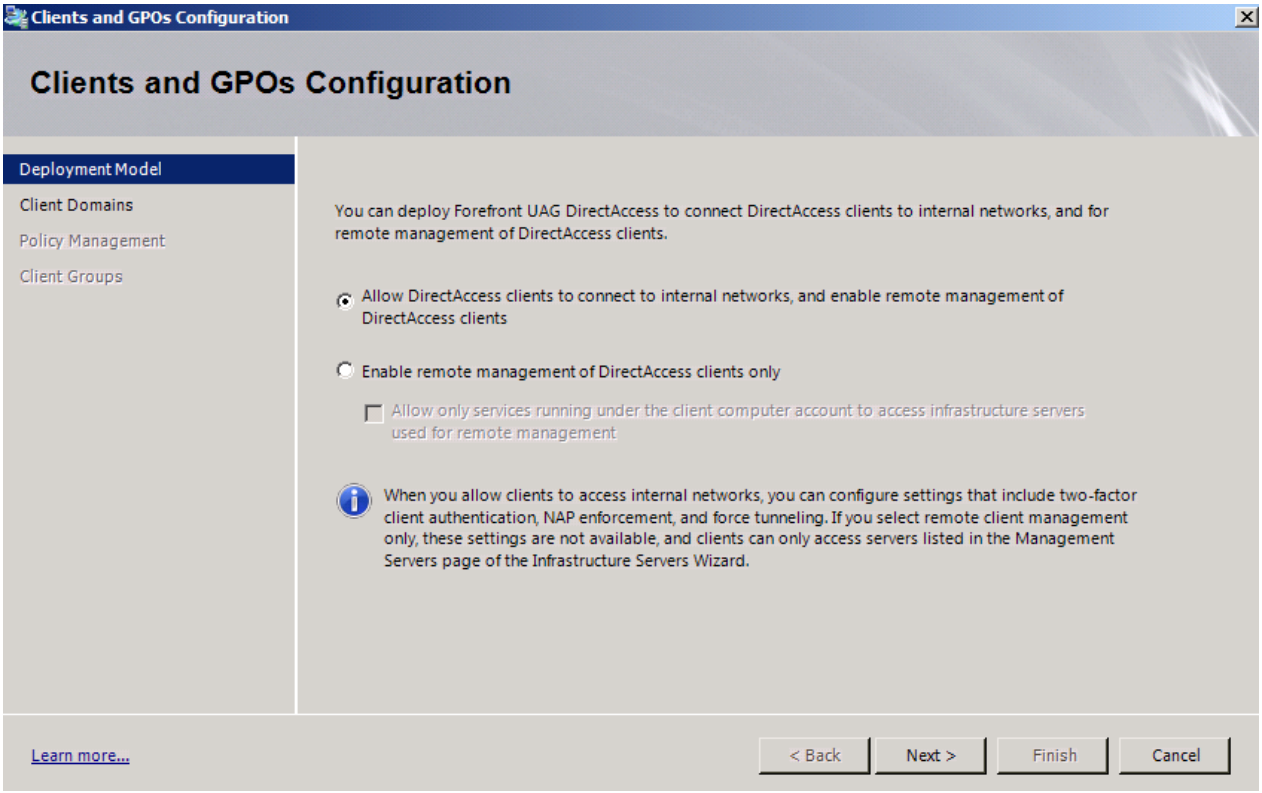

Figure 2: Enable DirectAccess to access internal resources

Enable DirectAccess for client computers in your Active Directory infrastructure and select the domain(s) for which you want to enable DirectAccess.

Forefront UAG automatically creates three group policy objects which will be linked later to the top level of the Active Directory domain and filtered via group policy security filtering. Administrators are able to modify the default settings.

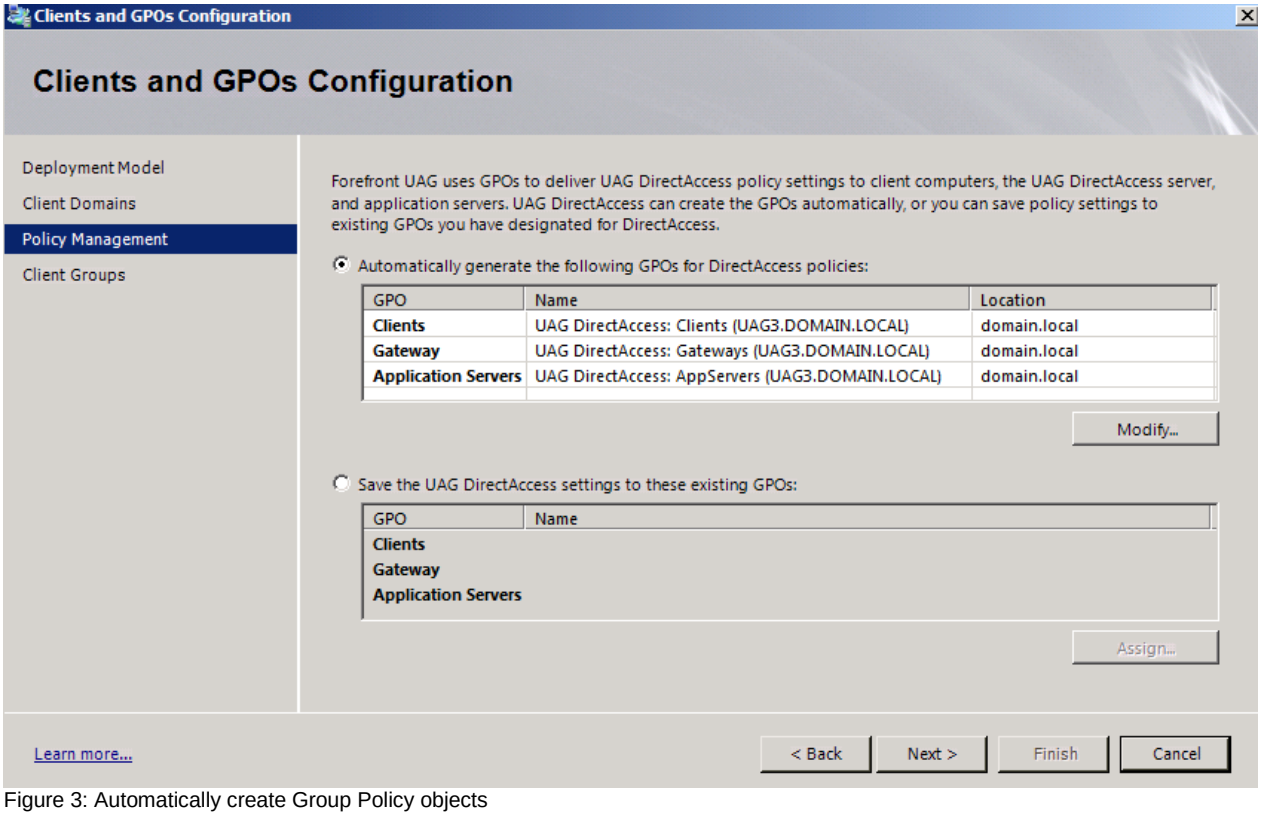

Figure 3: Automatically create Group Policy objects

It is possible to enable DirectAccess for an Active Directory security group or Organizational Units (OU). I recommend applying DirectAccess to a security group because this is more flexible.

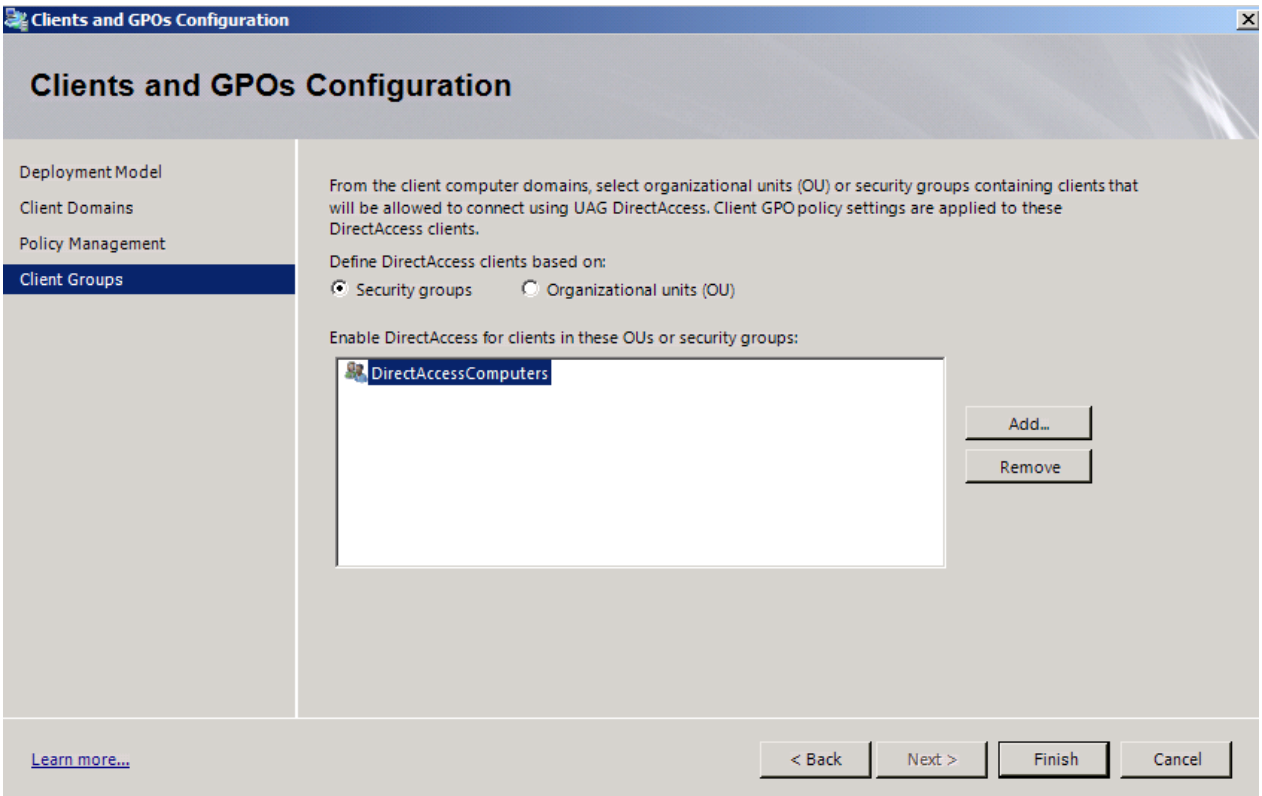

Figure 4: Enable DirectAccess for a windows group

Forefront UAG DirectAccess requires two conductive public Internet facing IPv4 addresses and for the internal IP address of the Forefront UAG Server you must create a host record with the name ISATAP in the internal DNS Forward Lookup zone of your Active Directory infrastructure. We did this in part I of this article series and also removed ISATAP from the DNS global query block list.

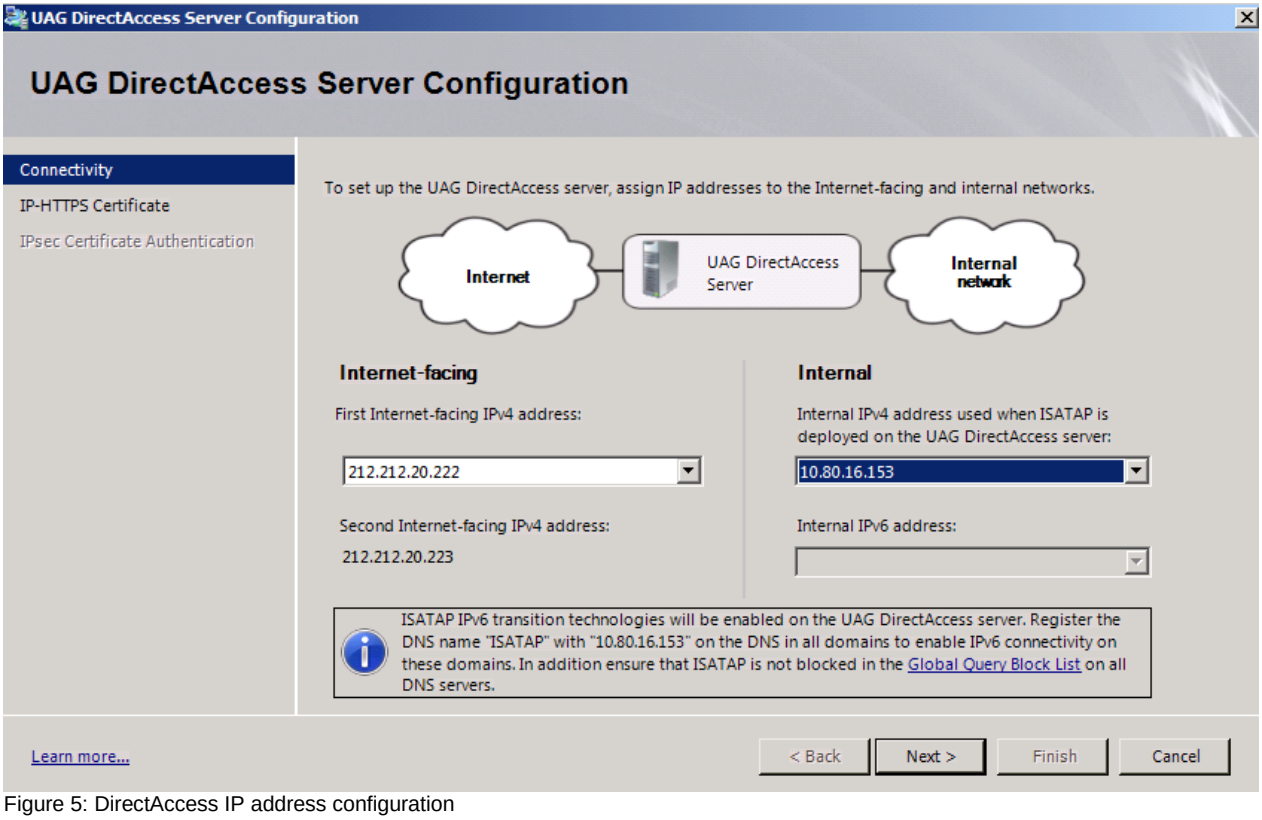

Figure 5: DirectAccess IP address configuration

Next we must select the server certificate used to authenticate DirectAccess clients. This certificate is used for IP-HTTPS the last transition technology used by a DirectAccess client when native IPv6 connectivity or a Teredo connection is not possible. Before it is possible to select this certificate in the Forefront UAG DirectAccess wizard we must request a computer certificate via the local computer certificate MMC SnapIn from the internal Certification Authority. DirectAccess clients must trust the issuing CA. This should be true when you use a Active Directory integrated CA where the Root CA certificate will be automatically distributed to every domain joined client.
The CDP (CRL Distribution Point) must be available from DirectAccess clients on the Internet. We changed the CDP of the CA and published the CDP in part I of this article series.

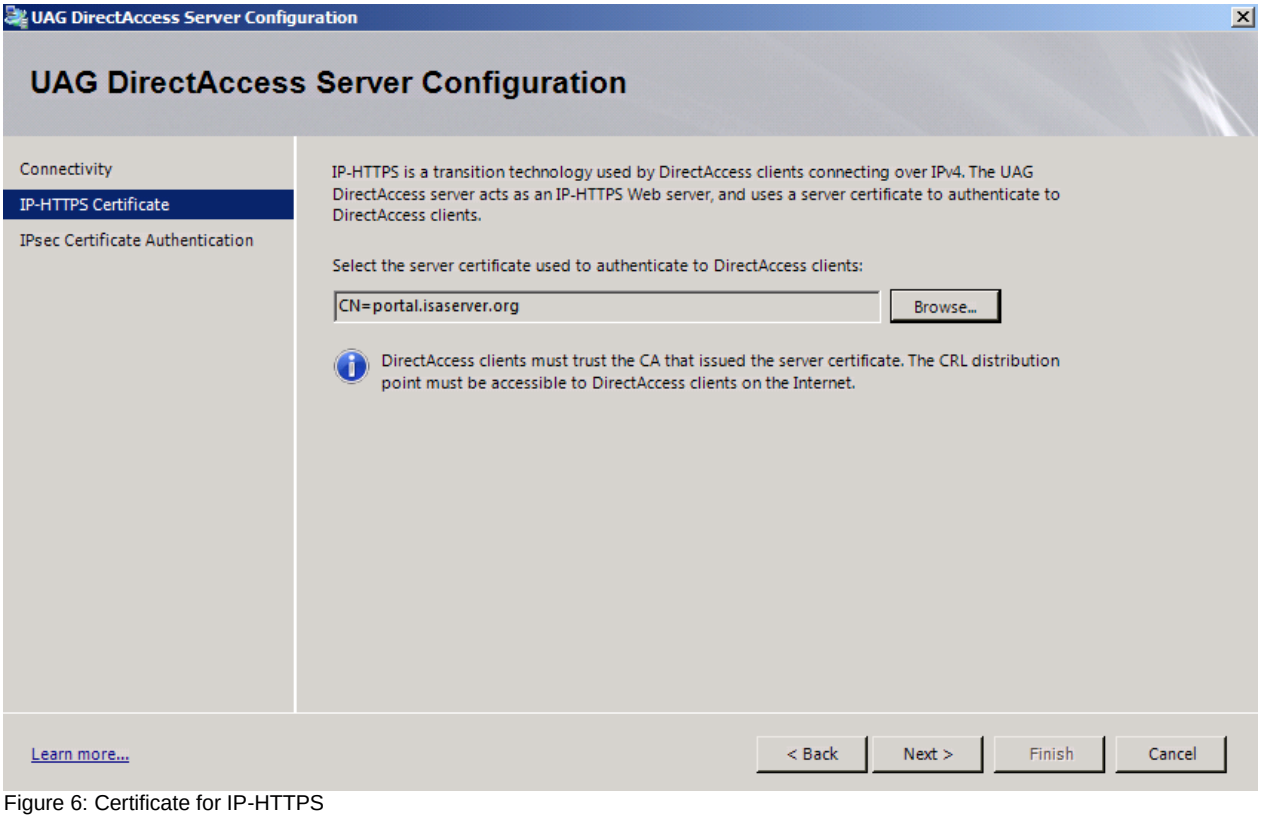

Figure 6: Certificate for IP-HTTPS

Select the CA that will issue certificates for IPsec authentication. Forefront UAG and the clients must trust the CA and the DirectAccess clients requires a computer certificate for establishing a IPsec infrastructure tunnel. We did this in part I of our article series.

One additional note: If you have a large number of DirectAccess clients it is also possible to use computer certificate autoenrollment to enroll computer certificates automatically.

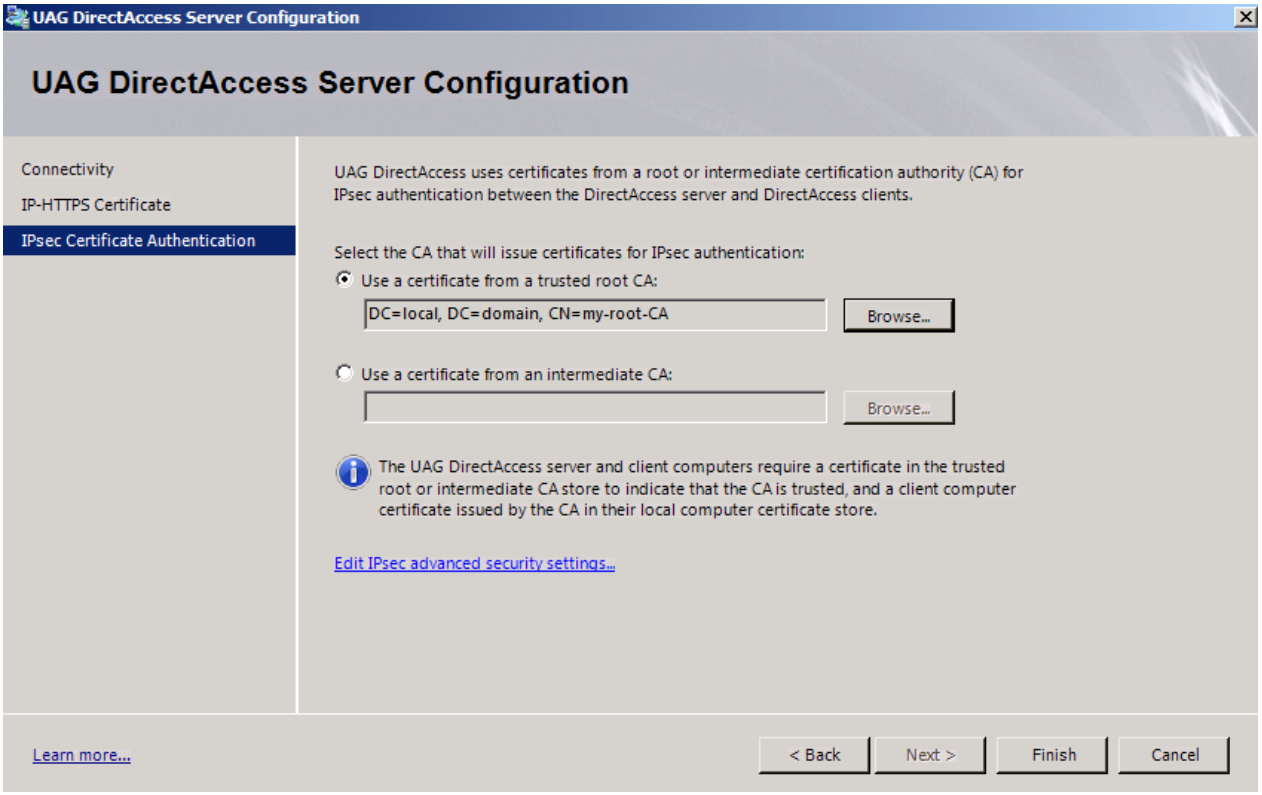

Figure 7: Specify internal Root CA

As a next step we must specify the URL used by DirectAccess clients to determine if they are connected to the corporate network or to the Internet. The NLS (Network Location Server) Server is a Web Server on the corporate network with a HTTPS binding and a Web Server certificate issued from the internal Certification Authority. We talked about the implementation of the NLS Server in part I of this article series.

Please note: The NLS Server will be excluded for access from DirectAccess clients from the Internet. So in typical environments you should use a dedicated NLS server with no required functionality from DirectAccess clients connected to the Internet.

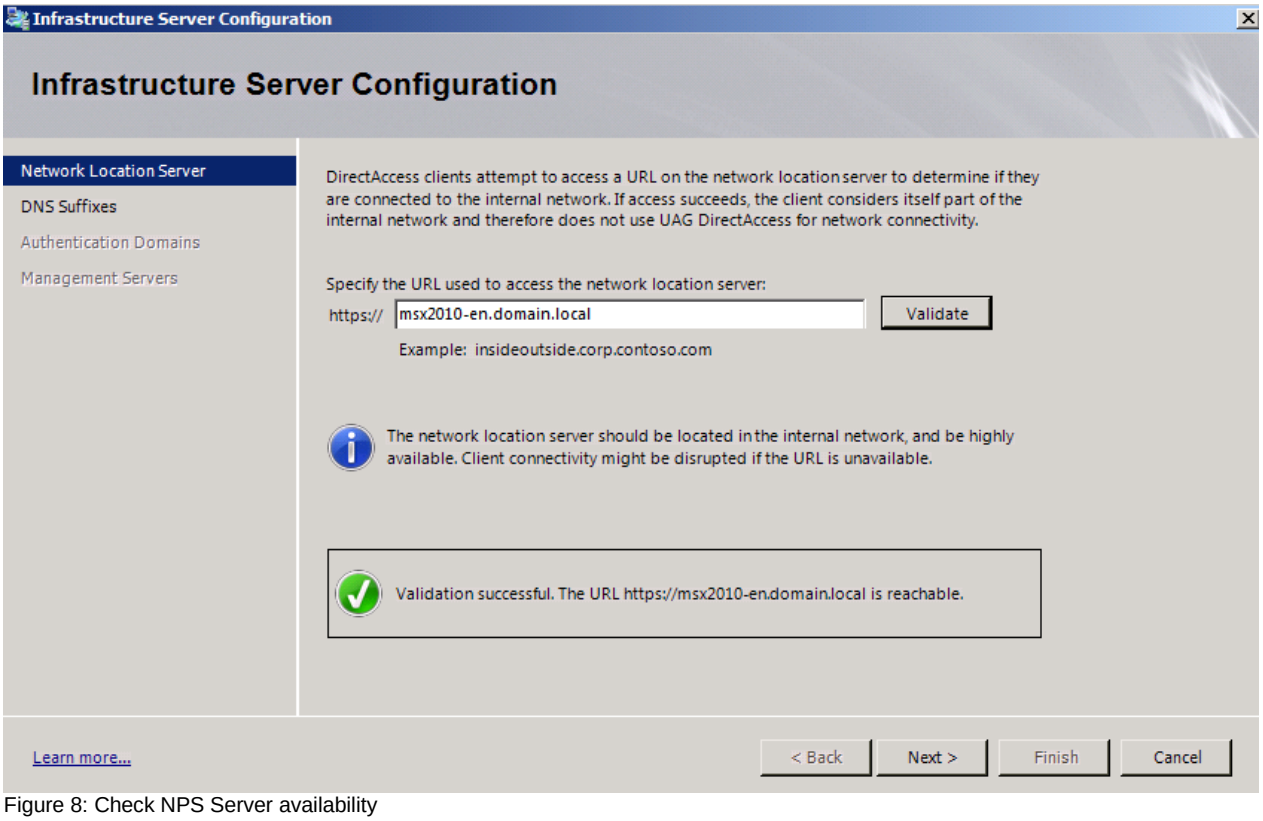

Figure 8: Check NPS Server availability

The next step is important for internal DNS name resolution for DirectAccess clients connected to the Internet. The DNS suffixes you specify here will be resolved by Forefront UAG DNS64. Forefront UAG installs its own DNS Server which is responsible for IPv4/IPv6 A and AAAA record name resolution.

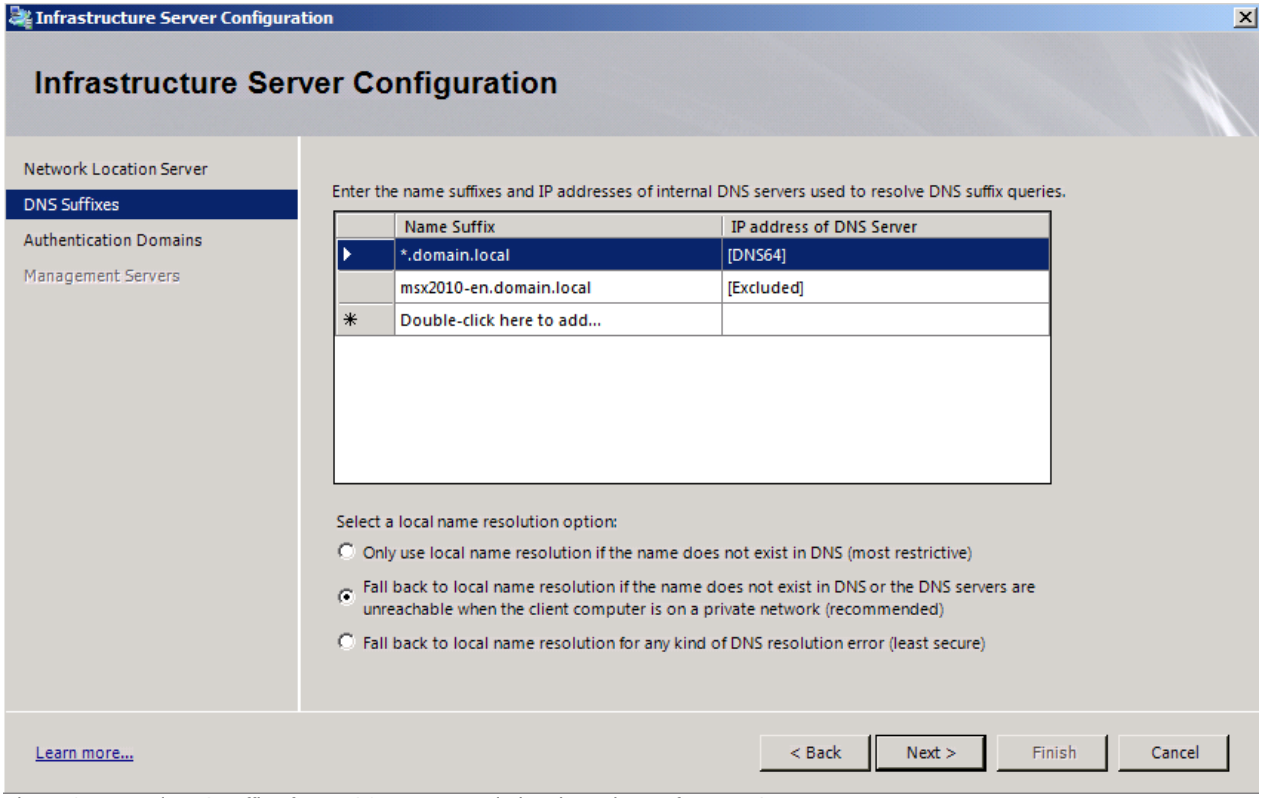

Figure 8: Internal DNS suffixe for DNS64 name resolution through Forefront UAG

We want to enable DirectAccess for the local Active Directory domain.

The next step in the Forefront UAG DirectAccess wizards allows Administrators to add internal management servers. These management servers are able to access the DirectAccess client after the first IPsec tunnel (the infrastructure tunnel) has been established.

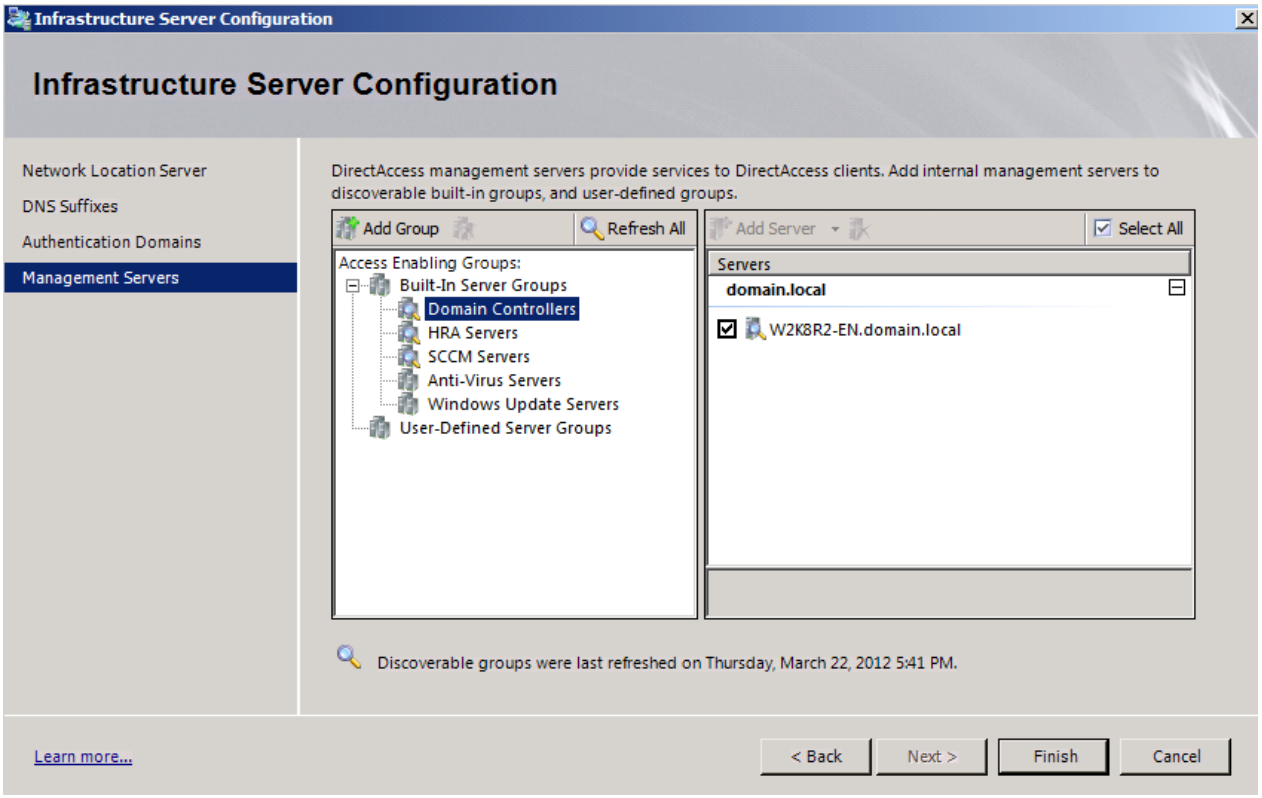

Figure 9: List of Infrastructure servers

Step 4 is a optional step and allows Administrators to setup end-to-end authentication and encryption for traffic to selected application servers.

After all configuration steps has been sucessfully configured, click Apply Policy. Forefront UAG allows you to review the configuration steps before Forefront UAG creates the group policy objects. Please check the settings carefully before you apply the configuration.

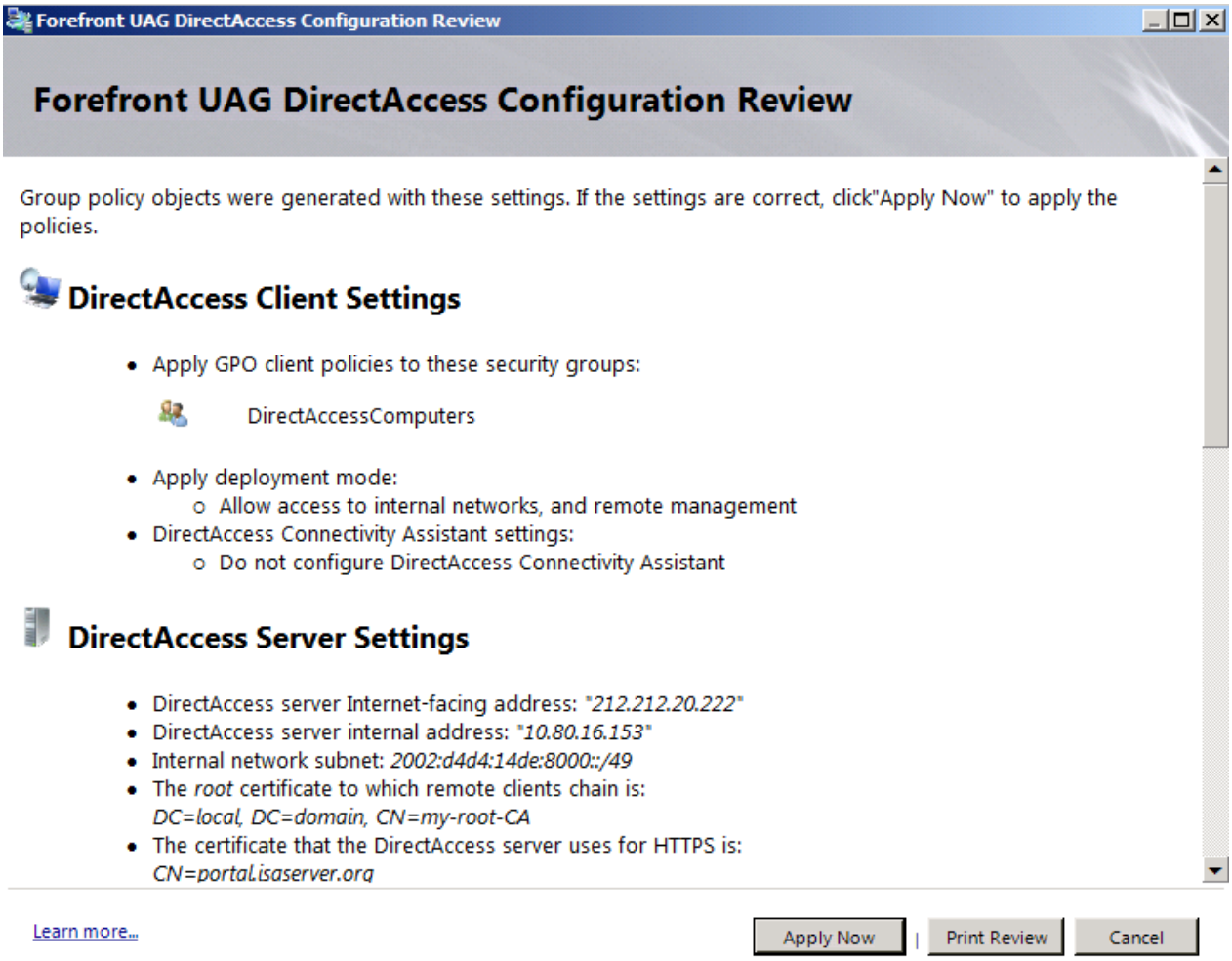

Figure 10: Group policy settings created by the DirectAccess wizard

Click Apply Now.

Forefront UAG now creates the group policy objects in Active Directory. If the Forefront UAG Server has not the required permissions to create group policy objects you are able to export the settings to a script and a other user with appropriate Active Directory permissions can use the Windows PowerShell to create the group policy objects with the script created earlier.

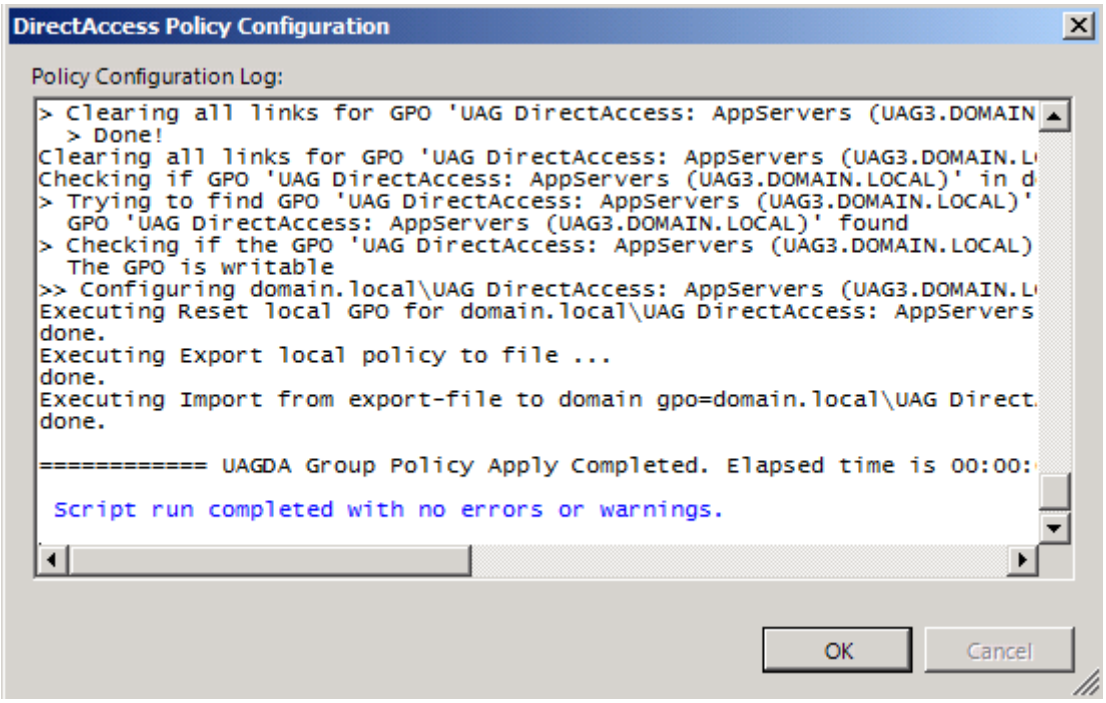

Figure 11: Group policy script creation

Click Activate to activate the DirectAccess configuration on the Forefront UAG Server. Forefront UAG now takes some configuration changes and activates for example its own DNS64/NAT64 services.

If you want to backup the Forefront UAG configuration before you activate the configuration, enable the appropriate checkbox.

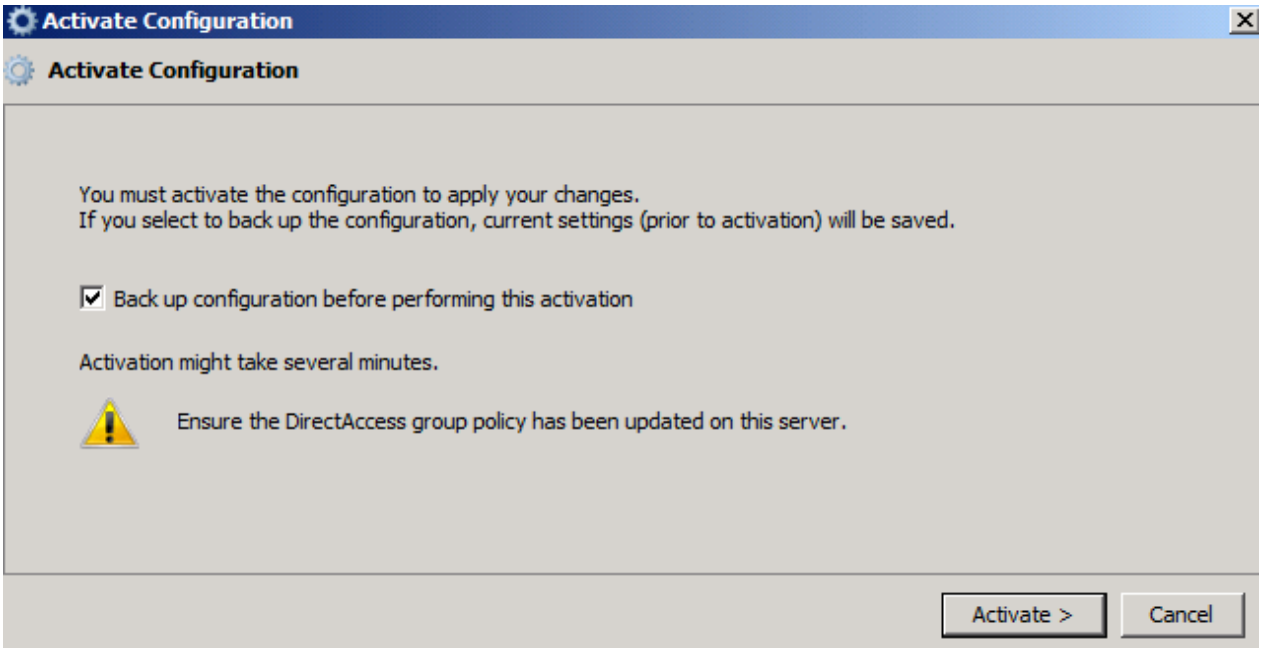

Figure 12: DirectAccess activation and backup

After the activation was successful check the group policy objects created by Forefront UAG. Start the group policy management console on the Forefront UAG Server or a Active Directory domain controller and locate the DirectAccess group policy objects.

Tip: For a better understanding how DirectAccess works it is very helpful to become familiar with the different group policy settings.

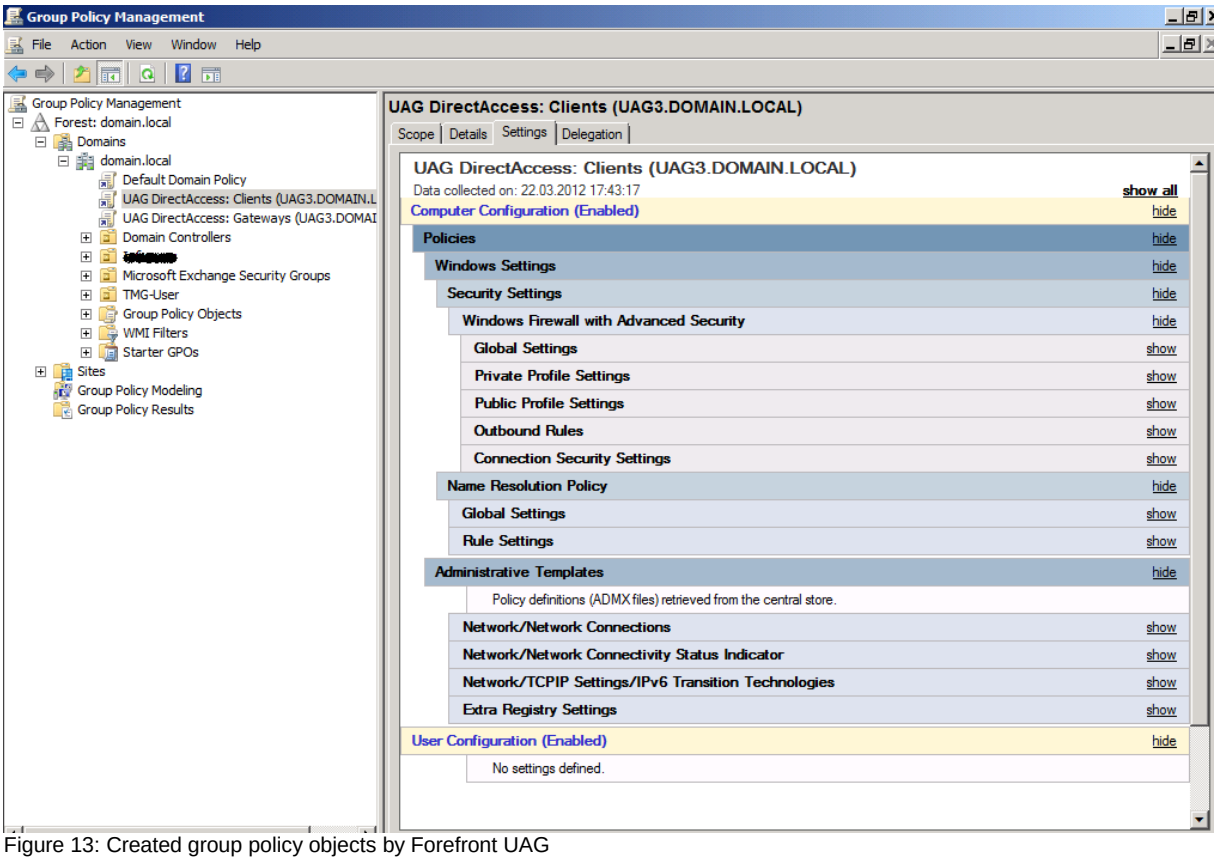

Figure 13: Created group policy objects by Forefront UAG

The last step is to apply the group policy named “UAG DirectAccess: Clients” to the DirectAccess Notebook. Connect the Notebook to the corporate network and run a GPUPDATE /force from the command line, reboot the machine and check if the DirectAccess group policy has been successfully applied to the client. After that, disconnect the client from the corporate network, enable access to a public ISP (Internet Service Provider) and test if the Notebook can access corporate network resources. If the connection was not successful or if you want to monitor DirectAccess clients connected to the Forefront UAG Server, you should read part III of this article series.

Conclusion

In this second article we walked through the activation of DirectAccess in Forefront UAG. I tried to show you the necessary steps for a successful DirectAccess implementation with Forefront UAG. In part III of this article series I will show you how to monitor and troubleshoot DirectAccess connection on the client side and with the help of Forefront UAG.

Related links

Forefront UAG DirectAccess deployment guide
http://technet.microsoft.com/en-us/library/dd857320.aspx
Forefront UAG DirectAccess planning guide
http://technet.microsoft.com/en-us/library/ee406191.aspx

Forefront UAG DirectAccess technical overview
http://technet.microsoft.com/en-us/library/ee809094.aspx
Secure CDP publishing with Forefront TMG and the HTTP-filter
http://www.isaserver.org/tutorials/Secure-CDP-publishing-Forefront-TMG-HTTP-filter.html
Planning CAs and certificates for Forefront UAG DirectAccess SP1
http://technet.microsoft.com/en-us/library/gg502563.aspx
Microsoft Forefront UAG – Overview of Microsoft Forefront UAG
http://www.isaserver.org/tutorials/Microsoft-Forefront-UAG-Overview-Microsoft-Forefront-UAG.html
Forefront UAG technical overview
http://technet.microsoft.com/en-us/library/ee690443.aspx