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

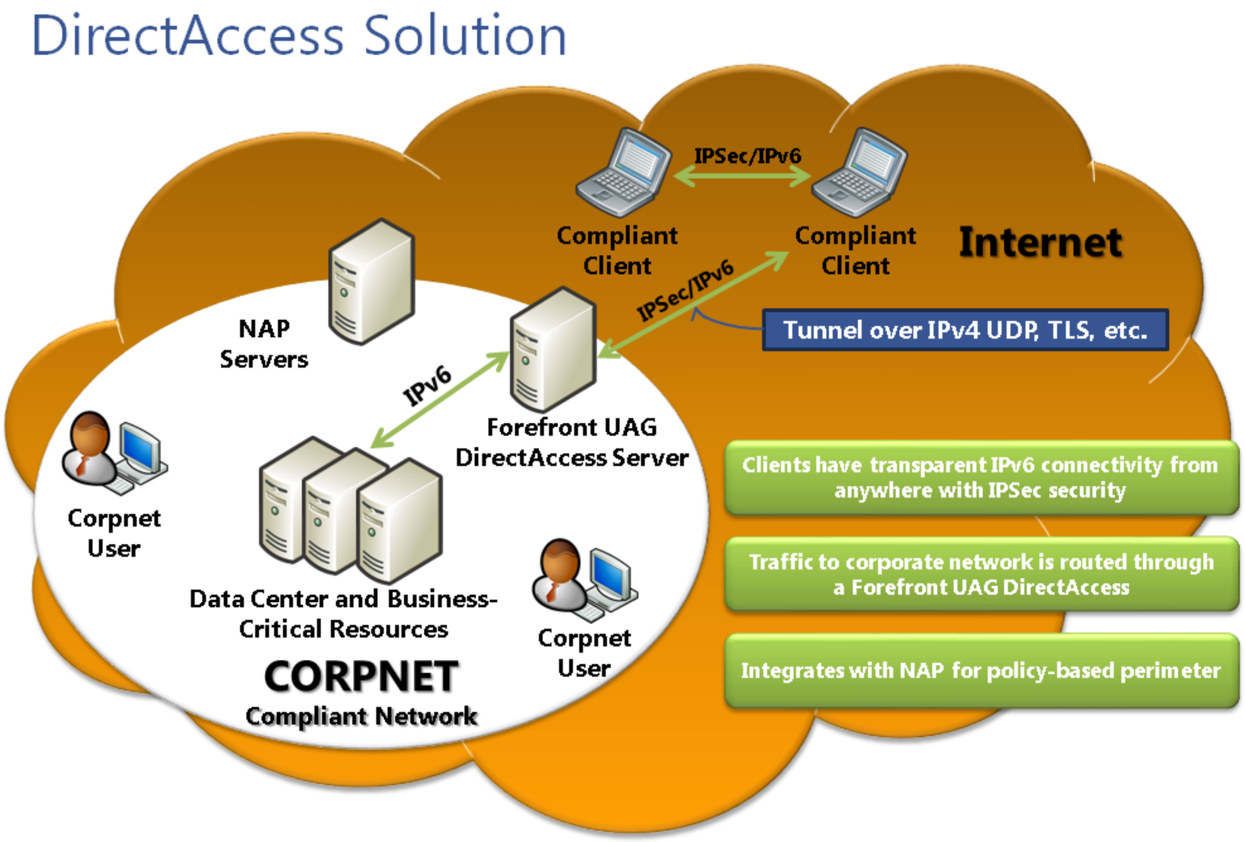
Microsoft Forefront UAG – Configuring Forefront UAG as a DirectAccess Server – Part I

Abstract

This is a three part article series.
In part I I will show you how to configure the prerequisites for using Forefront UAG as a DirectAccess Server
Part II 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

DirectAccess is a new feature which is built into Windows Server 2008 R2 and Windows 7 Ultimate and Enterprise. 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 Solution

Clients have transparent IPv6 connectivity from anywhere with IPSec security

Traffic to corporate network is routed through a Forefront UAG DirectAccess

Integrates with NAP for policy-based perimeter

Figure 1: DirectAccess overview (Source: MOC - 50402A-ENU_Module08.pptx)

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 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).

DirectAccess server

A domain-joined computer running Windows Server 2008 R2 or in this article series with Forefront UAG on top 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, Forefront UAG translates the incoming IPv6 traffic to IPv4 using NAT64/DNS64.

NAP Server

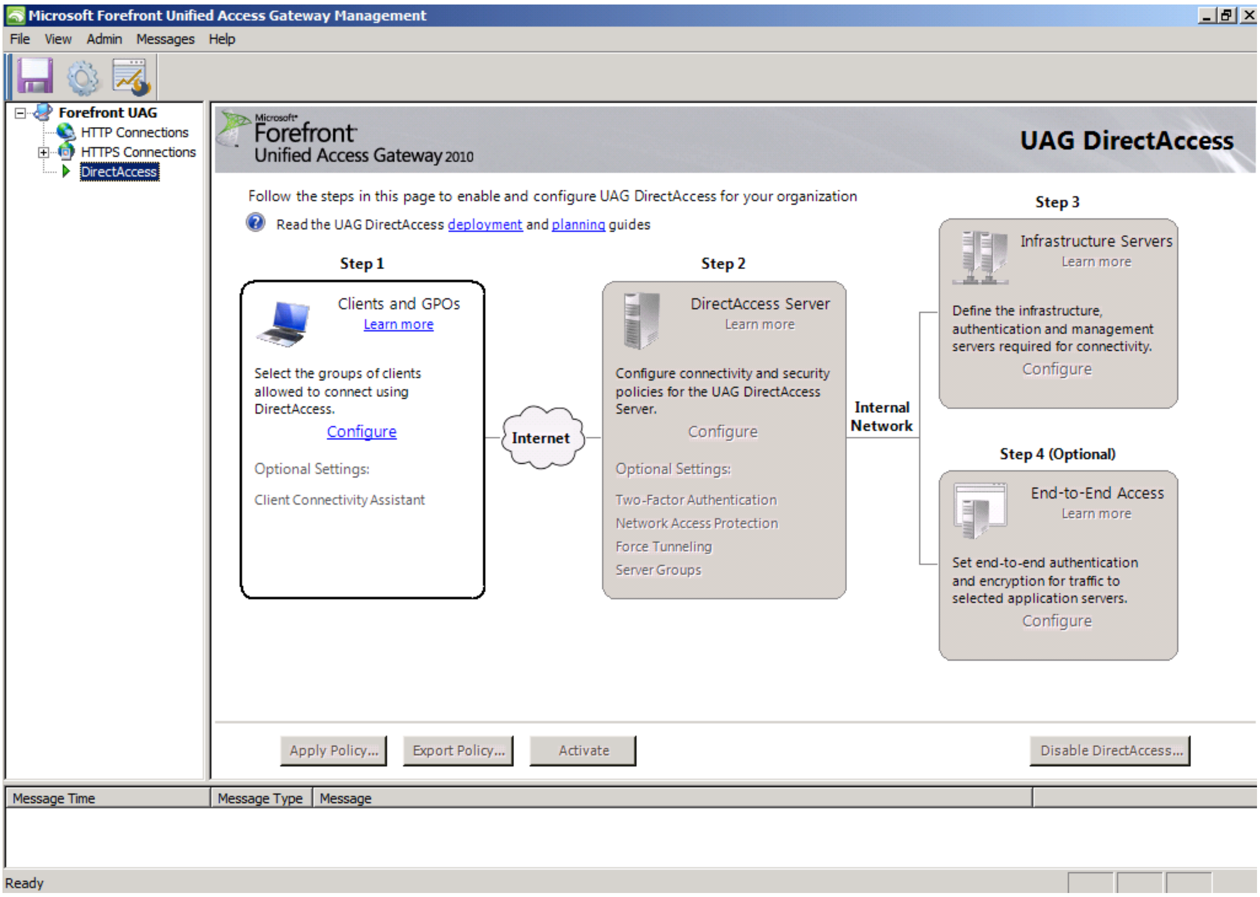
You can use Network Access Protection (NAP) as an optional component for DirectAccess clients which connect to the internal network through Forefront UAG.

DirectAccess console in Forefront UAG

On a first view the DirectAccess Management console in Forefront UAG looks like the same which comes with Windows Server 2008 R2, but there are some important differences. I will show you the differences and how to configure DirectAccess with Forefront UAG in part II of this article series.

Please note:

You should walk through the DirectAccess wizard after all prerequisites has been fulfilled. If not all prerequisites has been fulfilled DirectAccess will NOT be functional when the wizard has been finished.



Follow the steps in this page to enable and configure UAG DirectAccess for your organization

Read the UAG DirectAccess deployment and planning guides

Step 1 – Clients and GPOs: Select the groups of clients allowed to connect using DirectAccess.

Step 2 – DirectAccess Server: Configure connectivity and security policies for the UAG DirectAccess Server.

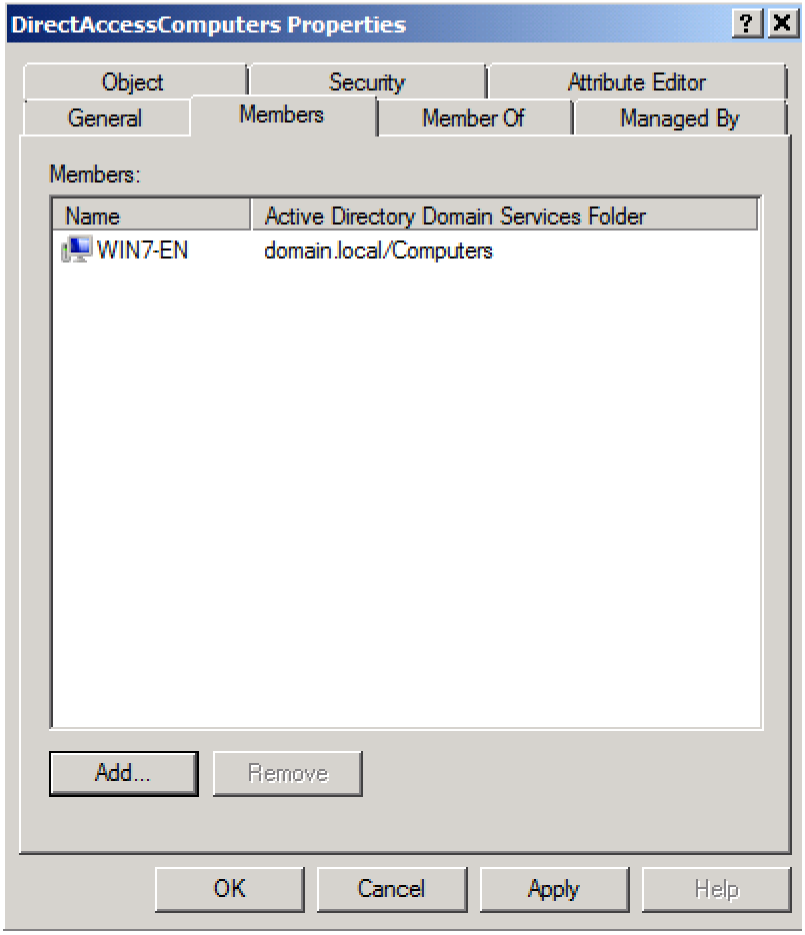
Step 3 – Infrastructure Servers: Define the infrastructure, authentication and management servers required for connectivity.

Step 4 (Optional) – End-to-End Access: Set end-to-end authentication and encryption for traffic to selected application servers.

Figure 2: DirectAccess wizard in Forefront UAG

Active Directory requirements

The Active Directory requirements are relative simple. Forefront UAG creates group policies for DirectAccess clients who can be associated via group policy security filtering to a Windows group or an Active Directory Organizational Unit (OU). In most of my DirectAccess implementations we used a global windows group which contains all Windows 7 Notebooks which should be enabled for DirectAccess. The Forefront UAG DirectAccess wizard creates the required group policy objects. The group policy for DirectAccess clients will be linked to the top level of the Active Directory domain with group policy security filtering for the specified windows group.



Members:

Name	Active Directory Domain Services Folder
WIN7-EN	domain.local/Computers

Figure 3: Active Directory user group for DirectAccess Notebooks

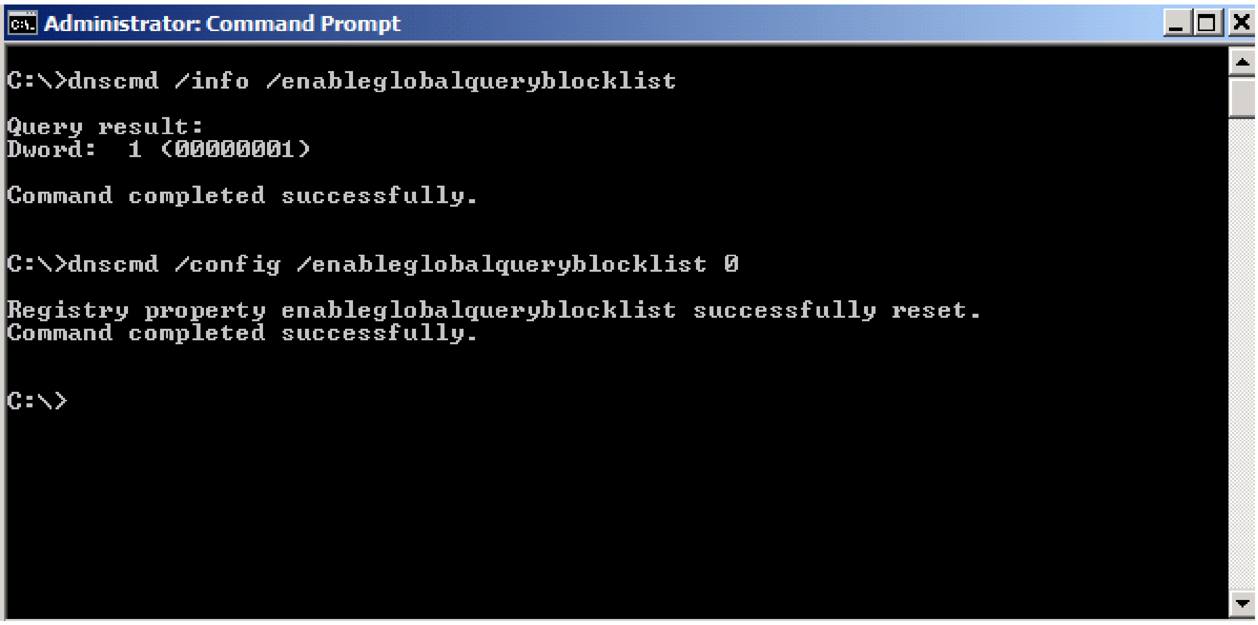
DNS Server requirements

First we must create a new host record with the name ISATAP in the internal DNS forward lookup zone of your Active Directory for which DirectAccess should be enabled. The ISATAP host record must be associated with the internal IP address of the Forefront UAG Server.

A Windows Server 2008 and higher DNS Server doesn’t answer requests for the following names: ISATAP and WPAD. Because DirectAccess uses ISATAP (Intra Site Automatic Tunnel Addressing Protocol) as an IPv6 transition technology for internal clients and Servers you must remove ISATAP from the global DNS query blocklist. After ISATAP has been removed from the blocklist all IPv6 capable Windows clients and Servers will activate their ISATAP interface and register an IPv6 IP address with the internal DNS Server. This IP address will be used for communication between these clients and servers to the DirectAccess client.

Please note: If you do not want to globally activate ISATAP on all clients and Servers it is also possible to create an ISATAP record with the IP address of the

Forefront UAG Server in the local HOSTS file on the client/server. The following screenshot tells you how to disable the DNS global query blocklist.



```
C:\>dnscmd /info /enableglobalqueryblocklist

Query result:
Dword:  1 (00000001)

Command completed successfully.


C:\>dnscmd /config /enableglobalqueryblocklist 0

Registry property enableglobalqueryblocklist successfully reset.
Command completed successfully.


C:\>
```

Figure 4: Disable the DNS global query blocklist

Certificate Authority

A Forefront UAG DirectAccess deployment requires the following certificates:

DirectAccess client computer

Each DirectAccess client computer requires a computer certificate that is used for establishing the IPSEC tunnel between the client and the Forefront UAG Server and when IP-HTTPS is used to connect the DirectAccess client to the Forefront UAG Server if other IPV6/IPv4 transition technologies cannot be used due to limitations or restriction in the public network infrastructure.

DirectAccess server

The DirectAccess server requires a computer certificate to establish IPsec connections with DirectAccess client computers.

IP-HTTPS server

IP-HTTPS is an IPv6 transition technology that enables DirectAccess clients to connect to the DirectAccess server over the IPv4 Internet. Forefront UAG acts as an IP-HTTPS Web Server. The IP-HTTPS website requires a Webserver certificate, and DirectAccess clients must be able to download the certificate revocation list (CRL) for the certificate.

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. A DirectAccess client must be able to download the CRL for the certificate issued to the NLS Server from the internal Certificate Authority.

Network Access Protection (NAP)

NAP is an optional component in Forefront UAG 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.

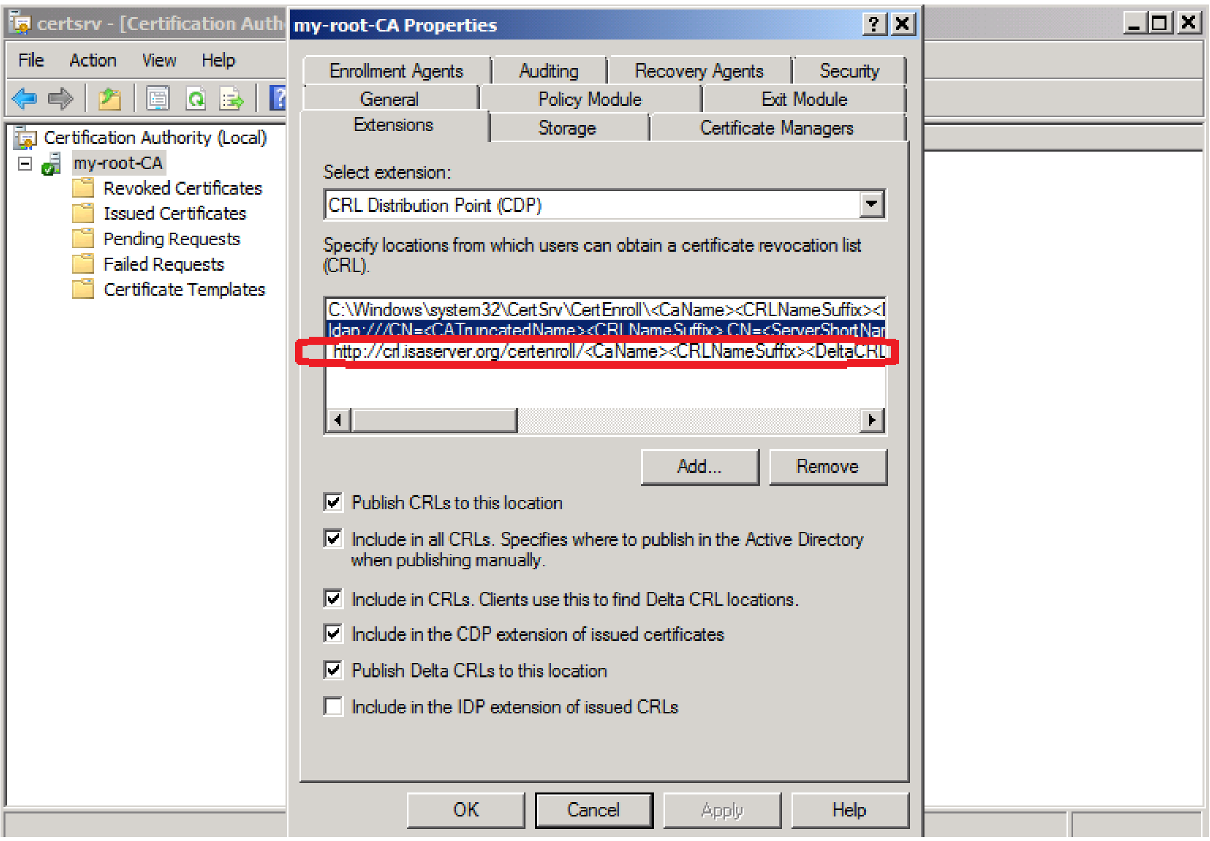
OTP authentication

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

Smartcard authentication

You can optionally implement two-factor authentication with smartcards

For all these certificate requirements it is recommended using an internal Active Directory integrated Certificate Authority.
If you use an internal Certificate Authority (CA), the CA will also publish a CRL (Certificate Revocation List). A DirectAccess client must have access to the CRL when the client is connected to the Internet to check the certificate for revocation when the IPSEC tunnel should be established or when IP-HTTPS as the last resort for IP46/IPv4 transition must be used. Because the default CDP (CRL Distribution Point) for HTTP is only available from internal clients we must extend the CA with a CRL with a public DNS name which is accessible from the Internet. To extend the CDP start the Certificate Authority Management Console, navigate to the properties of the CA and add an additional CDP from type HTTP as shown in the following screenshot.



Select extension:

CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><I
ldap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortNar
http://crl.isaserver.org/certenroll/<CaName><CRLNameSuffix><DeltaCRL

☑ Publish CRLs to this location

☑ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

☑ Include in CRLs. Clients use this to find Delta CRL locations.

☑ Include in the CDP extension of issued certificates

☑ Publish Delta CRLs to this location

☐ Include in the IDP extension of issued CRLs

Figure 5: Add the public hostname for the CRL access to the CA

CRL publish

After the CA has been extended with a new public available CDP for HTTP we must create a solution which gives clients from the Internet access to the CDP. There are two common ways to do this. You can use Forefront TMG or Forefront UAG to publish the CRL.
For more information how to publish the CRL with Forefront TMG read this following article.
For more information how to publish the CRL with Forefront UAG read this following article.

Network Location Server (NLS)

The Network Location Server (NLS) is a Webserver with a HTTPS binding and a certificate issued from your internal CA which is used by DirectAccess clients to determine if they are connected to the corporate network or to the Internet. If the client cannot reach the HTTPS URL of the NLS Server the client activates its DirectAccess configuration and tries to establish a DirectAccess IPSEC connection over Forefront UAG with the internal network. Because of the importance for a reachable NLS Server, Microsoft recommends to provide fault tolerance for the NLS Server. For example you can use Network Load Balancing or virtualization to provide high availability.
The configuration of a NLS Server is quite simple. Install a Windows Server / client with the IIS (Internet Information Server) role and issue a Webserver certificate for the NLS Server from your internal CA and add a HTTPS binding to the default website with the certificate issued previously.

Conclusion

In this first article we talked about the prerequisites before we are able to implement DirectAccess with Forefront UAG. I showed you how to configure your internal Certification Authority, how to publish the Certificate Revocation List. We also removed ISATAP from the DNS Global Query Blocklist, created a host record for ISATAP and we created the required Active Directory group with DirectAccess clients.

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