Introduction to UAG DirectAccess - Part 1

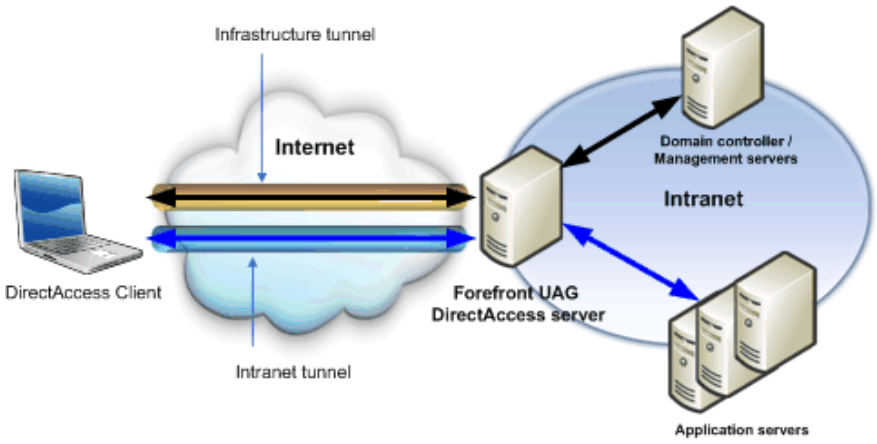
In this article we will provide an overview of what DirectAccess can do and the values ??it provides for both administrators and users.

Network Management - In this article we will provide an overview of what DirectAccess can do and the values ??it provides for both administrators and users.

DirectAccess is a new remote access technique available in Windows 7 and Windows Server 2008 R2, which allows users to connect to the corporate network at any time. From the user's point of view, the experience they have is exactly the same without being dependent on the connection location. Users can move from the corporate network to a network of a hotel, a cafe or a conference center that provides wireless connectivity. Once connected to the Internet, they can access resources on the local network, as if they are accessing those resources directly via an Ethernet connection or 802.11 wireless connection.

The ' *always-on* ' aspect of DirectAccess is arguably the most important part of this solution. Users do not need to initiate a VPN connection; They do not need to remember the URL of SSL VPN gateway (even SSL VPN gateway is a UAG server). They don't need to do anything - just click the links in the email or on the desktop or type in the name of the server you want to use, then make the connection. Such a seamless connection will certainly yield productivity.

However, DirectAccess provides more than what was introduced above. Because the DirectAccess connection is a two-way link, you - the network administrator - will be able to connect to DirectAccess clients over the Internet. Whenever a DirectAccess client is enabled, you can connect and manage this client. Users do not need to log in so you can connect to DirectAccess clients from within the corporate network. This means that the management infrastructure you use to control and configure hosts on the corporate network will always be available to the management of the connected computers. connect via DirectAccess.



How does DirectAccess work?

Along with DirectAccess, Windows 7 and Windows Server 2008 R2 users will meet some of the new technologies of these operating systems. Some of these technologies may be new, some may have been known for a long time. Even so, whether they're working with old or new technology, they're not all that complicated. It is important to avoid the notion that DirectAccess is not worth the complexity that users must attempt to overcome.

This perception is because before UAG 2010 was released, the only way to deploy DirectAccess was to use the included Windows DirectAccess solution. This solution has some limitations compared to UAG DirectAccess's solution:

- Windows DirectAccess supports high availability constraints, the common mechanism involved in using Hyper-V and Windows failover clusters to provide good *stand-by* capability. There is also no support for network load balancing (Network Load Balancing).
- Windows DirectAccess does not support DirectAccess arrays. If you want to set up multiple Windows DirectAccess servers, you need to configure and manage them separately. In contrast, UAG DirectAccess servers can be configured in arrays.
- Windows DirectAccess server does not support servers that only support IPv4 (IPv4 only). DirectAccess clients on the Internet also cannot connect to these servers. That means that, if you want to use the Windows DirectAccess solution, you need to upgrade your servers to Windows Server 2008 or later. In contrast, the UAG DirectAccess solution fully supports IPv4 servers in the corporate network.

If you plan to deploy DirectAccess on your corporate network, the best way to do that is to use the UAG DirectAccess solution.

Connect the DirectAccess client

IPv6 is still the core of the DirectAccess solution, which is one of the reasons many administrators have a feeling that they cannot deploy the solution at this time. IPv6 is clearly more complicated and with the reduction of funding and IT human resources, this is indeed a hindrance. However, with UAG, you don't need to become an IPv6 expert, the UAG DirectAccess solution will automatically deploy the necessary IPv6 infrastructure.

When the DirectAccess client is connected to the Internet, it tries to set up two IPsec tunnels to the UAG DirectAccess server. These two tunnels will use IPsec tunnel mode and the Encapsulating Security Payload (ESP) protocol with AES 192bit encryption to protect privacy.

The two tunnel types here are:

- **Infrastructure tunnel: The** Infrastructure tunnel starts when the computer starts but before the user logs on. The DirectAccess computer is always a domain member and its account is used to log in through a computer certificate and authenticate NTLMv2. In addition, it must belong to the security group reserved for DirectAccess clients. This tunnel has a two-way connection and the client management agents can call the management server on the corporate network. The management server can initiate connections to the DirectAccess client when the Infrastructure tunnel tunnel is set up. The DirectAccess client can only connect through this tunnel to access the servers you specify. This tunnel does not allow open access to the entire internal network.
- **Intranet tunnel:** Intranet tunnel is set after user login. This tunnel is also encrypted with ESP and AES 192. Authentication is done using a computer certificate (infrastructure tunnel) and Kerberos authentication for the user account. Intranet tunnel allows users to have access to any resources within the local network that they have authority.

There are two types of access you can use when enabling DirectAccess clients to connect to the local network. You can choose the 'end to edge' or 'end to end' option. Let's take a look at these two types:

- **End to Edge:** When using the 'end to edge' connection type, the DirectAccess client will establish a link in authenticated IPsec tunnel mode to the UAG DirectAccess server. After Ipsec connection is completed at the DirectAccess server, the transfer of traffic from the DirectAccess server to the servers on the local network is authenticated or encrypted at the network level.
- **End to End:** The 'end to end' network security type allows security of IPsec connections throughout. The connection between the DirectAccess client and server will be encrypted and authenticated by IPsec tunnel mode. After the traffic leaves the DirectAccess server to reach another server on the local network, the connection is transferred to the internal network using the IPsec transport mode. However, the default setting only authenticates for the endpoint; connection in unencrypted transport mode so that network IDS and other security devices can evaluate them on the network. This will reduce some of the overhead involved in IPsec connectivity.

In addition to computer certificates, computer accounts (NTLMv2) and user account authentication used during the creation of DirectAccess tunnels, you also have the option to force users to use Smart Card authentication to set up intranet. tunnel, improve the security of the solution. If authentication by smart card is not safe enough to meet the requirements, you can execute some policies on the DirectAccess client with NAP, at which point the unqualified client will be quarantined before enabling the setup tunnels infrastructure tunnel and intranet tunnel.

One important thing to note here is that the *End to Edge* connection supports all networks, which does not require you to have hosts that support IPv6 on the local network. However, if you want to implement ' *end to end* ' security with IPsec tunnel and IPsec transport mode, you need to have Windows Server 2008 servers behind the DirectAccess server. Alternatively, you can use *End to Edge* and *End to End* connection types; they are not

mutually exclusive.

All traffic traveling between the client and the DirectAccess server is IPv6 traffic. The implication is that, although the servers behind UAG DirectAccess are not IPv6 aware, client applications must support this protocol. To meet that, you need to ensure client applications are IPv6 compatible before deploying DirectAccess.

Note:

We need to clarify terms like 'IPv6 aware', 'IPv6 capable', 'IPv6 only' and 'native IPv6'. When it comes to 'native IPv6' networks, we need to understand that all network infrastructures are here (routers, DNS, DHCP, etc.) as well as fully supported IPv6 clients and servers. In contrast, the term 'IPv6 aware' refers to not using IPv6 seamlessly, only client applications and servers can take advantage of IPv6 transition techniques to be able to work on IPv4 networks. Meanwhile, IPv6 capable networks with hosts support Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) so that IPv6 messages can be sent over IPv6 network. When installing UAG as a DirectAccess server, it will configure an ISATAP router so that IPv6 messages are routed within an IPv4 header over the IPv4 network, so there is no need to upgrade the DNS router and switch as well as the DHCP server to works with IPv6 connection.

Conclude

In Part 1 of this series, we gave you an overview of what DirectAccess can do, the values ??it can provide for you and your users. We saw how DirectAccess set up two tunnels, intranet tunnel and infrastructure tunnel. In addition, there are two deployment modes: end to edge and end to end. In the next article in this series, I will go over some of the detailed IPv6 transition techniques used by UAG DirectAccess.