10 things you need to know about DirectAccess

DirectAccess promises to revolutionize the entire remote access experience so that all employees can work from anywhere, anytime without being tied to traditional techniques.

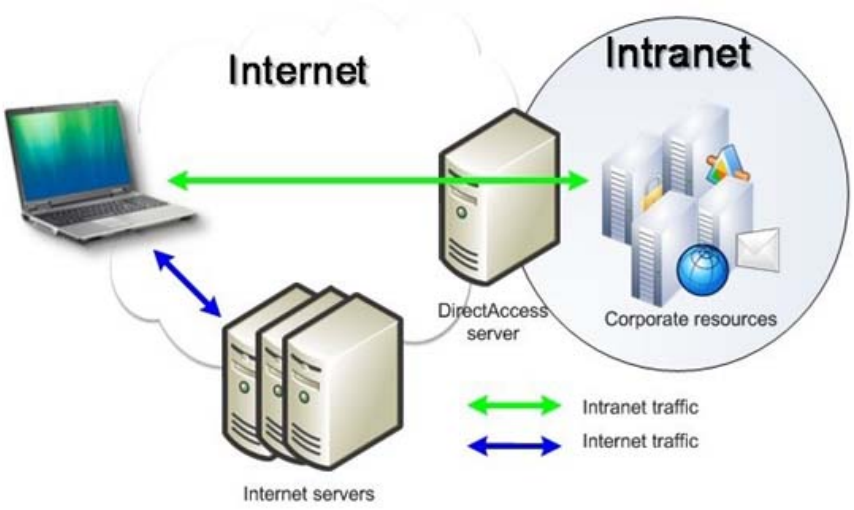
DirectAccess is a remote access technology available thanks to the combination of Windows Server 2008 R2 and Windows 7 Enterprise or Ultimate versions. DirectAccess promises to revolutionize the entire remote access experience so that all employees can work from anywhere, anytime without having to bind to traditional remote access techniques such as network-level VPN, SSL VPN gateway, and reverse proxy. It gives users a seamless experience, giving IT advanced management capabilities. DirectAccess allows access anywhere, even when the DirectAccess client system is behind a firewall.

1. Can expand the company network with an Internet-connected computer anywhere in the world

DirectAccess's goal is to expand the scope of the corporate network to any DirectAccess client connected to the Internet. DirectAccess computers here are a domain member, managed by control and management mechanisms such as computers within the corporate network boundary. In addition to expanding IT control over all of these computers, regardless of location, DirectAccess also provides a seamless network access experience for users. They do not need to remember to use a certain name (name) when they are on a corporate network and another name when not in that network; That's because they're always on the corporate network.

When the DirectAccess computer starts, it will set up an ' *infrastructure* ' tunnel. This base tunnel will allow DirectAccess clients to connect to domain resources, such as domain controllers, DNS servers, and management servers. This tunnel is also a two-way tunnel, so IT can initiate connections to DirectAccess clients on the Internet (called ' *manage out* ' connections), also in that tunnel, they can connect connect to hosts on the local network.

After the user logs in, a second tunnel, an *intranet tunnel* , allows the user to connect to company resources like the way a host in the local network connects to that resource. They can use a FQDN or a label name to connect to a file server, web server, database server, mail or any server and do not need to reconfigure applications when leaving the corporate network. . DirectAccess users are always on the corporate network, regardless of where they are.



2. Need to have all DirectAccess requests

You must have all the requirements before you start deploying DirectAccess. To get started, you need:

- At least one domain controller runs Windows Server 2003 or higher.
- An internal PKI to assign certificates to DirectAccess clients and servers.
- A private or public PKI to assign website certificates to the IP-HTTPS listener and Network Location Server listeners (discussed below).

In addition, you need other requirements:

- DirectAccess server must be Windows Server 2008 R2 Standard, Enterprise or higher.
- IPv6 must be enabled, technologies for forwarding IPv6 address space must also be disabled.
- DirectAccess clients must run Windows 7 Enterprise or Ultimate.
- DirectAccess clients must be members of an Active Directory domain.
- Network Location Server (Web server) high availability capability must be in the corporate network.
- If there are multiple firewalls in front or behind the DirectAccess server, the data filters must be enabled to allow the necessary traffic.
- The DirectAccess server must have two network interface adapters.

3. IPv6 is the cornerstone of DirectAccess communication

The DirectAccess client always uses IPv6 address space to communicate with the DirectAccess server. The DirectAccess server will forward these connections to IPv6 devices on the corporate network. The corporate network can use IPv6 infrastructure (say all routers, switches, operating systems and applications are capable of supporting IPv6) or it can use IPv6 transition techniques. to connect to IPv6 resources on the corporate network.

DirectAccess servers can use ISATAP (Intra-site Automatic Tunnel Addressing Protocol) for IPv6 tunnel packets within IPv4 headers, which can take advantage of your IPv4 routing infrastructure to migrate IPv6 data packets in the network. DirectAccess clients connected to IPv4 Internet can use a number of IPv6 transition technologies to connect to DirectAccess servers, including 6to4, Teredo and IP-HTTPS.

4. IPSec protects communication from beginning to end

Because the communication between the DirectAccess client and server will go through the external Internet, security communication is an extremely important issue. DirectAccess uses IPsec protocol to protect the communication safety between DirectAccess client and server. IPsec tunnel mode is used to set up intranet and infrastructure tunnels. In addition, you can configure DirectAccess to request *end-to-end* encryption between the DirectAccess client and the destination server on the corporate network in order to use IPsec transfer mode, from there. The connection is encrypted from the client to its destination. DirectAccess also takes advantage of the newly introduced AuthIP feature in Vista and Windows Server 2008, making authenticated connections through user or computer certificates instead of just computer certificates.

5. Client applications must understand IPv6 address space

While the goal is to provide a similar computing experience as connected clients on the corporate network, there are some key differences between the DirectAccess client and corporate network client: the DirectAccess client *must* and *always* use IPv6 to connect to the DirectAccess server. That means that the client application on the DirectAccess client must understand the IPv6 address space. If the client application does not understand the IPv6 address space, the connection will fail. This is true even when using an IPv6 adapter to IPv4, this is a converter that allows DirectAccess clients to connect to IPv4 servers on the corporate network.

6. Work with the support of Active Directory and Group Policy

Some changes to the DirectAccess server and client configuration to help the solution work. To make these changes in the most effective way, the solution DirectAccess offers is to use Active Directory and Active Directory Group Policy objects. The GPO is assigned to the DirectAccess server and client. In addition, Active Directory is required for authentication. The infrastructure tunnel uses NTLMv2 authentication to verify that the computer account is connected to the DirectAccess server, that computer account must be in the Active Directory domain. The intranet tunnel uses Kerberos authentication for the logged-in user to create the second tunnel.

Although Active Directory and GPO are required, the DirectAccess server does not need to be a member of the domain. As long as there is two-way trust between the DirectAccess server domain and the domains / forest resources, the solution will work.

7. Intranet servers allow DirectAccess clients to know when they're on the corporate network

DirectAccess is designed to work automatically and work in the background. Users do not have to do anything to initialize (*turn on*) DirectAccess connection. All they need to do is *turn on* (*turn on*) their computer. In fact, users don't even need to login! Before logging in, the infrastructure tunnel is set up automatically, and the DirectAccess client's *agents* can connect to their servers to update updates and configuration information. The necessary images, security settings, and anything needed to ensure the DirectAccess client strictly adheres to network security and configuration policies.

To make the process transparent, there must be a mechanism in which the DirectAccess client components know when they need to be turned on, always off. That's the Network Location Server. Network Location Server (NLS) is a Web server that allows incoming SSL connections. You can allow authentication to be integrated or anonymously to the NLS server. When the DirectAccess client connects to the NLS, it knows that it is on the corporate network, and will turn off the DirectAccess client components. If the DirectAccess client cannot contact the NLS server, then it knows that it is outside the corporate network and will automatically turn on the DirectAccess client components to set up IPsec tunnels to the DirectAccess server over the Internet. The

DirectAccess client will perform an NLS Web server certificate check on the Certificate Revocation List, so CRL must be available. Otherwise connecting to the NLS SSL website will fail and the internal network detection process will also fail.

8. Certificates, certificates, certificates!

Certificates are used in some locations in the DirectAccess client / server solution. Some places where you will see the certificates are:

- **DirectAccess client** . Each DirectAccess client needs a certificate to establish IPsec connections to the DirectAccess server. These certificates are used to create IPsec connections and are also used by IP-HTTPS, where the DirectAccess server will perform computer certificate validation before allowing IP-HTTPS connection to take place. on the Internet. Computer certificates are best assigned by using Microsoft Certificate Server and automatic certificate enrollment based on Group Policy.
- **IP-HTTPS listener on DirectAccess server.** IP-HTTPS is an IPv6 transition technology used for IPv6 tunnel packets on IPv4 Internet. This protocol is designed by Microsoft to allow the DirectAccess client to connect to the DirectAccess server, even if the DirectAccess client behind the firewall only allows HTTP / HTTPS connections to be sent or behind the Web proxy. server. The IP-HTTPS listener requires a website certificate, and the DirectAccess client must be able to contact the server that contains the CRL for certificate authentication. If the CRL check process fails, the IP-HTTPS connection will also fail. Commercial certificates are the best solution for IP-HTTPS listener, because their CRL is available globally.
- **DirectAccess server** . The DirectAccess server stores the IP-HTTPS website certificate, but it also requires a computer certificate to establish IPsec connections with the DirectAccess clients.

9. The naming policy table provides DNS queries according to the policy

The DirectAccess client uses the Name Resolution Policy Table (NRPT) table to determine which DNS server can use to identify the name. When the DirectAccess client is on the corporate network, the NRPT is automatically turned off. When the DirectAccess client detects that it is on the Internet, the DirectAccess client will activate the NRPT and check its entries to see which DNS server to use to connect to the resource. You set your internal domain and possible servers on the NRPT and configure it to use an internal DNS server for name identification.

When the DirectAccess client located on the Internet needs to connect to the resource using FQDN, it checks the NRPT. If this name is in it, the query will be sent to the internal network DNS server. If not in the NRPT, the DirectAccess client sends a query to the DNS server configured on its NIC, which is the Internet DNS server. The name of the NLS server is also placed on the NRPT, however it is grouped into a waiver list - meaning that the DirectAccess client never uses the intranet server to identify the name of the NLS server. So the DirectAccess client on the Internet will not be able to identify the name of the NLS server and so will know that it is on the Internet from which to turn on the DirectAccess client components. More importantly, when connecting to the corporate network via DirectAccess, the DirectAccess clients do not think it is connected to the corporate network by identifying the name of the NLS server.

10. DirectAccess allows ' *manage out* ' capability

As mentioned above, IT can take advantage of the ' *manage out* ' capability by infrastructure tunnel to connect to DirectAccess clients on the Internet. However, you still need to configure firewall rules in Windows Firewall with Advanced Security (WFAS) to allow these connections for Teredo clients. When creating these rules, make

sure that they have enabled the Edge Traversal feature for Firewall Rule. The DirectAccess client is Teredo when they are behind the NAT to connect to the Internet and the DirectAccess server, at which point the NAT device allows sending on UDP port 3544.