DIRECTACCESS FEATURE IN WINDOWS 7

What is DirectAccess

DirectAccess is an always on connection to our remote private network, regardless of where we are. Starting from Windows 7 and Windows Server 2008 R2, we can use DirectAccess feature. DirectAccess in Windows 7 uses IPv6 with IPsec VPN connection which is always on. DirectAccess is different from a VPN protocol. DirectAccess connection process doesn't require user intervention or logon (it is automatic) in contrast to a VPN solution. It starts from the moment we connect to the Internet and allows authorized users to access corporate network file server and intranet web sites.

Since DirectAccess is automatic, we will always have access to the remote (corporate) intranet, regardless of where we are. DirectAccess is bidirectional, which means that servers on corporate network can access remote clients in the same fashion as if they were connected to the local network. In many VPN solutions, the client can access the server, but the server can't access the remote client.

DirectAccess provides administrators the ability to control resources that are available to remote users and computers. Administrators can ensure that remote clients remain up to date with antivirus definitions and software updates. They can also apply security policies to isolate servers and hosts. Remote DirectAccess clients can still receive software and group policy updates from the sever on the corporate network, even if the user hasn't logged on. This allows administrators to manage and maintain remote computers like never before. DirectAccess reduces unnecessary traffic on the corporate network by not sending traffic that is headed for the Internet to the DirectAccess server. Intranet communications are encrypted and sent to the DirectAccess server, and then on to the intranet. Internet communications are sent directly to the Internet hosts without encryption and without going through the DirectAccess server.

DirectAccess Connection Methods

DirectAccess clients can connect to the internal resources by either using the selected server access (modified end-to-edge) or Full enterprise network access (end-to-edge) method. The connection method is configurable using DirectAccess console or manually trough IPsec policies.

It is recommended to use IPv6 and IPsec throughout organization, upgrade our application servers to Windows Server 2008 R2, and enable selected server access in order to provide the highest level of security. On the other hand, organizations can use full enterprise network access where the IPsec session is established between a DirectAccess client and the server.

DirectAccess Connection Process

DirectAccess client first detects if there is network connection available. Then it attempts to connect to the intranet site that was specified in the DirectAccess configuration. Then the client connects to the DirectAccess server using IPv6 and IPsec. In the case that a firewall or proxy server prevents the client computer from using either 6to4 or Toredo from connecting to DirectAccess server, the client automatically attempts to connect using the IP-HTTPS protocol, which uses an SSL (Secure Socket Layer connection) to ensure connectivity. After that the client and server mutually authenticate using their certificates. Active Directory group memberships are checked so that DirectAccess server can verify that the computer and user are authorized to connect using DirectAccess. If Network Access Protection (NAP) is enabled and configured for health validation, the DirectAccess client obtains a health certificate from a Health Registration Authority (HRA) located on the intranet prior to connecting to the DirectAccess server.

Once the client is clear to connect to the network, the DirectAccess begins forwarding traffic from the client to the intranet.

DirectAccess Client Configuration

If a client is connected to the network using a public IPv6 address, DirectAccess will also use a public IPv6 to connect. If a client is using a public IPv4 address, DirectAccess will use the IPv6 6to4 method to connect to the client. If the client is using private IPv4 address behind a NAT, DirectAccess will use the IPv6 Teredo method to connect to the client. If the client can't connect to the intranet, because they are being blocked by a firewall, but the client still has access to the Internet, DirectAccess will use IP-HTTPS method (the least secure form) to connect to the client.

Computers running Windows 7 Enterprise and Ultimate that have been joined to a domain can support DirectAccess. We can't use DirectAccess with any other edition of Windows 7, or earlier versions of Windows (Vista or XP). When configuring a client for DirectAccess we must add the clients' domain computer account to a special security group. We specify this security group when we are creating a DirectAccess server.

Group Policies are used to push down the DirectAccess client configuration in comparison to traditional VPN connections where we have to manually set VPN configuration or distribute using connection manager administration kit. Once we have added the computers account to that designated security group, we also need to install the computer certificate to allow DirectAccess authentication. This can be done using Active Directory Certificate Services which will enable automatic enrollment of the appropriate certificate.

When it comes to server, we have to have a DirectAccess server running on Windows Server 2008 R2 with two network cards. Also, we have to have Active Directory environment with at least one Domain Controller (DC) and a DNS server running Windows Server 2008 or 2008 R2. We also need to have a Public Key Infrastructure (PKI) with Active Directory Certificate Services (ADCS). We also need IPsec policies configured and IPv6 Transition Technologies that are available for use on a DirectAccess server such as 6to4 and Teredo.

When we first configure DirectAccess on a server, it creates a Group Policy Object (GPO) at the domain level and filters it for us for that specified security group that we create during the installation process. Only clients that are members of that group get DirectAccess policies and will be able to connect to the DirectAccess server.

Trough this Group Policy we can configure settings such as 6-to-4 relay server name, the IP-HTTPS server to connect to if all other connection methods fail, and weather the Teredo is used for DirectAccess and the Teredo server address.

We can also configure the DirectAccess from the command line using the netsh command. Have in mind that all configurations made manually with the netsh utility will be overwritten by corresponding Group Policy settings.

To determine if the client has made a successfull DirectAccess connection, we can connect on the network connection icon in the system tray. This will open a status of our connection which will say "Internet and Corporate" access. In that case we know that we have successfully connected to the DirectAccess server. If the status is "Local and Internet", we know that there is no connection to the DirectAccess server.

As we know, DirectAccess clients use certificate for authentication. If a computer doesn't have a valid computer certificate, which should be received from ADCS, it can't connect successfully. We can verify client certificate using the certificate snap-in.

Source: http://www.utilizewindows.com/7/networking/509-directaccess-feature-in-windows-7