Microsoft

DirectAccess

Seamless, secure, anytime remote connectivity without VPN

What is DirectAccess?

DirectAccess is a new feature in the Windows® 7 and Windows Server® 2008 R2 operating systems that seamlessly connects remote users to the corporate network any time they have Internet access.

With DirectAccess, users can securely access corporate resources (such as e-mail servers, shared folders, or intranet Web Sites) without having to go through a virtual private network (VPN). DirectAccess also enables IT administrators to manage remote computers as if they were on the corporate network.

How does it work?

Unlike VPNs, which require user intervention to initiate a remote connection to an intranet, DirectAccess automatically establishes a bi-directional connection from client computers to the corporate network.

DirectAccess is based on a deperimitization model that uses advanced encryption, authentication, and authorization technologies that enable all points on a network to securely exchange information and data over the Internet. It is built on a foundation of proven industry standards such as Internet Protocol version 6 (IPv6) and Internet Protocol security (IPsec). DirectAccess supports a range of network scenarios, including pure IPv6 and IPsec environments (end-to-end) non-IPsec intranets with IPv6 application servers (end-to-edge), or IPv4-only application servers.

Key Solution Benefits

Improved Productivity:

- Helps improve the productivity of remote staff by providing the same, always-on connectivity experience no matter if users are inside or outside the corporate network.

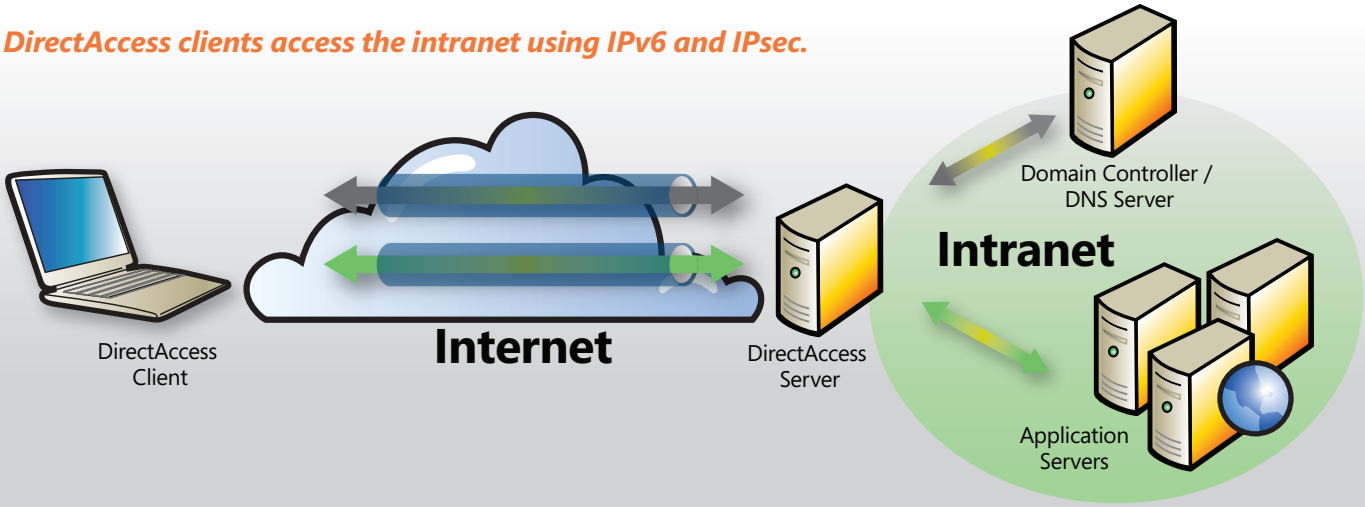
Secure Connectivity:

- Leverages IPsec for authentication and encryption.
- Provides the ability to apply granular policy control over access to resources, applications, and servers.
- Integrates with Microsoft Server and Domain Isolation, Network Access Protection (NAP), and BitLocker solutions, resulting in security, access, and health requirement policies that seamlessly interoperate between intranets and remote computers.

Greater Manageability:

- Helps ensure that machines both on the network and off are always healthy, managed, and up-to-date.
- Provides administrators with the ability to update Group Policy settings and distribute software updates any time a remote computer has Internet connectivity, even if the user is not logged on.
- Helps ensure that organizations can meet regulatory and privacy mandates for security and data protection for assets that must roam beyond the corporate network.

DirectAccess clients access the intranet using IPv6 and IPsec.



DirectAccess

System Requirements

- DirectAccess server running Windows Server 2008 R2 along with network adaptors for the Internet and the Intranet.
- DirectAccess clients running Windows 7.
- At least one domain controller and Domain Name System (DNS) server running Windows Server 2008 or Windows Server 2008 R2.
- A public key infrastructure (PKI) to issue computer certificates, smart card certificates, and, for NAP, health certificates. For more information, see http://www.microsoft.com/pki.
- IPsec policies to specify protection for traffic. For more information, see http://www.microsoft.com/ipsec.
- IPv6 transition technologies available for use on the DirectAccess server: ISATAP, Teredo, and 6to4.
- NAT-PT device to provide access to IPv4-only resources for DirectAccess clients.

Features List

- Always-on connectivity that requires no end-user steps to access corpnet.
- Remote management, updating, and health maintenance of remote computers even when the end user is not logged on.
- Granular policy controls for authorized access to corpnet resources and servers.
- Tight integration with policy-based network access approach.
- Support for multifactor authentication such as smart cards.
- IPsec authentication and encryption.
- Support for non IPsec and non-IPv6 environments (e.g., using IPv6-over-IPv4 tunneling with 6to4 or Teredo).

Resources

Web Sites and White Papers

- http://www.microsoft.com/directaccess
- http://technet.microsoft.com/en-us/network/dd420463.aspx

Demo

- http://www.microsoft.com/windows/enterprise/videos/windows-7/default.aspx#Introduction

DirectAccess and NAP

By using Microsoft Network Access Protection (NAP) with DirectAccess, a non-compliant client computer that becomes infected with malware can have its intranet access limited to prevent the spread of malware. NAP is not required to use DirectAccess, but it is recommended. For more information on NAP, see http://www.microsoft.com/nap.

Microsoft