Windows Server® 2008 R2

Windows® 7

Technical Overview of DirectAccess in Windows 7 and Windows Server 2008 R2

Microsoft Windows Family of Operating Systems

Microsoft Corporation

Published: April 2009

Abstract

The Windows 7 and Windows Server 2008 R2 operating systems introduce DirectAccess, a solution that provides users with the same experience working remotely as they would have when working in the office. With DirectAccess, remote users can access corporate file shares, Web sites, and applications without connecting to a virtual private network (VPN).

Microsoft®

Copyright information

This document supports a preliminary release of a software product that may be changed substantially prior to final commercial release. This document is provided for informational purposes only and Microsoft makes no warranties, either express or implied, in this document. Information in this document, including URL and other Internet Web site references, is subject to change without notice. The entire risk of the use or the results from the use of this document remains with the user. Unless otherwise noted, the companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in examples herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Contents

DirectAccess Technical Overview for Windows 7 and Windows Server 2008 R2 5

Mobile Workforce Needs 6

The Challenges with VPNs 6

DirectAccess Connections 6
End-to-end protection 8
End-to-edge protection 8

The DirectAccess Connection Process 9

Separating Internet and Intranet Traffic 10

DirectAccess Authentication 11

Using IPv6 12

DirectAccess and Network Access Protection 12

DirectAccess Requirements 12

Summary 13

References 14

DirectAccess Technical Overview for Windows 7 and Windows Server 2008 R2

The Windows® 7 and Windows Server® 2008 R2 operating systems introduce DirectAccess, a new solution that provides users with the same experience working remotely as they would have when working in the office. With DirectAccess, remote users can access corporate file shares, Web sites, and applications without connecting to a virtual private network (VPN).

DirectAccess establishes bi-directional connectivity with the user's enterprise network every time the user's DirectAccess-enabled portable computer is connected to the Internet, even before the user logs on. With DirectAccess, users never have to think about whether they are connected to the corporate network. DirectAccess also benefits IT by allowing network administrators to manage remote computers outside of the office, even when the computers are not connected to a VPN. DirectAccess enables organizations with regulatory concerns to extend regulatory compliance to roaming computer assets.

This document describes the benefits of DirectAccess, how it works, and what you will need to deploy it in your organization. The following topics are covered:

Mobile Workforce Needs

The Challenges with VPNs

DirectAccess Connections

The DirectAccess Connection Process

Separating Internet and Intranet Traffic

DirectAccess Authentication

Using IPv6

DirectAccess and Network Access Protection

DirectAccess Requirements

Summary

References

Notes

- For a complete view of Windows 7 resources, articles, demos, and guidance, please visit the Springboard Series for Windows 7 on the Windows Client TechCenter.
- For a downloadable version of this document, see the DirectAccess Technical Overview for Windows 7 and Windows Server 2008 R2 in the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=151748).

Mobile Workforce Needs

More users have become mobile to stay productive while they are away from the office. According to IDC, the third quarter of 2008 marked the point at which computer manufacturers began shipping more mobile computers than desktop computers worldwide (IDC Worldwide Quarterly PC Tracker, December 2008).

The number of mobile users is expected to grow; in 2008, mobile workers worldwide will be 26.8% of the total workforce, and that number will increase to 30.4% by 2011 (IDC, "Worldwide Mobile Worker Population 2007–2011 Forecast," Doc #209813, Dec 2007).

However, the way users access network resources hasn't changed. Although home broadband, wireless broadband, and Wi-Fi allow users to connect to the Internet while they are away from the office, corporate firewalls prevent them from connecting to resources on the intranet. Only users physically connected to the intranet can access intranet resources. This becomes a management problem because IT administrators can update computers only when they connect to the intranet. To circumvent this limitation, many organizations provide VPNs.

The Challenges with VPNs

Traditionally, users connect to intranet resources with a VPN. However, using a VPN can be cumbersome because:

- Connecting to a VPN takes several steps, and the user needs to wait for authentication. For organizations that check the health of a computer before allowing the connection, establishing a VPN connection can take several minutes.
- Any time users lose their Internet connection, they need to re-establish the VPN connection.
- VPN connections can be problematic in some environments that filter out VPN traffic.
- Internet performance is slowed if both intranet and Internet traffic goes through the VPN connection.

Because of these inconveniences, many users avoid connecting to a VPN. Instead, they use application gateways, such as Microsoft® Outlook® Web Access (OWA), to connect to intranet resources. With OWA, users can retrieve internal e-mail without establishing a VPN connection. However, users still need to connect to a VPN to open documents that are located on intranet file shares, such as those that are linked to in an e-mail message.

DirectAccess Connections

DirectAccess overcomes the limitations of VPNs by automatically establishing a bi-directional connection from client computers to the corporate network. DirectAccess is built on a foundation of proven, standards-based technologies: Internet Protocol security (IPsec) and Internet Protocol version 6 (IPv6).

DirectAccess uses IPsec to authenticate both the computer and user, allowing IT to manage the computer before the user logs on. Optionally, you can require a smart card for user authentication.

DirectAccess also leverages IPsec to provide encryption for communications across the Internet. You can use IPsec encryption methods such as Triple Data Encryption Standard (3DES) and the Advanced Encryption Standard (AES).

Clients establish an IPsec tunnel for the IPv6 traffic to the DirectAccess server, which acts as a gateway to the intranet. Figure 1 shows a DirectAccess client connecting to a DirectAccess server across the public IPv4 Internet. Clients can connect even if they are behind a firewall.

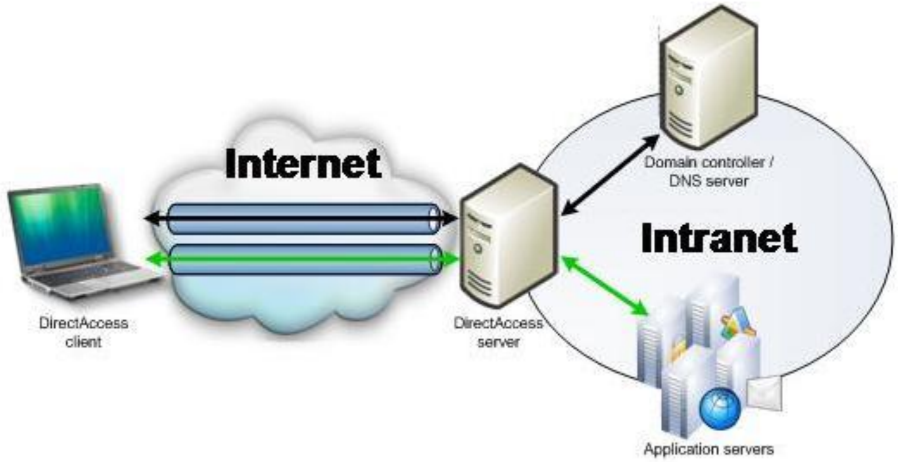

Figure 1 DirectAccess clients access the intranet using IPv6 and IPsec

The DirectAccess client establishes two IPsec tunnels:

- **IPsec Encapsulating Security Payload (ESP) tunnel using a computer certificate**. This tunnel provides access to an intranet DNS server and domain controller, allowing the computer to download Group Policy objects and to request authentication on the user’s behalf.
- **IPsec ESP tunnel using both a computer certificate and user credentials**. This tunnel authenticates the user and provides access to intranet resources and application servers. For example, this tunnel would need to be established before Microsoft Outlook could download e-mail from the intranet Microsoft Exchange Server.

After the tunnels to the DirectAccess server are established, the client can send traffic to the intranet through the tunnels. You can configure the DirectAccess server to control which applications remote users can run and which intranet resources they can access.

DirectAccess clients can connect to intranet resources by using two types of IPsec protection: end-to-end and end-to-edge.

End-to-end protection

With end-to-end protection, as shown in Figure 2, DirectAccess clients establish an IPsec session (shown in green) through the DirectAccess server to each application server to which they connect. This provides the highest level of security because you can configure access control on the DirectAccess server. However, this architecture requires that application servers run Windows Server 2008 or Windows Server 2008 R2 and use both IPv6 and IPsec.

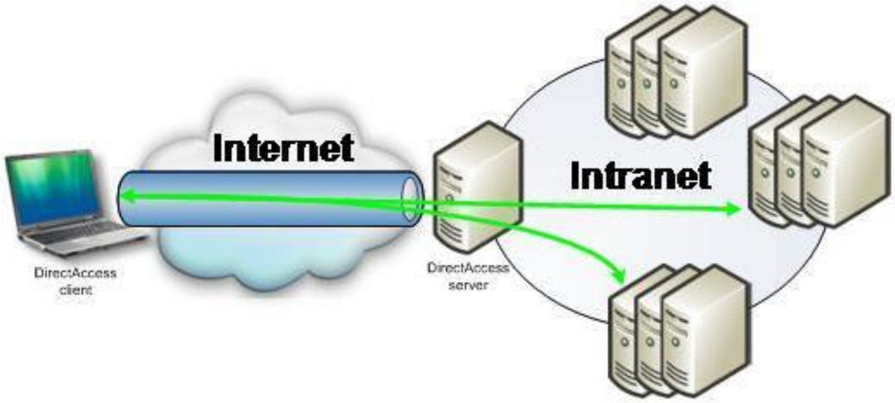

Figure 2 End-to-end protection

End-to-edge protection

For end-to-edge protection, as shown in Figure 3, DirectAccess clients establish an IPsec session to an IPsec gateway server (which can be the same computer as the DirectAccess server). The IPsec gateway server then forwards unprotected traffic, shown in red, to application servers on the intranet. This architecture does not require IPsec on the intranet and works with any IPv6-capable application servers.

For information about connecting to IPv4-only application servers, read Using IPv6 later in this document.

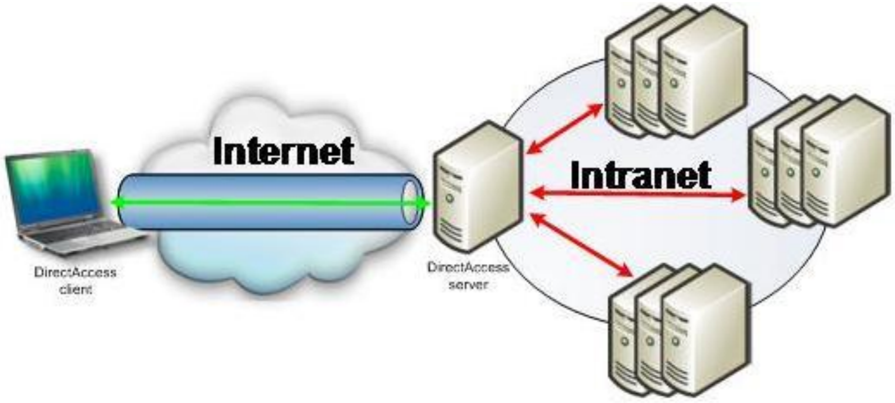

Figure 3 End-to-edge protection

For the highest level of security, deploy IPv6 and IPsec throughout your organization, upgrade application servers to Windows Server 2008 or Windows Server 2008 R2, and use end-to-end protection. This allows authentication and, optionally, encryption from the DirectAccess client to the intranet resources. Alternatively, use end-to-edge protection when you want to avoid deploying both IPv6 and IPsec throughout your enterprise network. End-to-edge protection closely resembles VPNs and, as such, can be more straightforward to deploy.

Note

For either of these architectures, you can deploy multiple DirectAccess servers with a load balancer to meet your redundancy and scalability requirements.

The DirectAccess Connection Process

DirectAccess clients use the following process to connect to intranet resources:

1. The DirectAccess client computer running Windows 7 detects that it is connected to a network.
2. The DirectAccess client computer attempts to connect to an intranet Web site that an administrator specified during DirectAccess configuration. If the Web site is available, the DirectAccess client determines that it is already connected to the intranet, and the DirectAccess connection process stops. If the Web site is not available, the DirectAccess client determines that it is connected to the Internet and the DirectAccess connection process continues.
3. The DirectAccess client computer connects to the DirectAccess server using IPv6 and IPsec. If a native IPv6 network isn't available (and it probably won't be when the user is connected to the Internet), the client establishes an IPv6-over-IPv4 tunnel using 6to4 or Teredo. The user does not have to be logged in for this step to complete.
4. If a firewall or proxy server prevents the client computer using 6to4 or Teredo from connecting to the DirectAccess server, the client automatically attempts to connect using the IP-HTTPS protocol, which uses a Secure Sockets Layer (SSL) connection to ensure connectivity.
5. As part of establishing the IPsec session, the DirectAccess client and server authenticate each other using computer certificates for authentication.
6. By validating Active Directory® group memberships, the DirectAccess server verifies that the computer and user are authorized to connect using DirectAccess.

   Note

   To mitigate the risk of denial of service (DoS) attacks, IPsec on the DirectAccess server de-prioritizes key negotiation traffic using Differentiated Services Code Points (DSCPs).

7. 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 Internet prior to connecting to the DirectAccess server. The HRA forwards the DirectAccess client's health status information to a NAP health policy server. The NAP health policy server processes the policies defined within the Network Policy Server (NPS) and determines whether the client is compliant with system health requirements. If so, the HRA obtains a health certificate for the DirectAccess client. When the DirectAccess client connects to the DirectAccess server, it submits its health certificate for authentication.

   For more information, see DirectAccess and Network Access Protection later in this document.
8. The DirectAccess server begins forwarding traffic from the DirectAccess client to the intranet resources to which the user has been granted access.

The DirectAccess connection process happens automatically, without requiring user intervention.

Separating Internet and Intranet Traffic

DirectAccess can separate intranet traffic to the intranet from Internet traffic, as shown in Figure 4, to reduce unnecessary traffic on the corporate network. Most VPNs send all traffic—even traffic that is destined for the Internet—through the VPN, which can slow both intranet and Internet access. Because communications to the Internet do not have to travel to the corporate network and back to the Internet, DirectAccess does not slow down Internet access.

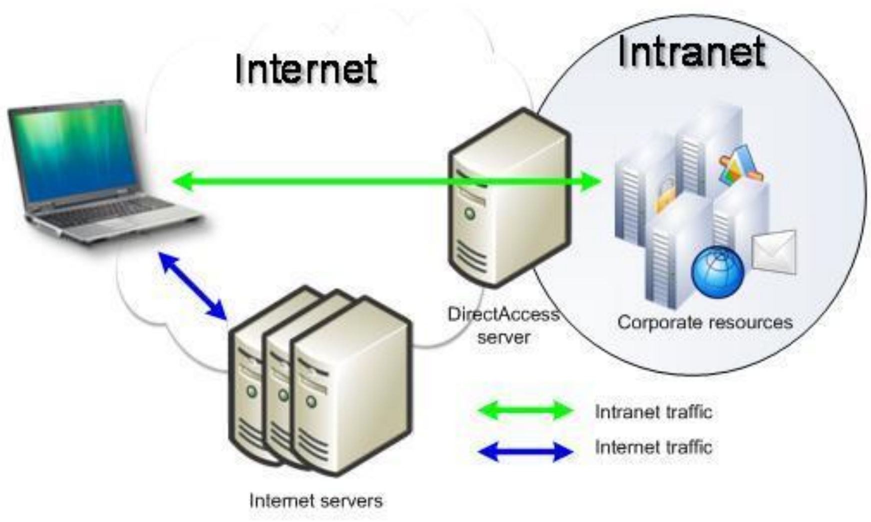

Figure 4 The default traffic flow for DirectAccess does not send Internet traffic through the DirectAccess server

IT administrators can also choose to route all traffic, except traffic for the local subnet, through the DirectAccess server and the intranet. When this option is enabled, all communications use the IP-

HTTPS protocol, which creates an IP tunnel within the HTTPS protocol, allowing it to pass through firewalls and proxy servers.

Combining this option with Windows Firewall with Advanced Security, IT administrators have complete control over which applications can send traffic and which subnets client computers can reach. For example, IT administrators can use outbound Windows Firewall rules to:

- Allow client computers to connect to the entire Internet, but only one specific subnet on the intranet.
- Allow client computers to connect directly to the Internet using Internet Explorer®, but send traffic for all other applications through the intranet.
- Prevent intranet applications from sending communications to the Internet by restricting them to specific servers on your intranet.

While the default DirectAccess traffic configuration is optimized for performance, IT administrators have the flexibility they need to meet their organization's security requirements.

DirectAccess Authentication

DirectAccess authenticates the computer before the user logs on. Typically, computer authentication grants access only to domain controllers and DNS servers. After the user logs on, DirectAccess authenticates the user, and the user can connect to any resources he or she is authorized to access.

DirectAccess supports standard user authentication using a user name and password. For greater security, you can implement two-factor authentication with smart cards. Typically, this requires a user to insert a smart card in addition to typing his or her user credentials. Smart card authentication prevents an attacker who acquires a user's password (but not the smart card) from connecting to the intranet. Similarly, an attacker who acquires the smart card but does not know the user's password is unable to authenticate.

You can require smart card authentication in the following configurations:

- **User authentication**. Smart card authentication is required for specified users, regardless of which computer they use.
- **Computer authentication**. Smart card authentication is required for specified computers, regardless of which user logs on.
- **Gateway authentication**. The IPsec gateway requires smart card authentication before allowing connectivity. This type of configuration allows users to access Internet resources without their smart card, but requires a smart card before users or computers can connect to intranet resources. This can be combined with either of the previous smart card authentication scenarios. When smart card authentication is required for end-to-end authentication, you must use Active Directory Domain Services (AD DS) in Windows Server 2008 R2.

Using IPv6

DirectAccess requires the use of IPv6 so that DirectAccess clients have globally routable addresses. For organizations that are already using a native IPv6 infrastructure, DirectAccess seamlessly extends the existing infrastructure to DirectAccess client computers, and those client computers can still access Internet resources using IPv4.

For organizations that have not yet begun deploying IPv6, DirectAccess provides a straightforward way to begin IPv6 deployment without requiring an infrastructure upgrade. You can use the 6to4 and Teredo IPv6 transition technologies for connectivity across the IPv4 Internet and the ISATAP IPv6 transition technology so that DirectAccess clients can access IPv6-capable resources across your IPv4-only intranet.

Additionally, you can deploy a Network Address Translation-Protocol Translation (NAT-PT) device so that DirectAccess client computers can access resources on your intranet that do not yet support IPv6.

DirectAccess and Network Access Protection

To encourage computers to comply with security and health requirement policies and reduce the risk of malware spreading, non-compliant clients can be restricted from accessing intranet resources or communicating with compliant computers. Using Network Access Protection (NAP) with DirectAccess, IT administrators can require DirectAccess client computers to be healthy and comply with corporate health requirement policies. For example, client computers can obtain a connection to the DirectAccess server only if they have recent security updates, anti-malware definitions, and other security settings.

Using NAP in conjunction with DirectAccess requires that NAP-enabled DirectAccess clients submit a health certificate for authentication when creating the initial connection with the DirectAccess server. The health certificate contains the computer’s identity and proof of system health compliance. As previously described, a NAP-enabled DirectAccess client obtains a health certificate by submitting its health state information to an HRA that is located on the Internet. The health certificate must be obtained prior to initiating a connection to a DirectAccess server.

By using NAP with DirectAccess, a non-compliant client computer that becomes infected with malware cannot connect to an intranet with DirectAccess, limiting the malware’s ability to spread. NAP is not required to use DirectAccess, but it is recommended. For more information, see Network Access Protection on the Microsoft Web site.

DirectAccess Requirements

DirectAccess requires the following:

- One or more DirectAccess servers running Windows Server 2008 R2 with two network adapters: one that is connected directly to the Internet, and a second that is connected to the intranet.
- On the DirectAccess server, at least two consecutive, public IPv4 addresses assigned to the network adapter that is connected to the Internet.
- DirectAccess clients running Windows 7.
- At least one domain controller and Domain Name System (DNS) server that is running Windows Server 2008 SP2 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 Public Key Infrastructure on the Microsoft Web site.
- IPsec policies to specify protection for traffic. For more information, see IPsec on the Microsoft Web site.
- IPv6 transition technologies available for use on the DirectAccess server: ISATAP, Teredo, and 6to4.
- Optionally, a non-Microsoft NAT-PT device to provide access to IPv4-only resources for DirectAccess clients.

Summary

DirectAccess provides the following benefits:

- **Seamless connectivity**. DirectAccess is on whenever the user has an Internet connection, giving users access to intranet resources whether they are traveling, at the local coffee shop, or at home.
- **Remote management**. IT administrators can connect directly to DirectAccess client computers to monitor them, manage them, and deploy updates, even when the user is not logged on. This can reduce the cost of managing remote computers by keeping them up-to-date with critical updates and configuration changes.
- **Improved security**. DirectAccess uses IPsec for authentication and encryption. Optionally, you can require smart cards for user authentication. DirectAccess integrates with NAP to require that DirectAccess clients must be compliant with system health requirements before allowing a connection to the DirectAccess server. IT administrators can configure the DirectAccess server to restrict the servers that users and individual applications can access.

DirectAccess also enables users to get more out of other Windows 7 networking improvements, such as:

- **Federated Search**. With Federated Search, desktop searches can include files and Web pages on your intranet whenever the user is connected to your intranet. Because DirectAccess connects users to the intranet when then connect to the Internet, Federated Search works automatically any time the user has an Internet connection.

- **Folder Redirection**. With Folder Redirection, folders can automatically synchronize between multiple computers across the network. If you enable DirectAccess, users with both mobile and desktop computers can stay synchronized automatically whenever they connect to the Internet.
- **Replaceable computer scenario**. In this scenario, a user's applications, documents, and settings are stored on the network and available from any computer. If a computer is lost or corrupted, the replacement computer does not require user-specific configuration.

With DirectAccess, client computers are always connected, better protected, and easier to manage.

References

Active Directory	http://go.microsoft.com/fwlink/?LinkID=147288
DirectAccess	http://go.microsoft.com/fwlink/?LinkId=147011
DNS	http://go.microsoft.com/fwlink/?LinkId=147013
Group Policy	http://go.microsoft.com/fwlink/?LinkId=100760
IPv6	http://go.microsoft.com/fwlink/?LinkId=17074
IPsec	http://go.microsoft.com/fwlink/?LinkId=50170
NAP	http://go.microsoft.com/fwlink/?LinkId=56443
PKI	http://go.microsoft.com/fwlink/?LinkId=83694