Using DirectAccess to Provide Secure Access to Corporate Resources from Anywhere

Published: May 2009

Although broadband services and Wi-Fi have dramatically improved, the connectivity experience for remote corporate users remains largely unchanged. Microsoft Information Technology (Microsoft IT) is adopting the DirectAccess feature in Windows® 7 and in Windows Server® 2008 R2 to enable employees to gain seamless remote access to corporate applications and data. The solution, which only requires Internet connectivity and credentials, significantly improves productivity and can be an important cost-saving mechanism.

Situation

In the past few years, advances in mobile computers and wireless broadband have enabled users to be more productive while 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. In 2008, remote workers will represent 26.8 % of the total workforce, and that number will increase to 30.4% by 2011‡. Clearly, users are becoming more mobile, and IT professionals must provide an infrastructure to allow them to remain productive.

The changing structure of business puts more pressure on IT professionals to provide a high-performance and secure infrastructure for connecting remote users while managing remote users and minimizing costs.

Solution

Microsoft IT is implementing DirectAccess, a new feature in Windows 7 and Windows Server 2008 R2, to provide remote users with seamless access to internal network resources whenever they are connected to the Internet.

Benefits

- Enhanced end user experience
- Improved remote monitoring for system health and management
- Potential cost-saving mechanism

Products & Technologies

- Windows Server 2008 R2
- Windows 7 Client
- IPsec
- IPv6
- Microsoft Network Access Protection (NAP)

Situation

Today’s workforce is more mobile than ever. In order to maximize productivity, employees need to have access to intranet resources wherever they travel. Providing this level of connectivity in a secure, manageable, and seamless way has been difficult with traditional virtual private networks (VPNs). Connecting to a VPN requires multiple steps, which causes delays while users wait for authentication.

Because of these inconveniences, IT organizations sometimes choose to deploy application gateways in order to provide users with intranet access across a firewall. Although application gateways can be excellent point solutions, not all application access problems are solved through gateways; there can still be situations when users are not able to access intranet file shares or other resources. More significantly, the more end users stay away from the corporate network, the harder it is for IT professionals to manage the systems, which increases the risk of a computer becoming unmanaged and unhealthy.

Solution

Microsoft Information Technology (Microsoft IT) is the core group at Microsoft responsible for supporting the company's technology infrastructure, and as such, they have been acutely aware of the limitations of traditional VPNs from both the end user and IT administrator perspective. To better support how the Microsoft remote workforce accesses the corporate network, Microsoft IT is implementing a new secure network access feature in Windows 7 and Windows Server 2008 R2 called DirectAccess, which improves user experience and worker productivity, enhances remote user manageability, and offers a more robust security model than is available in traditional VPNs.

In addition to its technological benefits, DirectAccess can be an important cost-saving mechanism that enables Microsoft Internet connected offices (ICOs) to maintain efficient and

Microsoft

secure connections to the corporate network instead of spending the estimated $250,000 US required to upgrade each facility to a dedicated connection (including purchasing racks, severs, network equipment, UPSs, card key, cooling and other infrastructure), as well as an additional annual $50,000 in circuit maintenance costs, adding up to a total savings of $300,000 per facility.

The End User Experience

Two common challenges that remote workers have with traditional VPNs is the manual effort and time required to establish a connection to the corporate network using the appropriate gateway, and tunnel type, and the manual effort involved in resetting the secure connection each time the computer system is restarted or whenever the user moves to a different network access point or is otherwise temporarily disconnected from the network.

"Always On," Transparent Connection to the Corporate Network

From the user's perspective, DirectAccess is always on. It offers the same connectivity experience both in and outside of the office. 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.

DirectAccess can be configured in a variety of ways to provide a transparent connection to the corporate network without requiring any user input. In order to enhance security, Microsoft IT requires two-factor authentication for remote workers, requiring a smart card in addition to a user ID and password. When Microsoft IT enables DirectAccess, Windows 7 securely directs requests for resources such as e-mail, shared folders, or access to intranet Web sites in the corporate network without requiring users to connect to a VPN.

Separate Connections to the Corporate Network and the Public Internet

DirectAccess supports intelligent routing, which directs corporate traffic through its secure connection while allowing public traffic to connect directly to the Internet through the user's Internet service provider (ISP) without passing through the corporate network. This separation of private and public data streams can be a cost benefit because companies do not need to pay for the bandwidth of Internet traffic being routed through the corporate network.

Intelligent routing is also a key feature that helps companies comply with international data transmission regulations. Ensuring that confidential data is being routed through the appropriate private network is especially important for remote users working in countries such as France and Switzerland that regulate how different types of data can be transmitted.

Seamless and Secure Access to Corporate Resources for Remote Workers

DirectAccess uses IPsec for authentication and encryption in order to provide a secure connection to the corporate network without having to use a VPN. Corporate network file shares, intranet Web sites, and line-of-business applications are accessible through DirectAccess wherever an Internet connection is available.

DirectAccess connects remote workers seamlessly to corporate resources. The ability for DirectAccess to provide an "always on" secure communication channel through the Internet using "standard" ports such as TCP 443 translates to significant productivity improvements for remote workers at their customer sites or in other remote locations with restrictive port or firewall policies. With DirectAccess, employees can access corporate resources from remote branch offices, extranets, or even while sitting at a Wi-Fi cafe.

Manageability

Not only does DirectAccess provide an enhanced end user experience, but also when using DirectAccess, Microsoft IT is better able to manage computer systems such as laptops that are frequently moved outside the corporate network. The key management benefits DirectAccess provides are described below.

Remote Computer Management

Systems that are not running DirectAccess are more of a challenge for Microsoft IT administrators to manage. When a laptop with Internet connectivity is running DirectAccess, the laptop is always connected to the corporate network. This "always on" connection promotes timely security scans, enables Helpdesk to "reach out" for remote assistance, simplifies updates to group policy, and allows the computer to pull down security and system updates as soon as they are required, *even if the user is not logged on.* This functionality gives Microsoft IT the opportunity to service remote machines on a regular basis and ensures that remote users stay up-to-date with company policies.

Monitoring and Reporting

Windows Server 2008 R2 provides built-in monitoring of the DirectAccess server and DirectAccess components through the DirectAccess Monitoring snap-in. The DirectAccess Monitoring snap-in provides the ability to monitor traffic activity, data, and control traffic counters and events for the different components of the DirectAccess server and the server's status.

System Design

This section of the document provides an overview of how DirectAccess works and discusses the underlying connectivity and security technologies that Microsoft IT has implemented as part of the DirectAccess system.

Architecture

The following figure illustrates the major components of the DirectAccess system.

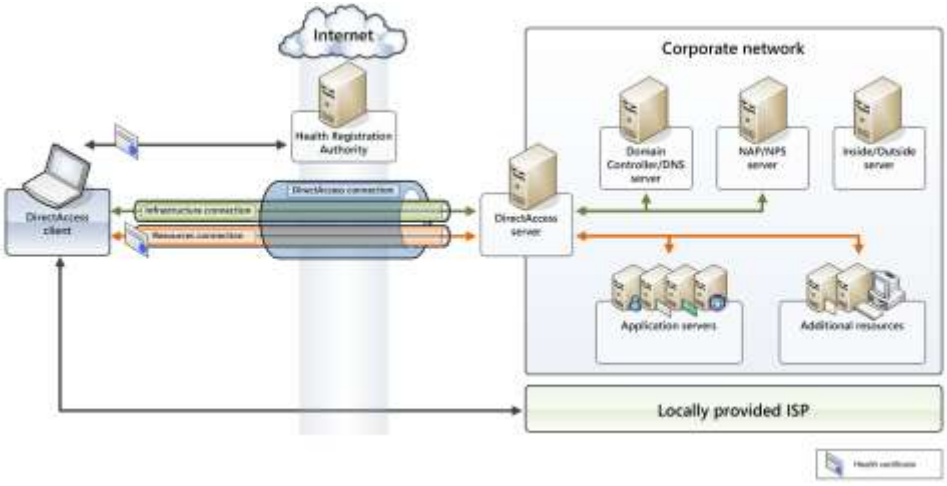

Figure 1. A schematic of Microsoft IT's DirectAccess implementation

Connectivity

The following technologies are used by DirectAccess to initiate and maintain a secure connection with the corporate network.

IPv6

DirectAccess clients maintain constant connectivity with the intranet, and Internet Protocol version 6 (IPv6) provides the end-to-end addressing necessary to accomplish this. Clients establish an IPv6 tunnel to the DirectAccess server, which acts as a gateway to the internal network. The preceding figure shows a DirectAccess client connecting to a DirectAccess server across the public IPv4 Internet. Clients can connect from behind a firewall using one of the transition technologies listed below.

IPv6 Transition Technologies

Because many organizations do not yet have IPv6 deployed in their IT infrastructure, DirectAccess includes IPv6 transition technologies to help ensure IPv6 connectivity.

Teredo and 6to4 are examples of IPv6 transition technologies. These technologies allow the use of IPv6 even if DirectAccess clients are on the IPv4 Internet and the network infrastructure does not yet support native IPv6 routing. IPv6 transition technologies can simplify and reduce the costs of an IPv6 deployment.

- **Teredo**: Teredo (RFC 4380) is an IPv6 transition technology used by Microsoft IT that provides IPv6 connectivity across the IPv4 Internet for hosts that are located behind an IPv4 network address translation (NAT) device and assigned a private IPv4 address.
- **6to4**: 6to4 (RFC 3056) is an IPv6 transition technology that provides IPv6 connectivity across the IPv4 Internet for hosts or sites that have a public IPv4 address.

IP-HTTPS

IP-HTTPS is a new protocol for Windows 7 and Windows Server 2008 R2 that allows hosts behind a Web proxy server or firewall to establish connectivity by tunneling IPv6 packets inside an IPv4-based HTTPS session. HTTPS is used instead of HTTP so that Web proxy servers will not attempt to examine the data stream and terminate the connection. Performance of IP-HTTPS may be lower than the other DirectAccess connection protocols.

Inside/Outside Determination

To determine the reachability of intranet resources and a computer's proximity to them, several configuration settings must be provided to the DirectAccess client. These settings are requested when the DirectAccess Management Console setup process is run, and consist of the following:

- The intranet IPv6 address prefix
- The DNS name for an intranet resource
- The IP addresses to which the DNS name of the intranet resource should resolve
- The HTTPS-based URL for the Inside/Outside Server

The DirectAccess client uses this information to independently determine whether intranet resources are reachable and whether the client is connected to the intranet or the Internet.

Security

DirectAccess supports a variety of complementary security components from which a company can choose in order to conform to its organizational security policies.

In its current deployment, Microsoft IT is using the following set of security technologies with DirectAccess: multifactor authentication, IPsec, and Network Access Protection. Each of these technologies is summarized below.

Multifactor Authentication

For enhanced security, DirectAccess can support two-factor authentication using smart cards. Microsoft IT's current implementation of DirectAccess requires that remote systems use a smart card for accessing corporate resources.

IPsec

DirectAccess uses Internet Protocol security (IPsec) to provide encryption for communications across the Internet. IPsec provides aggressive protection against attacks through end-to-end security. IPsec provides true end-to-end data transmission security, providing data protection all the way to the application servers.

IPsec enables DirectAccess to protect communication between any two authenticated people or systems, regardless of whether the computers are connected to a workgroup, a local area network, or other network.

Network Access Protection

Microsoft Network Access Protection (NAP) is a policy-enforcement platform built into Windows. NAP is designed to assess the health of any client attempting to access networked resources such as applications, data, and information, and drives clients towards compliance through NAP's remediation capabilities.

NAP is a key component of Microsoft IT security requirements. DirectAccess also integrates well with NAP to perform these critical functions:

- **Health Evaluation:** NAP provides a customizable definition of security and configuration "health" policy against which computers are evaluated for their compliance to that policy. Computers obtain NAP health certificates by contacting a NAP Health Registration Authority (HRA) and proving their compliance to a health policy that is located and evaluated on the NAP Server.
- **Network access control**: DirectAccess requires proof of health certificate to control or restrict access to the network. While a computer is healthy, it has complete access to the corporate network. Unhealthy systems will only be able to access remediation servers.
- **Automatic remediation**: For computers that are "unhealthy," NAP's automatic remediation feature drives the computer to a health state by automatically correcting those aspects of the computer's security, configuration, and state that are determined to be non-compliant, and then has the system automatically reconnect to the corporate network.
- **Compliance reporting**: NAP stores computer health policy compliance data and other related data in a database where it can be used for reporting purposes to assess the compliance state of machines, groups of machines, or an entire organization.

Server and Domain Isolation

Server and Domain Isolation allows administrators to dynamically segment the Windows environment into more secure and isolated logical networks based on IPsec policy without costly changes to the network infrastructure or applications. This creates an additional layer of policy-driven protection, helps protect against costly network attacks, and helps prevent unauthorized access to trusted networked resources, achieve regulatory compliance, and reduce operational costs. The Server and Domain Isolation solution is fully compatible with DirectAccess.

Security Best Practices

- Require two-factor authentication with smart cards when using DirectAccess
- Use NAP to enforce client health and compliance
- Use encryption on all communication to and from DirectAccess clients

Deployment Considerations

DirectAccess is a flexible solution that can be deployed in different ways to meet a company's specific requirements. This section discusses the options a company can choose from when considering how to deploy DirectAccess, which fall into three separate areas: the access model, the scalability model, and the deployment model. The choices available in each of these models are summarized below.

Choosing an Access Model

There are three access models from which to choose:

- **Full intranet access (end-to-edge)**: The Full intranet access model allows DirectAccess clients to connect to all resources inside the intranet. It does this by using IPsec-based tunnel policies that require authentication and encryption and IPsec sessions that terminate at the IPsec gateway. The IPsec gateway is a function that is hosted on the DirectAccess server by default, but can be moved to a separate computer.
- **Selected server access (modified end-to-edge)**: This model is very similar to the Full intranet access model previously described, with one important addition: communication between the DirectAccess client and the IPsec gateway is still protected by IPsec-based tunnel policies requiring encryption to the IPsec gateway, but this model also adds an additional authentication mechanism. By creating an additional IPsec rule requiring ESP+NULL or AH from the client to the application server, the client's communications will be encrypted to the IPsec gateway, but authenticated all the way to the application server. This allows the DirectAccess client to help ensure that they are communicating with the intended servers. Microsoft IT uses a combination of this model and the full intranet access model for DirectAccess implementation.
- **End-to-end**: The end-to-end access model extends these IPsec policies all the way to the application server. The DirectAccess clients use an IPsec transport policy that requires encryption and authentication that terminate at the application server. In this case the DirectAccess server/IPsec gateway acts as a pass-through device, allowing the IPsec connections to pass to the application servers.

Choosing a Scalability Model

There are two scalability models from which to choose:

- **Single server**: In the single server scenario, all of the components of DirectAccess are hosted on the same server computer. The benefit of this scenario is a relatively simple deployment, requiring only a single DirectAccess server. The limitations of this scenario are a single point of failure, and server performance bottlenecks can limit the maximum number of concurrent DirectAccess connections.
- **Multiple servers for high availability**: If high availability is a priority, the multiple server configuration will minimize any network outages. This is the model Microsoft IT has adopted, working with multiple DirectAccess servers and handling failovers via a DNS solution.

Choosing a Deployment Model

You can use the following methods to deploy and configure DirectAccess resources:

- **DirectAccess Management Console**: The DirectAccess Management Console provides several options for deploying DirectAccess. A setup wizard presents several questions to determine how the DirectAccess deployment should proceed, and before the changes are applied, the option of saving the settings into a set of script files is presented.
- **Scripted Installation using Netsh.exe**: For customized DirectAccess deployments that need to be modified to meet a unique set of needs, a scripted installation using Netsh.exe commands can be created. These custom scripted installations allow for maximum flexibility and the creation of unique solutions, including many permutations that are not covered in this case study.
- **Client Configuration using Group Policy**: DirectAccess works for managed computers who are domain-joined. Group Policy provides a policy-based method to create, distribute, and apply DirectAccess settings to clients, which allows for one-time and ongoing enforcement of DirectAccess settings. Group Policies are used by DirectAccess Setup and may optionally be used in a scripted setup.

Deployment Best Practices

- If possible, configure the intranet routing infrastructure to support native IPv6. Computers running Windows Vista®, Windows Server 2008, Windows 7, and Windows Server 2008 R2 are configured to use IPv6 by default. Native IPv6 transport allows for end-to-end IPsec between the DirectAccess client and the resource to which it connects.
- Deploy IP-HTTPS as soon as possible. Microsoft IT has seen UDP 3544 (Teredo) blocked outbound by many ISPs, corporations, MANs, and others, but TCP 443 (IP-HTTPS) is usually an open outbound port.
- Split-brain DNS environments—where the same namespace is used with different records—are challenging. DirectAccess clients are essentially forced to resolve either the internal or the external namespace via the Name Resolution Policy Table (NRPT), but the DirectAccess clients cannot resolve both. For Microsoft IT, the internal namespace is the preferred choice, with NRPT exceptions for the external FQDNs that need to be resolvable by the clients.
- The Inside/Outside Server should be treated as a very important part of the remote network access infrastructure. Because of its mission-critical role, an organization should

deploy the Inside/Outside Server using failover clustering on a high-availability network in order to minimize downtime.

- Use Group Policy to manage system configurations, and make sure to first perform a pilot test for all GPOs by restricting access down to a pilot users (and systems) security group.
- Implement DirectAccess with NAP to enable system health monitoring and support automatic remediation of computer health issues. Microsoft IT has opted to deploy the NAP HRA and remediation servers on the Internet in order to provide the benefits of NAP to computers that are not running DirectAccess in addition to those that are.

Benefits

By implementing DirectAccess, Microsoft IT has derived a number of benefits for end users and administrators alike as described below:

- **Always-on connectivity**: Whenever the client computer is online (on the Internet), it has a connection to the intranet. This connectivity makes remote client computers easy to access and update, and makes intranet resources always available.
- **Seamless connectivity**: DirectAccess provides a consistent connectivity experience whether the client computer is local or remote. It allows users to focus more on productivity and less on connectivity options and process, which can result in decreased training costs for users and fewer support incidents. In addition, DirectAccess' support of IP-HTTPS improves client connectivity rates even when behind firewalls and proxies.
- **Secure connectivity**: Security is derived from utilizing IPsec over IPv6 with two-factor authentication and by using NAP to ensure computers are compliant with IT security and configuration requirements before they are given access to the corporate network.
- **Integrated solution**: DirectAccess fully integrates with Server and Domain Isolation and Network Access Protection (NAP) solutions, resulting in security, access, and health requirement policies that seamlessly integrate between computers on the intranet and remote computers.
- **Remote management**: IT administrators can connect directly to clients to monitor them, manage them, and deploy updates, even when the user is not logged on but has Internet connectivity. This can reduce the cost of managing remote computers by keeping them up-to-date with critical updates and required configuration changes.
- **Cost savings**: In addition to technological benefits, DirectAccess can be an important cost-saving tool that enables Microsoft Internet connected offices (ICOs) to maintain efficient and secure connections to the corporate network instead of spending an estimated $300,000 needed to upgrade each facility to a dedicated connection.

Conclusion

Microsoft IT is addressing the productivity and security needs of the company's remote workforce by implementing DirectAccess as the preferred secure network access technology. By using DirectAccess to replace traditional VPN solutions, Microsoft IT can offer end users a completely transparent connection to the corporate network anywhere they have access to the Internet. DirectAccess enables management of computer systems at all time, as if the computer were physically located on the corporate network. At the same time, remote computers running DirectAccess with NAP can be constantly monitored for system health;

administrators have the ability to update the system and automatically remediate computer health issues, even when the user is not logged on.

DirectAccess is compelling not only from a usability and manageability perspective, but is expected to reduce costs as well: the ability for DirectAccess to be used at Microsoft Internet connected offices will save the company an estimated $300,000 per facility that would otherwise be required to upgrade to a dedicated connection.

Microsoft IT sees DirectAccess as the next generation of secure network access technology that, although in the early stages of use, will become the preferred technology used to remotely connect to the corporate network, handling over 90 percent of Microsoft domain-joined remote clients in the next three years.

For More Information

For more information about Microsoft products or services, call the Microsoft Sales Information Center at (800) 426-9400. In Canada, call the Microsoft Canada information Centre at (800) 563-9048. Outside the 50 United States and Canada, please contact your local Microsoft subsidiary. To access information via the World Wide Web, go to:

http://www.microsoft.com

http://www.microsoft.com/technet/itshowcase

www.microsoft.com/directaccess

† IDC Worldwide Quarterly PC Tracker, December 2008.
‡ IDC, "Worldwide Mobile Worker Population 2007–2011 Forecast," Doc #209813, Dec 2007.