SEAMLESS CONNECTIVITY: INTRODUCING MICROSOFT WINDOWS SERVER 2008 R2 DIRECTACCESS

The Microsoft® Windows® 7 and Windows Server® 2008 R2 operating systems introduce DirectAccess, a new feature designed to provide remote users with seamless, secure access to internal enterprise networks. This article describes the technologies underlying DirectAccess as well as best practices to help administrators successfully deploy, monitor, and manage it in their own environments.

Comparing Traditional Solutions with DirectAccess

Traditional VPN solutions generally require mobile users to carry out several steps, including launching the VPN client, providing login credentials, and waiting for authentication. For some enterprise networks that must check the client system’s health before allowing a connection, establishing a VPN connection can potentially take several minutes. This process can become even more cumbersome as users move around and as connections to the Internet become intermittent—whenever users lose their Internet connection, they must go through the same process to reestablish the VPN connection. VPN connections can also be problematic in some environments that filter out VPN traffic, and if the VPN implementation forces both Internet and intranet traffic to be routed through the VPN, performance can become a problem.

Utilizing application gateways such as the Citrix Access Gateway™ or Microsoft Office Outlook® Web Access solutions can provide an alternative to a VPN connection, but these solutions are not designed to provide access to all intranet resources. Outlook Web Access, for example, offers access to e-mail, but not to file shares or internally hosted application servers and Web sites.

Today’s enterprise workforce is more mobile than ever, requiring access to intranet resources from a wide range of locations outside the office, not only at home, but also at hotels, airports, coffee shops, and other hotspots all over the world. Although traditional solutions such as virtual private networks (VPNs) and application gateways can offer remote access to intranets and applications, these approaches also come with several disadvantages—and for IT administrators, supporting this type of remote access in a secure, seamless, and manageable way can be difficult.

To help overcome these challenges, the Microsoft Windows 7 and Windows Server 2008 R2 operating systems introduce DirectAccess, a new feature designed to maintain a seamless, secure bidirectional connection between Windows 7–based client systems and enterprise intranets without requiring a VPN connection. By doing so, it can provide remote users with the same experience they would have when they are physically in the office—including comprehensive access to intranet resources such as file servers, application servers, e-mail, and internal Web sites—while also helping significantly simplify remote management for administrators.
Traditional VPN solutions can also present significant challenges for IT administrators. Because the remote clients are not always connected to the VPN, pushing software updates and performing other management tasks can be difficult. Ensuring secure communication from the remote clients over the Internet to the enterprise intranet is also challenging.

The DirectAccess feature is designed to overcome these obstacles by maintaining a bidirectional connection between client systems and the intranet as long as the client is connected to the Internet—enabling remote users to access enterprise intranet resources without a VPN connection while also offering enhanced manageability for administrators (see Figure 1). For example, to help reduce unnecessary intranet traffic, DirectAccess separates intranet traffic from Internet traffic by default, routing only traffic bound for the intranet to the DirectAccess server (although IT staff can optionally configure DirectAccess to send all traffic through the DirectAccess server). And unlike traditional VPN solutions, which typically provide all-or-nothing connectivity to the intranet, DirectAccess can provide different levels of access control. Administrators can use Group Policy to control resource accessibility, granting remote users unlimited access to all intranet resources or limiting that access to specific applications, servers, or subnets.

The automatic bidirectional connection provided by DirectAccess also helps simplify remote client management: as long as a client system is online, it is visible on the intranet, and administrators can remotely push software updates and perform other management tasks just as if the client were physically connected to the intranet. This capability helps ensure remote clients can be updated regularly.

UNDERSTANDING THE UNDERLYING TECHNOLOGIES

The DirectAccess feature is built on IP Security (IPsec) and IP version 6 (IPv6) technologies. It uses computer certificates to authenticate remote client accounts, enabling seamless connectivity without requiring end users to provide login credentials.

**IPsec authentication and encryption**

DirectAccess uses IPsec to support secure communication between remote clients and the enterprise intranet. IPsec is a set of open standards that provides a flexible framework designed to secure network communications by authenticating and encrypting each IP packet of a data stream. DirectAccess authenticates both the clients and users with IPsec, and administrators can manage the clients before users log on. DirectAccess also uses IPsec to encrypt communication across the Internet. DirectAccess clients establish an IPsec tunnel for the IPv6 traffic to a DirectAccess server, which acts as a gateway to the intranet.

DirectAccess clients can connect to a DirectAccess server across the public IPv4 Internet, and can connect even if they are behind a firewall. Using the Encapsulating Security Payload (ESP) protocol, DirectAccess establishes two IPsec tunnels: one that uses a computer certificate and another that uses both a computer certificate and user credentials. The first tunnel provides access to an intranet Domain Name System (DNS) server and domain controller, allowing clients to download Group Policy Objects and request authentication on the user’s behalf. The second tunnel authenticates users and provides access to intranet resources and application servers; this tunnel would need to be established, for example, before Microsoft Outlook could download e-mail from a Microsoft Exchange server on the intranet.

**IPv6 and transitional technologies**

IPv6 provides the foundation of the DirectAccess solution. This implementation enables DirectAccess clients to be assigned as globally routable addresses. For organizations that already have a native IPv6 infrastructure, DirectAccess can provide a seamless connection between DirectAccess clients and a DirectAccess server. In addition, if a remote client connects directly to the IPv6 Internet and has a globally routable IPv6 address, the end-to-end DirectAccess connection can be established using native IPv6.

The protocol used to connect the clients to the intranet depends on the type of Internet connection. IPv4 is still the dominant protocol on the Internet and on enterprise intranets, and DirectAccess can be
used with IPv6 transitional technologies without the need for organizations to upgrade their existing infrastructure.

Figure 2 illustrates the typical process for a DirectAccess client to connect to a DirectAccess server. In most cases, connecting from the IPv4 Internet requires the 6to4 and Teredo tunneling protocols. If the client has a public, routable IPv4 address, then it uses the 6to4 protocol to tunnel IPv6 over the IPv4 Internet. If the client is behind a Network Address Translation (NAT) device such as a home router and therefore has a private, non-routable IPv4 address, then it uses the Teredo protocol. If the 6to4 or Teredo protocols are blocked by a firewall, then the client can use an IP over HTTP over Secure Sockets Layer (IP-HTTPS) session, which tunnels IPv6 over an IPv4 HTTPS session to get through the firewall. IP-HTTPS is used as a last resort because the additional overhead associated with HTTPS can reduce performance.

DirectAccess clients can only access intranet resources with an IPv6 address; reaching IPv6 resources on an IPv4-based intranet requires Intra-site Automatic Tunnel Addressing Protocol (ISATAP) or NAT-Protocol Translation (NAT-PT). ISATAP is an IPv6 transition mechanism designed to transmit IPv6 packets between dual-stack nodes (running IPv4 and IPv6 at the same time) on top of an IPv4 network, and provides connectivity between IPv4 and IPv6 on IPv4-only intranets. DirectAccess uses ISATAP to provide this connectivity to the intranet resources made available to the DirectAccess clients.

Hardware-based NAT-PT provides an alternative to ISATAP. NAT-PT is typically provided by Layer 2 and Layer 3 infrastructure switches and routers, and provides the required IPv4-to-IPv6 translation required for the DirectAccess clients to access intranet resources. In addition, deploying NAT-PT devices can enable DirectAccess clients to access intranet resources that do not yet support IPv6.

**CONFIGURING AND DEPLOYING DIRECTACCESS**

Each DirectAccess server must be running Windows Server 2008 R2 and have the DirectAccess feature installed. Because these servers reside at the edge of the intranet, they must also be configured with at least two physical network interfaces: one connected to the Internet and one connected to the intranet. The interface connected to the Internet must have two consecutive, publicly addressable, static IPv4 addresses bound to it, and cannot be behind a NAT device. The DirectAccess server must be joined to a Microsoft Active Directory® domain and should be dedicated to DirectAccess. DirectAccess clients must be running Windows 7 Enterprise or Ultimate or Windows Server 2008 R2, and must be joined to the Active Directory domain.

DirectAccess also requires the following infrastructure components:

- **Active Directory**: Installing the Active Directory Domain Services role on a server running Windows Server 2008 R2 provides directory services, user accounts, and security groups. At least one domain controller is required.

- **Group Policy**: Group Policy provides centralized management of security policies on the DirectAccess clients.

- **Public Key Infrastructure (PKI) Active Directory Certificate Services**: These services are required for the issuance of computer certificates used for authentication. All Secure Sockets
Layer (SSL) certificates must have a certificate revocation list (CRL) distribution point that is reachable from a publicly resolvable fully qualified domain name (FQDN), regardless of whether the DirectAccess client is on the Internet or an intranet.

- **IPsec policies**: Administrators can use Windows Firewall with Advanced Security to manage IPsec policies and create exception rules.

- **Internet Control Message Protocol version 6 (ICMPv6) Echo Request traffic**: Separate inbound and outbound rules are required to allow ICMPv6 Echo Request messages.

- **IPv6 and transition technologies**: These technologies provide access from the IPv4 Internet to IPv6 DirectAccess resources.

Figure 3 shows the basic steps for deploying DirectAccess. As shown in the figure, using the Dell™ Systems Build and Update Utility or the Dell Lifecycle Controller on an 11th-generation Dell PowerEdge™ server can streamline OS deployment and complete several DirectAccess deployment processes in one step, helping reduce total deployment time. In addition, the Lifecycle Controller can provide the latest compatible drivers during Windows Server 2008 R2 deployment.

After deploying the Windows Server 2008 R2 OS, administrators next deploy and configure DirectAccess on the remote clients, DirectAccess server, infrastructure servers, and application servers. Available deployment methods include using the DirectAccess Management Console, the Netsh.exe tool for scripted installation, or Group Policy Objects for manual client configuration. The DirectAccess Management Console helps simplify configuration by providing a set of steps and wizard pages (see Figure 4); the console is located in the Windows Server 2008 R2 Administrative Tools and can be installed through the Add Features function.

To help increase throughput, avoid downtime, and protect against a single node failure, best practices recommend using two Microsoft Hyper-V™ host servers with failover clustering to support a single shared DirectAccess server in a virtual machine. Before running the DirectAccess Setup Wizard, administrators should carry out the following recommended configuration steps on the Hyper-V servers:

- Ensure that the servers have identical hardware with Data Execution Prevention and Intel® Hyper-Threading Technology enabled. Each server needs at least three network adapters to serve the Internet, intranet, and failover clustering.
- Join the servers to the domain and deselect IPv4 and IPv6 on the network adapter for the Internet connection.
- To enhance performance, open the Failover Cluster Manager snap-in, do not set a preferred owner, and set the Failback option in the virtual machine properties to “Prevent Failback.”
- To help accelerate client reconnection when a node fails, enable NLBSFlags in the registry by setting the HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent\Oakley\NLBSFlags value to 1.1

MONITORING DIRECTACCESS

Administrators should monitor DirectAccess to help them quickly identify and troubleshoot problems. They can perform local monitoring using the DirectAccess Monitoring snap-in for the Microsoft Management Console, which is incorporated into Windows Server 2008 R2 and installed with the DirectAccess server feature. An enterprise deployment of multiple DirectAccess servers can be created by installing a management pack for Microsoft System Center Operations Manager 2007 with Service Pack 1 (SP1).

DirectAccess Monitoring snap-in

The DirectAccess Monitoring snap-in enables administrators to locally monitor server status, traffic patterns, and events. The overall DirectAccess server status is based on the state of the Teredo Relay, Teredo Server, 6to4, IP-HTTPS, ISATAP, Network Security, and DNS Server components (see Figure 5).

Each component can be in a healthy, warning, or error state. If a component is in a warning or error state, a detailed error message is displayed along with suggestions to correct the problem. Clicking the Details button next to each component launches performance-monitoring and load-performance counters associated with that component, helping administrators to identify potential problems.

System Center Operations Manager 2007

A management pack for System Center Operations Manager 2007 with SP1 supports centralized, one-to-many monitoring of multiple DirectAccess servers in large enterprise deployments. In addition to proactive monitoring, System Center Operations Manager adds enhanced capability for alarms and reporting and provides a convenient view showing the DirectAccess servers and their component states.

In addition, with the latest release of the Dell OpenManage™ suite, the Dell Management Console Powered by Altiris™ can help administrators manage the DirectAccess infrastructure. The Dell Management Console enables administrators to monitor both Dell and non-Dell devices; monitor processors, memory, and alerts; push BIOS, firmware, and driver updates to Dell PowerEdge servers; and push configuration changes to multiple devices simultaneously.

PROVIDING SEAMLESS, SECURE REMOTE CONNECTIVITY

Although traditional solutions such as VPNs and application gateways can provide the remote connectivity required by an increasingly mobile workforce, these approaches can also present obstacles for end users and a myriad of difficulties for IT administrators. The DirectAccess feature incorporated into the Microsoft Windows 7 and Windows Server 2008 R2 operating systems is designed to overcome these challenges—not only helping provide seamless, secure connections for remote users, but also helping significantly simplify ongoing management for enterprise administrators.

Steven Grigsby is a software engineer in the Dell Server Operating Systems Group. He has a B.S. in Computer Science from the University of Oklahoma.

Gong Wang is a software engineer in the Dell Server Operating Systems Group. He has an M.S. in Human-Computer Interaction from the Georgia Institute of Technology.