DirectAccess: The New VPN
DirectAccess: The New VPN

Mark Mizrahi, MCSE, CEH, CEI Instructor, MCT, MCTS, MCITP

Introduction

Windows 7 and Windows Server 2008 R2 have a new built-in architecture designed to create a Virtual Private Network (VPN) connection. This new technology is known as DirectAccess (DA) and is forecasted to replace traditional VPN connections for most of your remote access needs. DA can be installed as a Server Role on the inbound server. This role comes bundled with Windows Server 2008 R2 at no additional cost. The Windows 7 client is configured by default to optimize the usage of your DA infrastructure.

This white paper is divided into eight sections. Read all sections at least one time to understand the total concept of DA. Then go the specific sections as needed to reference and refresh your knowledge.

1. Defining DirectAccess

What is DirectAccess?

DirectAccess (DA) is a new feature in the Windows 7 and Windows Server 2008 R2 operating systems that allows users to remotely connect to their corporate network without a traditional VPN client configuration or application. It gives users the ability to seamlessly make a connection to their corporate network any time they have a Internet connection. With DA users are securely directed to their applications, email, shared folders and intranet websites. Public Internet access is available from the client directly or through the DA infrastructure. DA increases productivity for remote users by offering the same transparent look and feel when connecting from outside the office as if they were connecting from inside the office.
Benefits of DA

DA is an “Always On” remote corporate connection when the mobile user is connected to the Internet. DA leverages Windows 7 features, such as Federated Search, which searches intranet resources, and Folder Redirection, which synchronizes files across the network, remote users will be able to find and access their corporate resources seamlessly, wherever they are connected to the Internet. Another important benefit, particularly for Helpdesk and IT admins, is the two way, bi-directional connection allowing the DA Client to be remotely administered and configured, thereby reducing the maintenance and support costs of mobile users.

Manageability of Remote Users

DA establishes a bi-directional connection. With DA, IT admins can manage and support mobile computers very easily, so long as the computer remains connected to the Internet, even if the user is not logged on. Without DA, managing remote computers is only possible when the users connect to a VPN infrastructure or physically come in to the office. IT admins can remotely manage computers, update Group Policy settings, and distribute software updates any time the remote computer has Internet connectivity, even if the user is not logged on. This flexibility allows IT admins to manage the DA remote computers on a regular basis and ensures that mobile users stay up-to-date with security and system health policies.

2. Secure Network Infrastructure

Protocol. DA provides secure and flexible access to your internal corporate network. The protocol that DA uses is Internet Protocol version 6 (IPv6) and Internet Protocol security (IPsec).

Authentication. DA authenticates the computer and uses Public Key Infrastructure (PKI) for access control, allowing the computer to connect to the corporate network using certificates before the user logs on. DA can also authenticate the user and supports two-factor authentication using smart cards.

Encryption. DA uses IPsec to provide encryption for communications when connecting across the Internet. Encryption methods such as DES 56bit encryption and 3DES which uses three 56 bit encryption keys are used.

Access Control. Some of the choices that can be implemented through DA include which corporate resources different users can access. IT Admins can grant DA users unlimited access to the corporate network or only allow them to use specific applications and access specific servers or subnets.

IT Simplification and Cost Reduction. DA separates intranet from Internet traffic, which reduces unnecessary traffic on the corporate network by sending traffic destined for the corporate network through the DA server. Optionally, IT admins can configure DA clients to send all traffic through the DA server regardless of their intranet or Internet needs.

Integrating Network Access Protection (NAP). DA can be integrated with a NAP network which performs Health compliance checking, to check the health status of client operating systems before allowing them to connect to internal corporate resources.
3. How DA Works

DA clients use the following steps to connect to their corporate intranet resources:

1. The DA client computer running Windows 7 detects there it is a network connection present.
2. The DA client computer attempts to connect to an intranet Web site that an administrator specified during DA configuration.
3. The DA client computer connects to the DA server using IPv6 and IPsec.
4. If a firewall or proxy server prevents the client computer using IPv6to4 or Teredo from connecting to the DA 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 DA client and server authenticate each other using computer certificates.
6. By validating via Active Directory group memberships, the DA server verifies that the computer and user are authorized to connect using DA.
7. If Network Access Protection (NAP) is enabled and configured for health validation, the DA client obtains a health certificate from a Health Registration Authority (HRA) located on the Internet prior to connecting to the DA server.
8. The DA server begins forwarding traffic from the DA client to the corporate intranet resources to which the user has been granted access.
4. DirectAccess Requirements

The hardware requirements for DA Server (DAS) are the same as those for Windows Server 2008 R2. DAS requires Windows Server 2008 R2. More than one DAS may be needed depending on your deployment and scalability requirements. For reasons related to performance and security, Microsoft recommends that these servers run DA only.

DA requires the following:

- **Active Directory**: At least one AD domain must be deployed. Workgroups are not supported.
- **Group Policy**: Group Policy can be used to deploy client policies for DA
- **Domain Controller**: At least one domain controller in the domain containing user accounts must be running Windows Server 2008 or newer.
- **Public Key Infrastructure (PKI)**: Required to issue certificates. External certificates are not required.
- **SSL certificates**: All SSL certificates must have a CRL distribution that can be reached through a publicly resolvable FQDN while either local or remote.
- **IPsec policies**: DA uses IPsec policies, so administrators must be familiar with this technology.
- **Physical Network Interfaces**: Each DA server must have at least two physical network interfaces.
- **Transition Technologies**: ISATAP, Teredo, 6to4, and IPv6 must be available for use on the Direct Access Server.
- **Windows Server 2008 R2**: Windows Server 2008 R2 is on the DAS that will host, manage, and as necessary, either terminate or pass through the IPsec connections. DAS is a server function and cannot be installed on a client machine running Windows 7.
- **Windows 7 Client**: The DA Client can only be Windows 7 Enterprise or Ultimate SKUs that are domain-joined. Clients not joined to a domain are not supported. Clients running Windows Vista or earlier versions of Microsoft’s client operating system’s are not supported.

No IPv6 in your corporate network? No problem. Organizations not ready to fully deploy IPv6 can use IPv6 transition technologies such as ISATAP, 6to4, and Teredo to enable clients to connect across the IPv4 Internet and to access IPv4 resources on the corporate network.

5. Wikipedia Definition of ISATAP, Teredo, and 6to4

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 transition mechanism meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network. Unlike 6over4 (an older, similar protocol using IPv4 multicast), ISATAP uses IPv4 as a virtual nonbroadcast multiple-access network (NBMA) data link layer, so that it does not require the underlying IPv4 network infrastructure to support multicast.

Teredo is a tunneling protocol designed to grant IPv6 connectivity to nodes that are located behind IPv6-unaware NAT devices. It defines a way of encapsulating IPv6 packets within IPv4 UDP datagrams that can be routed through NAT devices and on the IPv4 Internet.
6to4 is an Internet transition mechanism for migrating from IPv4 to IPv6, a system that allows IPv6 packets to be transmitted over an IPv4 network (generally the IPv4 Internet) without the need to configure explicit tunnels. Special relay servers are also in place, which allow 6to4 networks to communicate with native IPv6 networks.

6. Designing a DA Solution
Before deploying DA, your environment must meet all of the network, infrastructure, hardware, and software requirements. When designing DA, the physical location of the servers is important. The following diagram shows one suggestion, and is sometimes considered a best practice. Based on the architectural details of your organization, you might decide to move servers around slightly.
Firewall Location Port/Protocol Direction & Destination

- Outer firewall IPv6 Inbound and Outbound
- Outer firewall IP Protocol 50 (ESP) Inbound and Outbound
- Outer firewall UDP 3544 (Teredo) Inbound
- Outer firewall IP Protocol 41 Inbound and Outbound
- Inner firewall UDP (AuthIP) Inbound and Outbound
- Outer firewall TCP 443 (SSL) Inbound and Outbound
- Inner firewall IP Protocol 50 (ESP) Inbound and

Split Tunneling Configuration

The default, and also the most common configuration, is to allow remote DA clients the ability to access the Internet, the corporate network, and their local IP subnet simultaneously. DA clients are configured to route all enterprise name resolution requests to their corporate DNS server(s), and unrecognized name resolution requests to their ISP’s DNS server(s). This feature is known as split tunneling.

The network administrator can disable split tunneling through Group Policies, if desired. When split tunneling is disabled, all traffic from the client will be routed to the corporate network over an IP-HTTPS tunnel. Clients who have had split tunneling disabled will still be able to access any resources on their local network but any network traffic that must cross a network router will be forwarded to the DA Server (DAS).

The IP-HTTPS protocol is always used when split tunneling is disabled. To reduce the load on the DA Server, packets that are originally destined for the corporate network will be encrypted, while packets that are originally destined outside of the corporate network will be left unencrypted.

The Group Policy location to manage Split Tunneling is Computer Configuration\Administrative Templates\Network\Network connections\ Default value: disabled

Group Policies can also configure Windows Firewall for advanced configuration options such as per-application control of split tunneling. This allows for more granular control over which applications are allowed to be access on the corporate network using DA while remotely connected.
Benefits of the Edge-To-Edge model

- Architecture similar to current VPN deployments
- Does not require IPSec traffic in the corporate network
- Works with any IPv6 capable application servers

Infrastructure Considerations

IPv6: DA leverages the IPv6 protocol to provide end-to-end connectivity between client computers and corporate resources. This means that Windows 7 DA enabled clients will have access only to those servers in your enterprise network that have a reachable IPv6 address. Those servers can obtain IPv6 connectivity from native IPv6 or an IPv6 transition technology. Although IPv6 is a requirement for DA, IPv6 does not have to be enabled on network infrastructure (such as routers), only on the client and server operating systems.

By default when you install DA, all Windows clients and servers in your network will automatically find the ISATAP server and begin using IPv6, so DA clients have no problems accessing Windows servers.

For IPv6 to work properly, ICMPv6 must not be blocked at the network firewall.
A DA client can still access an Internet resource using the IPv4 protocol. It is only when the client connects into a corporate resource that it must use IPv6.

IPv6 and IP protocol 41 (which is used by ISATAP and 6to4 transition technologies) must be allowed to pass at the corporate firewall.

Teredo must also be allowed to pass at the corporate firewall. This means that UDP/IPv4 port 3544 must be allowed in.

**NAT-PT:** A Network Address Translation – Protocol Translation (NAT-PT) device can be deployed to provide DA client computers access to IPv4 only resources in the corporate network. NAT-PT is generally configured to provide coverage for a particular DNS namespace, and once implemented, will make the necessary translations allowing DA clients to access any IPv4 resources located in that namespace.

The configuration of NAT-PT is beyond the scope of this document, but the devices are generally available from Layer 2 and Layer 3 switch and router vendors.

**IPsec:** DA achieves confidentiality through the use of IPsec with ESP+Encryption. Integrity of the data can be provided by IPsec with AH or IPsec with ESP+NULL encryption. The IPsec policies for either of these options can also be configured to require machine or user authentication (or both). A new feature of Windows Server 2008 R2 is the ability to create Authentication-Only IPsec which provides only authentication without integrity or encryption.

To provide the highest level of protection and interoperability, Microsoft recommends that you use

- IPsec with ESP+Encryption for confidentiality and
- IPsec with ESP+NULL encryption for integrity and authentication.

This combination is widely supported in the industry and will work through NAT devices, providing improved connectivity over the other options.

**DNS:** DA clients first query the DNS for the name isatap, and they also make queries to the DNS using the ISATAP protocol. All DNS servers must be able to resolve the ISATAP and must be listening on the ISATAP interface.

There are three main steps involved in implementing this:

- Selecting and upgrading some or all DNS servers to Windows Server 2008 SP2 or

  **Windows Server 2008 R2**
  - Unblocking ISATAP name resolution on all DNS servers
  - Configure the Name Resolution Policy Table (NRPT) for DA Clients so that each set of DNS servers responds to name resolution requests specific to its domain.
7. Step-by-Step Installation of DA

Although not a complete list, the following steps will prove helpful, as it has for me, getting started with the installation and setup of the DA infrastructure.

1. Install Windows Server 2008 R2 Enterprise Edition onto Server-based hardware with two physical NICs.

2. Join the Server to a Windows Domain. Although the DAS will function without being a member of the domain, Microsoft strongly recommends that the DAS be domain-joined.

3. Configure the DAS so that it is in the perimeter network with one NIC connected to the Internet and the other NIC connected to the corporate network. Ensure that both NICs are enabled and have their respective IPv4 addresses configured (if there is no native IPv6 connectivity available). This is critical for DAS to derive its configuration information automatically otherwise detailed configuration will need to be entered manually.

4. Verify that the firewall ports listed in the Subnet Configuration section of this white paper are opened on the Perimeter and Internet facing firewalls.

5. The DA Server will need at least one static address (IPv4 or IPv6, most likely IPv4) that is externally resolvable through DNS. Ensure that an IPv4 address is available and that you have the ability to have that address published in your externally facing DNS.

6. IPv6 - If your organization has disabled IPv6 on clients and/or servers, that restriction needs to be removed.

7. You must create a security group in Active Directory that contains the client machine accounts you wish to be DA enabled.

8. A web server (ISS) will be installed on the Direct Access Server.

9. Physical Network Interface - One of those two interfaces will end up being designated as the "Internet facing interface." That interface will require:
   a. Static DNS settings: The Internet facing interface must be configured with static DNS settings.
   b. Two, consecutive, public IPv4 addresses: On the Internet facing interface must be configured with two, consecutive, public IPv4 addresses (both IPv4 addresses are assigned to the same interface).

10. Windows Firewall - On the DAS server, ensure the Internet interface is configured to be either a Public or a Private interface (depending on your network design) and the Enterprise interface is configured to be a Domain interface. No other combinations are supported.

Install the Direct Access Management feature.

1. Open Server Manager
2. Highlight Features
3. Click Add Features Link
4. Select Direct Access Management Console and click Add Required Features in the pop-up window to add the GroupPolicy Management feature
5. Click Next, then click Install
6. Click Close to finish the installation.
Finally, run the DA Setup Wizard which will simplify the installation of DA by providing a list of questions. Once all the questions are answered, the information can either be saved as a set of script files for future use, or the answers can be applied directly.

Run the Direct Access Wizard
- Go to **Start** | **Run** and type **mmc**
- Hit **Enter**
- Go to **File** | **Add/Remove Snap-In**
- Click **Direct Access Server Management** in the left-hand pane of the Add or Remove Snap-Ins window and click **ADD**
- Click **OK**
- Expand Direct Access in the left-hand pane of the MMC
- Click on **Setup**
- Provide appropriate answers and click **Finish** when done

8. Troubleshooting
   DA Not Working? Try these Troubleshooting steps.

Troubleshooting Direct Access will involve all the legacy network troubleshooting tools such as PING, and DA specific tools.

Errors found during the DA Setup Wizard will be logged to C:\windows\tracing\DA.log.

Problem resolution will involve some or all of the following steps:
1. Determine whether the remote user can access Internet resources?
2. Determine whether the Network Connection icon displays Internet and Corporate access. If it says Local and Internet Access, there is no connection to the DA server.
3. Right click the network connection icon and select **Diagnose and Repair**
4. Ping a highly available internal server
   a. Is ping and name resolution successful?
5. From a **cmd** window, run **netsh** name show policy
   a. Any output other than the words “DNS Name Resolution Policy Table Settings” is a success.
6. Run **gpupdate /force**
7. Run **netsh int teredo show state**
   a. Verify Teredo’s state is ‘Qualified’ unless IP-HTTPS is being used (client is behind a proxy).
8. Use standard IP troubleshooting commands

Do not use NSLOOKUP when troubleshooting Direct Access issues. NSLOOKUP is not Name Resolution Policy Table (NRPT) aware, and will return improper results.
Summary

DA offers transparent, secure and highly available remote access to the corporate network needed by your remote users. In addition to Windows Server R2 DA will require Windows 7 Enterprise or Ultimate and a little planning on the back-end such as setting up an Active Directory based Public Key Infrastructure and IPv6. Once implemented it will make IT administrators, remote users and management very happy. I am providing a link for your viewing pleasure that shows a recorded webcast of the DA setup. Copy and paste this link into your Browser’s Address bar http://technet.microsoft.com/en-us/edge/directaccess-configuration-windows-7-demo-screencast-1-of-5.aspx and you will see a wonderful demonstration. You will find other useful webcasts from this webpage. Enjoy your new technology! If you have any questions or comments send me an e-mail to: markmiz@comcast.net; I’d love to hear from you.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

- Administering and Maintaining Windows 7 (M50292)
- Implementing Forefront Threat Management and Unified Access Gateway 2010 (M50357, M50402)
- Implementing Forefront Unified Access Gateway 2010 (M50402)
- Installing and Configuring Windows 7 Client (M6292)
- MCITP: Enterprise Administrator e-Camp
- MCITP: Server and Enterprise Administrator Combo Boot Camp
- MCITP: Windows 7 Enterprise Desktop Administrator Boot Camp
- MCTS: Windows 7 Certification Boot Camp

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

About the Author

Mark Mizrahi has been a Microsoft Certified Systems Engineer (MCSE) since Windows NT3.51. He holds a CEH Certified Ethical Hacker Security Certification and is a CEI Certified EC-Council Instructor. He is a Microsoft Certified Trainer (MCT) and MCTS and MCITP for Windows Server 2008, Vista, and Windows 7. He currently teaches Microsoft curriculum for Global Knowledge and other training vendors. Mark is president of Standard Computer Services and consults for various Fortune 500 companies. He designs and implements web-based Internet Security and Video Surveillance Systems for a diversified customer base. Keeping up the various hacking methods is part of his daily intake of information, and he loves sharing it with this clients and students.