Configure network services and access

The Configure Network Services and Access domain is another with just one objective tested on the 70-411 exam: Configure DirectAccess. DirectAccess is an improved alternative to a VPN that was first introduced in Windows Server 2008 R2 and Windows 7. If you earned your last certification before the release of Windows Server 2008 R2, you might have missed this major new technology completely. Even if you are already familiar with DirectAccess in Windows Server 2008 R2, you should know that this feature has changed for the better in Windows Server 2012.

DirectAccess in Windows Server 2008 R2 and Windows 7 was a very promising technology, but it was difficult to configure. In Windows Server 2012 and Windows 8, the infrastructure requirements of this technology have been simplified along with the configuration steps. At the same time, its feature set has expanded considerably.

For the 70-411 exam, you first need to understand basic DirectAccess concepts and components. You will also need to know how the infrastructure requirements to support DirectAccess clients differ to support various features. Finally, you will need to know how to configure DirectAccess by using either the GUI or Windows PowerShell commands.

This section covers the following topics:

- DirectAccess infrastructure options
- Configuring DirectAccess clients
- Configuring DirectAccess servers
- Configuring DirectAccess infrastructure servers

What is DirectAccess?
DirectAccess is an always-on remote access technology based on IPv6 communication. Through DirectAccess, a user's computer automatically, transparently, and securely connects to a private corporate network from any location in the world as soon as the computer is connected to the Internet. When a DirectAccess connection is active, remote users connect to resources on the corporate network as if they were on the local premises.
DirectAccess overcomes the limitations of VPNs by providing the following benefits:

 Always-on connectivity Unlike with a VPN, a DirectAccess connection is always on, even before the user logs on to his or her computer.

 Seamless connectivity To the user, the DirectAccess connection to the corporate network is completely transparent. Aside from any delay that could be caused by a slow Internet connection, the user experience is the same as if the user's computer were connected directly to the corporate network.

 Bidirectional access With DirectAccess, the user's remote computer has access to the corporate intranet and the intranet can see the user's computer. This means that the remote computer can be managed by using Group Policy and other management tools (such as System Center Configuration Manger [SCCM]) in the same way that computers located on the internal network are managed.

In addition, DirectAccess includes the following security features:

 DirectAccess uses IPsec to authenticate both the computer and user. If you want, you can require a smart card for user authentication.

 DirectAccess also uses IPsec to provide encryption for communications across the Internet.

IPv6 and DirectAccess

A DirectAccess connection from a remote client to an internal resource includes two legs. In the first half of the connection, the DirectAccess client always uses IPv6 to initiate contact with the DirectAccess server, typically found at the edge of the private network. IPv6 transition technologies are used to assist this connection when necessary. The second half of the connection occurs between the DirectAccess server and the internal network resource. This part of the connection can proceed either over IPv4 (only if the DirectAccess server is running Windows Server 2012 and acting as a NAT64/DNS64 device) or over IPv6.
Figure 6-1 shows the two legs of a DirectAccess connection between a remote client and an internal network resource.

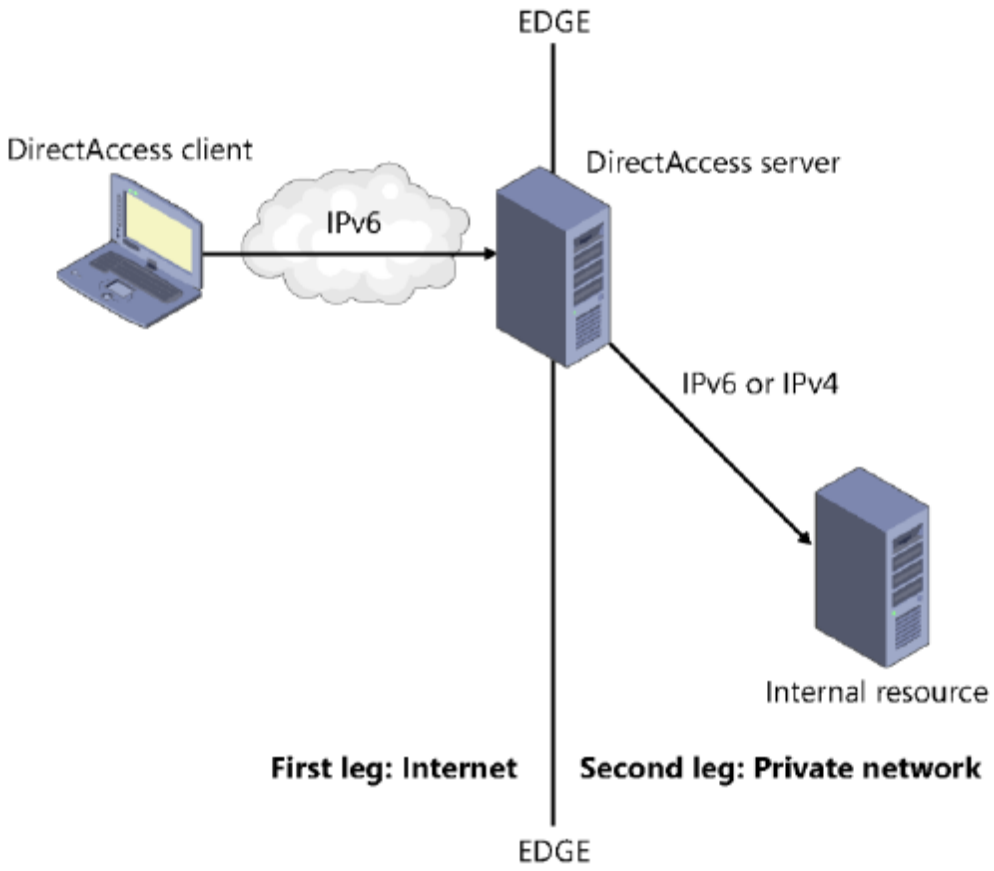

FIGURE 6-1 A DirectAccess connection to an internal resource.

First leg: External client to private network edge
If the DirectAccess client can obtain a global IPv6 address from its environment, then the connection to the DirectAccess server proceeds over the IPv6 Internet in a straightforward manner. However, IPv6 is not widely implemented yet on public networks, so three IPv6 transition technologies are used to assist in establishing the IPv6 connection to the DirectAccess server. If all three of the following transition technologies are enabled on the client through Group Policy, they are attempted in the following order of preference:

1. **6to4** For DirectAccess clients that have a *public* IPv4 address, 6to4 can be used to connect to the DirectAccess server via IPv6 across the public IPv4 Internet. 6to4 achieves this by tunneling or encapsulating IPv6 data within an IPv4 header, in a technique known as IPv6-over-IPv4. 6to4 requires any intervening router or firewall to be configured so that outbound traffic for Protocol 41 is allowed. Note that 6to4 does not work if the client is behind a network address translation (NAT) device.

2. **Teredo** For DirectAccess clients behind a NAT device and configured with a *private* IPv4 address, Teredo can be used to connect to the DirectAccess server via IPv6 across the public IPv4 Internet. Like 6to4, Teredo tunnels IPv6 traffic in IPv4. The intervening routers and firewalls must be configured to allow outbound traffic through User Datagram Protocol (UDP) port 3544.

3. **IP-HTTPS** For DirectAccess clients that cannot effectively establish IPv6 connectivity to the DirectAccess server through 6to4 or Teredo, IP-HTTPS is used. By using IP-HTTPS, DirectAccess clients encapsulate IPv6 traffic within HTTPS traffic. Virtually all routers allow outbound HTTPS traffic, so this option is almost always possible.

In Windows Server 2012 and Windows 8, the performance of IP-HTTPS is close to that of Teredo because a “null encryption” option is used for HTTPS communication. However, in Windows Server 2008 R2 and Windows 7, IP-HTTPS uses Secure Sockets Layer (SSL) encryption on top of the IPsec encryption that is used to secure the connection between the DirectAccess client and server. This “double encryption” significantly degrades network performance.

Second leg: Private network edge to internal resource
Between the network edge and the internal network resource, the connection can proceed over either IPv6 or IPv4. You don’t have to deploy global IPv6 on your internal network because Windows Server 2012 can act as a NAT64/DNS64 device when deployed as a DirectAccess server at the network edge. (A NAT64/DNS64 device translates between IPv6 and IPv4.) However, an all-IPv6 connection still provides the best performance and is the preferred scenario.

Windows Server 2008 R2 doesn’t provide NAT64/DNS64 functionality, but you could use Microsoft Forefront Unified Access Gateway 2010 or a third-party device to provide NAT64/DNS64 translation. Otherwise, to implement DirectAccess, you have to deploy global IPv6 on your internal network or use the IPv6 transition technology ISATAP. You can still use ISATAP in Windows Server 2012, but it is not recommended.
The DirectAccess connection process

A DirectAccess connection to a target intranet resource is initiated when the DirectAccess client connects to the DirectAccess server through IPv6. IPsec is then negotiated between the client and the server. Finally, the connection is established between the DirectAccess client and the target resource.

This general process can be broken down into the following specific steps:

1. The DirectAccess client computer attempts to connect to an internal computer configured as the *network location server*. If the network location server is available, the DirectAccess client determines that it is already connected to the intranet, and the DirectAccess connection process stops. If the network location server is not available, the DirectAccess client determines that it is connected to the Internet, and the DirectAccess connection process continues.

NETWORK LOCATION SERVER

A network location server is an intranet web server that a DirectAccess client attempts to access to determine whether the client is located on the intranet or Internet. An internal address of the DirectAccess server can be configured as the network location server, but using a separate, high-availability internal web server for the network location server is preferred. If you configure a separate web server as a network location server, the web server does not have to be dedicated to this one service.

2. The DirectAccess client computer connects to the DirectAccess server by using IPv6 and IPsec. If a native IPv6 network isn't available, the client establishes an IPv6-over-IPv4 tunnel by using 6to4, Teredo, or IP-HTTPS. The user does not have to be logged in for this step to complete.

3. As part of establishing the IPsec session, the DirectAccess client and server authenticate each other by using Kerberos or computer certificates.

4. By validating Active Directory Domain Services group memberships, the DirectAccess server verifies that the computer and user are authorized to connect using DirectAccess.

5. 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.

6. The DirectAccess server begins forwarding traffic from the DirectAccess client to the intranet resources to which the user has been granted access.

DirectAccess infrastructure options

You can deploy DirectAccess in a number of network scenarios, ranging from very simple to very complex. A few of these options are illustrated in the examples that follow.

Simple DirectAccess infrastructure

A simple DirectAccess infrastructure includes a DirectAccess server that is running Windows Server 2012 and is deployed at the network edge. This DirectAccess server is configured as a Kerberos proxy and NAT64/DNS64 translation device. The external interface is configured with a public IP address. (Two would be necessary to support Teredo.) The internal address is associated with the network location server.

Within the internal network is a domain controller/DNS server and at least one internal network resource, such as a file server or application server. Note that this simple infrastructure supports only Windows 8 clients because Windows 7 clients do not support Kerberos authentication for DirectAccess.

Figure 6-2 shows a simple DirectAccess infrastructure.

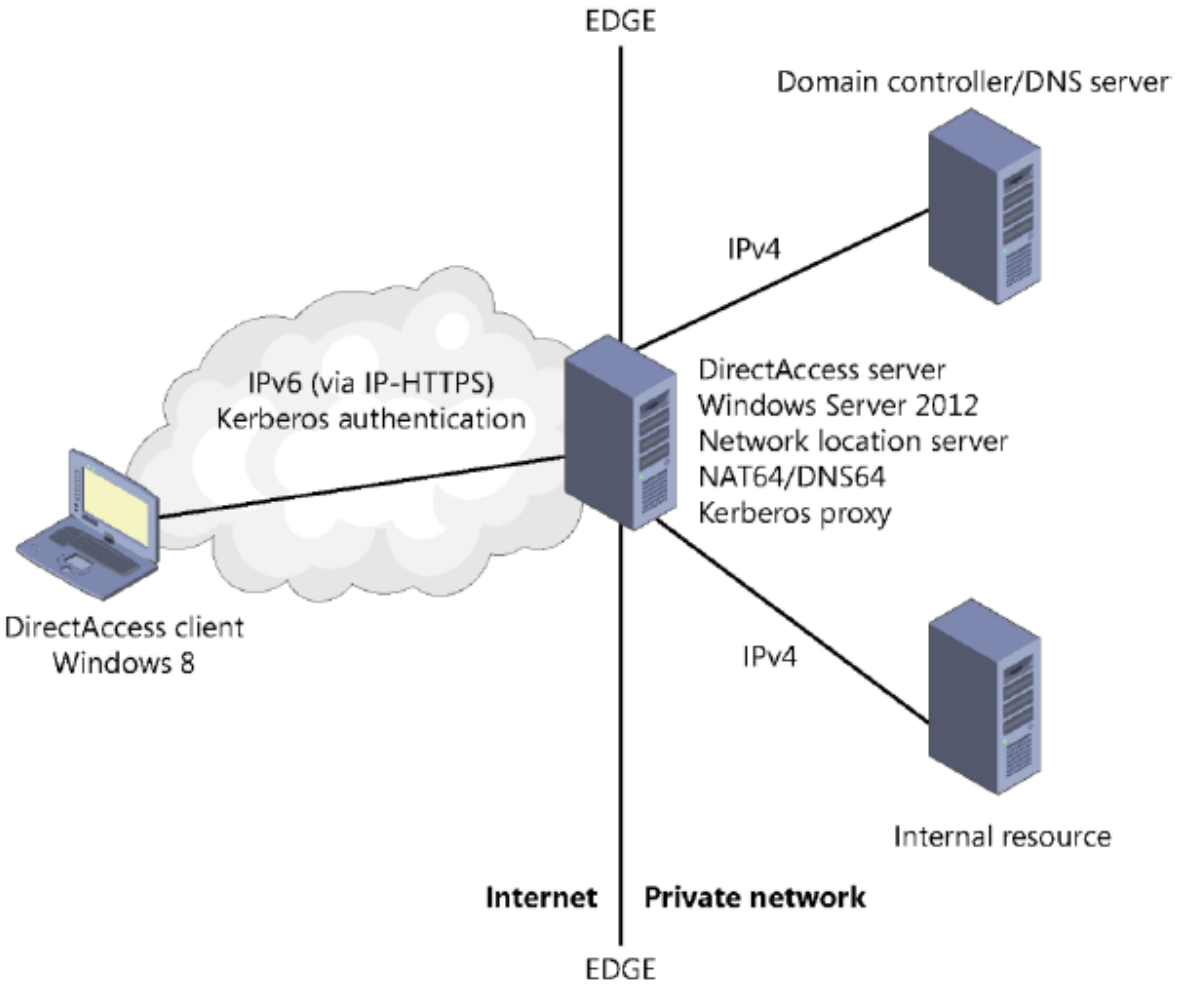

FIGURE 6-2 A simple DirectAccess infrastructure.

Remember that only Windows Server 2012 and Windows 8 support Kerberos proxy, which greatly simplifies authentication for DirectAccess clients. In addition, only Windows Server 2012 includes built-in support for NAT64/DNS64 translation, which enables you to use DirectAccess with your existing internal IPv4 infrastructure.

DirectAccess server behind NAT

Both Windows Server 2008 R2 and Windows Server 2012 enable you to deploy a DirectAccess server behind the network edge in a perimeter network. However, only in Windows Server 2012 can you deploy the DirectAccess server behind a NAT device. In such a scenario, the DirectAccess server needs only a single network adapter and a single address. Connections from the DirectAccess clients through the NAT device to the DirectAccess server are established by using IP-HTTPS.

Figure 6-3 illustrates a DirectAccess network topology in which a DirectAccess server is deployed behind a NAT device.

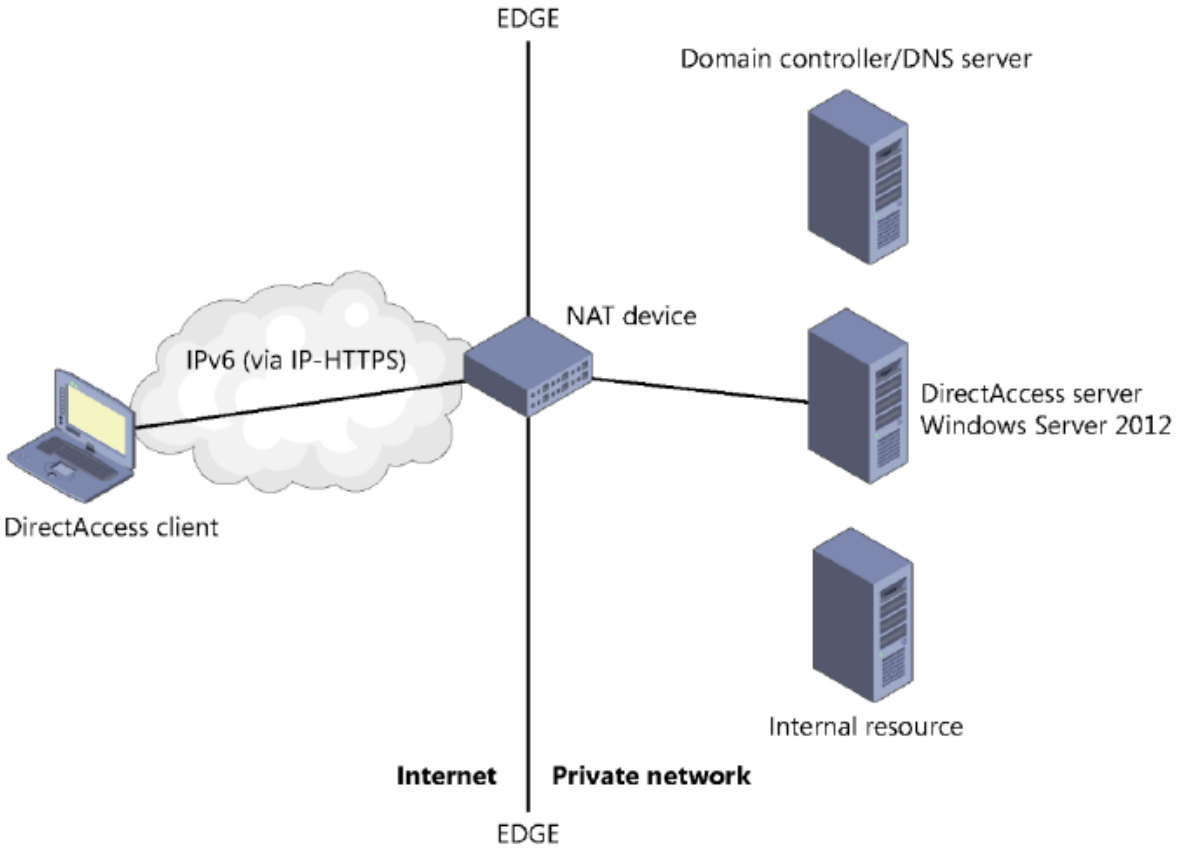

FIGURE 6-3 DirectAccess server deployed behind a NAT device.

EXAM TIP

Remember that only a Windows Server 2012 DirectAccess server can be deployed behind a NAT device.

Multisite/Multidomain DirectAccess infrastructure

Another infrastructure option new to Windows Server 2012 is the ability to deploy DirectAccess across multiple sites. A multisite deployment of DirectAccess requires a public key infrastructure (PKI) and computer authentication through certificates. In addition, in Windows Server 2012 *multidomain* support is a built-in feature of DirectAccess that requires no extra configuration. When you configure a multisite deployment, the DirectAccess clients are provided with a list of the DirectAccess servers that act as entry points to the private network at each site. Before connecting, DirectAccess clients running Windows 8 ping each of these DirectAccess servers. Windows 8 clients then initiate contact with the server whose latency is determined to be the shortest. (Windows 7 clients in a multisite deployment just use a single, preconfigured DirectAccess server address.)

Figure 6-4 shows a multisite DirectAccess infrastructure

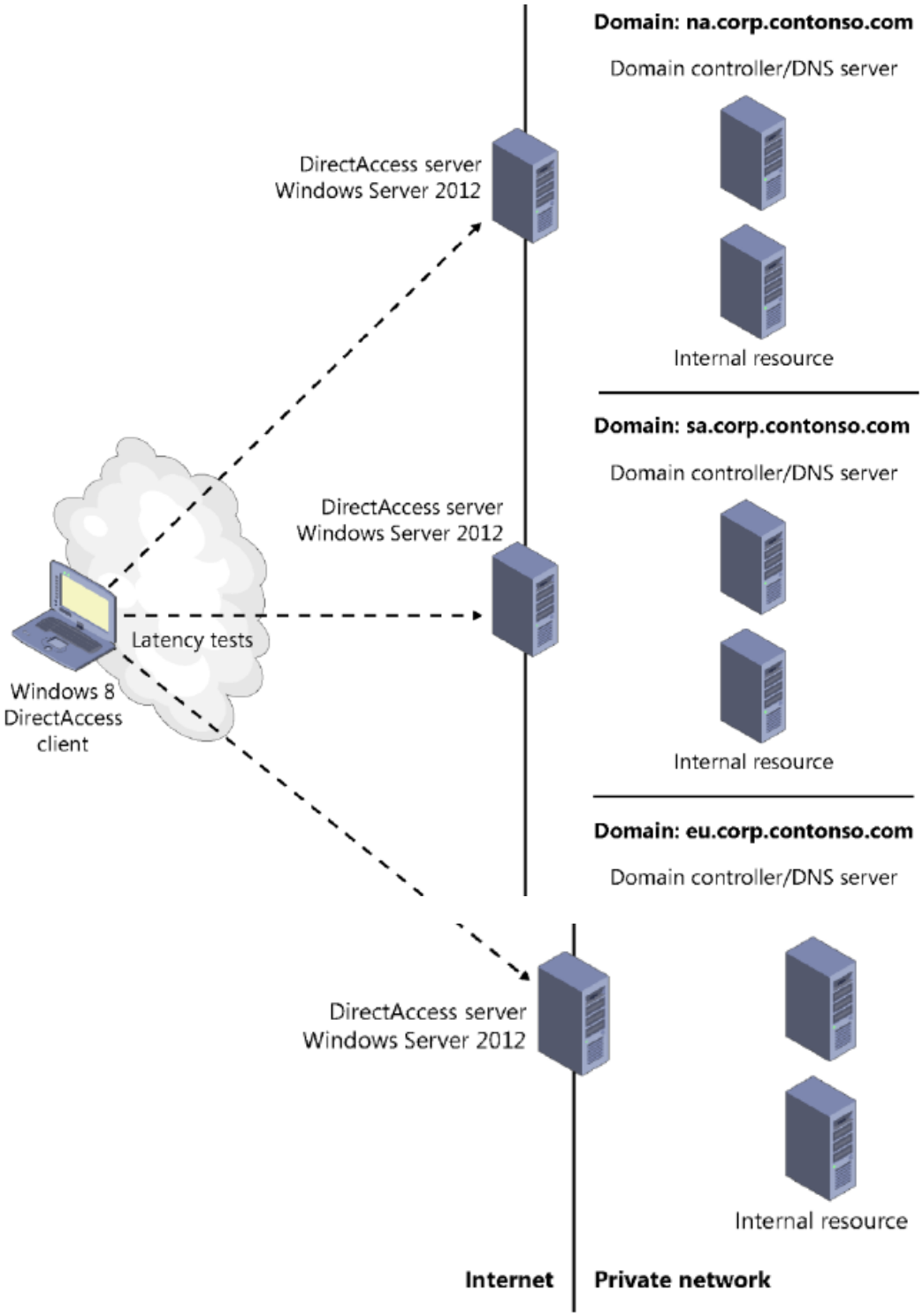
Domain: na.corp.contonso.com
Domain controller/DNS server
DirectAccess server
Windows Server 2012
Internal resource
Domain: sa.corp.contonso.com
Domain controller/DNS server
DirectAccess server
Windows Server 2012
Latency tests
Windows 8
DirectAccess
client
Internal resource
Domain: eu.corp.contonso.com
Domain controller/DNS server
DirectAccess server
Windows Server 2012
Internal resource
Internet
Private network

FIGURE 6-4 A multisite DirectAccess infrastructure.

ENABLE MULTISITE DIRECTACCESS To enable multisite capability in DirectAccess, in the Remote Access Management console, click Enable Multisite (as shown later in this chapter in Figure 6-20) or use the Windows PowerShell cmdlet Enable-DAMultiSite.

EXAM TIP

Remember that only Windows Server 2012 and Windows 8 support DirectAccess connectivity across multiple sites. Also remember that multisite deployments of DirectAccess require a PKI.

Installing and configuring DirectAccess

Windows Server 2012 has greatly simplified the process of installing and configuring DirectAccess. DirectAccess is now unified with traditional VPNs in a new Remote Access server role and managed with the same tool, the Remote Access Management console. You can now configure a Windows Server to act as both a DirectAccess server and a traditional VPN server at the same time, an option that was not possible in Windows Server 2008 R2. Even more significant than unified management are the new configuration wizards available in Windows Server 2012 that make the process of deploying and configuring DirectAccess and VPNs relatively easy.

Installing Remote Access

DirectAccess now belongs to the Remote Access server role. You can install the Remote Access role by using the Add Roles and Features Wizard or by typing the following at an elevated Windows PowerShell prompt:

```
Install-WindowsFeature RemoteAccess -IncludeManagementTools
```

You can then configure DirectAccess by using the Remote Access Management console, shown in Figure 6-6, or by using Windows PowerShell commands.

WINDOWS POWERSHELL To review the cmdlets used to configure DirectAccess, visit *http://technet.microsoft.com/en-us/library/hh918399* or type the following at a Windows PowerShell prompt:

```
Get-Command -Module RemoteAccess *da*
```

Note also that installing the Remote Access role and its role management tools installs the Windows PowerShell module named DirectAccessClientComponents, which provides the additional client cmdlets listed at the following address: *http://technet.microsoft.com/en-us/library/hh848426*.

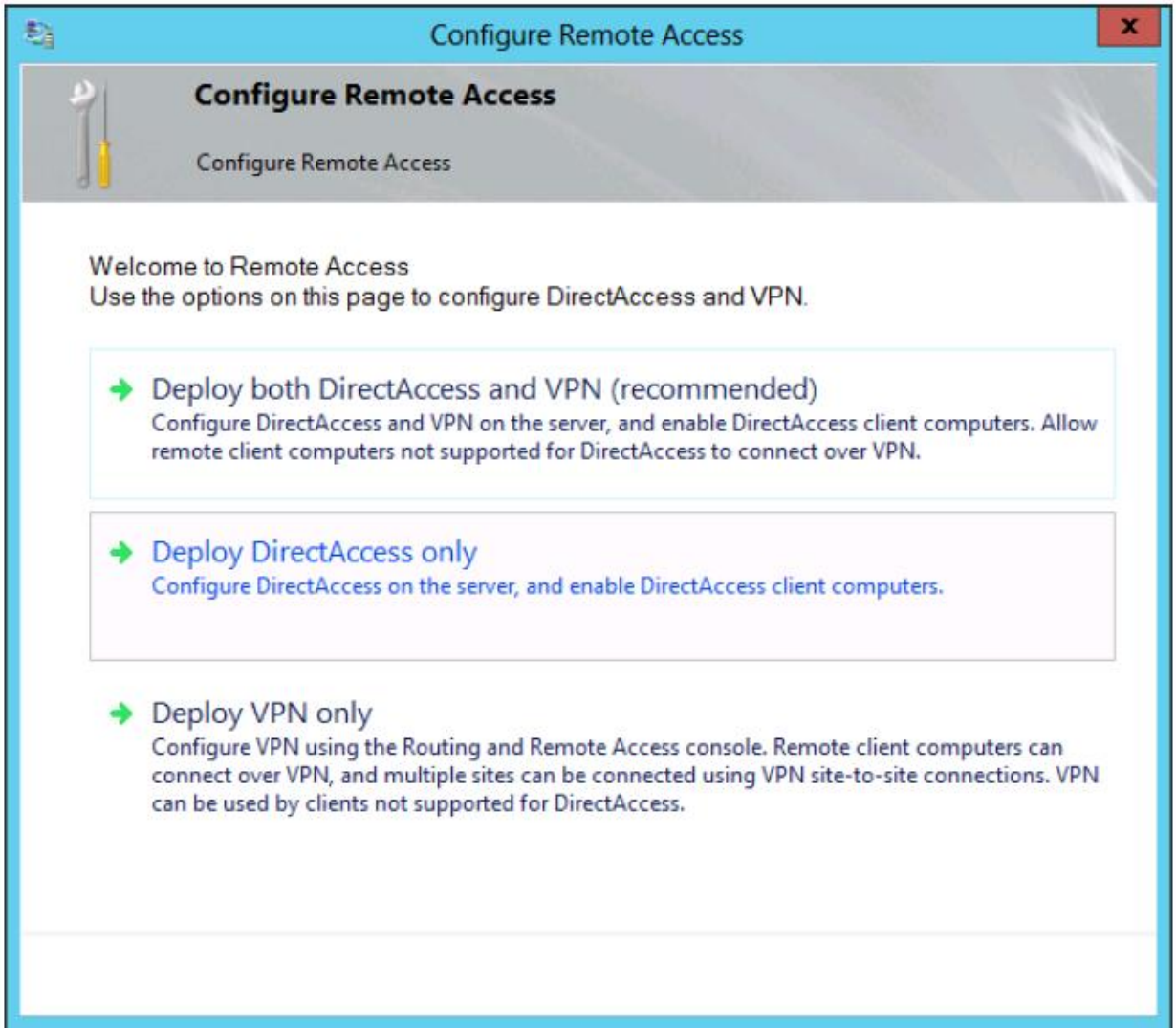

FIGURE 6-7 The Remote Access configuration wizards enable you to configure just DirectAccess, just a VPN, or both.

The Getting Started Wizard is an excellent new tool that helps you deploy a remote access solution quickly. However, it is not especially useful for exam preparation because it hides the configuration options you need to know and understand for the test. In addition, VPN configuration has not changed in Windows Server 2012 in any way that is significant for the 70-411 exam. For these reasons, to prepare for the Configure DirectAccess objective for the 70-411 exam, you should focus on configuration options that appear after you click Run The Remote Access Setup Wizard, as shown in Figure 6-6, and click Deploy DirectAccess Only, as shown in Figure 6-7.

After you click Deploy DirectAccess Only, the Remote Access Management console reappears with the center pane replaced by the image shown in Figure 6-8. The four steps in the map are associated with four configuration wizards you must complete in order. The first is for configuring DirectAccess clients, the second is for configuring the DirectAccess server, the third is for configuring infrastructure servers, and the fourth is for configuring the application

servers (if desired). These wizards create and configure group policy objects (GPOs) for DirectAccess servers and clients.

You won't be asked about any of these wizards (or any wizards) by name on the 70-411 exam. However, you may be asked about *any configuration option* that appears in any of these four wizards. These four wizards provide a useful way to organize the new configuration options you need to learn and understand for the 70-411 exam, so we will look at them in order.

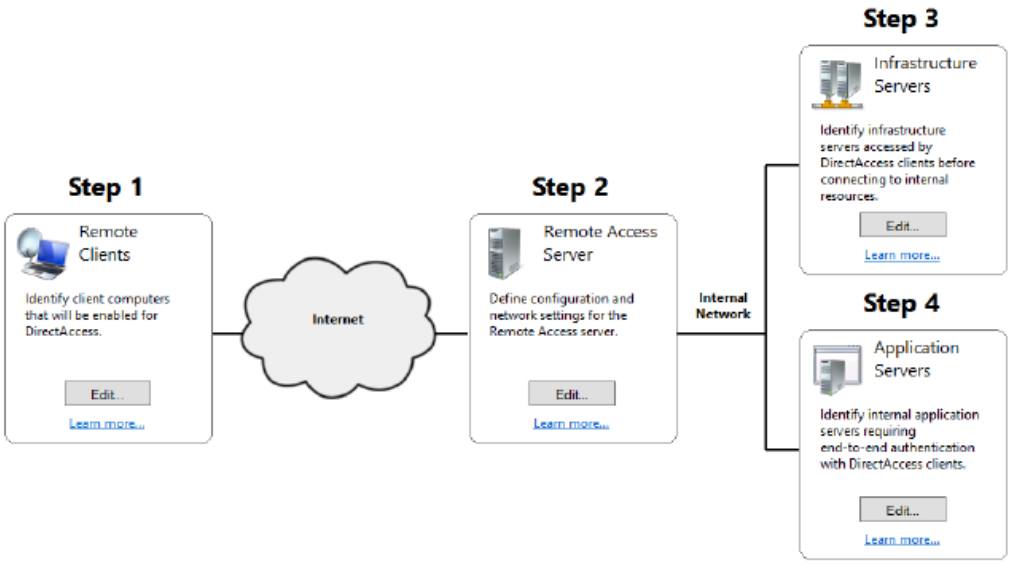

FIGURE 6-8 The four DirectAccess configuration wizards as they appear in the Remote Access Management console.

STEP 1: DIRECTACCESS CLIENT SETUP

The first page of the DirectAccess Client Setup wizard is shown in Figure 6-9. This Deployment Scenario page gives you the option to configure DirectAccess clients either for both remote access and remote management or for remote management only. The first, default option configures bidirectional communication for DirectAccess servers and clients. The second option allows administrators to manage remote DirectAccess clients by using tools such as SCCM, but prevents those clients from accessing the internal corporate network. Note that this second manage-only option is new to Windows Server 2012, so there is a good chance it will appear in some way on the 70-411 exam.

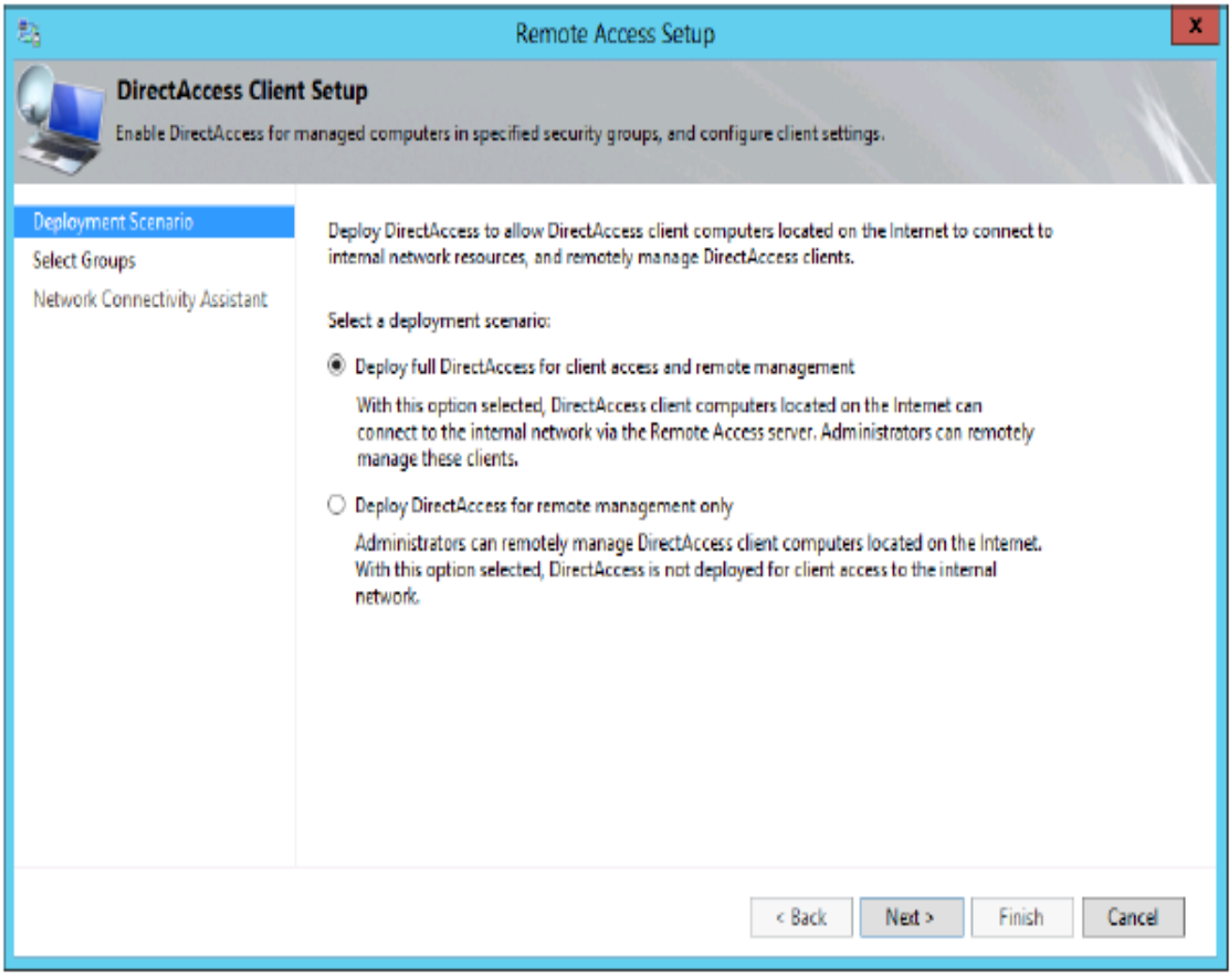

FIGURE 6-9 The Deployment Scenario page of the DirectAccess Client Setup wizard.

To configure the deployment scenario in Windows PowerShell, use the Set-DAServer cmdlet with the -DAInstall switch and either the FullInstall or ManageOut parameter. For example, to configure the DirectAccess deployment for remote management only, type the following at an elevated Windows PowerShell prompt on the DirectAccess server:

```
Set-DAServer -DAInstallType ManageOut
```

The second page of the DirectAccess Client Setup wizard is the Select Groups page, shown in Figure 6-10. The first option on this page enables you to specify the security groups that you want to enable for DirectAccess. This is an important step to remember: no DirectAccess client is allowed access to the internal network if you don't assign that client the right to do so. To perform this task in Windows PowerShell, use the Add-DAClient cmdlet with the -SecurityGroupNameList switch.

A second option on this page is to enable DirectAccess for mobile computers only. Interestingly, this option is selected by default if you run the Getting Started Wizard. Computers connecting remotely through DirectAccess are most likely mobile computers, but there are exceptions—and these exceptions could easily form the premise of an exam question. (Scenario: Some users working on domain-joined desktop computers from remote sites can't connect through DirectAccess. Why not? The option to enable DirectAccess for mobile computers only is selected.) In Windows PowerShell, this option is controlled by the use of the Set-DAClient cmdlet with the -OnlyRemoteComputers switch.

The third option on this page is Use Force Tunneling. This option forces the DirectAccess client to tunnel *all* network traffic through the private network, regardless of that traffic's ultimate destination. This behavior, for example, could be used to ensure that all web traffic from DirectAccess clients passes through an internal web proxy server. In Windows PowerShell, this option is configured by using the Set-DAClient cmdlet with the -ForceTunnel parameter.

EXAM TIP

Expect to see the Use Force Tunneling option in an exam question about DirectAccess.

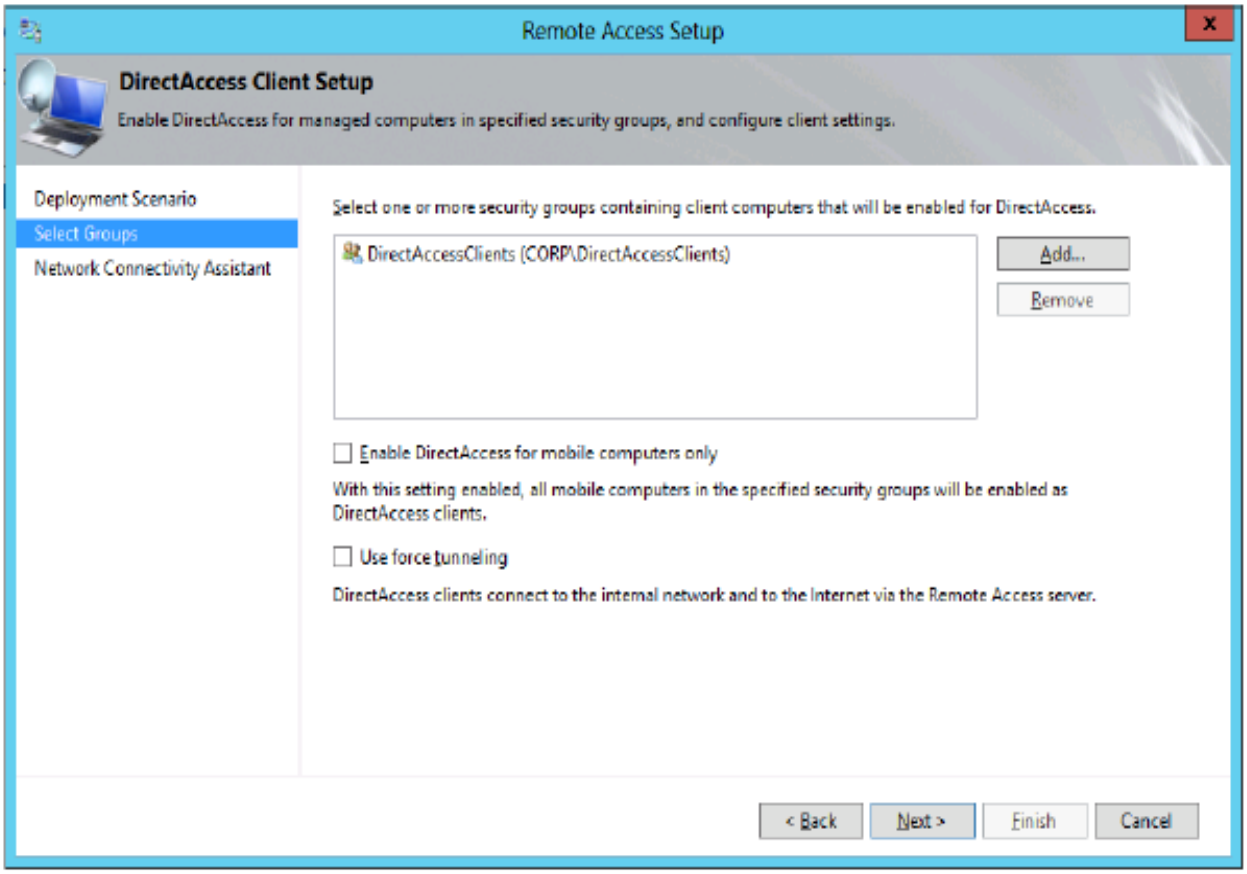

FIGURE 6-10 The Select Groups page of the DirectAccess Client Setup wizard.

The final page in the DirectAccess Client Setup wizard is the Network Connectivity Assistant page, shown in Figure 6-11.

The first setting on this page is the web probe host address. DirectAccess client computers use this web host to verify connectivity to the internal network. This setting is unlikely to appear on the 70-411 exam (except maybe as an incorrect answer choice), but if you need to enter this resource manually, you can use an address of **http://directaccess-webprobehost.yourdomain.** Your internal DNS should resolve this address to the internal IPv4 address of the Remote Access server or to the IPv6 address in an IPv6-only environment.

The most testable setting on this page is the option to allow DirectAccess clients to use local name resolution. Local name resolution in this case refers to the broadcast-based protocols of NetBIOS over TCP/IP and Link-Local Multicast Name Resolution (LLMNR). When this option is enabled, DirectAccess clients are allowed to resolve single label names such as App1 using local name resolution if they can't be resolved through DNS. Local name resolution must also be configured in the Infrastructure Server Setup wizard.

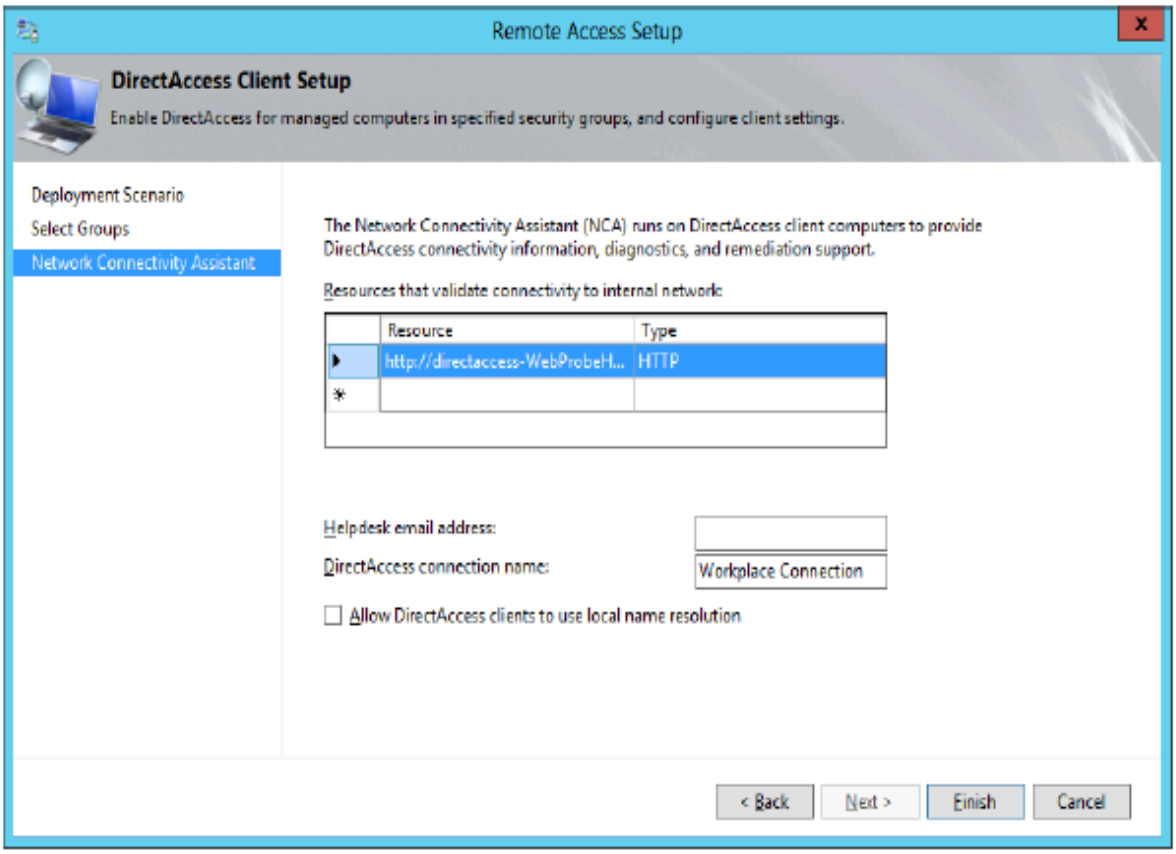

FIGURE 6-11 The Network Connectivity Assistant page of the DirectAccess Client Setup wizard.

STEP 2: REMOTE ACCESS SERVER SETUP

The first page of the Remote Access Server Setup wizard is the Network Topology page, shown in Figure 6-12. This page enables you to specify where in your network you are going to deploy your DirectAccess server.

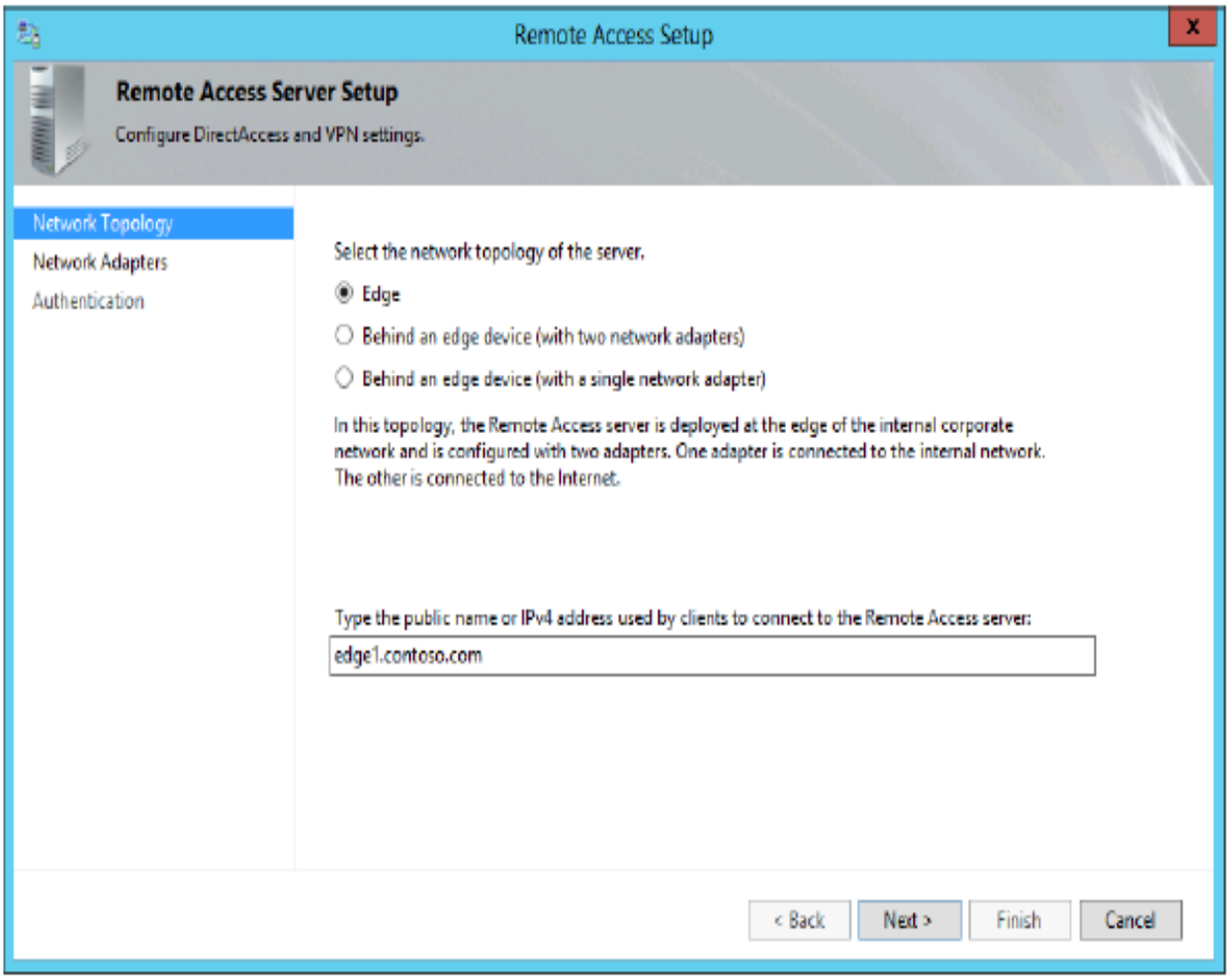

FIGURE 6-12 The Network Topology page of the Remote Access Server Setup wizard.

The first option is Edge. Choosing this option requires the DirectAccess server to be configured with two network adapters, one connected directly to the Internet and one

connected to the internal network. The external interface needs to be assigned two consecutive public IPv4 addresses if you need to support Teredo.

The second option is Behind An Edge Device (With Two Network Adapters). Select this option if you want to deploy the DirectAccess server in a perimeter network behind a firewall or router. In this topology, the network adapter attached to the perimeter network is assigned one or two consecutive public IPv4 addresses, and the second adapter attached to the internal network can be assigned a private address.
The third option is Behind An Edge Device (With A Single Network Adapter). Choose this option if you want to deploy the DirectAccess server behind a NAT device. In this topology, the DirectAccess server is assigned a single private IP address.

The Network Topology page also requires you to specify the name or IPv4 address the DirectAccess clients will use to connect to the DirectAccess server. Be sure to specify a name that can be resolved through public DNS or an IPv4 address that is reachable from the public network.

The second page of the Remote Access Server Setup wizard is the Network Adapters page, shown in Figure 6-13. This page requires you to choose the network adapter or adapters that will be assigned to internal network and external network, as required by your specified topology.

This page also requires you to specify a certificate that the DirectAccess server will use to authenticate IP-HTTPS connections. If your organization has deployed a PKI, you can browse to a copy of the computer certificate for the local server. If you don't have a PKI, you need to choose the option to use a self-signed certificate instead. Note that this latter option is new to Windows Server 2012 and could easily serve as the basis for a test question.

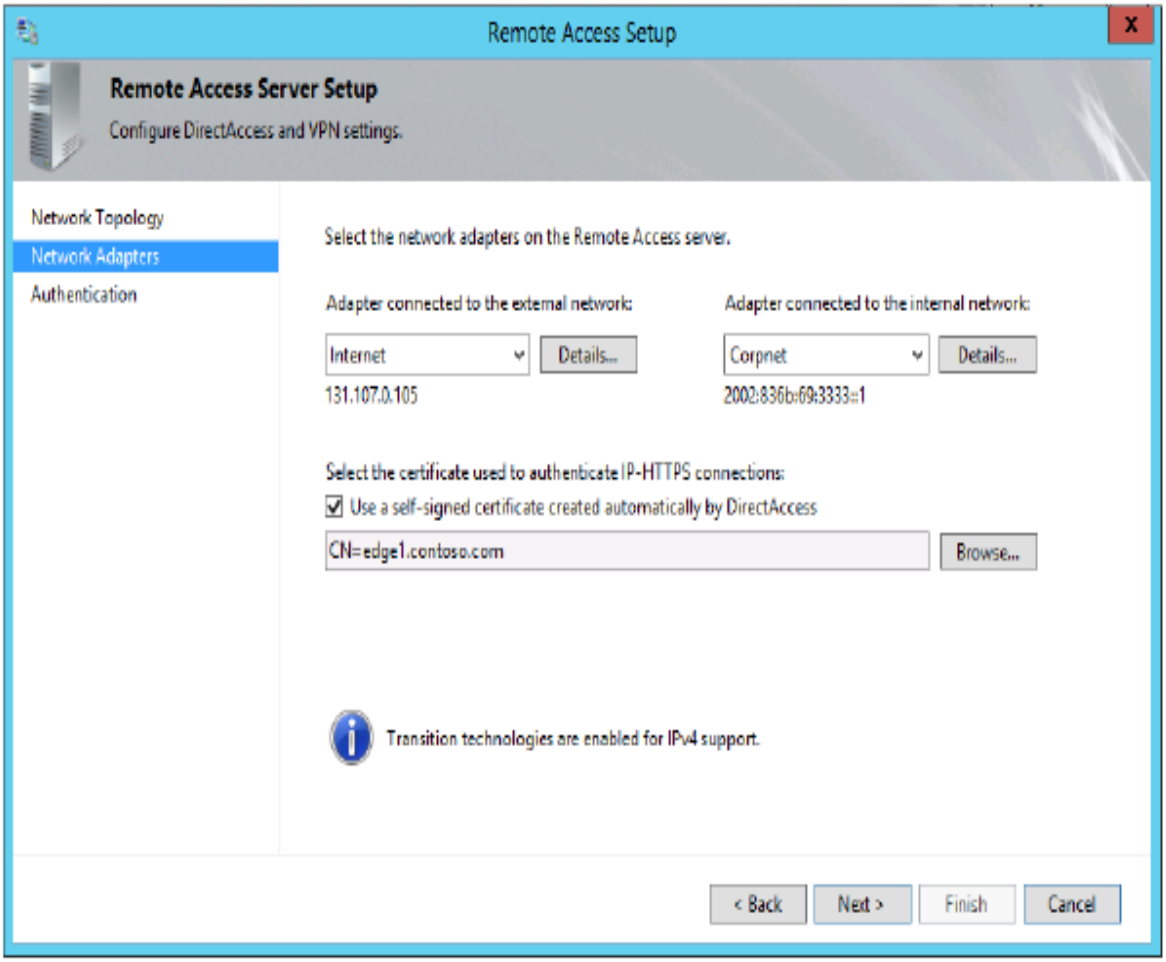

FIGURE 6-13 The Network Adapters page of the Remote Access Server Setup wizard.

The final page of the Remote Access Server Setup wizard is the Authentication page, shown in Figure 6-14. This page enables you to configure the following settings related to DirectAccess client authentication:

 User authentication By default, users authenticate only with Active Directory credentials. However, you can choose the option here to require two-factor authentication. Typically, two-factor authentication requires a user to insert a smart card in addition to typing his or her Active Directory credentials. Note that in Windows Server 2012, the Trusted Platform Module (TPM) of client computers can act as a virtual smart card for two-factor authentication.

As an alternative, you can configure two-factor authentication so that users must enter an OTP such as one provided through RSA SecurID in addition to their Active Directory credentials. OTP requires a PKI and RADIUS server along with a number of configuration steps you don't need to understand for the 70-411 exam. For the 70-411 exam, you just need to know that OTP is an alternative to smart cards for two-factor authentication in DirectAccess.

 Computer certificates If you configure DirectAccess in the GUI, client computers are authenticated through Kerberos by default. However, you can select an option to require computer authentication through the use of certificates. Computer certificate authentication is required to support two-factor authentication, a multisite deployment of DirectAccess, and Windows 7 DirectAccess clients.

 Windows 7 clients By default, Windows 7 client computers cannot connect to a Windows Server 2012 Remote Access deployment. You need to enable that functionality here.

 NAP This page enables you to require a health check of client computers through NAP. To configure this setting in Windows PowerShell, use the Set-DAServer cmdlet with the -HealthCheck parameter.

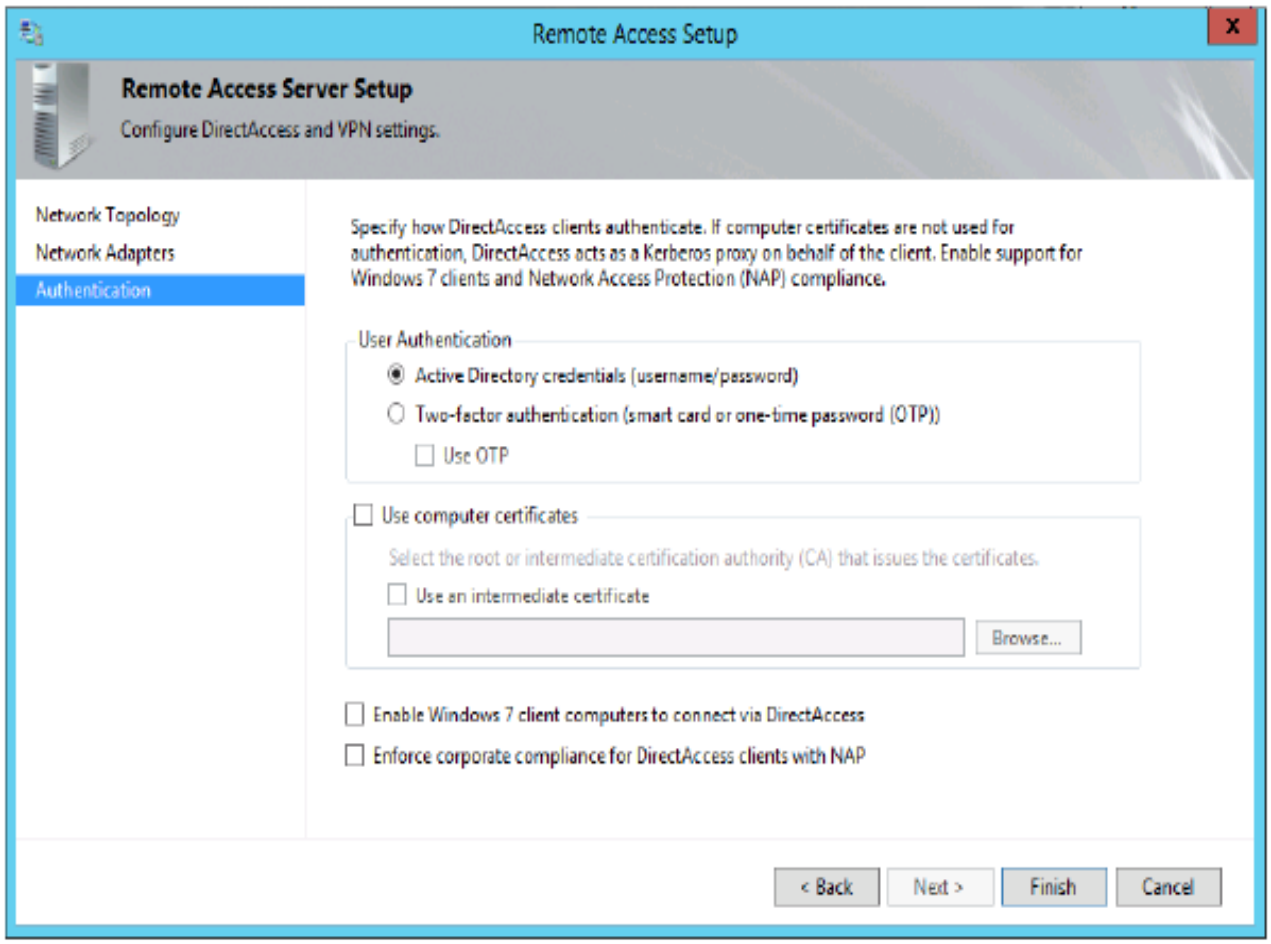

FIGURE 6-14 The Authentication page of the Remote Access Server Setup wizard.

STEP 3: INFRASTRUCTURE SERVER SETUP

The Infrastructure Server Setup wizard enables you to configure settings related to the network location server, the DNS server, and management servers such as update or antivirus servers.

The first page of this wizard is the Network Location Server page, shown in Figure 6-15. As explained earlier in this chapter, DirectAccess clients use this server to determine whether they are on the company network. It's recommended that you use an internal web server other than the DirectAccess (Remote Access) server for this purpose. (The DNS address and associated IP address in this case are naturally associated with the interface attached to the internal network.) If you do specify the DirectAccess server as the network location server, it must be authenticated by a computer certificate, a self-signed one if necessary. To configure the network location server using Windows PowerShell, use the Set-DANetworkLocationServer cmdlet.

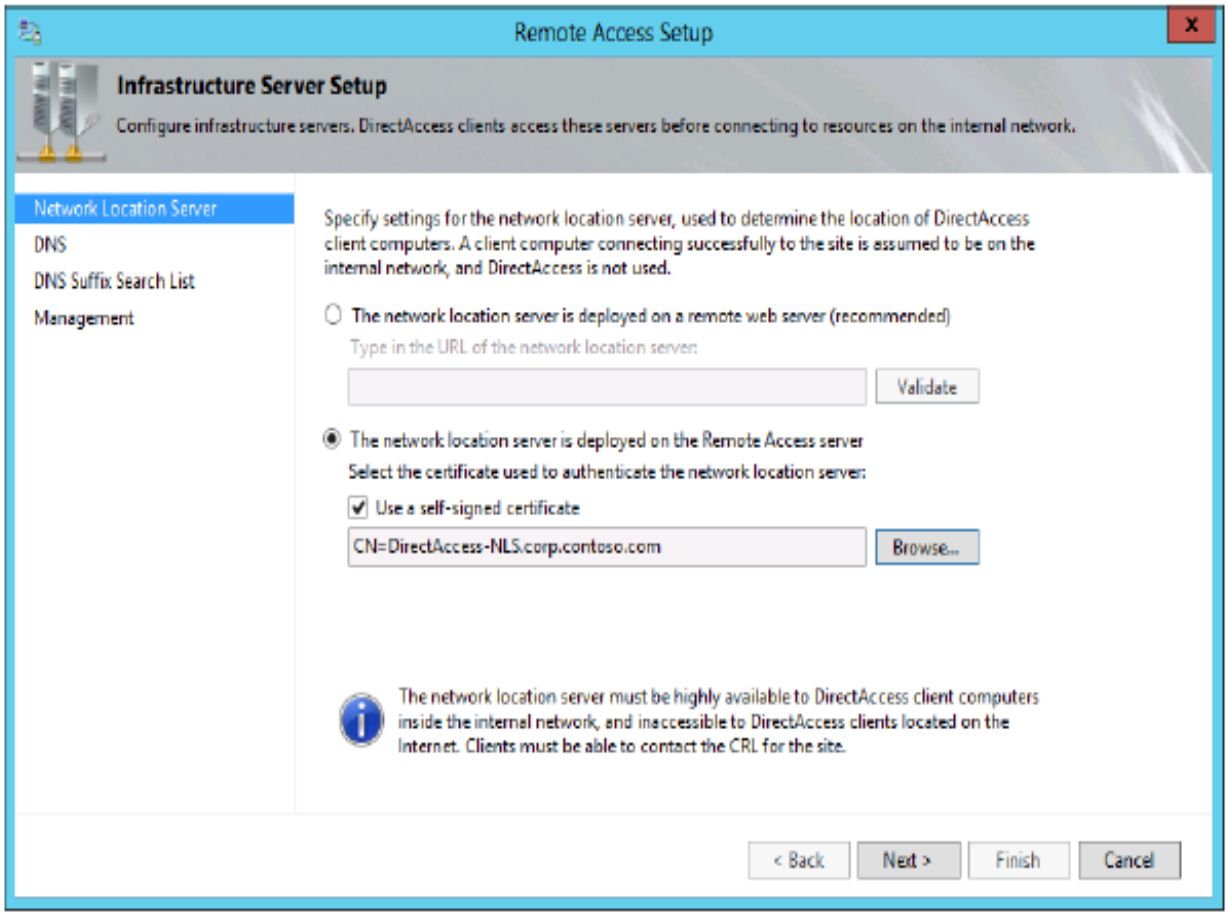

FIGURE 6-15 The Network Location Server page of the Infrastructure Server Setup wizard.

The second page of the Infrastructure Server Setup wizard is the DNS page, shown in Figure 6-16. The main function of this page is to enable you to configure the Name Resolution Policy Table (NRPT). The entries you create here are written to the GPO used to configure DirectAccess clients.

The NRPT is a feature that enables a DNS client to assign a DNS server address to particular namespaces rather than to particular interfaces. The NRPT essentially stores a list of name resolution rules that are applied to clients through Group Policy. Each rule defines a DNS namespace (a domain name or FQDN) and DNS client behavior for that namespace. When a DirectAccess client is on the Internet, each name query request is compared with the namespace rules stored in the NRPT. If a match is found, the request is processed according to the settings in the NRPT rule. The settings determine the DNS servers to which each request is sent. If a name query request does not match a namespace listed in the NRPT, it is sent to the DNS servers configured in the TCP/IP settings for the specified network interface.

You might need to configure NRPT entries if, for example, you need to enable DNS clients to resolve DNS suffixes found only within your intranet namespace. Another reason might be if you have a split public/private DNS environment based on the same domain name, and you need to direct remote DirectAccess clients to the proper DNS server to access resources.

EXAM TIP

You need to understand the function of the NRPT for the 70-417 exam. Also know that you can view the NRPT by using the Get-DnsClientNrptPolicy cmdlet in Windows PowerShell.

The second configuration decision you need to make on the DNS page relates to the DirectAccess clients' use of local name resolution methods such as NetBIOS and LLMNR. Unlike the setting in the DirectAccess Client Setup wizard, which just allows (does not block) the use of local name resolution, the setting here determines how local name resolution will be used if allowed. You have three options. The most restrictive is to use local name resolution only if the name does not exist in DNS. This option is considered the most secure because if the intranet DNS servers cannot be reached, or if there are other types of DNS errors, the intranet server names are not leaked to the subnet through local name resolution. The second and recommended option is to use local name resolution if the name doesn't exist in DNS or if DNS servers are unreachable when the client computer is on a private network. The third and least restrictive option is to use local name resolution for any kind of DNS resolution error. This option is considered the least secure because the names of intranet network servers can be leaked to the local subnet through local name resolution.

To configure local name resolution for clients in Windows PowerShell, use the Set-DAClientDNSConfiguration cmdlet with the -Local parameter. The three choices available in the GUI are designated by the FallbackSecure, FallbackPrivate, or FallbackUnsecure options, respectively.

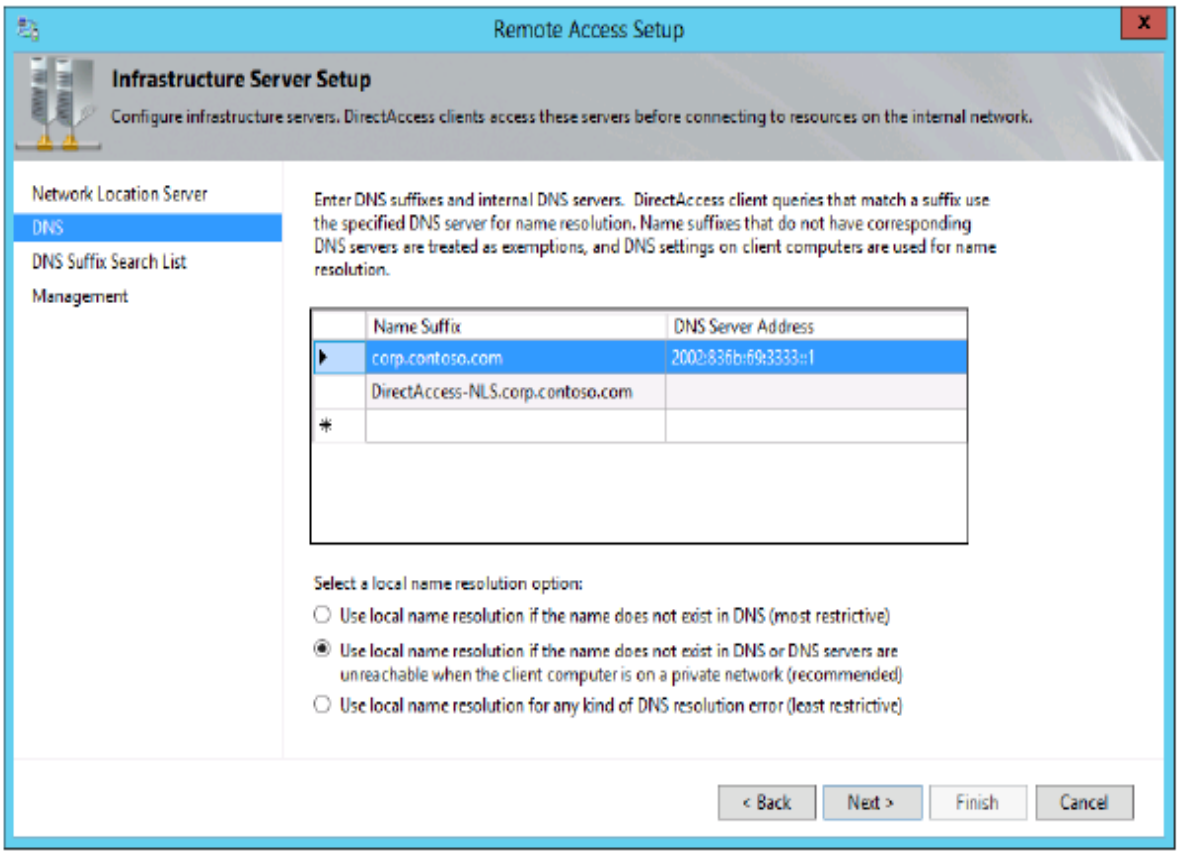

FIGURE 6-16 The DNS page of the Infrastructure Server Setup wizard.

The third page of the Infrastructure Server Setup wizard is the DNS Suffix Search List page, shown in Figure 6-17. DirectAccess clients use the list you configure here to resolve single label names, such as http://finance. DNS cannot resolve single label names unless the DNS client first appends a suffix. By default, clients append the primary DNS suffix of the client computer.

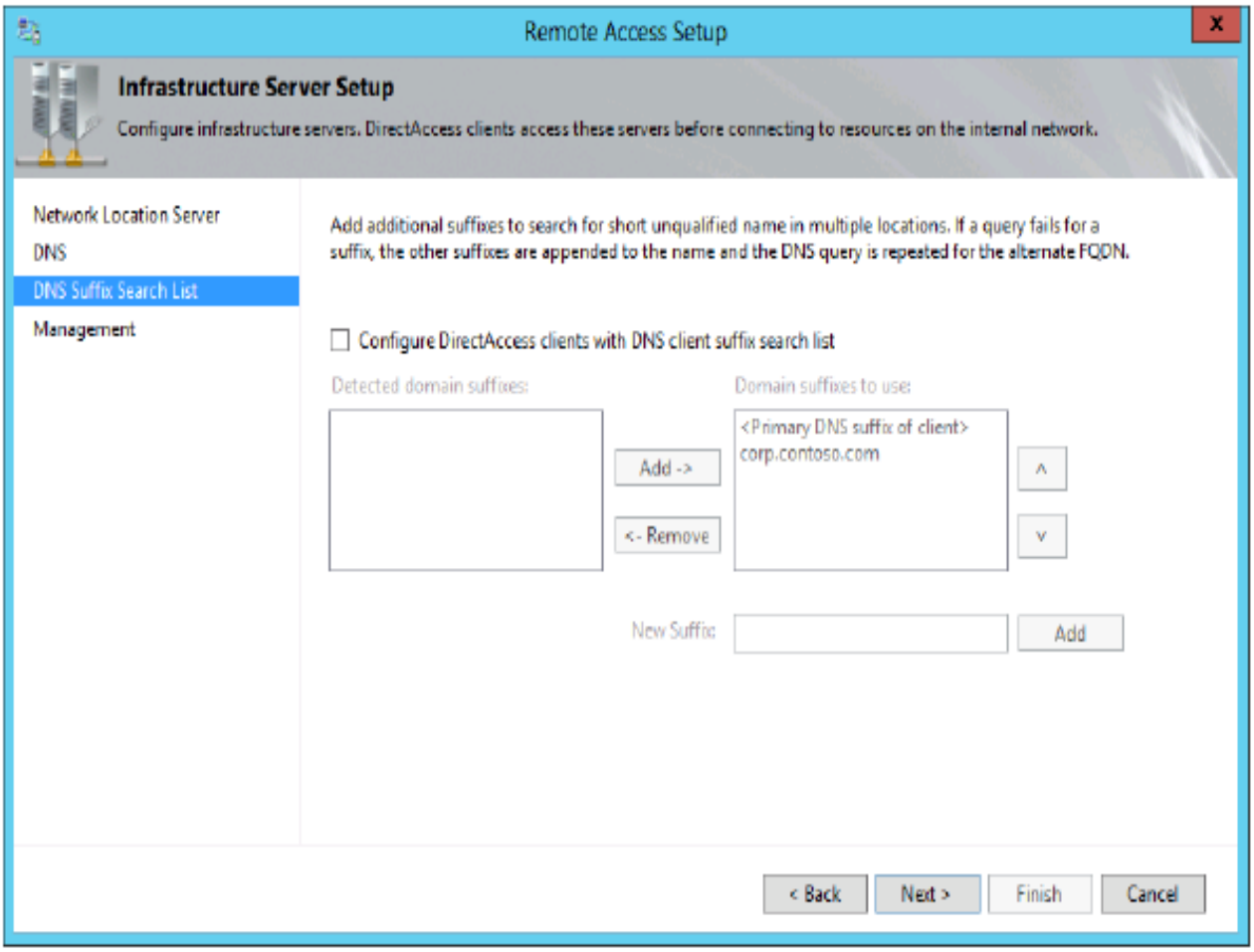

FIGURE 6-17 The DNS Suffix Search List page of the Infrastructure Server Setup wizard.

The fourth and final page of the Infrastructure Server Setup wizard is the Management page, shown in Figure 6-18. You don't need to enter any domain controllers or SCCM servers here because they are detected automatically the first time DirectAccess is configured. Instead, use this page to configure DNS clients with the names of management servers that cannot be detected automatically, such as Windows Server Update Services (WSUS) update servers and antivirus servers. Note that if the list of available domain controllers or SCCM servers is modified after you configure DirectAccess, you can just click Update Management Servers in the Remote Access Management console to refresh the management server list.

There is one other point to remember: management servers that initiate connections to DirectAccess clients must support IPv6 either natively or through ISATAP.

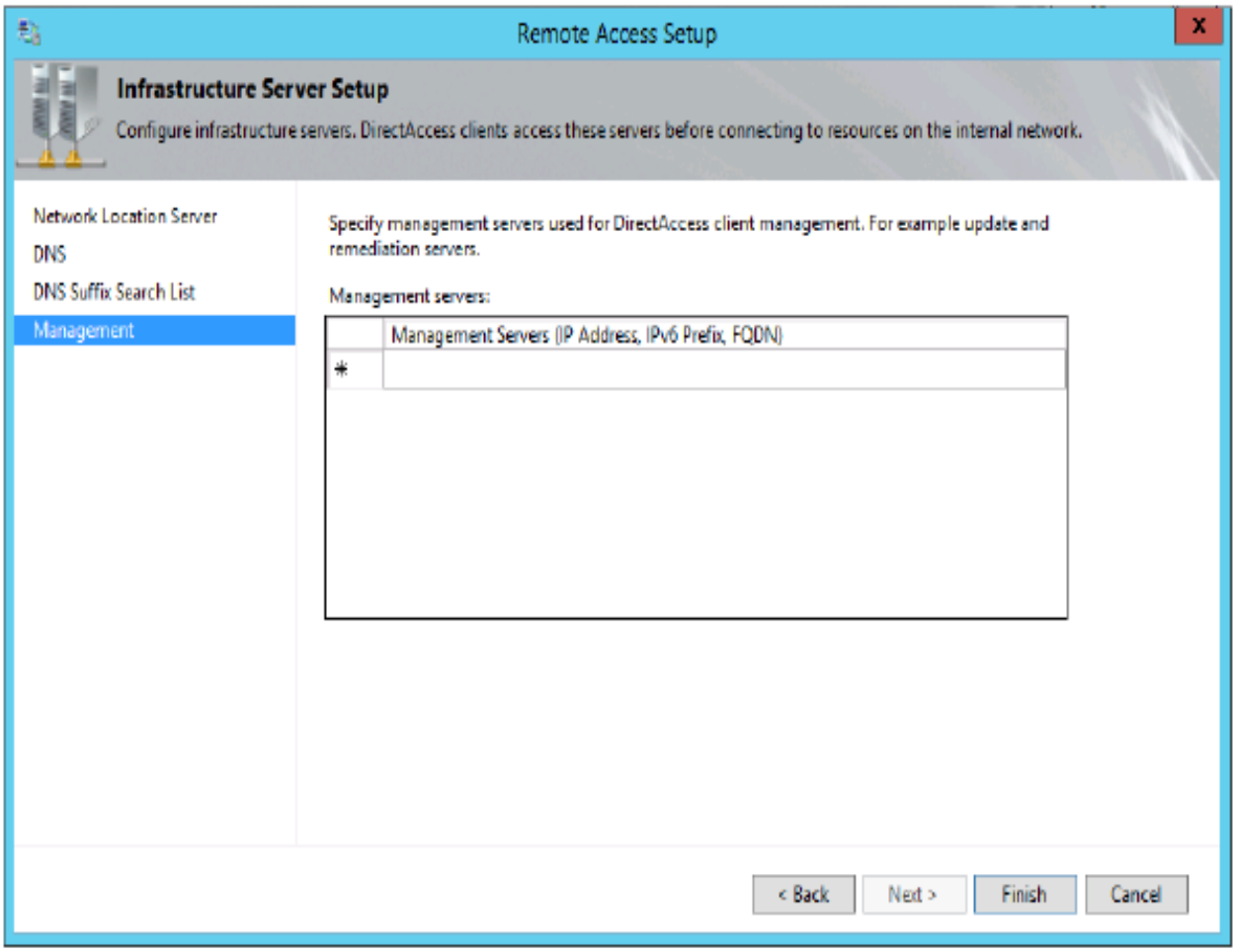

FIGURE 6-18 The Management page of the Infrastructure Server Setup wizard.

STEP 4: DIRECTACCESS APPLICATION SERVER SETUP

DirectAccess Application Server Setup is a single configuration page, shown in Figure 6-19. You can use this page to configure encryption between the application servers you specify here and the DirectAccess server. (By default, of course, traffic is already encrypted between the DirectAccess client and server.)

To configure the list of application servers using Windows PowerShell, use the Add-DAAppServer cmdlet.

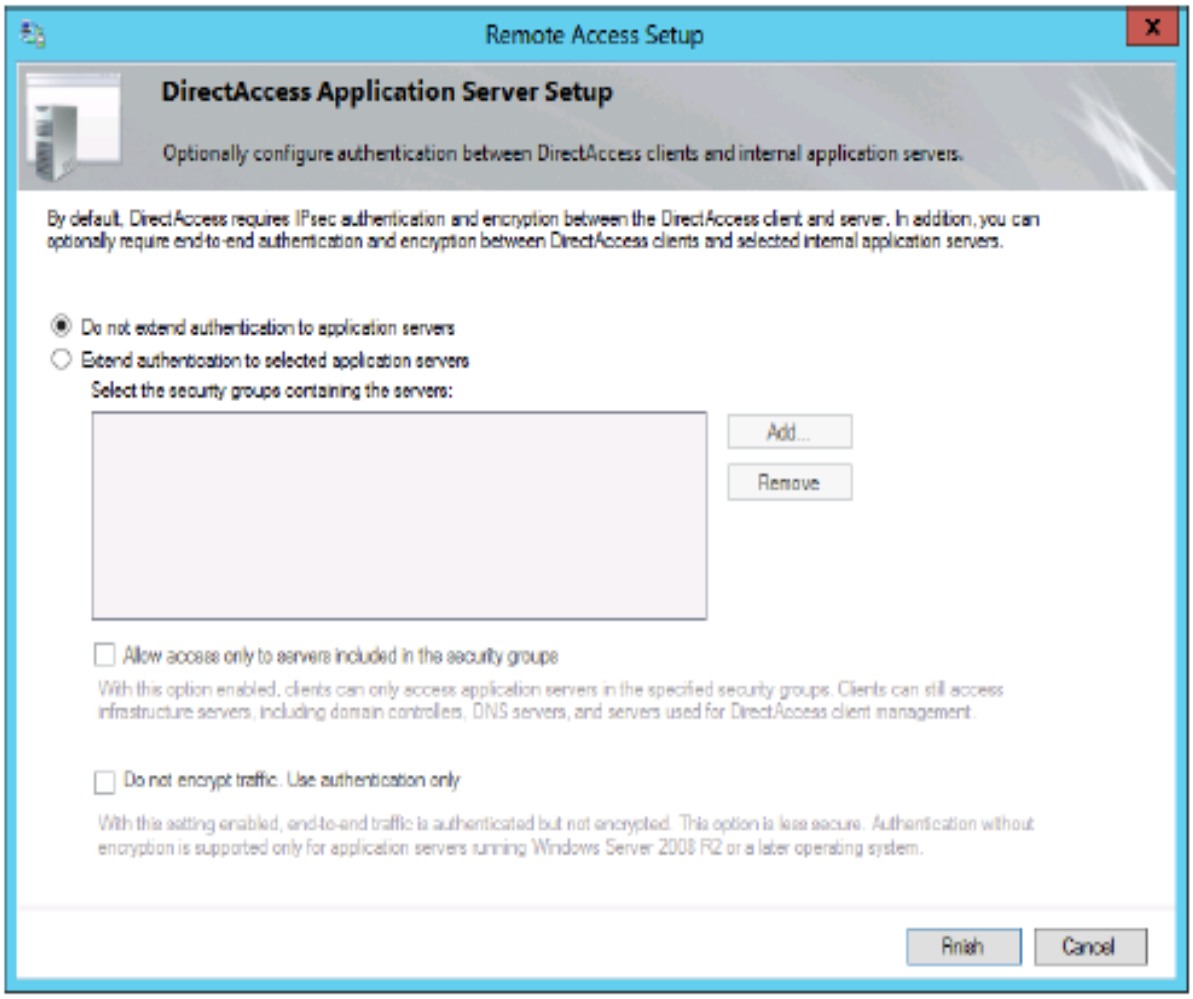

FIGURE 6-19 DirectAccess Application Server Setup.

STEP 5: ADVANCED CONFIGURATION OPTIONS

After you complete DirectAccess Application Server Setup, the Remote Access Management console appears as it does in Figure 6-20. At this point, you can start new wizards to configure advanced options such as a multisite deployment or load balancing by clicking the related options in the Tasks pane.

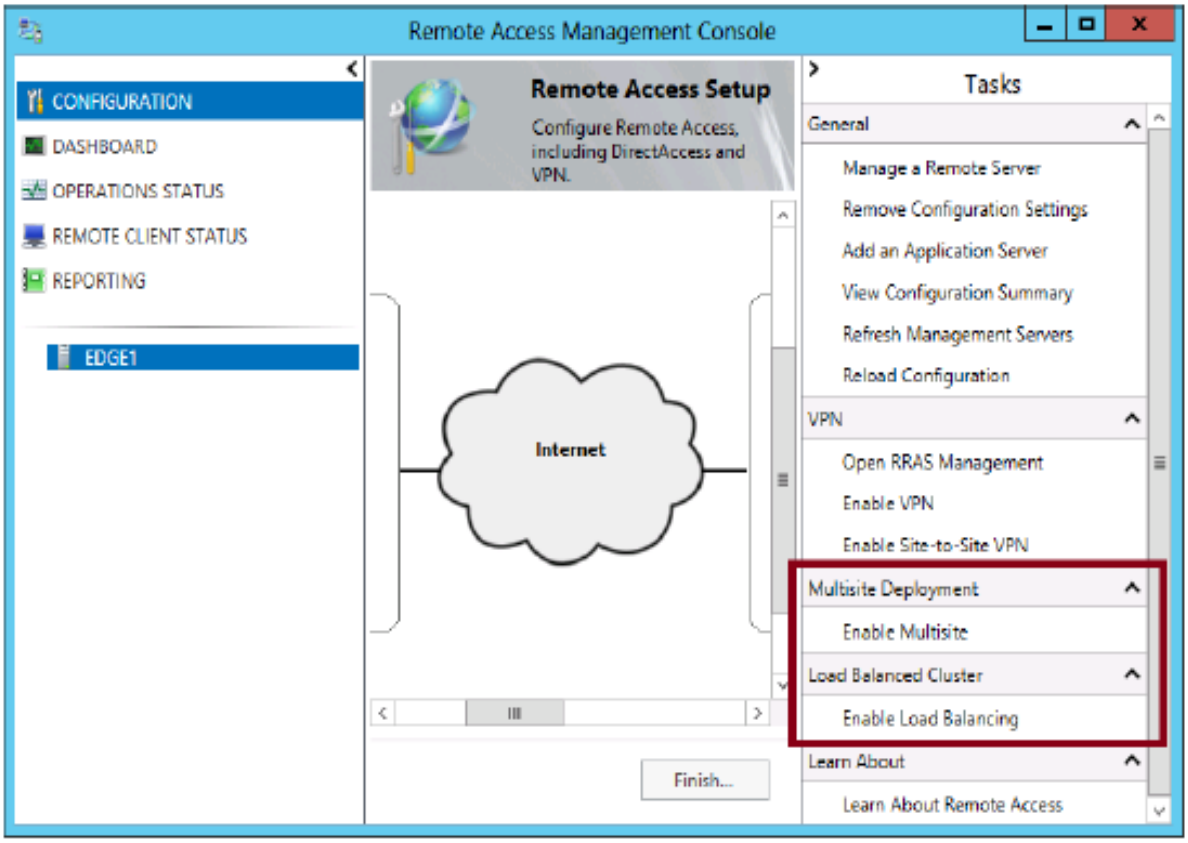

FIGURE 6-20 Configuring advanced DirectAccess options.

VERIFYING THE CONFIGURATION

After you have completed your configuration, you can use the Operations Status item in the left pane of the Remote Access Management console to verify that DirectAccess is ready to use. Remote clients can begin to connect to the network through DirectAccess after the operations status off all components is shown to be working, as shown in Figure 6-21. This process can take several minutes or longer after you complete the final configuration wizard.

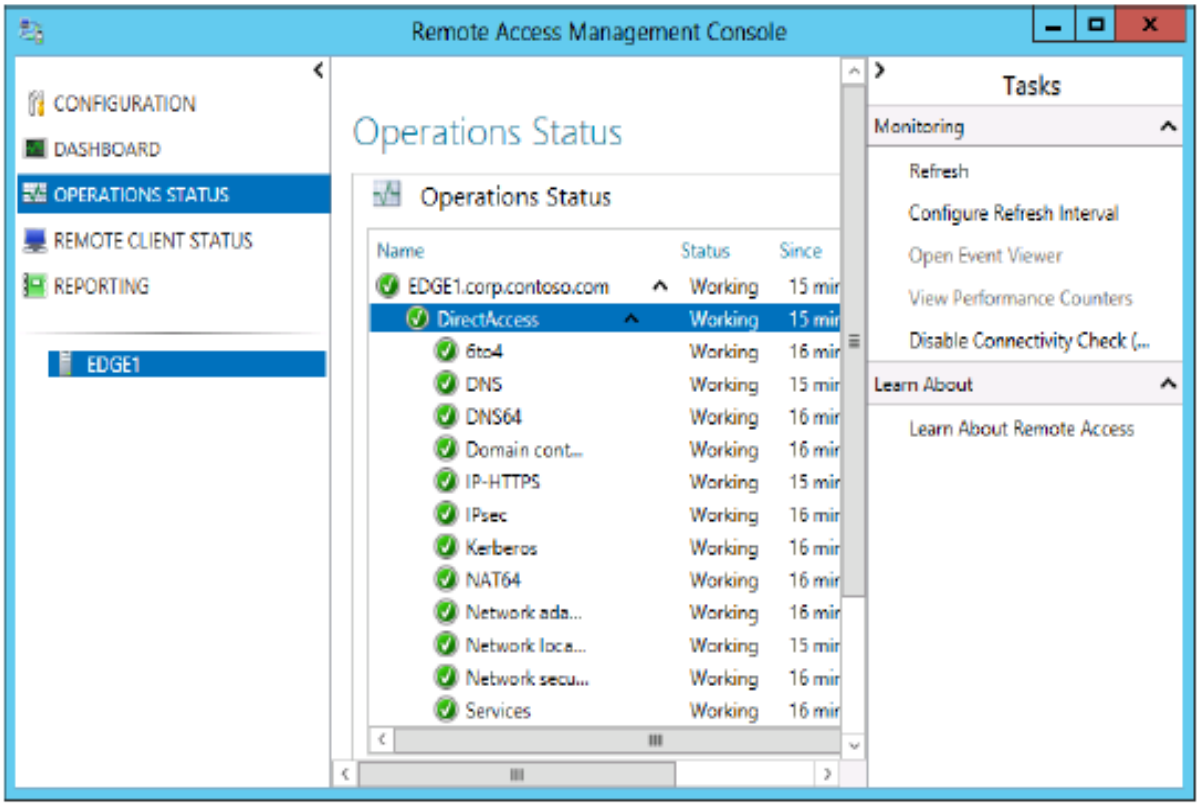

FIGURE 6-21 DirectAccess Operations Status.

After the server components are working, you can verify DirectAccess functionality from the client end. First, you can use the Get-DAConnectionStatus cmdlet to determine whether DirectAccess can properly determine the location of the client. Figure 6-22 shows a Windows PowerShell console session from a portable client that is initially plugged in to a corporate network. The first time the cmdlet is run, the client is shown to be connected locally. When the laptop is disconnected and an Internet broadband connection is enabled, the cmdlet is run again. This time, the client is determined to be connected remotely, and connectivity to the intranet is established through DirectAccess. Another way to verify DirectAccess functionality on the client end is to look at the connection status in the Networks bar. Figure 6-23 shows how a DirectAccess connection appears when it is available

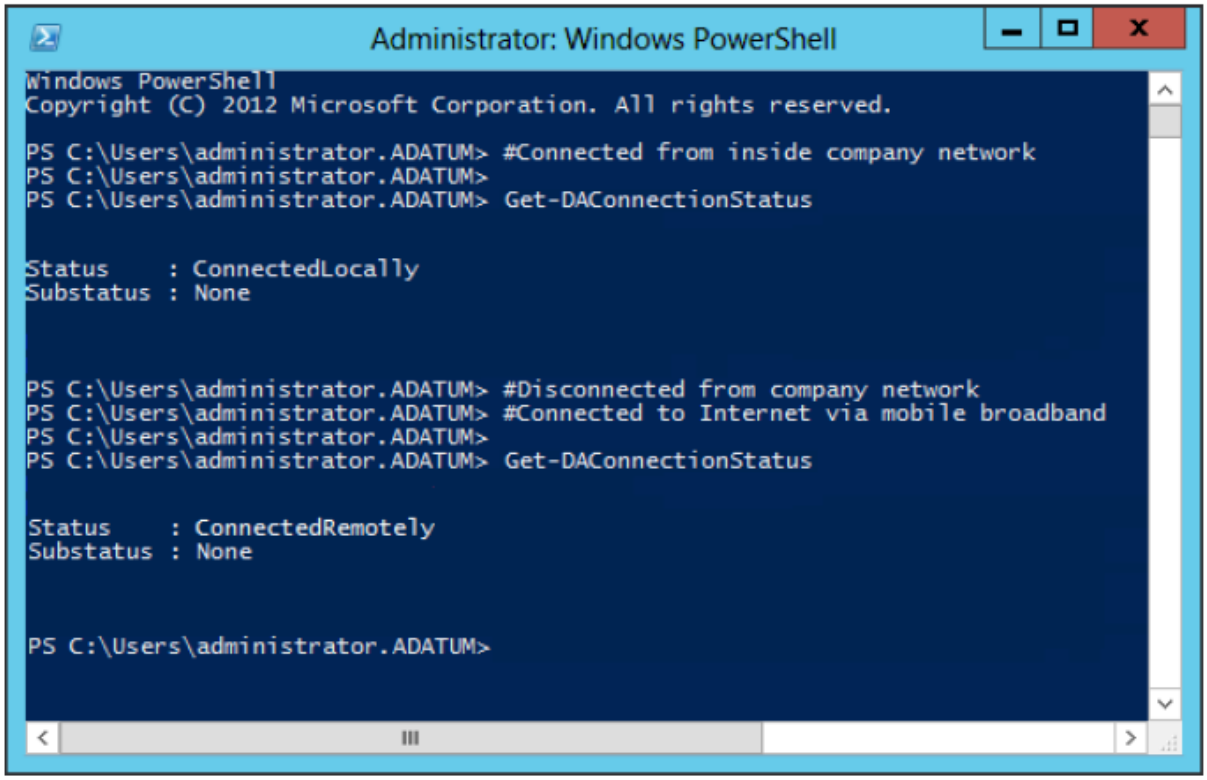

FIGURE 6-22 DirectAccess automatically determines when a client is connected locally or remotely.

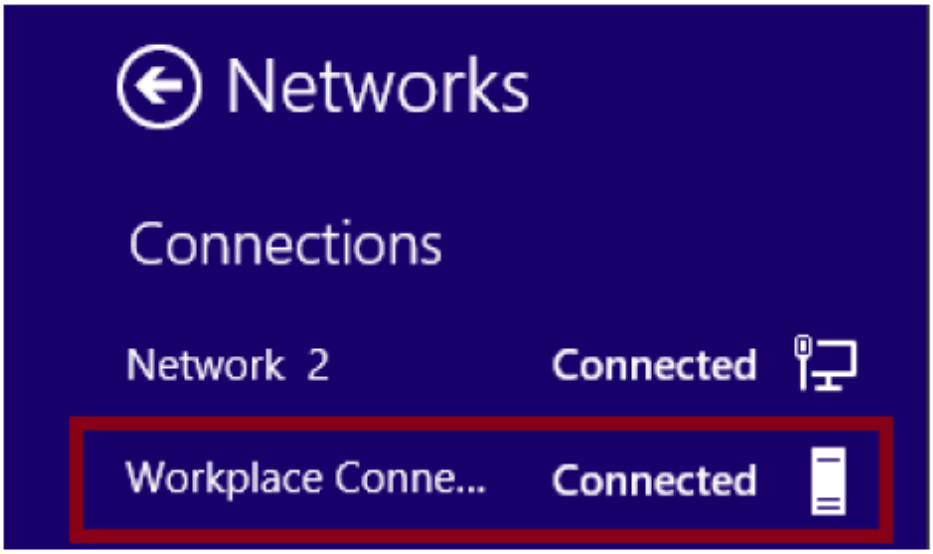

FIGURE 6-23 A DirectAccess connection as it appears in the Networks bar in Windows 8.