DIRECTACCESS CONNECTION

Direct Access is an automatic connectivity solution that allows clients running Windows 7 to connect seamlessly

to the corporate intranet the moment they establish a connection to the global Internet.

Direct Access enables remote users to access the corporate network anytime they have an Internet connection, without the extra step of initiating a virtual private networking (VPN) connection.

Direct Access is an always-on, IPv6, IPsec VPN connection

If the client running Windows 7 is unable to contact the specially configured intranet Web site, the client attempts to determine whether a native IPv6 network is present. If a native IPv6 network is present and the client has been assigned a public IPv6 address, DirectAccess makes a direct connection to the DirectAccess server across the Internet.

If a native IPv6 network is not present, Windows 7 attempts to establish an IPv6 over IPv4 tunnel using first the 6to4 and then Teredo transition technologies

If the client running Windows 7 cannot establish a Teredo or 6to4 connection due to an intervening firewall or proxy server, the client running Windows 7 attempts to Connect using Internet Protocol–Hypertext Protocol Secure (IP-HTTPS).

The DirectAccess IPsec session is established when the client running Windows 7 and the DirectAccess server authenticate with each other using computer certificates. DirectAccess supports only certificate-based authentication

TABLE 10-1 DirectAccess Connection Methods

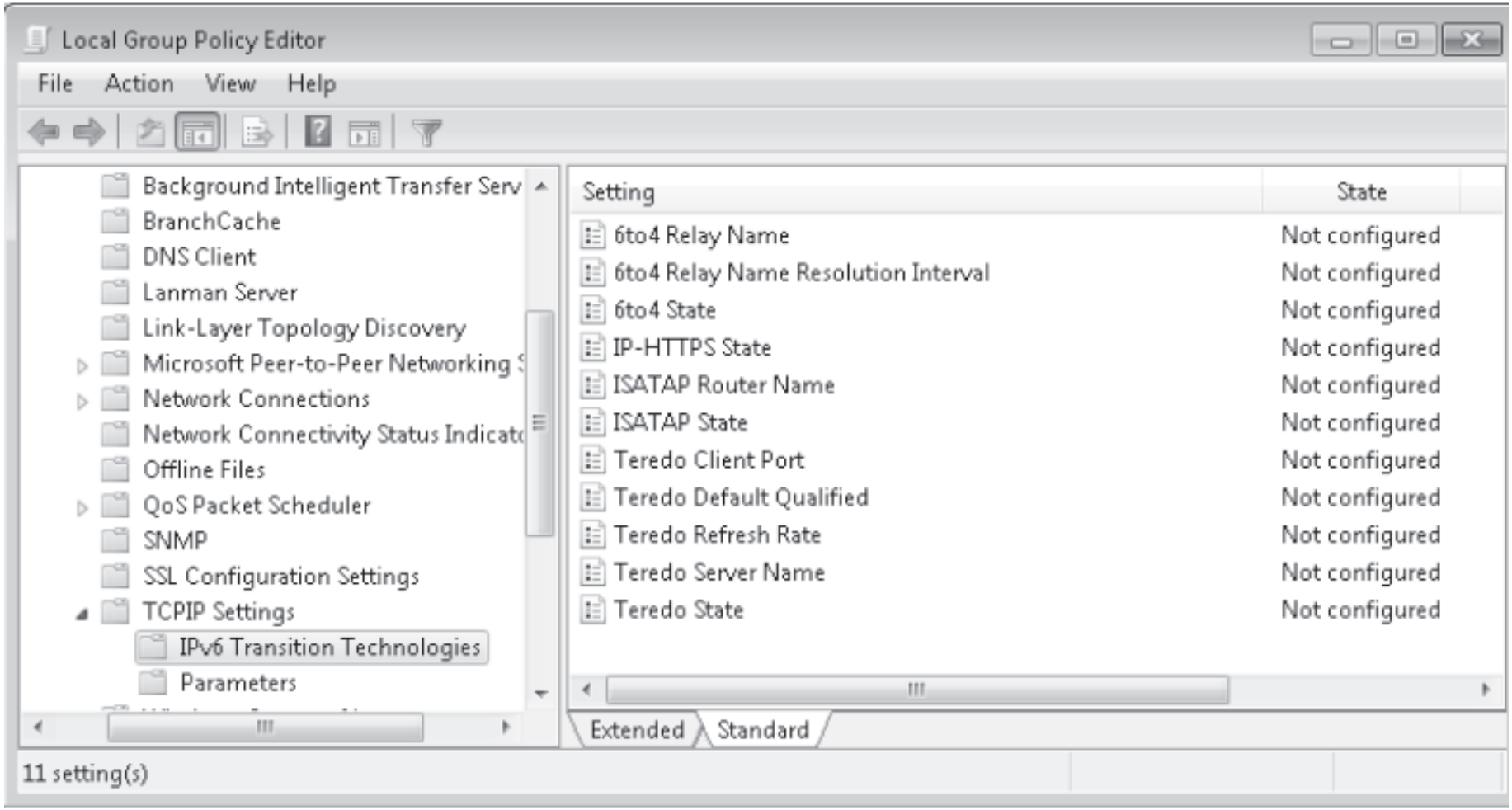
CLIENT NETWORK CONNECTION	DIRECTACCESS CONNECTION METHOD
Public IPv6 address	Public IPv6 address
Public IPv4 address	6to4
Private (NAT) IPv4 address	Teredo
Client unable to connect to network due to firewall, but is connected to the Internet	IP-HTTPS

DirectAccess Client Configuration

1. Only domain-joined clients running Windows 7 Enterprise and Ultimate editions Support DirectAccess.
2. When configuring a client for DirectAccess, you must add the client's domain computer account to a special security group. You specify this security group when running the DirectAccess wizard on the
   DirectAccess server.
3. Clients receive their DirectAccess configuration through Group Policy. This differs from traditional VPN configuration where connections are configured manually or distributed through the connection manager administration kit
4. Once you have added the computer's client account to the designated security group, you need to install a computer certificate on the client
   for the purpose of DirectAccess authentication. An organization needs to deploy Active Directory Certificate Services so that clients can automatically enroll with the appropriate certificates.

Group Policy for Direct Access

Computer Configuration\Administrative Templates\Network\TCPIP Settings\IPv6 Transition Technologies node (Server 2008R2/windows 7)



When you configure
DirectAccess on the DirectAccess server, it creates a GPO at the domain level and filters it for a specific security group. This GPO applies the following policies:

1. **6to4 Relay Name** This policy sets the 6to4 relay name and is configured to use one of the public IPv4 addresses applied to the DirectAccess server.
2. **IP-HTP S State** This policy sets the Uniform Resource Locator (URL) of the IP-HTTPS server, which will be the FQDN of one of the public IPv4 addresses applied to the DirectAccess server. The default policy state uses IP-HTTPS as a connection of last resort. It is possible to set this policy to always use IP-HTTPS even if other connectivity options, such as 6to4 or Teredo, are available.
3. **Teredo Default Qualified** This policy determines whether Teredo will be used. It is set to enabled for DirectAccess clients.
4. **Teredo Server Name** This policy sets the address of the Teredo server. This address will be one of the public IPv4 address assigned to the DirectAccess server.

Although it is possible to configure DirectAccess-related settings using the *Netsh* command- line utility, it is important to remember that Group Policy settings override Settings manually configured using Netsh. The commands that you can use to configure DirectAccess settings are as follows:

Netsh interface ipv6 set teredo enterpriseclient IPv4_address
Netsh interface 6to4 set relay IPv4_address
Netsh interface httpstunnel add interface client https://fqdn/IPHTTPS

The first command configures Teredo. The IPv4 address that you assign using this command should be one of the public IPv4 addresses of the DirectAccess server. The second command configures 6to4 and again uses one of the public IPv4 addresses of the DirectAccess server. The final command configures IP-HTTPS. You should use the FQDN that maps to one of the public IPv4 addresses, as well as the installed SSL certificate, on the DirectAccess server.

Troubleshooting DirectAccess

You can determine if a client has made a successful DirectAccess connection by clicking on the Network Connection icon. When the status message displays “Internet and Corporate Access,” as shown in Figure 10-3, the computer running Windows 7 has connected successfully DirectAccess. If the status message shows “Local and Internet Access,” there is no connection to the DirectAccess server.

DirectAccess clients and the DirectAccess server almost always receive their certificates from an Active Directory Certificate Services Certificate Authority that is integrated into the domain

You can verify the current DirectAccess configuration using several command-line utilities. To verify the DirectAccess client’s settings for 6to4, issue the command

Netsh interface 6to4 show relay

You can verify the Teredo configuration by issuing the command

Netsh interface ipv6 show teredo

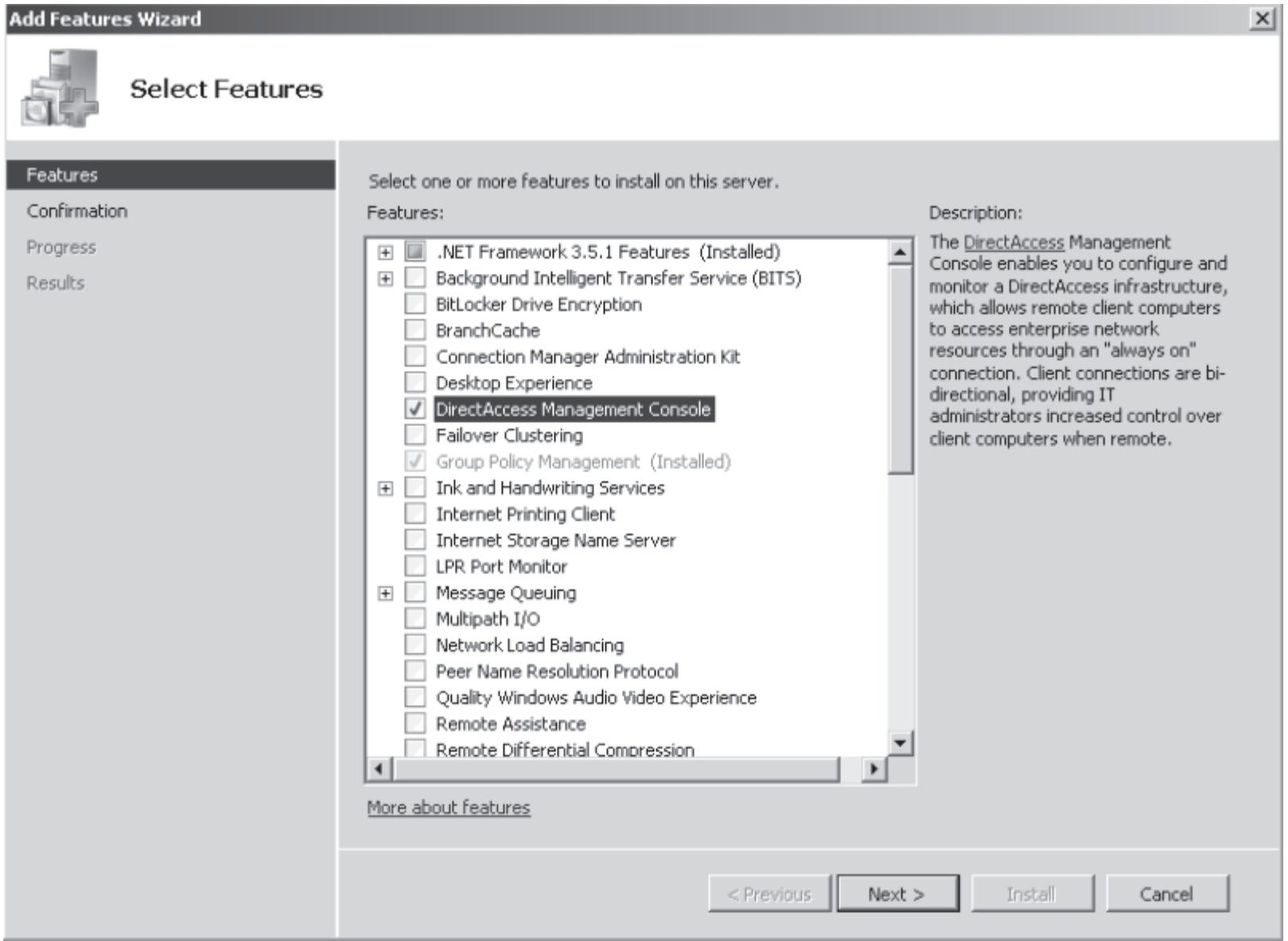
You can also get information about the IP-HTTPS configuration by issuing the command

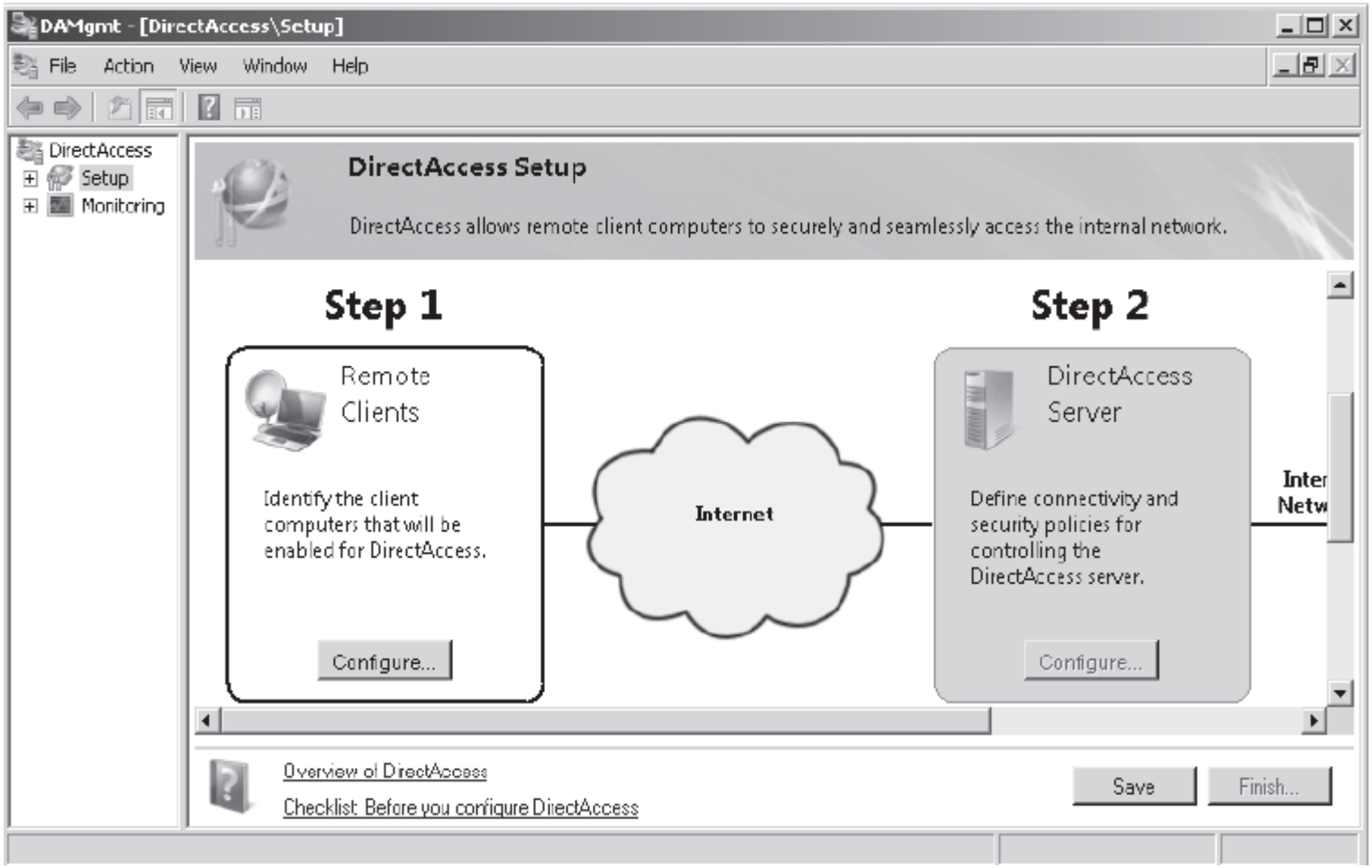
Netsh interface httpstunnel show interfaces

Configuring the DirectAccess server

You configure DirectAccess primarily by configuring the DirectAccess server.
When you configure the DirectAccess server, you also end up configuring the necessary Group Policy Objects (GPOs) that support DirectAccess.
Prior to installing DirectAccess, you should ensure
that the DirectAccess server meets the following requirements:
1. The computer needs to have Windows Server 2008 R2 installed and be a member of a domain.
2. This server must have two network adapters.
3.One of these network adapters needs to a direct connection to the Internet. You must assign this adapter two consecutive public IPv4 addresses.
4. The second network adapter needs a direct connection to the corporate intranet.
5 The computer needs digital certificates to support server authentication. This includes having a computer certificate that matches the fully qualified domain name (FQDN) that is assigned to the IP addresses on the DirectAccess server's external network interface.

To install DirectAccess on a server running Windows Server 2008 R2, add the DirectAccess Management Console feature using the Add Features Wizard





2. Select the Setup node. In the details pane, in the Remote Clients area, click Configure.

This opens the DirectAccess Client Setup dialog box. Click Add and then specify the name of the security groups to which you add computer accounts when you want to grant access to DirectAccess to specific clients running Windows 7. These groups can have any names. The one in Figure 10-7 is called DA_Clients

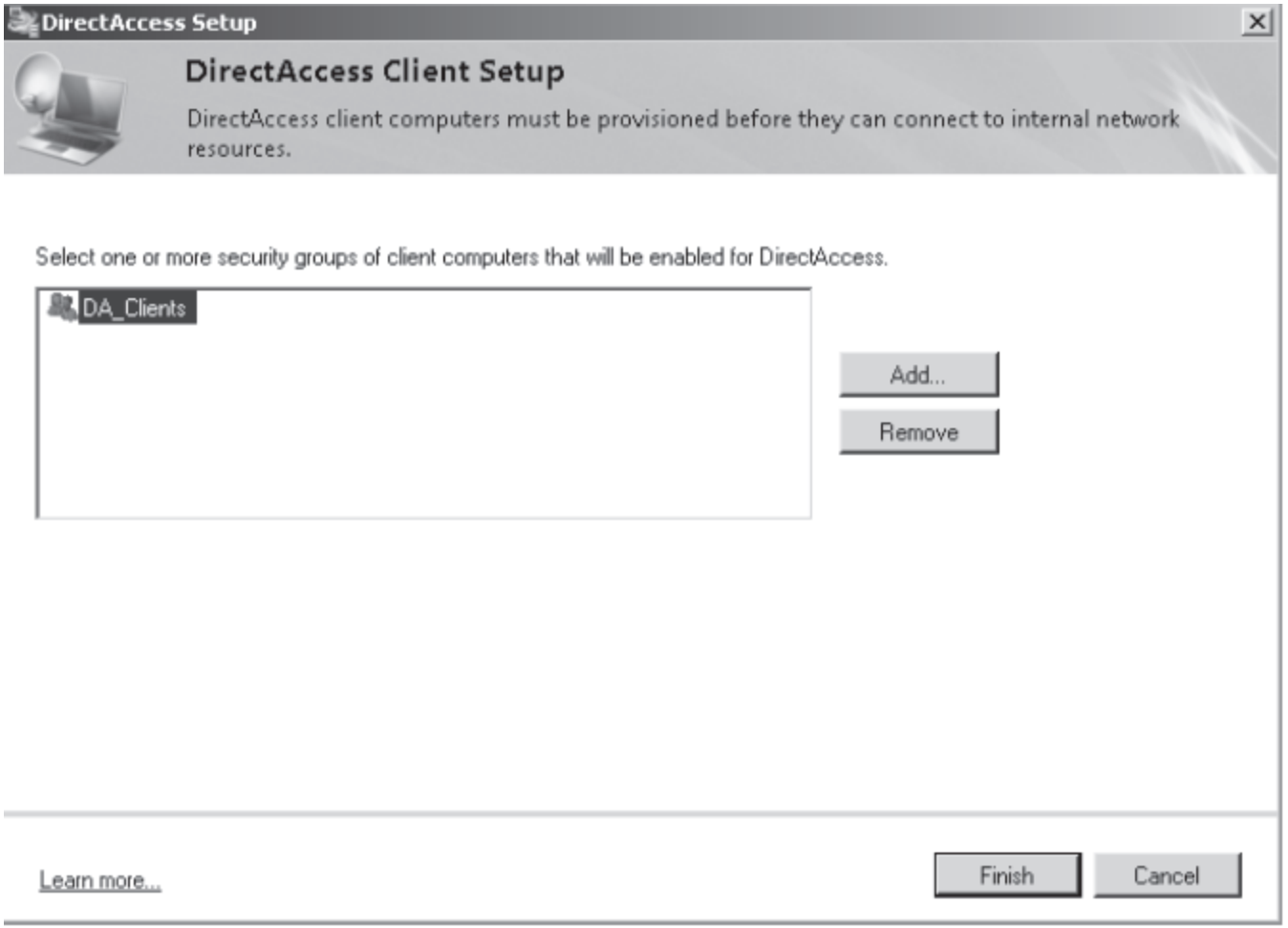


FIGURE 10-7 DirectAccess client groups

3. Use the DirectAccess Server Setup item to specify which interface is connected to the Internet and which interface is connected to the internal network. Performing this step will enable IPv6 transition technologies on the DirectAccess server, as shown in Figure 10-8. You use this item to specify the CA that client certificates must ultimately come from, either directly or through a subordinate CA. You also must specify the server certificate used to secure IP-HTTPS traffic.

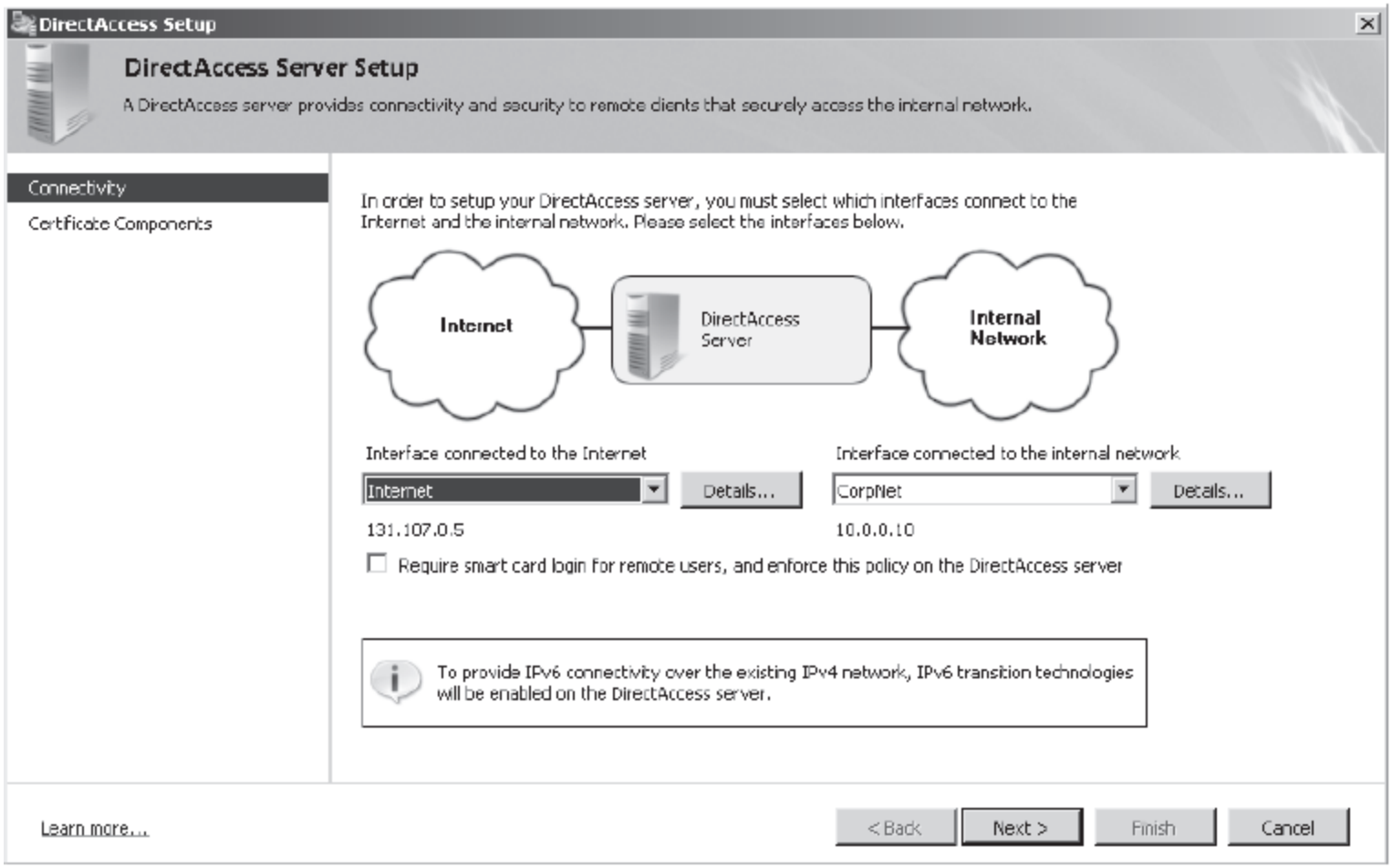


FIGURE 10-8 DirectAccess Server Setup

GO TO PAGE 524 (100%)