

# DIRECT ACCESS

SERVER 2012

## 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:

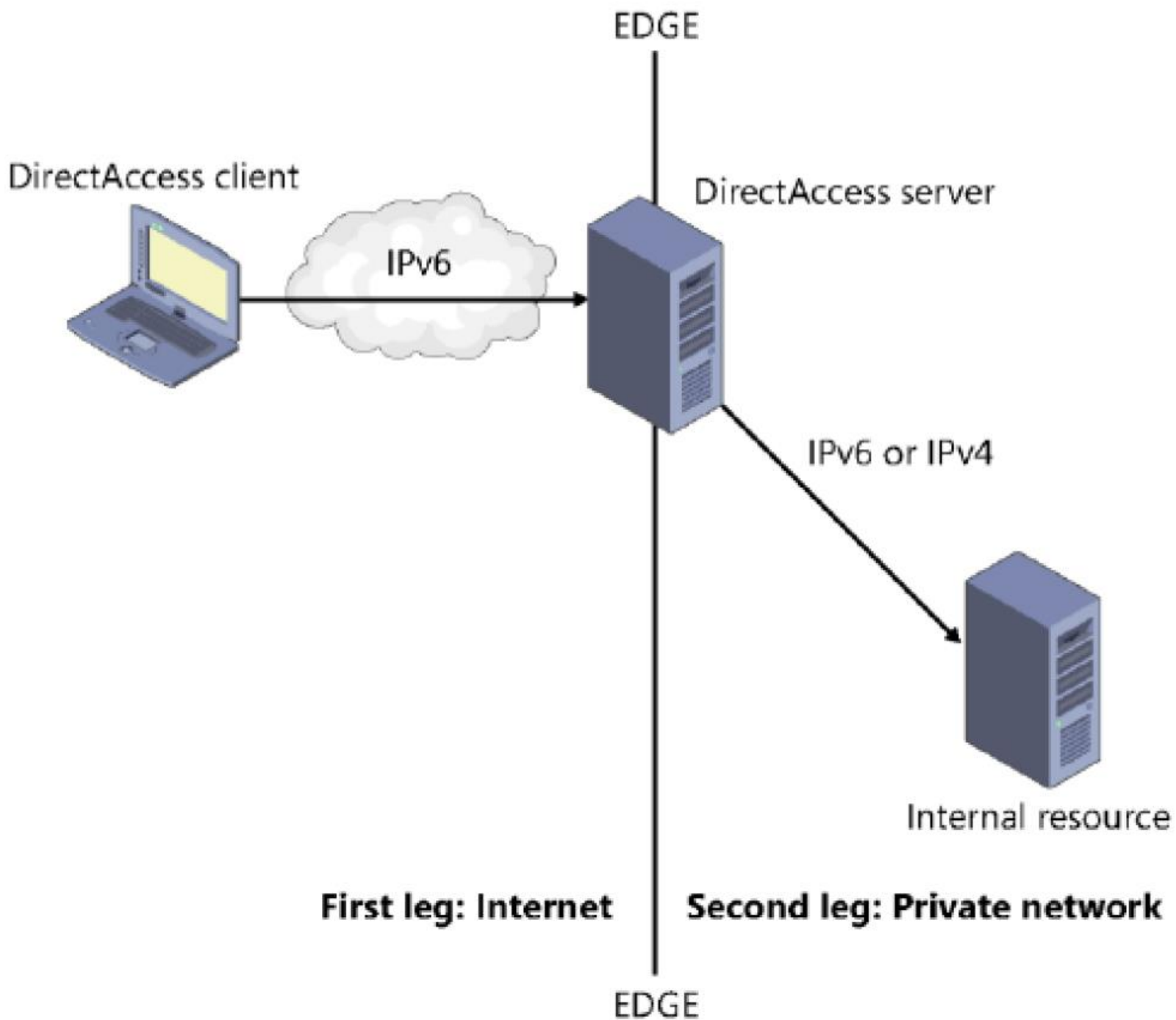
**Always-on connectivity** Unlike with a VPN, a DirectAccess connection is always on, even before the user logs on to his or her computer.

**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.



 Configuration

DirectAccess and VPN

Web Application Proxy

 testserver

## Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.



### Configure Remote Access

DirectAccess & VPN settings have not yet been configured. Select one of the wizard options.

→ [Run the Getting Started Wizard](#)

Use this wizard to configure DirectAccess and VPN quickly, with default recommended settings.

→ [Run the Remote Access Setup Wizard](#)

Use this wizard to configure DirectAccess and VPN with custom settings.



The Getting Started Wizard appears only the first time you open the Remote Access Management console. After you run this wizard, select the DirectAccess and VPN node to edit DirectAccess and VPN settings using the Remote Access setup wizard.

#### Welcome to Remote Access

Use the options on this page to configure DirectAccess and VPN.

→ **Deploy both DirectAccess and VPN (recommended)**

Configure DirectAccess and VPN on the server, and enable DirectAccess client computers. Allow remote client computers not supported for DirectAccess to connect over VPN.

→ **Deploy DirectAccess only**

Configure DirectAccess on the server, and enable DirectAccess client computers.

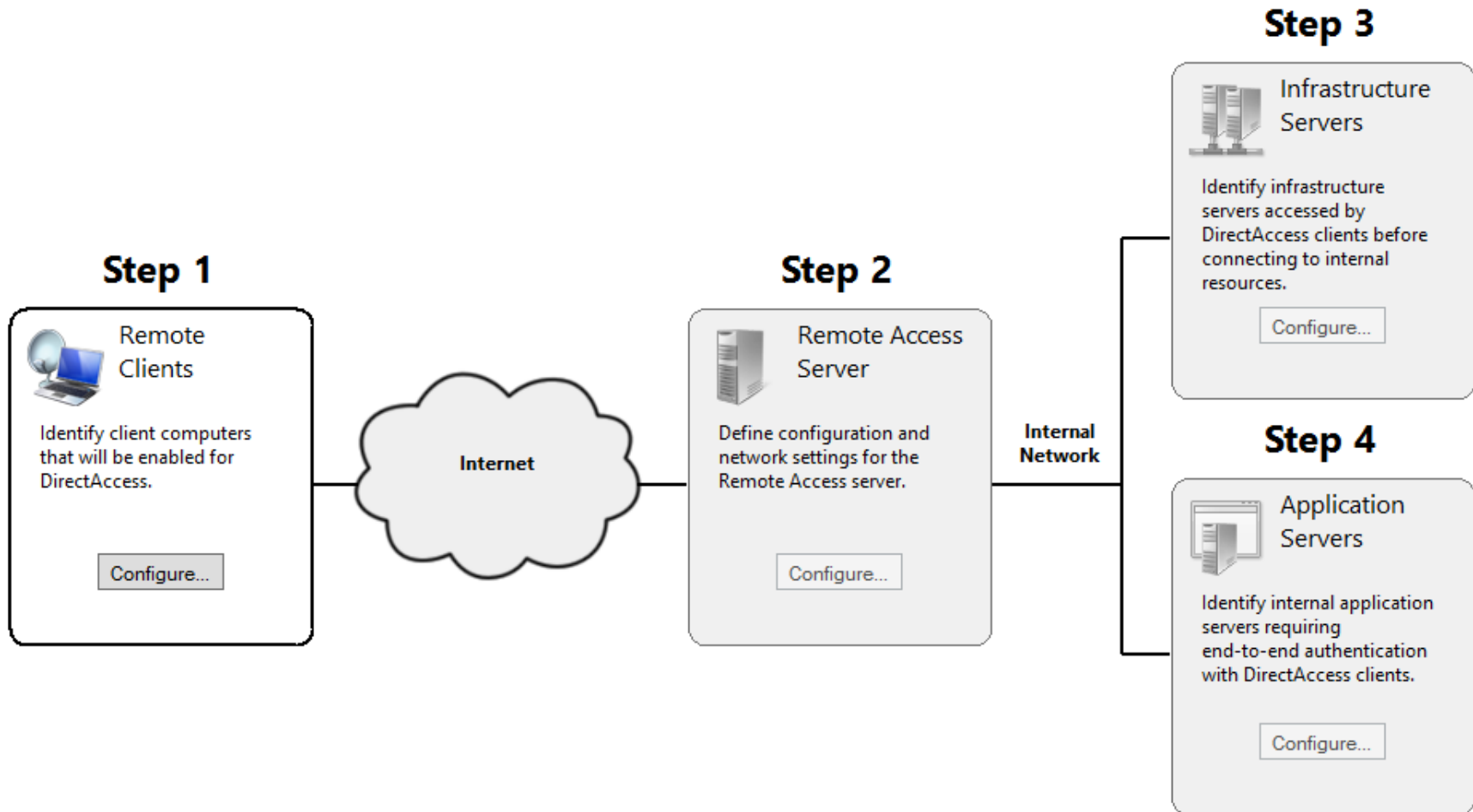
→ **Deploy VPN only**

Configure VPN using the Routing and Remote Access console. Remote client computers can connect over VPN, and multiple sites can be connected using VPN site-to-site connections. VPN can be used by clients not supported for DirectAccess.



## Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.



Finish...





## DirectAccess Client Setup

Enable DirectAccess for managed computers in specified security groups, and configure client settings.

### Deployment Scenario

Select Groups

Network Connectivity Assistant

Deploy DirectAccess to allow DirectAccess client computers located on the Internet to connect to internal network resources, and remotely manage DirectAccess clients.

Select a deployment scenario:

- Deploy full DirectAccess for client access and remote management

With this option selected, DirectAccess client computers located on the Internet can connect to the internal network via the Remote Access server. Administrators can remotely manage these clients.

- Deploy DirectAccess for remote management only

Administrators can remotely manage DirectAccess client computers located on the Internet. With this option selected, DirectAccess is not deployed for client access to the internal network.

< Back

Next >

Finish

Cancel

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
```

Remote Access Setup

### DirectAccess Client Setup

Enable DirectAccess for managed computers in specified security groups, and configure client settings.

Deployment Scenario

- Select Groups
- Network Connectivity Assistant

Select one or more security groups containing client computers that will be enabled for DirectAccess.

Domain Users (TESTSERVER0\Domain Users)

Add...

Remove

To perform this task in Windows PowerShell, use the `Add-DAClient` cmdlet with the `-SecurityGroupNameList` switch.

Enable DirectAccess for mobile computers only

With this setting enabled, all mobile computers in the specified security groups will be enabled as DirectAccess clients.

Use force tunneling

DirectAccess clients connect to the internal network and to the Internet via the Remote Access server.

Set-DAClient cmdlet with the `-OnlyRemoteComputers` switch.

< Back   Next >   Finish   Cancel

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.



## Remote Access Setup



### DirectAccess Client Setup

Enable DirectAccess for managed computers in specified security groups, and configure client settings.

Deployment Scenario

Select Groups

Network Connectivity Assistant

The Network Connectivity Assistant (NCA) runs on DirectAccess client computers to provide DirectAccess connectivity information, diagnostics, and remediation support.

Resources that validate connectivity to internal network:

	Resource	Type
▶	file://testserver.testserver.com/	HTTP
*		

Helpdesk email address:

DirectAccess connection name:

Allow DirectAccess clients to use local name resolution

< Back

Next >

Finish

Cancel



## Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.

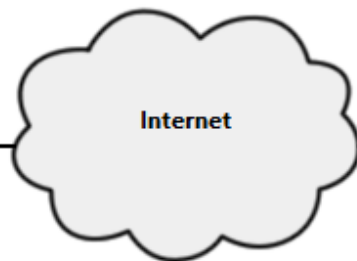
### Step 1



#### Remote Clients

Identify client computers that will be enabled for DirectAccess.

Edit...



### Step 2



#### Remote Access Server

Define configuration and network settings for the Remote Access server.

Configure...

Internal Network

### Step 3



#### Infrastructure Servers

Identify infrastructure servers accessed by DirectAccess clients before connecting to internal resources.

Configure...

### Step 4



#### Application Servers

Identify internal application servers requiring end-to-end authentication with DirectAccess clients.

Configure...



## Remote Access Setup



### Remote Access Server Setup

Configure DirectAccess and VPN settings.

#### Network Topology

Network Adapters

Authentication

Select the network topology of the server.

- Edge
- Behind an edge device (with two network adapters)
- Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed at the edge of the internal corporate network and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the Internet.

Type the public name or IPv4 address used by clients to connect to the Remote Access server:

< Back

Next >

Finish

Cancel



## Remote Access Server Setup

Configure DirectAccess and VPN settings.

### Network Topology

Network Adapters

Authentication

Select the network topology of the server.

- Edge
- Behind an edge device (with two network adapters)
- Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed behind an edge firewall or device, and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the perimeter network.

Type the public name or IPv4 address used by clients to connect to the Remote Access server:

< Back

Next >

Finish

Cancel

## Remote Access Setup



### Remote Access Server Setup

Configure DirectAccess and VPN settings.

#### Network Topology

Network Adapters

Authentication

Select the network topology of the server.

- Edge
- Behind an edge device (with two network adapters)
- Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed with a single network adapter that is connected to the internal network.

Type the public name or IPv4 address used by clients to connect to the Remote Access server:

< Back

Next >

Finish

Cancel

## Remote Access Setup



### Remote Access Server Setup

Configure DirectAccess and VPN settings.

#### Network Topology

Network Adapters

Authentication

Select the network topology of the server.

- Edge
- Behind an edge device (with two network adapters)
- Behind an edge device (with a single network adapter)

In this topology, the Remote Access server is deployed at the edge of the internal corporate network and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the Internet.

Type the public name or IPv4 address used by clients to connect to the Remote Access server:

< Back

Next >

Finish

Cancel



## Remote Access Setup



### Remote Access Server Setup

Configure DirectAccess and VPN settings.

Network Topology

Network Adapters

Authentication

Select the network adapters on the Remote Access server.

Adapter connected to the external network:

Internet

192.168.254.8

Adapter connected to the internal network:

Corporate

2002:836b:79:3333::1

Select the certificate used to authenticate IP-HTTPS connections:

Use a self-signed certificate created automatically by DirectAccess

CN=testserver.com

< Back

Next >

Finish

Cancel



## Remote Access Server Setup

Configure DirectAccess and VPN settings.

Network Topology

Network Adapters

Authentication

Specify how DirectAccess clients authenticate. If computer certificates are not used for authentication, DirectAccess acts as a Kerberos proxy on behalf of the client. Enable support for Windows 7 clients and Network Access Protection (NAP) compliance.

### User Authentication

- Active Directory credentials (username/password)
- Two-factor authentication (smart card or one-time password (OTP))
- Use OTP

### Use computer certificates

Select the root or intermediate certification authority (CA) that issues the certificates.

- Use an intermediate certificate

Browse...

- Enable Windows 7 client computers to connect via DirectAccess
- Enforce corporate compliance for DirectAccess clients with NAP

< Back

Next >

Finish

Cancel

**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.



## Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.

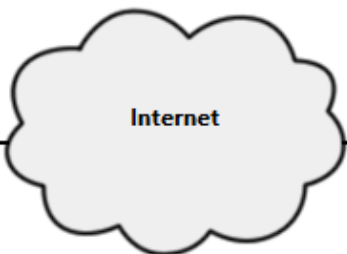
### Step 1



#### Remote Clients

Identify client computers that will be enabled for DirectAccess.

Edit...



### Step 2



#### Remote Access Server

Define configuration and network settings for the Remote Access server.

Configure...

Internal Network

### Step 3



#### Infrastructure Servers

Identify infrastructure servers accessed by DirectAccess clients before connecting to internal resources.

Configure...

### Step 4



#### Application Servers

Identify internal application servers requiring end-to-end authentication with DirectAccess clients.

Configure...

Finish...



## Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

### Network Location Server

DNS

DNS Suffix Search List

Management

Specify settings for the network location server, used to determine the location of DirectAccess client computers. A client computer connecting successfully to the site is assumed to be on the internal network, and DirectAccess is not used.

- The network location server is deployed on a remote web server (recommended)

Type in the URL of the network location server:

- The network location server is deployed on the Remote Access server

Select the certificate used to authenticate the network location server:

Use a self-signed certificate



The network location server must be highly available to DirectAccess client computers inside the internal network, and inaccessible to DirectAccess clients located on the Internet. Clients must be able to contact the CRL for the site.



# Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server

DNS

DNS Suffix Search List

Management

Enter DNS suffixes and internal DNS servers. DirectAccess client queries that match a suffix use the specified DNS server for name resolution. Name suffixes that do not have corresponding DNS servers are treated as exemptions, and DNS settings on client computers are used for name resolution.

	Name Suffix	DNS Server Address
▶	.local	...
	nls. .local	
*		

Select a local name resolution option:

- Use local name resolution if the name does not exist in DNS (most restrictive)
- Use local name resolution if the name does not exist in DNS or DNS servers are unreachable when the client computer is on a private network (recommended)
- Use local name resolution for any kind of DNS resolution error (least restrictive)

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.



## Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server

DNS

DNS Suffix Search List

Management

Add additional suffixes to search for short unqualified name in multiple locations. If a query fails for a suffix, the other suffixes are appended to the name and the DNS query is repeated for the alternate FQDN.

Configure DirectAccess clients with DNS client suffix search list

Detected domain suffixes:

Add ->

<- Remove

Domain suffixes to use:

<Primary DNS suffix of client>  
.local

^

v

New Suffix:

Add



The primary domain DNS suffix appears first in the list.

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.

### Infrastructure Server Setup

Configure infrastructure servers. DirectAccess clients access these servers before connecting to resources on the internal network.

Network Location Server

DNS

DNS Suffix Search List

Management

Specify management servers used for DirectAccess client management. For example update and remediation servers.

Management servers:

	Management Servers (IP Address, IPv6 Prefix, FQDN)
▶*	



After you complete the wizard and apply the settings, the management servers list will be updated with automatically-discovered System Center Configuration Manager servers.

< Back

Next >

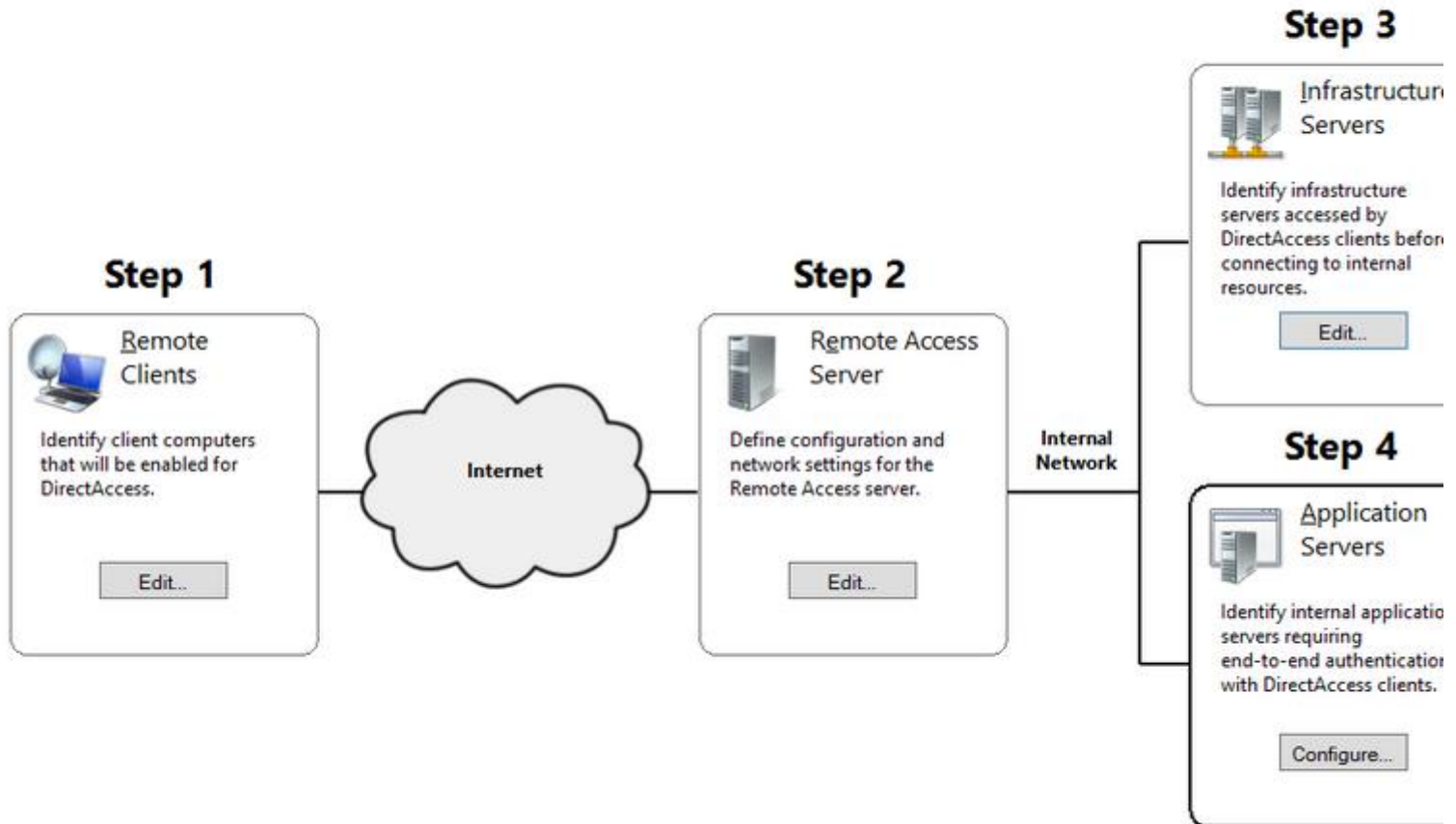
Finish

Cancel



## Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.



Some configuration changes have not been applied. Click Finish to apply the changes.





## DirectAccess Application Server Setup

Optionally configure authentication between DirectAccess clients and internal application servers.

By default, DirectAccess requires IPsec authentication and encryption between the DirectAccess client and server. In addition, you can optionally require end-to-end authentication and encryption between DirectAccess clients and selected internal application servers.

- Do not extend authentication to application servers
- Extend authentication to selectd application servers

Select the security groups containing the servers:

Add...

Remove

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

- Allow access only to servers included in the security groups

With this option enabled, clients can only access application servers in the specified security groups. Clients can still access infrastructure servers, including domain controllers, DNS servers, and servers used for DirectAccess client management.

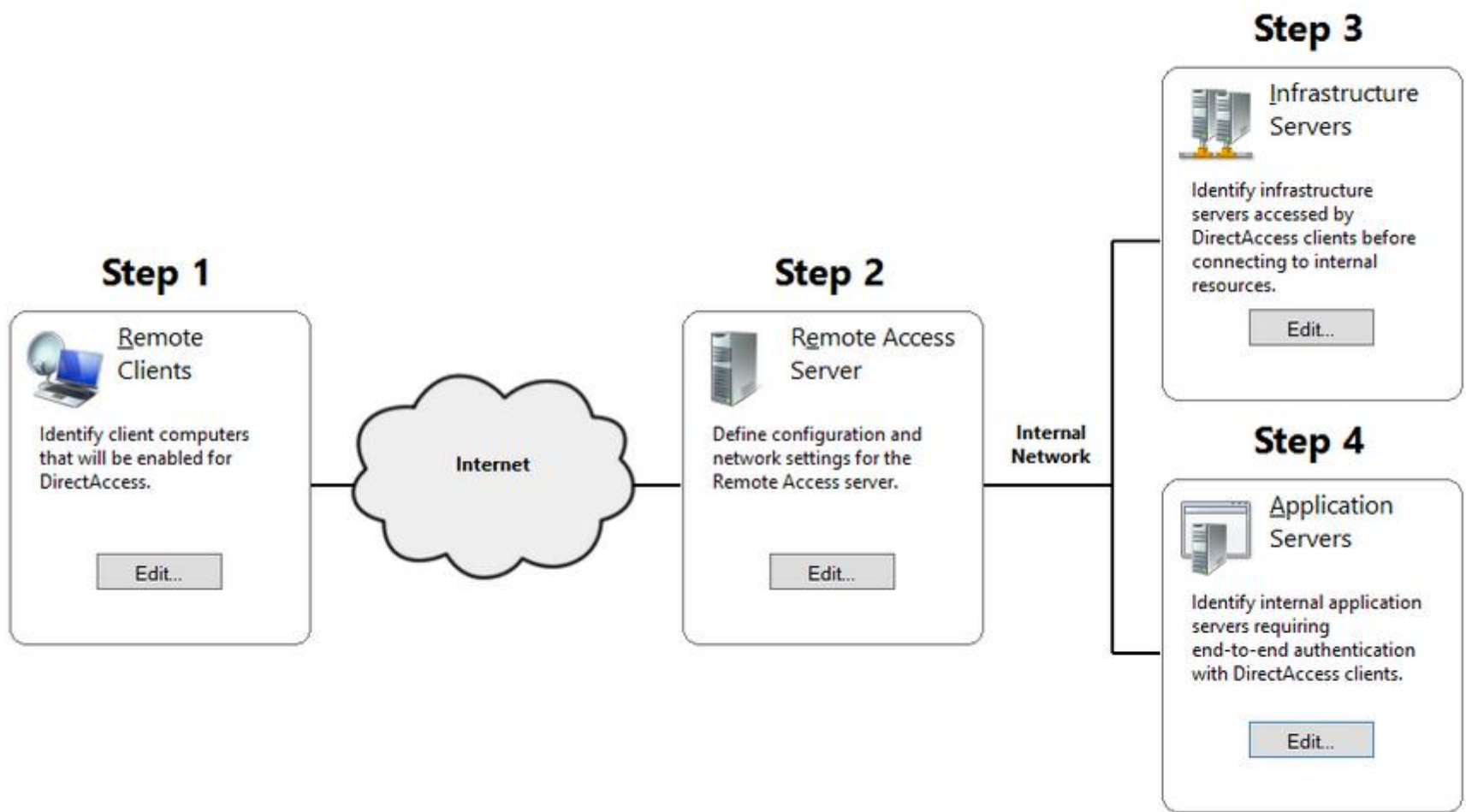
- Do not encrypt traffic. Use authentication only

With this setting enabled, end-to-end traffic is authenticated but not encrypted. This option is less secure. Authentication without encryption is supported only for application servers running Windows Server 2008 R2 or a later operating system.



## Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.



Some configuration changes have not been applied. Click Finish to apply the changes.

## Remote Access Review

Summary of Remote Access configuration settings.

Review the configuration settings.



### GPO Settings [Change...](#)

DirectAccess server GPO name:

DirectAccess Server Settings

Client GPO name:

DirectAccess Client Settings



### Remote Clients

- DirectAccess is deployed for client access and remote client management
- DirectAccess security groups:



\DirectAccess Computers

- Force tunneling is disabled
- Resource used to verify internal network connectivity:

[Save to a file](#) | [Print](#)

[Apply](#)

[Cancel](#)

## Applying Remote Access Setup Wizard Settings


### Applying Remote Access Setup Wizard Settings

Remote Access will be updated with configuration settings.



The configuration was applied successfully.



 More details

Close