Tutorial 9

Installing and Configuring a VPN

- **Lab Scenario & Preparation**

This lab, students are required to configure VPN connection to enable SRV-B to connect to Local Area Network of adatum.com.

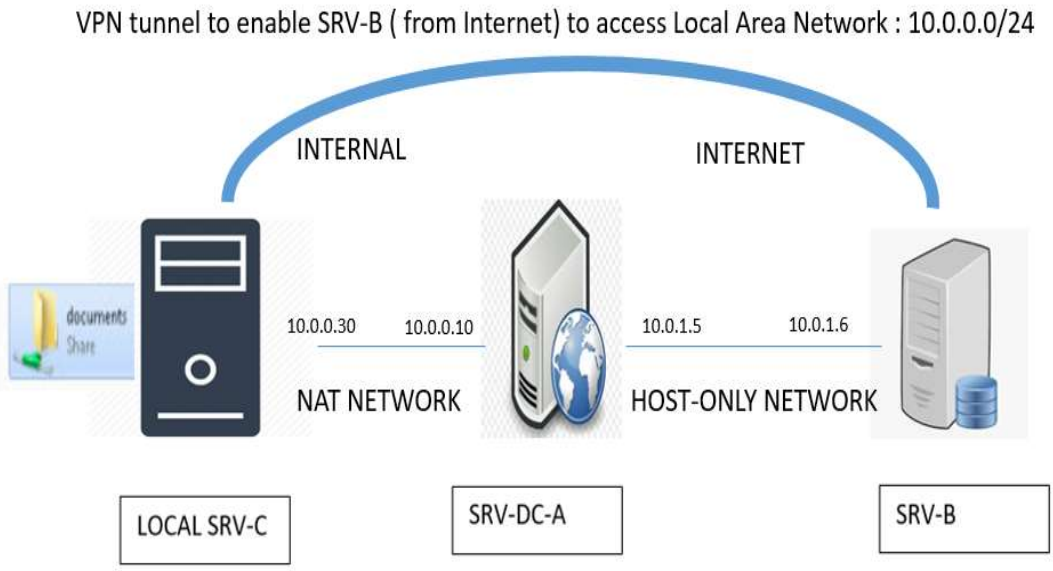
Without VPN, people from outside (the Internet) cannot connect to LOCAL network (10.0.0.0/24).

For some cases, for example, tele-workers or vendors want to connect to Local network to use Local services such as Local web server, Local email servers, local file servers (which is not published online, just available for local users), VPN is a good choice by utilizing the existing Internet connection to create a private tunnel to Local Network.

To prepare for the lab, we need 3 servers:

- **SRV-DC-A** has 2 network adapters:
  + External: 10.0.3.15 to mimic Internet by **adding 1 more network adapter** (*Host-only*)
  + Internal: 10.0.0.10 (current NAT network adapter).
- **SRV-B:** *restored* to the state of a *newly installed server* and set Adapter connection type to **Host-only network**
- **SRV-C:** 10.0.0.30 (NAT network) and already joined domain adatum.com *(Nothing to do with this Server)*.

Following figure is the lab model:



Exercise 1

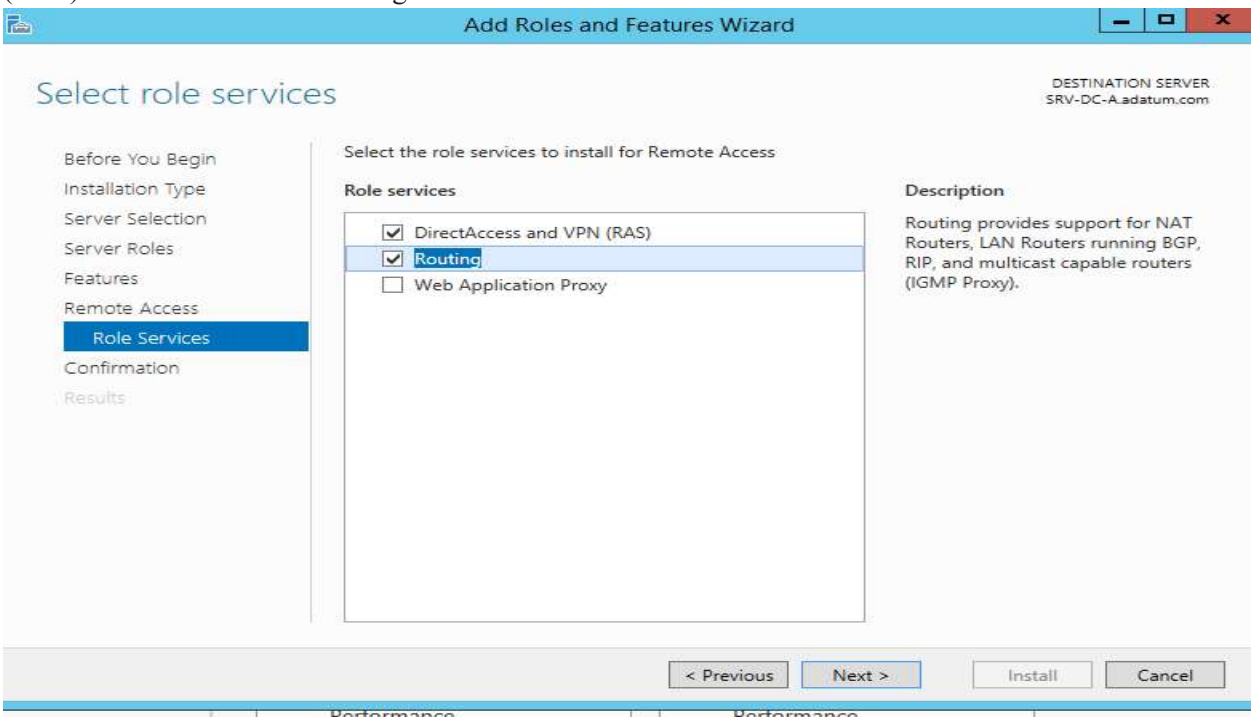
Overview: To configure standard VPN connections, you use Routing and Remote Access Server. You install Routing and Remote Access Server on SRV-DC1.

Completion time: 15 minutes

Mindset Question: During this lab, you install and configure Routing and Remote Access Server. What are all of the functions that the Routing and Remote Access Server can perform?

1. Log in to SRV-DC1 as the **ADATUM\Administrator** user account. The Server Manager console opens.
2. On Server Manager, click Manage and click Add Roles and Features. The Add Roles and Feature Wizard opens

3. On the Before you begin page, click Next.
4. Select *Role-based or feature-based installation* and then click Next.
5. On the Select destination server page, click Next.
6. Scroll down and select Remote Access.
7. When the Add Roles and Features Wizard dialog box opens, click Add Features.
8. Back on the Select server roles page, click Next. On the Select features page, click Next.
9. On the Remote Access page, click Next. On the Select role services page, keep DirectAccess and VPN (RAS) selected and select Routing. Click Next.



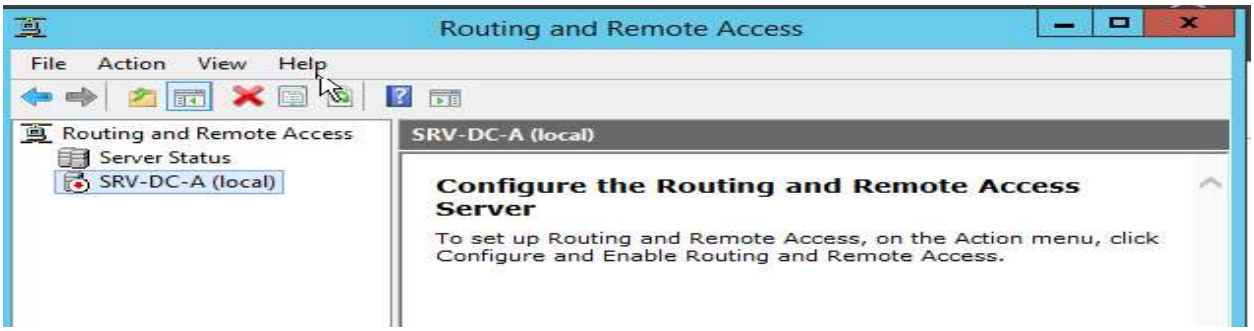
10. On the Confirm installation selections page, click Install.
11. When the installation is complete, click Close.
End of exercise

Exercise 2 Configuring a VPN Server

Overview Server01 will be the primary application server, which will be used for most applications.
Completion time 30 minutes

Mindset Question: Routing and Remote Access Server supports VPN connections. What are the types of VPN connections that are supported by Routing and Remote Access Server?

Preparation: See videos uploaded on FIT portal to setup Lab model.
1. On SRV-DC1, Server Manager, click Tools > Routing and Remote Access. The Routing and Remote Access console opens as shown in Figure.

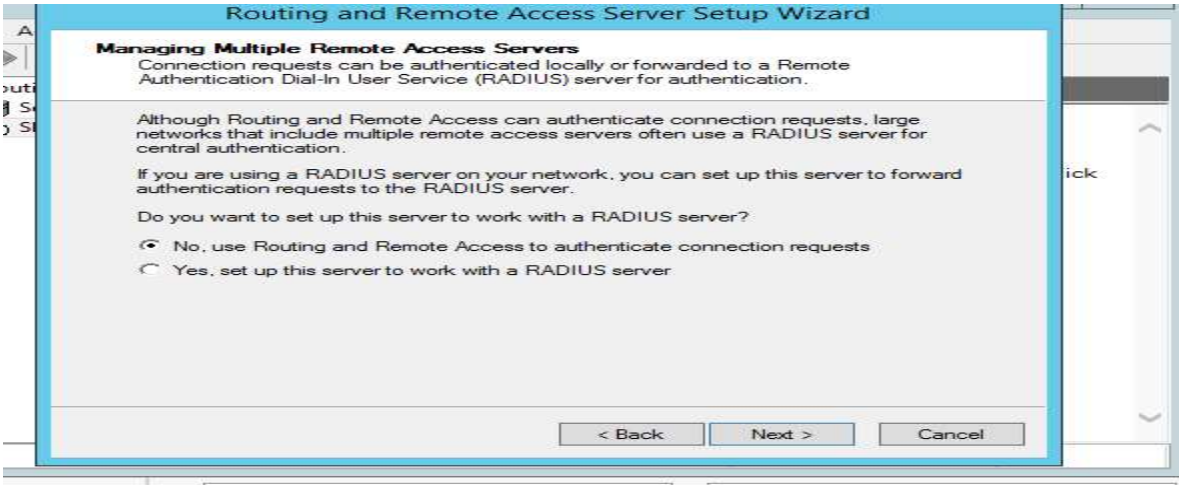


2. Right click on SRV-DC-A, choose Configure the Routing and Remote Access Server, Click Next. Choose Virtual Private Network and NAT.

On the VPN Connection page, select External and click Next.
3. On the IP Address Assignment page, click *From a specified range of addresses* and click Next.
4. On the Address Range Assignment page, click New.

5. When the New IPv4 Address Range dialog box opens, specify the Start IP address as **10.0.0.10** and the End IP address as **10.0.0.50**. Click OK

6. Back on the Address Range Assignment page, and Click Next.



7. On the *Managing Multiple Remote Access Servers* page. Choose *"No, use Routing and Remote Access to authenticate".* Click Next.

8. On the Completing the Routing and Remote Access Server Setup Wizard page, click Finish.

Note: [These following cases can happen if firewall is not disabled. It is not usually the case.

1. When is says that you have to open a port of Routing and Remote access in the Windows Firewall, click OK.
2 When it asks to support the relaying of DHCP messages from remote access clients message, click OK

3. After RRAS starts, click the Start button, and click Administrative Tools. When the Administrative Tools opens, double-click *Windows Firewall with Advanced Security*.
4. When Windows Firewall with Advanced Security opens, under Actions, click Properties.
5. When the *Windows Firewall with Advanced Security on Local Computer* dialog box opens, change the Firewall state to Off.
6. Change the Firewall state to Off in the Private profile and Public Profile tabs.
7**.** Click OK to close the *Windows Firewall with Advanced Security on Local Computer* dialog box.
8. Close *Windows Firewall with Advanced Security* and *Administrative Tools*.

9. Right-click Server01 in Routing and Remote Access, and click Properties.

Question 1	*Which tab would you use to specify a preshared key for RRAS?*

Question 2	*Which VPN method requires a digital ceritificate to provide a SSL connection?*

10. Click OK to close the SRV-DC1 Properties dialog box.
11. Right-click Ports and click Properties. The Ports Properties dialog box opens.

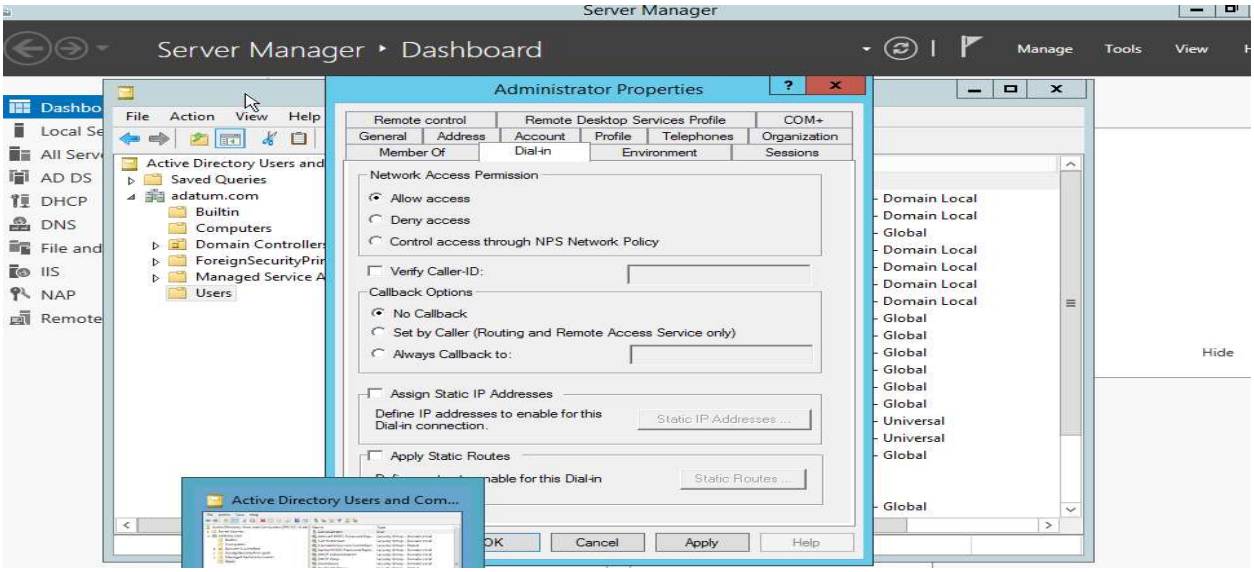
Question 3	*By default, how many IKEv2 connections are available?*

13. Click OK to close the Ports Properties dialog box.
14 On Server Manager, from Tools, click *Active Directory Users and Computers*.
15. Expand adatum.com, if needed, and then click Users.
16. Double-click the *Administrator* account. The Administrator Properties dialog box opens.

17. Click the Dial-in tab.

Question 4	*What is the default setting for Network Access Permission?*

18. In the Network Access Permission section, click to select Allow access, as shown in Figure:

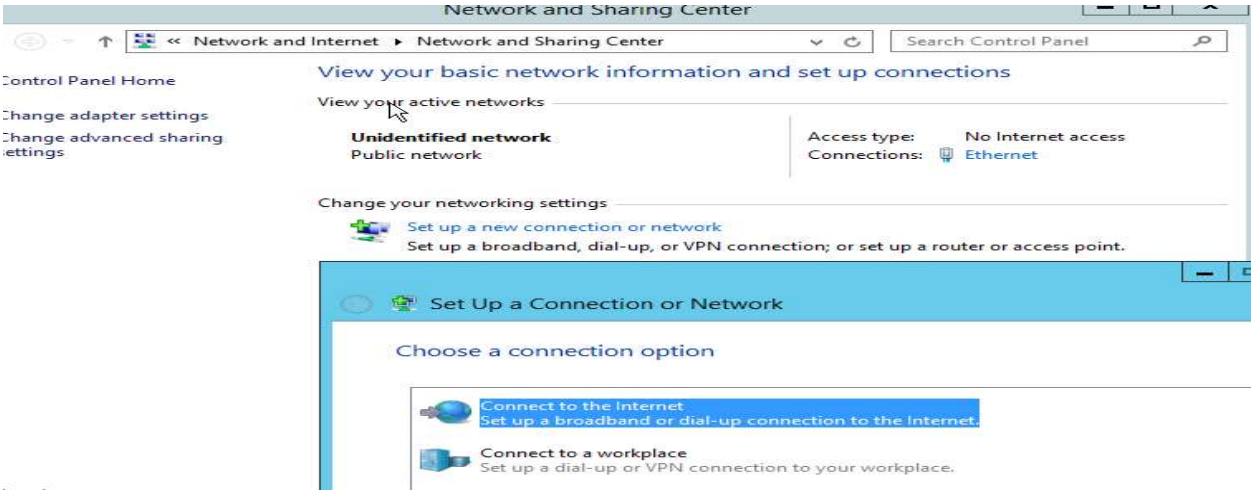


19. Click OK to close the Administrator Properties dialog box.
20. Close Active Directory Users and Computers.
End of exercise.

Exercise 2

Overview Now that you have configured the VPN server, you need to configure a client to connect to the VPN server. During this exercise, you use SRV-B to act as a VPN client.
Completion time 30 minutes

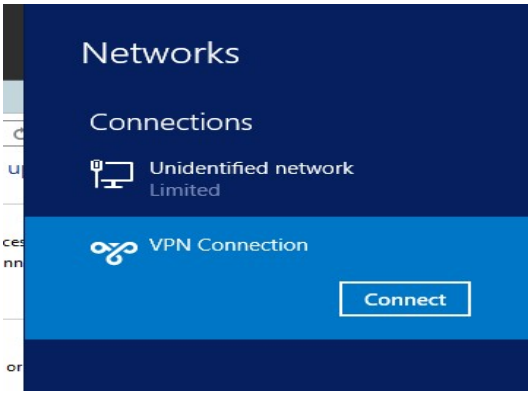
1. Log in to SRV-B as the local **Administrator** user account. The Server Manager console opens.
2. On SRV-B, on the Taskbar, right-click Network and Sharing Center icon and click Open Network and Sharing Center.
3. Choose *Set up a new connection or network*.
4. On the Set Up a Connection or Network page, choose Connect to a workplace. Click Next.



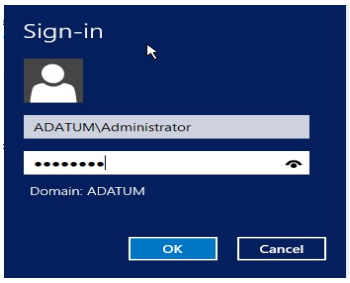
5. On the Connect to a Workplace page, click Use my Internet connection.
6. If it asks if you want to set up Internet connection, click *I'll set up an Internet connection later*.

7. When it asks you to type the Internet address to connect to, type **10.0.0.30 (***IP of SRV-C***)** in the Internet address text box. Click Create.

8. When the Networks pane appears as shown in Figure, click VPN Connection and click Connect.



9. It will ask you to enter Username & Password, in this case, type ADATUM\Administrator and Password to connect (This is the user that you configure Allow dial-in in previous exercise).



10. On CLIENT SRV-C, create a folder on Desktop named HR-Contact. Right click and Share this folder to Everyone.

11. Now back to SRV-B, go to Run, type \\10.0.0.30 (IP of SRV-C), you can see the shared document.

That means you successfully created VPN to enable SRV-B to connect to SRV-C in local network.

End of lab.