**NE259 – Windows Server – Lab8**

**Points deducted if All Answers Are Not In: Ariel, 14pt, Bold, Red!**

In this lab you will install and configure a VPN between the SRV16 system and WIN10. You will do this by installing the VPN Role to SRV16 and then providing the IP address range of the VPN network as well as defining users who may use the VPN. From there you’ll create a new network connection on the WIN10 system and use that connection to deploy a private and encrypted network between the two systems.

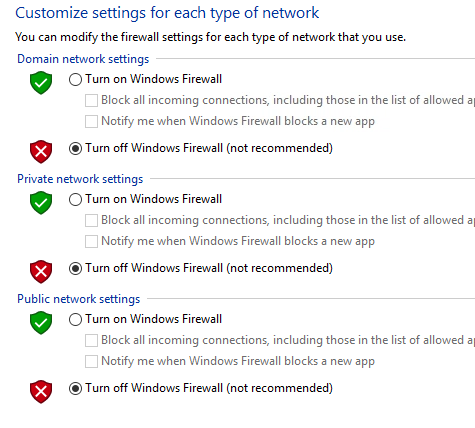
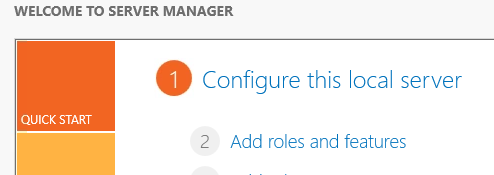
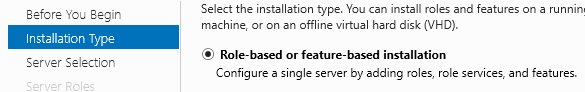
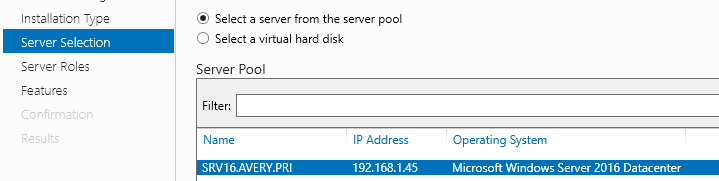
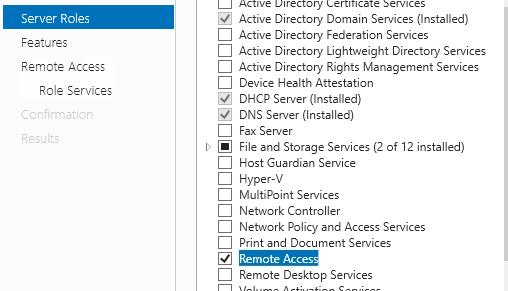
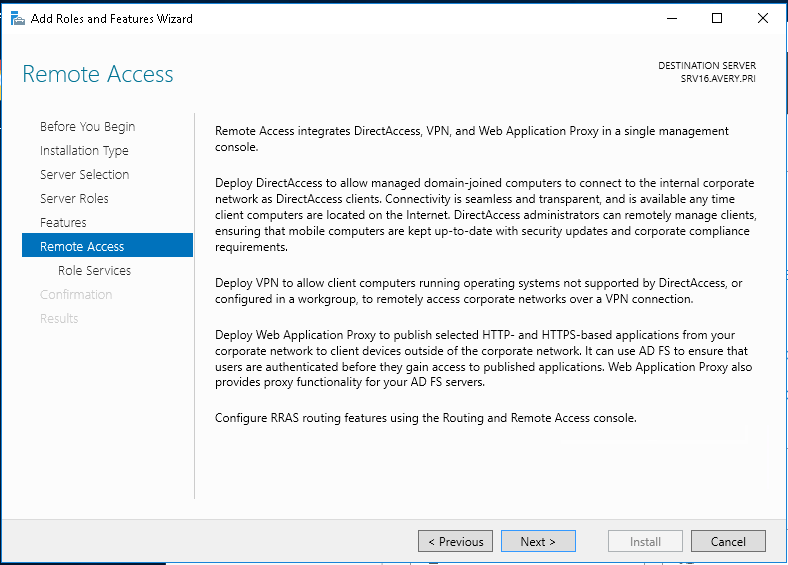
Required Materials:

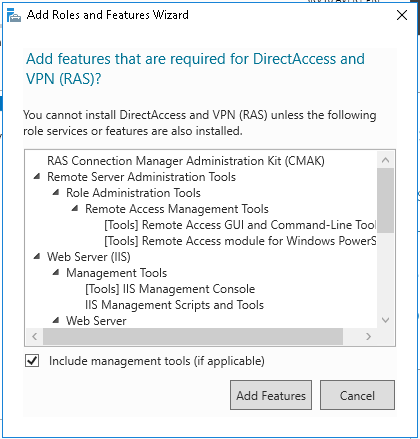
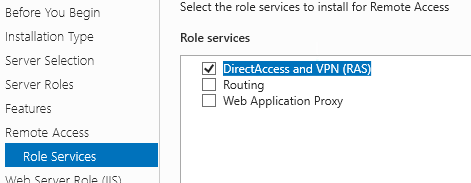
Windows Server 2016 and Windows 10 images prepared previously

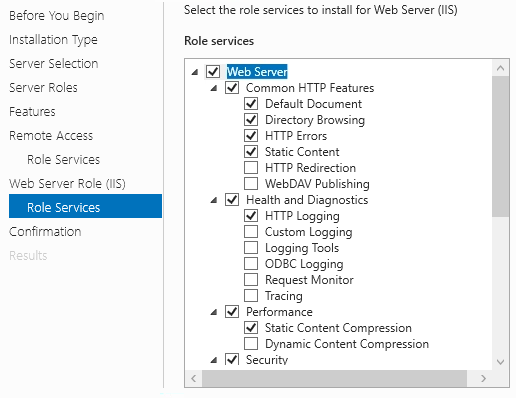
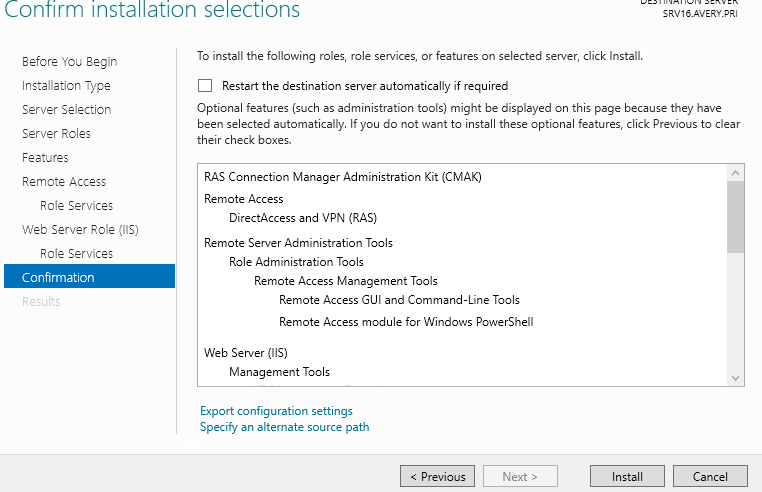
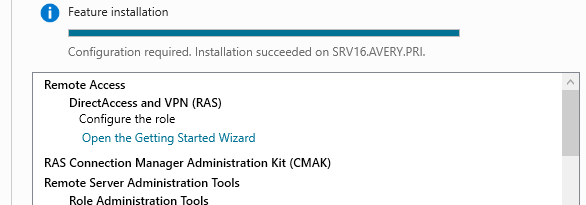
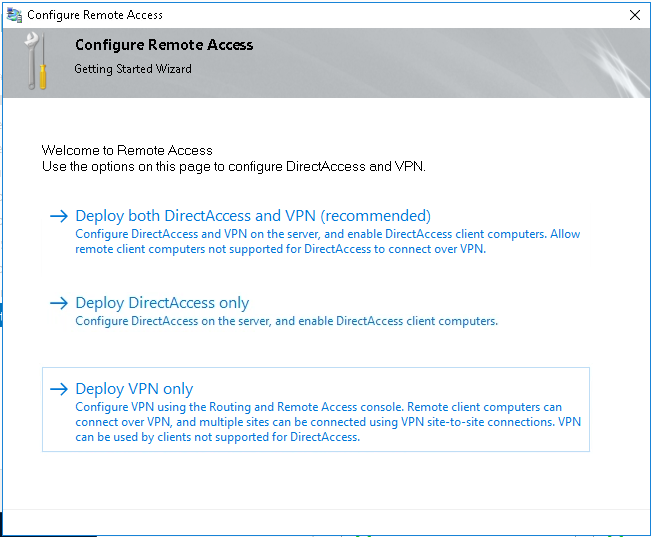
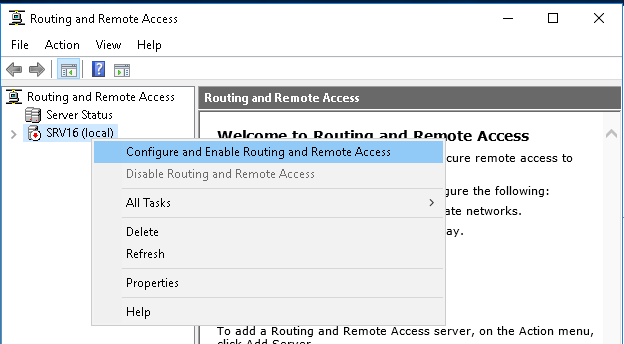
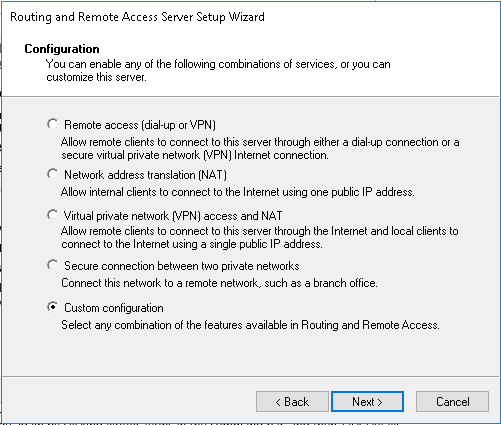
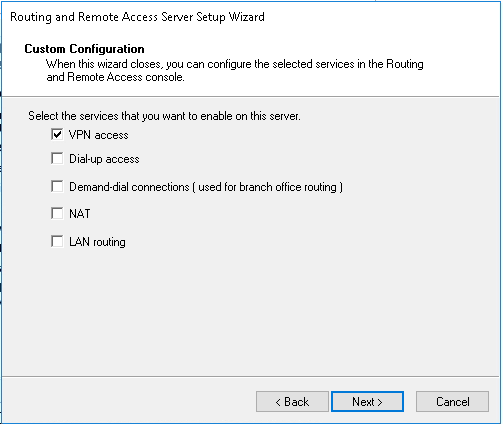
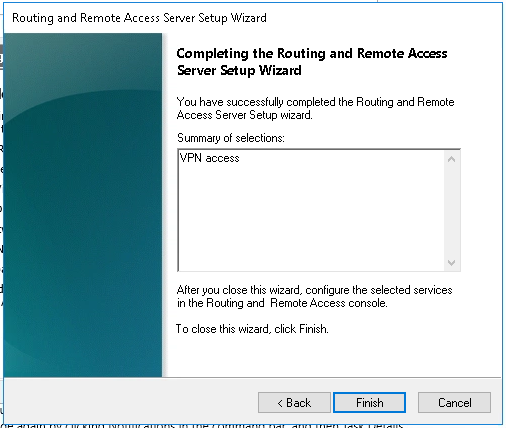
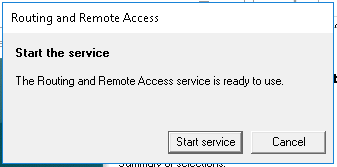
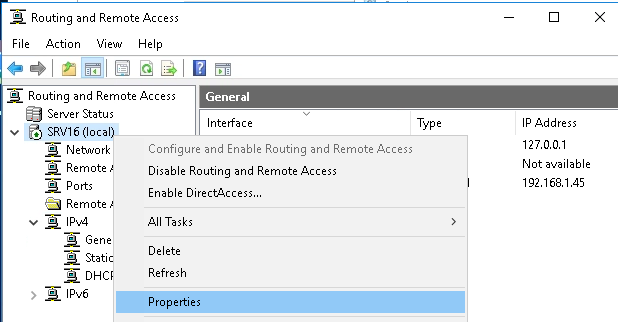
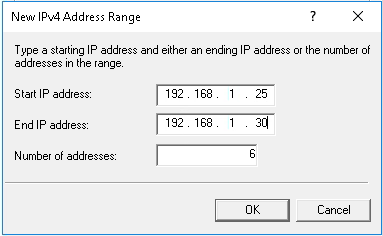
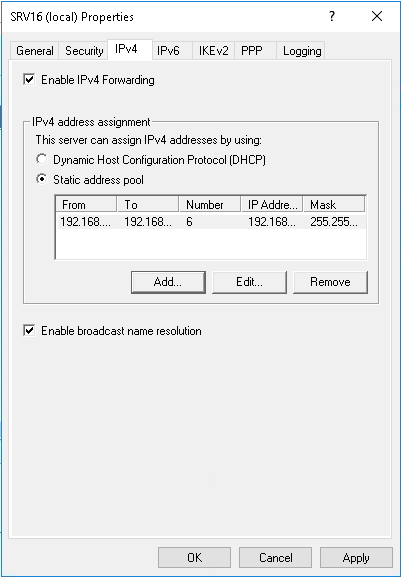
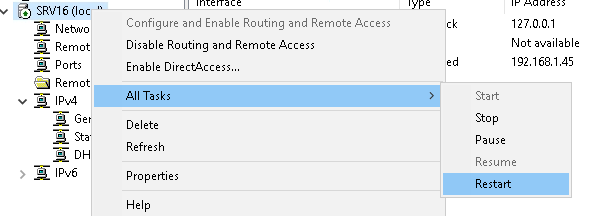
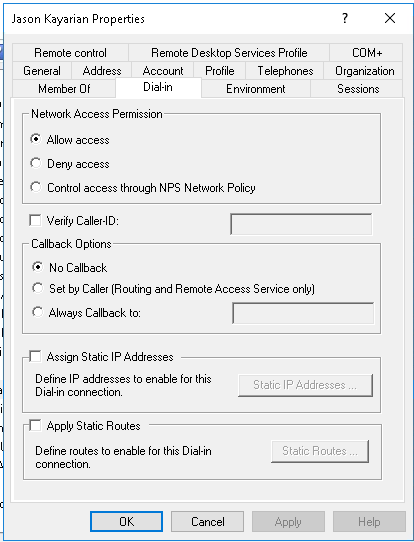
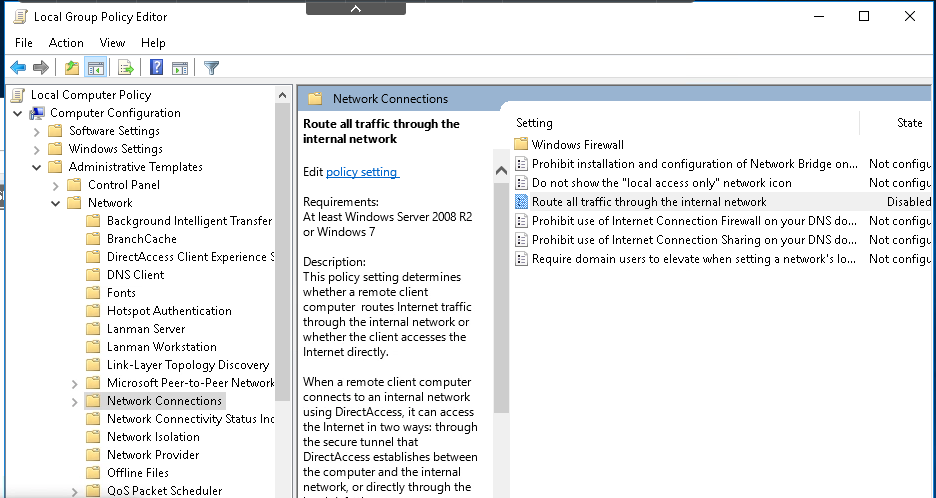
***Please note that the screen shots presented in this and other labs may not look exactly like what you will see on your computer. They are presented for orientation purposes only, and are not to be duplicated blindly.***

Part 1: Install the VPN Role to SRV16

Before you can connect WIN10 to the SRV16 VPN you must install the VPN role to SRV16. This is done through the Server Manager.

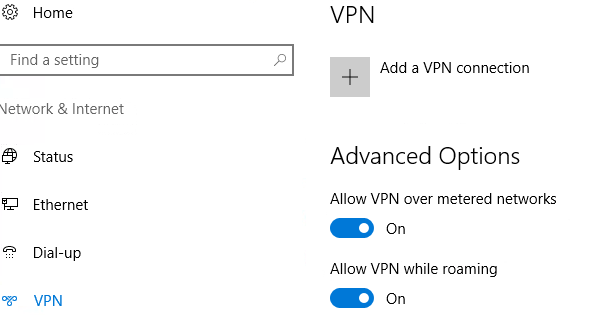
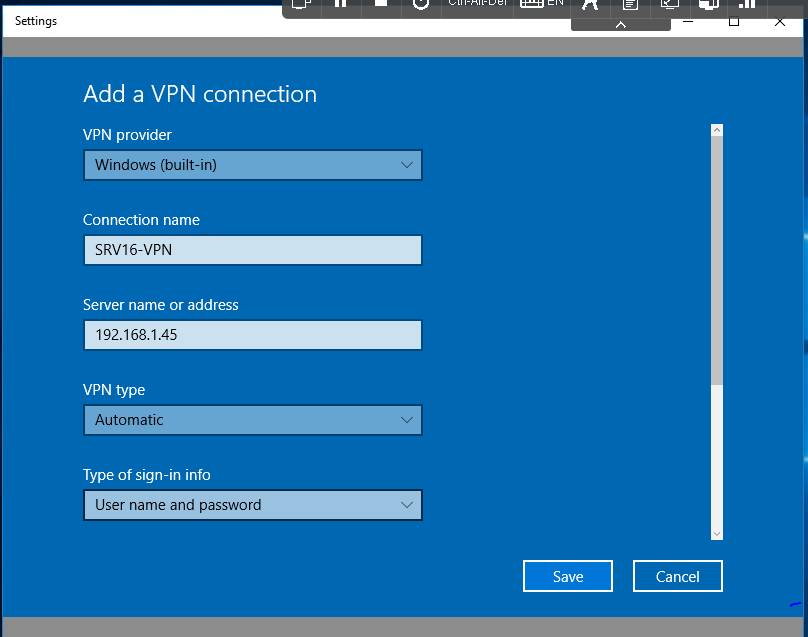
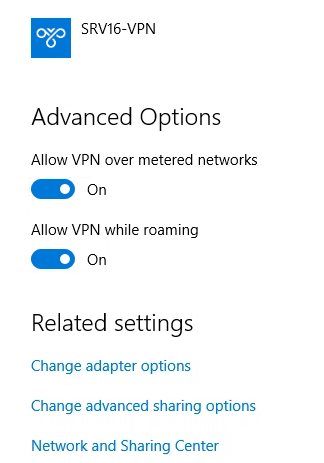
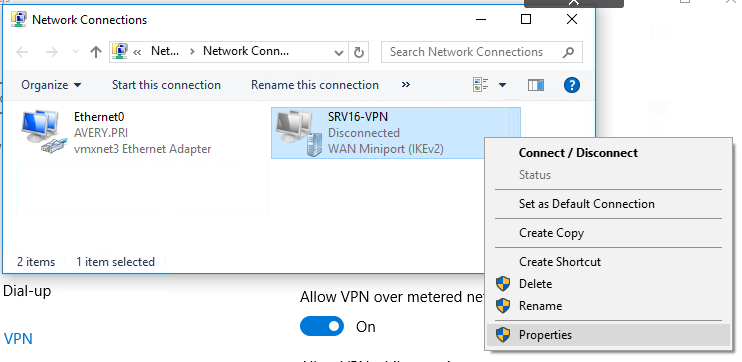
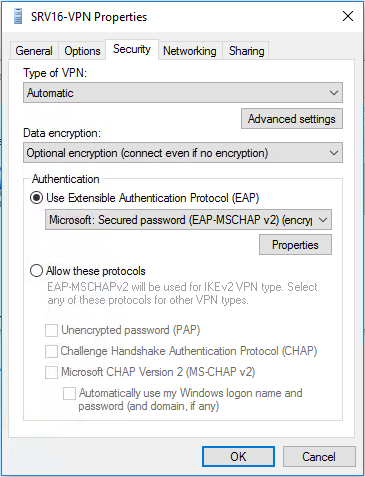
* Start your **SRV16** image and log on with your personal administrative credentials.
* Turn off the firewall  
    
  
* From the Server Manager choose ‘**Add roles and features’**.
* Leave the default ‘**Role-based or feature-based installation’**  
  
* Select the **SRV16** server and click next  
    
  
* From the list of server roles choose ‘**Remote Access’**  
  
* Leave the ‘features’ list as default and click ‘Next’
* Click ‘**Next’** to begin installing the ‘Remote Access’ services  
    
  
* Select the **‘DirectAccess and VPN (RAS)**’ role service and then click ‘Add Features’ on the next dialog box. Click ‘Next’ when finished.

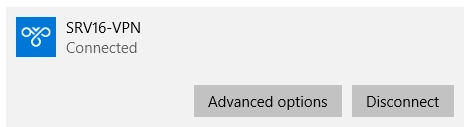
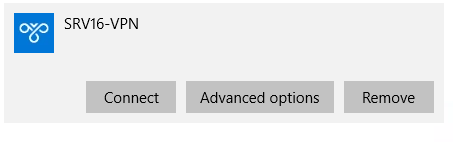


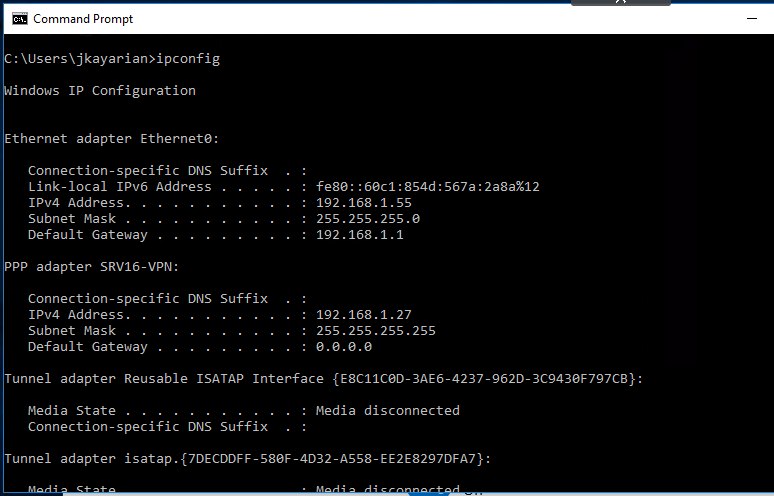
* Leave the Web Server (IIS) role services as default and click ‘Next’. 
* Leave the ‘Confirmation’ dialog as default and click ‘Install’  
    
  
* When the installation is finished click ‘Open the Getting Started Wizard’.  
  
* Select ‘Deploy VPN only’  
    
  
* On the ‘Routing and Remote Access’ snap-in right-click on the ‘SRV16 (local) server and select ‘Configure and Enable Routing and Remote Access’  
  
* Click ‘Next’ on the initial screen dialog box then select ‘Custom configuration’ on the Configuration dialog box.  
    
  
* Choose ‘VPN access’ then click ‘Next’  
    
  
* Click ‘Finish’  
    
  
* Click [Start service]  
  
* In the ‘Routing and Remote Access’ snap-in right-click the SRV16 (local) system and select ‘Properties’.  
    
  
* From the ‘IPv4’ tab, select ‘Static address pool’ and [**Add**] the range of 192.168.1.25 – 192.168.1.30. Click ‘OK’ > ‘OK’. Return back to the ‘Routing and Remote Access’ snap-in.
* Once again right-click the SRV16 (local) system > All Tasks > Restart.  
  
* Once done, go to ‘Active Directory Users and Computers’ and go to the properties of the **Administrator** account. On the ‘Dial-in’ tab set the ‘Network Access Permission’ for (\*) Allow access.  
  
* Now you’ll need to ensure that ALL VPN traffic from the Win10 machine goes through this connection. Do this by editing the ‘Local Group Policy’ with: **GPEDIT.MSC**  
  **Computer Configuration\Administrative Templates\Network\Network Connections\Route all traffic through the internal network > Disable.**  
    
  
* Now All of the Win10 network traffic will be forced through the secure VPN traffic. We’ll check this later.
* O
* P

Part 2: Create Win10 VPN Network Connection to SRV16

In this section of the lab you will create a secure VPN network connection to the SRV16 server.

* Log into the Win10 system with your personal domain administrative account.
* Open the ‘Network’ connections settings and click ‘VPN’ in the left side menu and click ‘Add a VPN connection’  
  
* Configure the VPN connection for the SRV16 server as shown below and click [Save] when finished.  
    
  
* Once done, click ‘**Change adapter options’** in the ‘Related settings’ section.  
    
  
* Right-click on the SRV16-VPN network connection and select ‘Properties’.  
  
* On the ‘Security’ tab ensure the settings for ‘Data encryption: ‘ is set for ‘Optional encryption (connect even if no encryption) and that the ‘Authentication’ is set for ‘Use Extensible Authentication Protocol (EAP) is selected, as shown. Click ‘OK’ when done.  
  
* Return to the VPN network settings page and click the ‘SRV16-VPN’ connection and then click [Connect].



* Once connected to the SRV16-VPN, open a Command Prompt (CMD) and run ‘ipconfig’. You should see the SRV16-VPN connection with an IPv4 Address within the configuration range set on the SRV16 server earlier.  
    
  

Part 3: Verify VPN network traffic

* Open the ‘Network Connections’ control panel and right-click the ‘Ethernet0’ connection and select ‘Status’. Do the same for the SRV16-VPN connection.

Are network traffic bytes being ‘sent’ and ‘received’ across both connections? **YES**

(**YES/NO**)

* What traffic is being sent across the ‘Ethernet0’ connection?

**Internal, un-encrypted packets used for control/management between client/server. No VPN packets.**

* What traffic is being sent across the ‘SRV16-VPN’ connection?

**Packets received by the server, encrypted, and sent to the client. As well as packets sent to the server, encrypted, and routed to the external internet.**