Implementing a Virtual Private Network in Windows

Scenario

You are tasked with configuring a Virtual Private Network solution for the sales team at Contoso. You have access to two Windows servers., which will permit you to demonstrate the process. First, you will add Routing and Remote Access functionality and configure the Sales users on the DC1 server. Next, you'll configure an access policy. Finally, you will then test the VPN connection.

Objectives

This activity is designed to test your understanding of and ability to apply content examples in the following CompTIA Security+ objectives:

- 3.3 Given a scenario, implement secure network designs.

Lab

- DC1 VM
- WS1 VM
- pfSense VM

Task 1

Configure the VPN server

Create a new Sales VPN group and add a Sales user. Next, configure the Routing and Remote Access and Network Policy Server roles on DC1.

NOTE: It is not recommended that you configure an Active Directory Domain Controller as a VPN server. DC1 is configured this way in the lab environment for convenience only.

1. On the **DC1** VM, send **CTRL+ALT+DEL**, and then sign in as **CONTOSO\Administrator** with **Pa$$w0rd**.

2. From **Server Manager**, select **Tools > Active Directory Users and Computers**. Browse to the **Users** container.

3. Create a new **Global Security Group** named **Sales VPN**.

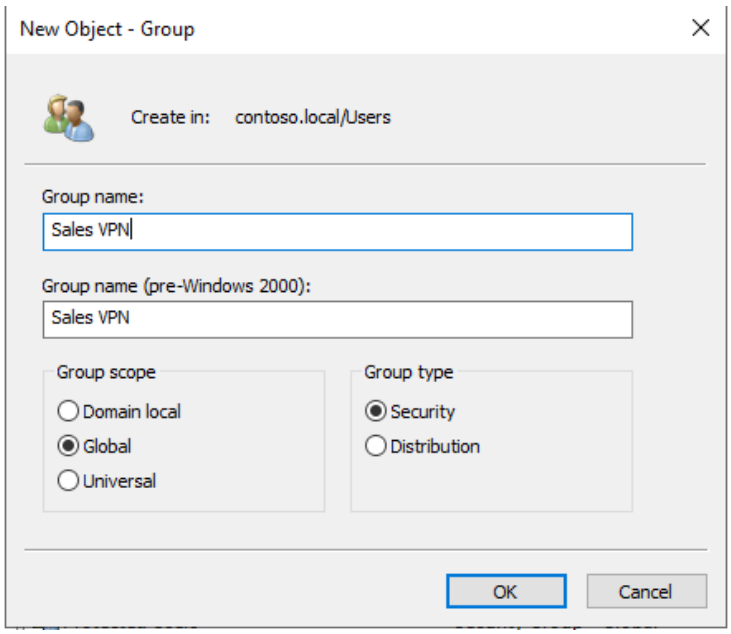

Figure 1.1 – Creating a new Group named Sales VPN.

4. Open the **Sales VPN** group, select the **Member** tab, and then add **Steve Logan** to the **Sales VPN** group.

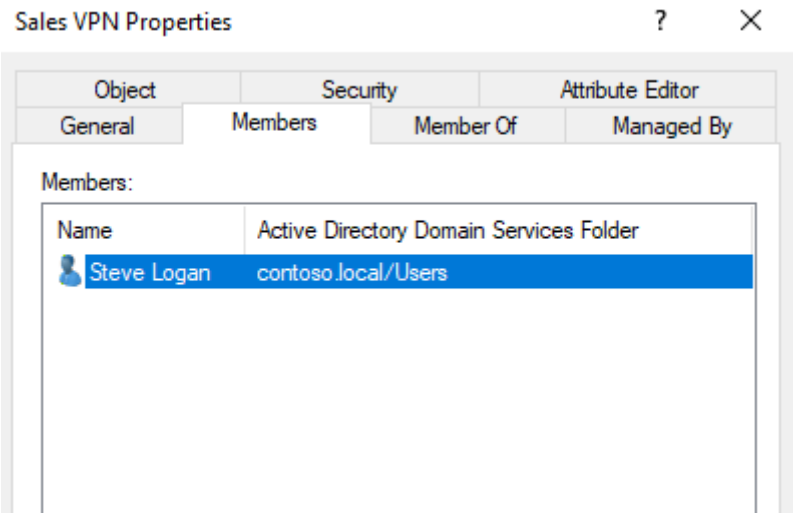

Figure 1.2 – Steve Logan as Member of the Sales VPN group.

5. **Close** Active Directory Users and Computers after adding **Steve Logan** to the **Sales VPN** group.

6. From **Server Manager**, select **Tools > Routing and Remote Access**.

7. Right-click **DC1 (local)** and then select **Configure and Enable Routing and Remote Access**. Select **Next** to start the wizard.

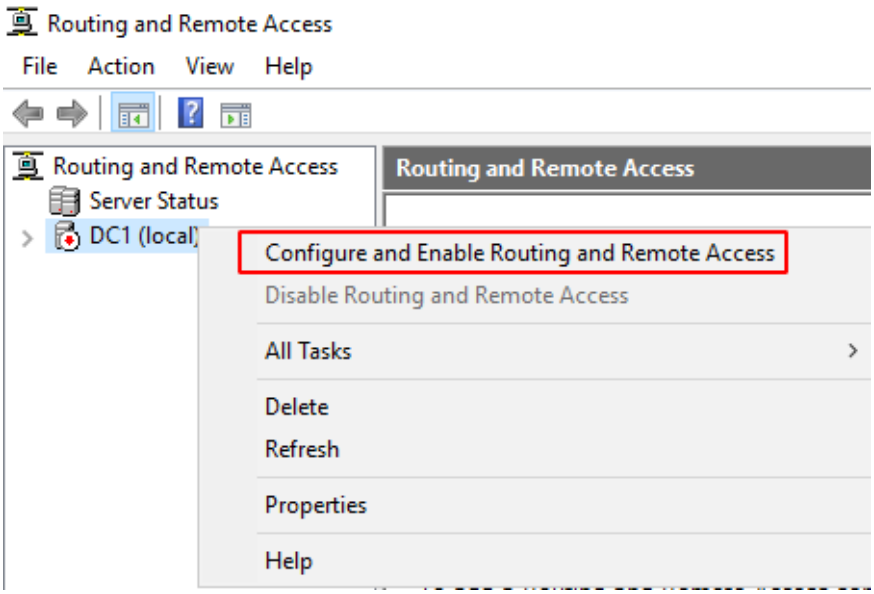

Figure 1.3 – Configure and Enable Routing and Remote Access on DC1.

8. Select **Virtual private network (VPN) access and NAT** and then select **Next**.

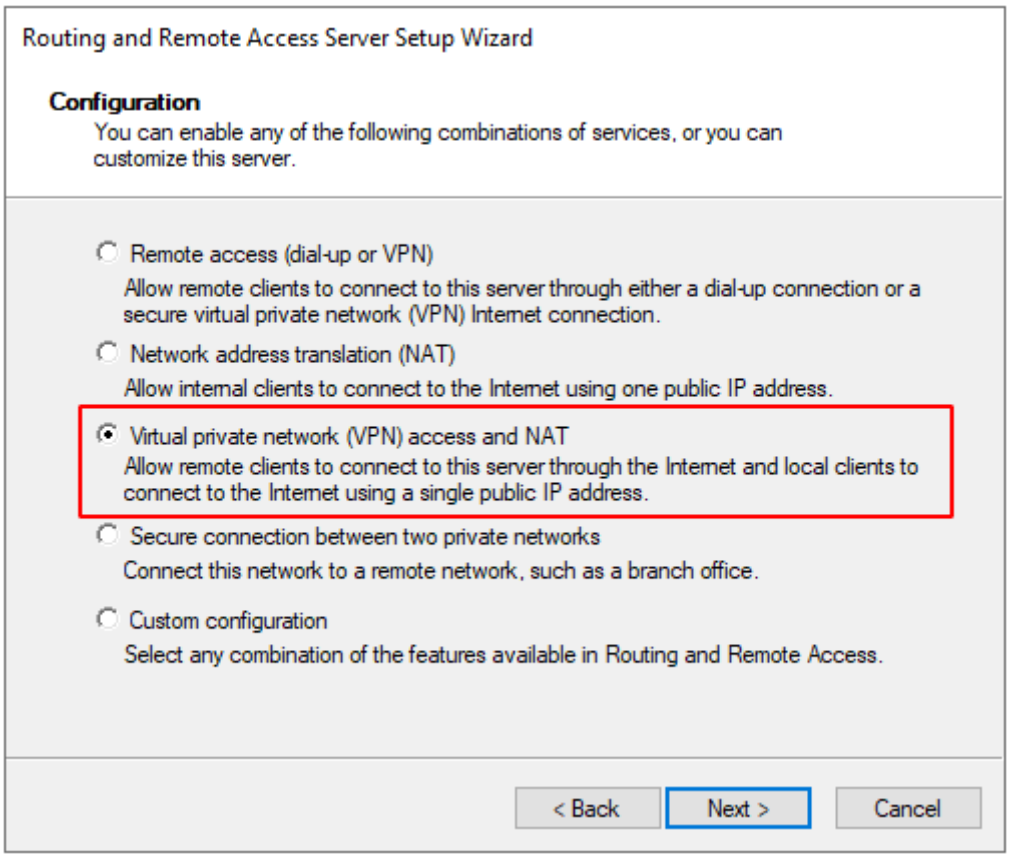

Figure 1.4 – Selecting Virtual Private Network (VPN) on the Configuration section.

9. When prompted select the **INTERNET** interface as the Internet connection.

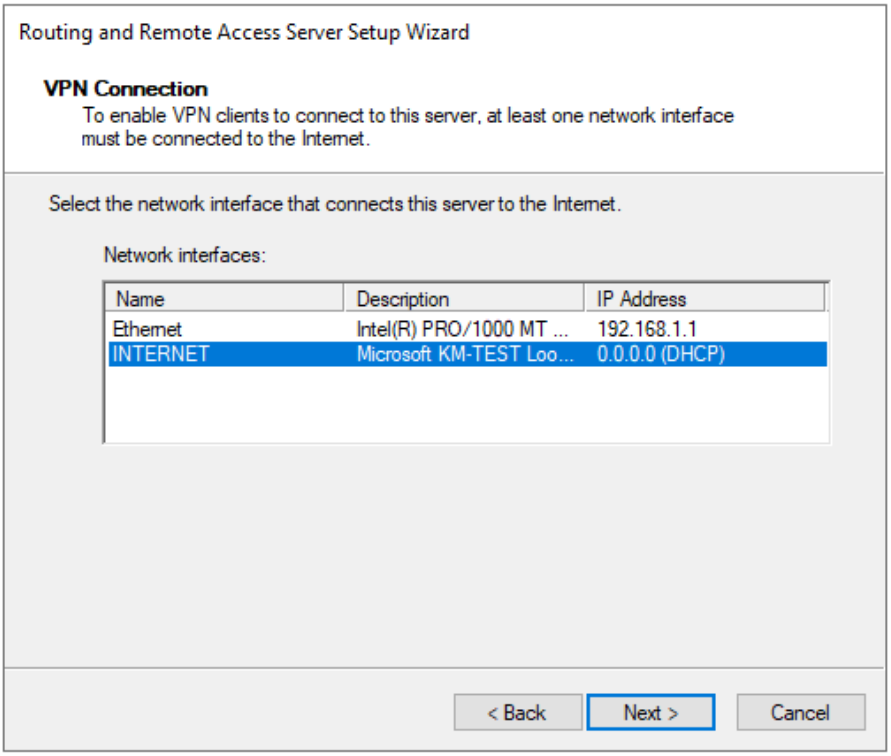

Figure 1.5 – Select the INTERNET interface.

10. Accept all the remaining details choosing their defaults, and then select **Finish**.

11. Acknowledge the policy message, and accept the DHCP message when prompted.

12. When the RRAS service has started, right-click the **DC1 (local)** node, select **Properties**. Select the **Logging** tab.

13. Select the radio button for **Log all events**, and then select **OK** to close the properties box.

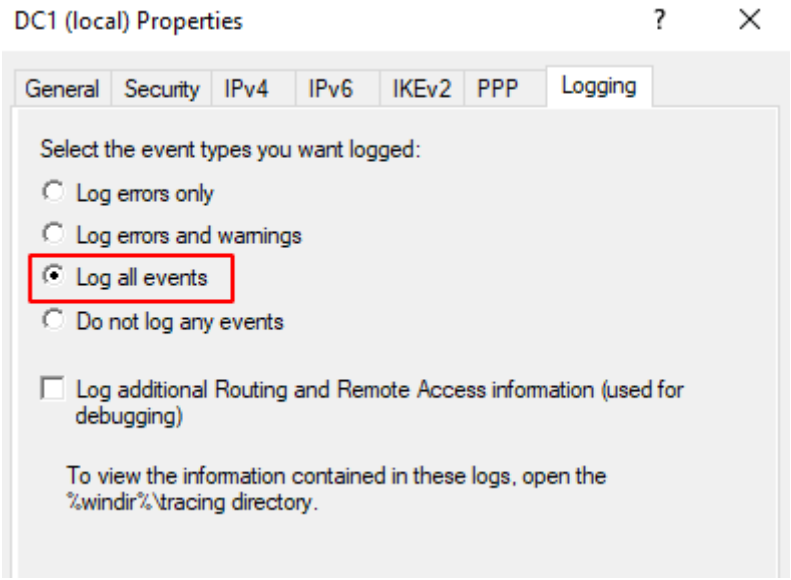

Figure 1.6 – Selecting Log all events in DC1 (local) Properties.

14. Select the **Remote Access Logging & Policies** node, and then right-click it and select **Launch NPS**.

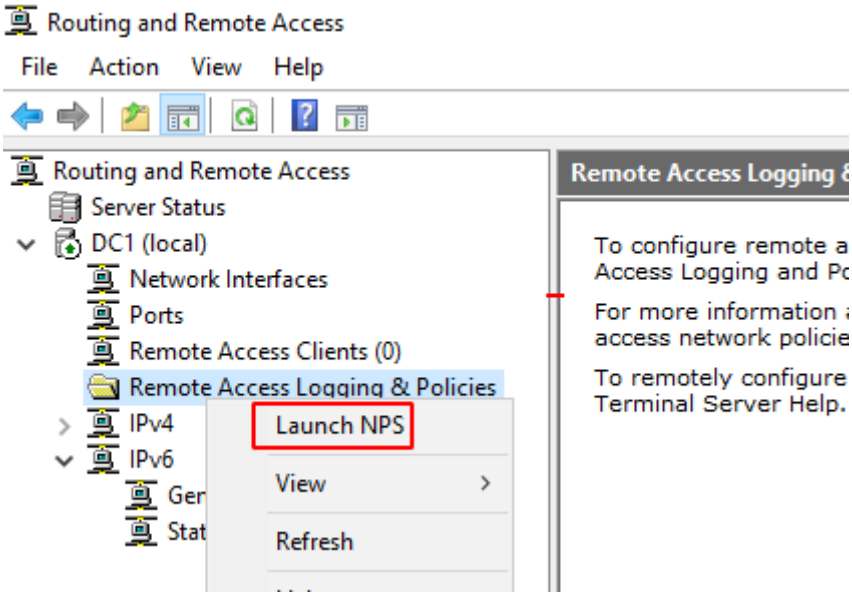

Figure 1.7 – Launching NPS from Remote Access Logging & Policies.

15. In the Network Policy Server console, select the **Network Policies** node.

16. Right-click the **Network Policies** node, and then select **New**. Use the following settings (unless otherwise stated, accept the defaults):

- **Policy name:** Enter **Sales VPN access**
- **Type of network access server:** Select **Remote Access Server (VPN-Dial up)**

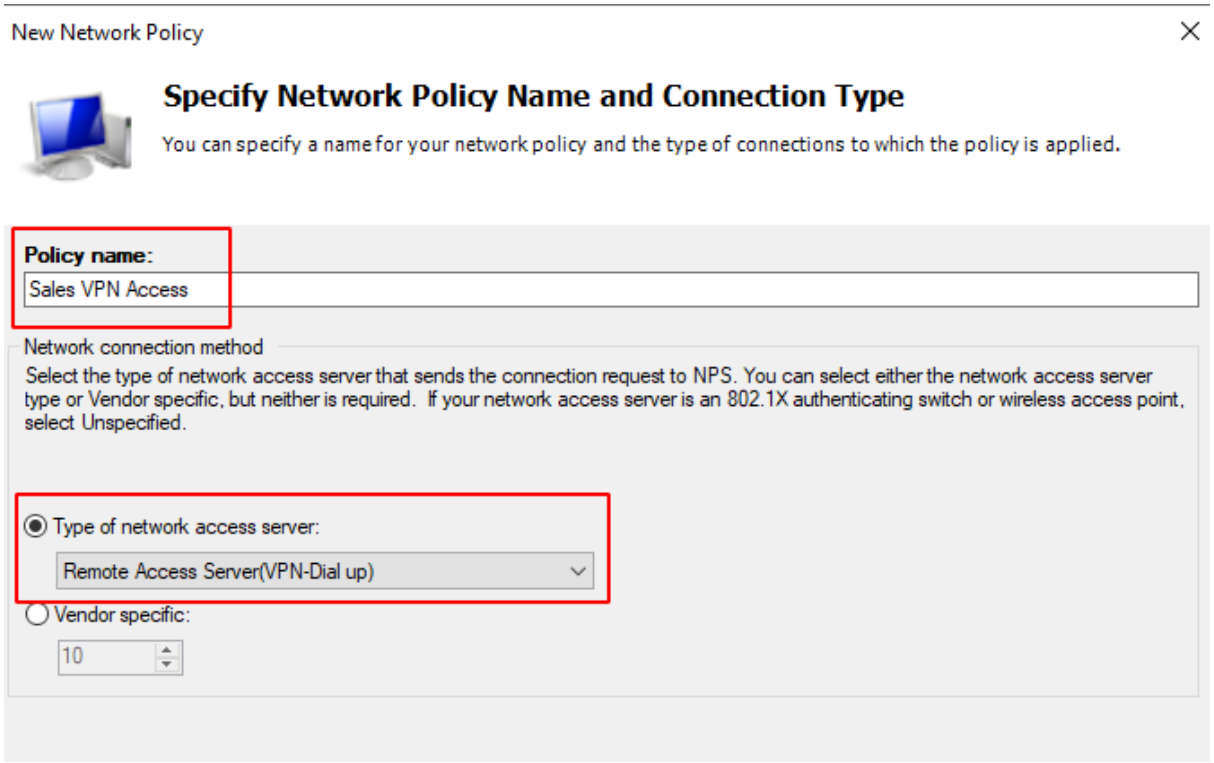

Figure 1.8 – Specifying Policy name and Connection Type.

- **Conditions:** Select **Add** button and **User Groups** and then add the **Sales VPN** group.

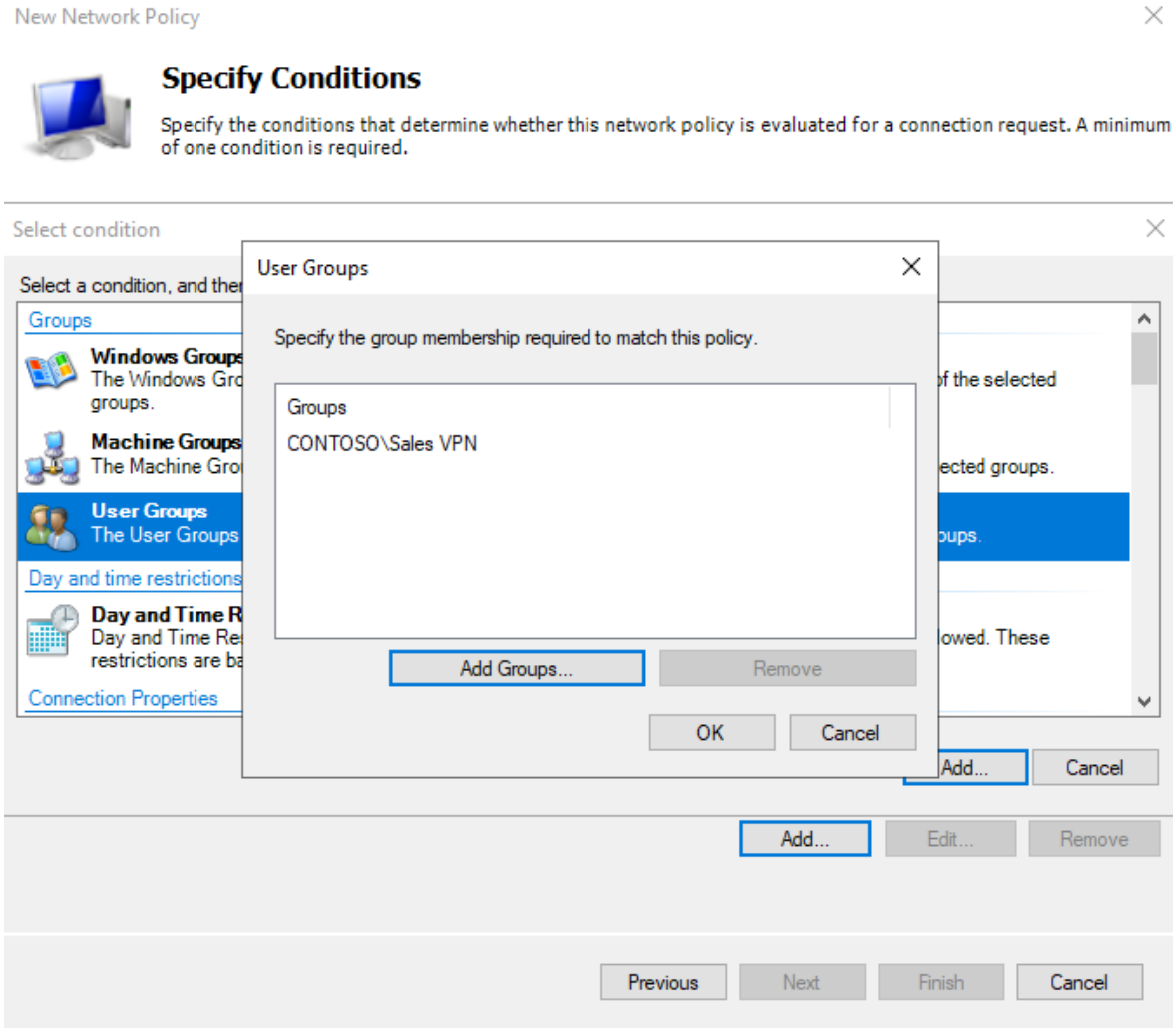

Figure 1.9 – Specify Conditions window.

- **Specify Access Permissions:** Select **Access Granted**
- **Configure Authentication Methods:** Check the box for **Encrypted authentication (CHAP),** and leave the MS-CHAP and MS-CHAPv2 boxes at their default (checked).

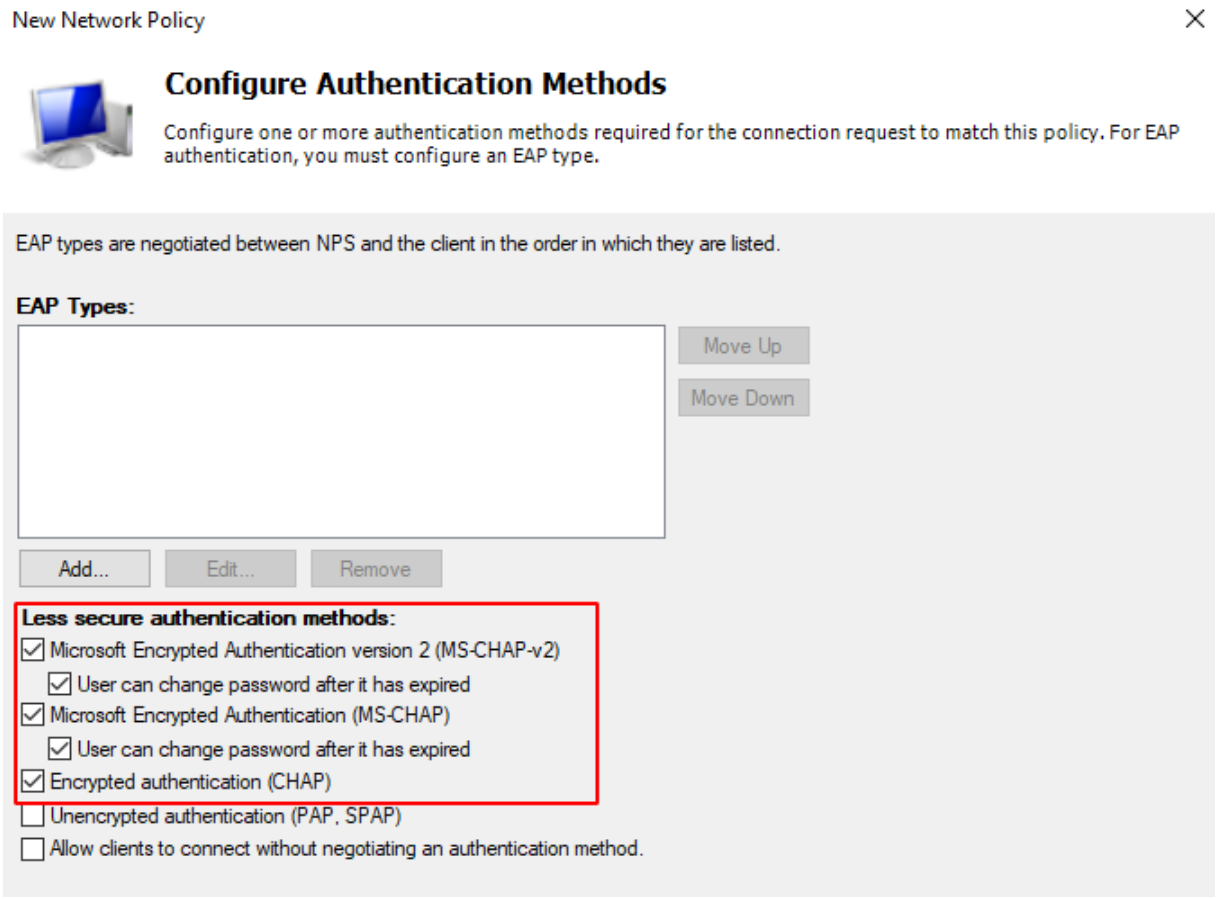

Figure 1.10 – Configure Authentication Methods.

- Select **Next** multiple times until the **Finish** button is available, and then select **Finish**.

17. Observe the new policy in the Network Policies console. Right click the new policy and select Move Up until it is at number 1.

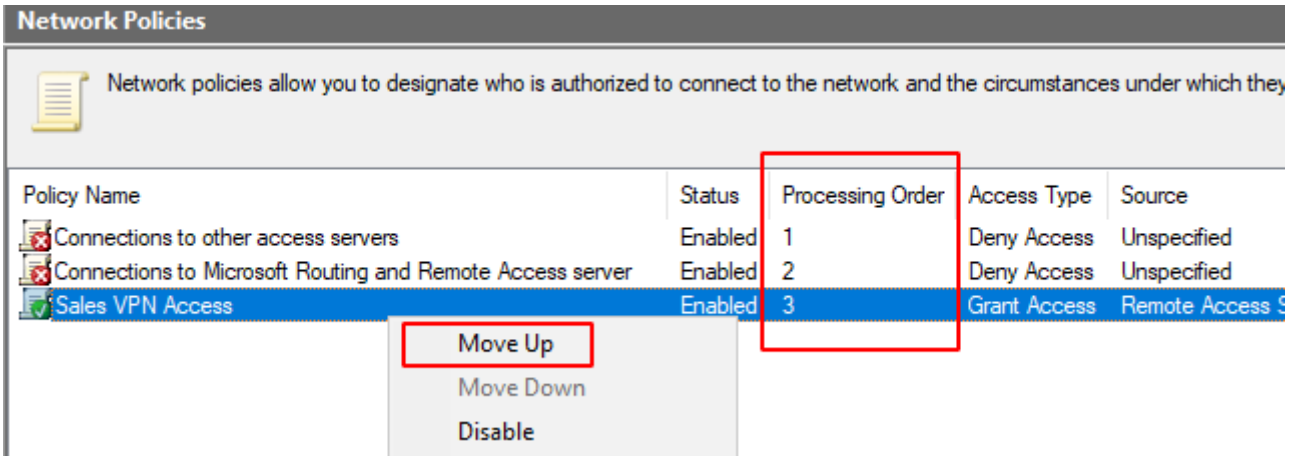

Figure 1.11 – Move Up the new policy.

18. In the NPS console, select **Accounting**, and then select **Configure Accounting**.

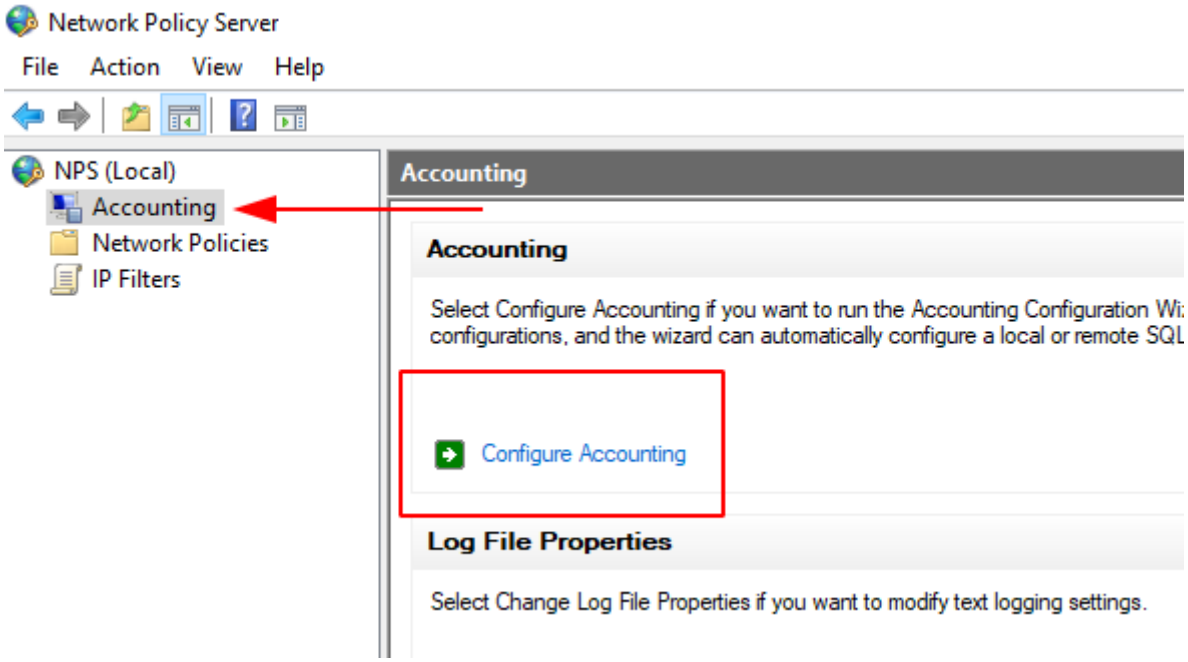

Figure 1.12 – Configuring Accounting.

19. Click **Next**. select **Log to a text file on the local computer**, click **Next**, accept the rest of the defaults, and then complete the configuration.

20. Right-click the **DC1 (local)** node and select **Properties**.

21. Select the **IPv4** tab and click on the **Add** button to add IPv4 Static Address pool of IP.

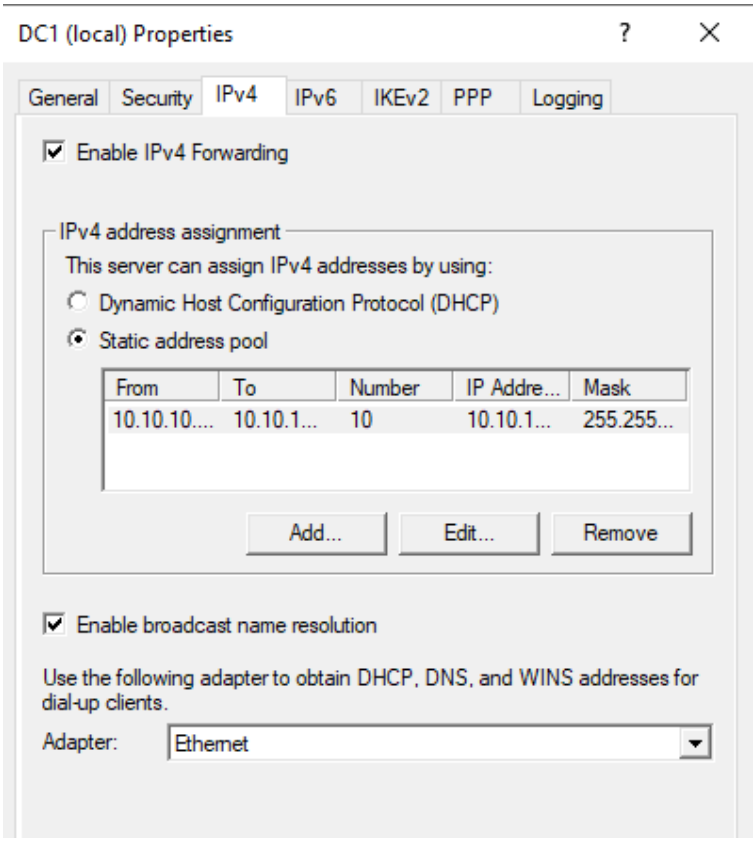

Figure 1.13 – DC1 (local) properties > IPv4.

22. Enter a range from 10.10.10.1 to 10.10.10.19 and click **OK**.

Task 2

Configure the VPN client

You are using the WS1 Client PC to act as the VPN client in this proof of concept scenario. You will configure the VPN connection software and establish the connection by using the Steve Logan user account. You will also evaluate connection information that is displayed on the DC1 VPN Server.

1. Switch to the **WS1** VM, and send **CTRL+ALT+DEL**.

2. Sign in as **steve.logan** , and type **Pa$$w0rd** as the password.

3. On the **Taskbar**, in the **notification area**, click on the **Networks icon**, and then select **Network & Internet settings**.

4. From the Settings pane, select **VPN**, and then select **Add a VPN connection**.

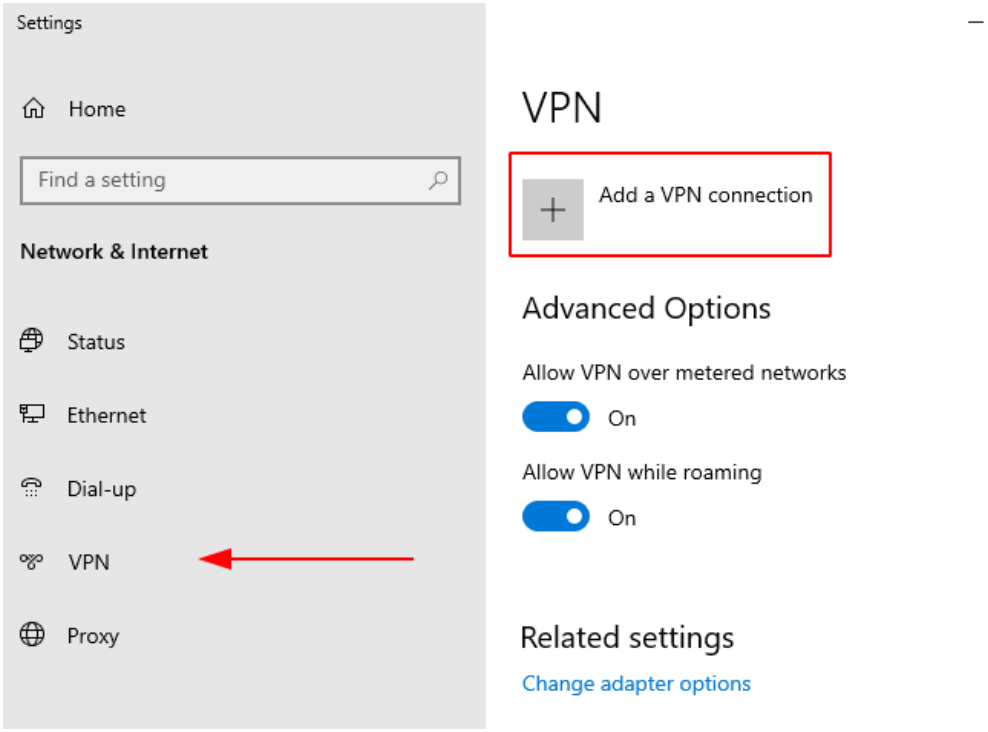

Figure 2.1 – Add a VPN connection.

Configure the following values:

VPN provider: Select **Windows (built-in)**
Connection name: Enter **Sales VPN**
Server name or address: Enter **192.168.1.1**
VPN type: Select **Automatic**
Type of sign-in info: Select **User name and password**
User name (optional): Enter **CONTOSO\Steve.Logan**
Password (optional): Pa$$w0rd

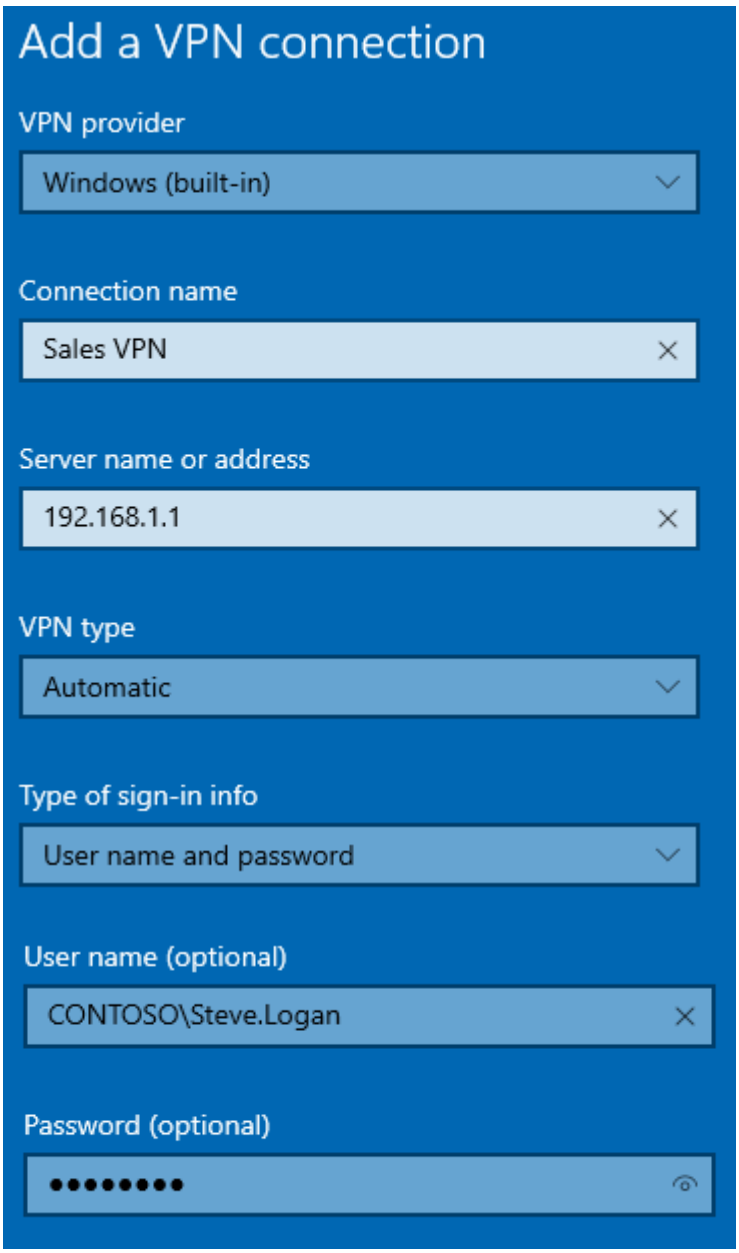

Figure 2.2 – Add VPN Connection settings.

5. When all values are configured, select **Save**.

6. In the Settings windows, scroll down to **Related Settings**, select the link for **Change adapter options**.

7. Right-click the **Sales VPN**, select **Properties**, and then select **Security** tab.

8. Select the radio button for **Allow these protocols**, and then check the boxes for the following:

- Microsoft CHAP version 2 (MS-CHAPv2)
- Automatically use my Windows logon name and password (and domain, if any)

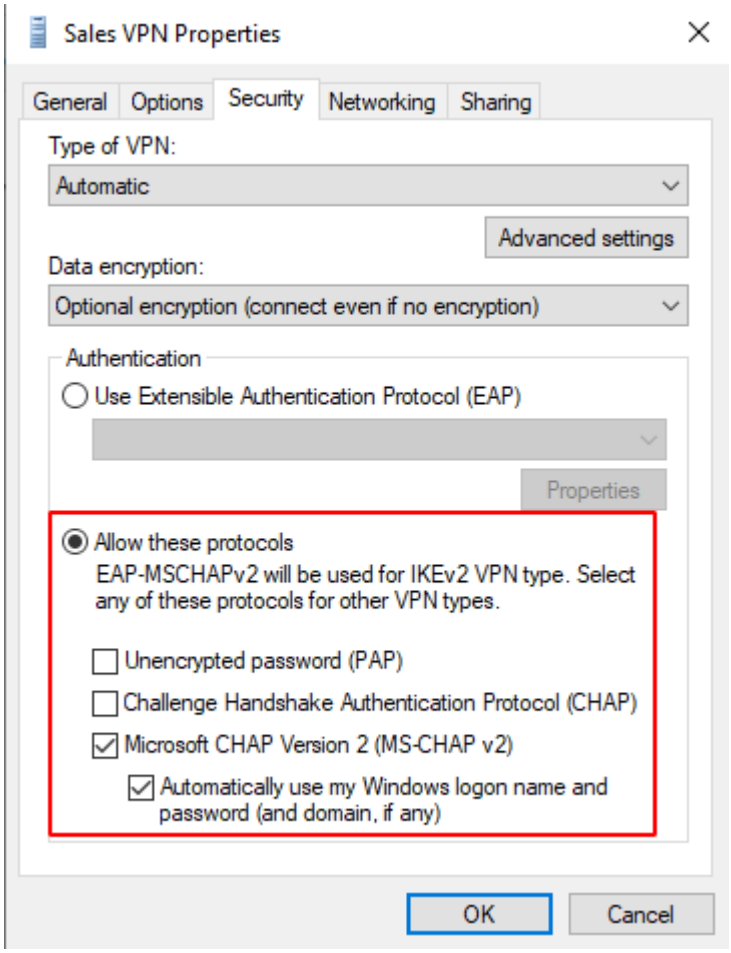

Figure 2.3 – Selecting the protocols under Sales VPN properties.

9. Select **OK**, to close the **Sales VPN** Properties.

10. On the network settings page, select the **Sales VPN** icon, and then select **Connect**.

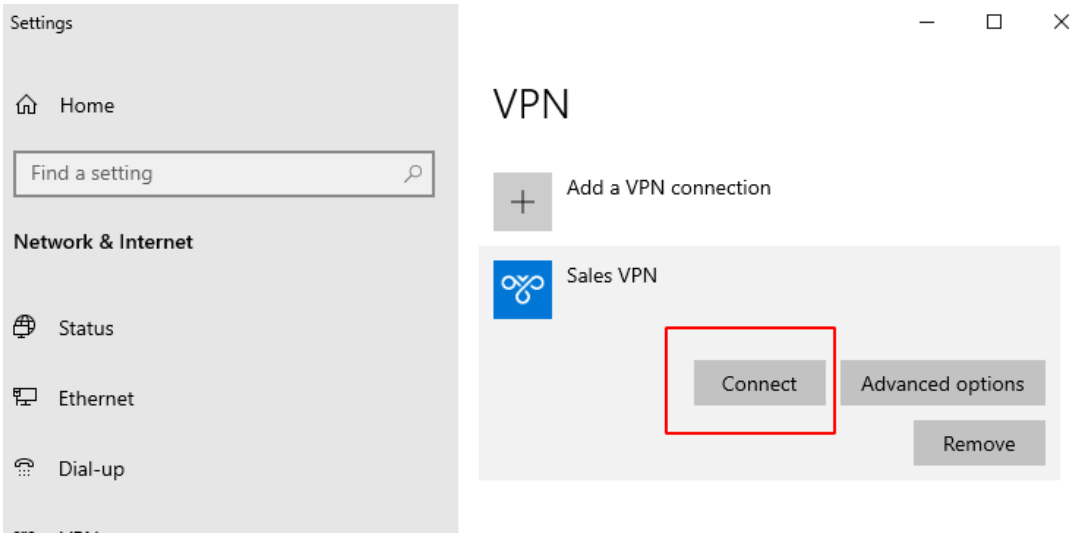

Figure 2.4 – Connecting to the Sales VPN.

The authentication process begins. The connection should display as **Connected**.

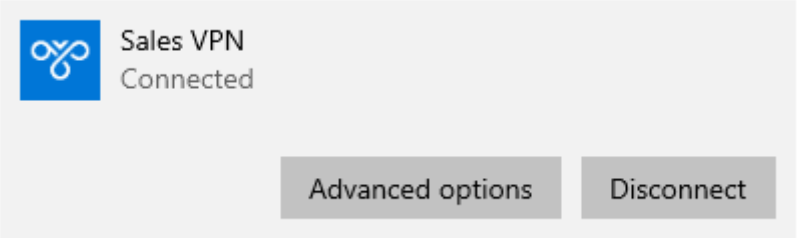

Figure 2.5 – Connected to the Sales VPN.

11. Switch to the **DC1** VM, in the **Routing and Remote Access** console, select the **Remote Access Clients** node.

You will see there's a connection present.

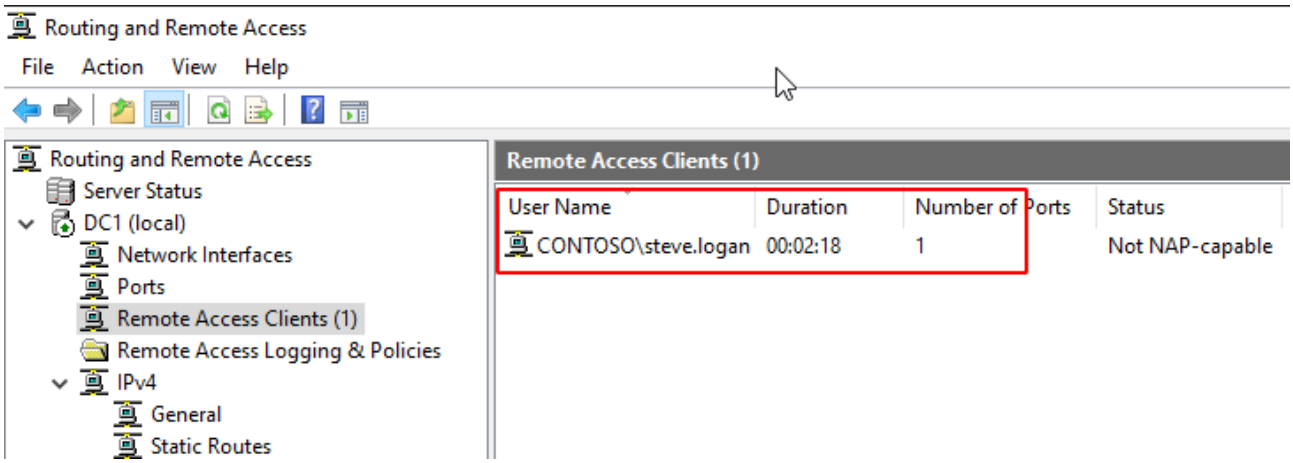

Figure 2.6 – A connection from a VPN Client.

12. Switch to the **WS1** VM, and then select **Disconnect** to end the VPN configuration test.

13. Switch back to the **DC1** VM, and from **Server Manager, select tools > Event Viewer**.

14. Open **System** log.

15. Look for Event ID **20274** (VPN Connection), Event ID **20275** (VPN Disconnection).

16. Close **Event viewer**.