**Module 2: Integrating with Azure virtual networks**

**Lab B: Implementing a point-to-site VPN by using Azure Resource Manager**

**Exercise 1: Preparing a Microsoft Azure subscription for implementing a point-to-site VPN**

**Note:** I have tested this lab on a Windows 10 client without issue. However, when run on a Windows Server 2016 computer with the Active Directory Domain Services added, nothing happens after Exercise 3, Task 2, step 5. The connection is not made.

**Task 1: Create an Azure virtual network**

1. On host computer, start the web browser.
2. In the browser, open the Azure portal at portal.azure.us
3. When prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
4. In the Azure portal, in the hub menu on the left-hand side, click **+Create a resource**.
5. On the **New** blade, click **Networking** and then, click **Virtual network**.
6. On the **Create virtual network** blade, specify the following settings and click **Create**:
   1. Name: **lab2bXX-vnet** (Replace XX with your student number)
   2. Address space: **10.3.0.0/20**
   3. Subscription: select the name of the Azure subscription which you will be using for this lab
   4. Resource group: click **Create new** and type **Lab2bXX-LabRG** as the name of the new resource group
   5. Location: select the name of an Azure region where you have the ability to provision virtual networks, preferably close to the lab location
   6. Subnet: **subnet-0**
   7. Address range: **10.3.0.0/24**
   8. Service endpoints (Preview): **Disabled**
7. Wait until the virtual network is provisioned.

**Task 2: Create the gateway subnet.**

1. On host, in the Azure portal, in the hub menu, click **Virtual networks**.
2. On the **Virtual networks** blade, click **lab2bXX-vnet**.
3. On the **lab2XX-vnet** blade, click **Subnets**.
4. On the **lab2bXX-vnet - Subnets** blade, click **+ Gateway Subnet**.
5. On the **Add subnet** blade, in the **Address range (CIDR block)** textbox, type **10.3.15.224/27** and then click **OK**.

**Result**: After you complete this exercise, you will have successfully used the Azure portal to create a virtual network including the gateway subnet.

**Exercise 2: Configuring point-to-site VPN**

**Task 1: Create the VPN gateway**

1. In the Azure portal, in the hub menu, click **+ Create a resource**.
2. On the **New** blade, click **Networking**, and then click **Virtual network gateway**.
3. On the **Create virtual network gateway**, specify the following settings and click **Create**:
   1. Name: **lab2bXX-gw**
   2. Gateway type: **VPN**
   3. VPN type: **Route-based**
   4. SKU: **VpnGw1**
   5. Enable active-active mode: leave the checkbox cleared
   6. Virtual network: **lab2bXX-vnet**
   7. First IP configuration: click **Create gateway IP configuration**, next, on the **Choose public IP address** blade, click **+ Create new**, on the **Create public IP address** blade, in the **Name** textbox, type **lab2bXX-gw-ip** and press the **Tab** key.
   8. Configure BGP ASN: leave the checkbox cleared
   9. Subscription: the name of your Azure subscription
   10. Resource group: **lab2bXX-LabRG**
   11. Location: the name of an Azure region where you created the virtual network in the previous exercise
4. Do not wait for the gateway to be provisioned but instead proceed to the next task.

**Note:** Provisioning of the VPN gateway can take up to 45 minutes.

**Task 2: Generate the root and client certificates**

1. On host, click **Start**.
2. In the Start menu, right-click **Windows PowerShell ISE**, in the right-click menu, click **More**, and then click **Run as administrator**.
3. In the **Administrator: Windows PowerShell ISE** window, click **File**¸ and then click **Open**.
4. In the **Open** dialog box, browse to (may need to download and create) **Labfiles\Mod02\**, click **New-WINGOVP2SVPNCerts.ps1**, and then click **Open**.
5. Review the content of the script. Note that the purpose of the script is to create two certificates. The first one is a root certificate, which public key you will upload to Azure. The second one is a client certificate that would need to be installed on every VPN client computer. The client certificate references the root certificate.
6. Execute the script by pressing the **F5** key or clicking the **Run Script** toolbar icon.

**Task 3: Export the private key of the client certificate**

1. Right-click the Start button and select Run. In the Run text box, type Certmgr.msc.
2. In the Certificates Microsoft Management Console window, in the **Certificates** subnode of the **Personal** node, right-click **wingovP2SChildCert** and click **All Tasks** in the right-click menu. Next, click **Export** in the **All Tasks** submenu. This will launch **Certificate Export Wizard.**
3. On the **Welcome to the Certificate Export Wizard** page, click **Next**.
4. On the **Export Private Key** page, select the **Yes, export the private key** option, and then click **Next**.
5. On the **Export File Format** page, accept the default options, and then click **Next**.
6. On the **Security** page, select the **Password** check box, type **Pa55w.rd** in both the **Password** and the **Confirm password** boxes, and then click **Next**
7. On the **File to Export** page, in the **File name** box, type **C:\Client1Certificate.pfx**, and then click **Next**.
8. On the **Completing the Certificate Export Wizard** page, click **Finish**.
9. In the **Certificate Export Wizard** dialog box, click **OK**.
10. Switch to the console pane of the **Administrator: Windows PowerShell ISE** window, type the following command, and then press Enter:

Get-Item -Path 'C:\Client1Certificate.pfx'

1. Verify that the file containing the private key of the client certificate has been successfully created.
2. In Certificate Manager,

.

**Note:** Before you proceed to the next task, verify that the VPN gateway has been successfully provisioned.

**Task 4: Configure the Point-to-Site VPN gateway**

1. On the host computer, in the Azure portal, in the hub menu, click **All services** and, in the service menu, locate and click the **Virtual network gateways** entry.
2. On the **Virtual network gateways** blade, click **lab2bXX-gw**.
3. On the **lab2bXX-gw** blade, click **Point-to-site configuration**.
4. On the **lab2bXX-gw - Point-to-site configuration** blade, click **Configure now**.
5. In the **Address pool** text box, type **10.255.255.0/24**.
6. In the **Tunnel type** section, leave the **SSL VPN (SSTP)** checkbox checked, but uncheck the checkbox labeled **IKEv2 VPN**
7. In the **Authentication type** section, ensure that the **Azure certificate** option is selected.
8. In the **Root certificates** section, in the **NAME** text box, type **wingovLabP2SRootCert**
9. To retrieve the root certificate, switch to the console pane of the **Administrator: Windows PowerShell ISE** window, type the following command, and then press Enter:

$rootCerText = Get-ChildItem -Path 'Cert:\CurrentUser\My' | Where-Object {$\_.Subject -eq 'CN=wingovLabP2SRootCert'}

1. To convert the certificate to Base64 format, in the console pane of the **Administrator: Windows PowerShell ISE** window, type the following command, and then press Enter:

$rootCertTextB64 = [System.Convert]::ToBase64String($rootCerText.RawData)

1. To copy the resulting string into Clipboard, in the console pane of the **Administrator: Windows PowerShell ISE** window, type the following command, and then press Enter:

Set-Clipboard -Value $rootCertTextB64

1. Switch to the **lab2bXX-gw - Point-to-site configuration** blade, and, in the **PUBLIC CERTIFICATE DATA** text box, paste the content of Clipboard, and press the **Tab** key.

**Note:** Before saving in step 13 below, make sure the VPN gateway from Task 1 has successfully completed deployment. Click the Bell icon in the menu to be sure.

1. Click **Save** (upper menu bar). The process can take several minutes.

**Result**: After you completed this exercise, you should have successfully created a point-to-site VPN gateway, generated a self-signed root and client certificate, exported the public key of the root certificate, exported the private key of the client certificate, and configured the point-to-site VPN gateway.

**Exercise 3: Testing a point-to-site VPN from an on-premises virtual machine**

**Task 1: Download and install the VPN client configuration package**

1. On the host computer, in the Azure portal, on the **lab2bXX-gw-Point-to-site configuration** blade, click **Download VPN client**.
2. When you receive a prompt asking whether to open or save the **lab2bXX-gw.zip** file, click **Save** and then click **Open folder**. This will open a File Explorer window displaying the **Downloads** folder.
3. Right-click the **lab2bXX-gw.zip** file and, in the right-click menu, click **Extract All**. This will open another File Explorer window displaying the content of the **lab2bXX-gw** folder.
4. In the File Explorer window, navigate to the **WindowsAmd64** folder and double-click **VpnClientSetupAmd64.exe** file.
5. When prompted whether to install a Vpn Client for lab03bXX-vnet, in the **lab2bXX-vnet** dialog box, click **Yes**.
6. Wait for the installation to complete. This should take less than a minute.

**Task 2: Establish a point-to-site VPN from the on-premises virtual machine**

1. On the host computer, click **Start**, and then click **Settings**.
2. In the **Settings** app, click **Network & Internet**.
3. Click **VPN**.
4. Click **lab2bXX-vnet**, and then click **Connect**. This will display a **lab2bXX-vnet** window.
5. In the **lab2bXX-vnet** window, click **Connect**.
6. When you receive a prompt that states **Connection Manager needs elevated privilege to run the following Custom Action(s) to proceed with the connection**, click **Continue**.
7. After you successfully connect, switch to the console pane of the **Administrator: Windows PowerShell ISE** window, type the following command, and then press Enter:

Get-NetIPConfiguration

1. The cmdlet returns the IP configuration of your lab computer. Notice the IPv4 address entry for **lab2bXX-vnet** interface alias. It should contain the IP address from the VPN client IP address pool of **10.255.255.0/24**.
2. Switch to the **Settings** app. On the **VPN** tab, click **lab03bXX-vnet**, and then click **Disconnect**. Close the VPN settings window.

**Task 3: Identify and delete all lab resources.**

1. On the host computer, start Internet Explorer.
2. In the Internet Explorer, browse to the Azure portal at [http://portal.azure.us](http://portal.azure.com/)
3. If prompted, sign in by using the Microsoft account that is the Service Administrator of your Azure subscription.
4. In the hub menu, click **Resource Groups**.
5. On the **Resource groups** blade, click **lab2bXX-LabRG**.
6. On the **lab2bXX-LabRG** blade, click **Delete**.
7. In the **Are you sure you want to delete "lab2bXX-LabRG"?** blade, in the **TYPE THE RESOURCE GROUP NAME** text box, type in the name of the resource group, and then click **Delete**.
8. Close all open windows.

**Result**: After you completed this exercise, you should have successfully downloaded and installed the VPN client configuration package and established a point-to-site VPN from your lab computer.