Networking Lab 8

IPSec VPN site-to-site

Lab Overview

In this lab, we will create a site to site IPSec VPN connection between two virtual networks within Azure. The vnet configuration is as shown in the lab diagram below.

Lab Diagram

A screenshot of a social media post

Description automatically generated

Create a virtual network

From a browser, navigate to the [Azure portal](https://portal.azure.com/) and sign in with your Azure account.

* 1. Click **Create a resource**. In the **Search the marketplace** field, type 'virtual network'. Locate **Virtual network** from the returned list and click to open the **Virtual Network** page.
  2. Click **Create**. This opens the **Create virtual network** page.
  3. On the **Create virtual network** page, configure the VNet settings. Use the following values:
     + **Name**: onprem
     + **Address space**: 10.128.0.0/16
     + **Subscription**: Verify that the subscription listed is the one you want to use. You can change subscriptions by using the drop-down.
     + **Resource group**: rg-lab
     + **Location**: West US 2
     + **Subnet**: onprem-subnet1
     + **Address range**: 10.128.1.0/24

* 1. Leave the rest as defaults and click **Review+Create**.
  2. Click **Create** to create the VNet.

If you don't already have virtual network vnet-hub created, follow steps from lab vnet-peering to add this virtual network.

Create GatewaySubnet

Create a gateway subnet in the virtual network vnet-hub

Create a subnet named GatewaySubnet in virtual network vnet-hub.

* 1. On the Azure portal home page, select **Resource group** > **rg-lab**.
  2. Select the virtual network **vnet-hub**
  3. Select **Subnets** > **+Subnet**.
  4. For **Name**, type **GatewaySubnet**.
  5. For **Address range**, type **10.0.254.0/27**.
  6. Select **OK**.

Create a gateway subnet in the virtual network onprem

Create a subnet named GatewaySubnet in virtual network onprem.

* 1. On the Azure portal home page, select **Resource groups** > **rg-lab**.
  2. Select the virtual network **vnet1**.
  3. Select **Subnets** > **+Subnet**.
  4. For **Name**, type **GatewaySubnet**.
  5. For **Address range**, type **10.128.254.0/27**.
  6. Select **OK**.

Create the VPN gateway

In this step, you create the virtual network gateway for your VNet. Ensure the GatewaySubnet is created as in the step above.

Create a VPN gateway in virtual network **vnet-hub**.

* 1. In the portal, on the left side, click **+ Create a resource** and type 'Virtual Network Gateway' in search. Locate **Virtual network gateway** in the search return and click the entry. On the **Virtual network gateway** page, click **Create**. This opens the **Create virtual network gateway** page.
  2. On the **Create virtual network gateway** page, fill in the values for your virtual network gateway.
     + **Subscription**: Select the subscription you want to use from the dropdown.
     + **Resource Group**: rg-lab
     + **Name:** vnet-hub-vpn-gw
     + **Region:** West US 2
     + **Gateway type**: Select **VPN**.
     + **VPN type**: Route-based
     + **SKU**: **VpnGw1**
     + **Virtual network:** vnet-hub
     + **Gateway subnet address range**:  10.0.254.0/27
     + **Public IP address**: Leave **Create new** selected.
     + **Public IP address name**: vnet-hub-vpngw-ip1
     + **Active-Active mode**: Disabled
     + **Configure BGP ASN:** Enabled
     + **Autonomous System number (ASN):** 65001
     + Click **Review + Create** to run validation.
     + Once validation passes, click **Create** to deploy the VPN gateway.

A gateway can take up to 45 minutes to fully create and deploy. You can see the deployment status on the Overview page for your gateway.

Create a VPN gateway in virtual network **onprem** with the following values:

* 1. **Subscription**: Select the subscription you want to use from the dropdown.
  2. **Resource Group**: rg-lab
  3. **Name:** onprem-vpn-gw
  4. **Region:** West US
  5. **Gateway type**: Select **VPN**.
  6. **VPN type**: Route-based
  7. **SKU**: **VpnGw1**
  8. **Virtual network:** onprem
  9. **Gateway subnet address range**:  10.128.254.0/27
  10. **Public IP address**: Leave **Create new** selected.
  11. **Public IP address name**: onprem-vpngw-ip1
  12. **Active-Active mode**: Disabled
  13. **Configure BGP ASN:** Enabled
  14. **Autonomous system number (ASN):** 65002
  15. Click **Review + Create** to run validation.
  16. Once validation passes, click **Create** to deploy the VPN gateway.

Create the local network gateway

The local network gateway refers to the vpn gateway details of the remote location. For this step, note down the public IP address of the remote vpn gateway, the BGP ASN and the BGP peering IP.

Create local network gateway to configure details of the virtual network vnet-hub.

1. First, let’s get the details on the vnet-hub-vpn-gw.

* Go to the **Virtual network gateway** page. Click on Overview tab and note the Public IP address of the vpn gateway.
* Next, under Settings, click on the **Configuration** tab and note the **BGP peer IP address**.

1. In the portal, click **+Create a resource**.
2. In the search box, type **Local network gateway**, then press **Enter** to search. This will return a list of results. Click **Local network gateway**, then click the **Create** button to open the **Create local network gateway** page.
3. On the **Create local network gateway page**, specify the values for your local network gateway.
   1. **Name:**vnet-hub-local-network-gateway
   2. **IP address:**<vnet-hub-vpn-gw IP address you noted above>
   3. **Address Space 10.0.0.0/16**

Address Space refers to the remote address ranges that will need to be reachable over the VPN tunnel.

* 1. **Configure BGP settings:** Check this box to configure BGP.
  2. **Autonomous system number (ASN):** 65001
  3. **BGP Peer IP address:** <BGP local IP address you noted above>
  4. **Subscription:** Verify that the correct subscription is showing.
  5. **Resource Group:** rg-lab
  6. **Location:** West US 2
  7. When you have finished specifying the values, click the **Create** button at the bottom of the page to create the local network gateway.

 The values should look something like this:

A screenshot of a cell phone

Description automatically generated

Create local network gateway to configure details of the virtual network onprem.

1. First, let’s get the details on the onprem-vpn-gw.

* Go to the **Virtual network gateway** page. Click on Overview tab and note the **Public IP address** of the vpn gateway.
* Next, under Settings, click on the **Configuration** tab and note the **BGP peer IP address.**

1. In the portal, click **+Create a resource**.
2. In the search box, type **Local network gateway**, then press **Enter** to search. Click **Local network gateway** from the search results, then click the **Create** button to open the **Create local network gateway** page.
3. On the **Create local network gateway page**, specify the values for your local network gateway.
   1. **Name: onprem-local-network-gateway**
   2. **IP address: onprem-vpngw-ip1**
   3. **Address Space** 10.254.0.0/16

Address Space refers to the remote address ranges that will need to be reachable over the VPN tunnel.

* 1. **Configure BGP settings:** Check this box to configure BGP.
  2. **Autonomous system number (ASN):** 65002
  3. **BGP Peer IP address:** <BGP local IP address you noted earlier>
  4. **Subscription:** Verify that the correct subscription is showing.
  5. **Resource Group:** rg-lab
  6. **Location:** West US 2
  7. When you have finished specifying the values, click the **Create** button at the bottom of the page to create the local network gateway.

Create VPN Connection

Create the Site-to-Site VPN connection between the two virtual network gateways. These connections will create a VPN tunnel between the two virtual networks.

Go to the Search bar at the top of the Azure portal. Type in *Virtual Network Gateway*. Select **Virtual Network Gateway** from the search results.

From the list of gateways, select gateway **vnet-hub-vpngw**.

Configure the vpn connection as below for gateway **vnet-hub-vpngw:**

.

* 1. On the page for the gateway, click **Connections**. At the top of the Connections page, click **+Add** to open the **Add connection** page.

* 1. On the **Add connection** page, configure the values for your connection.
     + **Name:** vpn-tunnel-vnet-hub-to-onprem
     + **Connection type:** Select **Site-to-site(IPSec)**.
     + **Virtual network gateway:** vnet-hub-vpn-gw
     + **Local network gateway:** Click **Choose a local network gateway.**

Select onprem-local-network-gateway.

* + **Shared Key:** key1234!
  + **IKE protocol:** IKEv2
  + The remaining values for **Subscription**, **Resource Group**, and **Location** are fixed.
  + Click **OK** to create your connection. You'll see *Creating Connection* flash on the screen.
  + You can view the connection in the **Connections** page of the virtual network gateway. The Status will go from *Unknown* to *Connecting*, and then to *Succeeded*.

Next, we will configure a tunnel from onprem gateway side.

From the list of gateways, select gateway **onprem-vpngw**.

Configure the vpn connection as below for gateway onprem-vpngw**:**

.

* 1. On the page for the gateway, click **Connections**. At the top of the Connections page, click **+Add** to open the **Add connection** page.

* 1. On the **Add connection** page, configure the values for your connection.
     + **Name:** vpn-tunnel-onprem-to-vnet-hub
     + **Connection type:** Select **Site-to-site(IPSec)**.
     + **Virtual network gateway:** onprem-vpn-gw
     + **Local network gateway:** Click **Choose a local network gateway.**

Select **vpn-hub-local-network-gateway**.

* + **Shared Key:** key1234!
  + **IKE protocol:** IKEv2
  + The remaining values for **Subscription**, **Resource Group**, and **Location** are fixed.
  + Click **OK** to create your connection.
  + You can view the connection in the **Connections** page of the virtual network gateway. The Status will go from *Unknown* to *Connecting*, and then to *Succeeded*.

Verify the VPN connection

In the Azure portal, you can view the connection status of a Resource Manager VPN Gateway by navigating to the connection. The following steps show one way to navigate to your connection and verify.

* 1. In the [Azure portal](https://portal.azure.com/), click **All resources** and navigate to your virtual network gateway.
  2. On the blade for your virtual network gateway, click **Connections**. You can see the status of each connection.
  3. Click the name of the connection that you want to verify to open **Essentials**. In Essentials, you can view more information about your connection. The **Status** is 'Succeeded' and 'Connected' when you have made a successful connection.

A screenshot of a cell phone

Description automatically generated

Verify the VPN connection

To verify the connection, create a virtual machine in the vnet onprem and verify private connectivity to a virtual machine vnet-hub-vm1 in vnet vnet-hub.

1. Create virtual machine onprem-vm1 in vnet vnet-hub-vm1.

ResourceGroup=rg-lab

VmName=onprem-vm2

VnetName=onprem

SubnetName=onprem-subnet1

AdminUser=azureuser

AdminPassword=Azure123456!

az vm create --resource-group $ResourceGroup --name $VmName --image UbuntuLTS --vnet-name $VnetName --subnet $SubnetName --admin-username $AdminUser --admin-password $AdminPassword

1. Note the public IP address of virtual machine onprem-vm1.
2. Note the private IP address of the virtual machine vnet-hub-vm1.
3. Connect to virtual machine onprem-vm1 using its public IP address.
4. ssh azureuser@<public\_ip\_of\_vm\_onprem-vm1>
5. From the ssh session, ping the private IP address of the virtual machine vnet-hub-vm1.

The ping should be successful.