Networking Lab 8

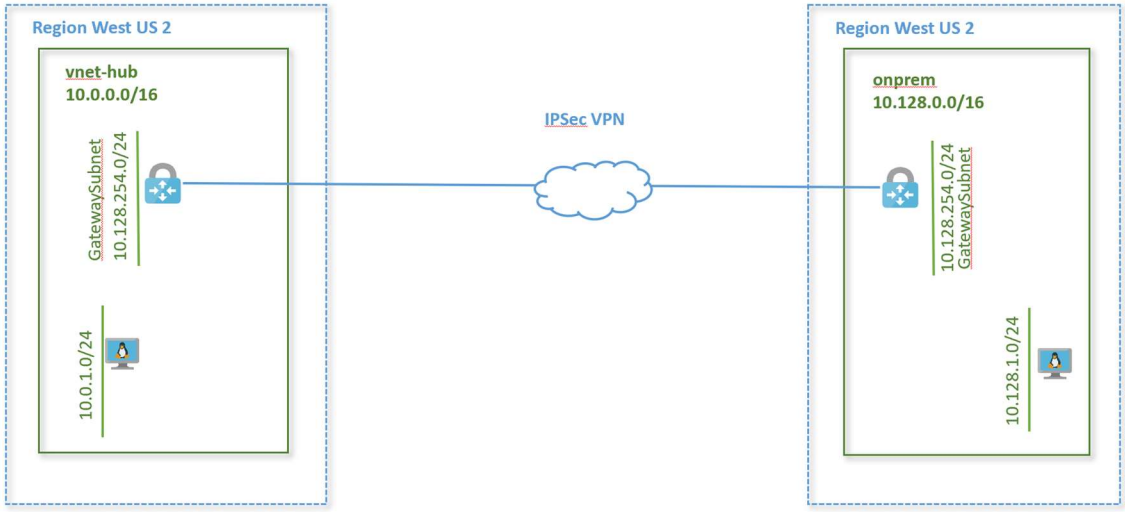
IPSec VPN site-to-site

Author:
Binal Shah
Principal Cloud Solution Architect, Microsoft

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



Create a virtual network using CLI

Open cloud shell window. Cloud Shell icon can be found on the top right of the portal. Define the following variables and run the command to create a virtual network **onprem**.

```
ResourceGroup=rg-lab
VnetName=onprem
VnetPrefix=10.128.0.0/16
SubnetName=onprem-subnet1
SubnetPrefix=10.128.1.0/24
Location=westus2

az network vnet create -g $ResourceGroup -n $VnetName --address-prefix $VnetPrefix --
subnet-name $SubnetName --subnet-prefix $SubnetPrefix -l $Location
```

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

Create GatewaySubnet

Create a gateway subnet in the virtual network vnet-hub

A VPN gateway needs to be deployed in a specific subnet named GatewaySubnet. Create a subnet named GatewaySubnet in virtual network vnet-hub.

1. From Azure portal, go the **Virtual networks** page.
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 **onprem**.
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.

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:

- **Subscription**: Select the subscription you want to use from the dropdown.
- **Resource Group**: rg-lab
- **Name:** onprem-vpn-gw
- **Region:** West US 2
- **Gateway type**: Select **VPN**.
- **VPN type**: Route-based

- **SKU**: **VpnGw1**
- **Virtual network:** onprem
- **Gateway subnet address range**: 10.128.254.0/27
- **Public IP address**: Leave **Create new** selected.
- **Public IP address name**: onprem-vpngw-ip1
- **Active-Active mode**: Disabled
- **Configure BGP ASN:** Enabled
- **Autonomous system number (ASN):** 65002
- Click **Review + Create** to run validation.
- Once validation passes, click **Create** to deploy the VPN gateway.

Create the local network gateway

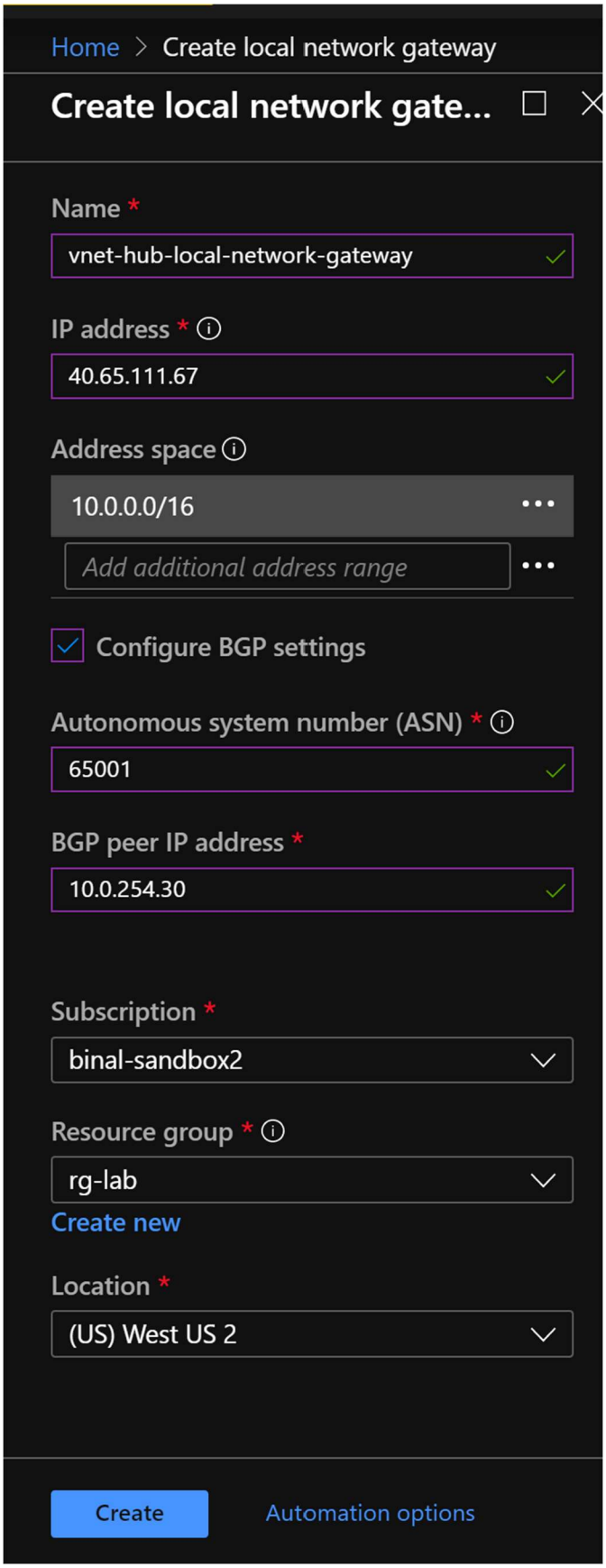
The local network gateway refers to the vpn gateway details of the remote location. For this step, note down the public IP address of the remote vpn gateway, the BGP ASN and the BGP peering IP.

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**.
2. In the portal, click **+Create a resource**.
3. 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.
4. On the **Create local network gateway page**, specify the values for your local network gateway.
   - **Name:** local-network-gateway-vnet-hub
   - **IP address:** <vnet-hub-vpn-gw IP address you noted above>
   - **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.
   - **Configure BGP settings:** Check this box to configure BGP.
   - **Autonomous system number (ASN):** 65001
   - **BGP Peer IP address:** <BGP local IP address you noted above>
     You can find the BGP IP address under **Virtual network gateway → Configuration** page
   - **Subscription:** Verify that the correct subscription is showing.
   - **Resource Group:** rg-lab
   - **Location:** West US 2

4. 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:


Home > Create local network gateway
Create local network gate...
Name *
vnet-hub-local-network-gateway
IP address *
40.65.111.67
Address space
10.0.0.0/16
Add additional address range
Configure BGP settings
Autonomous system number (ASN) *
65001
BGP peer IP address *
10.0.254.30
Subscription *
binal-sandbox2
Resource group *
rg-lab
Create new
Location *
(US) West US 2
Create
Automation options

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.**
2. In the portal, click **+Create a resource**.
3. 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.
4. On the **Create local network gateway page**, specify the values for your local network gateway.
   - **Name: local-network-gateway-onprem**
   - **IP address: onprem-vpngw-ip1**
   - **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.
   - **Configure BGP settings:** Check this box to configure BGP.
   - **Autonomous system number (ASN):** 65002
   - **BGP Peer IP address:** <BGP local IP address you noted earlier>
   - **Subscription:** Verify that the correct subscription is showing.
   - **Resource Group:** rg-lab
   - **Location:** West US 2
4. 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.

2. 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
    - Keep the rest as defaults.
- Click **OK** to create your connection.

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**:**

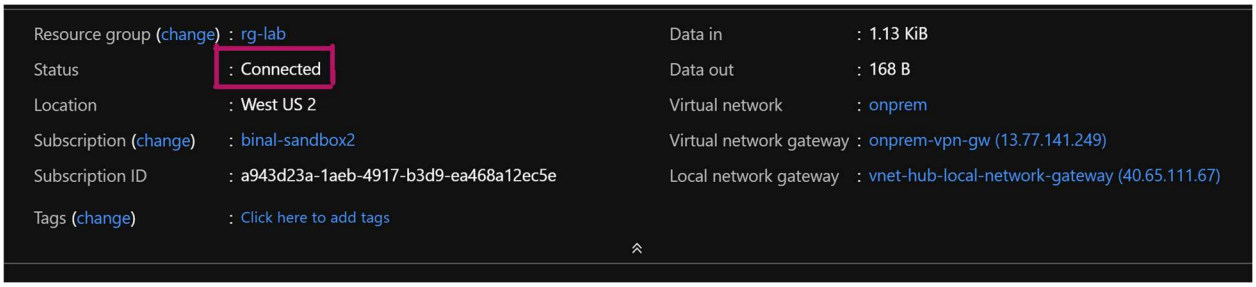
.

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

2. 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*.

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, 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.



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 virtual network onprem.

```
ResourceGroup=rg-lab
VmName=onprem-vm1
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
```

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

The ping should be successful.

We successfully established communication between (simulated) on-premises site and virtual network in Azure using site-to-site VPN.

VPN Gateway Transit with hub and spoke topology

From our previous lab on virtual network peering, we had established peering relationship between virtual networks vnet-hub and vnet1.

Verify if vnet1 has connectivity to the onpremises network:

1. Connect to virtual machine vnet-hub-vm1.
2. Do ping to the private IP of virtual machine vnet1-vm-mgmt1.
   The pings are not successful.

   azureuser@vnet1-vm1:~$ ping 10.128.1.5
   PING 10.128.1.5 (10.128.1.5) 56(84) bytes of data.
   ^C

   --- 10.128.1.5 ping statistics ---
   9 packets transmitted, 0 received, 100% packet loss, time 8170ms
   azureuser@vnet1-vm1:~$

Enable Gateway transit

We will enable vnet1 to leverage the VPN gateway in the virtual network vnet-hub.

1. From the portal, go to the **Virtual network** page and click on **vnet-hub**.
2. Go to **Peerings** under Settings and click on the peering link configured to vnet1
3. **peer-vnet-hub-to-vnet1**.
4. Check the box for **Allow gateway transit**.
5. Next, go back to the **virtual network** page and click on **vnet1**. This should take you to the **Overview** page for virtual network vnet1.
6. Click on **Peerings** under settings and then click on the peering link **peer-vnet1-to-vnet-hub**.
7. Check the box for **Use remote gateways**.

Verify again if vnet1 has connectivity to the on-premises network:

3. Connect to virtual machine vnet-hub-vm1.
4. Do ping to the private IP of virtual machine vnet1-vm-mgmt1.
   The pings are now successful.

   azureuser@vnet1-vm1:~$ ping 10.128.1.5

   PING 10.128.1.5 (10.128.1.5) 56(84) bytes of data.

64 bytes from 10.128.1.5: icmp_seq=133 ttl=64 time=4.19 ms

64 bytes from 10.128.1.5: icmp_seq=134 ttl=64 time=2.25 ms

We successfully enabled gateway transit to peered networks.

Conclusion

We successfully established communication between (simulated) on-premises site and virtual network in Azure using site-to-site VPN. We also verified gateway transit functionality with peered networks. We saw how to leverage hub and spoke topology and use gateway transit to enable spoke networks to reach on premises network.