Networking Lab 9

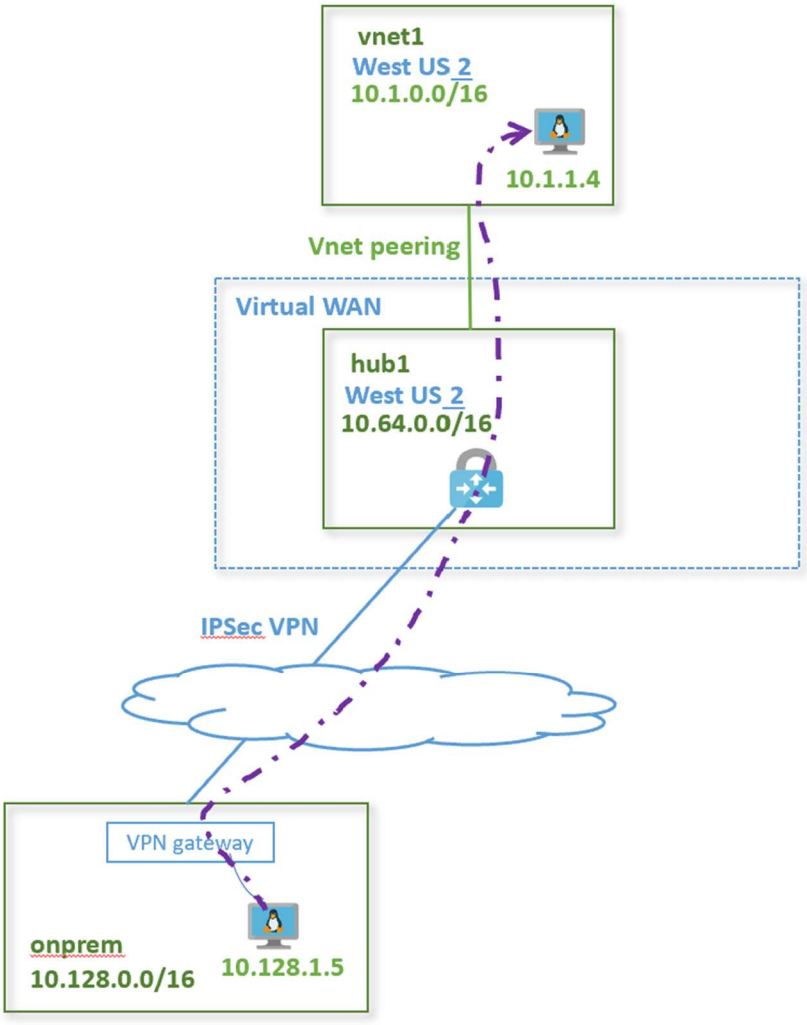
Virtual WAN

Author: Binal Shah

Lab Overview

In this lab, we will learn how to configure virtual WAN in Azure. We will start with connecting one on-premises site to virtual wan and connect to a virtual network through the virtual wan. We will then add an additional hub in another region and connect a branch site in this region.

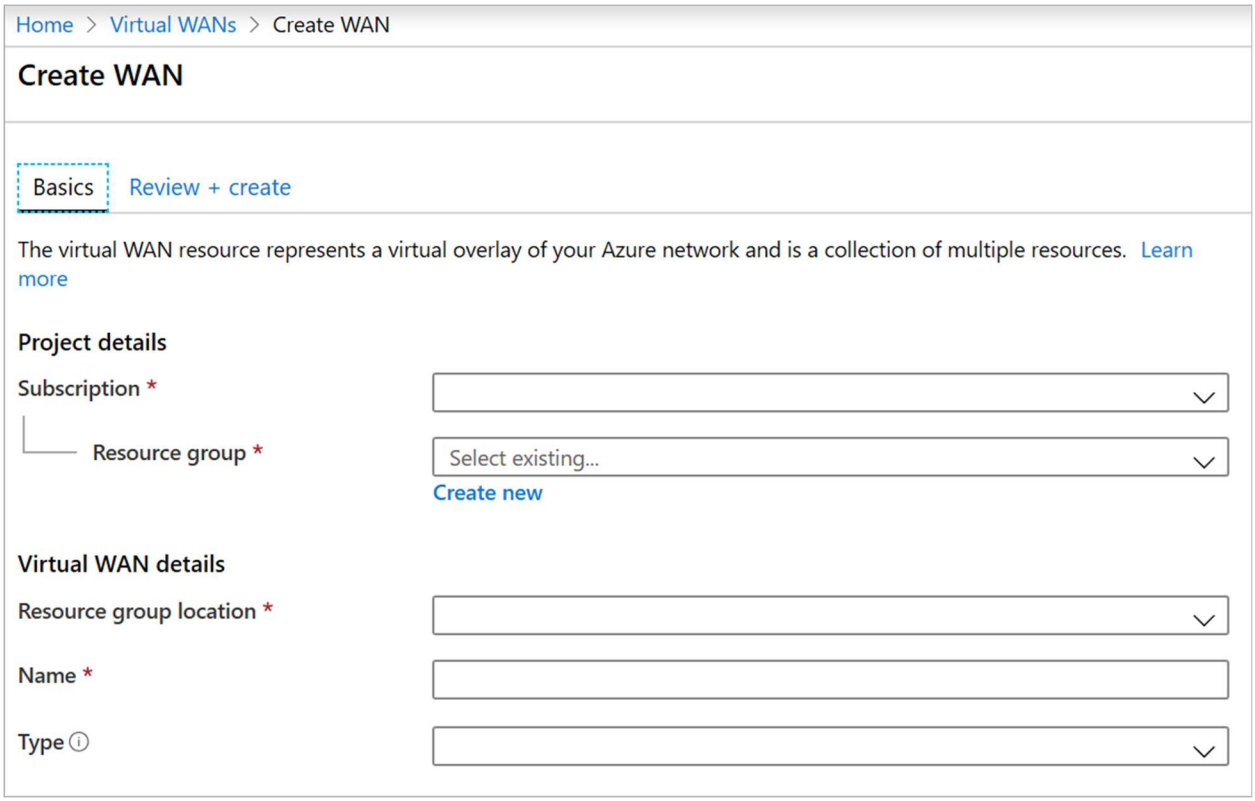
Lab Diagram



Create a virtual WAN

From a browser, navigate to the Azure portal and sign in with your Azure account.

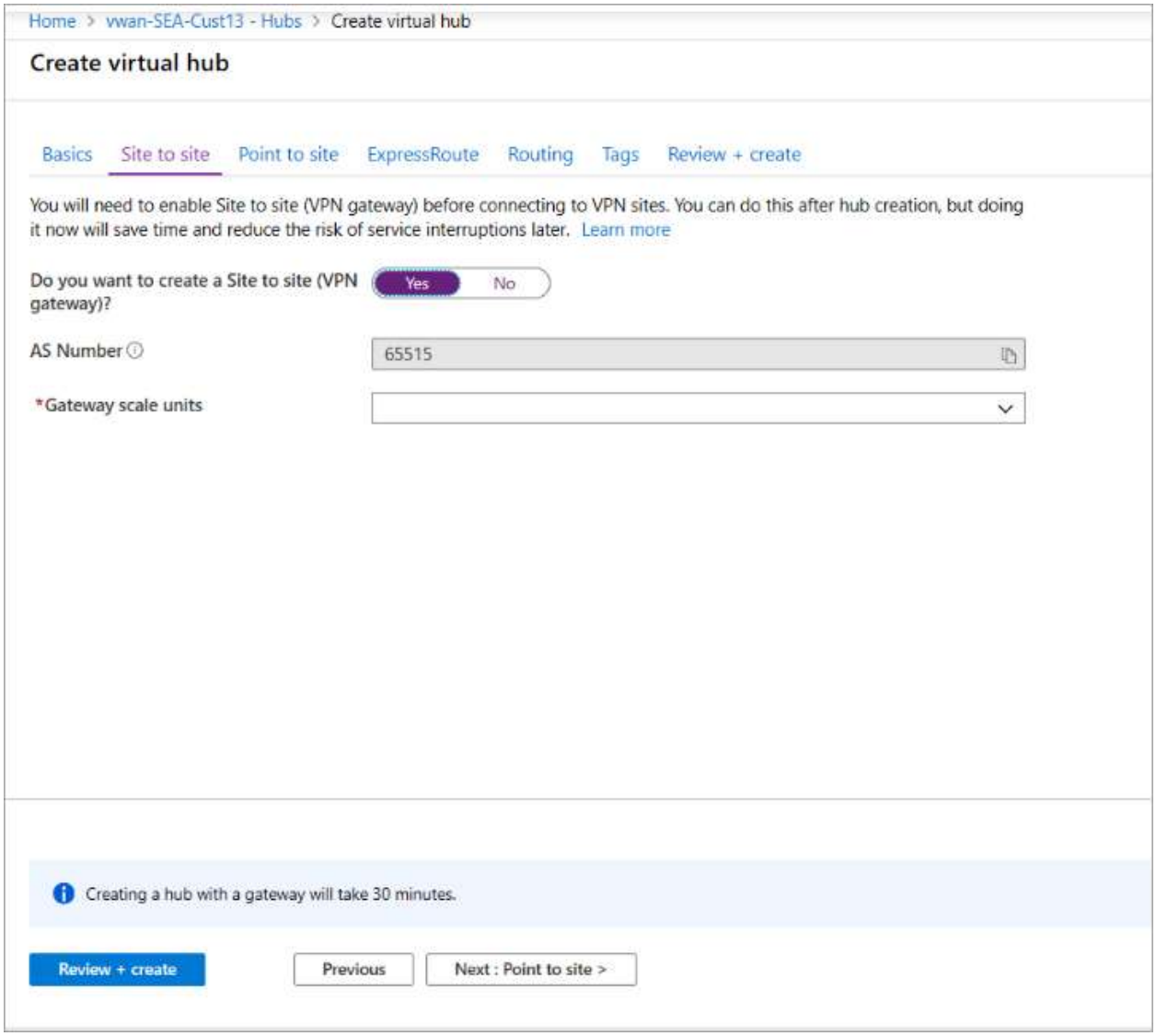
1. Navigate to the Virtual WAN page. In the portal, click **+Create a resource**. Type **Virtual WAN** into the search box and select Enter.
2. Select **Virtual WAN** from the results. On the Virtual WAN page, click **Create virtual WAN** to open the Create WAN page.
3. On the **Create WAN** page, on the **Basics** tab, fill in the following fields:



   - **Subscription** - Select the subscription that you want to use.
   - **Resource group** – Click **Create New** and give a name *rg-vwan*
   - **Resource group location** – West US 2
   - **Name** – vwan1
   - **Type:** Standard
4. After you finish filling out the fields, select **Review +Create**.
5. Once validation passes, select **Create** to create the virtual WAN.

Create a hub

1. Locate the Virtual WAN that you created. On the Virtual WAN page, under the **Connectivity** section, select **Hubs**.
2. On the Hubs page, select **+New Hub** to open the **Create virtual hub** page.
3. On the **Create virtual hub** page **Basics** tab, complete the following fields:
    - Region: West US 2
    - Name: vwan1-hub1
    - Hub private address space: 10.64.0.0/16
4. Select **Next: Site-to-site**.



5. On the **Site-to-site** tab, complete the following fields:
    - Select **Yes** to create a Site-to-site VPN.
    - **AS Number:** 65515
      This field is not editable in the virtual hub at this time.

- **Gateway scale units**: 1 scale unit – 500Mbps x 2

6. Select **Review + Create** to validate.
7. Select **Create** to create the hub.

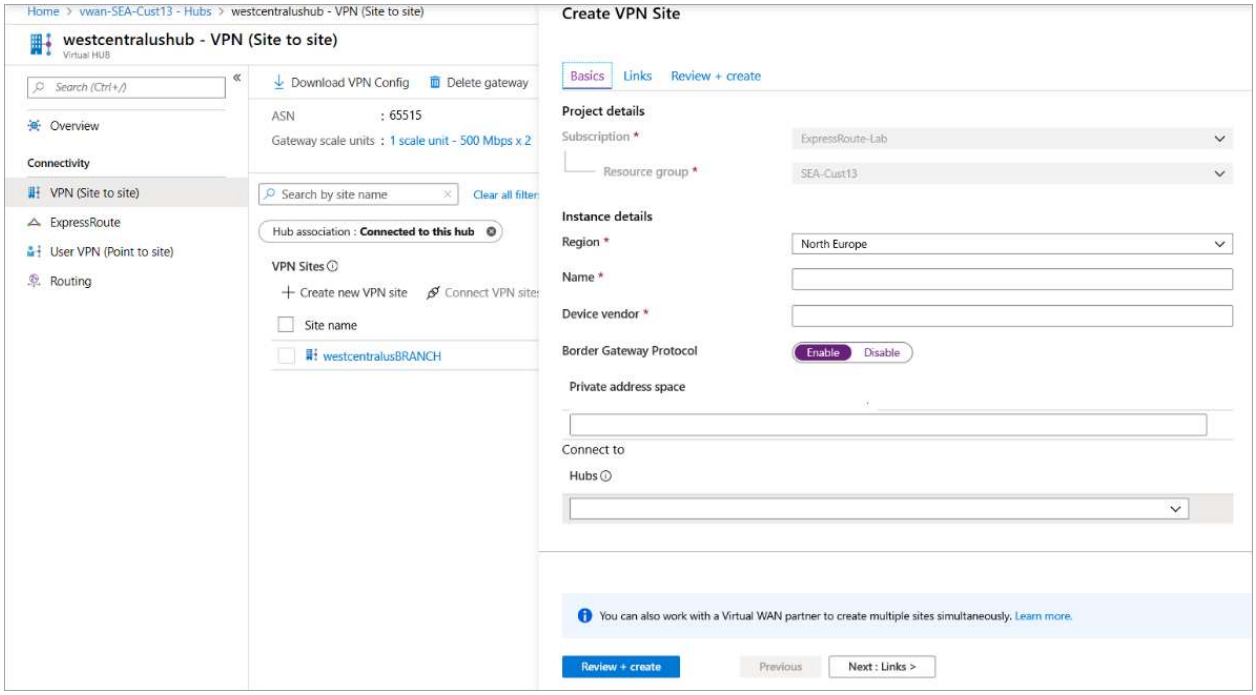
   After 30 minutes, **Refresh** to view the hub on the **Hubs** page. Select **Go to resource** to navigate to the resource.

Create a VPN site

You are now ready to create the sites corresponding to your physical locations.

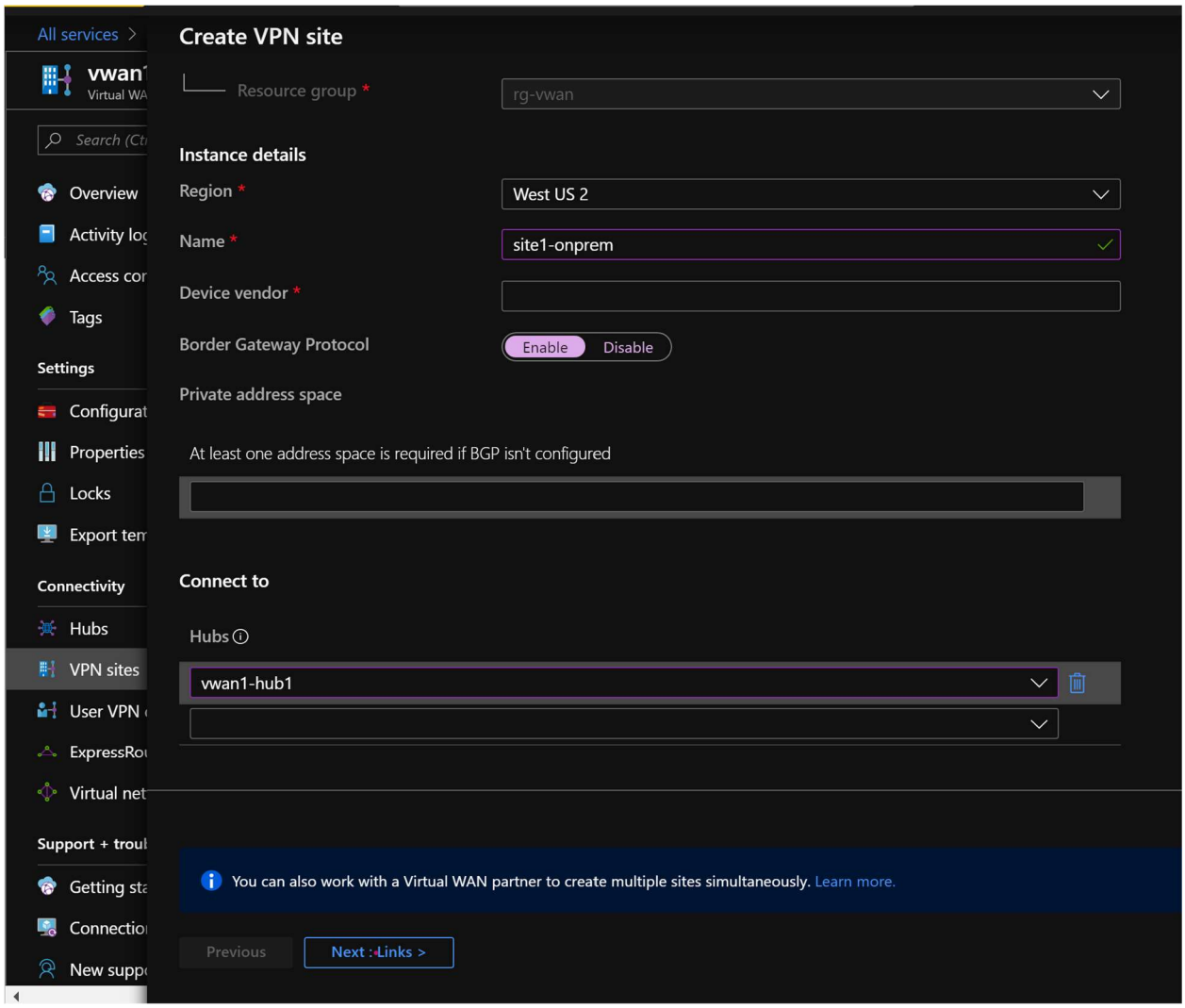
1. On the portal page for your virtual wan, in the **Connectivity** section, select **VPN sites** to open the VPN sites page.

6. On the **VPN sites** page, click **+**Create **site**.



2. On the **Create VPN Site** page, on the **Basics** tab, complete the following fields:
   - **Region** – *West US* .
   - **Name** – *site1-onprem*
   - **Border Gateway Protocol -** Select **Enable**

- **Private address space**: Leave blank since we are enabling BGP.
- **Hubs** - vwan1-hub1



3. Select **Links** to add information about the physical links at the branch.
   - **Link Name** - onprem-link1
   - **Provider Name** - MSN
   - **Speed** - 50
   - **IP Address** - <Public IP address of the onprem-vpngw>

4. Once you have finished filling out the fields, select **Review + create** to verify and create the site.
5. View the status on the VPN sites page. The site will go to **Connection Needed** because the site has not yet been connected to the hub.

Configure VPN connection

In this step, you edit and configure the VPN connection.

1. From the **Virtual WAN** page, go to the **Hubs** option.
2. Select the hub vwan1-hub1-westus2.
3. Go to the **VPN sites** page and find the site site1-onprem.
4. Click on the three dots on the right for the vpn site and click **Edit VPN connection**.
5. Complete the following fields:
    - **Connection name:** Connection-site1-onprem
    - **Border Gateway Protocol:** Enable
    - **Pre-shared key:** key1234!
    - **Protocol:** IKEv2
    - Leave the rest default and click Save.
6. Click Save.
7. In a few minutes, the site will show the connection and connectivity status.

Download VPN configuration

Use the VPN device configuration to configure your on-premises VPN device.

1. On the page for your virtual WAN, go to the **Hub ->VPNSite** page.
2. Click **Download VPN config**. Azure creates a storage account in the resource group 'microsoft-network-[location]', where location is the location of the WAN. After you have applied the configuration to your VPN devices, you can delete this storage account.
3. Once the file has finished creating, you can click the link to download it.
4. Note the following values from the downloaded VPN configuration file:
   Vwan hub's public IP addresses
   Vwan hub's IP address range.
   Vwan hub's BGP peer IP address.
   Vwan hub's ASN#.

Configure the local network gateway on the on-premises side

1. Go to **Local network gateway** page and click **Add**.
   Configure the following value and click create.
   Name: local-network-gateway-vwan1-hub1-westus2

IP Address: <IP address of the vwan hub vpn gateway from vpn config file>
Address space: 10.64.0.0/16
Configure BGP settings: Check the box to enable BGP
Autonomous system number ASN: 65515
BGP Peer IP address: <BGP peer IP address>

Create a vpn connection on on-premises side

1. Click on the newly created **local network gateway**.
2. Click **Connections** and then click **Add**.
3. Configure the following values and then click OK.
   Name: vpn-tunnel-onprem-to-vwan1-hub1-westus2
   Connection Type: Site-to-site VPN
   Virtual Network gateway: onprem-vpngw
   Local network gateway: local-network-gateway-vwan1-hub-westus2
   Shared key (PSK): key1234!
   IKE Protocol: IKEv2

Now that we have vpn tunnel connection created on both sides, the status of the connection should change to Connected.

Connect the VNet to the hub

In this step, you create the connection between your hub and a VNet.

On the page for your virtual WAN, click **Virtual network connections**.

1. On the virtual network connection page, click **+Add connection**.
2. On the **Add connection** page, fill in the following fields:
   - **Connection name** – peer-vwan-hub-westus2-to-vnet1
   - **Hubs** – vwan1-hub1-westus2
   - **Subscription** – Select your subscription
   - **Virtual network** – vnet1
3. Click **OK** to create the virtual network connection.

View your virtual WAN

1. Navigate to the virtual WAN.
2. On the **Overview** page, each point on the map represents a hub. Hover over any point to view the hub health summary, connection status, and bytes in and out.

3. In the Hubs and connections section, you should see the Hub status as Succeeded and the hub should show 1 VPN site connected.
4. Navigate to the **VPN sites**. You should see the status showing as Provisioned.
5. Click on the VPN site you created. Under connected hubs, you should find hub vwan1-hub1-westus2 listed with Connectivity status showing as Connected.

Verify Connectivity branch to vnet through same hub

From virtual machines page, find virtual machine onprem-vm1 and connect to it.

From the shell of this virtual machine, do a ping to the private IP address of the virtual machine vnet1-vm-mgmt1 in the virtual network vnet1. The pings should be successful.

azureuser@onprem-vm2:~$ ping 10.1.1.4

PING 10.1.1.4 (10.1.1.4) 56(84) bytes of data.

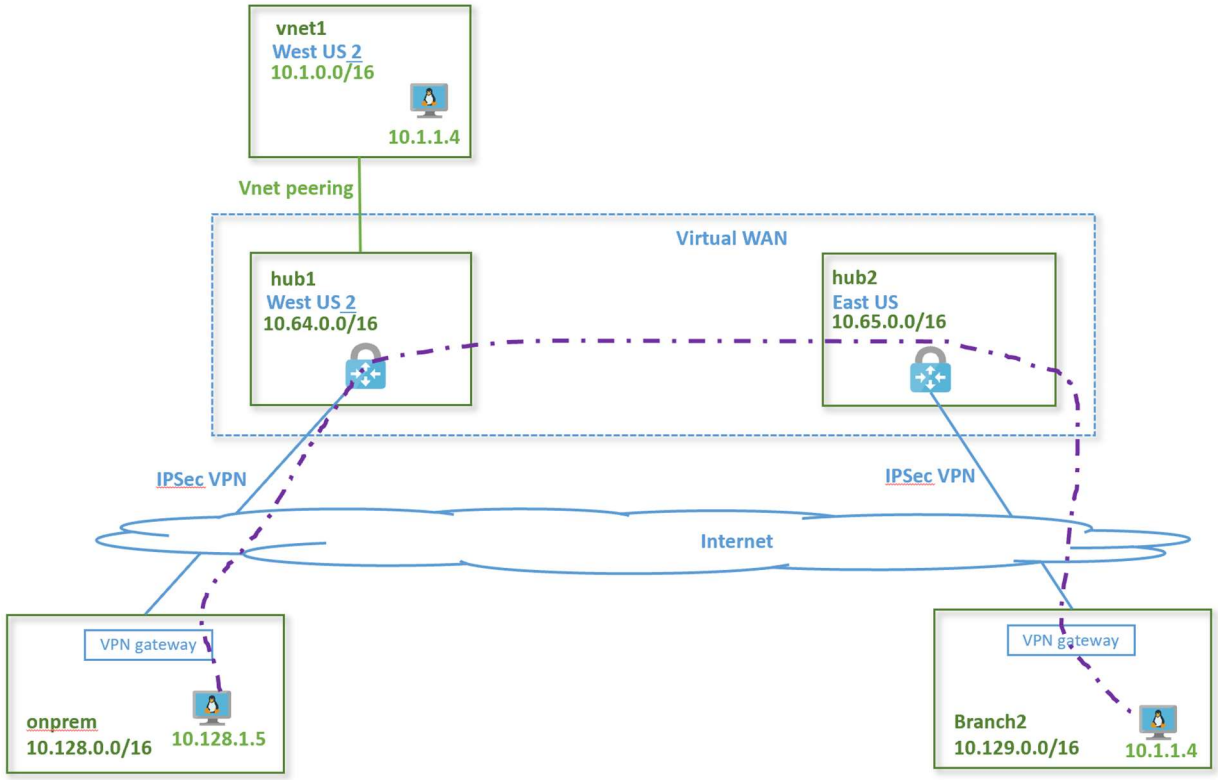
64 bytes from 10.1.1.4: icmp_seq=257 ttl=63 time=3.24 ms

64 bytes from 10.1.1.4: icmp_seq=258 ttl=63 time=2.51 ms

64 bytes from 10.1.1.4: icmp_seq=259 ttl=63 time=3.09 ms

We verified flow from a (simulated) on-premises location to a virtual machine in a virtual network through a virtual wan using VPN site-to-site connection.

Virtual WAN Branch to branch connectivity across hub



Repeat above steps to create a second hub vwan1-hub2-eastus in region East US.

Add a vnet to simulate branch-office2. Add a virtual machine in the vnet branch-office2 and create a VPN connection between branch-office2 and hub vwan1-hub2-eastus.

Verify Connectivity between branches

From **Virtual machines** page, find virtual machine branch-office2-vm1 in (simulated) branch office2 and connect to it.

From the shell of this virtual machine, do a ping to the private IP address of the virtual machine onprem-vm1 in (simulated) on-premise location. The pings should be successful.

azureuser@branch-office2-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=1 ttl=63 time=77.0 ms

64 bytes from 10.128.1.5: icmp_seq=2 ttl=63 time=73.6 ms

^C

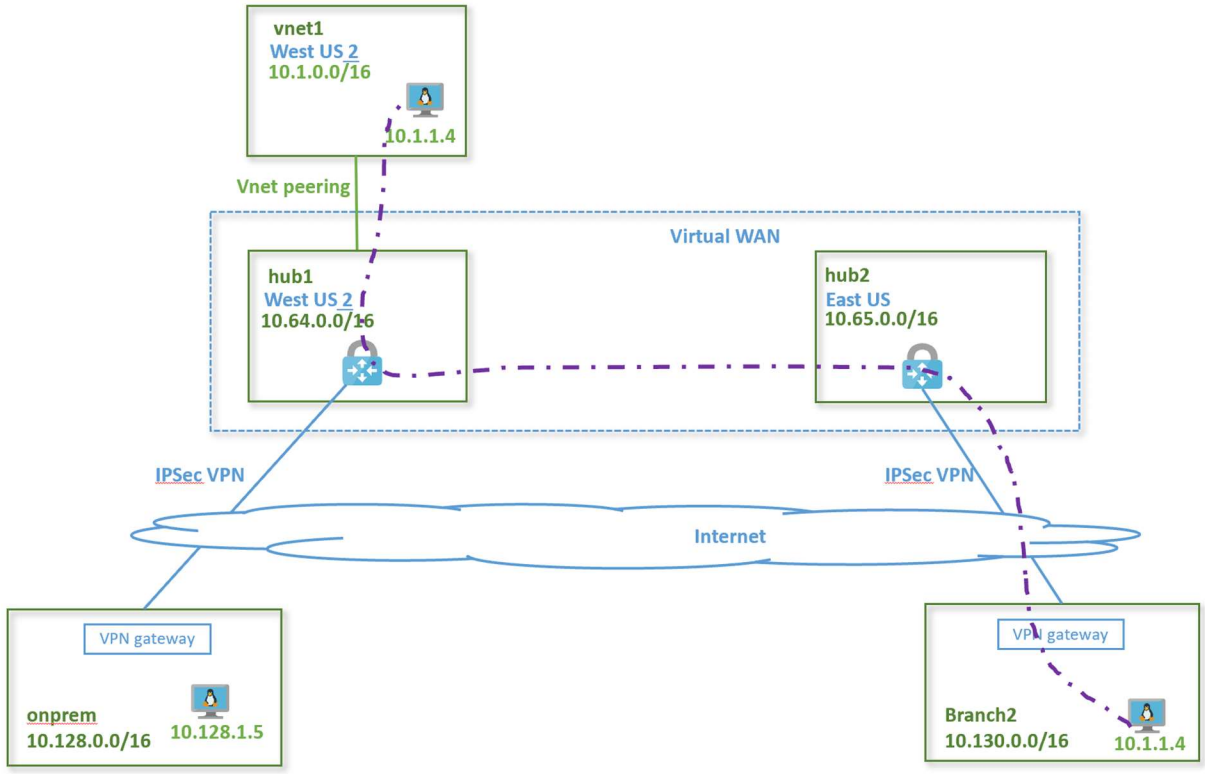
--- 10.128.1.5 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1001ms

rtt min/avg/max/mdev = 73.604/75.313/77.022/1.709 ms

We successfully verified flow from a (simulated) on-premises location to another branch office 2 location connected to the same hub via VPN site-to-site connection.

Verify Connectivity from branch to vnet across hubs



From the shell of this virtual machine, do a ping to the private IP address of the virtual machine vnet1-vm-mgmt1 in the virtual network vnet1. The pings should be successful.

azureuser@branch-office2-vm1:~$ ping 10.1.1.4

PING 10.1.1.4 (10.1.1.4) 56(84) bytes of data.

64 bytes from 10.1.1.4: icmp_seq=1 ttl=62 time=76.2 ms

64 bytes from 10.1.1.4: icmp_seq=2 ttl=62 time=75.2 ms

^C

--- 10.1.1.4 ping statistics ---

2 packets transmitted, 2 received, 0% packet loss, time 1001ms

rtt min/avg/max/mdev = 75.235/75.748/76.261/0.513 ms

azureuser@branch-office2-vm1:~$

We successfully verified flow from a (simulated) on-premises location connected to a virtual wan hub, to a virtual machine in a virtual network connected to a different hub in a different region.