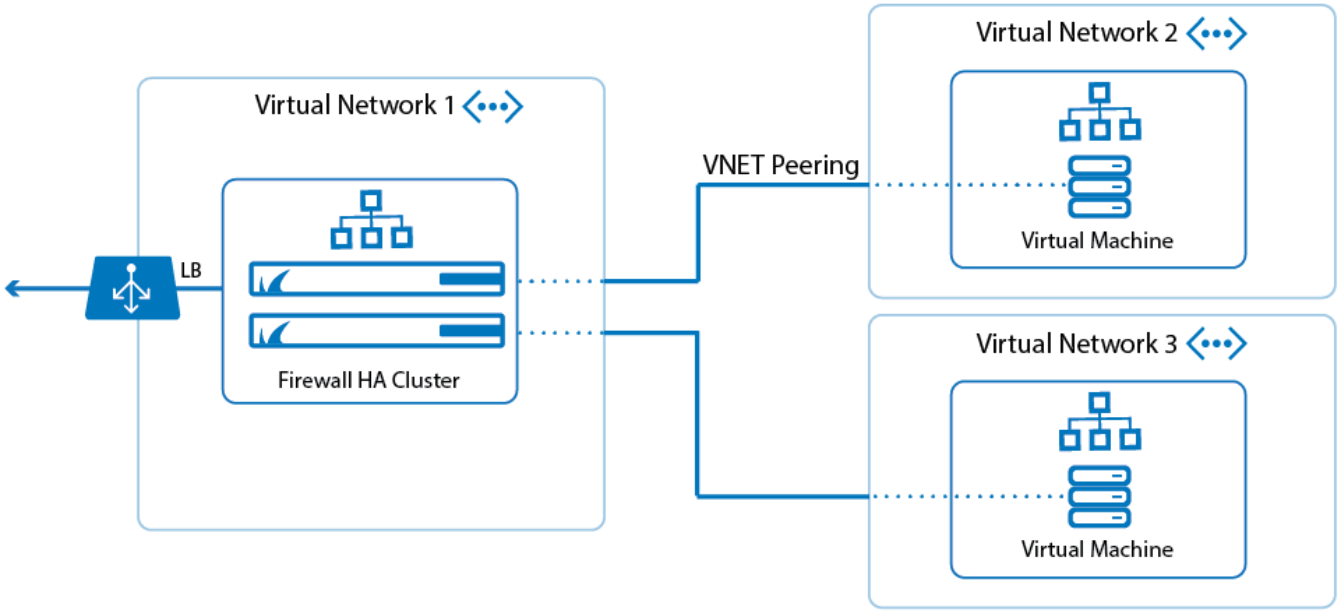
How to Configure VNET Peering with the CloudGen Firewall

https://campus.barracuda.com/doc/79462731/

If you have multiple virtual networks in the same Azure region, you can connect them with a high bandwidth, low-latency connection via virtual network peering. Create a hub and spoke architecture with all spoke VNETs peered to a central VNET containing the CloudGen Firewall VMs. The subnets in the spoke VNETs are associated with an Azure route table using the firewall VM in the central VNET as the next hop device. In this way, all traffic passes through the firewall, thereby allowing you to centrally apply security policies. Using the firewall as the next hop device also allows you to forward traffic between VNETs that are not directly peered with each other. The route table using the firewalls as nexthop routes must be associated with at least one (backend) subnet in the central hub, otherwise the routes will not be rewritten. The hub can contain not only the firewalls, but also additional backend subnets for services shared by all spoke VNETs. By default, you can create up to 10 VNET peerings per virtual network. Contact Microsoft Azure support to increase this limit to up to 50 peerings.



Limitations for VNET Peering with the CloudGen Firewall

- The virtual networks must be in the same Azure region.
- The virtual networks must use the same Azure subscription.
- The virtual networks and route tables must be in the same resource group.
- The networks of the hub VNET and the spoke VNETs may not overlap.
- The Azure route table must be associated with at least one (backend) subnet in the hub VNET for the routes to be updated.
- All virtual networks must use the Azure Resource Manger deployment mode.

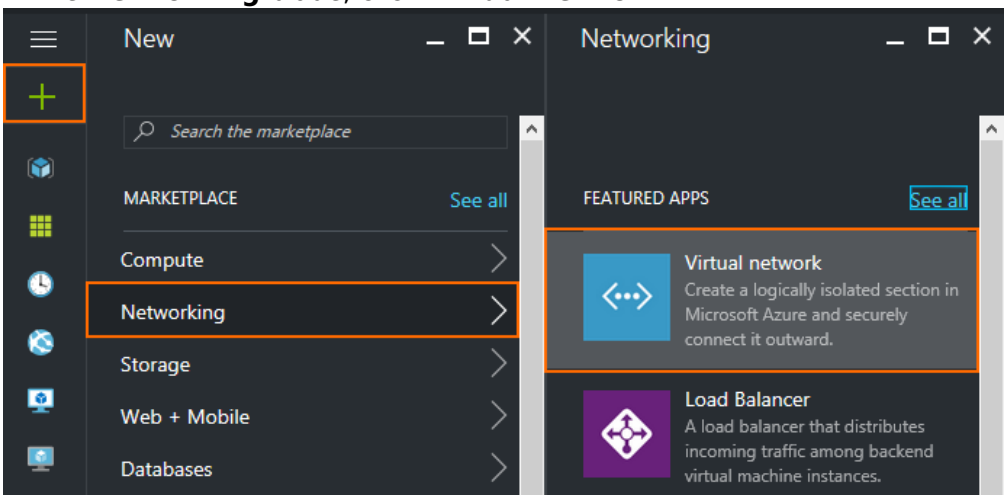
Before You Begin

- Deploy a high availability firewall cluster. This virtual network is used as the hub. For more information, see High Availability in Azure.
- Configure Cloud Integration for the firewall cluster. For more information, see Cloud Integration for Azure.
- Create an Azure route table and user defined routes (UDR). For more information, see How to Configure Azure Route Tables (UDR) using Azure Portal and ARM.

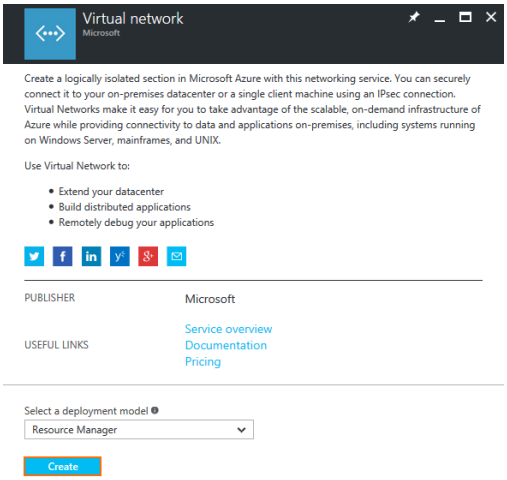
Step 1. Create Spoke Virtual Networks

Create the virtual networks that will be peered to the central virtual network.

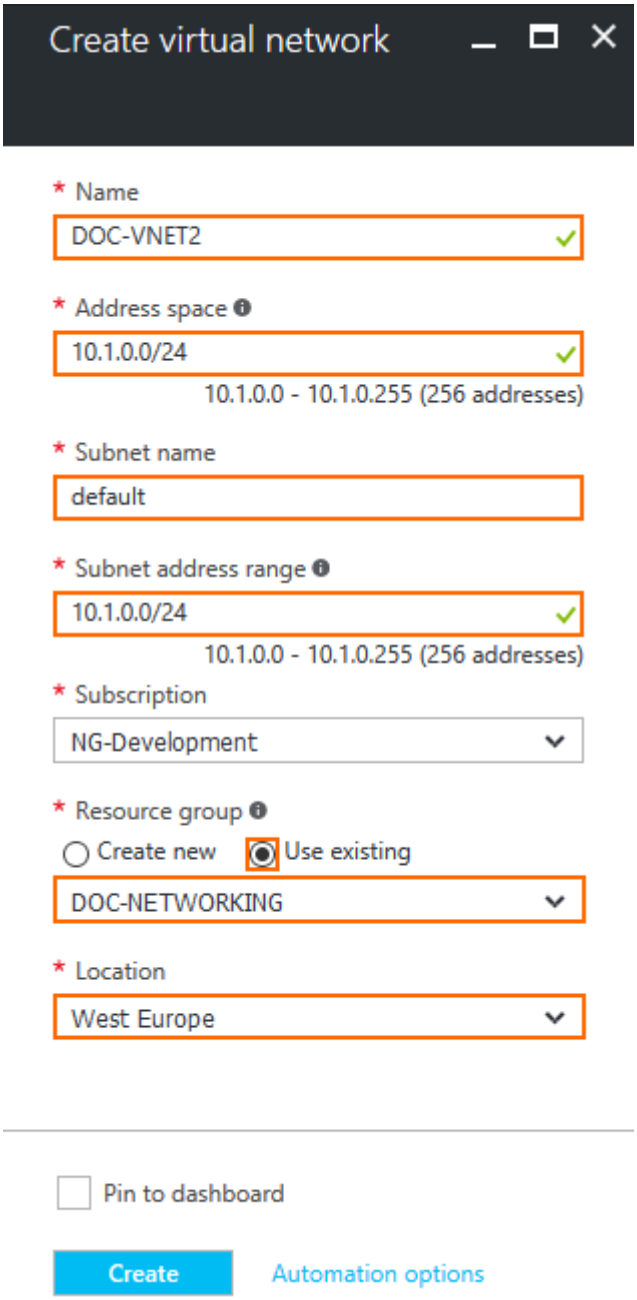
1. Go to the Azure Portal: https://portal.azure.com.
2. In the upper left corner, click **NEW**.
3. In the **NEW** blade, click **Networking**.
4. In the **Networking** blade, click **Virtual network**.



5. In the **Virtual network** blade, select **Resource Manager** from the **deployment model** drop-down list.
6. Click **Create**.



7. In the **Create virtual network** blade, enter:
   - **Name** – Enter a unique name for the virtual network.
   - **Address space** – Use either a large network not overlapping with the other virtual networks, or your on-premises networks.
   - **Subnet name** – Enter a name for the first subnet in the virtual network.
   - **Subnet address range** – Enter the network for the subnet. It must be a subnet of the network entered as the address space.
   - **Subscription** – Select the Azure subscription.
   - **Resource Group** – Click **Select Existing** and select the resource group the hub virtual network is in.
   - **Location** – Select the location the other virtual networks are in.



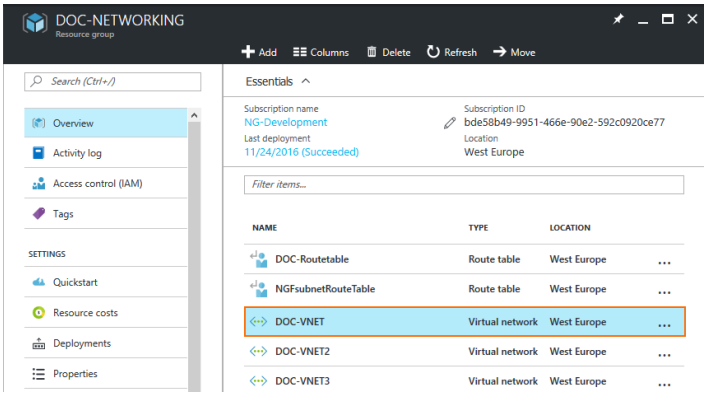
8. Click **Create**.

You now have at least two virtual networks in the same resource group. The route table created for the CloudGen Firewall HA cluster must also be in the same resource group.

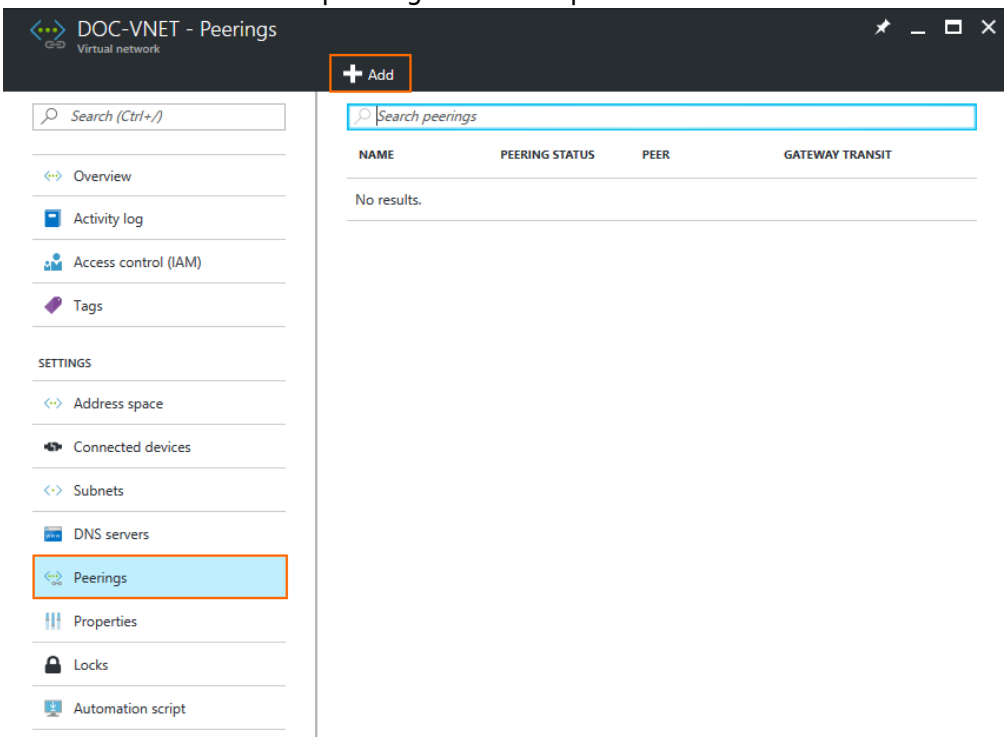
Step 2. Peer Hub Virtual Network with Spoke Virtual Networks

Create the VNET peering between the hub virtual network and the spoke virtual networks. This will initialize, but not yet connect, the VNET peering. Create a VNET peering for every spoke VNET:

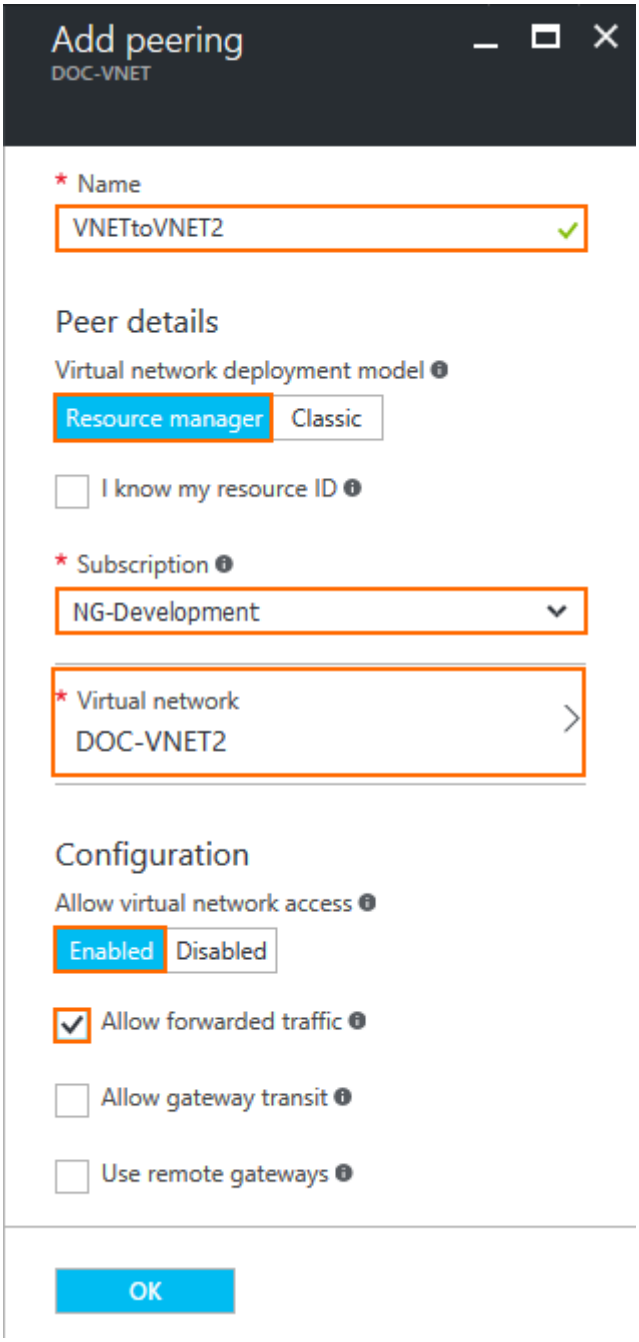
1. Go to the Azure Portal: https://portal.azure.com.
2. Select the resource group containing the virtual networks.
3. Select the Hub VNET.



4. In the left menu of the virtual network blade, select **Peerings**.
5. Click **Add** to add a new peering relationship.

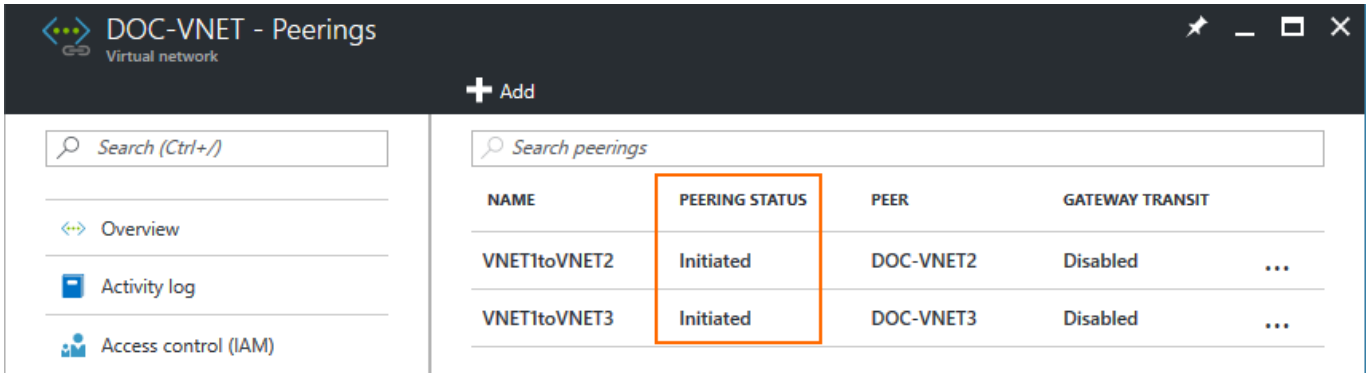


6. In the **Add peering** blade, enter the peering settings:
   - **Name** – Enter a name.
   - **Peer details** – Select **Resource manager**.
   - **Subscription** – Select the Azure subscription.
   - **Virtual network** – Click and select the spoke VNET you want to peer with.
   - **Allow virtual network access** – Select **Enabled** to allow access to the virtual network.
   - **Allow forward traffic** – Enable to allow virtual machines to forward traffic



7. Click **OK**.

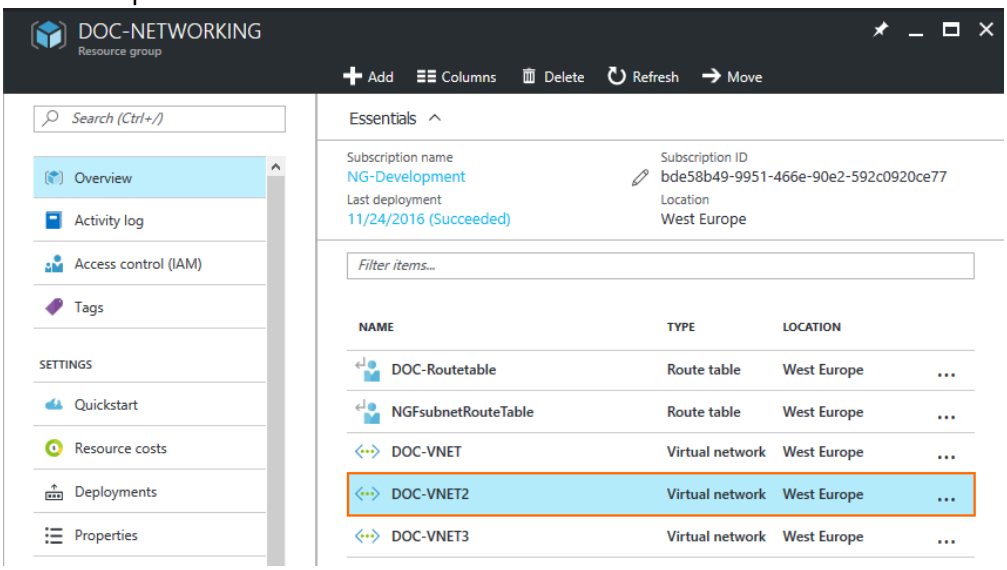
Repeat this process for every spoke VNET. The VNET **Peering Status** in the **Virtual network** blade is now **Initiated**.



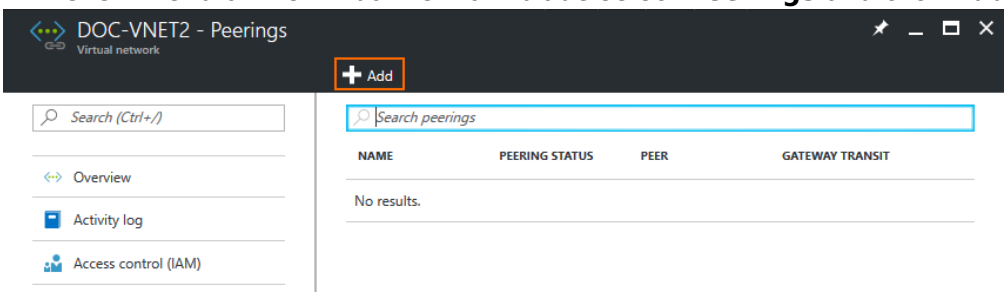
Step 3. Peer Spoke Virtual Networks with the Hub Virtual Network

Create the VNET peering between the spoke virtual networks and the hub virtual networks. This will change the peering state to **Connected** from **Initialized**. Repeat this step for every spoke VNET.

1. Go to the Azure Portal: https://portal.azure.com.
2. Select the resource group containing the virtual networks.
3. Select a spoke VNET.

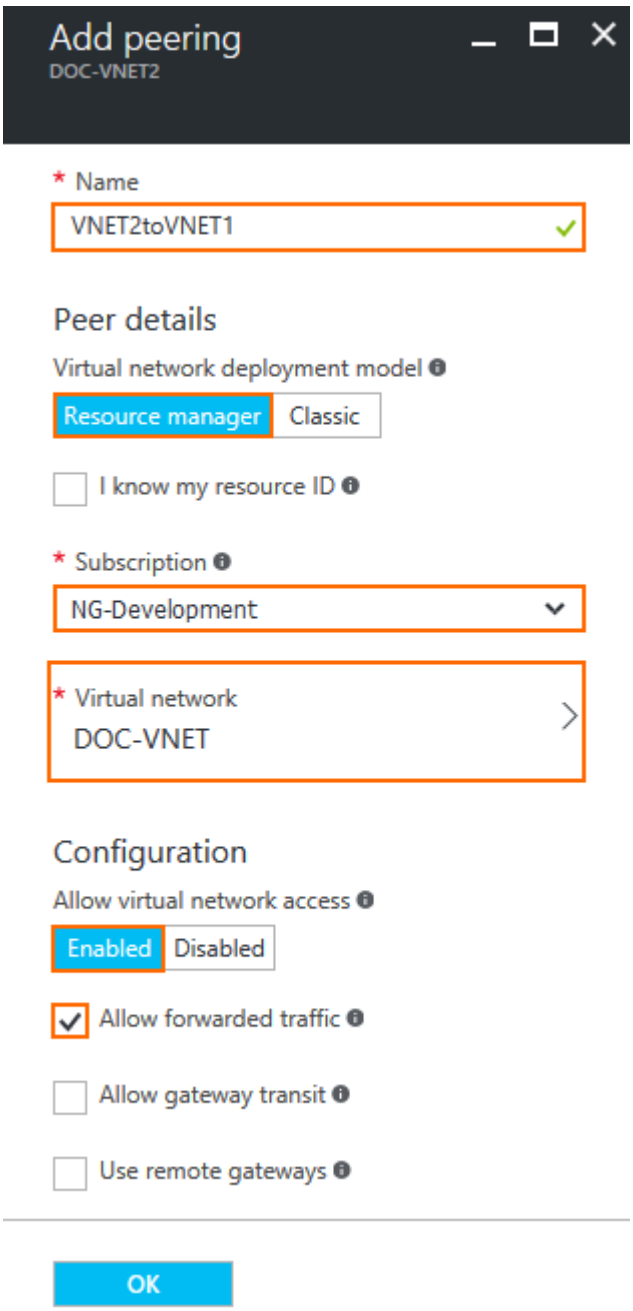


4. In the left menu of the virtual network blade select **Peerings** and click **Add**.



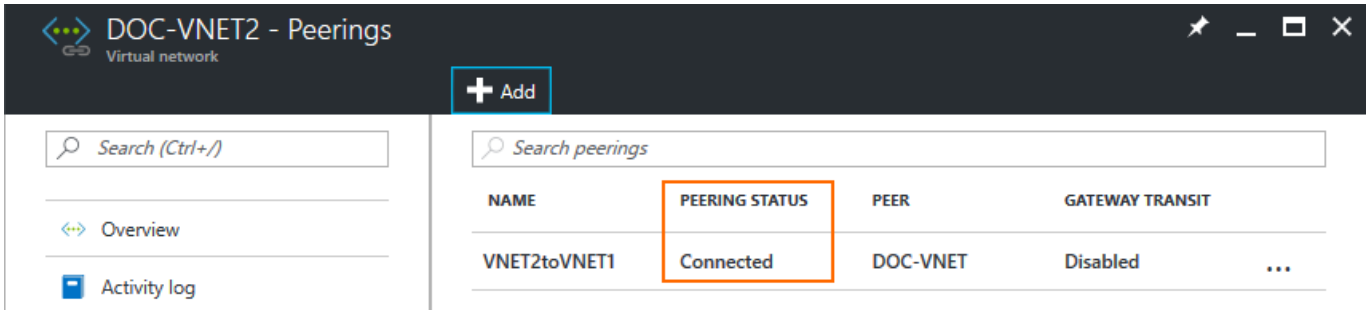
5. In the **Add peering** blade, enter the peering settings:
   - **Name** – Enter a name.

- **Peer details** – Select **Resource manager**.
- **Subscription** – Select the Azure subscription.
- **Virtual network** – Click and select the hub VNET.
- **Allow virtual network access** – Select **Enabled** to allow access to the virtual network.
- **Allow forward traffic** – Enable to allow virtual machines to forward traffic



6. Click **OK**.

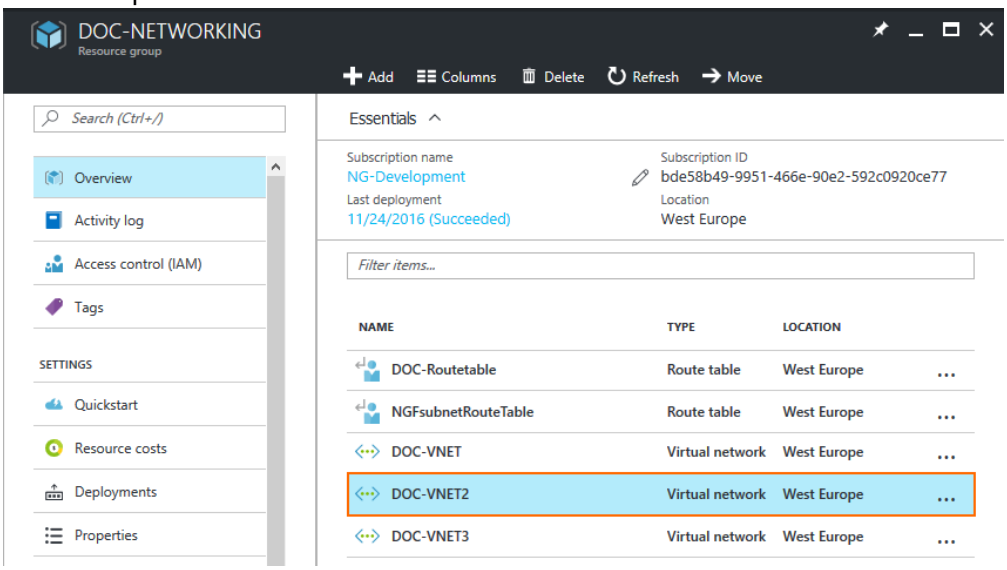
Repeat this process for every spoke VNET. The VNET **Peering Status** in the **Virtual network** blade is now **Connected**.



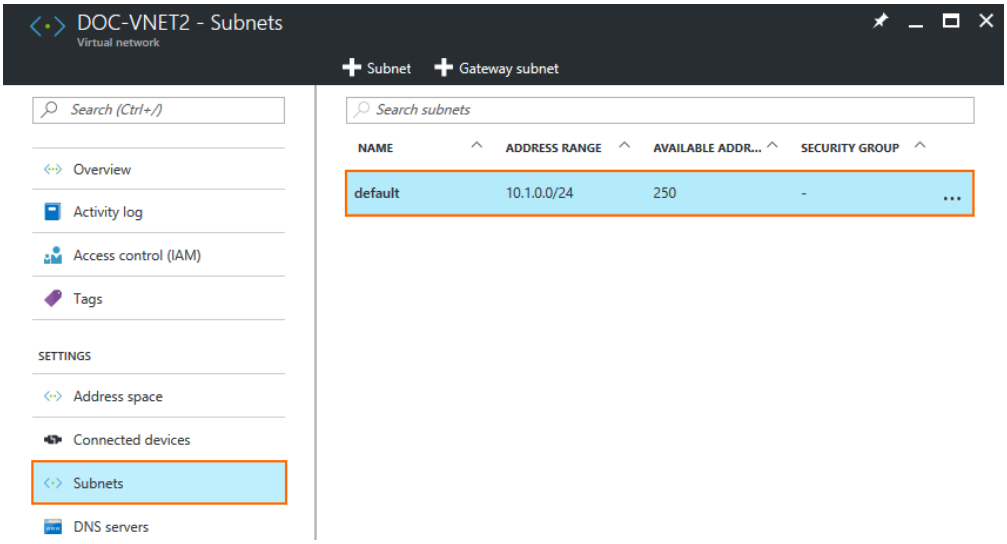
Step 4. Associate the Route Table with Spoke Subnets

To send traffic over the firewall in the peered subnet, associate the Azure route table containing the UDR routes with the subnets. Repeat this for each spoke VNET.

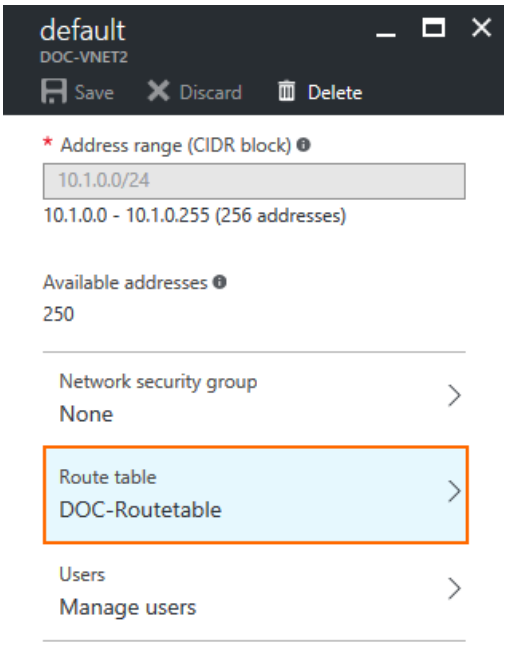
1. Go to the Azure Portal: https://portal.azure.com.
2. Select the resource group containing the virtual networks.
3. Select a spoke VNET.



4. In the left menu of the blade, click **Subnets**.
5. Select the subnet. A blade with the subnet name opens.



6. Click **Route Table** and select the route table created for the hub VNET.



7. Click **Save**.
8. Repeat for the other subnets in this virtual network that are allowed to send traffic to other VNETs or need access to the Internet.

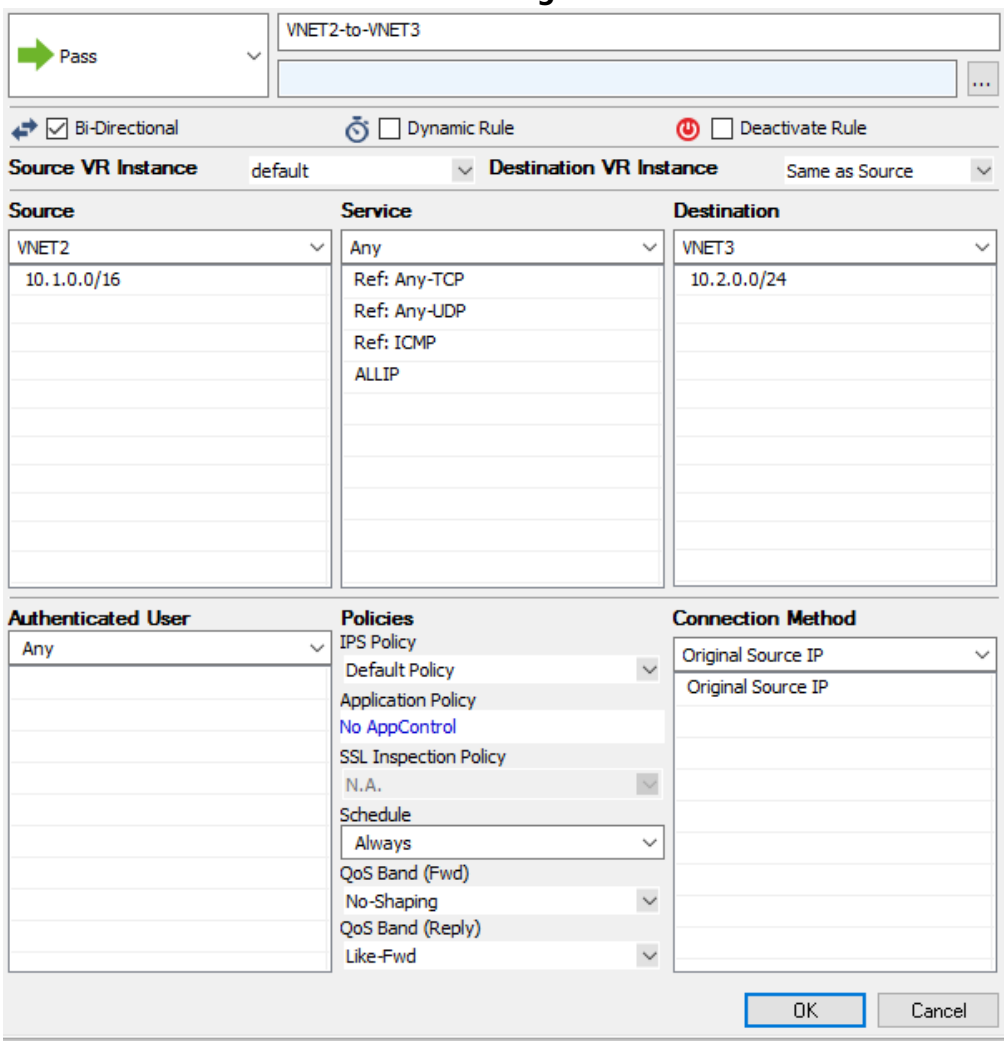
Traffic from VMs are now routed over the firewall VM in the hub VNET.

Step 5. Create Access Rules to Allow Traffic between Spoke VNETs

Create access rules to allow traffic between the spoke VNETS

1. Log into the primary firewall.

2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
3. Click **Lock**.
4. From the **Edit Rule** menu in the left menu, click **New**. The **New Rule** window opens.
5. Enter a **Name** E.g., VNET1-to-VNET2
6. In the **New Rule** window, configure the settings to allow traffic between both systems:
   - **Action** – Select **Pass**.
   - **Bi-Directional** – Select the check box to apply the rule in both directions.
   - **Source** – Enter the network of the first spoke VNET.
   - **Service** – Select the services allowed to access the tunnel. Default: **Any**
   - **Destination** – Enter the network of the second spoke VNET.
   - **Connection Method** – Select **Original Source IP**.



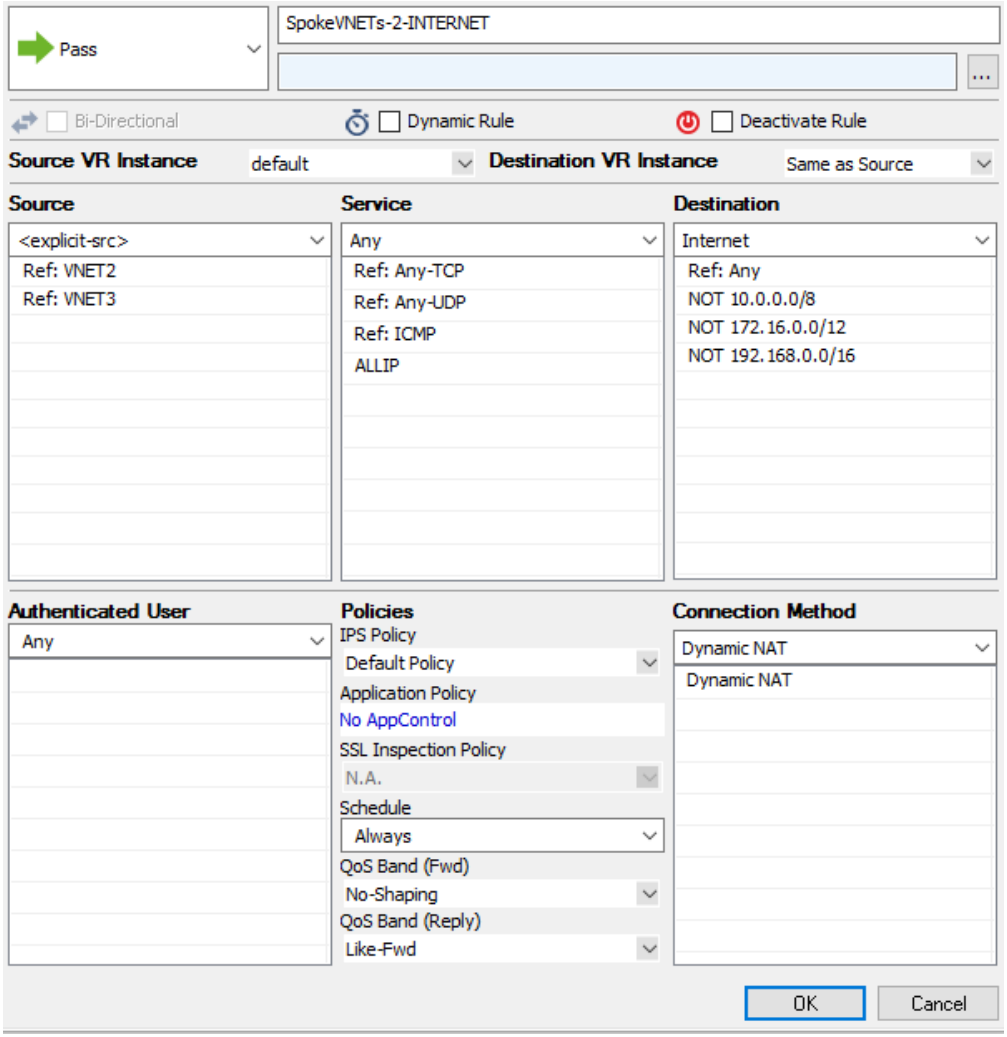
7. Click **OK**.
8. Reorder the access rule by dragging it to the correct position in the forwarding firewall's ruleset.
9. Click **Send Changes** and **Activate**.

The VMs in the first spoke VNET can now access the VMs in the second spoke. Replace this access rule with more specific rules to lock down traffic between the spokes further.

Step 6. (optional) Create an Access Rule to Allow Spoke VNETs Access to the Internet

Create an access rule that allows VMs in the spoke VNETs access to the Internet:

1. Log into the primary firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Rules**.
3. Click **Lock**.
4. From the **Edit Rule** menu in the left menu, click **New**. The **New Rule** window opens.
5. Enter a **Name** E.g., `SpokeVNETs-2-INTERNET`
6. In the **New Rule** window, configure the settings to allow traffic between both systems:
   - **Action** – Select **Pass**.
   - **Source** – Enter the networks for the spoke VNETs.
   - **Service** – Select the services allowed to access the tunnel. Default: **Any**
   - **Destination** – Select **Internet**.
   - **Connection Method** – Select **Dynamic NAT**.



7. Click **OK**.
8. Reorder the access rule by dragging it to the correct position in the forwarding firewall's ruleset.
9. Click **Send Changes** and **Activate**.

All traffic from the subnets in the spoke VNETs is now passing through the high availability firewall cluster in the hub VNET.

Figures

1. Azure_VNET_Peering.png
2. vnet_peering_01.png
3. vnet_peering_02.png
4. vnet_peering_03.png
5. vnet_peering_04.png
6. vnet_peering_05.png
7. vnet_peering_06.png
8. vnet_peering_07.png
9. vnet_peering_08.png
10. vnet_peering_09.png
11. vnet_peering_10.png
12. vnet_peering_11.png
13. vnet_peering_08.png
14. vnet_peering_12.png
15. vnet_peering_13.png
16. vnet_peering_14.png
17. vnet_peering_15.png