Express Route Gateway

About Express Route Gateway

Beginning with Release 5.1(2), support is now available for express route gateway deployment, where you can deploy an express route gateway in the hub VNet using redirect or without using redirect. The express route gateway is used to provide connectivity between a Cloud APIC-managed cloud site and a non-ACI remote site. The external EPG for the non-ACI remote site (in this case, connected by an express route gateway) has a contract with the cloud EPG in the hub or spoke VNet.

About Deploying Express Route Gateway Using Redirect

In situations where you are deploying a connection between a cloud endpoint and an external network through an express route gateway, you can insert a service device between them using redirect.

For this use case, the external EPG connected by the express route gateway has a contract with the cloud EPG in either the hub or the spoke VNet. In this situation:

- The redirect is configured on the gateway subnet route table by the Cloud APIC. The traffic destined to the provider cloud EPG is redirected to the service device deployed in the hub VNet as the next hop.

- You should have the service device that is used in the redirect in the same VNet as the external EPG connected by the express route gateway (in this case, in the hub VNet).

- Having the provider cloud EPG stretched across regions is supported in this case.

The following figure shows an example of a redirect for express route gateway to the provider EPG in the hub VNet.
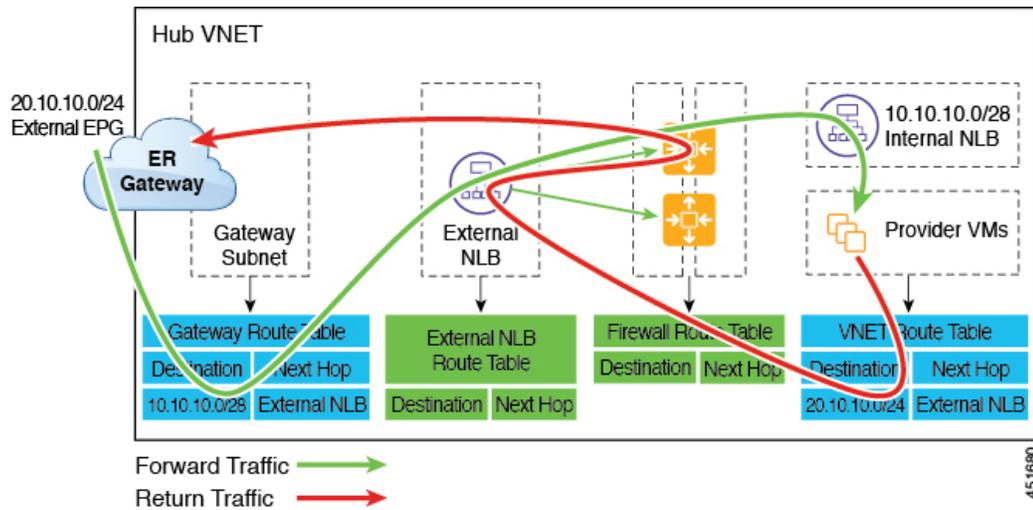
The following figure shows an example of a redirect for express route gateway to the provider EPG in the spoke VNet.
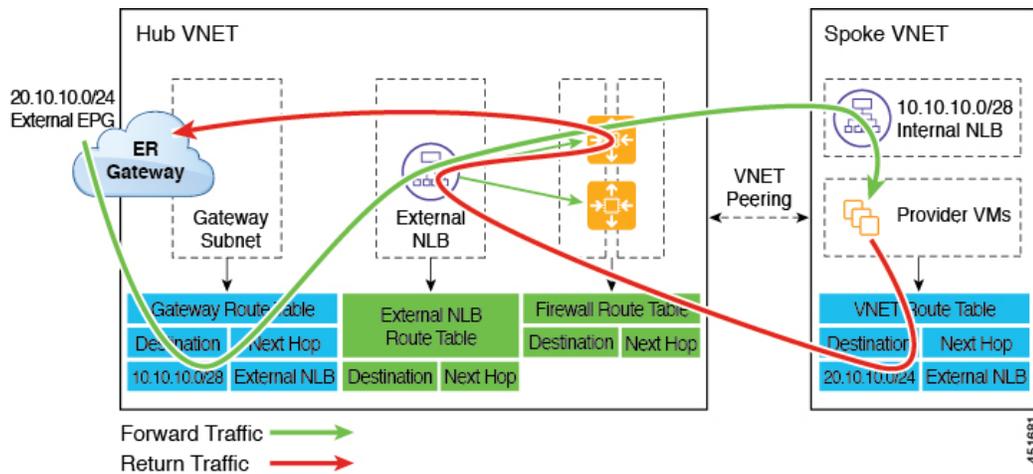
The following table describes how redirect is programmed.

Consumer	Provider	Redirect on Gateway Subnet Route Table	Redirect on Provider VNet
External EPG connected by the express route gateway	Cloud EPG with subnet-based endpoint selector	Redirect for the consumer-to-provider traffic using the subnets of the provider	Redirect for the provider-to-consumer traffic using the subnets of the external EPG

Deploying Express Route Gateway Using Redirect

Before you begin

Review the information provided in About Deploying Express Route Gateway Using Redirect, on page 1 before proceeding with these procedures.

Step 1   Enable VNet peering on your Cloud APIC.

Refer to Configuring VNET Peering for Cloud APIC for Azure for those instructions.

The gateway subnet in the hub VNet that is required for the express route gateway is deployed by the Cloud APIC when VNet peering is enabled. This is done to prepare the hub VNet for the deployment of the express route gateway.

Step 2   Create an external EPG in the hub VNet that represents the network for the non-ACI remote site.

- To create an external EPG using the GUI, see Creating an External EPG Using the Cisco Cloud APIC GUI.

   In the **Route Reachability** field for the external EPG, select **External-Site**.

- To create an external EPG using the REST API, see Creating an External Cloud EPG Using the REST API.

   Create an external cloud EPG with the type **site-external**.

Step 3   Through the Azure portal, deploy the express route gateway in the hub VNet using the gateway subnet that you configured in Step 1, on page 3.

Depending on the number of regions that you selected when you enabled VNet peering in Step 1, on page 3, if you need express route gateway access on multiple regions that the Cloud APIC will manage, deploy express route gateways in each of those regions separately.

a) In the Azure portal, navigate to the Resource Manager virtual network where you want to create a virtual network gateway.
b) On the left side, select **Create a resource**, and type **Virtual Network Gateway** in search.
c) Locate **Virtual network gateway** in the search return and click the entry.
d) On the **Virtual network gateway** page, choose **Create**.
e) On the **Create virtual network gateway** page, enter the appropriate information for these fields:

- **Subscription**: Verify that the correct subscription is selected.

- **Resource Group**: The resource group will automatically be chosen once you choose the virtual network.

- **Name**: The name of your express route gateway.

- **Region**: Change the **Region** field to point to the location where your virtual network is located. If the location isn't pointing to the region where your virtual network is, the virtual network won't appear in the **Choose a virtual network** dropdown.

- **Gateway type**: Choose **ExpressRoute**.

- **SKU**: Choose the gateway SKU from the dropdown.

- **Virtual network**: Choose the virtual network that was created by the Cloud APIC in Step 1, on page 3.

- **Public IP address**: Choose **Create new**.

- **Public IP address name**: Provide a name for the public IP address.

f) Select **Review + Create**, and then **Create** to begin creating the gateway.

The settings are validated and the gateway deploys. Creating virtual network gateway can take up to 45 minutes to complete.

To verify that the express route gateway was deployed successfully, navigate to the network gateways page in the Azure portal and verify that a network gateway with the type **express route** was created.

If you need express route gateway access on additional regions, repeat these steps for each of those regions.

Step 4   Configure the service device for the redirect.

To configure a service device for redirect using the GUI or REST API, see Deploying Layer 4 to Layer 7 Services.

Step 5   Configure a contract between the cloud EPG and the external EPG connected by the express route gateway.

- To create a contract using the GUI, see Creating a Contract Using the Cisco Cloud APIC GUI.

- To configure a contract using the REST API, see Creating a Contract Using the REST API.

# About Deploying Express Route Gateway Without Redirect

For this type of deployment, route propagation to the spoke VNet is automatically enabled by the Cloud APIC. This allows your non-ACI remote site subnet routes to be available to the spoke VNet through the hub VNet using VNet peering with gateway transit (also referred to as transit peering). VNet peering with gateway transit is also automatically enabled by the Cloud APIC in this situation.

As part of this configuration, you will deploy the express route gateway in the hub VNet. When the Cloud APIC detects that the express route gateway has been configured in the hub VNet, it automatically sets the transit peering properties, one for the hub → spoke peering and the other for the spoke → hub peering, in the Azure portal:

- **Hub VNet**: Automatically set to **Use this virtual network's gateway**

- **Spoke VNet**: Automatically set to **Use remote virtual network's gateway** in the spoke VNet that is managed by the Cloud APIC

In order to have the route propagation enabled for the egress route table of the spoke VNet, you must configure a contract between the cloud EPG in the spoke VNet and the external EPG connecting to the non-ACI remote site.

The following figure shows an example of this type of deployment.
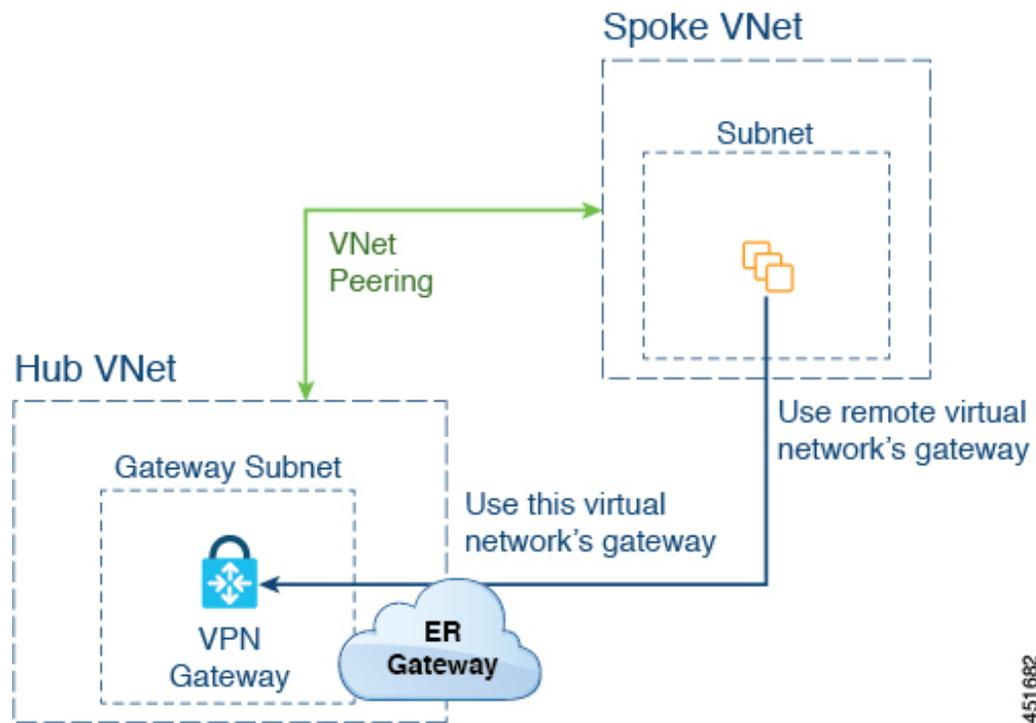
In this example:

- The following configurations are done automatically by the Cloud APIC:

    - The spoke VNet uses VNet peering with gateway transit (transit peering)

    - The VPN gateway in the hub VNet is connected to an on-premises non-ACI remote site

    - When the Cloud APIC detects that the express route gateway is deployed in the hub VNet, the transit peering properties are automatically set on each side of the peering (hub → spoke and spoke → hub):

        - **Hub VNet**: Automatically set to **Use this virtual network's gateway**

        - **Spoke VNet**: Automatically set to **Use remote virtual network's gateway** in the spoke VNet that is managed by the Cloud APIC

- The on-premises non-ACI routes learned by the VPN gateway are available to the spoke VNet if the EPG in the spoke VNet has a contract with the external EPG

- The hub VNet allows traffic from the EPG in the spoke VNet destined to the on-premises non-ACI remote site through the VPN gateway

Deploying Express Route Gateway Without Redirect

Before you begin

Review the information provided in About Deploying Express Route Gateway Without Redirect, on page 4 before proceeding with these procedures.

Step 1 Enable VNet peering on your Cloud APIC.

Refer to Configuring VNET Peering for Cloud APIC for Azure for those instructions.

The gateway subnet in the hub VNet that is required for the express route gateway is deployed by the Cloud APIC when VNet peering is enabled. This is done to prepare the hub VNet for the deployment of the express route gateway.

Step 2 Create an external EPG in the hub VNet that represents the network for the non-ACI remote site.

- To create an external EPG using the GUI, see Creating an External EPG Using the Cisco Cloud APIC GUI.

   In the **Route Reachability** field for the external EPG, select **External-Site**.

- To create an external EPG using the REST API, see Creating an External Cloud EPG Using the REST API.

   Create an external cloud EPG with the type **site-external**.

Step 3 Through the Azure portal, deploy the express route gateway in the hub VNet using the gateway subnet that you configured in Step 1, on page 6.

Depending on the number of regions that you selected when you enabled VNet peering in Step 1, on page 6, if you need express route gateway access on multiple regions that the Cloud APIC will manage, deploy express route gateways in each of those regions separately.

a) In the Azure portal, navigate to the Resource Manager virtual network where you want to create a virtual network gateway.
b) On the left side, select **Create a resource**, and type **Virtual Network Gateway** in search.
c) Locate **Virtual network gateway** in the search return and click the entry.
d) On the **Virtual network gateway** page, choose **Create**.
e) On the **Create virtual network gateway** page, enter the appropriate information for these fields:

   - **Subscription**: Verify that the correct subscription is selected.

   - **Resource Group**: The resource group will automatically be chosen once you choose the virtual network.

   - **Name**: The name of your express route gateway.

   - **Region**: Change the **Region** field to point to the location where your virtual network is located. If the location isn't pointing to the region where your virtual network is, the virtual network won't appear in the **Choose a virtual network** dropdown.

   - **Gateway type**: Choose **ExpressRoute**.

   - **SKU**: Choose the gateway SKU from the dropdown.

   - **Virtual network**: Choose the virtual network that was created by the Cloud APIC in Step 1, on page 6.

   - **Public IP address**: Choose **Create new**.

   - **Public IP address name**: Provide a name for the public IP address.

f) Select **Review** + **Create**, and then **Create** to begin creating the gateway.

   The settings are validated and the gateway deploys. Creating virtual network gateway can take up to 45 minutes to complete.

To verify that the express route gateway was deployed successfully, navigate to the network gateways page in the Azure portal and verify that a network gateway with the type **express route** was created.

If you need express route gateway access on additional regions, repeat these steps for each of those regions.

Step 4   Configure a contract between the cloud EPG and the external EPG connected by the express route gateway.

- To create a contract using the GUI, see Creating a Contract Using the Cisco Cloud APIC GUI.

- To configure a contract using the REST API, see Creating a Contract Using the REST API.