Cisco クラウド ネットワーク コントローラで管理されたクラウド サイトと非 ACI リモート サイト間の接続の設定

この章のセクションでは、エクスプレス ルート ゲートウェイを使用して、またはエクスプレス ルート ゲートウェイを使用せずに、Cisco Cloud ネットワーク コントローラで管理されたクラウド サイトと非 ACI リモート サイト間の接続を構成する方法について説明します。

- エクスプレス ルート ゲートウェイを使用して接続を構成する （1 ページ）
- VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成 （8 ページ）

エクスプレス ルート ゲートウェイを使用して接続を構成する

エクスプレス ルート ゲートウェイはリダイレクトを使用してまたは、リダイレクトを使用せずに、ハブ VNet の中でのエクスプレス ルート ゲートウェイの展開と一緒にサポートされます。エクスプレス ルート ゲートウェイは、Cisco Cloud Network Controller が管理するクラウド サイトと非 ACI リモート サイト間の接続を提供するために使用されます。非 ACI リモートサイト（この場合、エクスプレス ルート ゲートウェイによって接続されている）の外部 EPG には、ハブまたはスポーク VNet 内のクラウド EPG とのコントラクトがあります。

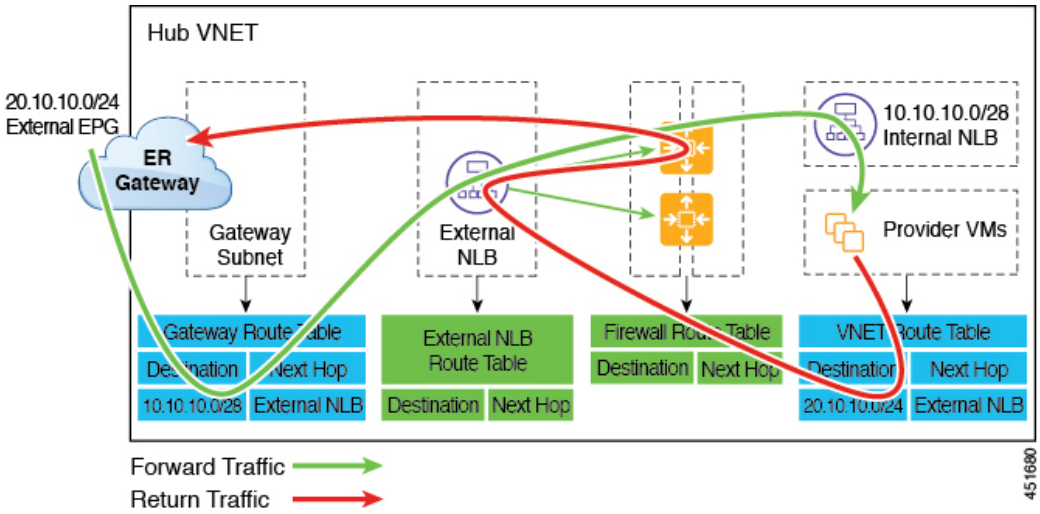
リダイレクトを使用してエクスプレス ルート ゲートウェイを展開することについて

エクスプレス ルート ゲートウェイを介してクラウド エンドポイントと外部ネットワーク間の接続を展開している状況では、リダイレクトを使用してそれらの間にサービス デバイスを挿入できます。

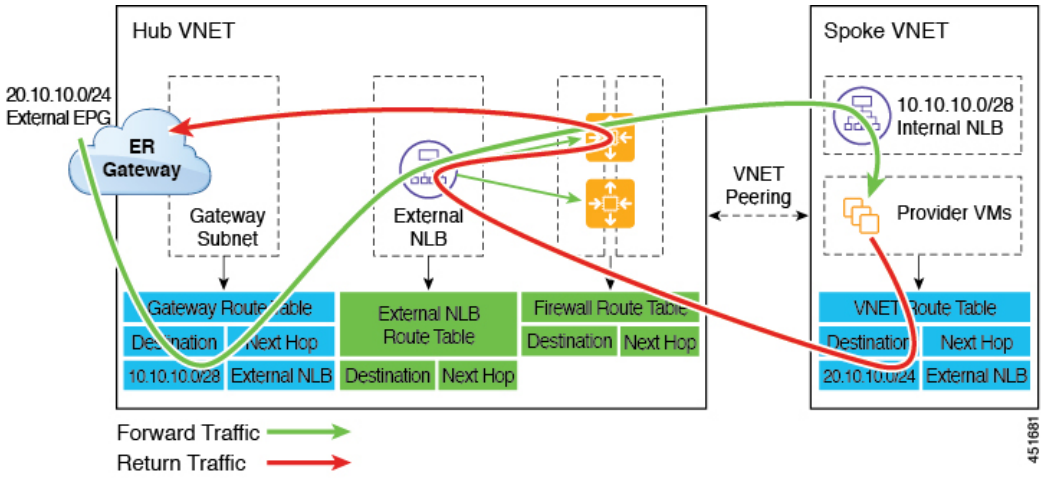
このユース ケースでは、エクスプレス ルート ゲートウェイによって接続された外部 EPG は、ハブまたはスポーク VNet のいずれかでクラウド EPG とコントラクトがあります。このケースから得られた結果を以下に示します。

- リダイレクトは、Cisco Cloud Network Controller によってゲートウェイ サブネット ルート テーブルで構成されます。プロバイダー クラウド EPG 宛てのトラフィックは、ハブ VNet に展開されたサービス デバイスにネクスト ホップとしてリダイレクトされます。
- リダイレクトで使用されるサービス デバイスは、エクスプレス ルート ゲートウェイ（この場合はハブ VNet）によって接続された外部 EPG と同じ VNet にある必要があります。
- この場合、プロバイダー クラウド EPG をリージョン全体に拡張することがサポートされています。

次の図は、ハブ VNet のプロバイダー EPG へのエクスプレス ルート ゲートウェイのリダイレクトの例を示しています。



次の図は、スポーク VNet 内のプロバイダー EPG へのエクスプレス ルート ゲートウェイのリダイレクトの例を示しています。



次の表は、、リダイレクトがどのようにプログラムされるかを示しています。

コンシューマ	プロバイダー	ゲートウェイ サブネット ルート テーブルでのリダイレクト	プロバイダー VNet でのリダイレクト
エクスプレス ルート ゲートウェイによって接続された外部 EPG	サブネットベースのエンドポイント セレクタを備えたクラウド EPG	プロバイダーのサブネットを使用したコンシューマからプロバイダーへのトラフィックのリダイレクト	外部 EPG のサブネットを使用したプロバイダーからコンシューマへのトラフィックのリダイレクト

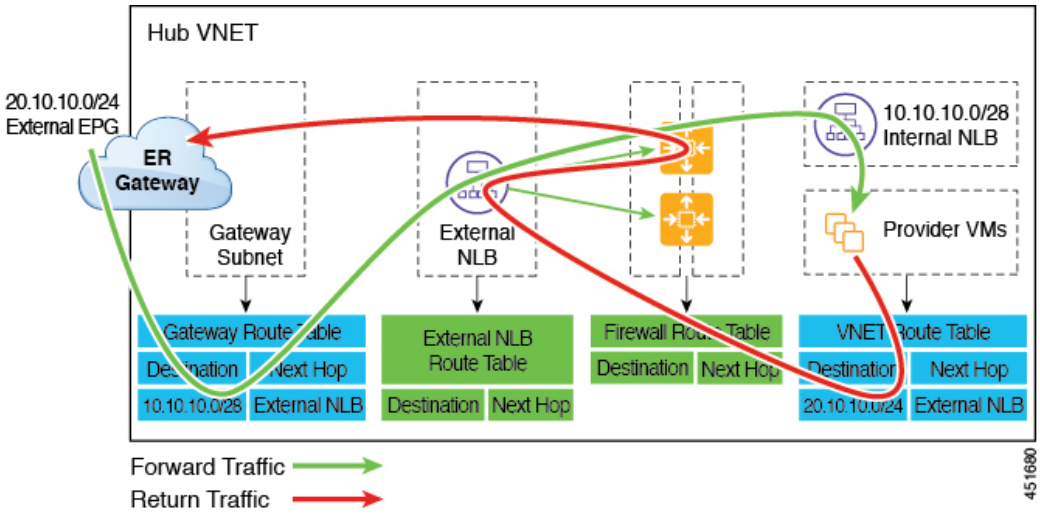
リダイレクトを使用してエクスプレス ルート ゲートウェイを展開することについて

エクスプレス ルート ゲートウェイを介してクラウド エンドポイントと外部ネットワーク間の接続を展開している状況では、リダイレクトを使用してそれらの間にサービス デバイスを挿入できます。

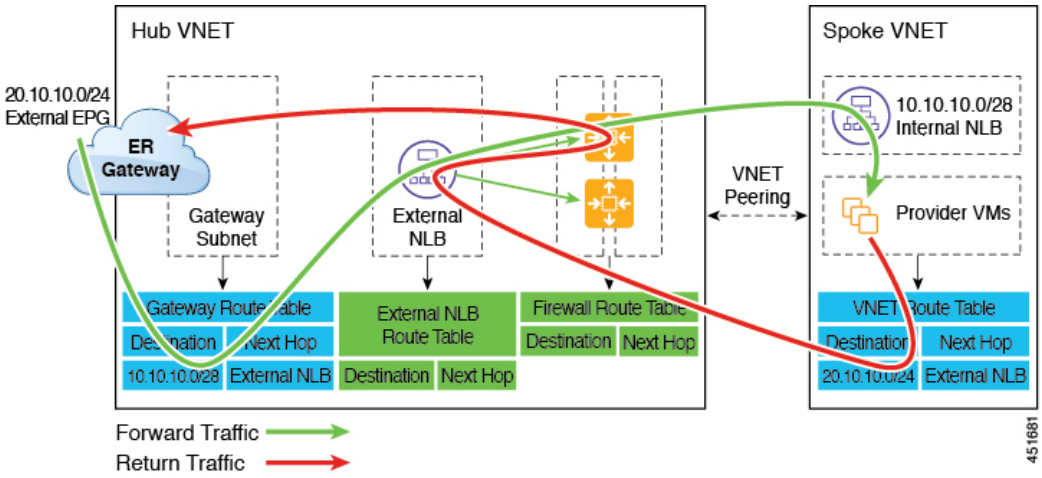
このユース ケースでは、エクスプレス ルート ゲートウェイによって接続された外部 EPG は、ハブまたはスポーク VNet のいずれかでクラウド EPG とコントラクトがあります。このケースから得られた結果を以下に示します。

- リダイレクトは、Cisco Cloud Network Controller によってゲートウェイ サブネット ルート テーブルで構成されます。プロバイダー クラウド EPG 宛てのトラフィックは、ハブ VNet に展開されたサービス デバイスにネクスト ホップとしてリダイレクトされます。
- リダイレクトで使用されるサービス デバイスは、エクスプレス ルート ゲートウェイ（この場合はハブ VNet）によって接続された外部 EPG と同じ VNet にある必要があります。
- この場合、プロバイダー クラウド EPG をリージョン全体に拡張することがサポートされています。

次の図は、ハブ VNet のプロバイダー EPG へのエクスプレス ルート ゲートウェイのリダイレクトの例を示しています。



次の図は、スポーク VNet 内のプロバイダー EPG へのエクスプレス ルート ゲートウェイのリダイレクトの例を示しています。



次の表は、、リダイレクトがどのようにプログラムされるかを示しています。

コンシューマ	プロバイダー	ゲートウェイ サブネット ルート テーブルでのリダイレクト	プロバイダー VNet でのリダイレクト
エクスプレス ルート ゲートウェイによって接続された外部 EPG	サブネットベースのエンドポイントセレクタを備えたクラウド EPG	プロバイダーのサブネットを使用したコンシューマからプロバイダーへのトラフィックのリダイレクト	外部 EPG のサブネットを使用したプロバイダーからコンシューマへのトラフィックのリダイレクト

リダイレクトなしの Express Route ゲートウェイの展開について

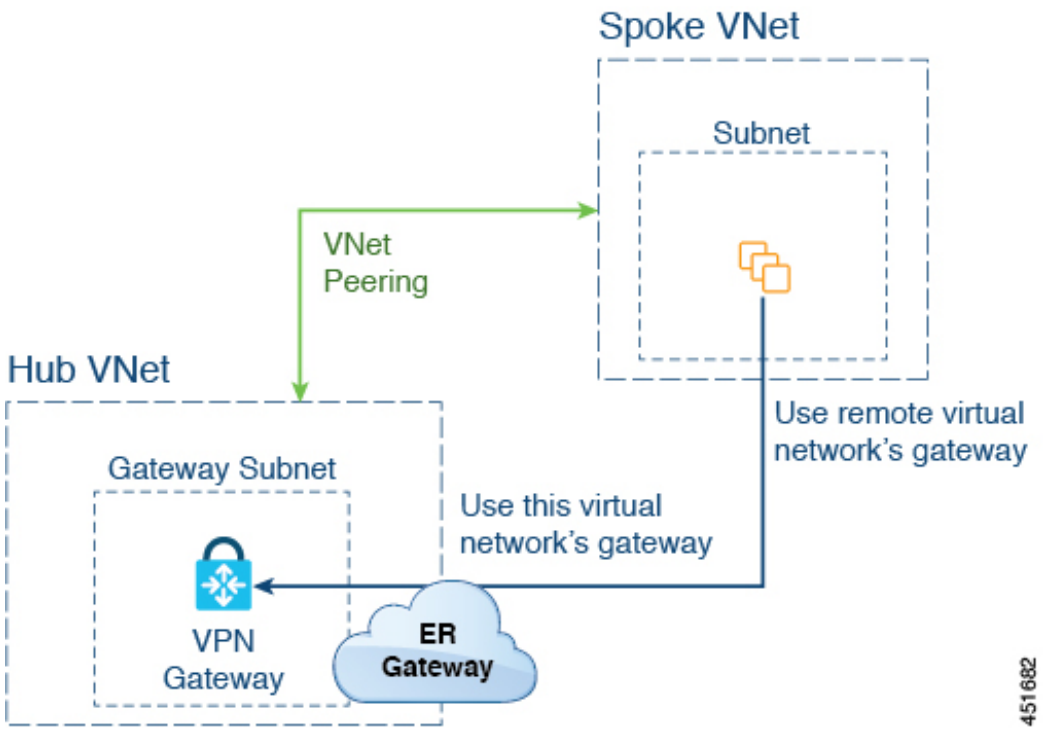
このタイプの展開では、スポーク VNet へのルート伝達が Cisco Cloud Network Controller によって自動的に有効になります。これにより、ゲートウェイ移行を使用した VNet ピアリング（移行ピアリングとも呼ばれます）を使用して、ハブ VNet を介してスポーク VNet で非 ACI リモート サイト サブネット ルートを使用できるようになります。ゲートウェイトランジットを使用した VNet ピアリングは、この場合Cisco Cloud Network Controller によって自動的に有効になります。

この構成の一部として、ハブ VNet にエクスプレス ルート ゲートウェイを展開します。Cisco Cloud Network Controller は、エクスプレス ルート ゲートウェイがハブ VNet で構成されていることを検出すると、Azure portal で移行ピアリング プロパティを自動的に設定します。1 つはハブ → スポーク ピアリング用、もう 1 つはスポーク → ハブ ピアリング用です。

- **Hub VNet**：**[この仮想ネットワークのゲートウェイを使用する（Use this virtual network's gateway）]** に自動的に設定されます。
- **スポーク VNet**：Cisco Cloud Network Controller によって管理されるスポーク VNet で **[リモート仮想ネットワークのゲートウェイを使用する（Use remote virtual network's gateway）]** に自動的に設定されます。

スポーク VNet の出力ルート テーブルに対してルート伝達を有効にするには、スポーク VNet のクラウド EPG と、非 ACI リモート サイトに接続する外部 EPG との間のコントラクトを構成する必要があります。

次の図に、この展開タイプの例を示します。



この例では、以下のようになっています。

- 次の構成は、Cisco Cloud Network Controller によって自動的に行われます。
  - スポーク VNet は、ゲートウェイ トランジット（トランジット ピアリング）で VNet ピアリングを使用する
  - ハブ VNet の VPN ゲートウェイがオンプレミスの非 ACI リモートサイトに接続されている
  - エクスプレス ルート ゲートウェイがハブ VNet に展開されていることを Cisco Cloud Network Controller が検出すると、移行ピアリング プロパティがピアリングの各側で自動的に設定されます（ハブ → スポークおよびスポーク → ハブ）。
    - **Hub VNet**：**[この仮想ネットワークのゲートウェイを使用する（Use this virtual network's gateway）]** に自動的に設定されます。
    - **スポーク VNet**：Cisco Cloud Network Controller によって管理されるスポーク VNet で **[リモート仮想ネットワークのゲートウェイを使用する（Use remote virtual network's gateway）]** に自動的に設定されます。
- スポーク VNet の EPG が外部 EPG とコントラクトしている場合、VPN ゲートウェイによって学習されたオンプレミスの非 ACI ルートは、スポーク VNet で使用できます。
- ハブ VNet は、VPN ゲートウェイを介してオンプレミスの非 ACI リモートサイトを宛先としたスポーク VNet 内の EPG からのトラフィックを許可します。

リダイレクトなしのエクスプレス ルート ゲートウェイの展開

始める前に

これらの手順を続行する前に、リダイレクトなしの Express Route ゲートウェイの展開について （5 ページ） の情報を確認します。

ステップ 1 Cisco Cloud Network Controller で VNet ピアリングを有効にします。

これらの指示については、「Azure 向け Cisco Cloud Network Controller の VNET ピアリングを構成する」を参照してください。

エクスプレス ルート ゲートウェイに必要なハブ VNet のゲートウェイ サブネットは、VNet ピアリングが有効な場合 Cisco Cloud Network Controller で展開されます。これは、エクスプレス ルート ゲートウェイの展開用にハブ VNet を準備するために行われます。

ステップ 2 非 ACI リモートサイトのネットワークを表すハブ VNet に外部 EPG を作成します。

- GUI を使用して外部 EPG を作成するには、Cisco Cloud Network Controller GUI を使用した外部 EPG の作成 を参照してください。

  外部 EPG の **[ルート到達可能性（Route Reachability）]** で、**[外部サイト（External-Site）]** を選択します。

- REST API を使用して外部 EPG を作成するには、REST API を使用した外部クラウド EPG の作成 を参照してください。

  タイプ **site-external** の外部クラウド EPG を作成します。

ステップ 3 Azure ポータルを通じて、ステップ 1 （6 ページ） で構成したゲートウェイ サブネットを使用してハブ VNet でエクスプレス ルート ゲートウェイを展開します。

ステップ 1 （6 ページ） で VNet ピアリングを有効にするときに選択したリージョンの数に応じて、Cisco Cloud Network Controller が管理する複数のリージョンでエクスプレス ルート ゲートウェイ アクセスが必要な場合は、それらの各リージョンにエクスプレス ルート ゲートウェイを個別に展開します。

a) Azure ポータルで、仮想ネットワーク ゲートウェイを作成する Resource Manager 仮想ネットワークに移動します。
b) 左側で、**[リソースの作成（Create a resource）]** を選択し、検索に**仮想ネットワーク ゲートウェイ**と入力します。
c) 検索結果で **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** を見つけて、エントリをクリックします。
d) **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** ページで、**[作成（Create）]** を選択します。
e) **[仮想ネットワーク ゲートウェイの作成（Create virtual network gateway）]** ページで、次のフィールドに適切な情報を入力します。

   - **サブスクリプション**：適切なサブスクリプションが選択されていることを確認します。
   - **リソース グループ**：仮想ネットワークを選択すると、リソース グループが自動的に選択されます。
   - **名前**：エクスプレス ルート ゲートウェイの名前。
   - **リージョン**：仮想ネットワークが配置されている場所を指すように**[リージョン（Region）]** フィールドを変更します。場所が仮想ネットワークのあるリージョンを指していない場合、仮想ネットワークは **[仮想ネットワークの選択（Choose a virtual network）]** ドロップダウンに表示されません。
   - **ゲートウェイの種類**：**ExpressRoute** を選択します。
   - **SKU**：ドロップダウンからゲートウェイ SKU を選択します。
   - **仮想ネットワーク**：ステップ 1 （6 ページ） で Cisco Cloud Network Controller によって作成された仮想ネットワークを選択します。
   - **パブリック IP アドレス**：**[新規作成（Create new）]** を選択します。
   - **パブリック IP アドレス名**：パブリック IP アドレスの名前を指定します。

f) **[確認 + 作成（Review + Create）]** を選択し、**[作成（Create）]** でゲートウェイの作成を開始します。

   設定が確認され、ゲートウェイが展開します。仮想ネットワーク ゲートウェイの作成には、完了までに最長 45 分かかります。

エクスプレス ルート ゲートウェイが正常に展開されたことを確認するには、Azure ポータルのネットワーク ゲートウェイ ページに移動し、タイプ **エクスプレス ルート** のネットワーク ゲートウェイが作成されたことを確認します。

追加のリージョンでエクスプレスルート ゲートウェイ アクセスが必要な場合、それらのリージョンそれぞれにこれらの手順を繰り返します。

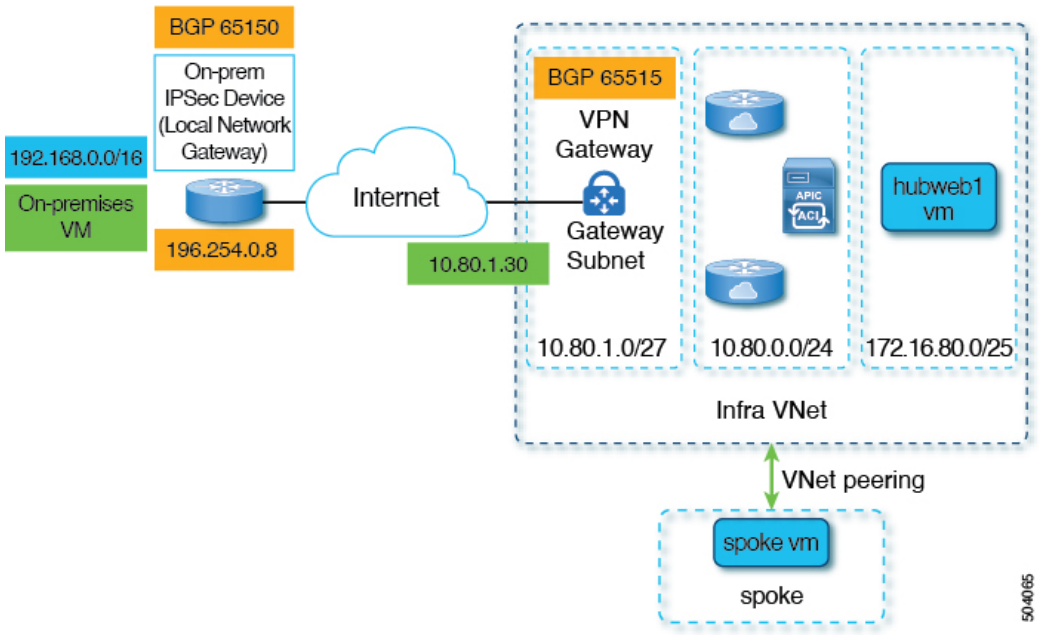
ステップ 4 エクスプレス ルート ゲートウェイで接続したクラウド EPG および外部 EPG 間のコントラクトを構成します。

- GUI を使用して契約を作成するには、Cisco Cloud Network Controller GUI を使用したコントラクトの作成 を参照してください。
- REST API を使用して契約を構成するには、REST API を使用したコントラクトの作成 を参照してください。

VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成

VPN ゲートウェイを使用して、Cisco Cloud Network Controller で管理されたクラウド サイトと非 ACI リモート サイト間の接続を提供するためのサポートを利用できます。このタイプの接続では、仮想ネットワーク ゲートウェイ（VNG）がインフラ（ハブ）VNet に展開され、Cisco Cloud Network Controller で管理されたクラウド サイトから非 ACI リモート ブランチ サイトに接続できるようにします。BGP は、インフラ VNet の CCR ルータと VNG と、非 ACI リモート ブランチ サイトのオンプレミス IPsec デバイス（ローカル ネットワーク ゲートウェイ）との間のルーティング プロトコルとして IPsec トンネル上で実行されます。

次の図では、このタイプの接続による構成例を示します。



次の手順では、このタイプの接続を構成する方法について説明します。最終的には、192.168.20.0/24 サブネットにあるオンプレミスの仮想マシンと、172.16.80.0/25 サブネットにある `hubweb` 仮想マシンの間で到達可能です。

Configuring Connectivity Using VPN Gateway

Before you begin

Review the information provided in VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成, on page 8 before proceeding with these procedures.

ステップ 1 Enable VNet peering on your Cisco Cloud Network Controller, if necessary.

Refer to Configuring VNET Peering for Cisco Cloud Network Controller for Azure for those instructions.

ステップ 2 Add the second subnet for the VPN gateway subnet.

a) In the Cisco Cloud Network Controller GUI, click the Intent icon ( ) and select **Cisco Cloud Network Controller Setup**.
b) In the **Region Management** area, click **Edit Configuration**.
c) In the **Regions to Manage** window, click **Next**.

The **General Connectivity** window appears.

d) Under the **General** area, in the **Subnet Pools for Cloud Routers** field, click **Add Subnet Pool for Cloud Routers**.
e) Enter the information for the second subnet for the VPN gateway router.

For example, using the example configuration in VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成, on page 8, you would add `10.80.1.0/24` for the second subnet for the VPN gateway router in this field.

f) Click **Next**, then enter the necessary information in the following page and click **Save and Continue**.

Cisco Cloud Network Controller will create the subnet for the VPN gateway router after you have completed the **Cisco Cloud Network Controller Setup** process. You can verify that the configuration for the subnet for the VPN gateway router was pushed to Azure successfully by navigating to the **Subnets** page in the Azure portal and locating the **GatewaySubnet** entry.

ステップ 3 Create an infra-hosted VRF and use that VRF for the site-external EPG.

You will create an infra-hosted VRF, where you have a VRF that is hosted within the parent infra VNet, and you will use that VRF for the site-external EPG that you will create in the next step.

a) In the Cisco Cloud Network Controller GUI, navigate to **Application Management** > **VRFs**.
b) Click **Actions** > **Create VRF**.
The **Create VRF** window appears.
c) Enter a name for this infra-hosted VRF, then click **Select Tenant** and select **infra** for the tenant and click Select.
d) Enter a description if necessary, then click **Save**.

ステップ 4 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 Cisco Cloud Network Controller GUI を使用した外部 EPG の作成.
  - In the **VRF** field for the external EPG, select the infra-hosted VRF that you just created for this external EPG.
  - In the **Route Reachability** field for the external EPG, select **External-Site**.
- To create an external EPG using the REST API, see REST API を使用した外部クラウド EPG の作成.
  - Use the infra-hosted VRF for this site-external EPG.
  - Create an external cloud EPG with the type **site-external**.

ステップ 5 Through the Azure portal, create the virtual network gateway in the infra VNet for the VPN gateway subnet that you configured in ステップ 2, on page 9.

In these steps, you will build the IPsec and BGP connections from the on-premises site to the Azure VPN gateway. For more information, see the following article in the Azure site:

https://docs.microsoft.com/en-gb/azure/virtual-network/virtual-network-configure-vnet-connections

a) In the Azure portal, create the virtual network gateways by navigating 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 virtual network 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 **VPN**.
- **VPN type**: Choose **Route-based**.
- **SKU**: Choose **VpnGw1**.
- **Generation**: Choose **Generation1**.
- **Virtual network**: Choose **overlay-1**.
- **Public IP address**: Choose **Create new**.
- **Public IP address name**: Provide a name for the public IP address.
- **Enable active-active mode**: Set to **Disabled**.
- **Configure BGP**: Set to **Enabled**.
- **Autonomous system number (ASN)**: Enter the appropriate BGP ASN value for the VPN gateway. By default, Azure uses an ASN value of 65515.

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

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

To verify that the virtual network gateway was deployed successfully, navigate to the virtual network gateways page and select the virtual network gateway that you just created, then click on **Settings: Configuration** to view and verify the configuration settings for the virtual network gateway.

ステップ 6 Create the local network gateway.

For this configuration, the local network gateway is an object that represents the on-premises IPsec device. Prepare the following parameters before creating the local network gateway:

- BGP autonomous system number (ASN)
- Public IP address
- An appropriate address space for the on-premises subnet that needs to be advertised to the virtual network gateway

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

- **Name**: The name of your local network gateway.
- **Endpoint**: Choose **IP address**.

- **IP address**: Enter the appropriate IP address for the local network gateway.
- **Address space**: Enter the appropriate value for the address space. For example, using the example configuration in VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成, on page 8, you would add `192.168.0.0/16` in this field.
- **Configure BGP settings**: Click the checkbox to enable this setting.
- **Autonomous system number (ASN)**: Enter the appropriate BGP ASN value for the local network gateway. This is the ASN value of the remote device. For example, using the example configuration in VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成, on page 8, you would add `65150` in this field.
- **BGP peer IP address**: Enter the BGP peer IP address that you will use for the on-premises device in this field (not the Azure virtual network gateway). For example, using the example configuration in VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成, on page 8, you would add `196.254.0.8` in this field.
- **Subscription**: Choose the same subscription that you used for the virtual network gateway in ステップ 5, on page 10.
- **Resource group**: Choose the same resource group that you used for the virtual network gateway in ステップ 5, on page 10.
- **Location**: Choose the same location (region) that you used for the virtual network gateway in ステップ 5, on page 10.

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

The settings are validated and the gateway deploys.

To verify that the local network gateway was deployed successfully, navigate to the local network gateways page and select the local network gateway that you just created, then click on **Settings: Configuration** to view and verify the configuration settings for the local network gateway.

ステップ 7 Create the VPN connection from the Azure virtual network gateway to the local network gateway (the on-premises IPsec device).

a) In the Azure portal, navigate to the virtual network gateway page and locate the Azure virtual network gateway that you created in ステップ 5, on page 10.

b) Select the virtual network gateway that you created and click on **Settings: Connections**.

c) Click **Add**.

The **Add connection** window appears.

d) Fill in the necessary information to add this VPN connection from the Azure virtual network gateway to the local network gateway (the on-premises IPsec device).

- In the **Connection type** field, select `Site-to-site (IPsec)`.
- In the **Virtual network gateway** field, select the Azure virtual network gateway that you created in ステップ 5, on page 10.
- In the **Local network gateway** field, select the local network gateway that you created in ステップ 6, on page 11.

- In the **Enable BGP** field, click the checkbox to enable BGP for this connection.
- In the **IKE Protocol** field, select `IKEv2`.

e) Click **OK** when you have finished entering the configuration information for this VPN connection.

ステップ 8 Download the VPN configuration template from Azure.

a) In the Azure portal, navigate to the virtual network gateway page and locate the Azure virtual network gateway that you created in ステップ 5, on page 10.

b) Select the virtual network gateway that you created and click on **Settings: Connections**.

c) Select the name of the VPN connection that you just configured.

The overview page for that VPN connection appears.

d) Click **Download configuration**.

The **Download configuration** page appears.

e) Make the following selections in the **Download configuration** page:

- In the **Device vendor** field, select `Cisco`.
- In the **Device family** field, select `IOS (ISR, ASR)`.
- In the **Firmware version** field, select `15.x (IKEv2)`.

f) Click **Download configuration**.

ステップ 9 Open the downloaded configuration template file in a text editor and make the necessary edits using the instructions in the configuration template.

Typically, the only changes needed in the configuration template are the following fields in the BGP configuration:

- **LOCAL_ROUTE**: Must be the network that needs to be advertised to Azure. For example, using the example configuration in VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成, on page 8, you would enter `192.168.0.0` in this field.
- **LOCAL_MASK**: Must be `255.255.255.0`

ステップ 10 Save and close the edited configuration template.

ステップ 11 Apply the edited configuration template to the on-premises IPsec device.

Following is an example edited configuration template based on the example configuration in VPN ゲートウェイ（仮想ネットワーク ゲートウェイ）を使用した接続の構成, on page 8:

```
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.80.0.0 0.0.0.127
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.80.0.128 0.0.0.127
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.80.1.0 0.0.0.127
access-list 101 permit esp host 52.152.235.192 host 173.39.125.130
access-list 101 permit udp host 52.152.235.192 eq isakmp host 173.39.125.130
access-list 101 permit udp host 52.152.235.192 eq non500-isakmp host 173.39.125.130
!
crypto ikev2 proposal Azure-Ikev2-Proposal
  encryption aes-cbc-256
  integrity sha1
  group 2
  exit
!
```

```
crypto ikev2 policy Azure-Ikev2-Policy
  proposal Azure-Ikev2-Proposal
  match address local 173.39.125.130
  exit
!
crypto ikev2 keyring singaporeisr-keyring
  peer 52.152.235.192
    address 52.152.235.192
    pre-shared-key 0123456789cisco
    exit
  exit

crypto ikev2 profile Azure-Ikev2-Profile
  match address local 173.39.125.130
  match identity remote address 52.152.235.192 255.255.255.255
  authentication remote pre-share
  authentication local pre-share
  lifetime 28800
  dpd 10 5 on-demand
  keyring local singaporeisr-keyring
  exit
!
crypto ipsec transform-set Azure-TransformSet esp-aes 256 esp-sha256-hmac
  mode tunnel
  exit
!
crypto ipsec profile Azure-IPsecProfile
  set transform-set Azure-TransformSet
  set ikev2-profile Azure-Ikev2-Profile
  set security-association lifetime seconds 3600
  ! Note: PFS (perfect-forward-secrecy) is an optional feature (commented out)
  !set pfs None
  exit
!
int tunnel 11
  ip address 169.254.0.1 255.255.255.255
  tunnel mode ipsec ipv4
  ip tcp adjust-mss 1350
  tunnel source 173.39.125.130
  tunnel destination 52.152.235.192
  tunnel protection ipsec profile Azure-IPsecProfile
  exit

interface Loopback 11
  ip address 196.254.0.8 255.255.255.255
  exit
!
router bgp 65150
  bgp log-neighbor-changes
  neighbor 10.80.1.30 remote-as 65515
  neighbor 10.80.1.30 ebgp-multihop 255
  neighbor 10.80.1.30 update-source loopback 11

  address-family ipv4
    network 192.168.0.0 mask 255.255.0.0
    neighbor 10.80.1.30 activate
    exit
  exit
!
ip route 10.80.0.0 255.255.255.128 Tunnel 11
ip route 10.80.0.128 255.255.255.128 Tunnel 11
ip route 10.80.1.0 255.255.255.128 Tunnel 11
ip route 10.80.1.30 255.255.255.255 Tunnel 11
```

ステップ 12 Verify the VPN connections.

a) In the Azure portal, navigate to the virtual network gateway page and locate the Azure virtual network gateway that you created in ステップ 5, on page 10.
b) Select the virtual network gateway that you created and click on **Settings: Connections**.
c) Verify that the VPN connection that you created is shown as `Connected` in the **Status** column.

ステップ 13 Determine if you are deploying the virtual network gateway with or without redirect.

- If you are deploying the virtual network gateway without redirect, go to ステップ 14, on page 15.
- If you deploying the virtual network gateway with redirect, configure the service device for the redirect.

  To configure a service device for redirect using the GUI or REST API, see レイヤ 4 から レイヤ 7 サービスの展開.

ステップ 14 Configure a contract between the cloud EPG and the external EPG connected by the virtual network gateway.

- To create a contract using the GUI, see Cisco Cloud Network Controller GUI を使用したコントラクトの作成.
- To configure a contract using the REST API, see REST API を使用したコントラクトの作成.

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。