Cloud APIC 管理対象クラウド サイトと非 ACI リモートサイト間の接続の構成

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 APIC 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

リリース 5.1(2) 以降では、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 にエクスプレス ルート ゲートウェイを展開可能なエクスプレス ルート ゲートウェイ展開がサポートされています。エクスプレス ルート ゲートウェイは、Cloud APIC 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。

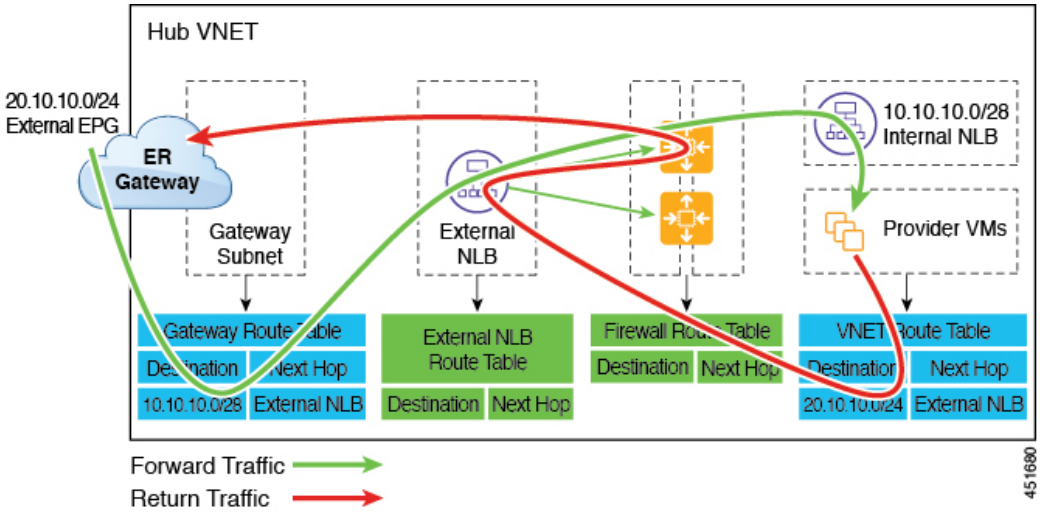
リダイレクトを使用してエクスプレス ルート ゲートウェイを展開することについて

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。

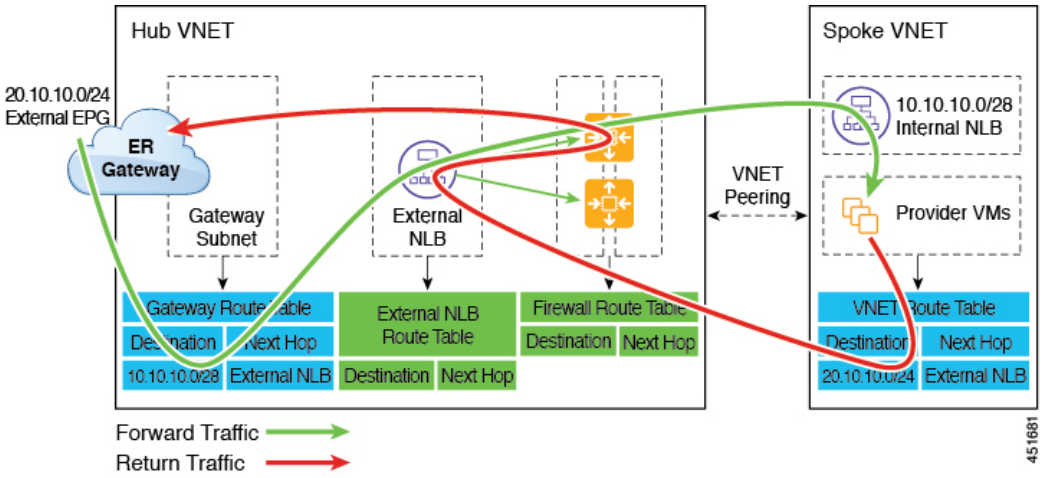
このユース ケースでは、エクスプレス ルート ゲートウェイによって接続された外部 EPG は、ハブまたはスポーク VNet のいずれかでクラウド EPG とコントラクトがあります。このケースから得られた結果を以下に示します。

- リダイレクトは、Cloud APIC 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たエクスプレス 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 （1 ページ） の情報を確認します。

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

これらの手順については、「Azure 用 Cloud APIC の VNET ピアリングの構成」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 Cloud APIC 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 APIC 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 （3 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 （3 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、Cloud APIC 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**Virtual Network Gateway** 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 （3 ページ） で Cloud APIC 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 リダイレクト用のサービス デバイスを構成します。

GUI または REST API を使用してリダイレクトのサービス デバイスを構成するには、レイヤ 4 から レイヤ 7 サービスの展開 を参照してください。

ステップ 5 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 を使用してコントラクトを作成するには、Cisco Cloud APIC 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 を使用してコントラクトを構成するには、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。

リダイレクトなしの Express Route ゲートウェイの展開について

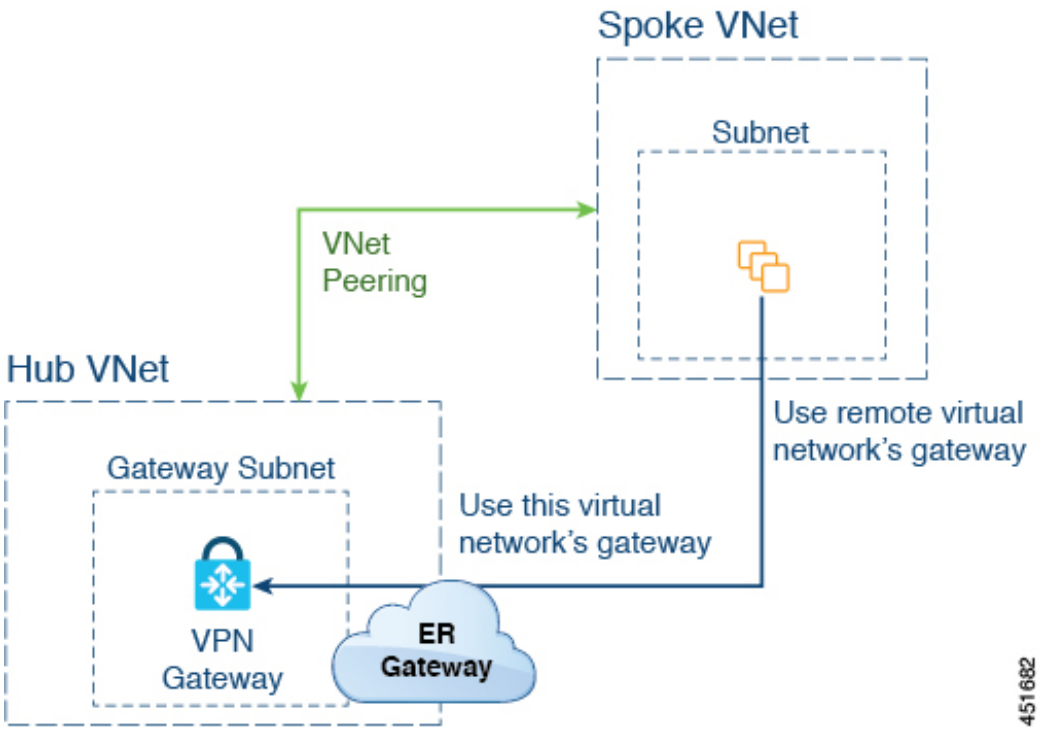
このタイプの展開では、スポーク VNet へのルート伝達が Cloud APIC によって自動的に有効になります。これにより、ゲートウェイ移行を使用した VNet ピアリング（移行ピアリングとも呼ばれます）を使用して、ハブ VNet を介してスポーク VNet で非 ACI リモートサイト サブネット ルートを使用できるようになります。ゲートウェイ トランジットを使用した VNet ピアリングは、この場合 Cloud APIC によって自動的に有効になります。

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。Cloud APIC 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 ポータルで移行ピアリング 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**：Cloud APIC 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、次のようになります。

- 次の構成は、Cloud APIC 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 Cloud APIC 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**：Cloud APIC 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 Cloud APIC で VNet ピアリングを有効にします。

これらの手順については、「Azure 用 Cloud APIC の VNET ピアリングの構成」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 Cloud APIC 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 APIC 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 （7 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 （7 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、Cloud APIC 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**Virtual Network Gateway** 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 （7 ページ） で Cloud APIC 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。

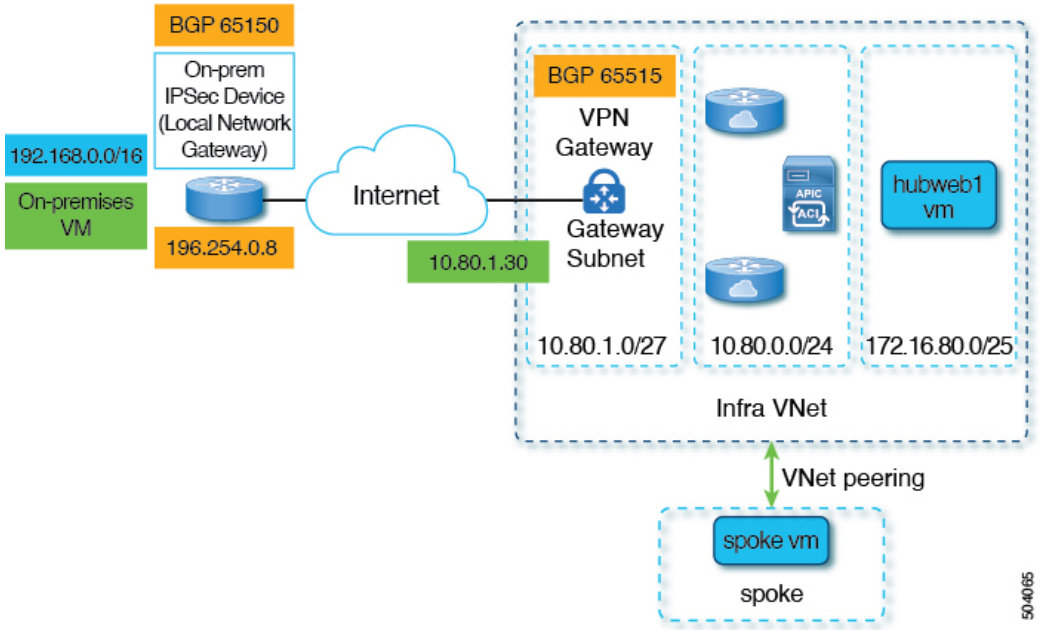
- GUI を使用してコントラクトを作成するには、Cisco Cloud APIC GUI を使用したコントラクトの作成 を参照してください。
- REST API を使用してコントラクトを構成するには、REST API を使用したコントラクトの作成 を参照してください。

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

リリース 25.0(2) 以降、VPN ゲートウェイを使用して、Cloud APIC 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が利用可能になりました。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、Cloud APIC 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。

VPN ゲートウェイを使用した接続の構成

始める前に

これらの手順を続行する前に、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） の情報を確認します。

ステップ 1 必要に応じて、Cloud APIC で VNet ピアリングを有効にします。

これらの手順については、「Azure 用 Cloud APIC の VNET ピアリングの構成」を参照してください。

ステップ 2 VPN ゲートウェイ サブネットの 2 番目のサブネットを追加します。

a) Cloud APIC GUI で、インテント アイコン（）をクリックし、**[クラウド APIC のセットアップ（Cloud APIC Setup）]** を選択します。

b) **[リージョン管理（Region Management）]** エリアで、**[設定の編集（Edit Configuration）]** をクリックします。

c) **[管理するリージョン（Regions to Manage）]** ウィンドウで、**[次へ（Next）]** をクリックします。

[一般接続（General Connectivity）] ウィンドウが表示されます。

d) **[全般（General）]** エリアの **[クラウド ルータのサブネット プール（Subnet Pools for Cloud Routers）]** フィールドで、**[クラウド ルータのサブネット プールの追加（Add Subnet Pool for Cloud Routers）]** をクリックします。

e) VPN ゲートウェイ ルータの 2 番目のサブネットの情報を入力します。

たとえば、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） の構成例を使用して、このフィールドの VPN ゲートウェイ ルータの 2 番目のサブネットに `10.80.1.0/24` を追加します。

f) **[次へ（Next）]** をクリックし、次のページに必要な情報を入力して、**[保存して続行（Save and Continue）]** をクリックします。

[Cloud APIC セットアップ（Cloud APIC Setup）] プロセスが完了すると、Cloud APIC によって VPN ゲートウェイ ルータのサブネットが作成されます。VPN ゲートウェイ ルータのサブネットの構成が Azure に正常にプッシュされたことを確認するには、Azure ポータルの **[サブネット（Subnets）]** ページに移動し、**[GatewaySubnet]** エントリを見つけます。

ステップ 3 インフラでホストされる VRF を作成し、その VRF をサイト外部 EPG に使用します。

親インフラ VNet 内でホストされる VRF があるインフラ ホスト VRF を作成し、次の手順で作成するサイト外部 EPG にその VRF を使用します。

a) Cloud APIC GUI で **[アプリケーション管理（Application Management）]** > > **[VRFs]** に移動します。

b) **[アクション（Actions）]** > **[VRF の作成（Create VRF）]** をクリックします。
[VRF の作成（Create VRF）] ウィンドウが表示されます。

c) このインフラでホストされる VRF の名前を入力し、**[テナントの選択（Select Tenant）]** をクリックし、テナントの **[インフラ（infra）]** を選択して [選択（Select）] をクリックします。

d) 必要に応じて説明を入力し、**[保存（Save）]** をクリックします。

ステップ 4 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 APIC 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 **[VRF]** フィールドで、この外部 EPG 用に作成したインフラ ホスト VRF を選択します。
  - 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。
  - このサイト外部 EPG には、インフラでホストされる VRF を使用します。
  - タイプ **site-external** の外部クラウド EPG を作成します。

ステップ 5 Azure portal を介して、ステップ 2 （9 ページ） で構成した VPN ゲートウェイ サブネットのインフラ VNet に仮想ネットワーク ゲートウェイを作成します。

これらの手順では、オンプレミス サイトから Azure VPN ゲートウェイへの IPsec および BGP 接続を構築します。詳細については、Azure サイトの次の記事を参照してください。

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

a) Azure portal で、仮想ネットワーク ゲートウェイを作成するリソース マネージャ仮想ネットワークに移動して、仮想ネットワーク ゲートウェイを作成します。

b) 左側で、**[リソースの作成（Create a resource）]** を選択し、検索に**Virtual Network Gateway** 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**：仮想ネットワーク 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 タイプ**：**[VPN]** を選択します。
- **VPN タイプ**：**[Route-based]** を選択します。
- **SKU**：**[VpnGw1]** を選択します。
- **世代**：**[Generation1]** を選択します。
- **仮想ネットワーク**：**[overlay-1]** 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。
- **active-active モードを有効にする**：**[無効（Disabled）]** に設定します。
- **BGP の構成**：**[有効（Enabled）]** に設定します。
- **自律システム番号（ASN）**：VPN ゲートウェイの適切な BGP ASN 値を入力します。デフォルトでは、Azure は 65515 の ASN 値を使用します。

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は、完了するまでに最長 45 分かかることがあります。

仮想ネットワーク ゲートウェイが正常に展開されたことを確認するには、[仮想ネットワーク ゲートウェイ（virtual network gateway）] ページに移動して、作成したばかりの仮想ネットワーク ゲートウェイを選択し、**[設定：構成（Settings: Configuration）]** をクリックして、仮想ネットワーク ゲートウェイの構成設定を表示および確認します。

ステップ 6 ローカル ネットワーク ゲートウェイを作成します。

この構成では、ローカル ネットワーク ゲートウェイは、オンプレミスの IPsec デバイスを表すオブジェクトです。ローカル ネットワーク ゲートウェイを作成する前に、次のパラメータを準備します。

- BGP 自律システム番号（ASN）
- パブリック IP アドレス（Public IP address）
- 仮想ネットワーク ゲートウェイにアドバタイズする必要があるオンプレミス サブネットの適切なアドレス スペース

a) Azure portal で、ローカル ネットワーク ゲートウェイを作成する Resource Manager ローカル ネットワークに移動して、ローカル ネットワーク ゲートウェイを作成します。
b) 左側で **[リソースの作成（Create a resource）]** を選択し、検索に「**Local Network Gateway**」と入力します。
c) 検索結果で [ローカル ネットワーク ゲートウェイ] を見つけて、エントリをクリックします。
d) **[ローカル ネットワーク ゲートウェイ（Local network gateway）]** ページで、**[作成（Create）]** を選択します。
e) **[ローカル ネットワーク ゲートウェイの作成（Create local 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。

- **名前**： ローカル ネットワーク ゲートウェイの名前。
- **エンドポイント**：**[IP アドレス（IP address）]** を選択します。
- **IP アドレス**：ローカル ネットワーク ゲートウェイの適切な IP アドレスを入力します。
- **アドレス空間**:アドレス空間に適切な値を入力します。たとえば、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） の構成例を使用して、このフィールドに `192.168.0.0/16` を追加します。
- **BGP 設定の構成**：この設定を有効にするには、チェックボックスをクリックします。
- **自律システム番号（ASN）**： ローカル ネットワーク ゲートウェイの適切な BGP ASN 値を入力します。これは、リモート デバイスの ASN 値です。たとえば、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） の構成例を使用して、このフィールドに `65150` を追加します。
- **BGP ピア IP アドレス**：このフィールドには、オンプレミス デバイスに使用する BGP ピア IP アドレスを入力します（Azure 仮想ネットワーク ゲートウェイではありません）。たとえば、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） の構成例を使用して、このフィールドに `196.254.0.8` を追加します。

- **サブスクリプション**：ステップ 5 （11 ページ）の仮想ネットワーク ゲートウェイに使用したものと同じサブスクリプションを選択します。
- **リソース グループ**：ステップ 5 （11 ページ） の仮想ネットワーク ゲートウェイに使用したのと同じリソース グループを選択します。
- **場所**：ステップ 5 （11 ページ） の仮想ネットワーク ゲートウェイに使用したのと同じ場所（リージョン）を選択します。

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。

ローカル ネットワーク ゲートウェイが正常に展開されたことを確認するには、[ローカル ネットワーク ゲートウェイ（local network gateway）]ページに移動して、作成したばかりのローカル ネットワーク ゲートウェイを選択し、**[設定：構成（Settings: Configuration）]** をクリックして、ローカル ネットワーク ゲートウェイの構成設定を表示および確認します。

ステップ 7 Azure 仮想ネットワーク ゲートウェイからローカル ネットワーク ゲートウェイ（オンプレミスの IPsec デバイス）への VPN 接続を作成します。

a) Azure ポータルで、仮想ネットワーク ゲートウェイのページに移動し、ステップ 5 （11 ページ） で作成した Azure 仮想ネットワーク ゲートウェイを見つけます。

b) 作成した仮想ネットワーク ゲートウェイを選択し、**[設定：接続（Settings: Connections）]** をクリックします。

c) [追加（Add）] をクリックします。

[接続の追加（Add connection）] ウィンドウが開きます。

d) この VPN 接続を Azure 仮想ネットワーク ゲートウェイからローカル ネットワーク ゲートウェイ（オンプレミスの IPsec デバイス）に追加するために必要な情報を入力します。

- **[接続タイプ（Connection type）]** フィールドで、`[サイト間（IPsec）（Site-to-site (IPsec)）]` を選択します。
- **[仮想ネットワーク ゲートウェイ（Virtual network gateway）]** フィールドで、ステップ 5 （11 ページ） で作成した Azure 仮想ネットワーク ゲートウェイを選択します。
- **[ローカル ネットワーク ゲートウェイ（Local network gateway）]** フィールドで、ステップ 6 （12 ページ） で作成したローカル ネットワーク ゲートウェイを選択します。
- **[BGP を有効にする（Enable BGP）]** フィールドでチェックボックスをクリックして、この接続の BGP を有効にします。
- **[IKE プロトコル（IKE Protocol）]** フィールドで、`[IKEv2]` を選択します。

e) この VPN 接続の構成情報の入力が完了したら、**[OK]** をクリックします。

ステップ 8 Azure から VPN 構成テンプレートをダウンロードします。

a) Azure ポータルで、仮想ネットワーク ゲートウェイのページに移動し、ステップ 5 （11 ページ） で作成した Azure 仮想ネットワーク ゲートウェイを見つけます。

b) 作成した仮想ネットワーク ゲートウェイを選択し、**[設定：接続（Settings: Connections）]** をクリックします。

c) 構成した VPN 接続の名前を選択します。

VPN 接続の概要ページが表示されます。

d) **[ダウンロード構成（Download configuration）]** をクリックします。

[ダウンロード構成（Download configuration）] ページが表示されます。

e) **[ダウンロード構成（Download configuration）]** ページで次の選択を行います。

- **[デバイス ベンダー（Device vendor）]** フィールドで、`[Cisco]` を選択します。
- **[デバイス ファミリ（Device family）]** フィールドで、`[IOS (ISR, ASR) ]` を選択します。
- **[ファームウェア バージョン（Firmware version）]** フィールドで、`[15.x (IKEv2)]` を選択します。

f) **[ダウンロード構成（Download configuration）]** をクリックします。

ステップ 9 ダウンロードした構成テンプレート ファイルをテキスト エディタで開き、構成テンプレートの指示に従って必要な編集を行います。

通常、構成テンプレートで必要な変更は、BGP 構成の次のフィールドのみです。

- **LOCAL_ROUTE**：Azure にアドバタイズする必要があるネットワークである必要があります。たとえば、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）の構成例を使用すると、このフィールドに `192.168.0.0` と入力します。
- **LOCAL_MASK**：`255.255.255.0` でなければなりません

ステップ 10 編集した構成テンプレートを保存して閉じます。

ステップ 11 編集した構成テンプレートをオンプレミスの IPsec デバイスに適用します。

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） の構成例に基づいて編集された構成テンプレートの例を次に示します。

```
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 VPN 接続を確認します。

a) Azure ポータルで、仮想ネットワーク ゲートウェイのページに移動し、ステップ 5 （11 ページ） で作成した Azure 仮想ネットワーク ゲートウェイを見つけます。

b) 作成した仮想ネットワーク ゲートウェイを選択し、**[設定：接続（Settings: Connections）]** をクリックします。

c) 作成した VPN 接続が [ステータス（Status）] 列に **[接続済み（Connected）]** と表示されていることを確認します。

ステップ 13 リダイレクトを使用して仮想ネットワーク ゲートウェイを展開するかどうかを決定します。

- リダイレクトなしで仮想ネットワーク ゲートウェイを展開する場合は、ステップ 14 （16 ページ）に進みます。
- リダイレクトを使用して仮想ネットワーク ゲートウェイを展開する場合は、リダイレクト用にサービス デバイスを構成します。

  GUI または REST API を使用してリダイレクト用にサービス デバイスを構成するには、レイヤ 4 から レイヤ 7 サービスの展開 を参照してください。

ステップ 14 クラウド EPG と、仮想ネットワーク ゲートウェイによって接続された外部 EPG との間のコントラクトを構成します。

- GUI を使用してコントラクトを作成するには、Cisco Cloud APIC 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 を使用してコントラクトを構成するには、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。

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。