Cisco Cloud APICおよびGoogle Cloudの概要

リリース25.0(1) 以降、Cisco Cloud APIC で Google Cloud のサポートが利用可能になりました。この章の次のトピックでは、Google Cloud を使用した Cisco Cloud APIC の展開方法について説明します。

- リリース 25.0(1) の変更のサマリー （1 ページ）
- 重要な Google Cloud プロジェクト情報の検索 （2 ページ）
- Cloud APIC での Google Cloud の展開について （2 ページ）
- 外部ネットワーク接続 （4 ページ）
- ルーティング ポリシーとセキュリティ ポリシーの個別の構成 （9 ページ）
- Google Cloud の下の VPC とサブネット、およびクラウド APIC でのクラウドコンテキストプロファイルについて （14 ページ）
- Google Cloud による Cisco Cloud APIC の設定に関するガイドラインと制限事項 （19 ページ）

リリース 25.0(1) の変更のサマリー

次に、リリース 25.0(1) の変更点の概要を示します。

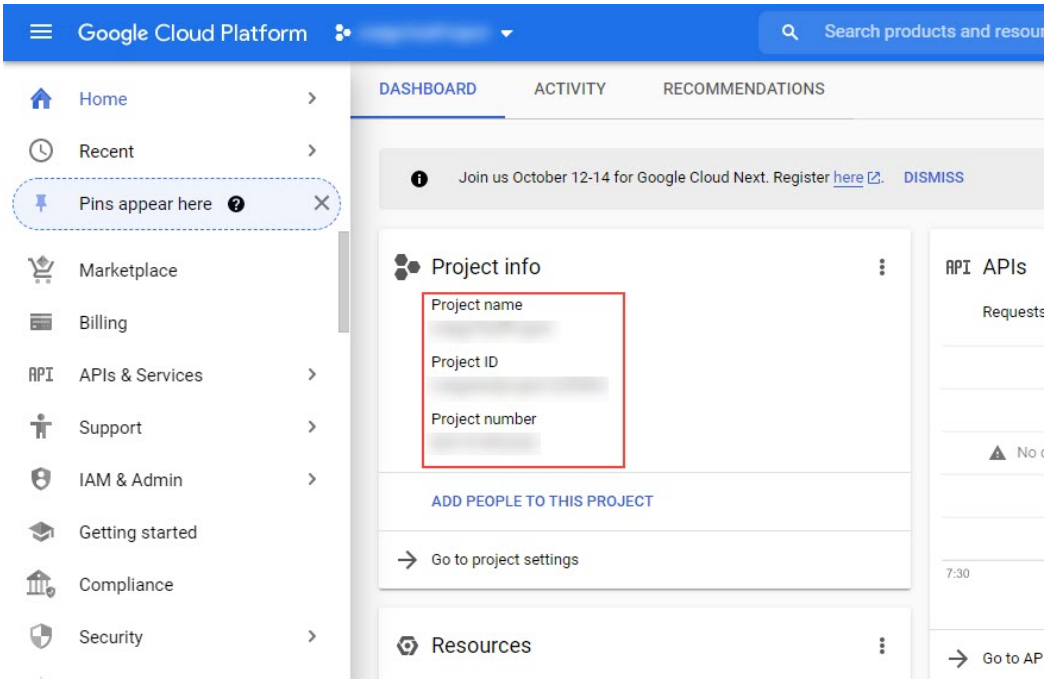
- Cisco Cloud APIC で Google Cloud のサポート。
- Google Cloud から他の外部サイトへの外部接続のサポートが可能です。詳細については、「外部ネットワーク接続 （4 ページ）」を参照してください。
- ルーティングポリシーとセキュリティポリシーの個別設定のサポート。詳細については、「ルーティング ポリシーとセキュリティ ポリシーの個別の構成 （9 ページ）」を参照してください。
  - Cisco Cloud APIC では、ルート マップを使用して、VRF のペア間のセキュリティ ポリシーとは無関係にルーティング ポリシーを設定できます。両方の VRF が内部 VRF であるか、一方の VRF が内部 VRF で、もう一方の VRF が 外部 VRF です。詳細については、「ルーティング ポリシーの設定 （9 ページ）」を参照してください。
  - ファイアウォール ルールを使用したセキュリティ ポリシーの設定のサポート。詳細については、「セキュリティ ポリシーの設定 （10 ページ）」を参照してください。

重要な Google Cloud プロジェクト情報の検索

Google Cloud プロジェクトを作成すると、そのプロジェクトには次の 3 つの固有識別子が割り当てられます。

- プロジェクト名
- プロジェクト ID
- プロジェクト番号

Cisco Cloud APIC 構成プロセスのさまざまな時点で、Google Cloud プロジェクトにこれらの 3 つの識別子が必要になります。これらの Google Cloud プロジェクトIDを含む **[プロジェクト情報（Project Info）]** ペインを見つけるには、Google Cloud アカウントにログインし、**[プロジェクトの選択（Select a Project）]** ウィンドウで特定のGoogle Cloudプロジェクトを選択します。このプロジェクトの **[ダッシュボード（Dashboard）]** が表示され、[プロジェクト情報（Project Info）] ペインに Google Cloud プロジェクトのこれら3つの一意の識別子が表示されます。



Cloud APIC での Google Cloud の展開について

Google Cloud は、ファイル システムに似た方法でリソースを編成します。

- 最上位の組織は複数のフォルダを持つことができます。
- すべてのフォルダには、他のフォルダを含めることも、すべてのプロジェクトに一意の ID があるプロジェクトを含めることもできます。

- クラウド リソース（VM、VPC、サブネットなど）はプロジェクトに含まれます。

組織とフォルダのレベルは、Google Cloud の観点から理解するのに有用な領域ですが、プロジェクトレベルは、Cloud APIC の観点から最も関連性があります。

各 Cloud APIC テナントは Google Cloud プロジェクトに 1 対 1 でマッピングされます。

- Cloud APIC テナントは複数の Google Cloud プロジェクトにまたがることはできません
- Google Cloud プロジェクトに複数の Cloud APIC テナントを含めることはできません

Cloud APIC では、Google Cloud は **サービス アカウント**を使用してプロジェクトにアクセスできます。これらのアカウントは、Google Cloud サービスにアクセスする必要があるアプリケーション用です。これらを使用して、Cloud APIC と他のテナントのポリシーを実行および展開し、プッシュすることができます。Google Cloud 内部で実行されるアプリケーションで使用されるサービスアカウントにはログイン情報は必要ありませんが、事前に生成された秘密キーを必要とする Google Cloud の外部で実行されるアプリケーションにはログイン情報が必要です。サービス アカウントは1つの Google Cloud プロジェクトに存在しますが、他のプロジェクト（Cloud APIC の場合、他のテナント用）のポリシーを管理するためのアクセス権も付与されます。

次の項では、Google Cloud を使用して Cloud APICテナントを設定するさまざまな方法について詳しく説明します。

- 管理対象ログイン情報を持つユーザテナント （3 ページ）
- 管理対象ログイン情報を持つユーザー テナント （4 ページ）

管理対象ログイン情報を持つユーザテナント

このタイプのユーザー テナントには、次の特性があります。

- このテナント アカウントは Cisco Cloud APIC によって管理されます。
- このタイプのユーザーテナントのテナント構成プロセスの一環として、最初に Cisco Cloud APIC GUIで **[管理対象アイデンティティ（Managed Identity）]** を選択します。
- Cisco Cloud APIC で必要なパラメータを構成したら、Google Cloud でこのテナントに必要な権限を設定する必要があります。クラウド APIC によって作成されたサービス アカウントを、次のルールを使用して IAM ユーザーとして追加します。
  - クラウド機能サービス エージェント
  - コンピューティング インスタンス管理（v1）
  - コンピューティング ネットワーク管理
  - コンピューティング セキュリティ管理
  - ロギング管理
  - パブ/サブ管理

- ストレージ管理者

このようなテナントの作成手順については、Google Cloud および Cisco Cloud APIC GUI を使用した管理対象テナントの作成 を参照してください。

管理対象ログイン情報を持つユーザー テナント

このタイプのユーザー テナントには、次の特性があります。

- このテナント アカウントは Cisco Cloud APIC では管理されません。
- このタイプのテナントの Cisco Cloud APIC に必要なパラメータを構成する前に、まず、このテナントに関連付けられたサービス アカウントの Google Cloud から必要な秘密キー情報を含むJSONファイルをダウンロードする必要があります。
- 次に、このタイプのユーザーテナントのテナント構成プロセスの一環として、Cisco Cloud APIC GUI で **[管理対象外アイデンティティ（Unmanaged Identity）]** を選択します。Cisco Cloud APIC でこのタイプのテナントの構成プロセスの一環として、ダウンロードした JSON ファイルから次の情報を提供します。
  - キー ID
  - RSA 秘密キー
  - Client ID
  - Email

このようなテナントの作成手順については、Google Cloud および Cisco Cloud APIC GUI を使用した管理対象外テナントの作成 を参照してください。

外部ネットワーク接続

サポートは、Google Cloud サイトと非Google Cloud サイトまたは外部デバイス間の外部接続に使用できます。この IPv4 接続を確立するには、Google Cloudルータと外部デバイス（CSR を含む）の間に VPN 接続を作成します。

次の項では、リリース 25.0(1) で提供される新しい外部ネットワーク接続を可能にするコンポーネントの詳細について説明します。

外部VRF

外部 VRF は、クラウド内に存在しない一意の VRF です。このVRFは、Cisco Cloud APIC によって使用されるクラウド コンテキスト プロファイルでは参照されません。

外部 VRFは、他のクラウドサイトまたはオンプレミス サイトに接続されている外部ネットワークを表します。複数のクラウド VRF は、外部 VRF にルートをリークしたり、外部 VRF からルートを取得したりできます。外部 VRFで外部ネットワークが作成されると、VRF 間ルーティ

ングが設定され、外部ネットワークで受信およびアドバタイズされたルートが 外部 VRF で受信またはアドバタイズされます。 を参照してください。

クラウド ネイティブ ルータ

Cisco Cloud APIC を Google Cloud で使用して設定すると、インフラ VPC は Google Cloud ネイティブ ルータ（クラウド ルータおよびクラウド VPN ゲートウェイ）を使用して、オンプレミス サイト、他のクラウド サイト、または任意のリモート デバイスへの IPsec トンネルと BGP セッションを作成します。IPv4 セッションが 外部 VRF で作成されているクラウド ネイティブ ルータを使用したこのタイプの接続では、IPv4 接続のみがサポートされます。

Google Cloud は、スタティック ルートと BGP の両方で VPN 接続をサポートします。BGP との VPN 接続を作成するために、Cisco Cloud APIC はクラウド ルータと VPN ゲートウェイの両方が必要です。VPC は複数のクラウド ルータと VPN ゲートウェイを持つことができます。ただし、Google Cloudには、クラウド ルータと VPN ゲートウェイの両方が同じリージョンおよび同じ VPC に存在する必要があるという制限があります。さらに、Cisco Cloud APIC ではリージョンごとに 1 つのクラウド ルータと 1 つのクラウド VPN ゲートウェイのみがサポートされるという制限があります。

VPN 通信

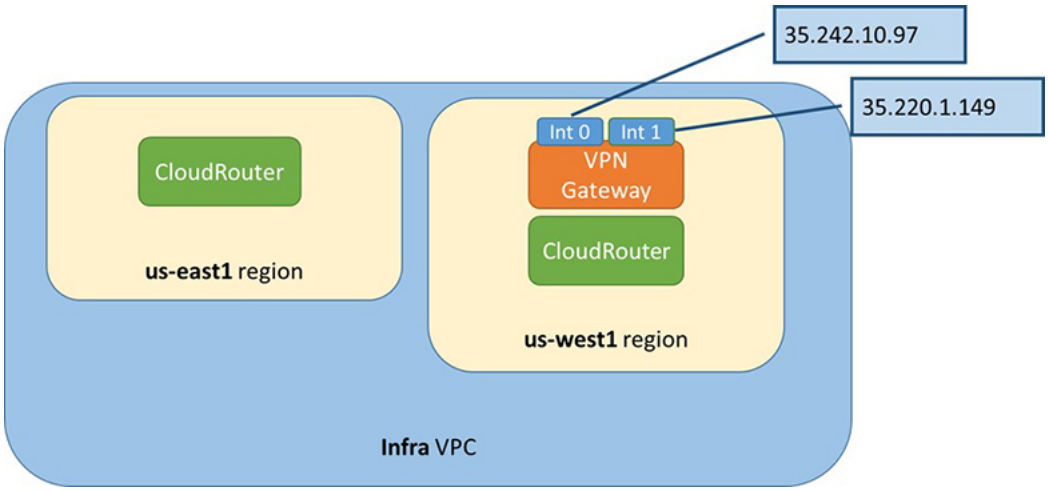
Cisco Cloud APIC を Google Cloud で設定する場合、インフラ VPC を使用して Cisco Cloud APIC をホストし、外部デバイスおよびサイトへの VPN 接続をホストします。ただし、インフラ VPC は、スポーク間通信を実装するための中継として使用されません。代わりに、Cisco Cloud APIC を Google Cloudを使用して設定すると、スポーク間通信はスポーク間 VPC ピアリングによって行われます。

インフラ VPC は、Google Cloud ルータとGoogle Cloud VPN ゲートウェイを使用して、オンプレミス サイトまたは他のクラウド サイトへの IPsec トンネルと BGP セッションを作成します。スポーク VPC は、インフラ VPC とピアリングして、外部サイトへの VPN 接続を共有します。

- VPN 接続で受信したルートがスポーク VPC にリークされる
- スポーク VPC ルートが VPN 接続でアドバタイズされる

VRF 間ルーティングを使用すると、VPN 接続の 外部 VRF とクラウド ローカル スポーク VRF 間でルートがリークされます。

VPN ゲートウェイには 2 つのインターフェイスがあり、Google Cloud は各インターフェイスにパブリック IP アドレスを割り当てます。Google Cloud VPN ゲートウェイは 1 つまたは 2 つのインターフェイスを持つことができますが、ハイアベイラビリティを実現するには2つのインターフェイスが必要であるため、Cisco Cloud APIC は 2 つのインターフェイスを持つ VPN ゲートウェイのみをサポートします。



ハブ ネットワーク構成

リリース 25.0(1) 以降では、スポーク接続に基づいてリージョンにハブ ネットワークを作成するのではなく、`cloudtemplateHubNetworkName` の下の `cloudRegionName` MOが、ハブ ネットワークが展開されるリージョンを表します。ここで、`cloudtemplateHubNetworkName`は Google Cloud ルータを表します。リリース 25.0(1) の場合、Cisco Cloud APIC では 1 つの `cloudtemplateHubNetworkName` の制限があります。

ハブ ネットワークは、外部サイトへの接続を確立する方法を提供します。ハブ ネットワークの作成は、外部ネットワークを作成するための前提条件です。リリース 25.0(1) 以降では、ハブの名前と、ハブ ネットワークを展開するリージョンを指定して、ハブ ネットワークを作成できます。たとえば、ハブ ネットワークを us-central1 と us-east1 に展開することを選択できます。Cisco Cloud APIC はこれらの地域の Google Cloud ルータをプロビジョニングします。作成できるハブ ネットワークは1つだけです。つまり、Cisco Cloud APICではリージョンごとに 1 つのクラウド ルータのみが展開されます。

次の POST は、このモデルを使用したリリース 25.0(1) 以降のネットワーク接続の例を示しています。`cloudtemplateHubNetwork` は、ハブ ネットワークを作成するために使用されます。この例では、ハブ ネットワークは 4 つの地域に展開されています。外部ネットワークは、`cloudtemplateExtNetwork` MOを使用して 4 つのリージョンのそれぞれから作成されます。

```
<polUni>
    <fvTenant name="infra" status="">
        <fvCtx name="extv1" pcEnfPref="enforced" status=""/>
         <fvCtx name="extv2" pcEnfPref="enforced" status=""/>
          <fvCtx name="extv3" pcEnfPref="enforced" status=""/>

           <cloudtemplateInfraNetwork name="default" vrfName="overlay-1"
hostRouterMode="manual" status="">
            <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.7.0/24"
poolname="pool1" />
             <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.8.0/24"
poolname="pool2" />
              <cloudtemplateIpSecTunnelSubnetPool subnetpool= "169.254.10.0/24"
poolname="pool3" />
```

```
            <cloudtemplateHubNetwork name="default" status="" >
                <cloudtemplateHubNetworkName name="foo1" asn="64514" status="">
                    <cloudRegionName provider="gcp" region="us-west4" status="" />
                    <cloudRegionName provider="gcp" region="us-west2" status="" />
                    <cloudRegionName provider="gcp" region="us-east1" status="" />
                      <cloudRegionName provider="gcp" region="us-west1" status=""/>
                </cloudtemplateHubNetworkName>
            </cloudtemplateHubNetwork>

            <cloudtemplateIntNetwork name="default">
                <cloudRegionName provider="gcp" region="us-west1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-west2">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
                <cloudRegionName provider="gcp" region="us-east1">
                    <cloudtemplateVpnRouter name="default" status=""/>
                  </cloudRegionName>
                    <cloudRegionName provider="gcp" region="us-west4">
                    <cloudtemplateVpnRouter name="default" status=""/>
                </cloudRegionName>
            </cloudtemplateIntNetwork>

            <cloudtemplateExtNetwork name="default">
            </cloudtemplateExtNetwork>
               <cloudtemplateExtNetwork name="extnwfoo1" vrfName="extv1"
hubNetworkName="foo1" vpnRouterName="default" status="">
                    <cloudRegionName provider="gcp" region="us-west1" status=""/>
                   <cloudtemplateVpnNetwork name="onprem01" remoteSiteId="1" status="">

                    <cloudtemplateIpSecTunnel peeraddr="128.1.1.1" preSharedKey="abcd"
poolname="pool1" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529"
status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
          <cloudtemplateExtNetwork name="extnwfoo2" vrfName="extv2" hubNetworkName="foo1"
 vpnRouterName="default" status="">
             <cloudRegionName provider="gcp" region="us-west2" status=""/>
                <cloudtemplateVpnNetwork name="onprem02" remoteSiteId="2" status="">
                      <cloudtemplateIpSecTunnel peeraddr="128.1.1.2" preSharedKey="def"
 poolname="pool2" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529"
status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
            </cloudtemplateExtNetwork>
             <cloudtemplateExtNetwork name="extnwfoo3" vrfName="extv3"
hubNetworkName="foo1" vpnRouterName="default" status="">
                <cloudRegionName provider="gcp" region="us-east1" status=""/>
                   <cloudtemplateVpnNetwork name="onprem03" remoteSiteId="3" status="">
                      <cloudtemplateIpSecTunnel peeraddr="128.1.1.3" preSharedKey="abc"
 poolname="pool3" status="">
                        <cloudtemplateBgpIpv4 peeraddr="0.0.0.0/0" peerasn="64529"
status=""/>
                    </cloudtemplateIpSecTunnel>
                </cloudtemplateVpnNetwork>
                  </cloudtemplateExtNetwork>
        </cloudtemplateInfraNetwork>
    </fvTenant>
</polUni>
```

この POST の例：

- **cloudtemplateExtNetwork**：複数の cloudtemplateExtNetwork エントリを持つことができ、それぞれが一意の名前を持ち、外部 VRF 上の外部ネットワークを表します。

  cloudtemplateExtNetwork エリアには、次のフィールドがあります。

  - **vrfName**：このプロパティは、外部ネットワークに使用される VRF（トランスポート VRF など）を表します。複数のリモート サイトで同じトランスポート VRF を使用できます。つまり、これらのリモート サイトはすべてクラウド上で 1 つの VRF として扱われ、すべてのリモート サイトがクラウドから同じルートを受信します。

  - **hubNetworkName**：このプロパティは、この外部ネットワークで使用されるハブ ネットワークの名前を表します。この名前は、cloudtemplateHubNetworkName 領域で作成されたハブ ネットワークの 1 つを参照します。

  - **vpnRouterName**：このプロパティは、この外部ネットワークで使用される VPN ルータの名前を表します。この名前は、cloudtemplateVpnRouter によって作成された VPN ルータを参照します。

  また、外部ネットワークは複数のリージョンに展開でき、外部ネットワークで使用されるルータはそれらのリージョンに展開する必要があります（つまり、hubNetworkName と vpnRouterName はそれらのリージョンに存在する必要があります）。

- **cloudtemplateVpnNetwork**：このMOはリモートサイトを表します。

  cloudtemplateVpnNetwork エリア内に **remoteSiteId** フィールドがあります。このプロパティは、リモート サイト ID を表します。

- **cloudtemplateVpnRouter**：この MO は Google CloudVPN ゲートウェイに変換されます。リリース 25.0(1) では、名前がdefault の 1 つの cloudtemplateVpnRouter のみが許可されます。

- **cloudtemplateIpSecTunnel**：この MO はリモート ピアを表します。

- **cloudtemplateBgpIpv4**：この MO はリモート サイトの IPv4 BGP ピアを表します。

  cloudtemplateBgpIpv4 の下の peeraddr エントリにデフォルト アドレス（0.0.0.0/0）がある場合、リモート BGP ピアはリモート デバイスのトンネルの内部アドレスであると見なされます。

上記のモデルは次をサポートしていることに注意してください。

- 外部デバイスへの ikev1 と ikev2 の両方。
- 複数の cloudtemplateIpSecTunnelSubnetPool サブネット プール。
  cloudtemplateIpSecTunnelSubnetPool サブネット プールで許可されるIP範囲は、クラウド プロバイダーと使用例によって異なります。たとえば、169.254.0.0 / 16 以下のサブネットが Google Cloud VPN接続でサポートされます。

ルーティングポリシーとセキュリティポリシーの個別の構成

異なるVRFの2つのエンドポイント間の通信を許可するには、ルーティング ポリシーとセキュリティ ポリシーを別々に確立する必要があります。

- **ルーティング ポリシー**：トラフィック フローを確立するルートを定義するために使用されるポリシー
- **セキュリティ ポリシー**：ゾーン分割ルール、セキュリティ グループ ルール、ACL など、セキュリティ目的で使用されるルール

Google Cloudの場合、ルーティングはセキュリティとは無関係に設定する必要があります。つまり、Google Cloudの場合、「契約」はセキュリティのためだけに使用されます。ルーティングを構成するには、ルートマップを構成する必要があります。

ルーティング ポリシーの設定

VRF 間ルーティングを使用すると、独立したルーティング ポリシーを設定して、VRF のペア間でリークするルートを指定できます。ルーティングを確立するには、VRFのペア間にルートマップを設定する必要があります。

ルート マップを使用して、VRF のペア間でリークするルートを設定できる状況では、VRF 間ルーティングに次のタイプの VRF が使用されます。

- **外部VRF** は、1 つ以上の外部ネットワークに関連付けられている VRF です。
- **内部 VRF** は、1 つ以上のクラウド コンテキスト プロファイルまたはクラウド サブネットが関連付けられているVRFです。

次のタイプの VRF で VRF 間ルーティングを設定する場合：

- 内部 VRF のペア間では、常にすべてのルートをリークする必要があります。
- 内部 VRF から外部 VRF へ、特定のルートまたはすべてのルートをリークできます。
- 外部 VRF から内部 VRF に、すべてのルートをリークする必要があります。

注意事項および制約事項

VRF 間ルーティングを使用してルートマップを使用して VRF ペア間のルートをリークする場合は、次の注意事項が適用されます。

- ルートは常に 2 つの VRF 間で双方向にリークされます。あるテナント/VRF から別のテナント/VRF へのルート リーク エントリごとに、対応するルート リーク エントリが反対方向に存在する必要があります。

たとえば、2 つのテナント（t1とt2）と 2 つの対応する VRF（v1 とv2）があるとします。VRF t2:v2 のすべてのルート リーク エントリ t1:v1 に対して、VRF t1:v1 の対応するルート リーク エントリ t2:v2 が必要です。

- 外部 VRF を外部ネットワークに関連付けた後、外部 VRF を変更する場合は、外部ネットワークを削除してから、新しい外部 VRF で外部ネットワークを再作成する必要があります。
- 「より大きな」プレフィックスがすでにリークされている間に、「より小さな」プレフィックスをリークするように設定することはできません。たとえば、10.10.0.0/16 プレフィックスがすでにリークされるように設定されている場合、10.10.10.0/24 プレフィックスの設定は拒否されます。同様に、0.0.0.0/0（すべてリーク）プレフィックスを設定した場合、他のプレフィックスは設定できません。

セキュリティ ポリシーの設定

Cisco Cloud APIC の EPG は AWS と Azure のセキュリティ グループに対応しますが、EPGに対する Google Cloud の対応コンポーネントはありません。Google Cloud で最も近いものは、ファイアウォール ルールとネットワーク タグの組み合わせです。

Google Cloudのファイアウォール リソースは、プロジェクト（テナント）に対してグローバルです。ファイアウォール ルールは単一の VPC に関連付けられ、その範囲は VPC 全体にグローバルに適用されます。ファイアウォール ルールの範囲は、Target パラメータによってさらに定義されます。つまり、ルールが適用されるインスタンスのセットは、次の 1 つ以上のターゲット タイプによって選択できます。

- **ネットワーク タグ**：ネットワークタグは、Google Cloudの VM のファイアウォールとルーティング設定を制御するキー文字列です。インスタンス（VM など）は、一意の文字列でタグ付けできます。ファイアウォール ルールは、等しいタグを持つすべてのインスタンスに適用されます。複数のタグ値は論理「or」演算子として機能し、少なくとも 1 つのタグが一致する限りファイアウォール ルールが適用されます。
- **ネットワーク内のすべてのインスタンス**：ファイアウォールルールは VPC 内のすべてのインスタンスに適用されます。

ファイアウォール ルールは、トラフィックの送信元と宛先も識別します。ルールが入力トラフィック（VM に向かう）または出力トラフィック（VM を離れる）のどちらであるかによって、送信元フィールドと宛先フィールドの値は異なります。次のリストに、これらの値の詳細を示します。

- **入力ルール**：
  - **ソース**：次を使用して識別できます。
    - ネットワーク タグ
    - IP アドレス
    - 論理「or」演算子を使用した IP アドレスとネットワーク タグの組み合わせ

- **宛先**：Target パラメータは、宛先インスタンスを識別します。

- **出力ルール**：
  - **送信元**：Target パラメータは、送信元インスタンスを識別します。
  - **宛先**：IP アドレスのみを使用して識別できます（ネットワーク タグは使用できません）。

Cisco Cloud APIC が Google Cloud を使用したファイアウォールルールの実装方法

次のリストは、Cisco Cloud APIC の Google Cloud を使用したファイアウォールルールの実装方法を示しています。

- **グローバル リソース**：Google Cloud の VPC とファイアウォールはグローバル リソースであるため、Cisco Cloud APIC は複数のリージョンにまたがるエンドポイントのファイアウォール ルールをプログラムする必要はありません。エンドポイントが存在するすべてのリージョンに同じファイアウォール ルールが適用されます。
- **ファイアウォール出力ルールとネットワーク タグ**：ファイアウォール出力ルールは、宛先フィールドとしてネットワーク タグをサポートしていないため、エンドポイントの個々の IP アドレスをリストする必要があります。
- **ファイアウォール入力ルールおよびエイリアス IP 範囲の送信元タグ**：ファイアウォール入力ルールには、送信元フィールドで使用されるネットワークタグに一致する VM のエイリアス IP 範囲は含まれません。
- **ファイアウォール ルールの優先度フィールド**：Google Cloud は優先度の値に従ってファイアウォール ルールを評価します。

Google Cloud ファイアウォール ルールがプライオリティ リストの後に続く場合、Cisco Cloud APIC は VPC の作成時に、低プライオリティの deny-all 入力ルールと出力ルールのペアを設定します。その後、Cisco Cloud APIC は EPG の優先度の高いコントラクトに従ってトラフィックを開くルールを設定します。したがって、EPGコントラクトの結果として特定のトラフィックを許可する明示的なルールがない場合は、優先順位の低いルールが一致し、デフォルトの動作はdeny-allになります。

エンドポイントおよびエンドポイント セレクタ

Cisco Cloud APICでは、クラウドEPGは、同じセキュリティ ポリシーを共有するエンドポイントの集合です。クラウドEPGは、1つまたは複数のサブネット内にエンドポイントを持つことができ、VRF に関連付けられます。

Cisco Cloud APIC には、エンドポイントをクラウドEPGに割り当てるために使用される、エンドポイント セレクタと呼ばれる機能があります。エンドポイント セレクタは、基本的に言って、Cisco ACI によって管理される Google Cloud VPC に割り当てられたクラウド インスタンスに対して実行される一連のルールです。エンドポイントインスタンスに一致するエンドポイント セレクタ ルールは、そのエンドポイントをクラウドEPGに割り当てます。エンドポイント

セレクタは、 Cisco ACI で使用可能な属性ベースのマイクロ セグメンテーションに似ています。

次に、2 種類のクラウド EPG で使用可能なエンドポイント セレクタのタイプを示します。

- **アプリケーション EPG**：
  - **IP**): IP アドレスまたはサブネットによって選択するために使用されます。
  - **リージョン**: エンドポイントのリージョンで選択するために使用されます。
  - **カスタム**：カスタム タグまたはラベルで選択するために使用されます。たとえば、Google Cloud のロケーション タグを追加する場合、Google Cloud で以前に追加したロケーション タグと一致するこのフィールドにカスタム タグのロケーションを作成できます。
- **外部 EPG**：

  サブネット：サブネット セレクタはエンドポイント セレクタのタイプで、一致表現ではサブネットの IP アドレスが使用されるため、サブネット全体が EPG の一部として割り当てられます。基本的に、サブネット セレクタをエンドポイント セレクタとして使用する場合、そのサブネット内のすべてのエンドポイントは関連付けられたEPGに属します。

Google Cloud で Cisco Cloud APIC エンドポイント セレクタを使用する場合、Google Cloudの一致する VM に EPG を関連付けるネットワーク タグが適用されます。ネットワーク タグが VM で設定されると、Google Cloud は VM のトラフィックにファイアウォール ルールが適用されます。

Google Cloud 上の VM もラベルをサポートします。ラベルは、組織的なツールとなるキーと値のペアです。Cisco Cloud APIC のカスタムエンドポイントセレクタは、Google Cloud のVMに割り当てられたラベルを認識します。

Cisco Cloud APIC は、EPG ごとに一意のネットワーク タグ文字列を予約します。Google Cloud では、この値が EPG 用に作成されたファイアウォール ルールのターゲット フィールドとして使用されます。新しいVMがEPGのエンドポイント セレクタに一致すると、Cisco Cloud APIC はこの値を既存の VM のネットワーク タグに追加します。さらに、EPG のネットワークタグは、Google Cloudファイアウォール ルールの送信元フィールドで使用されます。

たとえば、次の設定例について考えます。

```
<cloudEPg  name="epg1" >
    <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
    <fvRsProv tnVzBrCPName="httpSSHFamily"/>
    <cloudEPSelector name="web-selector" matchExpression="custom:server=='web'"/>
    <cloudEPSelector name="web-selector" matchExpression="custom:server==backend"/>
</cloudEPg>
<cloudEPg  name="epg2" status="">
    <cloudRsCloudEPgCtx tnFvCtxName="v1"/>
    <fvRsCons tnVzBrCPName="httpSSHFamily"/>
   <cloudEPSelector name="database-selector" matchExpression="custom:server=='database'"/>
</cloudEPg>
```

次の設定の VPC に 3 つのエンドポイントがあると仮定すると、Cisco Cloud APIC は次のネットワーク タグを設定します。Cisco Cloud APIC-configured ネットワーク タグは次の形式です。

```
capic-<app-profile-name>-<epg-name>
```

エンドポイント	アプリケーション プロファイル	EPG	Primary IP	ラベル	クラウド APIC で設定されたネットワーク タグ
EP1	最初のアプリケーション プロファイル（app01）	最初の EPG（epg01）	10.0.0.1	server:web	capic-app01-epg01
EP2	2 番目のアプリケーション プロファイル（app02）	2 番目の EPG（epg02）	20.0.0.1	server:backend	capic-app02-epg02
EP3	2 番目のアプリケーション プロファイル（app02）	3 番目の EPG（epg03）	30.0.0.1	server:database	capic-app02-epg03

Cisco Cloud APIC がネットワーク タグを設定するには、VMに対する管理者権限が必要です。この権限は、コンピューティング インスタンス管理者ロールによって付与されます。

Cisco Cloud APIC にこの権限がなく、VM のタグを管理できない場合があります。これらのシナリオでは、最初にVMでネットワークタグを設定し、その後で Cisco Cloud APIC に適切なエンドポイント セレクタ設定を指定できます。

ファイアウォール ルールを確認するには：

- **Google Cloud**内：Google Cloud アカウントで、**[VPC ネットワーク（VPC Network）]** > **[ファイアウォール（Firewall）]**に移動します。
  - VM が EPG の一部である場合は、ファイアウォール ルールを展開し、**[フィルタ（Filters）]** 列に表示される複数のエントリを表示することで、エンドポイントを検索できます。
  - **[タイプ（Type）]** 列のエントリを使用して、特定のファイアウォール ルールが入力ファイアウォール ルールか出力ファイアウォール ルールかを判別します。
    - ファイアウォール ルールが入力タイプの場合、トラフィックはこれらのエンドポイントに送信されます。
    - ファイアウォール ルールが出力タイプの場合、これらのエントリはトラフィックを受信できる場所を示します。

- **Cisco Cloud APIC**内：ファイアウォールルールはVPCに関連付けられているため、**[クラウド リソース（Cloud Resources）]** > **[VPC]**に移動し、VPC をダブルクリックして詳細画面を表示します。次に、**[クラウド リソース（Cloud Resources）]** タブをクリックします。入力ルールと出力ルールが表示されます。

Google Cloud の下の VPC とサブネット、およびクラウド APIC でのクラウドコンテキストプロファイルについて

Google Cloud では、VPC はグローバル リソースですが、サブネットはリージョン内にあり、リージョン内のすべてのアベイラビリティ ゾーンにまたがっていますが、同じ VPC またはピア VPC 内の他のサブネットと重複することはできません。

各サブネットには、プライマリ CIDR ブロック（IP 範囲）が 1 つだけ必要で、最大 30 個のセカンダリ CIDR ブロックを含めることができます。VPC には最大 300 のプライマリおよびセカンダリ CIDR を設定できます。各 VM の NIC はプライマリ CIDR ブロックからプライマリ内部 IP アドレスを取得しますが、セカンダリ IP 範囲は**エイリアス IP 範囲**にのみ使用できます。これは、VM 内で実行されているコンテナまたはアプリケーションにアドレス プールを割り当てるための Google Cloud 組織的なツールです。

次に、Cisco Cloud APIC オブジェクトと Google Cloud オブジェクト間の関連付けについて詳しく説明します。

- **Google Cloud VPC からCisco Cloud APIC VRF への 1 対 1 のマッピング**：Google CloudVPC が各Cisco Cloud APICVRF（`fvCtx` オブジェクト）に展開されます。クラウド コンテキスト プロファイル（`cloudCtxProfile`オブジェクト）は、展開するリージョン サブネットのセットを定義します。同じ VRF 内のすべてのクラウド コンテキスト プロファイルは、同じ VPC にマッピングされます。
- **Google Cloudサブネットとそのセカンダリ IP 範囲**：Cisco Cloud APIC は Cisco Cloud APICCIDR とサブネット オブジェクトを使用して、プライマリおよびセカンダリ IP 範囲でサブネットを展開します。Cisco Cloud APIC サブネット オブジェクトは IP 範囲を表すために使用され、Cisco Cloud APIC CIDR のプライマリ プロパティはプライマリまたはセカンダリかどうかを示します。セカンダリ Cisco Cloud APIC サブネット オブジェクトは、対応するプライマリ サブネット オブジェクトに関連付けられます。これは、Google Cloud だけが実際のサブネットを展開するためです。

VPC グループについて

クラウド コンテキスト プロファイルは Cisco Cloud APIC 内で VPC のマッピング ツールとして使用され、1 つのクラウド コンテキスト プロファイルが 1 つの VPC に関連付けられます。クラウド コンテキスト プロファイルには、リージョンの関連付けに関する情報も含まれます。クラウド コンテキスト プロファイルは、VPC が展開されるリージョンを決定するために使用されます。

Google Cloudでは、VPC を作成するときに、複数のリージョンにサブネットを展開する場合は、複数のクラウド コンテキスト プロファイルを Cisco Cloud APIC を通じて作成する必要があります。ただし、VPC は Google Cloud で本質的にグローバルであり、VPC はすべてのリージョンにまたがっています。

したがって、**VPC グループ**（vpcGroup）と呼ばれるプロパティは、Cisco Cloud APIC が複数のクラウド コンテキスト プロファイルをグループ化して 1 つの VPC を形成できるクラウド コンテキスト プロファイル内で使用できます。Google Cloud 内VPC グループ機能を使用して相互に関連付けられた複数のクラウド コンテキスト プロファイルは、Google Cloud でVPC グループ名が表示されているVPC構造を形成します。

リリース 25.0(1) では 1 つの Google Cloud VRF 内で1つの Cisco Cloud APIC VPC のみが許可されるため、VRF にリストされている各クラウド コンテキスト プロファイルの VPC グループ プロパティに同じ名前を使用する必要があります。同じ VPC グループ名を持つプロファイルは、同じ VPC に存在します。

この照合メカニズムの範囲はテナント レベルです。同じ値をテナント間で再利用できますが、異なるGoogle Cloudプロジェクトの一部であるため、異なるグループを暗黙的に定義します。

Cisco Cloud APIC は少なくとも1つのcloudSubnetが定義されている限り、fvCtx、cloudRsToCtx、および vpcGroup の各タプルに対して VPC を展開します。クラウド コンテキスト プロファイルは、VRF に関連付けられたサブネットなどのリージョン リソースのコンテナになり、VPC にマッピングされなくなります。

次の例では、1 つの VPC グループ（vpc-1）を持つ同じ VRF（v1）内の 2 つのコンテキストプロファイル（c1 と c2）を定義します。この設定では、プロファイル c1 と c2 で定義されたサブネットが同じ VPC グループの一部であるため、1 つの VPC を展開します。

```
<fvTenant name="t1">
    <fvCtx name="v1"/>
    <cloudCtxProfile name="c1" vpcGroup="vpc-1">
        <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1" />
        <cloudRsToCtx tnFvCtxName="v1"/>
        <cloudCidr addr="10.0.0.0/16" primary="yes" >
            <cloudSubnet ip="10.0.1.0/24">
                <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
            </cloudSubnet>
        </cloudCidr>
    </cloudCtxProfile>
    <cloudCtxProfile name="c2" vpcGroup="vpc-1">
        <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-east1" />
        <cloudRsToCtx tnFvCtxName="v1"/>
        <cloudCidr addr="20.0.0.0/16" primary="yes" >
            <cloudSubnet ip="20.0.1.0/24">
                <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-east1/zone-default"/>
            </cloudSubnet>
        </cloudCidr>
    </cloudCtxProfile>
</fvTenant>
```

プライマリおよびセカンダリ サブネットとサブネット グループについて

Cisco Cloud APIC は cloudRsCtxProfileToRegion 関係が指すリージョンの VPC（タプル fvCtx、cloudRsToCtx、および vpcGroup によって識別される）内のすべてのサブネット（cloudSubnet）を展開します。

Google Cloudでは、VPC の**プライマリ** CIDR の概念はありませんが、クラウド コンテキスト プロファイルの CIDR（cloudCidr）フィールドのプライマリ フラグは、セカンダリ IP 範囲をサポートするために Cisco Cloud APIC を使用できます。プライマリ CIDR で設定されたすべてのサブネットは、指定されたプライマリ IP 範囲（プライマリ サブネット）の実際の Google Cloud サブネットとして展開されます。Google Cloud のリリース 25.0(1) では、特定のクラウド コンテキスト プロファイル（cloudCtxProfile）で複数の CIDR をプライマリとして設定できます。したがって、複数のプライマリ サブネットを持つ特定のクラウド コンテキスト プロファイルの下に、複数のプライマリ CIDR を設定できます。

次の POST は、1 つの VPC と 3 つのサブネットが Google Cloud で展開されている例を示しています。

```
<polUni>
    <fvTenant name="t1">
        <fvCtx name="v1"/>
        <cloudCtxProfile name="c1" vpcGroup="vpc-1">
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1" />
            <cloudRsToCtx tnFvCtxName="v1"/>
            <cloudCidr addr="10.0.0.0/16" primary="yes" >
                <cloudSubnet ip="10.0.1.0/24">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="10.0.2.0/24">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr addr="20.0.0.0/16" primary="yes" >
                <cloudSubnet ip="20.0.1.0/24">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
</polUni>
```

上記の例では、1 つの VPC v1 が、us-west リージョンに展開された 3 つのプライマリサブネット（10.0.1.0/24、10.0.2.0/24、および 20.0.1.0/24）で設定されています。

セカンダリ CIDR には、既存のプライマリ サブネットで設定されているセカンダリ IP 範囲（セカンダリ サブネットと呼ばれる）が含まれます。CIDR をプライマリまたはセカンダリとして指定する場合は、次の 2 つの違いを考慮すると役立ちます。

- 通常、プライマリ CIDR は VM です。
- セカンダリ CIDR は、アプリケーションに使用されるコンテナです。

プライマリ サブネットとセカンダリ サブネットを 1 つの**サブネット グループ**にグループ化できます。このグループ化メカニズムは、実際の Google Cloud サブネットにマッピングされたプ

ライマリ サブネットにセカンダリ サブネット（IP 範囲など）を割り当てます。サブネット グループの範囲は、クラウド コンテキスト プロファイル レベルです。同じテナント内に複数のクラウド コンテキスト プロファイルを持つことができますが、サブネットは同じクラウド コンテキスト プロファイル内のサブネット グループにのみ属します。

サブネット グループ ラベルを使用して、特定のサブネット グループに一意のラベルを割り当てます。同じサブネット グループ ラベルを持つ複数のサブネットがある場合、それらがすべて同じクラウド コンテキスト プロファイル内にある限り、それらのサブネットはすべて同じサブネット グループに属します。サブネット グループ ラベルは Cisco Cloud APIC 内でプライマリ サブネットとセカンダリサブネットをグループ化するために使用されますが、Google Cloud では使用されません。

プライマリおよびセカンダリ CIDR に関する次のガイドラインに注意してください。

- **プライマリ CIDR**：
  - サブネット グループは、プライマリ CIDR から最大 1 つのサブネットのみを持つことができます。
  - プライマリ CIDR には複数のサブネットを含めることができますが、すべてのサブネットを別のサブネット グループに含める必要があります。
- **セカンダリ CIDR**：同じサブネット グループにセカンダリ CIDR の複数のサブネットを設定できます。

次の POST は、それぞれが異なるリージョンにあり、セカンダリCIDRを持つ 2 つのサブネットを持つ 2 つの VPC が Google Cloud で展開されている例を示しています。

```
<polUni>
    <fvTenant name="t1">
        <fvCtx name="v1"/>
        <fvCtx name="v2"/>
        <cloudCtxProfile name="c1" vpcGroup="vpc-1">
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-west1" />
            <cloudRsToCtx tnFvCtxName="v1"/>
            <cloudCidr addr="10.0.0.0/16" primary="yes" >
                <cloudSubnet ip="10.0.1.0/24" subnetGroup="subnet-1">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="10.0.2.0/24" subnetGroup="subnet-2">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr addr="40.0.0.0/16" primary="no">
                <cloudSubnet ip="40.0.1.0/24" subnetGroup="subnet-1">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-west1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
        <cloudCtxProfile name="c2" vpcGroup="vpc-2">
            <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-gcp/region-us-east1" />
            <cloudRsToCtx tnFvCtxName="v2"/>
            <cloudCidr addr="20.0.0.0/16" primary="yes">
```

```
                <cloudSubnet ip="20.0.1.0/24" subnetGroup="subnet-1">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-east1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
            <cloudCidr addr="30.0.0.0/16" primary="no">
                <cloudSubnet ip="30.0.1.0/24" subnetGroup="subnet-1">
                    <cloudRsZoneAttach
tDn="uni/clouddomp/provp-gcp/region-us-east1/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
    </fvTenant>
</polUni>
```

クラウド コンテキスト プロファイル c2 のサブネット グループ subnet-1 は、クラウド コンテキスト プロファイル c1 のサブネット グループとは異なります。これは、サブネット グループの範囲がクラウド コンテキスト プロファイル レベルにあるためです。

上記の例の目的は次のとおりです。

- テナント t1 は VRF v1 および v2 を定義します。
- クラウド コンテキスト プロファイルc1は、VRF v1 および VPC グループ vpc-1 のリージョンus-west1のサブネットを定義します。これにより、VPC vpc-1 が展開されます。
- クラウド コンテキストプロファイル c2 は、VRF v2 および VPC グループ vpc-2 のリージョン us-east1 のサブネットを定義します。これにより、VPC vpc-2 が展開されます。
- 次のサブネットは、リージョン us-west1 の VPC vpc-1 に展開されます。
  - サブネット-1 サブネット グループ：
    - プライマリ IP 範囲：10.0.1.0/24
    - セカンダリ IP 範囲：40.0.1.0/24
  - サブネット 2 サブネット グループ：
    - プライマリ IP 範囲：10.0.2.0/24
- 次のサブネットは、リージョン us-east1 の VPC vpc-2 に展開されます。
  - サブネット1：
    - プライマリ IP 範囲：20.0.1.0/24
    - セカンダリ IP 範囲：30.0.1.0/24

Google Cloud による Cisco Cloud APIC の設定に関するガイドラインと制限事項

Google Cloud で Cisco Cloud APIC を設定する際の注意事項と制約事項を次に示します。

- Google Cloud は、コントラクトに基づくルーティングをサポートしていません。
- 2 つの Google Cloud サイト間の外部接続は、リリース 25.0(1) ではサポートされていません。
- 外部 VRF は、Cisco Cloud APIC のインフラテナントでのみ設定できます。
- Cisco Cloud APIC に共通するテナントは、どの Google Cloud プロジェクトにも関連付けることができません。
- Inでは、インフラVPCとスポークVPCはVPCピアリングを介して接続されます。Google Cloud
- リリース 25.0(1) では、オンプレミス データセンターとパブリック クラウド間の接続を設定するには、外部デバイス設定ファイルをダウンロードし、Google Cloud と外部デバイス間の接続を手動で有効にすることによって、リモートデバイスを手動で設定する必要があります。

  ダウンロードする外部デバイス設定ファイルは、最終設定ではありません。代わりに、外部デバイス設定ファイルがガイダンスとして提供されます。Google Cloud ルータを IPSec で設定するには、設定ファイルの情報を手動で変更する必要があります。これは、オンプレミスのデータ センターとパブリック クラウド間の接続を確立するために使用されます。

  - Google Cloud ルータとトンネルは、インフラ（ハブ）VPC に導入されます。
  - リリース 25.0(1) では、リージョンごとに 1 つのクラウド ルータがサポートされます。クラウド ルータは、最大 4 つのリージョンに展開できます。
  - スポーク VPC は、インフラ VPC とピアリングして、オンプレミス データセンターなどの外部サイトへの VPN 接続を共有します。

Google Cloud ファイアウォール ルールによる命名の長さの制限

Google Cloud ファイアウォール ルールは名前付きリソースであり、Cisco Cloud APIC は内部ポリシーから名前を取得し、それを使用して Google Cloud ファイアウォール ルールを展開します。Cisco Cloud APICは内部ポリシーに次の命名規則を使用します。

```
{VPC-name}-{in/eg}-{target App-name}-{target EPG-name}-{contract-name}
```

ファイアウォールルール名の最大長は62文字です。Google Cloudこれにより、Google Cloudファイアウォール ルール名で名前が使用される次の Cisco Cloud APIC コンポーネントを設定するときに使用できる名前が制限されます。

- VPC グループ

- アプリケーション プロファイル
- アプリケーション EPG または 外部 EPG
- コントラクト

Google Cloudファイアウォール ルール名の最大文字数が 62 であることを認識し、Google Cloud ファイアウォール ルール名を構成する文字列の固定領域を考慮します。

- ハイフン（合計 4 文字）
- `in` (ingress) または `eg` (egress) の値（2 文字）

つまり、すべての個々の Cisco Cloud APIC コンポーネントを組み合わせた名前に使用できる文字の合計数は56文字を超えることはできません。

62 - 4 (ハイフンの数) - 2 (`in` または `eg` 文字数) = 56 文字

したがって、VPC グループ、アプリケーション プロファイル、アプリケーション EPG または外部 EPG、およびコントラクトの名前の長さの合計は、56 文字未満である必要があります。平均すると、各コンポーネントの名前には約 14 文字を使用できます。