レイヤ 4 から レイヤ 7 サービスの展開

概要

Cisco Cloud APIC を使用すると、レイヤ 4 からレイヤ 7 のサービス デバイスをパブリック クラウドに展開できます。初期リリース (4.2(x)) では、Azure での Azure Application Gateway（アプリケーション ロード バランサ）の展開がサポートされています。リリース 5.0(2) 以降、Azure での Azure Load Balancer（ネットワーク ロード バランサ）およびサード パーティ ファイアウォールの展開がサポートされています。リリース 5.1(2) 以降、Azure でのサード パーティ ロード バランサの展開がサポートされています。

Azure での展開では、次の 4 種類のレイヤ 4 からレイヤ 7 サービスがサポートされています。

- ALB は、Azure アプリケーション ゲートウェイまたはアプリケーション ロード バランサを指します。
- NLB は Azure ロード バランサまたはネットワーク ロード バランサを指します。
- サードパーティ ファイアウォール
- サードパーティ ロード バランサ

サービス グラフについて

サービス グラフは、2 つ以上の EPG ペア間に挿入された一連のレイヤ 4 ～ レイヤ 7 サービス デバイスを表すために使用されます。EPG は、クラウド（Cloud EPG など）またはインターネット（cloudExtEPG）内で実行されているアプリケーション、または他のサイト（オンプレ

ミスまたはリモート クラウド サイトなど）から実行されているアプリケーションを表すことができます。レイヤ 4 からレイヤ 7 のサービス デバイスは、NLB、ALB、サード パーティのファイアウォールのクラスタ、またはサード パーティのロード バランサにすることができます。

サービス グラフと契約（およびフィルタ）は、2 つの EPG 間の通信を指定するために使用されます。Cisco Cloud Network Controller は、契約およびサービス グラフで指定されたポリシーに基づいて、セキュリティ ルール（ネットワーク セキュリティ グループ/NSG および ASG）と転送ルート（UDR）を自動的に導出します。

複数のサービス グラフを指定して、さまざまなトラフィック フローまたはトポロジを表すことができます。

サービス グラフでは、次の組み合わせが可能です。

- 同じデバイスを複数のサービス グラフで使用できます。
- 複数のコンシューマ EPG とプロバイダ EPG の間で同じサービス グラフを使用できます。

サービス グラフを使用することで、ユーザーはポリシーを一度指定するだけで、リージョン内またはリージョン間でサービス チェーンを展開できます。グラフを展開するたびに、Cisco ACI は新しい論理トポロジでの転送を行えるように、ネットワーク構成の変更を行います。

サードパーティのファイアウォールの場合、デバイス内の構成は Cisco Cloud Network Controller によって管理されません。

サービス グラフは、次の要素を使ってネットワークを表します。

- サービス グラフ ノード：ロードバランサなどのトラフィックに適用される機能を示すノード。サービス グラフ内の 1 つの機能は 1 つ以上のパラメータを必要とし、1 つまたは複数のコネクタを持っている場合があります。
- コネクタ：コネクタはノードからの入出力を有効にします。

グラフが設定されると、Cisco APIC はサービス グラフに明記されたサービス機能の要件に従って、サービスを自動的に設定します。Cisco APIC もまた、サービス グラフで指定されるサービス機能のニーズに応じてネットワークを自動的に設定します。これにより、サービス デバイスを変更する必要がなくなります。

クラウド ネイティブおよびサードパーティ サービスでのサービス グラフの使用

リリース 5.1(2) 以降、クラウド ネイティブおよびサードパーティのサービスでサービス グラフを使用できるようになりました。これらの状況では、リダイレクトの有無にかかわらずサービス グラフを使用できます。リダイレクトの有無にかかわらず使用例については クラウド ネイティブおよびサードパーティ サービスによるサービス グラフの使用例 （34 ページ） を参照してください。

このタイプのサービス グラフでは、同じくリリース 5.1(2) で導入されたクラウド サービス エンドポイント グループ（サービス EPG）を使用します。サービス EPG、およびサービス EPG で使用できる展開タイプとアクセス タイプの詳細については、クラウド サービス エンドポイント グループ を参照してください。

この目的でサービス EPG で使用されるサービス グラフでは、次の展開タイプとアクセス タイプがサポートされています。

表 *1:* プロバイダ サービスの *EPG* タイプ

導入タイプ	アクセス タイプ
クラウドネイティブ	プライベート
クラウド ネイティブ管理対象	パブリックとプライベート
サードパーティ製の	プライベート

表 *2:* コンシューマ サービス *EPG* タイプ

導入タイプ	アクセス タイプ
クラウド ネイティブ管理対象	パブリックとプライベート

注意事項と制約事項

- サービス EPG を使用して、クラウド ネイティブおよびサードパーティ サービスでサービス グラフを使用するには、新しいサブネットごとの NSG 構成を有効にする必要があります。サブネットごとの NSG 構成の詳細については、セキュリティ グループ を参照してください。
- クラウド EPG とサービス グラフの組み合わせに適用される制限は、サービス EPG とサービス グラフの組み合わせにも適用されます。たとえば、タグベースのコンシューマとプロバイダが同じリージョンの同じ VRF に存在できないというクラウド EPG/サービス グラフの制限は、サービス EPG とサービス グラフにも適用されます。
- リダイレクトを実行しない 2 つのノード グラフでは、SNAT と DNAT が有効になっています。DNATed アドレスはロードバランサと同等のデバイスであると想定されており、異なるサブネットにある可能性のある異なるターゲット間でトラフィックを分散させることができます。

  これらのターゲットが異なるサブネットにある場合、サービス グラフはそれらのターゲットのルート到達可能性ルールを提供しないことに注意してください。この場合、サービス EPG が到達可能性を処理すると想定されます。
- AKS とサービス グラフが関係する場合、サービス グラフは、AKS クラスタのロードバランサのサブネットへのルートの到達可能性のみを確立します。

アプリケーション ロード バランサの概要

アプリケーション ロード バランサ（Azure Application Gateway または ALB とも呼ばれます）は、HTTP リクエスト、URL フィルタリングなどの属性に基づいて Web トラフィックを分散

するレイヤ 7 ロード バランサです。 詳細については、『Microsoft マニュアル』を参照してください。

Cisco ACI では、2 つのアプリケーション ロード バランサを展開する方法があります。

- インターネット向け：アプリケーション ロード バランサを、コンシューマ外部 EPG とプロバイダ クラウド EPG の間のサービスとして挿入します。
- 内部向け：アプリケーションロードバランサを、コンシューマ クラウド EPG とプロバイダ クラウド EPG 間のサービスとして挿入します。

サービス グラフを使用してアプリケーション ロード バランサを使用できます。一般的な構成には次のものが含まれます。

- アプリケーション ロード バランサとしてのレイヤ 4 からレイヤ 7 サービス デバイスの作成
- サービス グラフのノードとして ALB を使用する
- サービス グラフが契約に関連付けられている場合、EPG 通信での 1 つ以上のリスナーの作成。

リスナーを使用すると、アプリケーション ロード バランサ がトラフィックを受け入れるポートとプロトコル（HTTP または HTTPS）を指定できます。HTTPS を指定する場合は、セキュリティ ポリシーと SSL 証明書も選択します。

（注） リスナーは複数の証明書をもつことができます。

すべてのリスナーで、少なくとも 1 つのルール (条件のないデフォルトのルール) を構成する必要があります。ルールを使用すると、条件が満たされたときにロードバランサが実行するアクションを指定できます。たとえば、指定されたホスト名またはパスへの要求が行われたときに、トラフィックを指定された URL にリダイレクトするルールを作成できます。

アプリケーション ロード バランサ（ALB）は、他のアプリケーションの展開に使用しない別のサブネットに配置する必要があります。Cloud APIC は、ALB の NSG を作成し、ALB に関連付けられたサブネットに接続します。Cloud APIC は Azure アプリケーション ゲートウェイの標準および Standard_v2 SKUs をサポートします。

ネットワーク ロード バランサについて

ネットワーク ロード バランサ（Azure ロード バランサまたは NLB）は、レイヤ 4 ポートに基づいてインバウンド フロー パケットを分散するレイヤ 4 デバイスです。詳細については、『Microsoft マニュアル』を参照してください。

ALB と同様に、NLB はサービス グラフを使用して展開できます。1 以上のリスナーを構成することで、これらのアクションを指定できます。

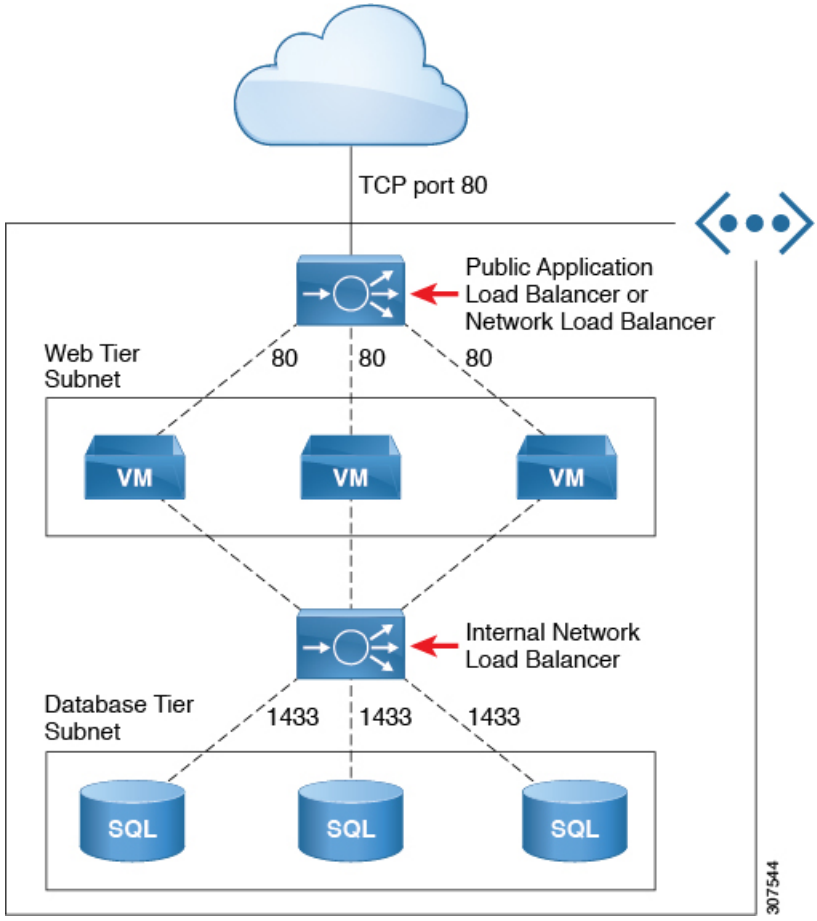
リスナーでは、ロードバランサがトラフィックを受け入れて転送するポートおよびプロトコル（TCP または UDP）を指定できます。すべてのリスナーで、少なくとも 1 つのルール (条件のないデフォルトのルール) を構成する必要があります。ルールを使用すると、条件が満たされたときにロードバランサが実行するアクションを指定できます。アプリケーション ゲートウェイとは異なり、ここではルールはバックエンドプールの特定のポートにのみトラフィックを転送できます。NLB は ALB と同様に別のサブネットにある必要があります。ネットワーク ロード バランサには、次の 2 つの動作モードがあります。

- 転送モード：トラフィックは、特定のリスナー ポートから指定されたバックエンド ポートに転送されます。
- HA ポート モード：ネットワーク ロード バランサは、すべてのポートで TCP フローと UDP フローを同時に負荷分散します。

Cloud APIC は、標準 SKU ネットワーク ロード バランサのみをサポートしています。

図 1 では、フロントエンド ロード バランサ（ALB/NLB）- VM またはファイアウォール - バックエンド ロード（ALB/NLB）バランサがサービスとして、コンシューマの外部 EPG とプロバイダのクラウド EPG の間に挿入されます。

図 *1*：インターネットおよび内部向け展開



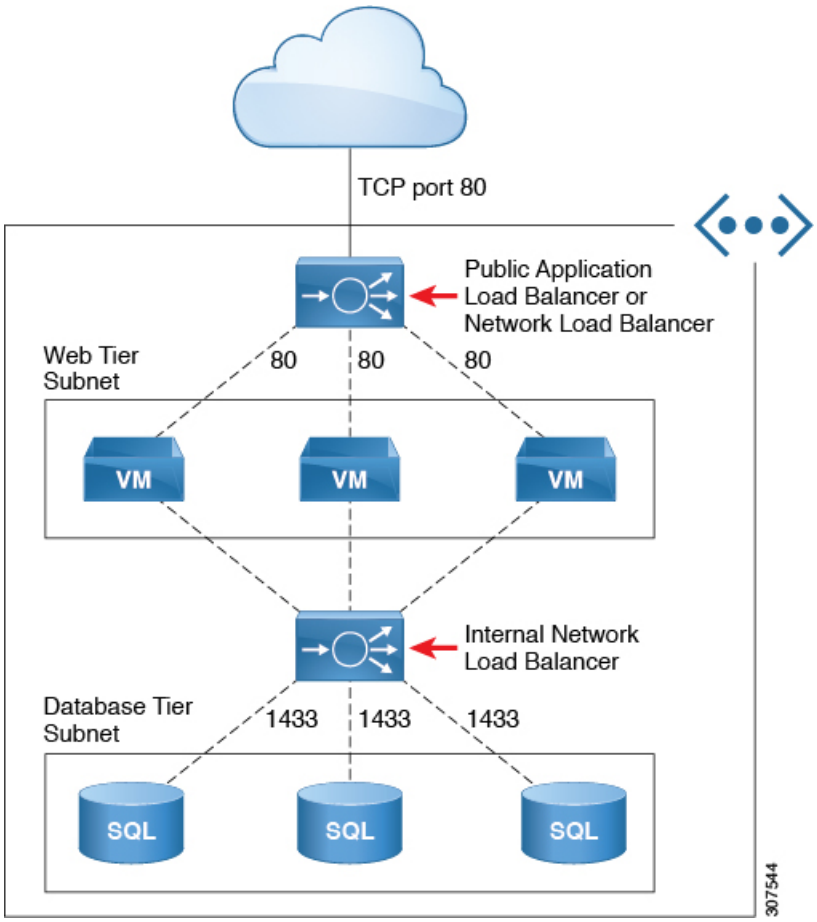
Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について

次のセクションでは、Cisco Cloud APIC リリース 25.0(3) 以降で使用できる Azure Network Load Balancer での複数のフロントエンド IP アドレスのサポートに関する情報を提供します。

Azure Network Load Balancer の複数のフロントエンド IP アドレスについて

インターネット向けのネットワーク ロード バランサを構成する場合、インターネット トラフィックのフロントエンドに割り当てることができるパブリック IP アドレスの数は、リリースによって異なります。

- Cisco Cloud APIC リリース 25.0(3) より前では、インターネット向けのネットワーク ロード バランサには、インターネット トラフィックのフロントエンドに割り当てられた単一のパブリック IP アドレスがあります。次の図は、マルチノード サービス グラフ構成の例を示しています。インターネット向けのネットワーク ロード バランサがグラフィックの上部に表示され、その後に VM またはファイアウォールが表示され、次に内部向けのネットワーク ロード バランサがこのマルチノード サービス グラフの一部として表示されます。

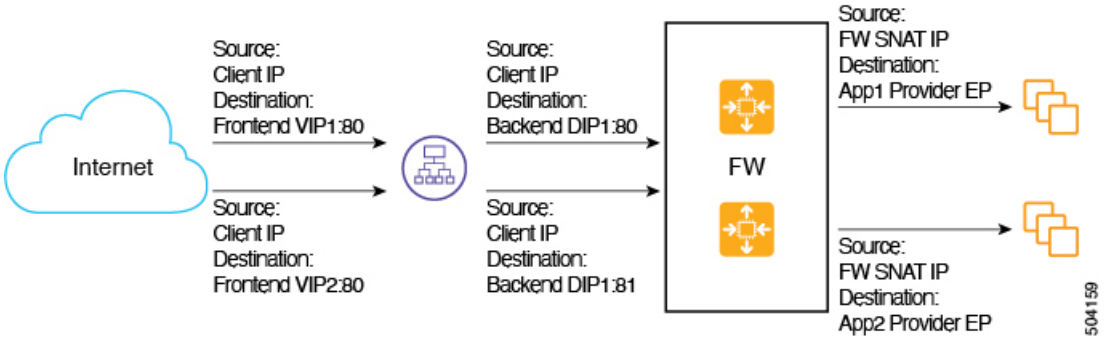


この例では、インターネット向けのネットワーク ロード バランサには、インターネット トラフィックのフロントエンドに割り当てられた単一のパブリック IP アドレスがあります。

ただし、この構成では、サービス グラフがあり、複数の HTTPS サービスを公開する必要がある場合に問題が発生する可能性があります。インターネット向けネットワーク ロード バランサのインターネット トラフィックのフロントエンドに割り当てられる単一のパブリック IP アドレスに制限があるということは、そのネットワーク ロード バランサにフロントエンド IP アドレスを追加できないことを意味します。さらに、Azure の制限により、複数のネットワーク ロード バランサが同じバックエンド デバイス（この例ではファイアウォール）を共有できないため、この状況ではネットワーク ロード バランサを追加できません。

- Cisco Cloud APIC リリース 25.0(3) 以降、インターネットに接続するネットワーク ロード バランサの複数のフロントエンド IP アドレスを構成するためのサポートが利用できるようになりました。この更新により、各フロントエンド IP アドレスは、特定のバックエンド プールに対する 1 つ以上のルールにアタッチされます。

  次の図は、インターネットに接続するネットワーク ロード バランサに対して複数のフロントエンド IP アドレスが構成されている構成例を示しています。



この構成例は、次のリスナー ルールのパケット フローを示しています。

	リスナー ルール（フロントエンド構成）	ルール アクション（バックエンド構成）
Rule1	• **IP**: VIP1 • **Port**: 80	**Port**: 80
Rule2	• **IP**: VIP2 • **Port**: 80	**Port**: 81

サービス グラフでは、サービス デバイスでのリスナー ルールとルール アクションの設定を構成できます。ネットワーク ロード バランサで定義されている場合、リスナー ルールとルール アクションの設定は、ロードバランサのフロントエンド構成からバックエンドプールへのマッピングを構築します。Cisco Cloud APIC リリース 25.0(3) より前は、インターネット向けのネットワーク ロード バランサは、単一のフロントエンド IP アドレスを使用してリスナーを構成する機能を提供していましたが、ポートとプロトコルの組み合わせは異なりました。Cisco Cloud APIC リリース 25.0(3) 以降では、インターネットに接続するネットワーク ロード バランサの複数のフロントエンド IP アドレス構成がサポートされ、その機能が拡張されて、各フロントエンドがフロントエンド IP アドレス、ポート、およびプロトコルのタプルの組み合わせとして示される複数のフロントエンドでリスナー ルールが構成可能です。

注意事項と制約事項

インターネット向けのネットワーク ロード バランサに複数のフロントエンド IP アドレスを構成するためのサポートに関するガイドラインと制限を次に示します。

- 複数のフロントエンド IP アドレスのサポートは、インターネット向けのネットワーク ロード バランサでのみ使用できます。
- 複数のリスナー ルールでのバックエンド ポートの再利用はサポートされていません。

サードパーティのロードバランサについて

サードパーティ ロード バランサは、非クラウド ネイティブのレイヤ 4 からレイヤ 7 のロード バランサです。Cloud APIC は、サードパーティのロード バランサの構成を管理しません。ただし、Cloud APIC は、サードパーティのロード バランサへの接続のためのネットワーク スティッチングを自動化します。

外部インターフェイス サブネットからサード パーティのロード バランサの VIP を構成できます。サード パーティのロード バランサ用の追加の VIP を、外部インターフェイスのセカンダリ IP アドレスとして構成することもできます。

Cloud APIC は、ソース NAT が有効になっている 2 アーム モード（外部インターフェースと内部インターフェース）で展開されたサードパーティのロードバランサをサポートしています。

サードパーティ ロード バランサの制限事項：

- Cloud APIC は、サードパーティのロード バランサでの Direct Server Return（DSR）構成をサポートしていません。
- サードパーティのロードバランサは、active/standby の高可用性構成ではサポートされていません。

  active/active モードのサードパーティ ロード バランサ VM の詳細については、ユースケースの例 （16 ページ） を参照してください。
- エイリアン VIP 範囲は、サードパーティのロードバランサではサポートされていません。

すべてのトラフィックを許可について

リリース 5.1(2g) 以降、**[すべてのトラフィックを許可（Allow All Traffic）]** オプションは、リダイレクト対応のサービス グラフでパススルー デバイスとして展開されたサード パーティ ファイアウォールおよび Azure network load balancers で使用できます。

（注） このオプションは、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスを許可します。このオプションを有効にする前に、これがセキュリティ リスクとならないことを確認します。

次のセクションでは、**[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にする手順について説明します。

- サードパーティ ファイアウォール （9 ページ）
- Azure Network Load Balancer （11 ページ）

サードパーティ ファイアウォール

- 新しいサービス グラフ タイプを作成するときにこのオプションを有効にするには：

1. **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]**>**[デバイス（Devices）]**>**[デバイスの作成（Create Device）]**をクリックします。
2. **[サービス タイプ（Service Type）]** として **[サード パーティ ファイアウォール（Third party firewall）]** を選択します。
3. **[インターフェイスの追加（Add Interface）]** をクリックし、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域を見つけます。
4. **[すべてのトラフィックを許可（Allow All Traffic）]** 領域の **[許可（Enabled）]** フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスを許可します。
5. 設定が終わったら [Save] をクリックします。

- 既存のサービス グラフ タイプを編集するときにこのオプションを有効にするには:

1. **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]** をクリックし、**[デバイス タイプ（Device Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** が表示されている既存のサービス デバイスをクリックします。

   このサービス デバイス タイプの詳細を示すパネルがウィンドウの右側からスライドします。
2. [詳細（Details）] アイコンをクリックします（  ）。

   このサービスデバイスタイプの詳細情報を提供する別のウィンドウが表示されます。
3. ウィンドウの **[インターフェイス（Interfaces）]** 領域を見つけ、**[インターフェイス セレクタ（Interface Selectors）]** 列で必要なインターフェイス セレクタをクリックします。

   このインターフェースの詳細を示すパネルが、ウィンドウの右側からスライドして表示されます。
4. [詳細（Details）] アイコンをクリックします（  ）。

   このインターフェイスの詳細情報を提供する別のウィンドウが表示されます。
5. 鉛筆アイコンをクリックして、このインターフェイスの構成設定を編集します。
6. **[すべてのトラフィックを許可（Allow All Traffic）]** 領域を見つけ、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域の **[許可（Enabled）]** フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスを許可します。
7. 設定が終わったら [Save] をクリックします。

Azure Network Load Balancer

- 新しいサービス グラフ タイプを作成するときにこのオプションを有効にするには:

  1. **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]**>**[デバイス（Devices）]**>**[デバイスの作成（Create Device）]**をクリックします。
  2. **[サービス タイプ（Service Type）]**として **[Network Load Balancer]** を選択します。
  3. **[設定（Settings）]** 領域で、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域の **[有効（Enabled）]** フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスを許可します。
  4. 設定が終わったら [Save] をクリックします。

- 既存のサービス グラフ タイプを編集するときにこのオプションを有効にするには:

  1. **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]** をクリックし、**[デバイス タイプ（Device Type）]** として **[Network Load Balancer]** が表示されている既存のサービス デバイスをクリックします。

     このサービス デバイス タイプの詳細を示すパネルがウィンドウの右側からスライドします。

  2. [詳細（Details）] アイコンをクリックします（  ）。

     このサービスデバイス タイプの詳細情報を提供する別のウィンドウが表示されます。
  3. 鉛筆アイコンをクリックして、このサービス デバイスの構成設定を編集します。
  4. **[設定（Settings）]** 領域で、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域を見つけ、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域の **[有効（Enabled）]** フィールドの横にあるボックスをクリックして、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスを許可します。
  5. 設定が終わったら [Save] をクリックします。

サーバー プールへのダイナミック サーバーのアタッチ

プロバイダ EPG 内のサーバ、または ALB/NLB の背後にあるサードパーティ ファイアウォールなどのサービスデバイスは、ターゲット グループに動的に追加されます。Azure では、ターゲット グループはバックエンド プールとして参照されます。フロントエンドとバックエンドのプロトコルとポート番号、および負荷分散アクションを定義するリスナーとルール構成は、ユーザーによって提供されます。サービス グラフ構成の一部として最後のノードである ALB/NLB でリスナー ルールを構成する場合、特定のルールに対してプロバイダ EPG を選択できます。その EPG からのエンドポイントは、ロード バランサのターゲット グループに動的に追加され

ます。サードパーティ ファイアウォールなどの別のノードが ALB/NLB とプロバイダ EPG の間に存在する場合、ファイアウォール エンドポイントはロード バランサのターゲット グループに動的に追加されます。ターゲットのエンドポイントまたはFQDNを指定する必要はありません。

Azure リリース 25.0(2) の Cisco Cloud APIC より前は、VM スケール セットはロード バランサのバックエンド ターゲットとしてサポートされていませんでした。Azure リリース 25.0(2) の Cisco Cloud APIC は、バックエンド ターゲットとして VM スケール セットを追加します。

（注） ファイアウォールに VM スケール セットを使用する場合は、ファイアウォール インターフェイスにサブネット ベースの EP セレクタのみを使用します。Azure は、複数のインターフェイスを持つ VM スケール セットの NIC ごとのタグ付けをサポートしていません。

VNet 間サービスについて

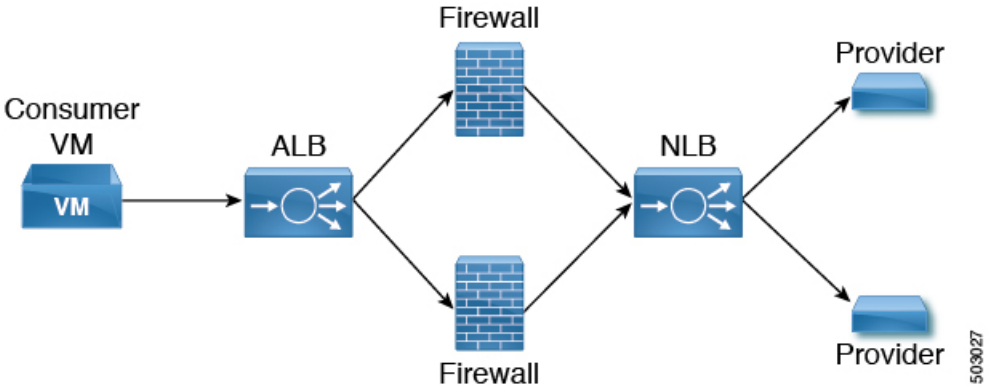
リリース 5.0(2) 以降、VNet 間サービスの展開と自動化がサポートされています。これは、クラウド内の East-West と North-South の両方のユース ケースに当てはまります。

このサポートについては、以下の点に注意してください。

- VNet ピアリングは、ハブスポーク トポロジ用に構成する必要があります。詳細については、「Azure 向け Cloud APIC の VNet ピアリングを構成する」を参照してください。
  - リダイレクトを使用したマルチノード サービスの場合: サービス デバイスがインフラ VNet に存在する必要があります。プロバイダの前にある ALB などのサービス デバイスは、プロバイダ VNet に存在できます。
  - リダイレクトのないマルチノード サービスの場合：サービス デバイスは、プロバイダ VNet 内にあるか、ハブ VNet とプロバイダ VNet にまたがって分散することができます。
- VNet 間トラフィックは、インフラ VNet のアプリケーション ロード バランサまたはネットワーク ロード バランサ、および非インフラ VNet のプロバイダでサポートされます。VNet は相互にピアリングする必要があり、ロード バランサとプロバイダは同じリージョンからのものである必要があります。

マルチノードについて

リリース 5.0(2) 以降、マルチノード サービス グラフがサポートされています。マルチノードにより、サービス グラフを使用した複数の展開シナリオが可能になります。



展開可能なサービス デバイスは、アプリケーション ロード バランサ、ネットワーク ロード バランサ、およびサードパーティ ファイアウォールです。

グラフには 2 種類のノードが許可されます。

- 非リダイレクト: トラフィックはサービス デバイスに向けられます（ロード バランサ、DNAT と SNAT を備えたサードパーティ ファイアウォール、ネットワーク ロード バランサ）。
- リダイレクト：サービス デバイスはパススルー デバイス（ネットワーク ロード バランサまたはファイアウォール）です。

レイヤ 4 ～レイヤ 7 サービス リダイレクト

リリース 5.0(2) 以降、レイヤ 4 からレイヤ 7 へのサービス リダイレクト機能は、Cisco Cloud APIC で使用できます。これは、Cisco APIC で使用可能なポリシーベースのリダイレクト（PBR）機能と同様です。レイヤ 4 からレイヤ 7 へのサービス リダイレクト機能は、Cisco Cloud APIC の **[リダイレクト（Redirect）]** オプションを使用して設定されます。

（注） このセクション全体で、「コンシューマからプロバイダへ」という用語は、ポイント A からポイント B に向かうトラフィックを表す包括的な用語として使用されることがあり、これらの 2 つのポイントの間にリダイレクト サービス デバイスが挿入される場合があります。ただし、これは、コンシューマからプロバイダへのトラフィックのみがリダイレクトでサポートされるという意味ではありません。トラフィックは、スポークツースポーク （19 ページ） で説明されているユース ケースのように、プロバイダからコンシューマへの場合もあります。

リダイレクトでは、ポリシーを使用して特定のサービス デバイス経由でトラフィックをリダイレクトします。サービス デバイスは、ネットワーク ロード バランサまたはサードパーティのファイアウォールとして展開できます。このトラフィックは、標準のコンシューマからプロバイダへの構成の一部として、必ずしもサービス デバイスを宛先とするものではありません。むしろ、通常どおりにコンシューマからプロバイダへのトラフィックを構成し、そのコンシュー

マからプロバイダへのトラフィックを特定のサービスデバイスにリダイレクトするようにサービス グラフを構成します。

Cisco Cloud APIC のリダイレクトのサポートは、VNet ピアリングで使用されるハブ アンド スポーク トポロジを利用して、VNet ピアリング機能と組み合わせてのみ利用できます。VNet ピアリング機能の詳細については、『Configuring VNet Peering for Cloud APIC for Azure』ドキュメントを参照してください。

パススルー ルール

リダイレクトを有効にすると、サービス デバイスにアタッチされている NSG（ネットワーク セキュリティ グループ）のルールが更新され、コンシューマからプロバイダへのトラフィックが許可されます。これらのルールは「パススルー ルール」と呼ばれます。一般に、パススルー ルールは、コンシューマ IP からプロバイダ IP へのトラフィックを許可することです。宛先 IP がアプリケーション ロード バランサ（ALB）VIP の場合、ルールはコンシューマ IP から ALB VIP へのトラフィックを許可することです。

リダイレクト プログラミング

リダイレクト プログラミングは、宛先 EPG の分類（タグベースまたはサブネットベース）によって異なります。

- サブネット ベースの EPG の場合、宛先 EPG のサブネットを使用してリダイレクトをプログラムします。
- タグベースの EPG の場合、宛先 VNet の CIDR を使用してリダイレクトをプログラムします。

この結果、リダイレクトは、EPG がリダイレクトのサービス グラフの一部でない場合でも、リダイレクトで同じ宛先に向かう他の EPG からのトラフィックに影響を与えます。リダイレクトの一部ではない EPG からのトラフィックも、サービス デバイスにリダイレクトされます。

次の表は、さまざまなシナリオで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	コンシューマ VNet でのリダイレクト	プロバイダ VNet でのリダイレクト
タグベース	タグベース	プロバイダのリダイレクトは、プロバイダの VNet の CIDR です。	コンシューマのリダイレクトは、コンシューマの VNet の CIDR です。
タグベース	サブネットベース	プロバイダのリダイレクトはプロバイダのサブネットです	コンシューマのリダイレクトは、コンシューマの VNet の CIDR です。

コンシューマ	プロバイダー	コンシューマ VNet でのリダイレクト	プロバイダ VNet でのリダイレクト
サブネットベース	タグベース	プロバイダのリダイレクトは、プロバイダの VNet の CIDR です。	コンシューマのリダイレクトは、コンシューマのサブネットです
サブネットベース	サブネットベース	プロバイダのリダイレクトはプロバイダのサブネットです	コンシューマのリダイレクトは、コンシューマのサブネットです

リダイレクト ポリシー

レイヤ 4 からレイヤ 7 へのサービス リダイレクト機能をサポートするために、サービス デバイス コネクタで新しいリダイレクト フラグを使用できるようになりました。次の表に、サービス デバイス コネクタの既存のフラグと新しいフラグに関する情報を示します。

接続タイプ	説明
redir	この値は、サービス ノードがその接続のリダイレクト ノードにあることを意味します。この値は、サードパーティのファイアウォールとネットワーク ロードバランサでのみ使用可能または有効です。
snat	この値は、サービス ノードがトラフィックに対してソース NAT を実行していることをサービス グラフに通知します。この値は、サードパーティ ファイアウォールのプロバイダ コネクタでのみ、ノードのプロバイダ コネクタでのみ使用可能または有効です。
snat_dnat	この値は、サービス ノードがトラフィックに対してソース NAT と宛先 NAT の両方を実行していることをサービス グラフに伝えます。この値は、サードパーティ ファイアウォールのプロバイダー コネクタでのみ、ノードのプロバイダー コネクタでのみ使用可能または有効です。
none	デフォルト値。

リダイレクトを構成するためのワークフロー

リダイレクトを構成するための一般的なワークフローは次のとおりです。

1. サービス グラフで使用する 1 つ以上のサービス デバイスを作成します。

- ネットワーク ロードバランサ（NLB）
- アプリケーション ロードバランサ（ALB）
- サードパーティ ファイアウォール

2. サービス グラフを作成し、この特定のサービス グラフに適切なサービス デバイスを選択します。

   手順のこの時点でリダイレクトを構成します。

   1. ネットワーク ロード バランサ、アプリケーション ロード バランサ、またはファイアウォール アイコンを **[デバイスのドロップ（Drop Device）]** 領域にドラッグ アンド ドロップして、サービス グラフ用にそのサービス デバイスを選択します。
   2. リダイレクト機能を有効にするには、表示される **[サービス ノード（Service Node）]** ウィンドウで、リダイレクト機能を有効にする場所に応じて、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** または **[プロバイダ コネクタ タイプ（Provider Connector Type）]** 領域の下にある **[リダイレクト（Redirect）]** オプションの横にあるボックスをオンにします。

（注） サービス グラフにアプリケーション ロード バランサがある場合でも、アプリケーション ロード バランサ サービス デバイスでリダイレクトを有効にすることはできません。

   3. **[サービス ノード（Service Node）]** ウィンドウで残りの構成を完了し、**[追加（Add）]** をクリックします。

3. コンシューマとプロバイダの EPG 間の契約を作成する EPG 通信を構成します。
4. サービス グラフを契約に添付します。
5. サービス デバイスのパラメータを構成します。

ユースケースの例

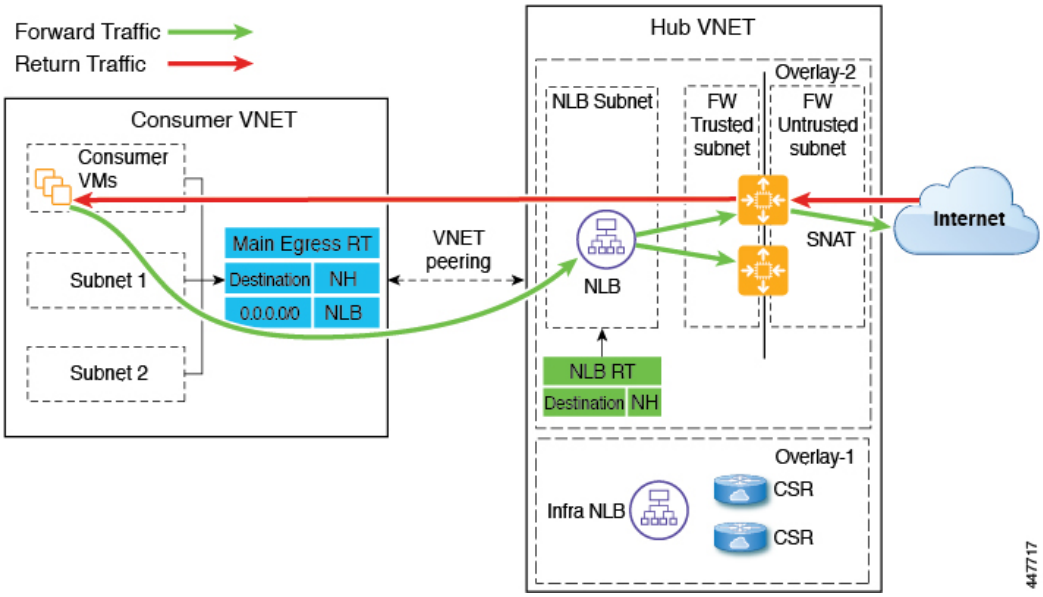
次に、いくつかのユース ケースの例を示します。

• 2 つの個別の VNet でのコンシューマおよびプロバイダ EPG を使用した VNet のハブ （32 ページ）

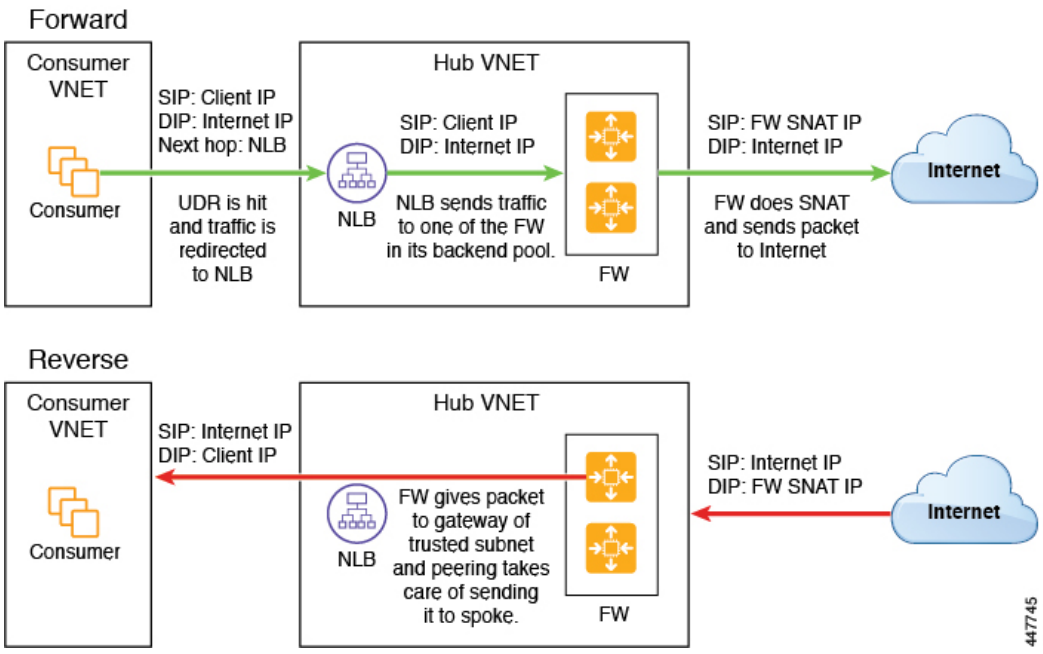
スポークツーインターネット

このユース ケースでは、コンシューマ VNet（コンシューマ VM を含む）とハブ VNet は、VNet ピアリングを使用してピアリングされます。ネットワーク ロードバランサも展開され、スケーリングのために 2 つのファイアウォールに面しています。このユース ケースでは、パッチの更新など、特定の理由でコンシューマ VM がインターネットにアクセスする必要があります。この場合、コンシューマ VNet では、インターネットへのリダイレクトを含むようにルート テーブルが変更され、トラフィックはハブ VNet のファイアウォールの前にある NLB にリダイレクトされます。インターネットに向かうサービス グラフの一部であるこのコンシューマからのトラフィックは、すべてネクスト ホップとして NLB に行きます。VNet ピアリングでは、トラフィックは最初に NLB に送られ、次に NLB がトラフィックをバックエンドのファイアウォールの 1 つに転送します。ファイアウォールは、トラフィックをインターネットに送信するときに、ソース ネットワーク アドレス変換（SNAT）も実行します。

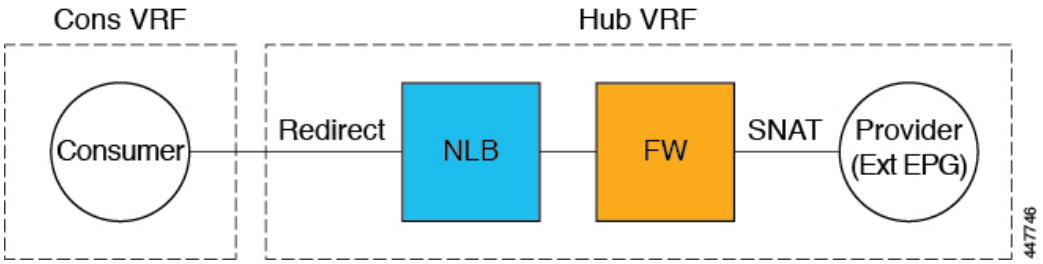
このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



次の図は、このユース ケースのパケット フローを示しています。



次の図は、このユース ケースのサービス グラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

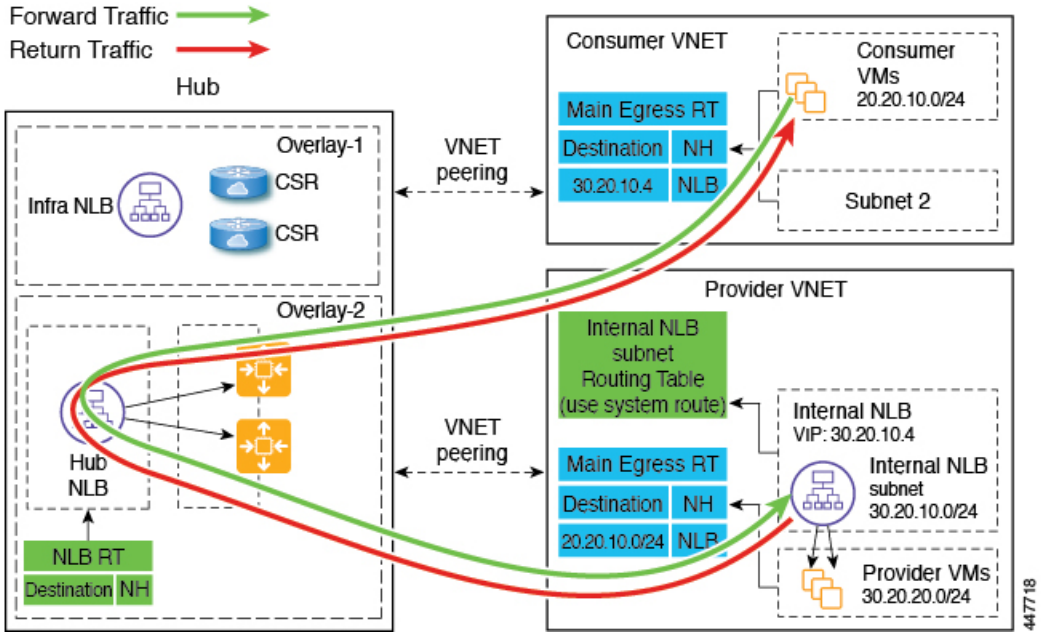
- **[デバイスの作成（Create Device）]** ウィンドウで
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ネットワーク ロードバランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。
- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

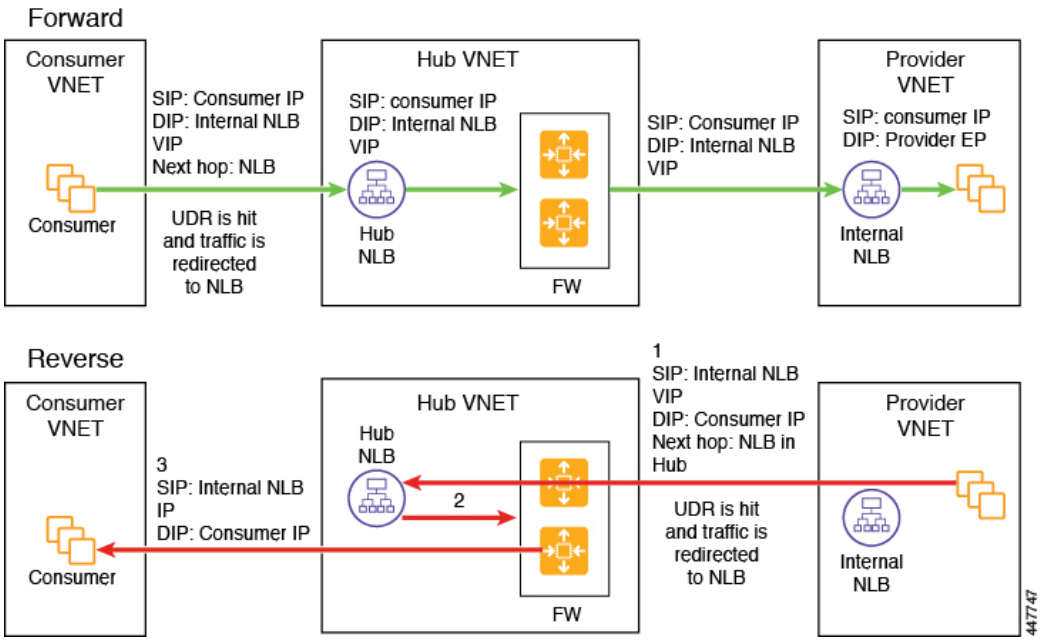
スポークツースポーク

このユース ケースでは、トラフィックはスポークからスポークへ、ハブ NLB が前面にあるハブ ファイアウォールを通過します。コンシューマ エンドポイントはコンシューマ VNet 内にあり、プロバイダ VNet には内部 NLB（またはサード パーティ ロード バランサ）が前面にある VM があります。コンシューマとプロバイダの VNet で出力ルート テーブルが変更され、トラフィックが NLB の前にあるファイアウォール デバイスにリダイレクトされるようになります。このユース ケースでは、リダイレクトが双方向に適用されます。

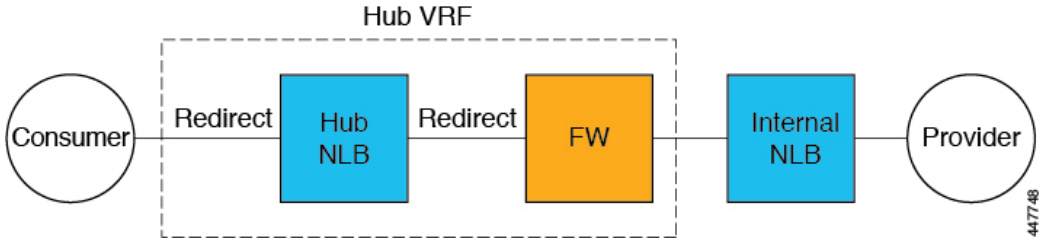
このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



次の図は、このユース ケースのパケット フローを示しています。



次の図は、このユース ケースのサービス グラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[デバイスの作成（Create Device）]** ウィンドウで、次にプロバイダー VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、プロバイダー テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドで **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダー VRF のサブネットを選択します。

（注） 内部 NLB の代わりにサードパーティ ロード バランサを使用できます。**[サービス タイプ（Service Type）]** として **[サードパーティ ロード バランサ（Third Party Load Balancer）]** を選択します。**[インターフェイスの追加（Add Interface）]** をクリックして、**[VRF]** を選択し、インターフェイスの詳細を設定します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。

- ネットワーク ロードバランサ（ハブ VNet 用）
- サードパーティ ファイアウォール（ハブ VNet 用）
- ネットワーク ロード バランサまたはサードパーティ ロード バランサ（プロバイダ VNet の場合）

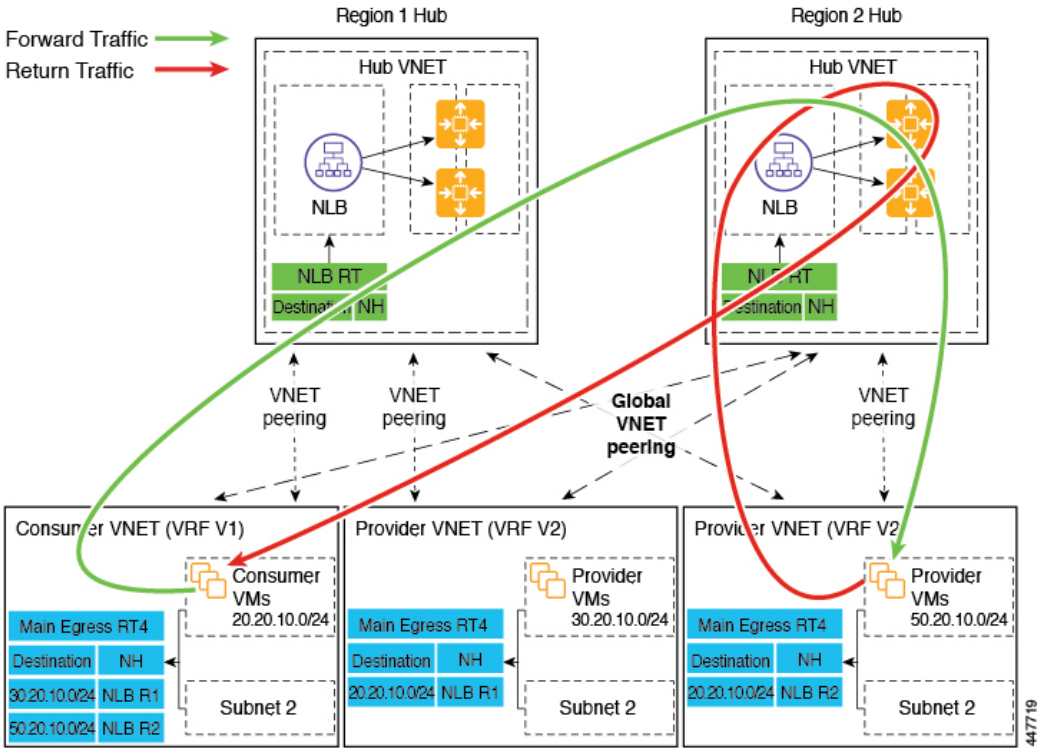
- ハブ VNet のネットワーク ロードバランサの **[サービス ノード（Service Node）]** ウィンドウで、次のようにします。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの横にあるボックスにチェックを入れ、プロバイダー側でリダイレクト機能を有効にします。
- サード パーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）** と **[プロバイダー コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。
- プロバイダー VNet でネットワーク ロードバランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダー コネクタ タイプ（Provider Connector Type）]** のチェックボックスをオフのままにします。

（注） SNATがサードパーティのロードバランサで構成されていることを確認します。

リージョン間スポーク ツー スポーク

このユース ケースでは、両方のリージョンにサービス デバイスが必要です。コンシューマ VNet はリージョン 1 にあり、プロバイダは両方のリージョン（リージョン 1 と 2）にまたがっており、一部のエンドポイントはリージョン 1 にあり、一部のエンドポイントはリージョン 2 にあります。ローカル プロバイダ エンドポイントとリモート リージョン エンドポイントには、異なるリダイレクトがプログラムされています。この場合、使用されるファイアウォールは、プロバイダ エンドポイント側に最も近いファイアウォールになります。

このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



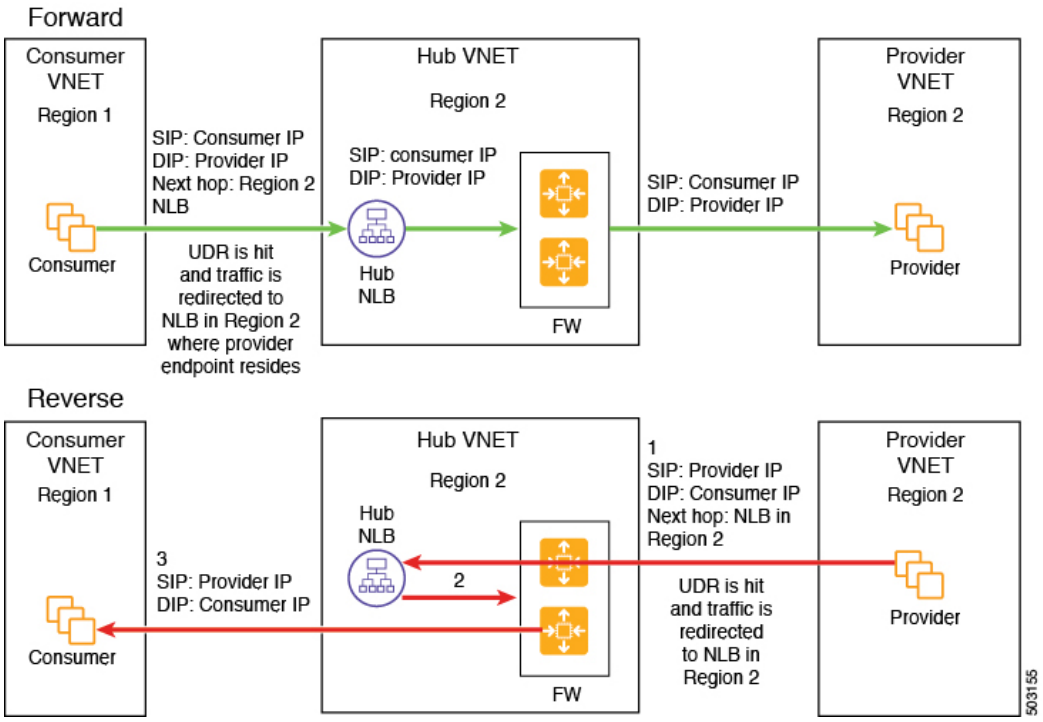
たとえば、コンシューマ VNet（VRF 1）の出力ルート テーブル（RT）の 2 つのサブネットについて考えてみます。

- 30.20.10.0/24（リージョン 1 [R1] の NLB）
- 50.20.10.0/24 （リージョン 2 [R2] の NLB）

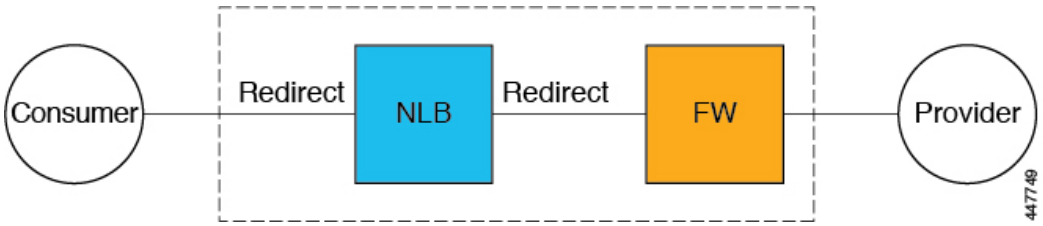
コンシューマが、ローカルにあるプロバイダ VM 30.20.10.0/24 にトラフィックを送信するとします。その場合、トラフィックはリージョン 1 のハブ NLB とファイアウォールにリダイレクトされ、プロバイダに移動します。

ここで、コンシューマがプロバイダー VM 50.20.10.0/24 にトラフィックを送信するとします。この場合、ファイアウォールはプロバイダ エンドポイントに対してローカルであるため、トラフィックはリージョン 2 のハブ NLB とファイアウォールにリダイレクトされます。

次の図は、このユース ケースのパケット フローを示しています。



次の図は、このユース ケースのサービス グラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ハブ NLB の **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの横にあるボックスにチェックを入れ、プロバイダー側でリダイレクト機能を有効にします。
- サード パーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）** と **[プロバイダー コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

上記のユース ケースでは、プロバイダ VM は、クラウド ネイティブまたはサードパーティ ロード バランサによってフロントエンドにすることもできます。

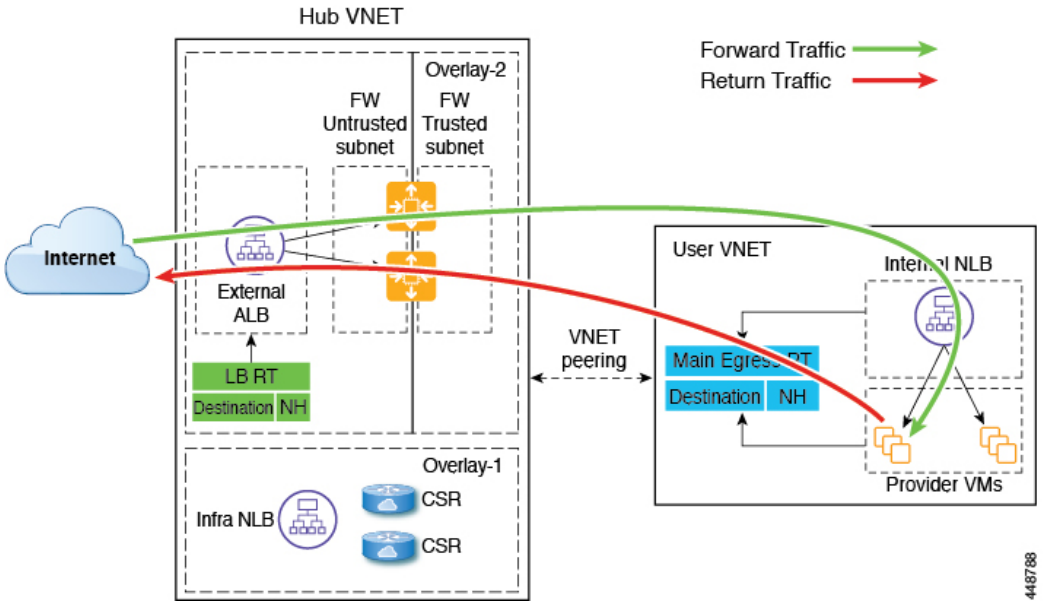
インターネット ツー スポーク（VRF 間）

このユース ケースでは、インターネットからのトラフィックは、プロバイダのエンドポイントに到達する前にファイアウォールを通過する必要があります。このユース ケースではリダイレクトは使用されません。

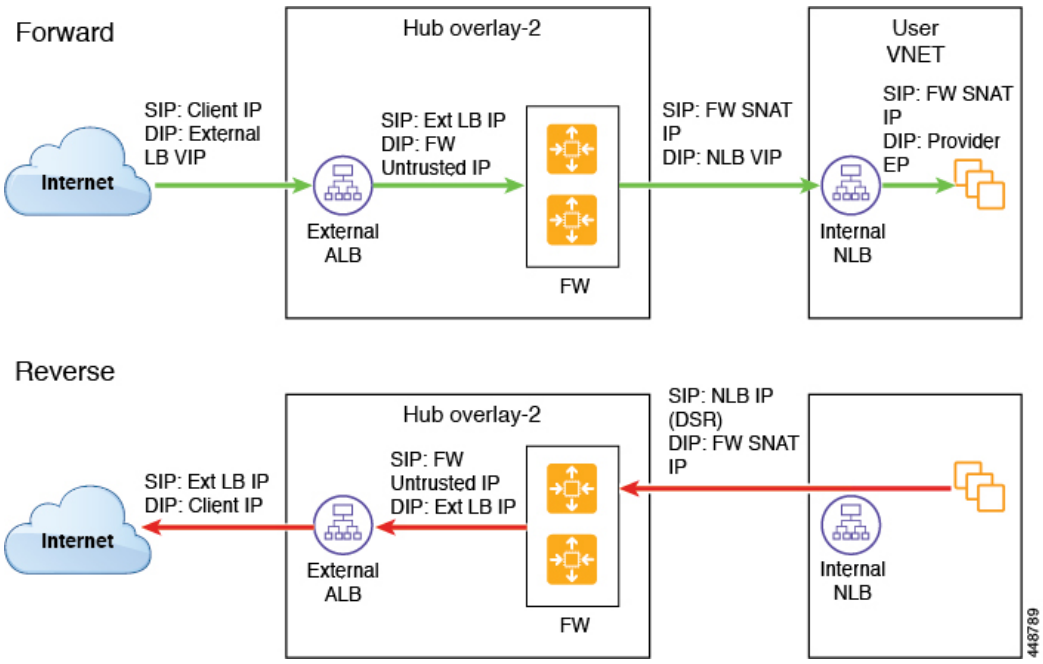
（注） このセクションでは、一般的な用語「外部ロード バランサー」が使用されています。これは、このユース ケースで外部ロード バランサが NLB、ALB、またはサード パーティ ロード バランサのいずれかになる可能性があるためです。次の例は、ALB を使用した構成を示していますが、外部ロード バランサは代わりに NLB またはサードパーティ ロード バランサである可能性があることに注意してください。

外部ロード バランサは、VIP を介してサービスを公開します。インターネット トラフィックはその VIP に送信され、外部ロード バランサはトラフィックをバックエンド プール内のファイアウォールに送信します（外部ロード バランサにはファイアウォールの信頼できないインターフェイスがバックエンド プールとしてあります）。ファイアウォールは SNAT と DNAT を実行し、トラフィックは内部 NLB VIP に送られます。次に、内部 NLB はプロバイダ エンドポイントの 1 つにトラフィックを送信します。

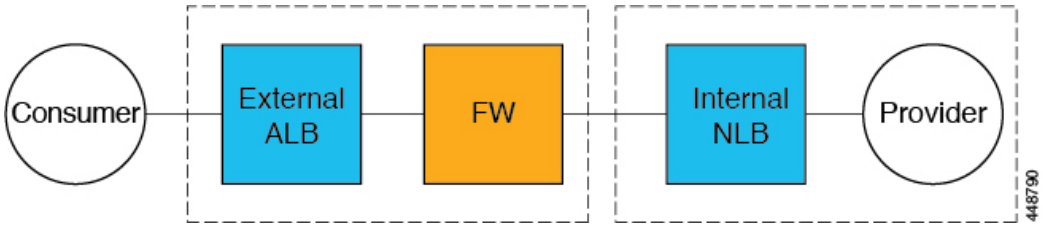
このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



次の図は、このユース ケースのパケット フローを示しています。



次の図は、このユース ケースのサービス グラフを示しています。



このユースケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[アプリケーション ロードバランサ（Application Load Balancer）]** または **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ロード バランサ（Third Party Load Balancer）]** を選択し、**[VRF]** を選択し、**[インターフェイスの追加（Add Interface）]** をクリックしてインターフェイスの詳細を設定します。
- **[デバイスの作成（Create Device）]** ウィンドウで、次にプロバイダー VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、プロバイダー テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドで **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダー VRF のサブネットを選択します。
- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサまたはアプリケーション ロード バランサ（ハブ VNet 用）
  - サードパーティ ファイアウォール（ハブ VNet 用）
  - ネットワーク ロード バランサまたはサードパーティ ロード バランサ（プロバイダ VNet の場合）
- ハブ VNet のネットワーク ロード バランサまたはアプリケーション ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユース ケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT および DNAT を実行するため、**[プロバイダ コネクタ タイプ（Third-Party Firewall）]** フィールドで、**[SNAT]** および **[DNAT]** オプションの隣のボックスにチェックを入れます。
- プロバイダ VNet でネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のチェックボックスをオフのままにします。

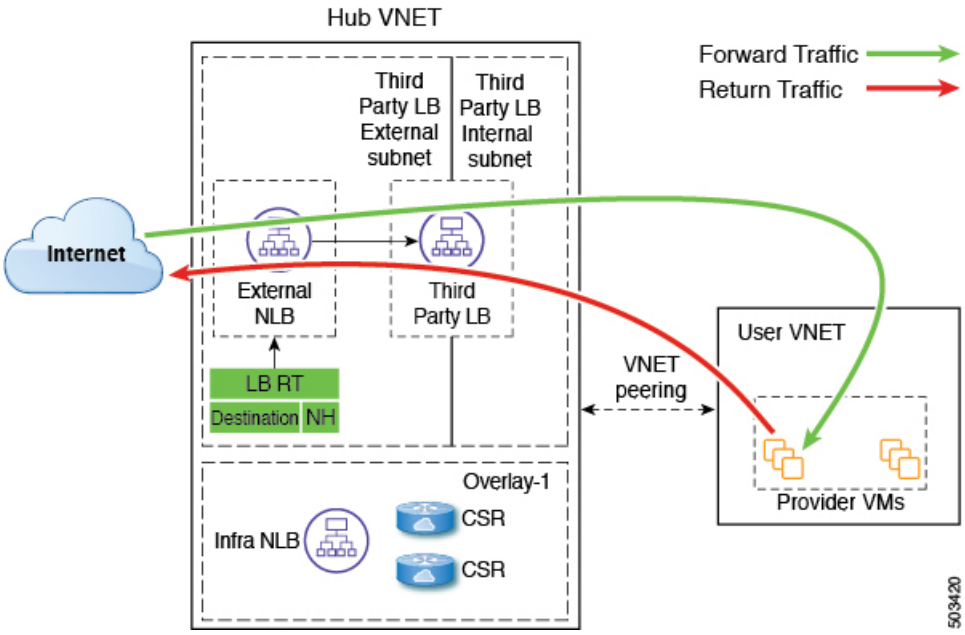
（注） SNAT がサードパーティのロードバランサで構成されていることを確認します。

サードパーティ ロード バランサの高可用性サポート

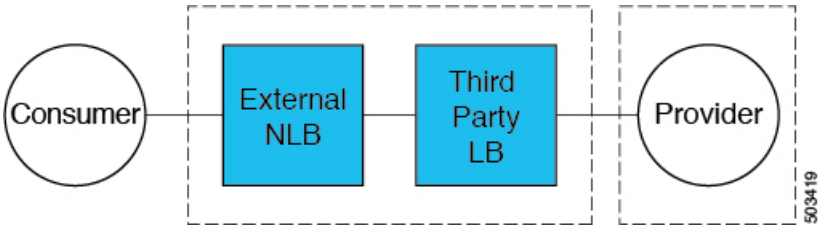
このユースケースでは、インターネットからのトラフィックは、プロバイダのエンドポイントに到達する前にサードパーティ ロード バランサを通過する必要があります。このユース ケースではリダイレクトは使用されません。

サードパーティ ロードバランサは、NLB のバックエンド プールとして構成されます。デバイスのセカンダリ IP アドレスは、NLB のターゲットとして機能します。NLB のターゲットとして、プライマリまたはセカンダリ IP アドレス（またはその両方）を追加することを選択できます。サードパーティ ロードバランサ VM は、アクティブ/アクティブ モードでのみ展開されます。サードパーティ ロード バランサは、アクティブ/スタンバイの高可用性構成では使用できません。

サードパーティ ロードバランサとネットワーク ロードバランサに専用のサブネットがあることを確認します。



次の図は、このユース ケースのサービス グラフを示しています。



このユース ケースの構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ロード バランサ（Third Party Load Balancer）]** を選択し、**[VRF]** を選択し、**[インターフェイスの追加（Add Interface）]** をクリックしてインターフェイスの詳細を設定します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ロード バランサ

（注） ネットワーク ロード バランサとサードパーティのロード バランサが同じ VNet にあることを確認します。

- ハブ VNet のネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

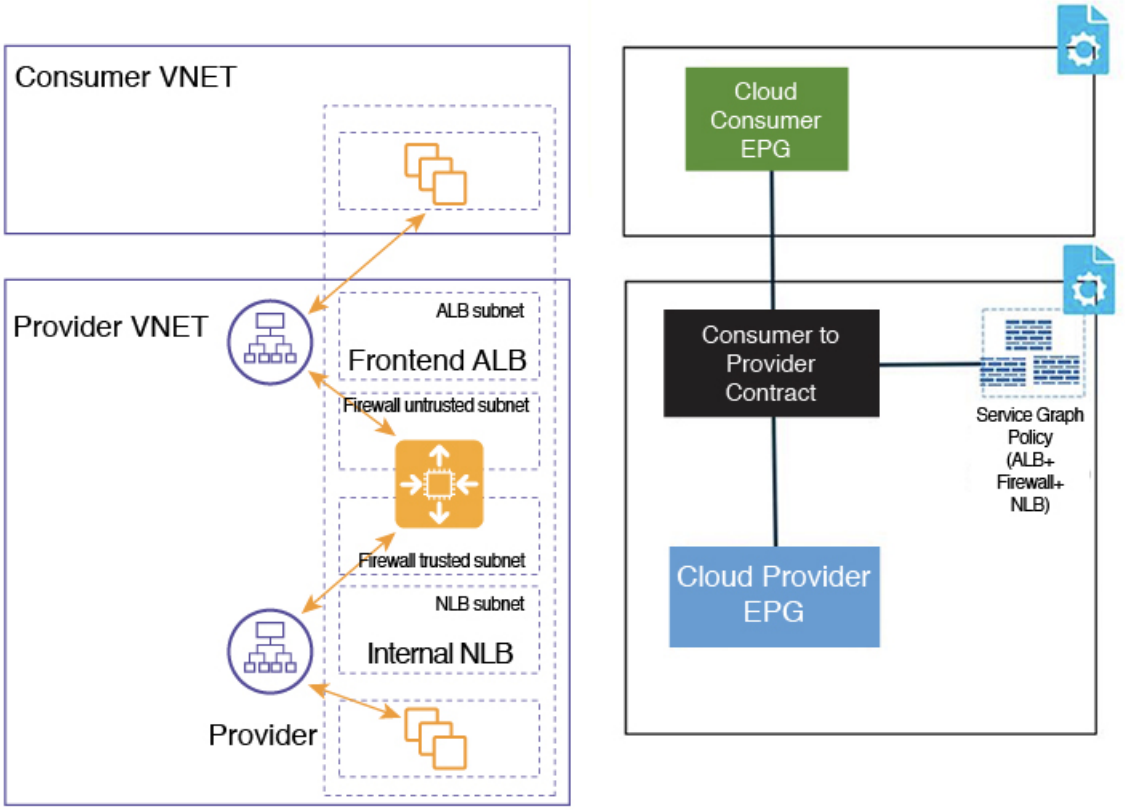
（注） SNAT がサードパーティのロードバランサで構成されていることを確認します。

2 つの個別の VNet 内のコンシューマとプロバイダの EPG

このユース ケースは、2 つの VNet を使用した構成例であり、コンシューマ EPG とプロバイダ EPG が別々の VNet にあります。

- フロントエンド ALB、ファイアウォール、および内部 NLB は、コンシューマとプロバイダの EPG の間に挿入されます。
- コンシューマ エンドポイントは、フロントエンドの ALB VIP にトラフィックを送信し、ファイアウォールに転送します。
- ファイアウォールは SNAT と DNAT を実行し、トラフィックは内部 NLB VIP にフローが流れます。
- 内部 NLB は、バックエンド プロバイダのエンドポイントへのトラフィックを負荷分散します。

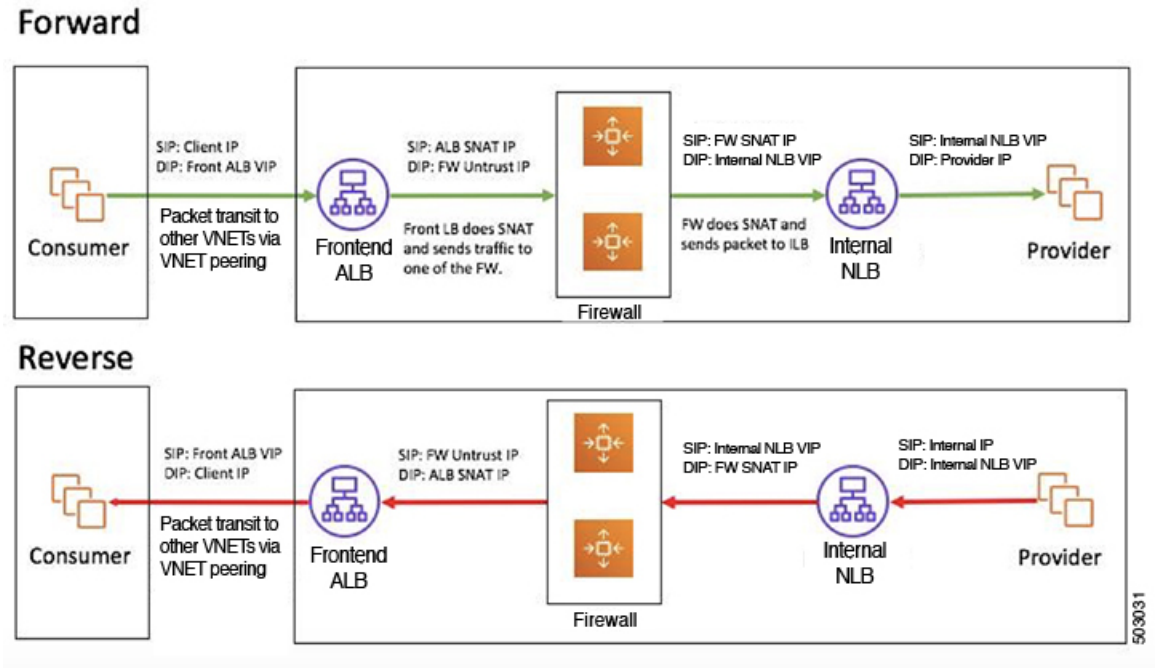
このユース ケースでは、フロントエンド ALB または内部 NLB の代わりにサードパーティのロード バランサを使用できます。このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



この図では次のようになっています。

- コンシューマ EPG はコンシューマ VNet にあります。
- プロバイダ EPG とすべてのサービス デバイスはプロバイダ VNet にあります。
- アプリケーション ロード バランサ、ネットワーク ロード バランサ（またはサードパーティのロード バランサ）、およびファイアウォールは、VNet 内に独自のサブネットを持つ必要があります。

両方向のパケット フローを次の図に示します。

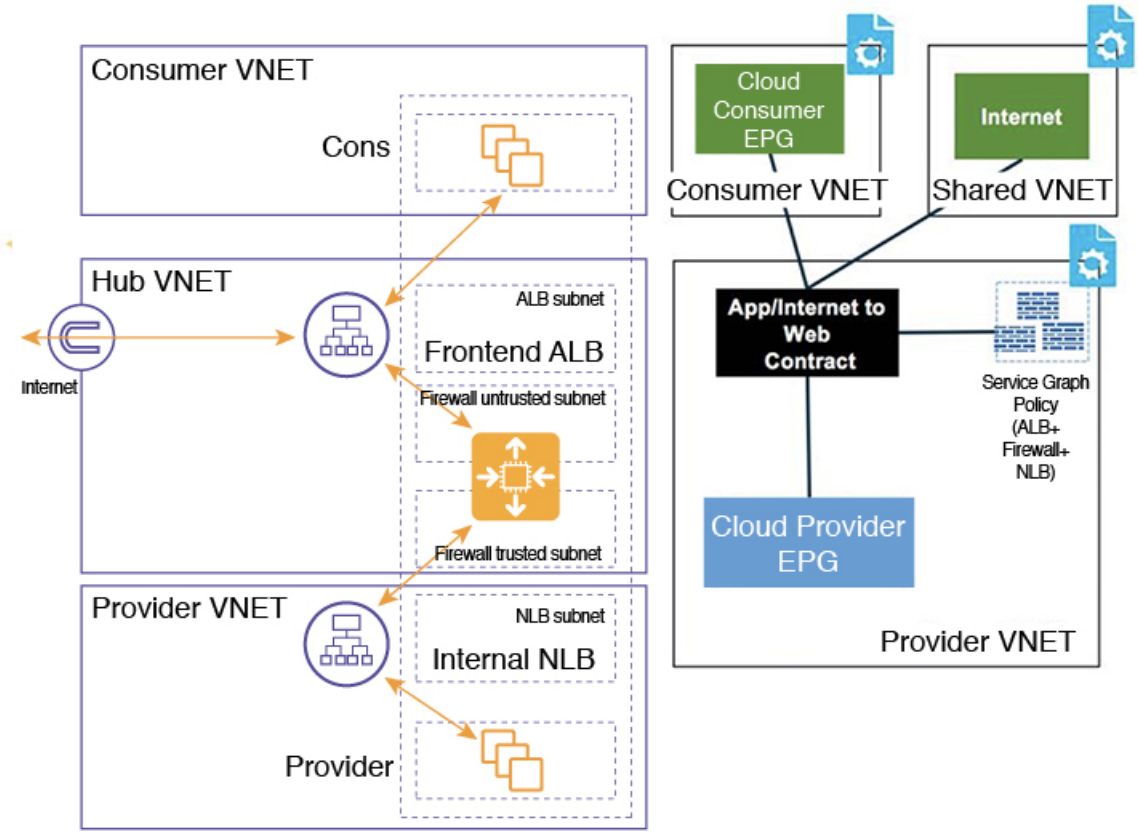


2 つの個別の VNet でのコンシューマおよびプロバイダ EPG を使用した VNet のハブ

このユース ケースは、ハブ VNet、2 つの個別の VNet 内のコンシューマ EPG とプロバイダ EPG の 3 つの VNet を使用した構成例です。

- フロントエンド ALB とファイアウォールは、コンシューマとプロバイダの EPG の間にあるハブ VNet 内に挿入されます。
- 内部 NLB はプロバイダ EPG に挿入されます。
- コンシューマ エンドポイントは、フロントエンドの ALB VIP にトラフィックを送信し、ファイアウォールに転送します。
- ファイアウォールは SNAT と DNAT を実行し、トラフィックは内部 NLB VIP にフローが流れます。
- 内部 NLB は、バックエンド プロバイダのエンドポイントへのトラフィックを負荷分散します。

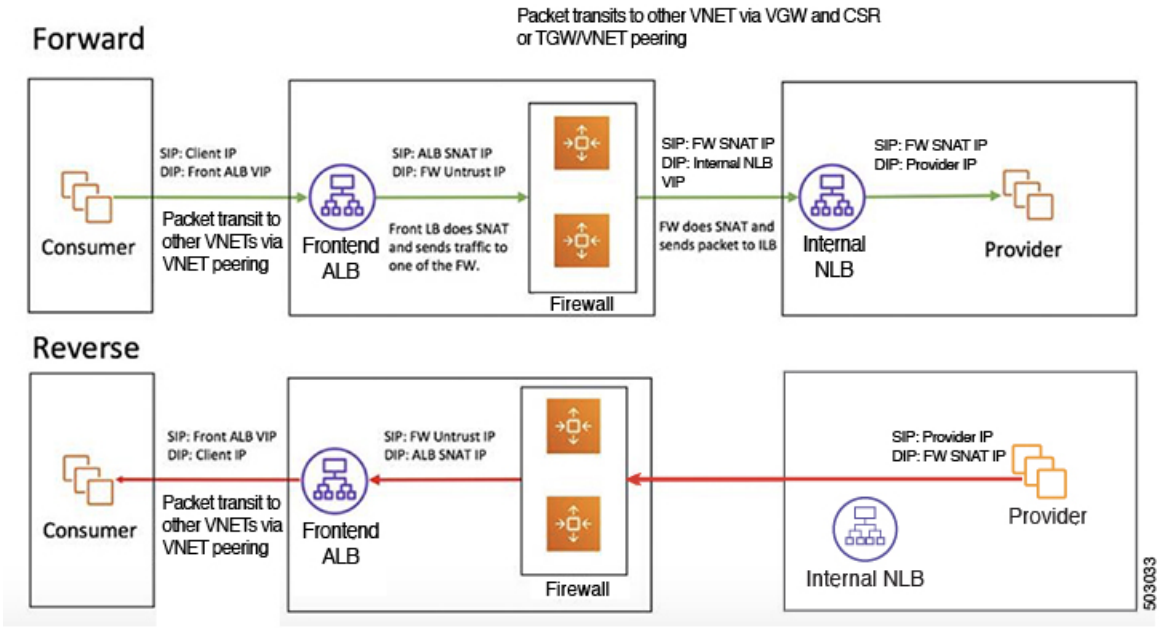
このユース ケースでは、フロントエンド ALB または内部 NLB の代わりにサードパーティのロード バランサを使用できます。このユース ケースで使用されるすべてのレイヤ 4 からレイヤ 7 サービス デバイスに専用サブネットがあることを確認します。



この図では次のようになっています。

- コンシューマ EPG はコンシューマ VNet にあります。
- プロバイダ EPG と内部 NLB はプロバイダ VNet にあります。
- フロントエンド ALB とファイアウォールはハブ VNet にあります
- アプリケーション ロード バランサ、ネットワーク ロード バランサ（またはサードパーティのロード バランサ）、およびファイアウォールは、VNet 内に独自のサブネットを持つ必要があります。

両方向のパケット フローを次の図に示します。



クラウドネイティブおよびサードパーティ サービスによるサービス グラフの使用例

以下は、リダイレクトの有無にかかわらず、クラウド ネイティブおよびサードパーティ サービスを使用したサービス グラフの使用例です。詳細、ガイドラインおよび制限事項については、クラウド ネイティブおよびサードパーティ サービスでのサービス グラフの使用 （2 ページ） を参照してください。

リダイレクトのないユースケースの例

以下は、リダイレクトのないクラウドネイティブおよびサードパーティのサービスを使用したサービス グラフのユース ケースの例です。

これらの各ユースケースのプロセスの一部として、クラウド サービス EPG を構成します。クラウドサービス EPG を構成している場合は、**サブネットごとの NSG** 構成を有効にする必要があります。詳細については、セキュリティ グループおよびクラウド サービス エンドポイント グループを参照してください。

- インターネット インバウンド トラフィックの単一ノード サービス グラフ：プロバイダとしての非管理サービス EPG （35 ページ）
- インターネット インバウンド トラフィックの単一ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ サービス EPG （37 ページ）

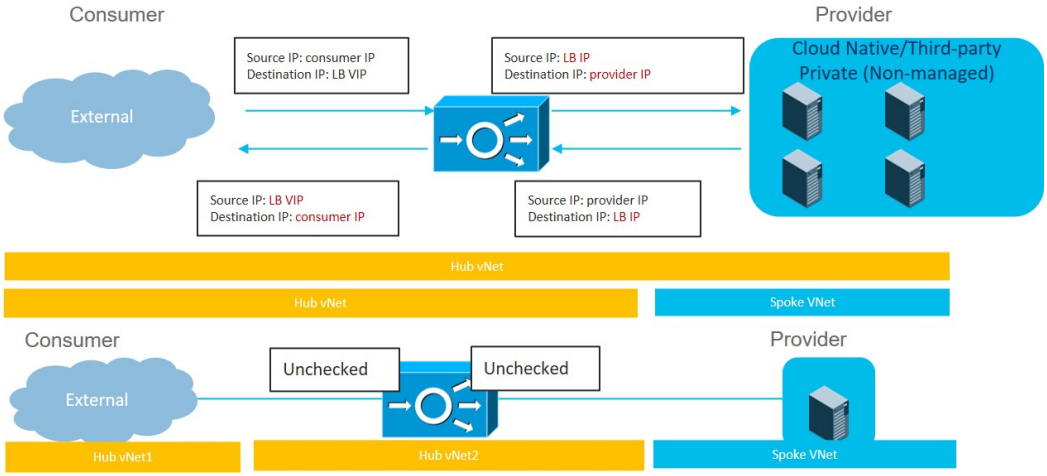
- インターネット インバウンド トラフィックの 2 ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ管理対象サービス EPG （38 ページ）
- インターネット インバウンド トラフィックの 3 ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ管理対象サービス EPG （40 ページ）

（注） 次の各ユース ケースでは、プロバイダとしてサービス EPG を使用する、単一ノード、2 ノード、および 3 ノードのサービス グラフを使用する同様のトポロジを、クラウドの東西トラフィックに対してサポートできます。これらのユース ケースでは、コンシューマはクラウド EPG になり、使用されるロード バランサーは内部ロード バランサになります。

インターネット インバウンド トラフィックの単一ノード サービス グラフ：プロバイダとしての非管理サービス EPG

このユース ケースには、サービス ノードがロードバランサ（アプリケーション ロードバランサ、ネットワーク ロードバランサ、またはサードパーティのロードバランサ）である単一ノード サービス グラフがあります。

このユース ケースでは、サービス EPG はプロバイダであり、外部 EPG はコンシューマ側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。サービス エンドポイントは動的に学習され、アプリケーション ロードバランサまたはネットワーク ロードバランサに追加されます。



このユース ケースを構成するには：

1. コンシューマ側で外部 EPG を作成します。

   これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 を参照してください。この外部 EPG の `infra` テナントを選択します。

2. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   これらの手順については、次の設定を使用して Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure Storage` は、クラウド ネイティブ 展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：クラウド ネイティブまたはサードパーティ
   - **アクセス タイプ**：`Private`

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   次のように選択します。

   - **[デバイスの作成（Create Device）]** ウィンドウで、ハブ VNet のサービス デバイスを作成します。
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** として **[アプリケーション ロード バランサ（Application Load Balancer）]** または **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、アプリケーション ロード バランサまたはネットワーク ロード バランサをドラッグ アンド ドロップします。
   - ハブ VNet のアプリケーション ロード バランサまたはネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

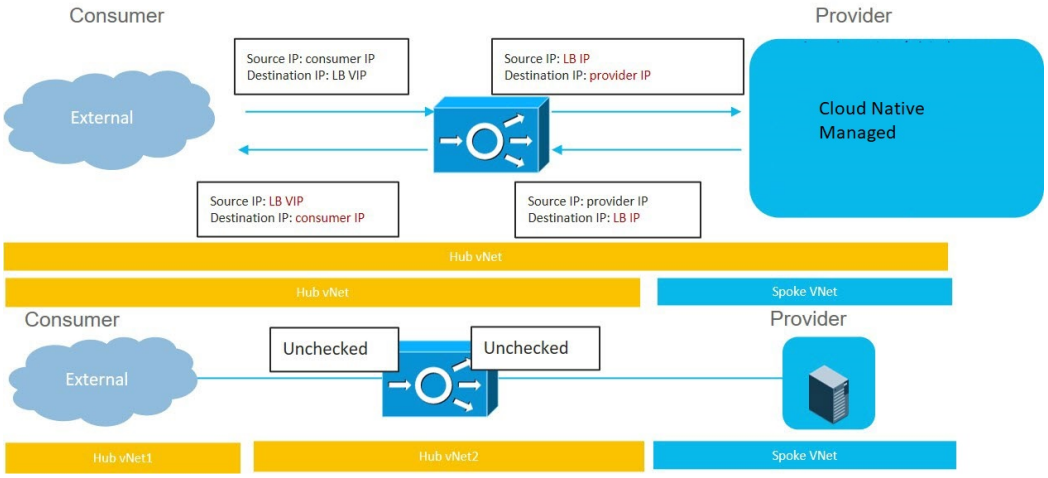
4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

インターネット インバウンド トラフィックの単一ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ サービス EPG

このユース ケースには、サービス ノードがロードバランサ（アプリケーション ロードバランサ、ネットワーク ロードバランサ、またはサードパーティのロードバランサ）である単一ノード サービス グラフがあります。

このユース ケースでは、サービス EPG はプロバイダであり、外部 EPG はコンシューマ側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。



このユース ケースを構成するには：

1. コンシューマ側で外部 EPG を作成します。

   これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 を参照してください。この外部 EPG の `infra` テナントを選択します。

2. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   これらの手順については、次の設定を使用して Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure ApiManagement Services` は、`Cloud Native Managed` 展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：`Cloud Native Managed`
   - **アクセス タイプ**：パブリックおよびプライベート

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   次のように選択します。

- **[デバイスの作成（Create Device）]** ウィンドウで、ハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** として **[アプリケーション ロード バランサ（Application Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、アプリケーション ロード バランサをドラッグ アンド ドロップします。
- ハブ VNet のアプリケーション ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

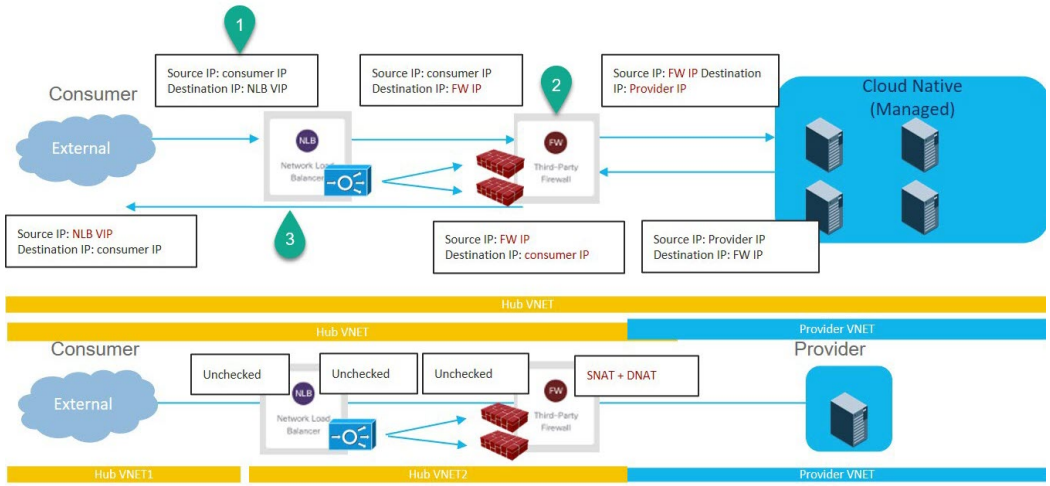
インターネット インバウンド トラフィックの 2 ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ管理対象サービス EPG

このユースケースには2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。この 2 ノード サービス グラフはリダイレクトを使用しないため、SNAT+DNAT はファイアウォールで実行されます。DNATed アドレスは、ネットワーク ロードバランサまたは同等のサービスであると想定されます。このユース ケースでは、サービス グラフは、ロードバランサのサブネットへのルートの到達可能性のみを確立します。

このユース ケースでは、サービス EPG はプロバイダであり、外部 EPG はコンシューマ側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサのパブリック VIP に送信され、ファイアウォール（DNAT）へのトラフィックが負荷分散されます。
2. SNAT+DNAT はファイアウォールで実行されます。
3. リターン トラフィックの場合、Azure はソース IP をネットワーク ロード バランサのパブリック VIP に変換します。



このユース ケースを構成するには：

1. コンシューマ側で外部 EPG を作成します。

   これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 を参照してください。この外部 EPG の `infra` テナントを選択します。

2. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   これらの手順については、次の設定を使用して Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure Kubernetes Services（AKS）` は、`Cloud Native Managed` 展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：`Cloud Native Managed`
   - **アクセス タイプ**：`Private`

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   このユースケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。

- **[サービス タイプ（Service Type）]** として **[ネットワーク ロードバランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** エリアで **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のチェックボックスをオフのままにします。
- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT および DNAT を実行するため、**[プロバイダ コネクタ タイプ（Third-Party Firewall）]** フィールドで、**[SNAT]** および **[DNAT]** オプションの隣のボックスにチェックを入れます。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

インターネット インバウンド トラフィックの 3 ノード サービス グラフ：プロバイダとしてのクラウド ネイティブ管理対象サービス EPG

このユースケースには3 ノードのサービス グラフがあり、サービス ノードは次のとおりです。

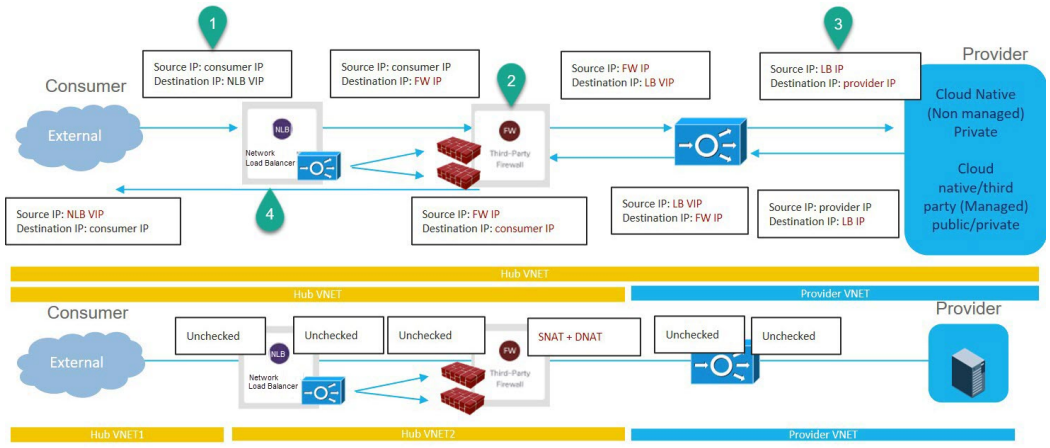
- 最初のサービス デバイス: ハブ VNet のネットワーク ロードバランサ
- 2 番目のサービス デバイス：ハブ VNet のファイアウォール
- サード サービス デバイス：ハブ VNet またはスポーク VNet 内のサード パーティのロードバランサ

この 3 ノード サービス グラフはリダイレクトを使用しないため、SNAT+DNAT はファイアウォールで実行されます。DNATedアドレスは、ロードバランサまたは同等のサービスであると想定されます。

このユース ケースでは、サービス EPG はプロバイダであり、外部 EPG はコンシューマ側で構成されます。サービス EPG は、ハブまたはスポーク VNet に配置できます。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックは最初のサービス デバイスであるネットワーク ロード バランサのパブリック VIP に送信され、次にファイアウォール（DNAT）へのトラフィックの負荷分散が行われます。
2. SNAT+DNAT は、2 番目のサービス デバイスであるファイアウォールで実行されます。
3. トラフィックは、SNAT が構成されているサードパーティのロード バランサであるサード サービス デバイスに移動します。
4. リターン トラフィックの場合、Azure はソース IP をネットワーク ロード バランサのパブリック VIP に変換します。



このユース ケースを構成するには：

1. コンシューマ側で外部 EPG を作成します。

   これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 を参照してください。この外部 EPG の `infra` テナントを選択します。

2. プロバイダー側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure ApiManagement Services` は、`Cloud Native Managed` 展開タイプでサポートされるサービス タイプです。

- **展開タイプ**：`Cloud Native Managed`
- **アクセス タイプ**：`Private`

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   このユースケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
       - 最初のデバイスとして、**[サービス タイプ（Service Type）]** として **[アプリケーション ロード バランサ（Application Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウドコンテキストプロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
       - 2 番目のサービス デバイスについては、**[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドで、セカンダリ VRF を選択します。
       - 3 番目のサービス デバイスがハブ VNet にある場合は、**[サービス タイプ（Service Type）]** として **[サードパーティ ロード バランサ（Third-Party Load Balancer）]** を選択し、**[VRF]** を選択し、**[インターフェイスの追加（Add Interface）]** をクリックしてインターフェイスの詳細を設定します。

   - **[デバイスの作成（Create Device）]** ウィンドウで、次に、必要に応じて (3 番目のサービス デバイスがプロバイダ VNet にある場合)、プロバイダ VNet のサービス デバイスを作成します。
     - **[テナント（Tenant）]** フィールドで、プロバイダー テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドで **[サードパーティ ロード バランサ（Third-Party Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダ VRF のサブネットを選択します。

   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
     - アプリケーション ロード バランサ（ハブ VNet 用）

- サードパーティ ファイアウォール（ハブ VNet 用）
- サード パーティ ロード バランサ（ハブまたはプロバイダ VNet 用）

- ハブ VNet のアプリケーション ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。
- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユース ケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT および DNAT を実行するため、**[プロバイダ コネクタ タイプ（Third-Party Firewall）]** フィールドで、**[SNAT]** および **[DNAT]** オプションの隣のボックスにチェックを入れます。
- SNAT がサードパーティのロードバランサで構成されていることを確認します。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

リダイレクトの使用例

以下は、リダイレクトを備えたクラウド ネイティブ サービスとサードパーティ サービスを使用したサービス グラフのユース ケースの例です。

これらの各ユース ケースのプロセスの一部として、クラウド サービス EPG を構成します。クラウド サービス EPG を構成している場合は、**サブネットごとの NSG** 構成を有効にする必要があります。詳細については、セキュリティ グループおよびクラウド サービス エンドポイント グループを参照してください。

- インターネット アウトバウンドの 2 ノード サービス グラフ （44 ページ）
- East-West の 2 ノード サービス グラフ （46 ページ）
- SNAT オプションを使用した East-West の 2 ノード サービス グラフ （49 ページ）
- エクスプレス ルート ゲートウェイ経由の受信トラフィックの 2 ノード サービス グラフ （51 ページ）
- SNAT オプションを使用したエクスプレス ルート ゲートウェイ経由のインバウンド トラフィックの 2 ノード サービス グラフ （54 ページ）

- エクスプレス ルート ゲートウェイ経由の受信トラフィックの 3 ノード サービス グラフ（56 ページ）

インターネット アウトバウンドの 2 ノード サービス グラフ

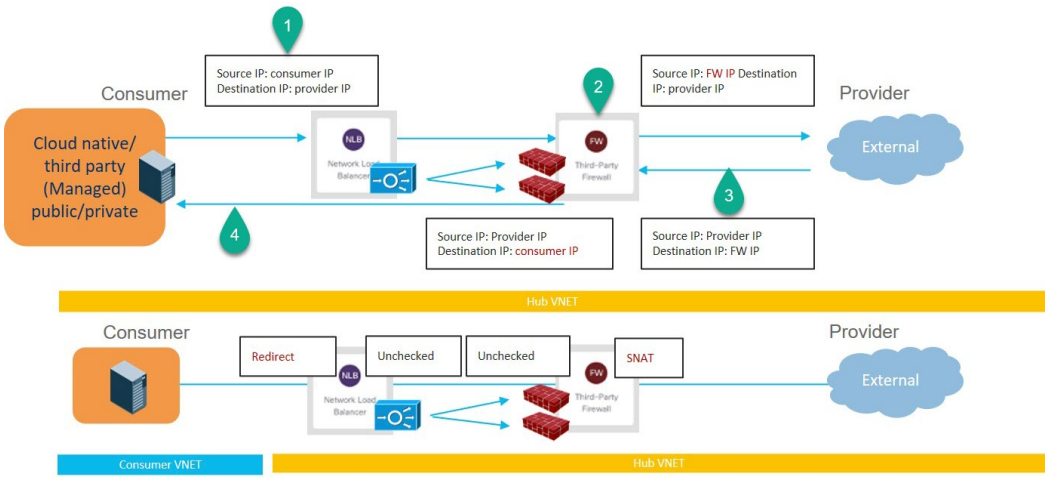
このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、コンシューマ側でリダイレクトが有効になっており、ファイアウォールで SNAT が有効になっています。

このユース ケースでは、サービス EPG はコンシューマであり、外部 EPG はプロバイダ側で構成されます。

（注） レイヤ 4 からレイヤ 7 のサービス グラフが、インターネットの到達可能性のために独自の UDR を使用する PaaS に使用されている場合は、外部 EPG で 0.0.0.0/0 を使用しないことをお勧めします。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. SNAT はファイアウォールで実行されます。
3. リターン トラフィックはファイアウォールの SNAT IP アドレスに戻ります。
4. 戻り方向のこの時点では、戻りトラフィックはネットワーク ロード バランサを通過しません。



このユース ケースを構成するには：

1. プロバイダ側で外部 EPG を作成します。

これらの手順については、Cisco Cloud APIC GUI を使用した外部 EPG の作成 を参照してください。

- この外部 EPG の [インフラ（infra）] テナントを選択します。
- 0.0.0.0/0 サブネットで外部 EPG を設定しないでください。

2. コンシューマ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、Azure Kubernetes Services（AKS）は、クラウド ネイティブ管理対象展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：クラウド ネイティブ管理対象
   - **アクセス タイプ**：Private

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
       - **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
       - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
     - ネットワーク ロード バランサ

- サードパーティ ファイアウォール

- ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。

- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

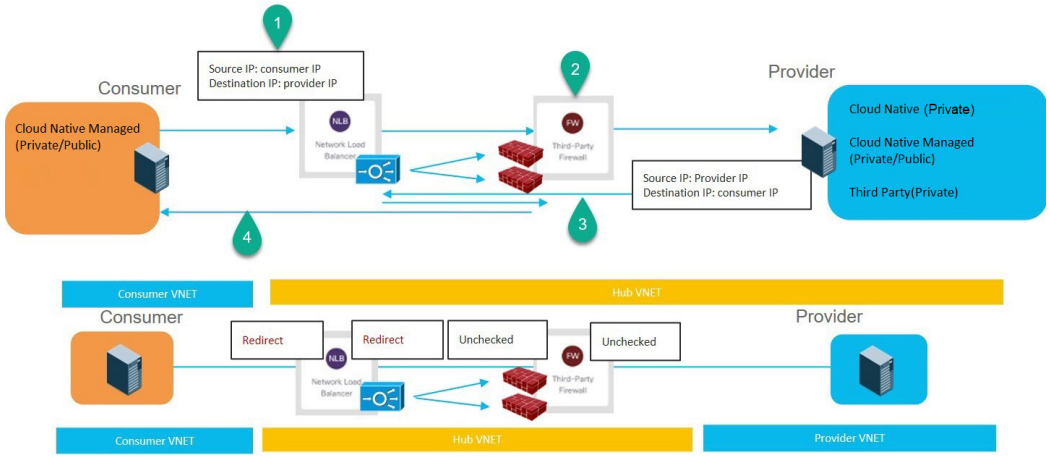
East-West の 2 ノード サービス グラフ

このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、コンシューマ側とプロバイダ側の両方でリダイレクトが有効になっています。

このユース ケースでは、コンシューマとプロバイダはクラウド EPG またはサービス EPG である可能性があります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. このユース ケースでは、ファイアウォールで SNAT は実行されません。
3. リターン トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
4. 戻り方向のこの時点で、戻りトラフィックはコンシューマに戻ります。



このユース ケースを構成するには：

1. コンシューマまたはプロバイダのサービス EPG を使用している場合は、サービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - コンシューマとしてのサービス EPG には、次の設定があります。
     - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure Kubernetes Services (AKS)` は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
     - **展開タイプ**：`クラウド ネイティブ管理対象`
     - **アクセス タイプ**：`Private`
   - プロバイダとしてのサービス EPG には、次の設定があります。
     - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure Storage File` は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
     - **展開タイプ**：`クラウド ネイティブ`
     - **アクセス タイプ**：`Private`

2. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

- **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
    - **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
    - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ハブ NLB の **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、プロバイダ側でリダイレクト機能を有効にします。
- サード パーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。

3. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

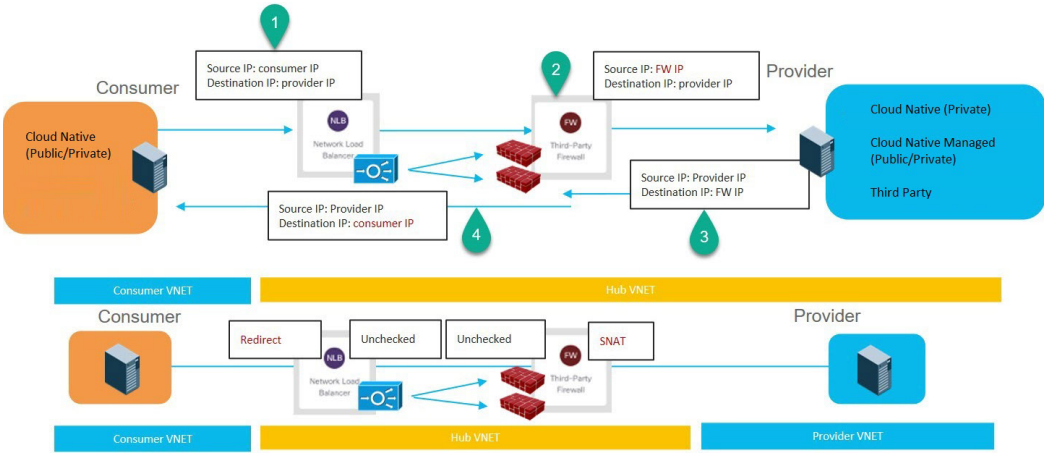
SNAT オプションを使用した East-West の 2 ノード サービス グラフ

このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、リダイレクトはコンシューマ側でのみ有効になっており、SNAT はファイアウォールで有効になっています。

このユース ケースでは、コンシューマとプロバイダはクラウド EPG またはサービス EPG である可能性があります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. SNAT はファイアウォールで実行されます。
3. リターン トラフィックはファイアウォールの SNAT IP アドレスに戻ります。
4. 戻り方向のこの時点では、戻りトラフィックはネットワーク ロード バランサを通過しません。



このユース ケースを構成するには：

1. コンシューマまたはプロバイダのサービス EPG を使用している場合は、サービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - コンシューマとしてのサービス EPG には、次の設定があります。
     - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure Active Directory Domain Services` は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
     - **展開タイプ**：`クラウド ネイティブ管理対象`
     - **アクセス タイプ**：`Private`

- プロバイダとしてのサービス EPG には、次の設定があります。
  - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure Storage File` は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
  - **展開タイプ**：`クラウド ネイティブ`
  - **アクセス タイプ**：`Private`

2. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
       - **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
       - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
     - ネットワーク ロード バランサ
     - サードパーティ ファイアウォール
   - ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
     - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。

- **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。

- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

3. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダーの間に存在するコントラクトをサービス グラフにアタッチします。

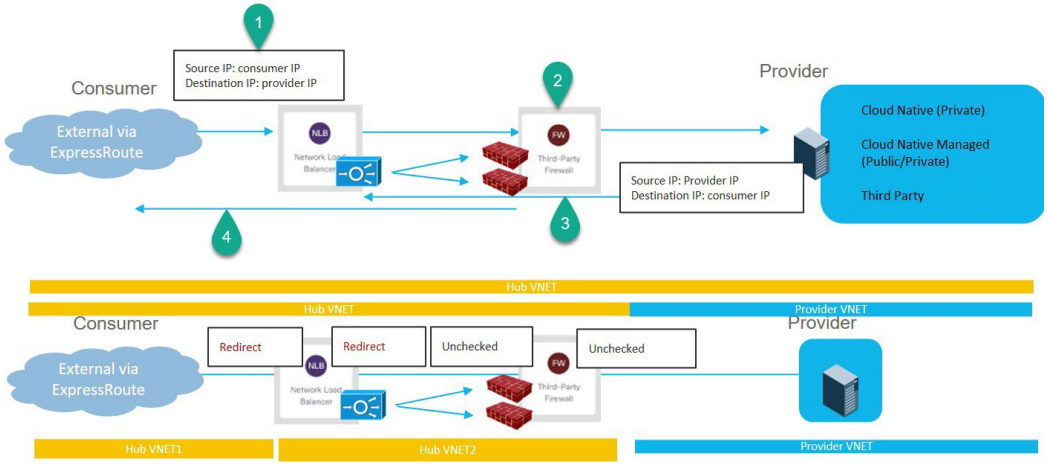
エクスプレス ルート ゲートウェイ経由の受信トラフィックの 2 ノード サービス グラフ

このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、コンシューマ側とプロバイダ側の両方でリダイレクトが有効になっています。

このユース ケースでは、サービス EPG がプロバイダであり、エクスプレス ルートがコンシューマ側にあります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. このユース ケースでは、ファイアウォールで SNAT は実行されません。
3. リターン トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
4. 戻り方向のこの時点で、戻りトラフィックはコンシューマに戻ります。



このユース ケースを構成するには：

1. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure Active Directory Domain Services` は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：`クラウド ネイティブ管理対象`
   - **アクセス タイプ**：`Private`

2. コンシューマ側にエクスプレス ルート ゲートウェイを展開します。

   これらの手順については、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 を参照してください。

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。

- **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ
  - サードパーティ ファイアウォール
- ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。
- サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。
  - このユースケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダー コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

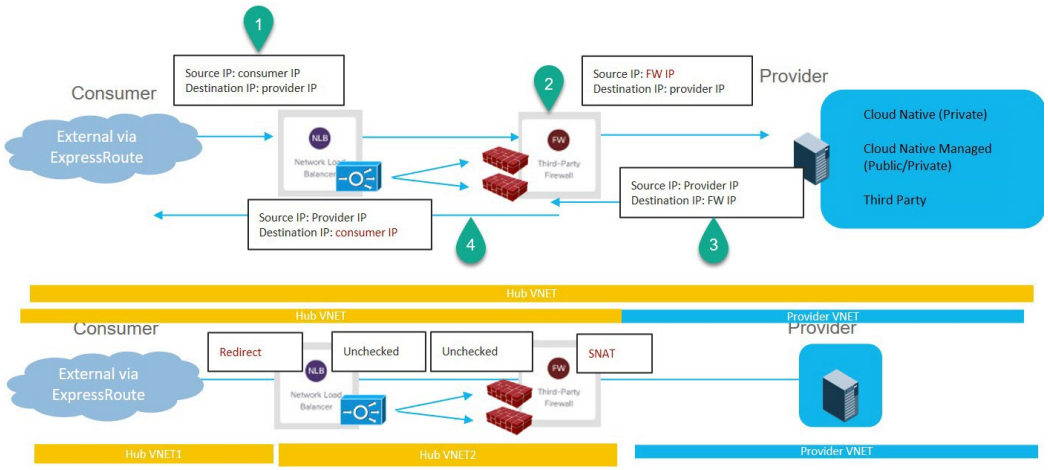
SNATオプションを使用したエクスプレス ルート ゲートウェイ経由のインバウンド トラフィックの 2 ノード サービス グラフ

このユース ケースには 2 ノードのサービス グラフがあり、サービス ノードはネットワーク ロードバランサとファイアウォールです。このユースケースでは、リダイレクトはコンシューマ側でのみ有効になっており、SNAT はファイアウォールで有効になっています。

このユース ケースでは、サービス EPG はプロバイダであり、エクスプレス ルートはコンシューマ側にあります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. SNAT はファイアウォールで実行されます。
3. リターン トラフィックはファイアウォールの SNAT IP アドレスに戻ります。
4. 戻り方向のこの時点では、戻りトラフィックはネットワーク ロード バランサを通過しません。



このユースケースを構成するには：

1. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Redis キャッシュ`は、`クラウド ネイティブ管理対象`展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：`クラウド ネイティブ管理対象`
   - **アクセス タイプ**：`Private`

2. コンシューマ側にエクスプレス ルート ゲートウェイを展開します。

   これらの手順については、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 を参照してください。

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。
       - **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
       - **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。
   - **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
     - ネットワーク ロード バランサ
     - サードパーティ ファイアウォール
   - ネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
     - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]**オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
     - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、ボックスをオフのままにします。
   - サードパーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、次の手順を実行します。
     - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、ボックスをオフのままにします。

- このユース ケースでは、インターネットにトラフィックを送信するときにファイアウォールが SNAT を実行するため、**[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[SNAT]** オプションの隣のボックスにチェックを入れます。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

エクスプレス ルート ゲートウェイ経由の受信トラフィックの 3 ノード サービス グラフ

このユース ケースには3 ノードのサービス グラフがあり、サービス ノードは次のとおりです。

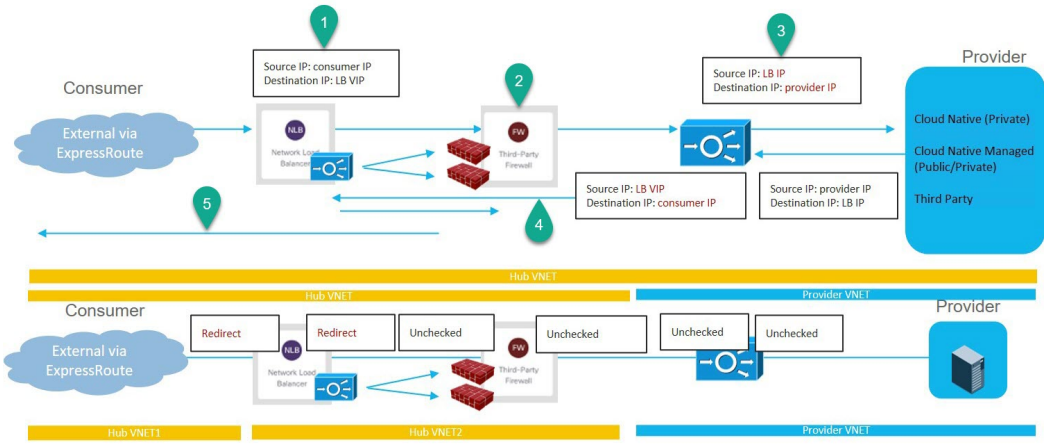
- 最初のサービス デバイス：ハブ VNet のネットワーク ロード バランサ
- 2 番目のサービス デバイス：ハブ VNet のファイアウォール
- 3 番目のサービス デバイス：ハブまたはスポーク VNet のアプリケーション ロード バランサ

このユースケースでは、コンシューマ側とプロバイダ側の両方でリダイレクトが有効になっています。

このユース ケースでは、サービス EPG はプロバイダです。エクスプレス ルートはコンシューマ側にあり、コンシューマはクラウド EPG またはサービス EPG である可能性があります。

これらのアクションは、次の図に示すように、このユース ケースで実行されます。

1. トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
2. このユース ケースでは、ファイアウォールで SNAT は実行されません。
3. トラフィックは、SNAT が構成されているアプリケーション ロード バランサであるサード サービス デバイスに移動します。
4. リターン トラフィックはネットワーク ロード バランサにリダイレクトされ、ファイアウォールへのトラフィックの負荷分散が行われます。
5. 戻り方向のこの時点で、戻りトラフィックはコンシューマに戻ります。



このユースケースを構成するには：

1. プロバイダ側でサービス EPG を作成し、適切な展開タイプとアクセス タイプをサービス EPG に割り当てます。

   次の設定によるこれらの手順については、Cisco Cloud APIC GUI を使用したサービス EPG の作成 を参照してください。

   - **サービス タイプ**：展開の種類に応じて、サポートされているサービス タイプ（詳細については クラウド サービス エンドポイント グループ を参照）。たとえば、`Azure ApiManagement Services` は、クラウド ネイティブ管理対象展開タイプでサポートされるサービス タイプです。
   - **展開タイプ**：クラウド ネイティブ管理対象
   - **アクセス タイプ**：プライベート

2. コンシューマ側にエクスプレス ルート ゲートウェイを展開します。

   これらの手順については、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 を参照してください。

3. サービス グラフを構成します。

   これらの手順については、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） を参照してください。

   このユース ケースのリダイレクト構成の一部として、次の選択を行います。

   - **[デバイスの作成（Create Device）]** ウィンドウで、最初にハブ VNet のサービス デバイスを作成します。
     - **[テナント（Tenant）]** フィールドで、**[インフラ（infra）]** テナントを選択します。
     - **[サービス タイプ（Service Type）]** フィールドでサービス デバイスのタイプを選択します。

- **[サービス タイプ（Service Type）]** として **[ネットワーク ロード バランサ（Network Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびセカンダリ VRF で作成されたサブネットを選択します。
- **[サービス タイプ（Service Type）]** として **[サードパーティ ファイアウォール（Third-Party Firewall）]** を選択し、**[VRF]** フィールドでセカンダリ VRF を選択します。

- **[デバイスの作成（Create Device）]** ウィンドウで、次にプロバイダ VNet のサービス デバイスを作成します。
  - **[テナント（Tenant）]** フィールドで、プロバイダ テナントを選択します。
  - **[サービス タイプ（Service Type）]** フィールドで **[アプリケーション ロード バランサ（Application Load Balancer）]** を選択し、**[サブネット（Subnets）]** 領域で **[サブネットの追加（Add Subnet）]** をクリックしてから、適切なリージョン、クラウド コンテキスト プロファイル、およびプロバイダ VRF のサブネットを選択します。

（注） 内部 NLB の代わりにサードパーティのロードバランサを使用できます。**[サービス タイプ（Service Type）]**として **[サードパーティ ロード バランサ（Third Party Load Balancer）]** を選択します。**[インターフェイスの追加（Add Interface）]** をクリックして、**[VRF]** を選択し、インターフェイスの詳細を設定します。

- **[サービス グラフの作成（Create Service Graph）]** ウィンドウで、次のサービス デバイスをこの順序でドラッグ アンド ドロップします。
  - ネットワーク ロード バランサ（ハブ VNet 用）
  - サードパーティ ファイアウォール（ハブ VNet 用）
  - アプリケーション ロード バランサ（プロバイダ VNet 用）
- ハブ VNet のネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、次のようにします。
  - **[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、コンシューマ側でリダイレクト機能を有効にします。
  - **[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れ、プロバイダ側でリダイレクト機能を有効にします。

- サード パーティ ファイアウォールの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のボックスをオフのままにします。
- プロバイダ VNet でネットワーク ロード バランサの **[サービス ノード（Service Node）]** ウィンドウで、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** と **[プロバイダ コネクタ タイプ（Provider Connector Type）]** のチェックボックスをオフのままにします。

（注） SNAT がサード パーティのロード バランサで構成されていることを確認します。

4. レイヤ 4 ～ レイヤ 7 サービスを展開します。

   これらの手順については、Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開 （80 ページ） を参照してください。コンシューマとプロバイダの間に存在するコントラクトをサービス グラフにアタッチします。

リダイレクトの注意事項と制約事項

リダイレクトの注意事項と制約事項は次のとおりです。

- レイヤ 4 ～ レイヤ 7 のすべてのサービス デバイスには、独自の専用サブネットが必要です。
- リージョン内の VRF 内レイヤ 4 ～ レイヤ 7 サービスへのリダイレクション：
  - コンシューマ EPG とプロバイダ EPG が同じ VNet にある場合、レイヤ 4 ～ レイヤ 7 サービスへのリダイレクトは、east-west 展開ではサポートされません。
  - 外部 EPG がプロバイダ EPG である場合、コンシューマ EPG とプロバイダ EPG が同じ VNet にあるかどうかに関係なく、レイヤ 4 からレイヤ 7 へのサービス リダイレクトが North-South 展開でサポートされます。
- リージョンでの VRF 間レイヤ 4 からレイヤ 7 サービスへのリダイレクト：
  - リージョン間レイヤ 4 ～ レイヤ 7 サービスへのリダイレクトがサポートされています。ただし、コンシューマ EPG とプロバイダ EPG は拡大しないでください。
  - リージョンでは、同じ VRF にコンシューマ EPG とプロバイダ EPG の両方を含めることはできません。たとえば、リージョン 1 にコンシューマ EPG のみがあり、リージョン 2 にプロバイダ EPG のみがある場合、これはサポートされますが、リージョン 1 にコンシューマ EPG とプロバイダ EPG の両方を含めることはできません。
  - コンシューマおよびプロバイダの EPG は、サブネット ベースの EPG である必要があります。

- レイヤ 4 ～レイヤ 7 サービスへのリダイレクションを伴うリージョン間サービス グラフの場合、サービス デバイスはプロバイダ EPG のリージョンに展開する必要があります。プロバイダ EPG がリージョン全体に拡張されている場合、サービス デバイスは各リージョンに展開する必要があります。
- プロバイダとしての外部 EPG の場合、サービス デバイスはコンシューマ EPG に対してローカルなリージョンに展開する必要があります。コンシューマ EPG が複数のリージョンにまたがっている場合は、サービス デバイスを各リージョンに展開する必要があります。
- コンシューマ VNet とプロバイダ EPG の間では、サービス グラフを介して挿入できるリダイレクト デバイスは 1 つだけです。たとえば、コンシューマ EPG1 とコンシューマ EPG2 がコンシューマ VNet にあり、プロバイダ EPG3 がプロバイダ VNet にある場合、EPG1 と EPG3 間の契約、および EPG2 と EPG3 間の契約に同じリダイレクト デバイスを使用する必要があります。

（注） この制限は、クラウド プロバイダがユーザー定義ルートの特定の宛先に対して 1 つのネクスト ホップのみを許可するためです。

- 次の表に、サポートされている、またはサポートされていない特定のリダイレクト構成に関する情報を示します。
  - NLB はネットワーク ロード バランサの略
  - ALB はアプリケーション ロード バランサの略
  - FW はファイアウォールの略

（注） サードパーティのロードバランサへのリダイレクトはサポートされていません。

サービス チェイン オプション	スポークツースポーク		スポークツー外部へ（コンシューマが話す）		外部ツースポークへ（コンシューマは外部）	
	VNet 内	**VNet 間**	**VNet 内**	**VNet 間**	**VNet 内**	**VNet 間**
NLB/ALB[1] LB(SNAT) 1	サポート対象	サポート対象	非対応	サポート対象外	サポート対象	サポート対象
FW（SNAT なし）[2]	非対応	サポート対象	非対応	サポート対象外	サポート対象外	サポート対象外

サービス チェイン オプション	スポークツースポーク		スポークツー外部へ（コンシューマが話す）		外部ツースポークへ（コンシューマは外部）	
FW（SNAT）リダイレクトは、コンシューマ コネクタで有効になっています。[3]	サポート対象	サポート対象	サポート対象	サポート対象	非対応	サポート対象外
• NLB[2]-FW(no SNAT)[1] • NLB[2]-FW(no SNAT)[1]-NLB/ALB[1] • NLB[2]-FW(no SNAT)[1]-LB(SNAT)[1]	非対応	サポート対象	非対応	サポート対象外	サポート対象外	サポート対象外
NLB[4]-FW(SNAT)[5]	非対応	サポート対象	サポート対象	サポート対象	非対応	サポート対象外
NLB/ALB[1]-FW(SNAT+DNAT)[6]-NLB/ALB[1] NLB/ALB[1]-FW(ANT+DNAT)[6]-LB(SNAT)[1] （リダイレクトなし）	サポート対象	サポート対象	未サポート	非対応	サポート対象	サポート対象
NLB[1]-LB(SNAT)[1] （リダイレクトなし）	サポート対象	サポート対象	未サポート	非対応	サポート対象	サポート対象

[1] コンシューマ コネクタとプロバイダ コネクタの両方でチェックを外すか、オプションは ALB に適用されません。
[2] リダイレクトは、コンシューマ コネクタとプロバイダ コネクタの両方で有効になっています。
[3] プロバイダ コネクタで SNAT が有効になっています。
[4] リダイレクトは、コンシューマ コネクタで有効になっています。プロバイダ コネクタではオフになっています。
[5] コンシューマ コネクタではチェックを外します。プロバイダ コネクタで SNAT が有効になっています。
[6] コンシューマ コネクタではチェックされていません。プロバイダ コネクタで SNAT+DNAT が有効になっています。

Cloud APIC GUI を使用したセカンダリ VRF への新しい CIDR の追加

状況によっては、新しい CIDR を追加したり、セカンダリ VRF で既存の CIDR を編集したりする前に、VNet ピアリングを無効にする必要がある場合があります。これは、アクティブな VNet ピアリングがある場合、VNet 上の CIDR を更新できないという Azure の制限によるものです。CIDR を追加するには、最初にその VNet の VNet ピアリングを削除する必要があります。その後、CIDR を更新できます。CIDR を更新したら、VNet ピアリングを再度有効にすることができます。

これらの手順では、特定のインフラ VNet に関連付けられているすべての VNet ピアリングを削除するハブ ネットワーク ピアリングを無効にする手順について説明します。

- インフラ VNet に追加の CIDR が既に作成されているが、その既存の CIDR にサブネットを追加するだけでよい場合は、それらのサブネットを追加する前に、その特定のインフラ VNet のハブ ネットワーク ピアリングを無効にする必要はありません。既存の CIDR にサブネットを追加するには：

  1. その場合は、適切なクラウド コンテキスト プロファイルに移動します（**[アプリケーション管理（Application Management）]**>**[クラウド コンテキスト プロファイル（Cloud Context Profiles）]**）。
  2. サブネットを既存の CIDR に追加するクラウド コンテキスト プロファイルをダブルクリックし、ステップ 10 （64 ページ） に移動して、新しいサブネットを既存の CIDR に追加します。

- インフラ VNet に新しい CIDR を追加する場合、またはインフラ VNet で CIDR を削除するか、他の方法（サブネットの追加以外）で CIDR を編集する場合は、その特定のインフラ VNet のハブ ネットワーク ピアリングを無効にする必要があります。 。CIDR を追加した後、ハブ ネットワーク ピアリングを再度有効にします。以下の手順では、それらの手順について説明します。

（注） 新しい CIDR をセカンダリ VRF に追加しており、次のリリースで実行しているマルチサイト展開がある場合：

- Cloud APIC のリリース 5.2(1) 以降
- Nexus Dashboard Orchestrator のリリース 3.3 以降

新しい CIDR を追加し、ハブ ネットワーク ピアリングを再度有効にしたら、Nexus Dashboard Orchestrator でサイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を展開する前に、CIDR が起動するまで少なくとも 5 分間待機します。CIDR が Azure に展開されるには時間がかかるため、サイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を展開する前に少なくとも数分待たないと、新しく追加された CIDR が Nexus Dashboard Orchestrator を介してリモート サイトに伝達されない可能性があります。

Nexus Dashboard Orchestrator からインフラ構成を展開した後に、次のエラー メッセージが表示された場合：

```
Invalid configuration CT_Remotectx_cidr: Remote Site CIDR
```

これは、Nexus Dashboard Orchestrator からインフラ構成を展開しする前に十分な時間を待たず、新しく追加された CIDR がリモート サイトに伝達されなかったことを意味します。この場合、次のようになります。

1. Cloud APIC でハブ ネットワーク ピアリングを無効にする
2. Nexus Dashboard Orchestrator でサイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を展開します。
3. Cloud APIC でハブ ネットワーク ピアリングを再度有効にする
4. 少なくとも 5 分（または以前に待機したよりも長い時間）待ってからサイトを更新し、Nexus Dashboard Orchestrator からインフラ構成を再度展開します。

ステップ 1 まだログインしていない場合は、Cloud APIC にログインします。

ステップ 2 左側のナビゲーションバーで、**[アプリケーション管理（Application Management）]** > **[クラウド コンテキスト プロファイル（Cloud Context Profiles）]**に移動します。

既存のクラウドコンテキストプロファイルが表示されます。

ステップ 3 ハブ ネットワーク ピアリングを無効にするクラウド コンテキスト プロファイルをダブルクリックします。

そのクラウド コンテキスト プロファイルの概要ウィンドウが表示されます。この概要ウィンドウの **[ハブ ネットワーク ピアリング（Hub Network Peeri）]** 領域に **[有効（Enabled）]** と表示されます。これは、ハブ ネットワーク ピアリングが有効になっていることを示しています。

ステップ 4 鉛筆アイコンをクリックして、このクラウド コンテキスト プロファイルを編集します。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

ステップ 5 [クラウド コンテキスト プロファイルの編集] ウィンドウで、[ハブ ネットワーク ピアリング] フィールドを見つけ、チェック ボックスをクリックして [有効] フィールドからチェックマークを外します。

[ハブ ネットワーク ピアリング（Hub Network Peering）] オプションを無効にしても、グローバル レベルで VNet ピアリングが削除されるのではなく、この特定のインフラ VNet に関連付けられているすべての VNet ピアリングが削除されます。

ステップ 6 [保存（Save）] をクリックします。

そのクラウドコンテキストプロファイルの概要ウィンドウが再び表示されます。この概要ウィンドウの **[ハブ ネットワーク ピアリング（Hub Network Peeri）]** 領域に **[無効（Disabled）]** と表示されます。これは、ハブ ネットワーク ピアリングが無効になっていることを示しています。

ステップ 7 新しい CIDR を追加するには、鉛筆アイコンをクリックして、このクラウド コンテキスト プロファイルを再度編集します。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

ステップ 8 **[CIDR の追加（Add CIDR）]** をクリックします。

[CIDR の追加（Add CIDR）] ダイアログボックスが表示されます。

ステップ 9 **[CIDR ブロック範囲（CIDR Block Range）]** フィールドに新しい CIDR を追加します。

[プライマリ（Primary）] フィールドのボックスをクリックしないでください（**[プライマリ'（Primary）]** フィールドの **[はい（yes）]** の横のボックスにチェックを入れないでください）。

ステップ 10 **[サブネットの追加（Add subnet）]** をクリックして、必要なサブネットアドレスを **[アドレス（Address）]** に入力します。

必要に応じて、追加のサブネットの **[サブネットの追加（Add Subnet）]** をクリックし続けます。

ステップ 11 **[CIDR の追加（Add CIDR）]** ウィンドウで必要な情報をすべて追加し終わったら、**[追加（Add）]** をクリックします。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

ステップ 12 **[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）]** ウィンドウで情報を確認し、**[保存（Save）]** をクリックします。

そのクラウドコンテキストプロファイルの概要ウィンドウが表示されます。**[CIDR ブロック範囲（CIDR Block Range）]** 領域にリストされた新しい CIDR が表示されます。

ステップ 13 これらの手順の最初にハブ ネットワーク ピアリングを無効にした場合は、この時点で再度有効にします。

a) 鉛筆アイコンをクリックして、このクラウド コンテキスト プロファイルを編集します。

[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）] ウィンドウが表示されます。

b) **[クラウド コンテキスト プロファイルの編集（Edit Cloud Context Profile）]** ウィンドウで、**[ハブ ネットワーク ピアリング（Hub Network Peering）]** フィールドを見つけ、チェック ボックスをクリックして **[有効（Enabled）]** フィールドにチェックマークを追加し、この特定のインフラ VNet の VNet ピアリングを再度有効にします。

c) [保存（Save）] をクリックします。

そのクラウド コンテキスト プロファイルの概要ウィンドウが再び表示されます。この概要ウィンドウの **[ハブ ネットワーク ピアリング（Hub Network Peeri）]** 領域に **[有効（Enabled）]** と表示されます。これは、ハブ ネットワーク ピアリングが再び有効になっていることを示しています。

前に説明したように、この時点で Azure portal にアクセスすると、Azure の overlay-1 VNet にてこれらの手順で追加した追加の CIDR とサブネットが 表示されます。これは、正しく予期される動作です。

サービス グラフの展開

サービス グラフを使用すると、デバイス間のトラフィック フロー、ネットワークへのトラフィックの流入方法、トラフィックが通過するデバイス、およびトラフィックがネットワークから出る方法を定義できます。

サービス グラフは、次の 2 つの方法で展開できます。

- 単一ノード サービス グラフ：1 つのデバイスのみが展開されます。
- マルチノード サービス グラフ：最大 3 つのノードをサービス チェーンに追加できます。

単一ノードまたはマルチキャストノードのいずれかでサービス グラフを展開可能になる前に、以下を構成する必要があります。

1. テナント
2. アプリケーション プロファイル
3. コンシューマ EPG
4. プロバイダーEPG
5. VRF
6. クラウド コンテキスト プロファイル
7. フィルタとの契約

GUI を使用してサービス グラフの展開

次のセクションでは、GUI を使用してサービス グラフを展開する方法について説明します。

Cloud APIC GUI を使用したサービス デバイスの作成

始める前に

このセクションでは、Cisco Cloud APIC GUI を介してサービス グラフで使用できるサービス デバイスを作成する方法について説明します。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが **[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストから、**[サービス（Services）]** > **[デバイス（Devices）]** > **[デバイスの作成（Create Device）]**をクリックします。**[[デバイスの作成（Create Device）]** ダイアログボックスが表示されます。

ステップ 4 次の *[デバイスの作成ダイアログボックスのフィールド（Create Device Dailog Box Fields）]* の表にリストされた各フィールドに該当する値を入力し、続行します。

各タイプのサービス デバイスに固有の情報については、次の表を参照してください。

- アプリケーション ロード バランサについては、4.a （66 ページ） を参照してください。
- ネットワーク ロード バランサについては、4.b （68 ページ） を参照してください。
- サード パーティのロード バランサについては、4.c （73 ページ） を参照してください。
- サードパーティのファイアウォールについては、4.d （74 ページ） を参照してください。

a) アプリケーション ロード バランサに必要な情報を入力します。

[プロパティ（Properties）]	**説明**
全般	
名前	デバイスの名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]**をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択（Select）] をクリックします。**[デバイスの作成（Create Device）]** ダイアログボックスに戻ります。
[設定（Settings）]	

[プロパティ（Properties）]	説明
サービス タイプ	デバイス タイプを選択します。 • アプリケーションロードバランサ
ALB SKU	次から選択します。 • Standard • Standard V2
VM インスタンス数	*[VM インスタンス数（VM Instance Count）]* テキスト ボックスに数値を入力します。 （注） これは、Application Gateway にのみ適用されます。
VM インスタンス サイズ	選択する VM インスタンスのサイズ（**大**、**中**、または**小**）のラジオ ボタンをクリックします。 （注） これは、Application Gateway にのみ適用されます。
スキーム	**[インターネット向け]** または **[内部]** を選択します。 • **インターネット向け**：これは、バランサのパブリック IP を構成するために使用されます。これは Azure によって割り当てられます。 • 内部：クリックして、**[IP アドレスの割り当て（IP Address Assignment）]** で **[動的（Dynamic）]** または **[静的（Static）]** を選択します。 • **動的**：Azure によって動的 IP アドレスが割り当てられます。動的 IP アドレスは、VM が起動するたびに変更されます。 • **静的**：クラウド コンテキスト プロファイルで定義されている CIDR に基づいて IP アドレスを入力し、IP アドレスが ALB と同じサブネットにあることを確認します。 ALB SKU Standard は、静的および動的 IP アドレスをサポートします。ALB SKU Standard V2 は、静的 IP アドレスのみをサポートします。

[プロパティ（Properties）]	説明
サブネット	サブネットを選択するには: 1. **[リージョンの選択（Select Region）]** をクリックします。**[リージョンの選択（Select Region）]** ダイアログボックスが表示されます。**[リージョンの選択（Select Region）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。 2. **[クラウド コンテキスト プロファイルの選択（Select Cloud Context Profile）]** をクリックします。**[クラウド コンテキスト プロファイルの選択（Select Cloud Context Profile）]** ダイアログ ボックスが表示されます。 3. **[サブネットの選択（Select Subnet）]** をクリックします。**[サブネットの選択]** ダイアログボックスが表示されます。静的 IP アドレス テキスト ボックスが表示されます。ロード バランサの IP アドレスを入力します。右の「ティック」マークをクリックして確定します。 4. さらにサブネットを追加するには、手順 a ～ c を繰り返します。

b) ネットワーク ロード バランサに必要な情報を入力します。

表 *3:* ネットワーク ロード バランサの *[デバイスの作成（Create Device）]* ダイアログ ボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	ロード バランサーの名前を入力します。
[設定（Settings）]	
サービス タイプ	デバイス タイプを選択します。 • ネットワーク ロード バランサ

[プロパティ（Properties）]	説明
すべてのトラフィックを許可	**[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にするかどうかを決定します。 **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にすると、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンド アクセスが許可されます。詳細については、「すべてのトラフィックを許可について （9 ページ）」を参照してください。 （注） このオプションを有効にする前に、これによってセキュリティ リスクが発生しないことを確認してください。 • すべてのトラフィックを許可する場合は、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域で、**[有効（Enabled）]** フィールドの横にあるボックスをクリックします。 • すべてのトラフィックを許可しない場合は、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域で、**[有効（Enabled）]** フィールドの横のボックスをオフ（選択解除）したままにします。
スキーム	**[インターネット向け]** または **[内部]** を選択します。 • **インターネット向け**：これは、バランサのパブリック IP を構成するために使用されます。これは Azure によって割り当てられます。 • リリース 25.0(3) より前のリリースでは、**インターネット向け**オプションの選択は、1 つのデフォルトのパブリック フロントエンド IP アドレスのみを構成するために使用されます。 • リリース 25.0(3) 以降では、このページの **[フロントエンド IP 名（Frontend IP Names）]** フィールドでの選択に応じて、**インターネット向けオプション**を選択して、単一のデフォルト パブリック フロントエンド IP アドレスまたは複数のパブリック フロントエンド IP アドレスを構成できます。。 • 内部：クリックして、**[IP アドレスの割り当て（IP Address Assignment）]** で **[動的（Dynamic）]** または **[静的（Static）]** を選択します。 • **動的**：Azure によって動的 IP アドレスが割り当てられます。動的 IP アドレスは、VM が起動するたびに変更されます。 • **静的**：クラウド コンテキスト プロファイルで定義されている CIDR に基づいて IP アドレスを入力し、IP アドレスが NLB と同じサブネットにあることを確認します。静的 IP アドレスは、ロード バランサに関連付けられます。 （注） Cloud APIC は、標準の SKU NLB のみを作成します。

[プロパティ（Properties）]	説明
カスタム リソース グループ	必要に応じて、カスタム リソース グループの名前を入力します。
Subnets	サブネットを選択するには: **1.** **[+ サブネットの追加 (+Add Subnet)]** をクリックします。 **2.** **[リージョンの選択（Select Region）]** をクリックします。**[リージョンの選択（Select Region）]** ダイアログボックスが表示されます。 **[リージョンの選択（Select Region）]** ダイアログで、左側の列のテナントをクリックして選択し、**[選択（Select）]** をクリックします。 **3.** **[クラウド コンテキスト プロファイルの選択（Select Cloud Context Profile）]** をクリックします。**[クラウド コンテキスト プロファイルの選択（Select Cloud Context Profile）]** ダイアログ ボックスが表示されます。 **[クラウド コンテキスト プロファイル（Select Cloud Context Profile）]** ダイアログで、左側の列のクラウド コンテキスト プロファイルをクリックして選択し、**[選択（Select）]** をクリックします。 **4.** **[サブネットの選択（Select Subnet）]** をクリックします。**[サブネットの選択]** ダイアログボックスが表示されます。 **[サブネット の選択（Select Subnet）]** ダイアログで、左側の列のサブネットをクリックして選択し、**[選択（Select）]** をクリックします。 **5.** 右の「ティック」マークをクリックして確定します。 **6.** さらにサブネットを追加するには、**[+ サブネットの追加（+ Add Subnet）]** を再度クリックして、これらの手順を繰り返します。
詳細設定	下矢印をクリックして、**[詳細設定（Advanced Settings）]** 領域を展開します。 次のエントリが表示されます。

[プロパティ（Properties）]	説明
フロントエンド IP 名	

[プロパティ（Properties）]	説明
	リリース 25.0(3) 以降、インターネット向けのネットワーク ロード バランサに対して複数のフロントエンド IP アドレスを構成するためのサポートが利用可能になりました。 • デフォルトでは、インターネット向けのネットワーク ロード バランサ用に単一のフロントエンドIPアドレスが自動的に作成されます。これは、リリース 25.0(3) 以前で利用可能な既存の機能です。 • インターネット向けネットワーク ロード バランサに追加のフロントエンド IP アドレスが必要な場合は、**[+ フロントエンド IP 名の追加（+ Add Frontend IP Name）]** をクリックします。これは、リリース 25.0(3) で導入された新機能です。詳細については、Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について （6 ページ）を参照してください。 この領域にフロントエンドIP名を追加すると、このインターネット向けネットワーク ロード バランサに複数のフロントエンド IP アドレスを割り当てることが Azure に通知されます。この領域に入力する各フロントエンド IP 名は、単一の追加フロントエンド IP アドレスになります。 この領域のパブリック フロントエンド IP アドレス (既定のフロントエンド IP アドレスと追加のフロントエンド IP アドレス) は、Azure によって割り当てられます。 1. **[+ フロントエンド IP 名の追加（+ Add Frontend IP Name）]** をクリックして、Azure でネットワーク ロード バランサに割り当てる追加のフロントエンド IP アドレスの名前を追加します。 2. 追加のフロントエンド IP アドレスの名前を入力し、右側のチェック マークをクリックして新しいフロントエンド IP 名を確認します。 3. **[+ フロントエンド IP 名の追加（+ Add Frontend IP Name）]** を再度クリックして、Azure でネットワーク ロード バランサに割り当てる追加のフロントエンド IP アドレスの名前を追加します。 たとえば、インターネット向けのネットワーク ロード バランサに合計 3 つのフロントエンド IP アドレスが必要だとします。 • 3 つのフロントエンド IP アドレスの最初のアドレスは、リリース 25.0(3) より前に使用できる既存の動作を使用して、デフォルトで自動的に割り当てられます。 • 次に、**[+ フロントエンド IP 名の追加（+ Add Frontend IP Name）]** を 2 回クリックし、2 つの個別のフロントエンド IP 名（たとえば、`frontend2` と `frontend3`）を入力して、インターネット向けネットワーク ロード バランサに対して合計 3 つのフロントエンド IP アドレスを割り当てることを Azure に通知します。

[プロパティ（Properties）]	説明
	デフォルトおよび構成済みのフロントエンド IP 名に関連付けられたフロントエンド IP アドレスを表示するには： 1. **[アプリケーション管理（Application Management）]** > **[サービス（Services）]** > **[デバイス（Devices）]** に移動します。 2. 構成されたサービス デバイスをダブルクリックして、そのサービス デバイスの **[概要（Overview）]** ページを表示します。 3. **[クラウド リソース（Cloud Resources）]** > **[フロントエンド IP 名（Frontend IP Names）]** をクリックします。 デフォルトのフロントエンド IP アドレスは、この詳細ページの [デフォルト（Default）] タグとともに表示されます。

c) サード パーティ ロード バランサに必要な情報を入力します。

表 *4:* サード パーティ ロード バランサの *[デバイスの作成（Create Device）]* ダイアログ ボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	デバイスの名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択（Select）] をクリックします。**[デバイスの作成（Create Device）]** ダイアログボックスに戻ります。
[設定（Settings）]	
サービスの種類	デバイス タイプを選択します。 • サードパーティ ロード バランサ
作成モード	**[セレクタ（Selectors）]** を選択します。 **[VRF]** および **[インターフェイス（Interfaces）]** フィールドが表示されます。

[プロパティ（Properties）]	説明
VRF	**[VRF の選択（Select VRF）]** をクリックします。開いている [VRF の選択（Select VRF）] ダイアログで、クリックして左の列の VRF を選択します。[選択（Select）] をクリックします。
インターフェイス	[インターフェイスの追加（Add Interface）] をクリックします。**[インターフェイス（Interfaces）]** ウィンドウが表示されます。 **1. [インターフェイス設定（Interface Settings）]** フィールドで外部インターフェイスの名前を入力します。 **2. [インターフェイス セレクタの追加（Add Interface selector）]** をクリックします。 **3. [インターフェイス セレクタの設定（Interface Selector Settings）]** ページで、インターフェイスの名前を入力します。 **4. [一致式（Match Expressions ）]** フィールドで、**[一致式（Match Expressions ）]** をクリックして選択します。 • **キー**：これは、IP、リージョン、またはカスタム ベースのタグ セレクタです。 • **演算子**：これは、equal、not equals、in、not in、key あり、または key なしのいずれかです。 • **値**：サード パーティのロード バランサの外部または内部ネットワークの IP アドレス。 **5.** チェック マークをクリックしてインターフェイスを追加し、**[保存（Save）]**（[インターフェイス ウィンドウ）をクリックします。 **6. [保存（Save）]**（[デバイスの作成（Create Device）] ウィンドウ）をクリックします。 **[インターフェイスの追加（Add Interface）]** をクリックし、手順 a ～ e を繰り返して、さらにインターフェイスを追加します。 （注） サードパーティのロードバランサインターフェイスは、マルチノード サービス グラフに展開する場合、サブネット ベースのセレクタで構成する必要があります。

d) サード パーティ ファイアウォールに必要な情報を入力します。

表 *5 :* サード パーティ ファイアウォールの *[*デバイスの作成（***Create Device***）*]* ダイアログ ボックスのフィールド

[プロパティ（Properties）]	説明
全般	
名前	デバイスの名前を入力します。
[設定（Settings）]	
サービス タイプ	デバイス タイプを選択します。 • サードパーティ ファイアウォール （注） サードパーティのファイアウォールをマルチノード サービス グラフの最初のデバイスにすることはできません。
VRF	VRF を選択するには、次の手順を実行します。 1. **[VRF の選択（Select VRF）]** をクリックします。**[VRF の選択（Select VRF）]** ダイアログボックスが表示されます。 2. **[VRF の選択（Select VRF）]** ダイアログで、左側の列の VRF をクリックして選択し、**[選択（Select）]** をクリックします。

[プロパティ（Properties）]	説明
インターフェイス	[インターフェイスの追加（Add Interface）] をクリックします。 **[設定]** ページが表示されます。 **1.** **[名前（Name）]** フィールドに、インターフェイスの名前を入力します。 **2.** **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にするかどうかを決定します。 **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを有効にすると、インターフェイスが属するサブネットへのすべてのインバウンドおよびアウトバウンドアクセスが許可されます。詳細については、「すべてのトラフィックを許可について （9 ページ）」を参照してください。 （注） このオプションを有効にする前に、これによってセキュリティ リスクが発生しないことを確認してください。 • すべてのトラフィックを許可する場合は、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域で、**[有効（Enabled）]** フィールドの横にあるボックスをクリックします。 • すべてのトラフィックを許可しない場合は、**[すべてのトラフィックを許可（Allow All Traffic）]** 領域で、**[有効（Enabled）]** フィールドの横のボックスをオフ（選択解除）したままにします。 **3.** **[インターフェイス セレクタの追加（Add Interface Selector）]** をクリックします。 **4.** インターフェイス セレクタの名前を入力します。 **5.** **[一致式（Match Expressions）]** をクリックして選択します。 • **キー**：これは、IP、リージョン、またはカスタム ベースのタグ セレクタです。 • **演算子**：これは、equal、not equals、in、not in、key あり、または key なしのいずれかです。 • **値**：アプリ、Web、内部ネットワーク、管理ネットワーク、または外部ネットワークの IP アドレス。 **6.** [追加] をクリックします。 **7.** 手順 a から f を繰り返して、さらにインターフェイスを追加します。

ステップ 5 設定が終わったら [Save] をクリックします。

ステップ 6 **[サービス グラフの作成（Create Service Graph）]** ダイアログボックスが表示されます。**[別のサード パーティ ファイアウォールを作成（Create another Third Party Firewall）]** をクリックして、別のデバイスを作成します。**[[デバイスの作成（Create Device）]** ダイアログボックスが表示されます。

（注） UI は通常、以前に作成したデバイスを作成するように求めます。ただし、それをクリックすると、**[デバイスの作成（Create Device）]** ページに戻ります。ここで、作成する必要があるデバイスを選択できます。最初のデバイスは、サード パーティのファイアウォールにしないでください。

Cisco Cloud APIC GUIを使用したサービス グラフ テンプレートの作成

このセクションでは、Cisco Cloud APIC GUI を使用した単一ノードまたはマルチノード向けサービス グラフ テンプレートの作成方法について説明します。

始める前に

デバイスはすでに作成されています。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]**検索ボックスの下にあるドロップダウン矢印をクリックし、**[アプリケーション管理（Application Management）]** を選択します。

[アプリケーション管理（Application Management）] オプションのリストが**[インテント（Intent）]** メニューに表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[アプリケーション管理（Application Management）]** リストで、**[サービス（Services）]** > **[サービス グラフ（Service Graph）]** > **[サービス グラフの作成（Create Service Graph）]** をクリックします。**[サービス グラフの作成（Create Service Graph）]** ポップアップが表示されます。**[では始めましょう（Let's Get Started）]** をクリックします。

ステップ 4 次の *[サービス グラフの作成ダイアログ ボックスのフィールド（Create Service Graph Dialog Box Fields）]* の表に示されているように、各フィールドに適切な値を入力し、続行します。

表 *6*：サービス グラフの作成ダイアログ ボックスのフィールド（単一ノード向け）

[プロパティ（Properties）]	**説明**
全般	
名前	サービス グラフ テンプレートの名前を入力します。

[プロパティ（Properties）]	説明
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択（Select）] をクリックします。**[サービス グラフの作成（Create Service Graph）]** ダイアログボックスに戻ります。
説明	サービス グラフ テンプレートの説明を入力します。
[設定（Settings）]	
デバイスを選択	デバイスを選択します。 1. **[デバイスの選択（Select Device）]** をクリックします。**[デバイスの選択（Select Device）]** ダイアログが表示されます。 2. 左側の列から、デバイスをクリックして選択します。下の**[デバイスのドロップ（Drop Device）]** スペースにデバイスをドラッグ アンド ドロップします。これにより、このデバイス タイプの実際のデバイスを選択できる小さなウィンドウが開きます。 3. [選択（Select）] をクリックします。**[サービス グラフの作成（Create Service Graph）]** ダイアログボックスに戻ります。

表 *7:* サービス グラフの作成ダイアログ ボックスのフィールド（マルチノード向け）

[プロパティ（Properties）]	説明
全般	
名前	サービス グラフ テンプレートの名前を入力します。
テナント	テナントを選択します。 1. **[テナントの選択（Select Tenant）]** をクリックします。**[テナントの選択（Select Tenant）]** ダイアログが表示されます。 2. 左側の列から、クリックしてテナントを選択します。 3. [選択（Select）] をクリックします。**[サービス グラフの作成（Create Service Graph）]** ダイアログボックスに戻ります。
説明	サービス グラフ テンプレートの説明を入力します。

[プロパティ（Properties）]	説明
設定：必要なトポロジに基づいて、デバイスを下のボックスにドラッグ アンド ドロップします。	
アプリケーション ロード バランサ	1. アプリケーション ロード バランサ デバイスを下のボックスにドラッグ アンド ドロップします。 2. **[サービス ノード（Service node）]** ダイアログ ボックスで、**[アプリケーション ロード バランサの選択（Select Application Load Balancer）]** をクリックし、左側の列で [アプリケーション ロード バランサ（Application Load Balancer）] をクリックして選択し、**[追加（Add）]** をクリックします。
サードパーティ ファイアウォール	1. 下のボックスでデバイスの隣にサードパーティ ファイアウォールをドラッグアンド ドロップします。 2. **[サービス ノード（Service node）]** ダイアログ ボックスで、**[サード パーティ ファイアウォール（Third Party Firewall）]** をクリックし、左側の列で [サードパーティ ファイアウォール（Third Party Firewall）] をクリックして選択し、**[追加（Add）]** をクリックします。 （注） サード パーティ ファイアウォールをサービス グラフの最初のノードにすることはできません。 3. サードパーティ ファイアウォールのコンシューマ側でユーザー ベースのリダイレクト機能を有効にする場合は、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れます。 4. サードパーティ ファイアウォールのプロバイダ側でユーザー ベースのリダイレクト機能を有効にする場合は、**[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れます。 5. **[プロバイダ コネクタ タイプ（Provider Connector Type）]** で、該当するオプションの横にチェックを入れます。詳細については、「レイヤ4～レイヤ7サービス リダイレクト」を参照してください。 6. [追加] をクリックします。

[プロパティ（Properties）]	説明
ネットワーク ロード バランサ	1. ネットワーク ロードバランサデバイスを下のボックスにドラッグアンドドロップします。 2. **[サービス ノード（Service node）]** ダイアログ ボックスで、**[ネットワーク ロード バランサの選択（Select Network Load Balancer）]** をクリックし、左側の列で [ネットワーク ロード バランサ（Network Load Balancer）] をクリックして選択し、**[追加（Add）]** をクリックします。 3. ネットワーク ロードバランサのコンシューマ側でユーザーベースのリダイレクト機能を有効にする場合は、**[コンシューマ コネクタ タイプ（Consumer Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れます。 4. ネットワーク ロードバランサのプロバイダ側でユーザーベースのリダイレクト機能を有効にする場合は、**[プロバイダ コネクタ タイプ（Provider Connector Type）]** フィールドで、**[リダイレクト（Redirect）]** オプションの隣のボックスにチェックを入れます。 5. [追加] をクリックします。
サードパーティ ロードバランサ	1. サード パーティのロード バランサ デバイスを下のボックスにドラッグ アンド ドロップします。 2. **[サービス ノード（Service node）]** ダイアログ ボックスで、**[サード パーティ ロード バランサの選択（Select Third Party Load Balancer）]** をクリックし、左側の列でサード パーティ ロード バランサをクリックして選択します。 3. **[コンシューマ インターフェイスの選択（Select Consumer Interface）]** をクリックします。外部としてマークされたインターフェースを選択します。 4. **[プロバイダ インターフェイスの選択（Select Provider Interface）]** をクリックします。内部としてマークされたインターフェイスを選択します。 5. **[追加（Add）]** をクリックします。

ステップ 5 設定が終わったら [Save] をクリックします。

ステップ 6 **[EPG 通信（EPG Communication）]** ダイアログボックスが表示されます。**[詳細に移動（Go to details）]** をクリックして、サービス グラフ テンプレートを確認します。

Cisco Cloud APIC GUI を使用したレイヤ 4 からレイヤ 7 サービスの展開

このセクションでは、レイヤ4～ レイヤ7サービスを展開する方法について説明します。この手順は、シングル ノードおよびマルチノードの展開に適用できます。

始める前に

- デバイスを構成しました。
- サービス グラフが構成されました。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 **[インテント（Intent）]** 検索ボックスの下のドロップダウン□をクリックし、**[構成（Configuration）]** を選択します。

[インテント（Intent）] の **[構成（Configuration）]** オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]**メニューの **[構成（Configuration）]** リストで、**[EPG Communication]** をクリックします。**[EPG通信（EPG Communication）]** ダイアログボックスに、**コンシューマ EPG**、**コントラクト**、および**プロバイダー EPG**の情報が表示されます。

ステップ 4 コントラクトを選択します。

a) **[コントラクトの選択（Select Contract）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが表示されます。

b) **[コントラクトの選択（Select Contract）]** ダイアログの左側のペインで、契約をクリックして選択し、**[選択（Select）]** をクリックします。**[コントラクトの選択（Select Contract）]** ダイアログ ボックスが閉じます。

ステップ 5 コンシューマ EPG を追加するには、次の手順を実行します。

a) **[コンシューマ EPG の追加（Add Consumer EPGs）]** をクリックします。**[コンシューマー EPG の選択（Select Consumer EPGs）]** ダイアログが表示されます。

b) **[コンシューマ EPG の選択（Select Consumer EPGs）]** ダイアログの左側のペインで、チェック ボックスをクリックして、クラウドEPG（内部向けロードバランサの場合）またはクラウド外部EPG(インターネット向けロードバランサの場合) を選択します。**[選択（Select）]** をクリックします。**[コンシューマ EPG の選択（Select Consumer EPGs）]** ダイアログボックスが閉じます。

ステップ 6 プロバイダー EPG を追加するには、次の手順を実行します。

a) **[プロバイダー EPG の追加（Add Provider EPGs）]** をクリックします。**[プロバイダー EPG の選択（Select Provider EPGs）]** ダイアログが表示されます。

b) **[プロバイダ EPG の選択（Select Provider EPGs）]** ダイアログの左側のペインで、チェックボックスをオンにしてプロバイダ EPG を選択し、**[選択]** をクリックします。**[プロバイダー EPG の選択（Select Provider EPGs）]** ダイアログボックスが閉じます。

ステップ 7 サービス グラフを選択するには:

a) **[EPF 通信の構成（EPG Communication Configuration）]** ダイアログで、**[サービス グラフの選択（Select Service Graph）]** をクリックします。**[サービス グラフの選択（Select Service Graph）]** ダイアログボックスが表示されます。

b) **[サービス グラフの選択（Select Service Graph）]** ダイアログの左側のペインで、サービス グラフをクリックして選択し、**[選択（Select）]** をクリックします。**[サービス グラフの選択（Select Service Graph）]** ダイアログボックスが閉じます。

ステップ 8 **[サービス グラフのプレビュー（Service Graph Preview）]** で、**[クラウド ロード バランサ リスナーの追加（Add Cloud Load Balancer Listner）]** をクリックします。**[クラウド ロード バランサ リスナーの追加（Add Cloud Load Balancer Listner）]** ダイアログが表示され、リスナーを追加できます。

リスナーは、デバイスが動作するポートとプロトコルです。

ステップ 9 次の *[クラウドロードバランサ リスナーの追加ダイアログボックスのフィールド（Add Cloud Load Balancer Listener Dialog Box Fields）]* テーブルでリストされた各フィールドに該当する値を入力し、続行します。

表 *8*: アプリケーション ゲートウェイ用クラウド ロード バランサ リスナーの追加ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（Name）	リスナーの名前を入力します。
[ポート（Port）]	デバイスがトラフィックを受け入れるポートを入力します。
プロトコル	Application Gateway の場合は、クリックして **[HTTP]** または **[HTTPS]** を選択します。
Security Policy	ドロップダウンリストをクリックし、セキュリティポリシーを選択します **(HTTPS** が選択されている場合にのみ選択可能)。
SSL 証明書（SSL Certificate）	SSL 証明書を選択するには **(HTTPS** が選択されている場合にのみ選択可能): **1.** **[SSL 証明書の追加]** をクリックします。 **2.** クリックして、追加する証明書のチェックボックスをオンにします。 **3.** キー リングを選択してください: **1.** **[キー リングの選択]** をクリックします。**[キー リンクの選択（Select Key Ring）]** ダイアログが表示されます。 **2.** **[キー リンクの選択（Select Key Ring）]** ダイアログで、左側の列のキー リングをクリックして選択し、**[選択（Select）]** をクリックします。**[キー リンクの選択（Select Key Ring）]** ダイアログボックスが閉じます。 **4.** **[証明書ストア]** ドロップダウンリストをクリックして、証明書を選択します。 （注） リスナーは複数の証明書を持つことができます。
ルールの追加	ルール設定をデバイス リスナーに追加するには、**[ルールの追加]** をクリックします。**[ルール]** リストに新しい行が表示され、**[ルール設定]** フィールドが有効になります。

[プロパティ（**Properties**）]	説明
ルール設定	

[プロパティ（Properties）]	説明
	[ルール設定（Rule Settings）] ペインで、次のオプションを設定します。 • **名前** ：規則の名前を入力します。 • **ホスト**：ホスト名を入力して、ホストベースの条件を作成します。このホスト名に対して要求が行われると、指定したアクションが実行されます。 • **パス**：パスを入力して、パスベースの条件を作成します。このパスに対して要求が行われると、指定したアクションが実行されます。 • **タイプ**：アクションタイプは、実行するアクションをデバイスに通知します。アクション タイプのオプション: • **固定応答を返す**：次のオプションを使用して応答を返します。 • **固定応答本文**：応答メッセージを入力します。 • **固定応答コード**：応答コードを入力します。 • **固定の応答コンテンツ タイプ**：コンテンツ タイプを選択します。 • **転送**：次のオプションを使用してトラフィックを転送します。 • **ポート**：デバイスがトラフィックを受け入れるポートを入力します。 • **プロトコル**：**[HTTP]** または **[HTTPS]** を選択します。 • **プロバイダー EPG**：トラフィックを処理する Web サーバーを持つ EPG。 • **EPG**：EPG を選択するには: 1. **[EPG の選択]** をクリックします。**[EPG の選択]** ダイアログボックスが表示されます。 2. **[EPG の選択]** ダイアログで、左側の列の EPG をクリックして選択し、**[選択（Select）]** をクリックします。**[EPG の選択]** ダイアログボックスが閉じます。 • **リダイレクト**：次のオプションを使用して、リクエストを別の場所にリダイレクトします。 • **リダイレクト コード**：**[リダイレクト コード]** ドロップダウン リストをクリックして、コードを選択します。 • **リダイレクト ホスト名** ：リダイレクトのホスト名を入力します。 • **リダイレクト パス**：リダイレクト パスを入力します。 • **リダイレクト ポート**：デバイスがトラフィックを受け入れるポートを入力します。

[プロパティ（Properties）]	説明
	• **リダイレクト プロトコル**：**[リダイレクト プロトコル（Redirect Protocol）]** ドロップダウン リストをクリックして、**[HTTP]**、**[HTTPS]**、または **[継承（Inherit）]** を選択します。 • **リダイレクト クエリ**：リダイレクト クエリを入力します。
正常性チェック（Health Checks）	アプリケーション ロードバランサは、高可用性のためにバックエンドプール ターゲットでヘルス チェックを実行します。これは、ヘルス チェックで構成できます。 • **プロトコル**：**[HTTP]** または **[HTTPS]** を選択します。 • **パス**：パスを入力します。 デフォルトは / です • **ポート**：ヘルスチェックを実行するポートを入力します。 • **詳細設定** **異常なしきい値**：このしきい値を構成して、バックエンド ターゲットが異常であると通知されるタイミングを決定します。 • **タイムアウト**：ヘルス チェックのタイムアウトの値を入力します。 • **間隔**：チェックを実行する間隔を決定する時間を秒単位で入力します。 • **成功コード**：成功コードを入力します。デフォルトは 200 ～ 399 です。 • **ルールからホストを使用**：ホスト名をルールから選択する必要がある場合は、チェックボックスをクリックします。 • **ホスト**：**[ルールのホストを使用（Use host from rule）]** がチェックされていない場合は、ヘルス チェックに使用するホスト名を指定します。 完了したら、**[ルールの追加]** をクリックします。

表 *9:* ネットワーク ロード バランサ用クラウド ロード バランサ リスナーの追加ダイアログボックスのフィールド

[プロパティ（Properties）]	説明
名前（Name）	リスナーの名前を入力します。
プロトコル	クリックして **[TCP]** または **[UDP]** を選択します。
[ポート（Port）]	デバイスがトラフィックを受け入れるポートを入力します。

[プロパティ（Properties）]	説明
フロントエンド IP 名	クラウド ロード バランサ リスナーを構成するフロントエンド IP アドレスを選択します。 • **デフォルト IP を使用**：デフォルトのフロントエンド IP アドレスでクラウド ロード バランサ リスナーを構成するには、このオプションを選択します。これは、リリース 25.0(3) 以前で利用可能な既存の機能です。 • **<frontend_ip_name>**：このオプションを選択して、Cloud APIC GUI を使用したサービス デバイスの作成 （66 ページ） でこのインターネット向けネットワーク ロードバランサのサービスデバイスを作成したときに構成した、フロントエンド IP 名に関連付けられた追加のフロントエンド IP アドレスにクラウド ロード バランサー リスナーを構成します。これは、リリース 25.0(3) で導入された新機能です。 詳細については、Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について （6 ページ）を参照してください。
ルール設定	**[ルール設定（Rule Settings）]** ペインで、次のオプションを設定します。 • **名前** ：規則の名前を入力します。 • **アクション タイプ**：デフォルトで [転送先（Forward to）] に設定されています。トラフィックは、以下で選択したプロトコルを使用して、選択した EPG のポートに転送されます。 • **ポート**：バックエンド プール サーバがロードバランサからのトラフィックを受け入れるポートを入力します。 • **プロトコル**：クリックして **[TCP]** または **[UDP]** を選択します。 • **EPG**：Web サーバがトラフィックを処理する EPG。
正常性チェック（Health Checks）	ロード バランサは、高可用性のためにバックエンド プール ターゲットでヘルス チェックを実行します。ここで構成できます。· • **プロトコル**：クリックして **[TCP]**、**[HTTP]** または **[HTTPS]** を選択します。 • **ポート**：ヘルス チェックを実行するポートを入力します。 • **詳細設定** 異常なしきい値 - このしきい値を構成して、バックエンド ターゲットが異常であると通知されるタイミングを決定します。 • **間隔**：チェックを実行する間隔を決定する時間を秒単位で入力します。 終了したら、[Add] をクリックします。

ステップ 10 終了したら、[Add] をクリックします。
サービス グラフが展開されます。

REST API を使用したサービス グラフの展開

次のセクションでは、REST API を使用してサービス グラフを展開する方法について説明します。

REST API を使用したインターネット向けロード バランサの作成

この例では、REST API を使用して内部向けのロード バランサを作成する方法を示します。

ステップ 1 アプリケーション ゲートウェイ（アプリケーション ロード バランサ）の内部向けロード バランサを作成するには：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />
        <cloudLB scheme="internal" type="application" name="alb-151-15" status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]"/>
        </cloudLB>
      </fvTenant>
</polUni>
```

ステップ 2 Azure ロードバランシング（ネットワーク ロードバランサ）の内部向けロードバランサを作成するには：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[subscription id]-vendor-azure" />
        <cloudLB scheme="internal" type="network" name="nlb-151-15" status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]" />
        </cloudLB>
    </fvTenant>
</polUni>
```

ステップ 3 すべてのトラフィックを許可について （9 ページ） で説明されている **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを使用して、Azure ロード バランシング（ネットワーク ロード バランサ）用の内部向けロード バランサを作成するには、次の手順を実行します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[subscription id]-vendor-azure" />
        <cloudLB scheme="internal" type="network" name="nlb-151-15" allowAll="true" status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]" />
        </cloudLB>
    </fvTenant>
</polUni>
```

REST API を使用したインターネット向けロード バランサの構成

この例では、REST API を使用してインターネット向けのロード バランサを作成する方法を示します。

ステップ 1 アプリケーション ゲートウェイ（アプリケーション ロード バランサ）のインターネット向けロード バランサを作成するには：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />

        <cloudLB scheme="internet" type="application" name="alb-151-15" status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]"/>
        </cloudLB>


      </fvTenant>
</polUni>
```

ステップ 2 インターネット向けネットワーク ロード バランサ：

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->

<polUni>
    <fvTenant name="tn15">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[<subscription id>]-vendor-azure" />
        <cloudLB scheme="internet" type="network" name="nlb-151-15" status="">
            <cloudVip name="IP1"/>
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn15/ctxprofile-cProfilewestus151/cidr-[15.151.0.0/16]/subnet-[15.151.2.0/24]" />
        </cloudLB>
    </fvTenant>
</polUni>
```

この例では、以下のようになっています。

- cloudLB ラインは、単一のデフォルト IP アドレスを持つインターネット向けのネットワーク ロード バランサを作成するために使用されます。これは、リリース 25.0(3) 以前で利用可能な既存の機能です。
- cloudVip ラインは、インターネットに接続するネットワーク ロード バランサの追加フロントエンド IP アドレスを作成するために使用されます。これは、リリース 25.0(3) で導入された新機能です。詳細については、Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について （6 ページ）を参照してください。

REST API を使用したサードパーティ ファイアウォールの作成

この例では、REST API を使用したサードパーティ ファイアウォールを作成する方法を示します。

ステップ 1 サードパーティ ファイアウォールを作成するには：

例：

```
<cloudLDev name="HubFW" svcType="FW" status="">
    <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-overlay-2"/>
    <cloudLIf name="provider">
       <cloudEPSelector name="east" matchExpression="IP=='{{eastus_FwUntrustSubnet}}'" status=""/>

    </cloudLIf>
    <cloudLIf name="consumer">
        <cloudEPSelector name="east" matchExpression="IP=='{{eastus_FwTrustSubnet}}'" status=""/>
    </cloudLIf>
</cloudLDev>
```

ステップ 2 すべてのトラフィックを許可について （9 ページ） で説明されている **[すべてのトラフィックを許可（Allow All Traffic）]** オプションを使用してサードパーティ ファイアウォールを作成するには、次の手順を実行します。

例：

```
<cloudLDev name="HubFW" svcType="FW" status="">
    <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-overlay-2"/>
    <cloudLIf name="provider"  allowAll="true" status="">
        <cloudEPSelector name="1" matchExpression="IP=='10.1.1.0/28'" status=""/>
    </cloudLIf>
    <cloudLIf name="consumer"  allowAll="true" status="">
        <cloudEPSelector name="east" matchExpression="IP=='10.1.2.0/28'" status=""/>
    </cloudLIf>
</cloudLDev>
```

REST API を使用したサードパーティ ロード バランサの作成

この例では、REST API を使用してサードパーティ ロード バランサを作成する方法を示します。

この例では、REST API を使用してサードパーティ ロード バランサを作成する方法を示します。

例：

```
<cloudLDev name="ThirdPartyLB" svcType="ADC" status="">
    <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-overlay-2"/>
    <cloudLIf name="external">
        <cloudEPSelector name="ExtInterfaceSelector" matchExpression="IP=='{{ExtInterfaceSubnet}}'"
 status=""/>
    </cloudLIf>
    <cloudLIf name="internal">
        <cloudEPSelector name="IntInterfaceSelector" matchExpression="IP=='{{IntInterfaceSubnet}}'"
 status=""/>
    </cloudLIf>
</cloudLDev>
```

アプリケーション ゲートウェイの REST API を使用してサービス グラフの作成

この例では、REST API を使用してサービス グラフを作成する方法を示します。

この例では、REST API を使用してサービス グラフを作成する方法を示します。

アプリケーション ゲートウェイのサービス グラフを作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">

       <vnsAbsGraph name="c15_g1" type="cloud" status="">
      <vnsAbsTermNodeProv name="p1">
        <vnsAbsTermConn/>
      </vnsAbsTermNodeProv>
      <vnsAbsTermNodeCon name="c1">
        <vnsAbsTermConn/>
      </vnsAbsTermNodeCon>
      <vnsAbsNode managed="yes" name="N1" funcType="GoTo">
          <vnsRsNodeToCloudLDev tDn="uni/tn-tn15/clb-alb-151-15"/>
        <vnsAbsFuncConn name="provider"/>
        <vnsAbsFuncConn name="consumer"/>
      </vnsAbsNode>
      <vnsAbsConnection  connDir="consumer" connType="external" name="con1">
          <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeCon-c1/AbsTConn"/>
         <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-consumer"/>

      </vnsAbsConnection>
      <vnsAbsConnection connDir="provider" connType="internal"  name="con2">
          <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeProv-p1/AbsTConn"/>
         <vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-provider"/>

      </vnsAbsConnection>
```

```
  </vnsAbsGraph>

  </fvTenant>
</polUni>
```

Azure ロード バランサの REST API を使用してサービス グラフを作成する

Azure ロード バランサのサービス グラフを作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- api/node/mo/uni/.xml -->

<polUni>

<fvTenant name="tn15">

<vnsAbsGraph name="c15_g1" type="cloud" status="">

<vnsAbsTermNodeProv name="p1">

<vnsAbsTermConn />

</vnsAbsTermNodeProv>

<vnsAbsTermNodeCon name="c1">

<vnsAbsTermConn />

</vnsAbsTermNodeCon>

<vnsAbsNode managed="yes" name="N1" funcType="GoTo">

<vnsRsNodeToCloudLDev tDn="uni/tn-tn15/clb-nlb-151-15" />

<vnsAbsFuncConn name="provider" />

<vnsAbsFuncConn name="consumer" />

</vnsAbsNode>

<vnsAbsConnection connDir="consumer" connType="external" name="con1">

<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeCon-c1/AbsTConn"
/>

<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-consumer"
 />

</vnsAbsConnection>

<vnsAbsConnection connDir="provider" connType="internal" name="con2">

<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsTermNodeProv-p1/AbsTConn"
/>

<vnsRsAbsConnectionConns tDn="uni/tn-tn15/AbsGraph-c15_g1/AbsNode-N1/AbsFConn-provider"
 />

</vnsAbsConnection>
```

```
</vnsAbsGraph>

</fvTenant>

</polUni>
```

サード パーティ ロード バランサの REST API を使用してサービス グラフを作成する

サードパーティのロードバランサのサービス グラフを作成するには、次の手順を実行します。

```
<polUni>
<fvTenant name="infra" >
<!-- Abs Graph Creation -->
<vnsAbsGraph name="{{graphName}}" uiTemplateType="UNSPECIFIED" type="cloud" status="">
<vnsAbsTermNodeProv name="T2">
<vnsOutTerm/>
<vnsInTerm />
<vnsAbsTermConn attNotify="no" name="1" />
</vnsAbsTermNodeProv>
<vnsAbsTermNodeCon name="T1" >
<vnsOutTerm/>
<vnsInTerm />
<vnsAbsTermConn attNotify="no" name="1" />
</vnsAbsTermNodeCon>
<vnsAbsNode funcTemplateType="ADC_TWO_ARM" name="{{F5Name}}" managed="no">
<vnsRsNodeToCloudLDev tDn="uni/tn-infra/cld-{{F5Name}}" />
<vnsAbsFuncConn attNotify="no" name="consumer" deviceLIfName="external"/>
<vnsAbsFuncConn attNotify="no" name="provider" deviceLIfName="internal"/>
</vnsAbsNode>
<vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="ConsTermToF5">
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsTermNodeCon-T1/AbsTConn"/>
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsNode-{{F5Name}}/AbsFConn-consumer"/>
</vnsAbsConnection>
<vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="F5ToProv">
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsNode-{{F5Name}}/AbsFConn-provider" />
<vnsRsAbsConnectionConns
tDn="uni/tn-infra/AbsGraph-{{graphName}}/AbsTermNodeProv-T2/AbsTConn"/>
</vnsAbsConnection>
</vnsAbsGraph>
</fvTenant>
</polUni>
```

REST API を使用してマルチノード サービス グラフを作成する

この例では、REST API を使用してマルチノード サービス グラフを作成する方法を示します。

マルチノード サービス グラフを作成するには、次の例のような投稿を入力します。

```
<polUni>
 <fvTenant name="tn12_iar_iavpc" status="">
  <fvRsCloudAccount  tDn="uni/tn-infra/[SubscriptionId]-vendor-azure"/>
  <fvCtx name="vrf50" status=""/>
  <fvCtx name="vrf60" status=""/>
  <cloudVpnGwPol name="VgwPol0"/>
```

```
<cloudCtxProfile name="c50" status="">
 <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus"/>
 <cloudRsToCtx tnFvCtxName="vrf50"/>
 <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
 <cloudCidr addr="12.3.0.0/16" primary="true" status="">
  <cloudSubnet ip="12.3.30.0/24" status="" name="GatewaySubnet" usage="gateway">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.2.0/24" status="" name="ALBSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.1.0/24" status="" name="FwMgmtSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.3.0/24" status="" name="FwUntrustSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.4.0/24" status="" name="FwTrustSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.3.5.0/24" status="" name="ConsumerSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus/zone-default"/>
  </cloudSubnet>
 </cloudCidr>
</cloudCtxProfile>
<cloudCtxProfile name="c60" status="">
 <cloudRsCtxProfileToRegion tDn="uni/clouddomp/provp-azure/region-westus2"/>
 <cloudRsToCtx tnFvCtxName="vrf60"/>
 <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
 <cloudCidr addr="12.4.0.0/16" primary="true" status="">
  <cloudSubnet ip="12.4.1.0/24" status="" name="ProviderSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus2/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.4.2.0/24" status="" name="NLBSubnet">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus2/zone-default"/>
  </cloudSubnet>
  <cloudSubnet ip="12.4.30.0/24" status="" name="GatewaySubnet" usage="gateway">
   <cloudRsZoneAttach tDn="uni/clouddomp/provp-azure/region-westus2/zone-default"/>
  </cloudSubnet>
 </cloudCidr>
</cloudCtxProfile>
<cloudApp name="ap50" status="">
 <cloudEPg name="ap50vrf50epg1" status="">
  <cloudRsCloudEPgCtx tnFvCtxName="vrf50"/>
  <fvRsCons tnVzBrCPName="con50"/>
  <fvRsProv tnVzBrCPName="con60"/>
  <cloudEPSelector matchExpression="IP=='12.3.5.0/24'" name="100"/>
 </cloudEPg>
 <cloudEPg name="ap50vrf50epg2" status="">
  <cloudRsCloudEPgCtx tnFvCtxName="vrf50"/>
  <fvRsProv tnVzBrCPName="con60"/>
  <cloudEPSelector matchExpression="IP=='12.3.1.0/24'" name="100"/>
 </cloudEPg>
 <cloudExtEPg routeReachability="internet" name="ap50extepg1">
  <cloudExtEPSelector name="1" subnet="0.0.0.0/0"/>
  <cloudRsCloudEPgCtx tnFvCtxName="vrf50"/>
  <fvRsCons tnVzBrCPName="con60"/>
 </cloudExtEPg>
</cloudApp>
<cloudApp name="ap60" status="">
 <cloudEPg name="ap60vrf60epg1" status="">
  <cloudRsCloudEPgCtx tnFvCtxName="vrf60"/>
  <fvRsProv tnVzBrCPName="con50"/>
  <fvRsProv tnVzBrCPName="con70"/>
```

```
    <cloudEPSelector matchExpression="IP=='12.4.1.0/24'" name="100"/>
   </cloudEPg>
   <cloudExtEPg routeReachability="internet" name="ap60extepg1">
    <cloudExtEPSelector name="1" subnet="0.0.0.0/0"/>
    <cloudRsCloudEPgCtx tnFvCtxName="vrf60"/>
    <fvRsCons tnVzBrCPName="con70"/>
   </cloudExtEPg>
  </cloudApp>
  <vzBrCP name="con50" scope="tenant" status="">
   <vzSubj name="con50">
    <vzRsSubjFiltAtt tnVzFilterName="f10"/>
    <vzRsSubjGraphAtt tnVnsAbsGraphName="g1" status=""/>
   </vzSubj>
  </vzBrCP>
  <vzBrCP name="con60" scope="tenant" status="">
   <vzSubj name="con60">
    <vzRsSubjFiltAtt tnVzFilterName="f20"/>
   </vzSubj>
  </vzBrCP>
  <vzBrCP name="con70" scope="context" status="">
   <vzSubj name="con70">
    <vzRsSubjFiltAtt tnVzFilterName="f20"/>
   </vzSubj>
  </vzBrCP>
  <vzFilter name="f10" status="">
   <vzEntry etherT="ip" prot="icmp" name="f10entry1" status=""/>
   <vzEntry etherT="ip" prot="udp" dFromPort="1" dToPort="65535" name="f10entry2" status=""/>
   <vzEntry etherT="ip" prot="tcp" dFromPort="1" dToPort="65535" name="f10entry3" status=""/>
  </vzFilter>
  <vzFilter name="f20" status="">
   <vzEntry etherT="ip" prot="tcp" dFromPort="http" dToPort="http" name="f20entry1" status=""/>
   <vzEntry etherT="ip" prot="tcp" dFromPort="https" dToPort="https" name="f20entry2" status=""/>
   <vzEntry etherT="ip" prot="tcp" dFromPort="22" dToPort="22" name="f20entry3" status=""/>
  </vzFilter>
  <cloudLB name="FrontALB" type="application" scheme="internal" >
   <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn12_iar_iavpc/ctxprofile-c50/cidr-[12.3.0.0/16]/subnet-[12.3.2.0/24]"/>
  </cloudLB>
  <cloudLDev name="FW" svcType="FW" status="">
   <cloudRsLDevToCtx tDn="uni/tn-tn12_iar_iavpc/ctx-vrf50" />
   <cloudLIf name="provider" >
    <cloudEPSelector name="1" matchExpression="custom:tagp=='trustFW'"/>
   </cloudLIf>
   <cloudLIf name="consumer" >
    <cloudEPSelector name="1" matchExpression="custom:tagp=='untrustFW'"/>
   </cloudLIf>
  </cloudLDev>
  <cloudLB name="BackNLB" type="network" scheme="internal" >
   <cloudRsLDevToCloudSubnet
tDn="uni/tn-tn12_iar_iavpc/ctxprofile-c60/cidr-[12.4.0.0/16]/subnet-[12.4.2.0/24]"/>
  </cloudLB>
  <vnsAbsGraph name="g1" type="cloud" status=""  >
   <vnsAbsTermNodeProv name="Input1" >
    <vnsAbsTermConn  name="C1"/>
   </vnsAbsTermNodeProv>
   <vnsAbsTermNodeCon descr="" name="Output1" nameAlias="" ownerKey="" ownerTag="">
    <vnsAbsTermConn name="C2" />
   </vnsAbsTermNodeCon>
   <vnsAbsNode funcType="GoTo" name="N1" managed="yes" funcTemplateType="ADC_ONE_ARM" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-tn12_iar_iavpc/clb-FrontALB" />
    <vnsAbsFuncConn attNotify="no" descr="" name="provider" nameAlias="" ownerKey="" ownerTag=""/>
    <vnsAbsFuncConn attNotify="no" descr="" name="consumer" nameAlias="" ownerKey="" ownerTag=""/>
    <cloudSvcPolicy tenantName="tn12_iar_iavpc" contractName="con50" subjectName="con50" >
     <cloudListener name="http_listener1" port="80" protocol="http">
```

```
      <cloudListenerRule name="rule1" priority="20" default="yes" >
       <cloudRuleAction type="forward" port="80" protocol="http"/>
      </cloudListenerRule>
     </cloudListener>
    </cloudSvcPolicy>
   </vnsAbsNode>
   <vnsAbsNode funcType="GoTo" name="N2" managed="no" funcTemplateType="ADC_TWO_ARM" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-tn12_iar_iavpc/cld-FW" />
    <vnsAbsFuncConn attNotify="no" descr="" connType="snat_dnat" name="provider" nameAlias=""
ownerKey="" ownerTag=""/>
    <vnsAbsFuncConn attNotify="no" descr="" connType="none" name="consumer" nameAlias="" ownerKey=""
 ownerTag=""/>
   </vnsAbsNode>
   <vnsAbsNode funcType="GoTo" name="N3" managed="yes" funcTemplateType="ADC_ONE_ARM" >
    <vnsRsNodeToCloudLDev tDn="uni/tn-tn12_iar_iavpc/clb-BackNLB" />
    <vnsAbsFuncConn attNotify="no" descr="" name="provider" nameAlias="" ownerKey="" ownerTag=""/>
    <vnsAbsFuncConn attNotify="no" descr="" name="consumer" nameAlias="" ownerKey="" ownerTag=""/>
    <cloudSvcPolicy tenantName="tn12_iar_iavpc" contractName="con50" subjectName="con50" >
     <cloudListener name="http_listener1" port="80" protocol="tcp">
      <cloudListenerRule name="rule1" priority="20" default="yes" >
       <cloudRuleAction type="forward" port="80" protocol="tcp"
epgdn="uni/tn-tn12_iar_iavpc/cloudapp-ap60/cloudepg-ap60vrf60epg1"/>
      </cloudListenerRule>
     </cloudListener>
    </cloudSvcPolicy>
   </vnsAbsNode>
   <vnsAbsConnection connDir="provider" connType="external" name="CON4">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N3/AbsFConn-provider"/>

    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsTermNodeProv-Input1/AbsTConn"/>

   </vnsAbsConnection>
   <vnsAbsConnection  connDir="consumer" connType="external" name="CON1">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsTermNodeCon-Output1/AbsTConn"/>

    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N1/AbsFConn-consumer"/>

   </vnsAbsConnection>
   <vnsAbsConnection  connDir="consumer" connType="external" name="CON2">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N1/AbsFConn-provider"/>

    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N2/AbsFConn-consumer"/>

   </vnsAbsConnection>
   <vnsAbsConnection  connDir="consumer" connType="external" name="CON3">
    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N2/AbsFConn-provider"/>

    <vnsRsAbsConnectionConns tDn="uni/tn-tn12_iar_iavpc/AbsGraph-g1/AbsNode-N3/AbsFConn-consumer"/>

   </vnsAbsConnection>
  </vnsAbsGraph>
 </fvTenant>
</polUni>
```

REST API を使用してリダイレクトでマルチノード サービス グラフを作成する

この例では、REST API を使用してマルチノード サービス グラフを作成する方法を示します。

ステップ 1 インフラ テナントを設定するには、次の手順を実行します。

```
<polUni>
    <fabricInst>
        <commPol name="default">
            <commSsh name="ssh" adminSt="enabled" passwordAuth="enabled" />
        </commPol>
        <dnsProfile name="default">
            <dnsProv addr="172.23.136.143" preferred="yes" status=""/>
        </dnsProfile>
    </fabricInst>
   <fvTenant name="infra">
      <fvRsCloudAccount tDn="uni/tn-infra/act-[{{subscriptionId}}]-vendor-azure"/>
      <cloudAccount name="insbu" id="{{subscriptionId}}" vendor="azure" accessType="credentials"
status="">
        <cloudRsCredentials tDn="uni/tn-infra/credentials-cApicApp"/>
      </cloudAccount>
      <cloudCredentials name="cApicApp" keyId="{{accessKeyId}}" key="{{accessKey}}" httpProxy="">
        <cloudRsAD tDn="uni/tn-infra/ad-{{adId}}"/>
      </cloudCredentials>
    <cloudAD name="CiscoINSBUAd" id="{{adId}}" />
    <cloudApicSubnetPool subnet="10.10.1.0/24" />
    <cloudtemplateInfraNetwork name="default" numRoutersPerRegion="2" vrfName="overlay-1"
numRemoteSiteSubnetPool="1" status="">
         <cloudtemplateProfile name="default" routerUsername="cisco" routerPassword="ins3965" />
         <cloudtemplateExtSubnetPool subnetpool="11.11.0.0/16" status=""/>
         <cloudtemplateExtNetwork name="default" status="">
            <cloudRegionName provider="azure" region="{{region}}" />
            <cloudtemplateVpnNetwork name="default">
               <cloudtemplateIpSecTunnel peeraddr="{{peerAddress}}"/>
               <cloudtemplateOspf area="0.0.0.1" />
            </cloudtemplateVpnNetwork>
         </cloudtemplateExtNetwork>
         <cloudtemplateIntNetwork name="default">
            <cloudRegionName provider="azure" region="{{region}}"/>
         </cloudtemplateIntNetwork>
    </cloudtemplateInfraNetwork>
   </fvTenant>
   <cloudDomP>
      <cloudBgpAsP asn="1111"/>
      <cloudProvP vendor="azure">
         <cloudRegion adminSt="managed" name="{{region}}">
            <cloudZone name="default"/>
         </cloudRegion>
      </cloudProvP>
  </cloudDomP>
</polUni>
```

ステップ 2 ハブ VNet でサービス デバイスを構成するには:

```
<polUni>
    <fvTenant name="infra">
        <fvRsCloudAccount tDn="uni/tn-infra/act-[{{subscriptionId}}]-vendor-azure"/>
        <cloudCtxProfile name="ct_ctxprofile_{{region}}" status="modified">
          <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-{{region}}"/>

            <cloudCidr name="cidr1" addr="{{HubCidrSvc}}" primary="no" status="">
                <cloudSubnet ip="{{HubNLBSubnet}}" name="HubNLBSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="{{HubFWSubnetInt}}" name="HubFWSubnetInt" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
```

```
                </cloudSubnet>
                <cloudSubnet ip="{{HubFWSubnetExt}}" name="HubFWSubnetExt" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="{{HubFWMgmtSubnet}}" name="HubFWMgmtSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="{{ConsHubEPgSubnet}}" name="ConsHubEPgSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
             </cloudCidr>
        </cloudCtxProfile>
        <cloudLDev name="{{FWName}}" status="">
            <cloudRsLDevToCtx tDn="uni/tn-infra/ctx-{{ServicevVNetName}}"/>
            <cloudLIf name="external" >
                <cloudEPSelector matchExpression="custom:EPG=='FwExt'"  name="1"/>
            </cloudLIf>
            <cloudLIf name="internal" >
               <cloudEPSelector matchExpression="custom:EPG=='FwInt'"  name="1"/>
            </cloudLIf>
        </cloudLDev>
       <cloudLB name="{{NLBName}}" type="network" scheme="internal" size="small" instanceCount="2"
 status="">
            <cloudRsLDevToCloudSubnet
tDn="uni/tn-infra/ctxprofile-ct_ctxprofile_{{region}}/cidr-[{{HubCidrSvc}}]/subnet-[{{HubNLBSubnet}}]"
 status=""/>
        </cloudLB>
    </fvTenant>
</polUni>
```

ステップ 3 プロバイダとスポークのグラフを構成するには:

```
<polUni>
    <fvTenant name="{{tnNameProv}}" status="" >
        <fvRsCloudAccount tDn="uni/tn-infra/act-[{{subscriptionId}}]-vendor-azure"/>
        <fvCtx name="{{ProviderVNetName}}"/>
        <cloudCtxProfile name="{{ProviderVNetName}}" status="">
            <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
           <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-{{region}}"/>

            <cloudRsToCtx tnFvCtxName="{{ProviderVNetName}}"/>
            <cloudCidr name="cidr1" addr="{{VnetCidrProv}}" primary="yes" status="">
                <cloudSubnet ip="{{ProviderSubnet}}" name="ProviderSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
                <cloudSubnet ip="{{BackALBSubnet}}" name="BackALBSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
        <!-- contract-->
        <vzFilter descr="" name="HttpsFilter" ownerKey="" ownerTag="">
            <vzEntry dFromPort="443" dToPort="443" etherT="ip" name="https" prot="tcp" status=""/>
            <vzEntry dFromPort="80" dToPort="80" etherT="ip" name="http" prot="tcp" status=""/>
            <vzEntry dFromPort="22" dToPort="22" etherT="ip" name="ssh" prot="tcp" status=""/>
        </vzFilter>
        <vzBrCP name="{{contractName}}" scope="global" status="">
            <vzSubj name="Sub1" revFltPorts="yes">
```

```
                <vzRsSubjGraphAtt directives="" tnVnsAbsGraphName="{{graphName}}"/>
                <vzRsSubjFiltAtt tnVzFilterName="HttpsFilter"/>
            </vzSubj>
        </vzBrCP>
        <!-- cloud App Profile-->
        <cloudApp name="provApp" status="">
            <cloudEPg name="App" status="">
                <cloudRsCloudEPgCtx tnFvCtxName="{{ProviderVNetName}}"/>
                <cloudEPSelector matchExpression="custom:EPG=='App'" name="1"/>
                <fvRsProv status="" tnVzBrCPName="{{contractName}}"/>
                <fvRsProv tnVzBrCPName="mgmt_common"/>
            </cloudEPg>
        </cloudApp>
        <!-- Abs Graph Creation -->
        <vnsAbsGraph name="{{graphName}}" uiTemplateType="UNSPECIFIED" type="cloud">
            <vnsAbsTermNodeProv name="T2">
                <vnsOutTerm/>
                <vnsInTerm />
                <vnsAbsTermConn attNotify="no" name="1" />
            </vnsAbsTermNodeProv>
            <vnsAbsTermNodeCon name="T1" >
                <vnsOutTerm/>
                <vnsInTerm />
                <vnsAbsTermConn attNotify="no" name="1" />
            </vnsAbsTermNodeCon>
            <vnsAbsNode  name="{{NLBName}}" managed="yes" >
                <vnsRsNodeToCloudLDev tDn="uni/tn-infra/clb-{{NLBName}}" status=""/>
                <cloudSvcPolicy tenantName="{{tnNameProv}}" contractName="{{contractName}}"
subjectName="Sub1" status="">
                  <cloudHealthProbe name="http_listener1-rule1" protocol="tcp" port=22 interval=15
 unhealthyThreshold=2/>
                    <cloudListener name="http_listener1" port="80" protocol="tcp" status="">
                        <cloudListenerRule name="rule1" default="true">
                            <cloudRuleAction type="haPort" port="80" protocol="tcp"
healthProbe="http_listener1-rule1"/>
                        </cloudListenerRule>
                    </cloudListener>
                </cloudSvcPolicy>
                <vnsAbsFuncConn attNotify="no" name="provider" connType="redir"/>
                <vnsAbsFuncConn attNotify="no" name="consumer" connType="redir"/>
            </vnsAbsNode>
            <vnsAbsNode funcTemplateType="FW_ROUTED" name="{{FWName}}" managed="no">
                <vnsRsNodeToCloudLDev tDn="uni/tn-infra/cld-{{FWName}}" />
                <vnsAbsFuncConn attNotify="no" name="consumer" deviceLIfName="internal"/>
                <vnsAbsFuncConn attNotify="no" name="provider" deviceLIfName="internal"/>
            </vnsAbsNode>
            <vnsAbsNode  name="{{BackALBName}}" managed="yes">
                <vnsRsNodeToCloudLDev tDn="uni/tn-{{tnNameProv}}/clb-{{BackALBName}}"/>
                <cloudSvcPolicy tenantName="{{tnNameProv}}" contractName="{{contractName}}"
subjectName="Sub1" status="">
                    <cloudListener name="http_listener1" port="80" protocol="http" status="">
                        <cloudListenerRule name="rule1" default="true">
                            <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-{{tnNameProv}}/cloudapp-provApp/cloudepg-App"/>
                        </cloudListenerRule>
                    </cloudListener>
                </cloudSvcPolicy>
                <vnsAbsFuncConn attNotify="no" name="provider"/>
                <vnsAbsFuncConn attNotify="no" name="consumer"/>
            </vnsAbsNode>
           <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="ConsTermToNLB">
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsTermNodeCon-T1/AbsTConn"/>
```

```
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{NLBName}}/AbsFConn-consumer"/>
              </vnsAbsConnection>
             <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="NLBToFW">
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{NLBName}}/AbsFConn-provider" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{FWName}}/AbsFConn-consumer"/>
              </vnsAbsConnection>
             <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="FWToBackALB">
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{FWName}}/AbsFConn-provider" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{BackALBName}}/AbsFConn-consumer"/>
              </vnsAbsConnection>
             <vnsAbsConnection adjType="L3" connDir="provider" connType="external" directConnect="no"
 name="BackALBToProv">
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsNode-{{BackALBName}}/AbsFConn-provider" />
                <vnsRsAbsConnectionConns
tDn="uni/tn-{{tnNameProv}}/AbsGraph-{{graphName}}/AbsTermNodeProv-T2/AbsTConn"/>
              </vnsAbsConnection>
        </vnsAbsGraph>
        <cloudLB name="{{BackALBName}}" type="application" scheme="internal" size="small"
instanceCount="2">
              <cloudRsLDevToCloudSubnet
tDn="uni/tn-{{tnNameProv}}/ctxprofile-{{ProviderVNetName}}/cidr-[{{VnetCidrProv}}]/subnet-[{{BackALBSubnet}}]"
 status=""/>
        </cloudLB>
  </fvTenant>
</polUni>
```

ステップ 4 コンシューマを構成し、プロバイダで定義されたコントラクトをインポートするには:

```
<polUni>
    <fvTenant name="{{tnNameCons}}" >
        <fvRsCloudAccount tDn="uni/tn-infra/act-[{{subscriptionId}}]-vendor-azure"/>
        <fvCtx name="{{ConsumerVNetName}}"/>
        <cloudCtxProfile name="{{ConsumerVNetName}}" status="">
            <cloudRsCtxProfileToGatewayRouterP tDn="uni/tn-infra/gwrouterp-default" status=""/>
           <cloudRsCtxProfileToRegion status="" tDn="uni/clouddomp/provp-azure/region-{{region}}"/>

            <cloudRsToCtx tnFvCtxName="{{ConsumerVNetName}}"/>
            <cloudCidr name="cidr1" addr="{{VnetCidrCons}}" primary="yes" status="">
                <cloudSubnet ip="{{ConsumerSubnet}}" name="ConsumerSubnet" status="">
                    <cloudRsZoneAttach status=""
tDn="uni/clouddomp/provp-azure/region-{{region}}/zone-default"/>
                </cloudSubnet>
            </cloudCidr>
        </cloudCtxProfile>
        <vzCPIf name="imported_{{contractName}}">
            <vzRsIf tDn="uni/tn-{{tnNameProv}}/brc-{{contractName}}" />
        </vzCPIf>
        <!-- cloud App Profile-->
        <cloudApp name="consApp" status="">
            <cloudEPg name="Web" status="">
                <cloudRsCloudEPgCtx tnFvCtxName="{{ConsumerVNetName}}"/>
                <cloudEPSelector matchExpression="custom:EPG=='Web'" name="1"/>
                <fvRsConsIf tnVzCPIfName="imported_{{contractName}}"/>
                <fvRsProv tnVzBrCPName="mgmt_common"/>
            </cloudEPg>
```

```
        </cloudApp>
  </fvTenant>
</polUni>
```

REST API を使用してサービス グラフを添付する

この例では、REST API を使用してサービス グラフを作成する方法を示します。

ステップ 1 Application Gateway のサービス グラフをアタッチするには:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/node/mo/uni/.xml -->
<polUni>
    <fvTenant name="tn15">

    <vzBrCP name="c1">
        <vzSubj name="c1">
            <vzRsSubjGraphAtt tnVnsAbsGraphName="c15_g1"/>
      </vzSubj>
    </vzBrCP>

  </fvTenant>
</polUni>
```

ステップ 2 Azure Load Balancing のサービス グラフをアタッチするには:

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- api/node/mo/uni/.xml -->

<polUni>

<fvTenant name="tn15">

<vzBrCP name="c1">

<vzSubj name="c1">

<vzRsSubjGraphAtt tnVnsAbsGraphName="c15_g1" />

</vzSubj>

</vzBrCP>

</fvTenant>

</polUni>
```

REST API を使用した HTTPS サービス ポリシーの構成

この例では、REST API を使用して HTTP サービス ポリシーを作成する方法を示します。

ステップ 1 Application Gateway の HTTP サービス ポリシーを作成するには：

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="http_listener1" port="80" protocol="http" status="">
            <cloudListenerRule name="rule1" priority="10" default="yes" status="">
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
            </cloudListenerRule>
            <cloudListenerRule name="redirectRule" priority="20">
              <cloudRuleCondition type="path" value="/img/*"/>
              <cloudRuleAction type="redirect" RedirectPort="8080"/>
            </cloudListenerRule>
            <cloudListenerRule name="FixedRspRule" priority="30">
              <cloudRuleCondition type="host" value="example.com"/>
              <cloudRuleAction type="fixedResponse" FixedResponseCode="200"/>
            </cloudListenerRule>
            <cloudListenerRule name="redirectHPRule" priority="40" status="">
              <cloudRuleCondition type="host" value="example.com"/>
              <cloudRuleCondition type="path" value="/img/*"/>
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t2/cloudapp-ap/cloudepg-provEPG"/>
            </cloudListenerRule>
          </cloudListener>
        </cloudSvcPolicy>
      </vnsAbsNode>
    </vnsAbsGraph>
  </fvTenant>
</polUni>
```

ステップ 2 ネットワーク ロード バランサの HTTP サービス ポリシーを作成するには：

```
<?xml version="1.0" encoding="UTF-8"?>

<polUni>
    <fvTenant name="tn15">
        <vnsAbsGraph name="CloudGraph" type="cloud" status="">
            <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
                <cloudSvcPolicy tenantName=" tn15" contractName="httpFamily" subjectName="consubj">

                    <cloudListener name="tcp_listener" port="80" protocol="tcp" status="">
                        <cloudListenerRule name="rule1" priority="10" default="yes" status="">
                            <cloudRsListenerToVip tDn="uni/tn-infra/clb-NLB/vip-IP1" status=""/>
                            <cloudRuleAction type="forward" port="80" protocol="tcp" epgdn="uni/tn-
 tn15/cloudapp-ap/cloudepg-provEPG" />
                        </cloudListenerRule>
                    </cloudListener>
                    <cloudListener name="udp_listener" port="55" protocol="udp" status="">
                        <cloudListenerRule name="rule1" priority="10" default="yes" status="">
                            <cloudRsListenerToVip tDn="uni/tn-infra/clb-NLB/vip-IP1" status=""/>
                            <cloudRuleAction type="forward" port="55" protocol="udp" epgdn="uni/tn-
 tn15/cloudapp-ap/cloudepg-provEPG" />
                        </cloudListenerRule>
                    </cloudListener>
                </cloudSvcPolicy>
            </vnsAbsNode>
        </vnsAbsGraph>
```

```
    </fvTenant>
</polUni>
```

このドキュメントで前述したように、ネットワーク ロードバランサで定義されている場合、リスナー ルールとルールアクションの設定は、ロードバランサのフロントエンド構成からバックエンドプールへのマッピングを構築します。この例では、以下のようになっています。

- `cloudListenerRule` 行は、単一のフロントエンド IP アドレスを使用してリスナーを構成するために使用されますが、Cisco Cloud APIC 上のインターネットに接続されたネットワーク ロード バランサ用に異なるポートとプロトコルの組み合わせを使用します。これは、リリース 25.0(3) 以前で利用可能な既存の機能です。
- `cloudRsListenerToVip` 行は、Cisco Cloud APIC 上のインターネット向けネットワーク ロード バランサの複数のフロントエンドでリスナー ルールを構成するために使用されます。各フロントエンドは、フロントエンド IP アドレス、ポート、およびプロトコルのタプルの組み合わせとして表されます。これは、リリース 25.0(3) で導入された新機能です。詳細については、Azure Network Load Balancer の複数のフロントエンド IP アドレスの構成について （6 ページ）を参照してください。

REST API を使用したキー リングの設定

この例では、REST API を使用したキー リングのリーク ルートを構成する方法を示します。キー リング構成の詳細については、*Cisco APIC* 基本構成ガイドを参照してください。

（注） この手順は、アプリケーション ゲートウェイにのみ適用されます。

キー リングを設定するには:

```
<polUni>
     <fvTenant name="tn15" >
    <cloudCertStore>
    <pkiKeyRing status="" name="lbCert" tp="lbTP" key="-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEA4DGxaK+RHv/nToHLnmDBq2BfLimgX/zNJQC9bGuzr8Mj7dm0
XuHfQYGv0h1PtL4Pdxf5qjB0NbHjAVB1Gw8cDiErEgAXy9Km27ySo2foKryNqCRe
Ginn/CgF75QPIed568eScNDZPt/eMeHAuRX/PykKUatWWncGanjvHqc+SOLPF6TD
gQ5nwOHHFvyM2DY8bfdYWrWmGsO7JqZzbPMptA2QWblILsSoIrdkIIgf6ZfYy/EN
bH+nYN2rJT8lzYsxz0YmR0oRQHTiN2NiDY/ZV63yxCXfLg9qpNZCuD8KOfdCZPEq
8takiWBxiR5/HRPscWAdWQsoiKgG1k4NEbFA9QIDAQABAoIBAQDQqA9IslYrdtqN
q6mZ3s2BNfF/4kgb7gn0DWs+9EJJLCJNZVhFEo2ZxxyfPp6HRnjYS50W83/E1anD
+GD1bSucTuxqFWIQVh7r1ebYZIWk+NYSjr5yNVxux8U2hCNNV8WWVqkJjKcUqICB
Bm47FKj53LV46zE0gyCaibFrYxZJ9+farGneyBdnoV+3thmez7534KCi0t3J3Eri
lgSY3ql6hPXB2ZXAP4jdAoLgWDU4I1M6OqOiWopZM/QYIE/WtPYyJ0QzNCXObtc5
FboDcvedsgd4x5GlfV2A4xTBQMCTZUZJ9fYAcFogTZXD+UVqxorh47tf/mz+1fjq
f1XphEDlAoGBAPVlvKfGW46qqRnYovfryxxz4OMlsVSgcJpQTQtBQi2koJ8OwEZJ
2s+CX0r+oDqwP23go/QEVYVkcic9RGkJBNge1+dm/bTjzgMQYtqSCNtecTsZD5JN
y1jkciizznDkjcjReSZ2kh3dGXIbRiYk7ezp2z7EKfDrHe5x5ouGMgCnAoGBAOnh
buDEohv8KJaB+DiUfhtoa3aKNPBO+zWPCHp0HFGjPXshJcIYZc1GcycmuDKVNnDd
MxhE/yOnQHowi4T9FMLpz5yh5zuCUVqOBgB1P6MzbC5t5MtLrEYr/AqFN11CqyXQ
cVcT6iCW1OAFJRw3c/OiESwLMzchsl8RnbwOi6kDAoGBANVlzmPb07zB3eGTCU0t
KGiqwFLncUkVaDZZRFZYPpNwiRkoe73j9brkNbgCqxW+NLp5UjoeFry0N6y106q/
ZA4I7FnXryLBw2HYuw41Vixl+XOZ/HeO3RmFN1z717dGmaGbv43aKIB9x+X5n8wF
```

```
6z1NtBHmBk7yNwom1IRag1sbAoGAX0p4cJ/tJNXSe7AswHDQCL68uimJdDfZ5nKG
k83nE+Qc0qQozDJAmCiSFmuSNRnSep3FiafjBFXK0X4h+mdbJCc7bagRnI92Mh0X
mOwsp4P2GdywkZwdbuHQ6UBp1Ferf9aztzTn+as6xKOUATEezy9DK9zMWzQhhtaY
m9yZTp0CgYEA1UtcpWjAzQbXODJGmxGdAAakPpeiKw/Da3MccrTdGJt88ezM1Oej
Pdoab0G2PcfgJZoTSGk7N4XArVKeq7pgZ0kwcYAshO6A2Hal+D1z/bGoZP+kmD/x
Ny82phxYOXCnEc5Vv92lU59+j7e067UFLAYJe6fu+oFImvofRnP4DIQ=
-----END RSA PRIVATE KEY-----" cert="-----BEGIN CERTIFICATE-----
MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRIwEAYDVQQK
EwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3JnMRgwFgYDVQQDFA8qLmFtYXpvbmF3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY2lzY28uY29tMB4XDTE4MTAw
MjIwNTMwNVoXDTE5MTAwMjIwNTMwNVowgY0xCzAJBgNVBAYTAlVTMQswCQYDVQQI
EwJDQTERMA8GA1UEBxMIU2FuIEpvc2UxEjAQBgNVBAoTCU15Q29tcGFueTEOMAwG
A1UECxMFTXlPcmcxGDAWBgNVBAMUDyouYW1hem9uYXdzLmNvbTEgMB4GCSqGSIb3
DQEJARYRcmFtc2hhaEBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDgMbFor5Ee/+dOgcueYMGrYF8uKaBf/M0lAL1sa7OvwyPt2bRe4d9B
ga/SHU+0vg93F/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXvlA8h53nrx5Jw0Nk+394x4cC5Ff8/KQpRq1ZadwZqeO8epz5I4s8XpMOBDmfA
4ccW/IzYNjxt91hataYaw7smpnNs8ym0DZBZuUguxKgit2QgiB/pl9jL8Q1sf6dg
3aslPyXNizHPRiZHShFAdOI3Y2INj9lXrfLEJd8uD2qk1kK4Pwo590Jk8Sry1qSJ
YHGJHn8dE+xxYB1ZCyiIqAbWTg0RsUD1AgMBAAGjgfUwgfIwHQYDVR0OBBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMEgbowgbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIGNMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNV
BAcTCFNhbiBKb3NlMRIwEAYDVQQKEwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3Jn
MRgwFgYDVQQDFA8qLmFtYXpvbmF3cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY2lzY28uY29tggkApY2On/9qsGwwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAe/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iuR84mQzhoT
nx5CN109xu5ml5baCYZZsSnn6D7usC092bPA/kRCGxt29gkjpWA74tJHqIhVWgbM
mOrLiSHoelewv+wRl0oVRChlTfKtXO68TUk6vrqpw76hKfOHIa7b2h1IIMdq6VA/
+A5FQ0xqYfqKdVd2RaINpzI8mqZiszqw+7E6j1PL5k4tftWEaYpfGPlVesFEyJEL
gHBUiPt8TIbaMYI8qUQmB/emnLXeKQ5PRxdRnleA3h8jfq3D1CQRTLjmDL3tpFwg
qopM6et5ZKqShX4T87BsgZIoiquzXqsuHg==
-----END CERTIFICATE-----">
    </pkiKeyRing>


    <pkiTP status="" name="lbTP" certChain="-----BEGIN CERTIFICATE-----
MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCFNhbiBKb3NlMRIwEAYDVQQK
EwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3JnMRgwFgYDVQQDFA8qLmFtYXpvbmF3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY2lzY28uY29tMB4XDTE4MTAw
MjIwNTMwNVoXDTE5MTAwMjIwNTMwNVowgY0xCzAJBgNVBAYTAlVTMQswCQYDVQQI
EwJDQTERMA8GA1UEBxMIU2FuIEpvc2UxEjAQBgNVBAoTCU15Q29tcGFueTEOMAwG
A1UECxMFTXlPcmcxGDAWBgNVBAMUDyouYW1hem9uYXdzLmNvbTEgMB4GCSqGSIb3
DQEJARYRcmFtc2hhaEBjaXNjby5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDgMbFor5Ee/+dOgcueYMGrYF8uKaBf/M0lAL1sa7OvwyPt2bRe4d9B
ga/SHU+0vg93F/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXvlA8h53nrx5Jw0Nk+394x4cC5Ff8/KQpRq1ZadwZqeO8epz5I4s8XpMOBDmfA
4ccW/IzYNjxt91hataYaw7smpnNs8ym0DZBZuUguxKgit2QgiB/pl9jL8Q1sf6dg
3aslPyXNizHPRiZHShFAdOI3Y2INj9lXrfLEJd8uD2qk1kK4Pwo590Jk8Sry1qSJ
YHGJHn8dE+xxYB1ZCyiIqAbWTg0RsUD1AgMBAAGjgfUwgfIwHQYDVR0OBBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMEgbowgbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIGNMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNV
BAcTCFNhbiBKb3NlMRIwEAYDVQQKEwlNeUNvbXBhbnkxDjAMBgNVBAsTBU15T3Jn
MRgwFgYDVQQDFA8qLmFtYXpvbmF3cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY2lzY28uY29tggkApY2On/9qsGwwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAe/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iuR84mQzhoT
nx5CN109xu5ml5baCYZZsSnn6D7usC092bPA/kRCGxt29gkjpWA74tJHqIhVWgbM
mOrLiSHoelewv+wRl0oVRChlTfKtXO68TUk6vrqpw76hKfOHIa7b2h1IIMdq6VA/
+A5FQ0xqYfqKdVd2RaINpzI8mqZiszqw+7E6j1PL5k4tftWEaYpfGPlVesFEyJEL
gHBUiPt8TIbaMYI8qUQmB/emnLXeKQ5PRxdRnleA3h8jfq3D1CQRTLjmDL3tpFwg
qopM6et5ZKqShX4T87BsgZIoiquzXqsuHg==
-----END CERTIFICATE-----">
    </pkiTP>
```

```
    </cloudCertStore>
     </fvTenant>
</polUni>
```

REST API を使用した HTTPS サービス ポリシーの作成

このセクションでは、REST API を使用して HTTPS サービス ポリシーを作成する方法を示します。

（注） リスナーは複数の証明書をもつことができます。証明書のオプションは次のとおりです。

- ELBSecurityPolicy-2016-08 – セキュリティ ポリシーが選択されていない場合のデフォルト。
- ELBSecurityPolicy-FS-2018-06
- ELBSecurityPolicy-TLS-1-2-2017-01
- ELBSecurityPolicy-TLS-1-2-Ext-2018-06
- ELBSecurityPolicy-TLS-1-1-2017-01
- ELBSecurityPolicy-2015-05
- ELBSecurityPolicy-TLS-1-0-2015-04

複数の証明書を使用する場合は、デフォルトの証明書を指定する必要があります。デフォルトは、**cloudRsListenerToCert** の **defaultCert** プロパティを使用して指定されます。

始める前に

キー リング証明書は既に構成されています。

（注） これは、アプリケーション ゲートウェイにのみ適用されます。

HTTPS サービス ポリシーを作成するには:

```
<polUni>
  <fvTenant name="t2">
    <vnsAbsGraph name="CloudGraph" type="cloud" status="">
      <vnsAbsNode funcType="GoTo" name="N1" managed="yes">
        <cloudSvcPolicy tenantName="t2" contractName="httpFamily" subjectName="consubj">
          <cloudListener name="https_listener" port="443" protocol="https"
secPolicy="eLBSecurityPolicy-2016-08" status="">
            <cloudRsListenerToCert defaultCert="yes" certStore="default"
tDn="uni/tn-t2/certstore/keyring-lbCert" status=""/>
            <cloudListenerRule name="defaultRule" default="yes" priority="100" status="">
```

```
              <cloudRuleAction type="forward" port="80" protocol="http"
epgdn="uni/tn-t1/cloudapp-ap/cloudepg-ep1">
                                                  </cloudRuleAction>
            </cloudListenerRule>
          </cloudListener>
        </cloudSvcPolicy>
      </vnsAbsNode>
    </vnsAbsGraph>
  </fvTenant>
</polUni>
```

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。