



レイヤ4からレイヤ7サービスの展開

- [概要 \(1 ページ\)](#)
- [ユースケースの例 \(16 ページ\)](#)
- [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 \(34 ページ\)](#)
- [リダイレクトの注意事項と制約事項 \(59 ページ\)](#)
- [Cloud APIC GUI を使用したセカンダリ VRF への新しい CIDR の追加 \(61 ページ\)](#)
- [サービス グラフの展開 \(64 ページ\)](#)

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 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 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。
- サードパーティのファイアウォール
- サードパーティのロードバランサ

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。

サービスグラフとコントラクト（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。クラウドAPICは、コントラクト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とプロバイダー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クラウドAPIC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: プロバイダー 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ー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 クラスター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 とプロバイダークラウド 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 とプロバイダークラウド 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
- サービスグラフがコントラクト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。

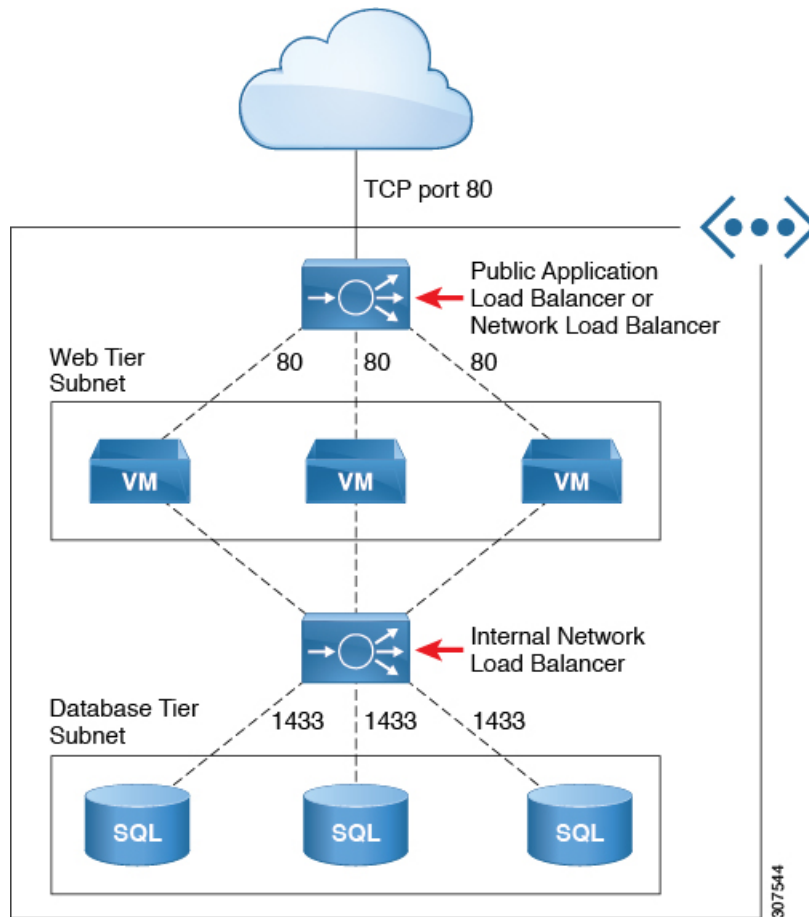
リスナーでは、ロードバランサがトラフィックを受け入れて転送するポートおよびプロトコル (TCP または UDP) を指定できます。すべてのリスナーで、少なくとも 1 つのルール (条件のないデフォルトのルール) を構成する必要があります。ルールを使用すると、条件が満たされたときにロードバランサが実行するアクションを指定できます。アプリケーションゲートウェイとは異なり、ここではルールはバックエンドプールの特定のポートにのみトラフィックを転送できます。NLB は ALB と同様に別のサブネットにある必要があります。ネットワーク ロードバランサには、次の 2 つの動作モードがあります。

- 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、標準規格 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 とプロバイダーのクラウド 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 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 ネットワーク ロードバランサ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。

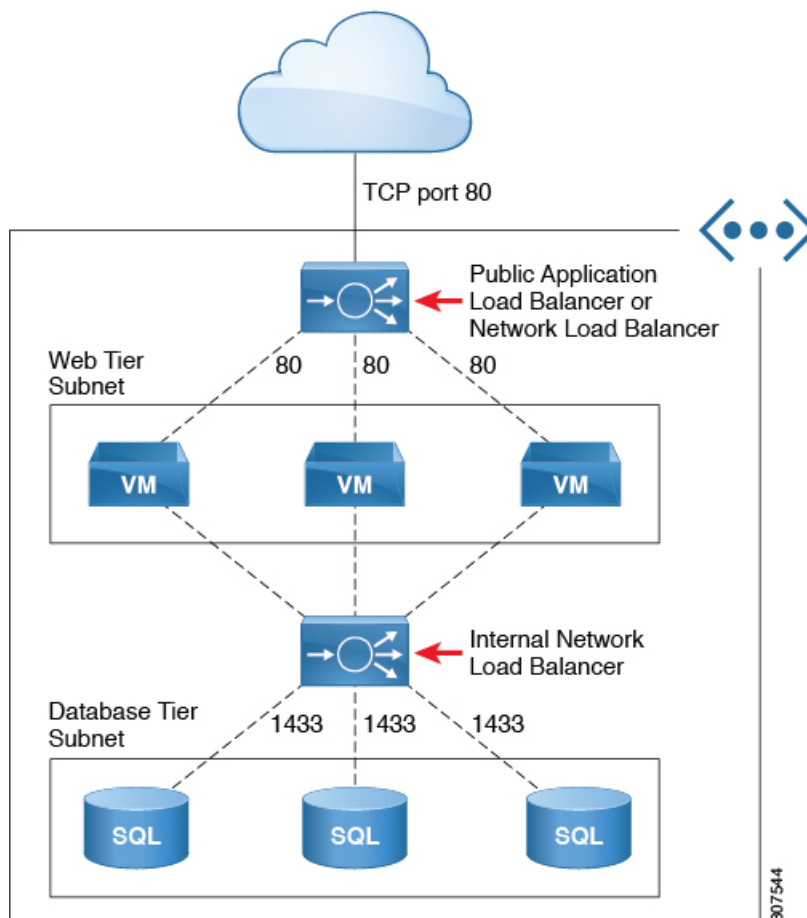
- [Azure ネットワーク ロードバランサの複数のフロントエンド IP アドレスについて \(6 ページ\)](#)
- [注意事項と制約事項 \(8 ページ\)](#)

Azure 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。

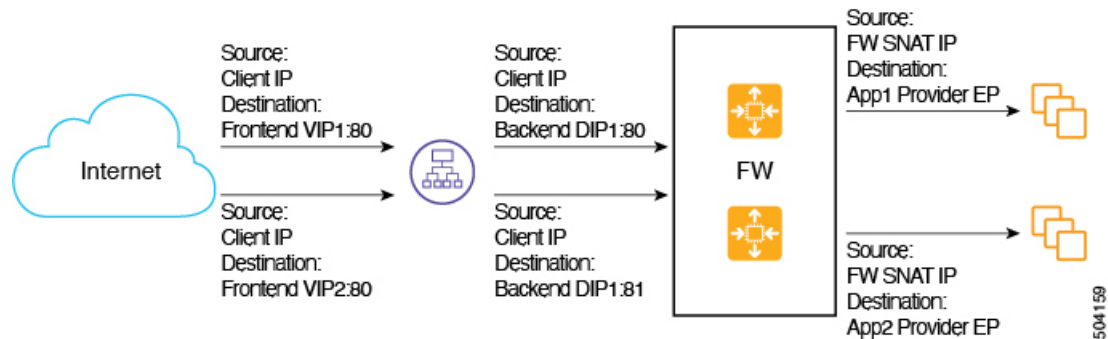


この例では、インターネット向けのネットワークロードバランサには、インターネットトラフィックのフロントエンドに割り当てられた単一のパブリック IP アドレスがありません。

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	<ul style="list-style-type: none"> • IP: VIP1 • Port: 80 	Port: 80
Rule2	<ul style="list-style-type: none"> • 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（外部インターフェイスと内部インターフェイス）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 (Limitations for Third-Party Load Balancers)] :

- 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のオプションについて

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 ネットワーク ロードバランサで使用できます。





- (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 ネットワーク ロードバランサ \(11 ページ\)](#)


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. [**Intent**]メニューの[**Application Management**]リストから、[**Services**]>>[**Devices**]>>[**Create Device**]をクリックします。
 2. [**Service Type**]として[**Third party firewall**]を選択します。
 3. [**Add Interface**]をクリックし、[**Allow All Traffic**]エリアを見つけます。
 4. [**Allow All Traffic**]エリアの[**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このオプションを有効にするには :
1. [**Intent**]メニューの[**Application Management**]リストから、[**Services**]をクリックし、[**Device Type**]として[**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. [**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 [**Interfaces**] エリアを見つけ、[**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. [**Details**] アイコンをクリックします () 。
このインターフェー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、このインターフェースの構成設定を編集します。
 6. [**Allow All Traffic**] エリアを見つけ、[**Allow All Traffic**] エリアの [**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 ネットワーク ロードバランサ

- 新しいサービス グラフ タイプを作成するとき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[ネットワーク ロードバランサ (Network Load Balancer)]を選択します。
 3. [設定 (Settings)]エリアで、[すべてのトラフィックを許可 (Allow All Traffic)]エリアの[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[ネットワーク ロードバランサ (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)]エリアで、[すべてのトラフィックを許可 (Allow All Traffic)]エリアを見つけ、[すべてのトラフィックを許可 (Allow All Traffic)]エリアの[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

プロバイダー EPG 内のサーバー、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ー 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 とプロバイダー 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

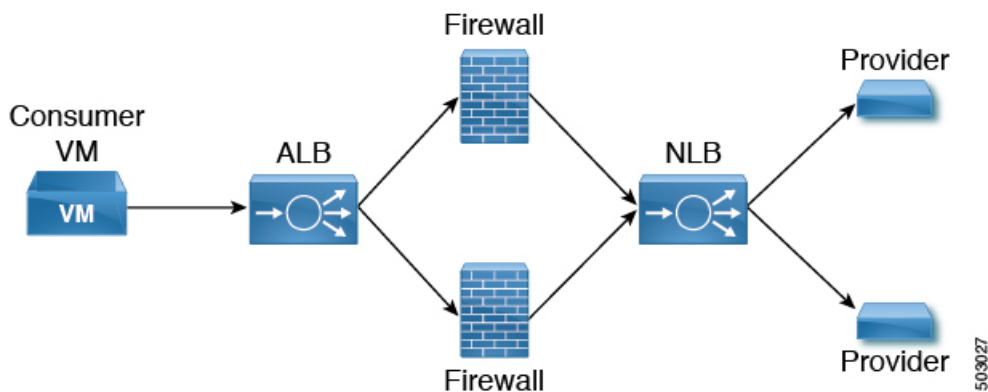
リリース 5.0(2) 以降、VNet 間サービスの展開と自動化がサポートされています。これは、クラウド内の East-West と North-South の両方のユースケースに当てはまります。

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 ピアリングの構成](#)」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。プロバイダーの前にある ALB などのサービス デバイスは、プロバイダー 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、プロバイダー VNet 内にあるか、ハブ VNet とプロバイダー 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 のプロバイダー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ー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構成されます。



- (注) このセクション全体で、「コンシューマからプロバイダーへ」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ー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、プロバイダー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ー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ー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ー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ー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 からプロバイダー IP へのトラフィックを許可することです。接続先 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、接続先 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、接続先 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、接続先 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接続先に向かう他の 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	プロバイダー VNet でのリダイレクト
タグベース	タグベース	プロバイダーのリダイレクトは、プロバイダーの 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	プロバイダーのリダイレクトはプロバイダーのサブネットです	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	プロバイダー VNet でのリダイレクト
サブネットベース	タグベース	プロバイダーのリダイレクトは、プロバイダーの 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	プロバイダーのリダイレクトはプロバイダーのサブネットです	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送信元 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。
snat_dnat	この値は、サービスノードがトラフィックに対して送信元 NAT と接続先 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)]** エリア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 **[プロバイダーコネクタタイプ (Provider Connector Type)]** エリアの下にある **[リダイレクト (Redirect)]** オプションの横にあるチェック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ーのEPG間のコントラクトを作成するEPG通信を構成します。
4. サービス グラフをコントラクトに添付します。
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。

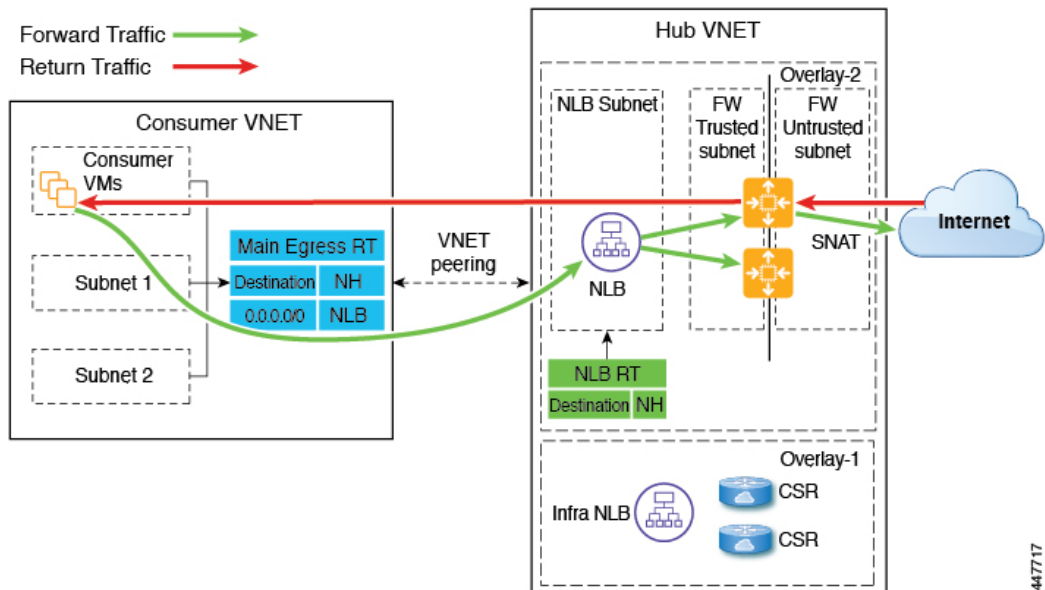
- [スポークツーインターネット \(17 ページ\)](#)
- [スポークツースポーク \(19 ページ\)](#)
- [リージョン間スポーク ツー スポーク \(22 ページ\)](#)
- [インターネット ツー スポーク \(VRF 間\) \(25 ページ\)](#)
- [サードパーティ ロードバランサの高可用性サポート \(28 ページ\)](#)

- 2つの個別の VNet 内のコンシューマとプロバイダーの EPG (30 ページ)
- 2つの個別の VNet でのコンシューマおよびプロバイダー EPG を使用した VNet のハブ (32 ページ)

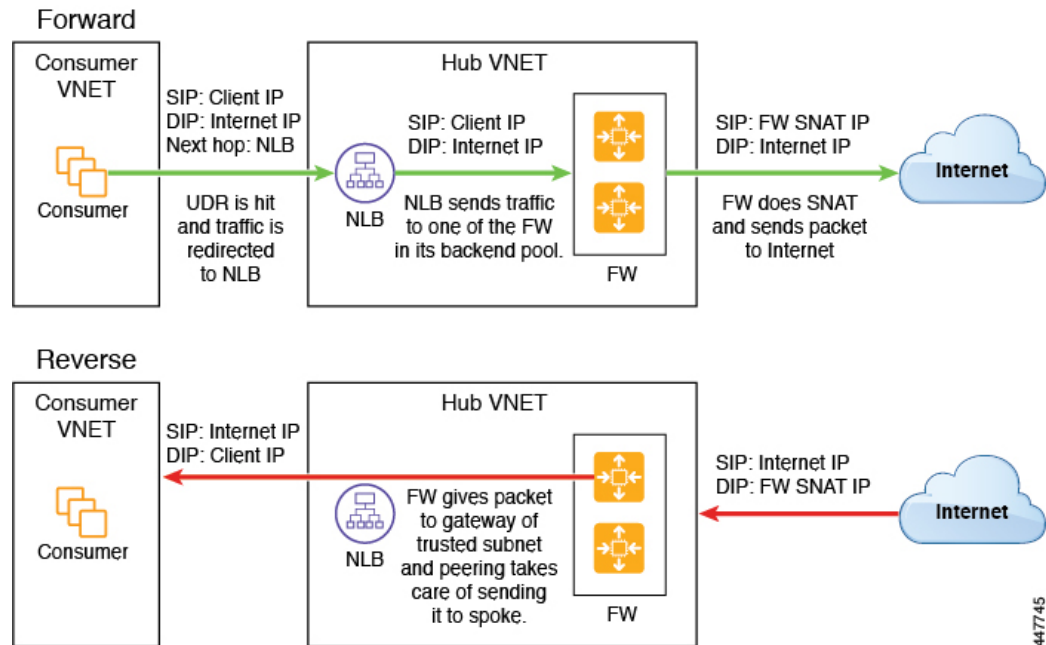
スポークツーインターネット

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、スケールリングのために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、ソース ネットワーク アドレス変換 (SNAT) も実行します。

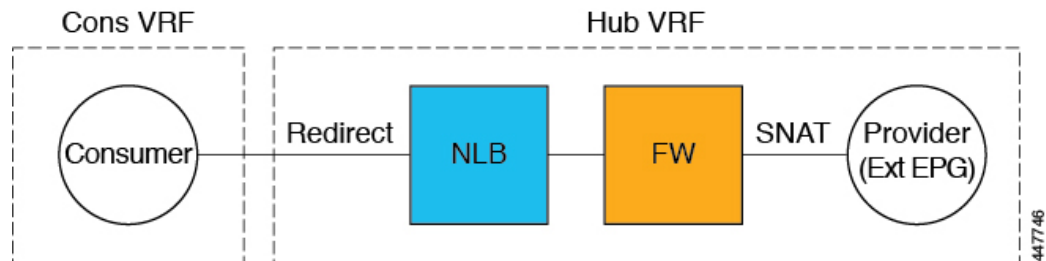
このユースケースで使用されるすべてのレイヤ4からレイヤ7サービス デバイスに専用サブネットがあることを確認します。



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。

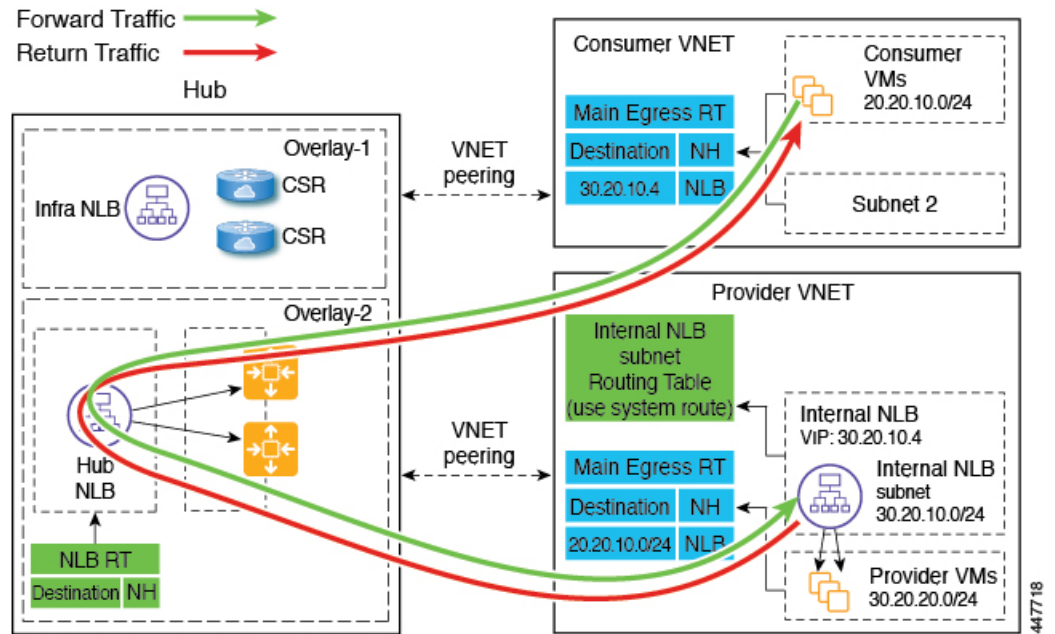
- [デバイス の作成 (Create Device)] ウィンドウで
 - [テナント (Tenant)] フィールドで、[インフラ (infra)] テナントを選択します。
 - [サービス タイプ (Service Type)] フィールドでサービス デバイスのタイプを選択します。
 - [サービス タイプ (Service Type)] として [ネットワーク ロードバランサ (Network Load Balancer)] を選択し、[サブネット (Subnets)] エリアで [サブネットの追加 (Add Subnet)] をクリックしてから、適切なリージョン、クラウドコンテキスト 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。

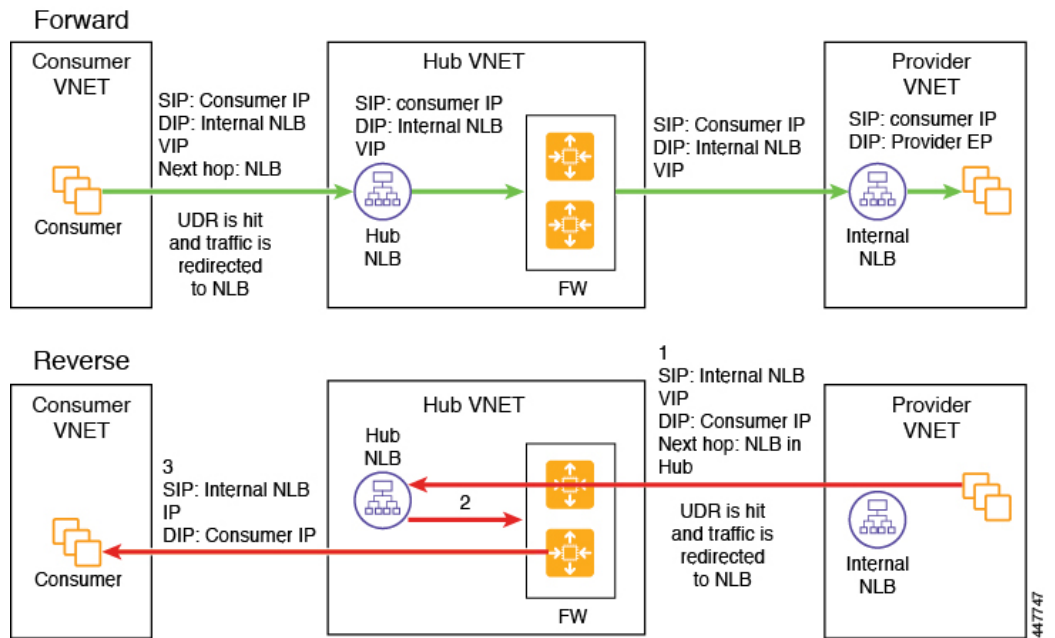
スポークツースポーク

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、プロバイダー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ーのVNetで出カ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。

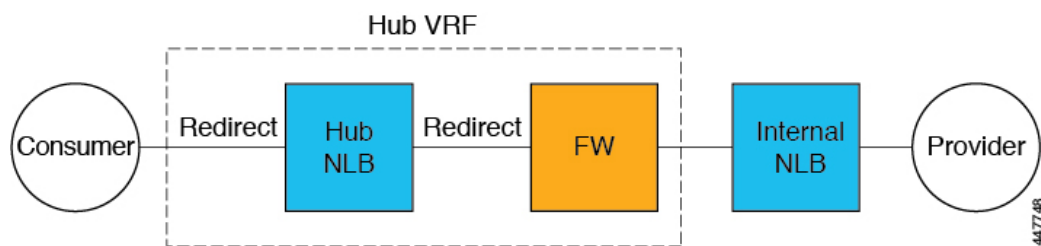
このユースケースで使用されるすべてのレイヤ4からレイヤ7サービスデバイスに専用サブネットがあることを確認します。



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。

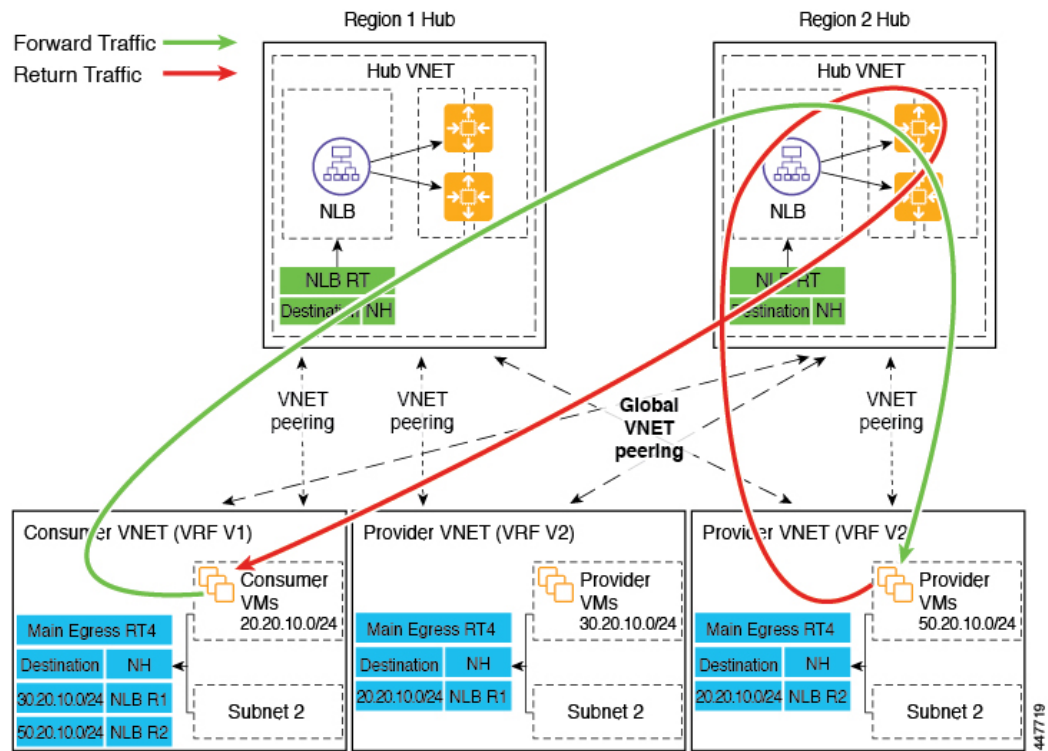


(注) SNAT がサードパーティのロードバランサで構成されていることを確認します。

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、プロバイダー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ー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、プロバイダー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。



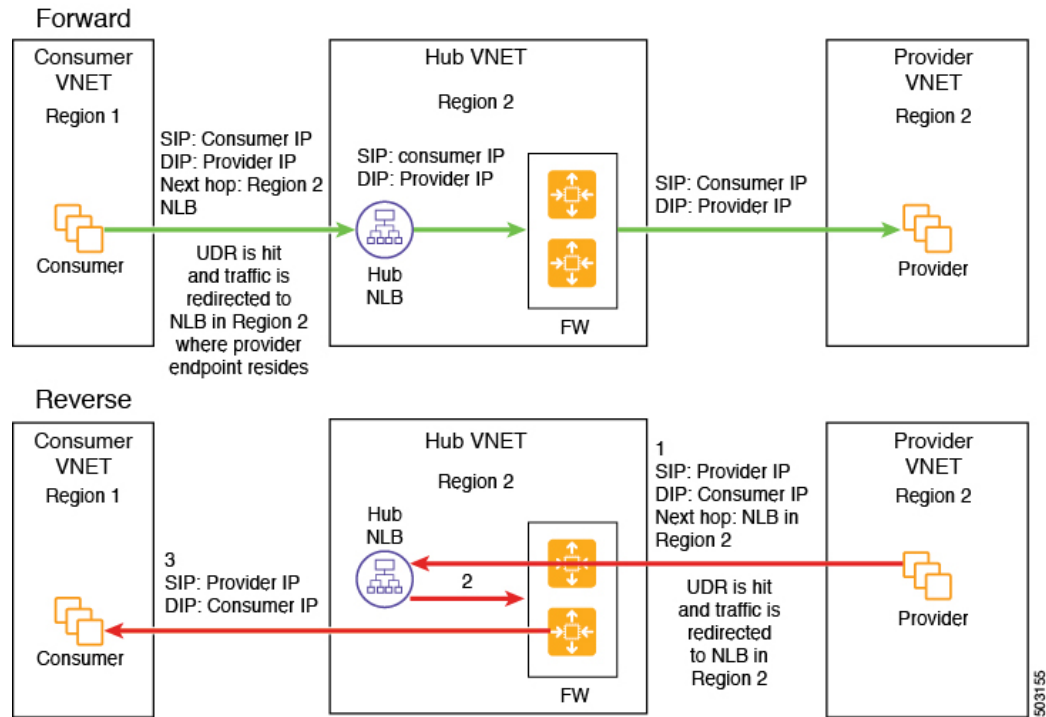
たとえば、コンシューマ VNet (VRF 1) の出カルートテーブル (RT) の2つのサブネットについて考えてみます。

- 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)

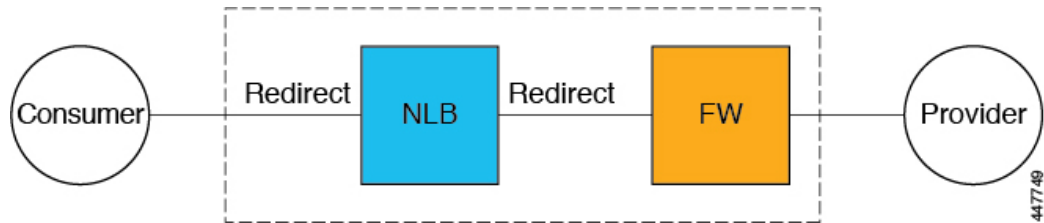
コンシューマが、ローカルにあるプロバイダー VM 30.20.10.0/24 にトラフィックを送信するとします。その場合、トラフィックはリージョン 1 のハブ NLB とファイアウォールにリダイレクトされ、プロバイダーに移動します。

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ー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 packets 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、プロバイダー 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)

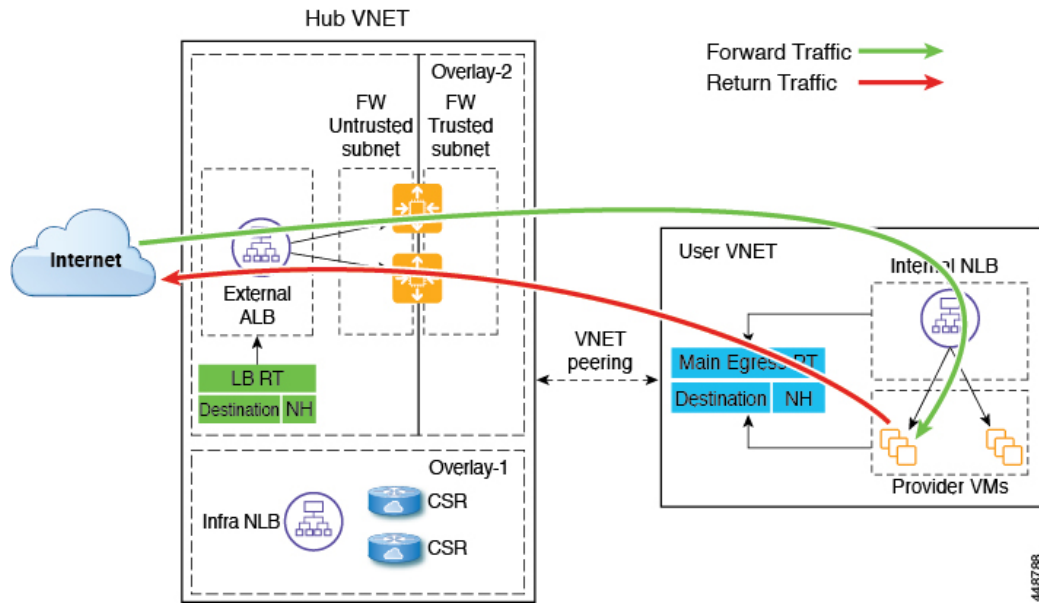
このユース ケースでは、インターネットからのトラフィックは、プロバイダーエンドポイントに到達する前にファイアウォールを通過する必要があります。このユースケースではリダイレクトは使用されません。



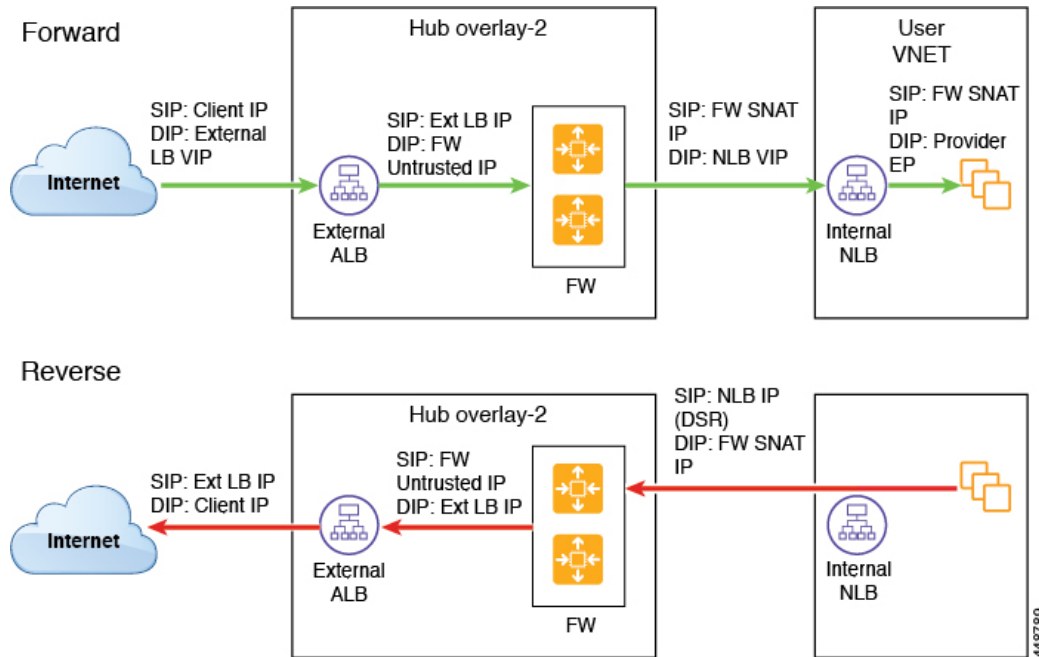
- (注) このセクションでは、一般的な用語「外部ロードバランサ」が使用されています。これは、このユースケースで外部ロードバランサがNLB、ALB、またはサードパーティロードバランサのいずれかになる可能性があるためです。次の例は、ALBを使用した構成を示していますが、外部ロードバランサは代わりにNLBまたはサードパーティロードバランサである可能性があることに注意してください。

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はプロバイダーエンドポイントの1つにトラフィックを送信します。

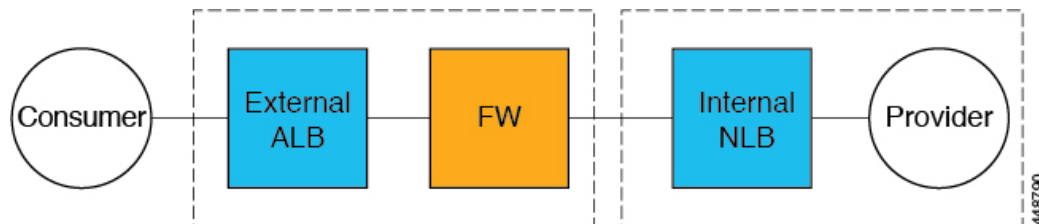
このユースケースで使用されるすべてのレイヤ4からレイヤ7サービス デバイスに専用サブネットがあることを確認します。



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)]** 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 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 (プロバイダー 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。

- 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。



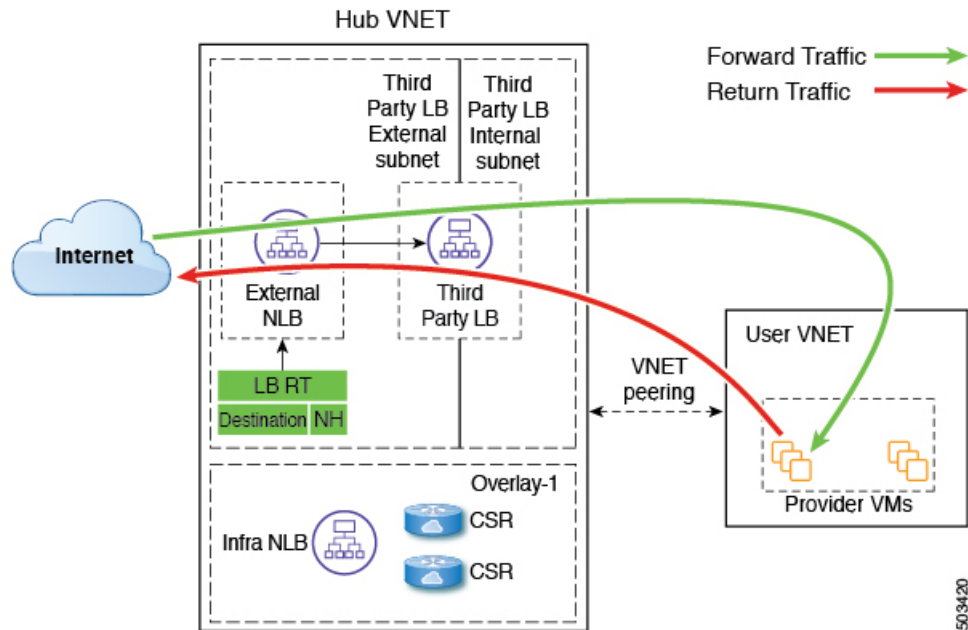
(注) SNAT がサードパーティのロードバランサで構成されていることを確認します。

サードパーティロードバランサの高可用性サポート

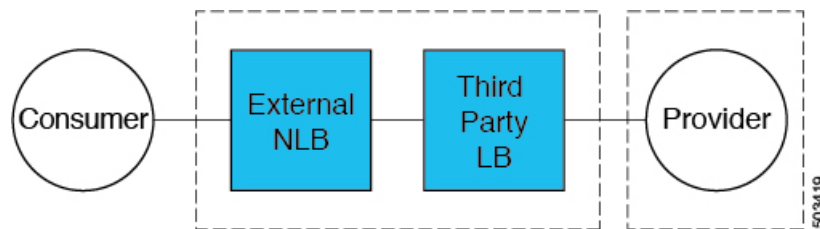
このユースケースでは、インターネットからのトラフィックは、プロバイダーエンドポイントに到達する前にサードパーティロードバランサを通過する必要があります。このユースケースではリダイレクトは使用されません。

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。



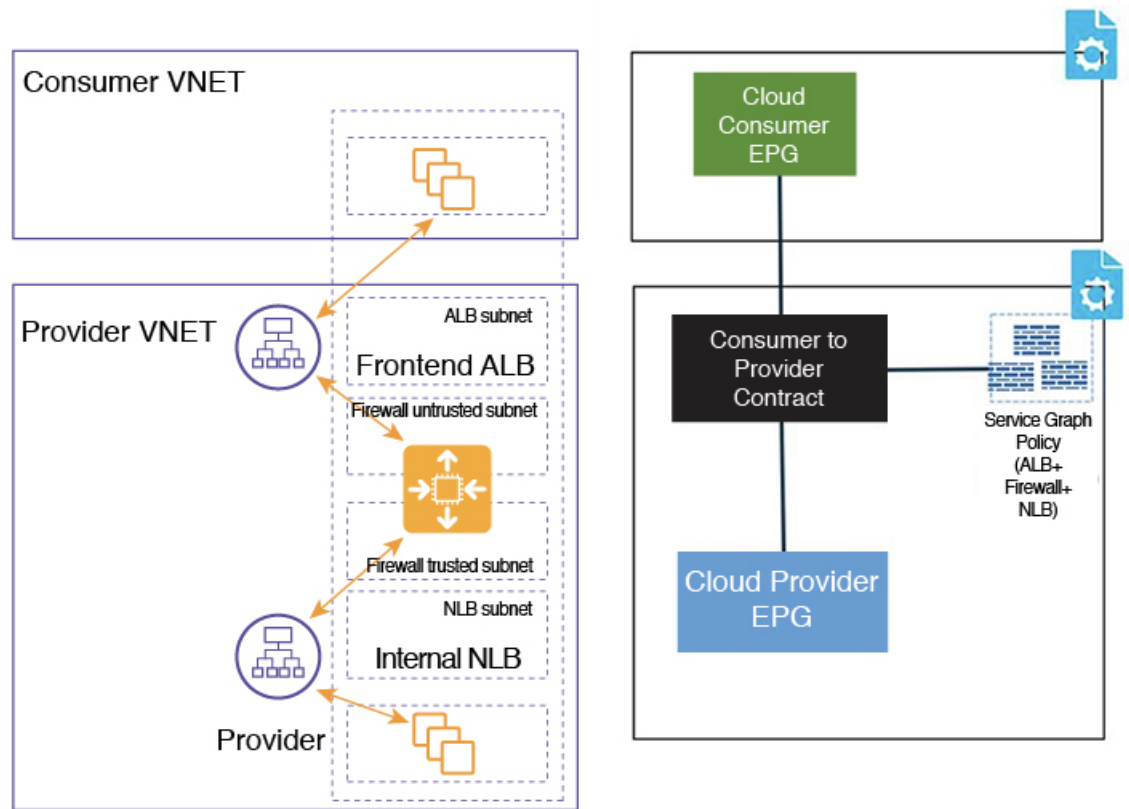
(注) SNAT がサードパーティのロードバランサで構成されていることを確認します。

2つの個別の VNet 内のコンシューマとプロバイダーの 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 とプロバイダー 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ーの 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ー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。

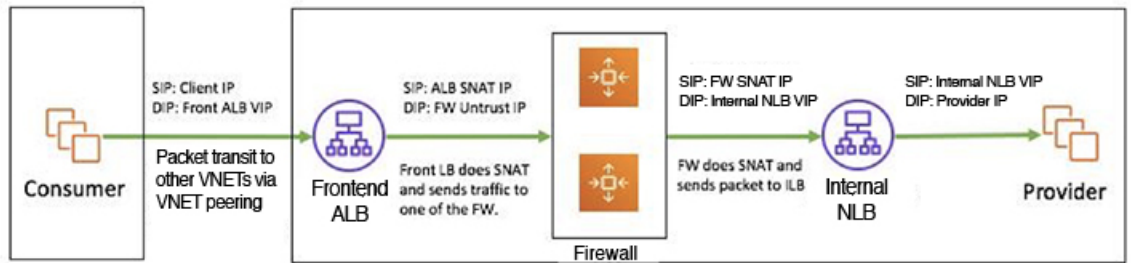


この図では次のようになっています。

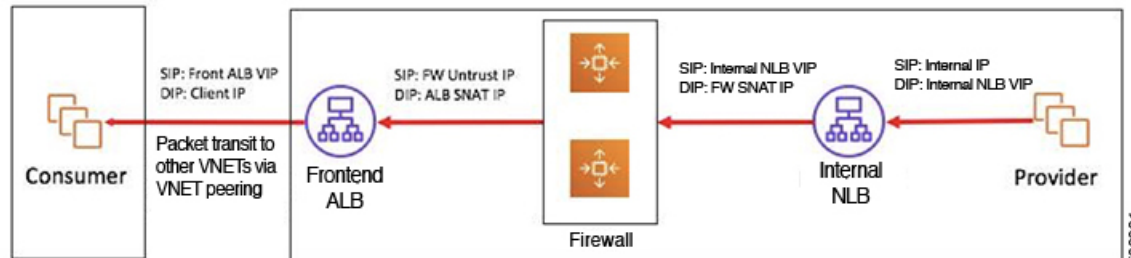
- コンシューマ EPG はコンシューマ VNet にあります。
- プロバイダー EPG とすべてのサービス デバイスはプロバイダー VNet にあります。
- アプリケーションロードバランサ、ネットワークロードバランサ（またはサードパーティのロードバランサ）、およびファイアウォールは、VNet 内に独自のサブネットを持つ必要があります。

両方向のパケットフローを次の図に示します。

Forward



Reverse



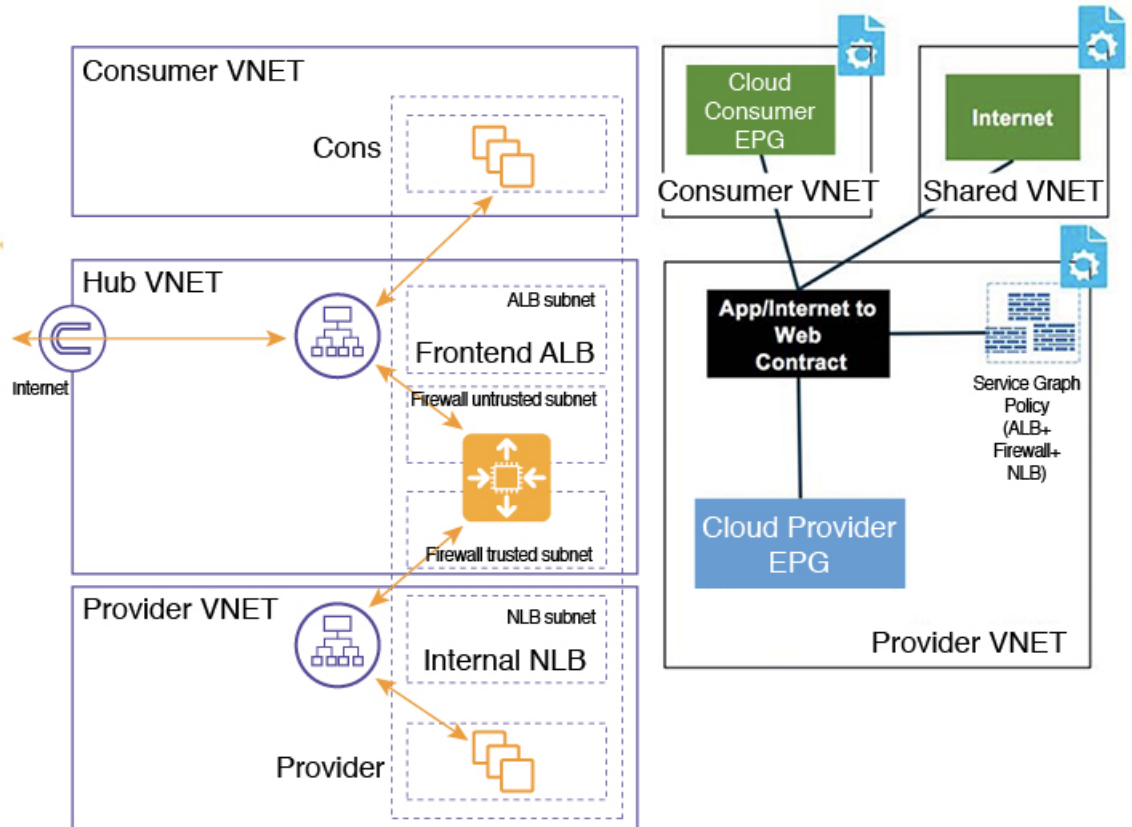
503031

2つの個別のVNetでのコンシューマおよびプロバイダー 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 とプロバイダー 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ーの EPG の間にあるハブ VNet 内に挿入されます。
- 内部 NLB はプロバイダー 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ーエンドポイントへのトラフィックを負荷分散します。

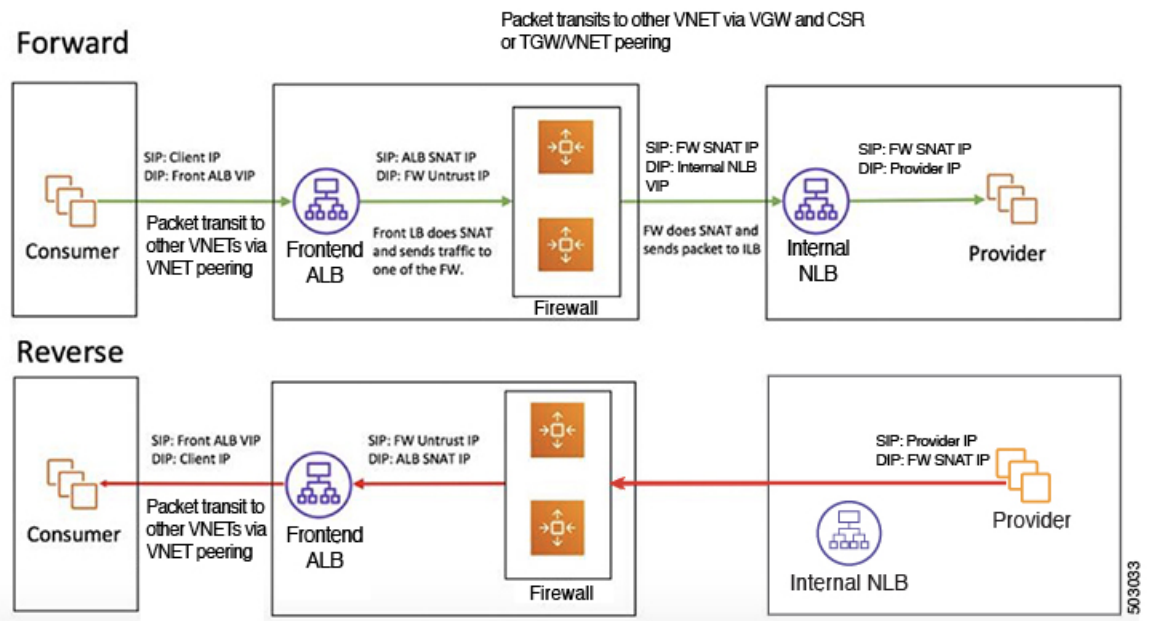
このユースケースでは、フロントエンド ALB または内部 NLB の代わりにサードパーティのロードバランサを使用できます。このユースケースで使用されるすべてのレイヤ4からレイヤ7サービス デバイスに専用サブネットがあることを確認します。



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。
- プロバイダー EPG と内部 NLB はプロバイダー 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ユースケースの例です。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](#)」と「[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：プロバイダー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：プロバイダー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：プロバイダー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）

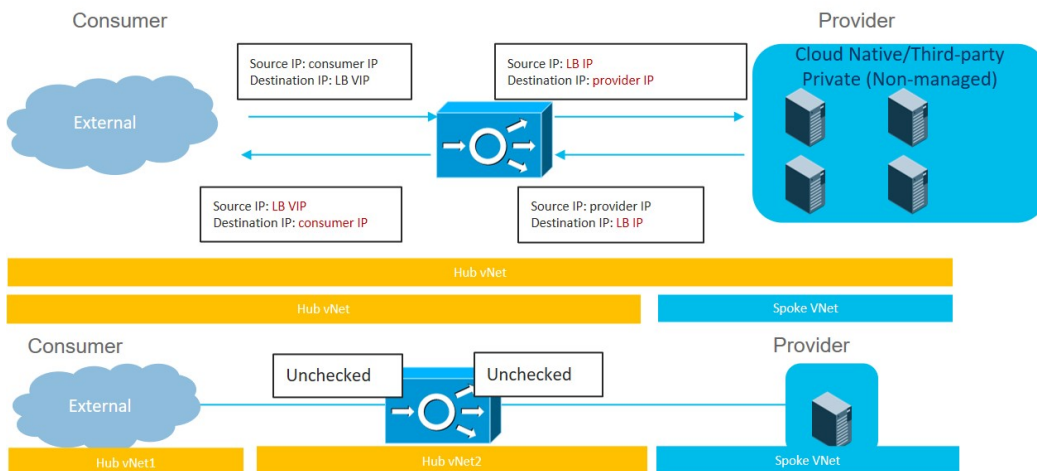


(注) 次の各ユースケースでは、プロバイダーとしてサービス EPG を使用する、単一ノード、2ノード、および3ノードのサービスグラフを使用する同様のトポロジを、クラウドの東西トラフィックに対してサポートできます。これらのユースケースでは、コンシューマはクラウド EPG になり、使用されるロードバランサは内部ロードバランサになります。

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：プロバイダー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 はプロバイダーであり、外部 EPG はコンシューマー側で構成されます。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. コンシューマー側で外部 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、Cloud Native 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 またはThird-Party
- **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（65 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）]** 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 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。

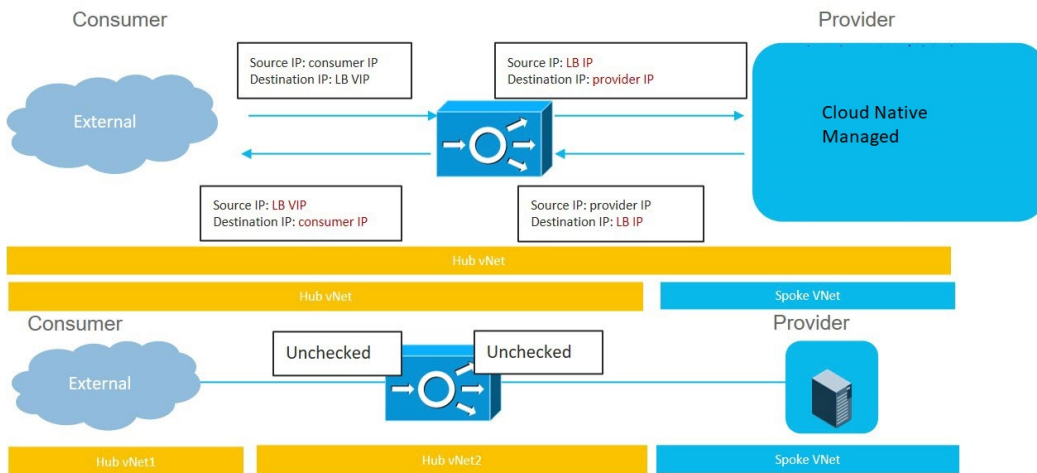
4. レイヤ4～レイヤ7サービスを展開します。

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：プロバイダー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 はプロバイダーであり、外部 EPG はコンシューマー側で構成されます。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. コンシューマー側で外部 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**：Public and 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](#)（65 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)] 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 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。

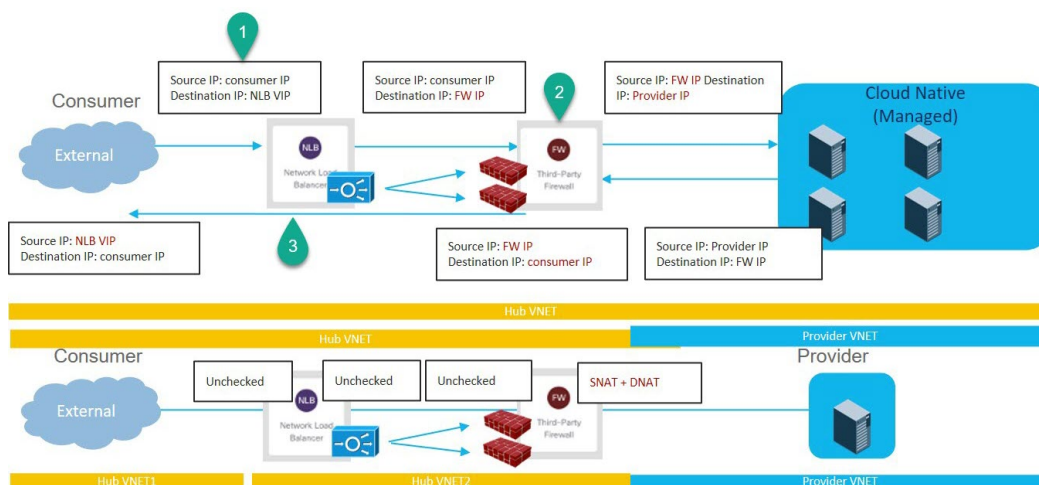
インターネットインバウンドトラフィックの2ノードサービスグラフ：プロバイダーとしてのクラウドネイティブ管理対象サービス EPG

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 はプロバイダーであり、外部 EPG はコンシューマー側で構成されます。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. コンシューマー側で外部 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 \(65 ページ\)](#) 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。

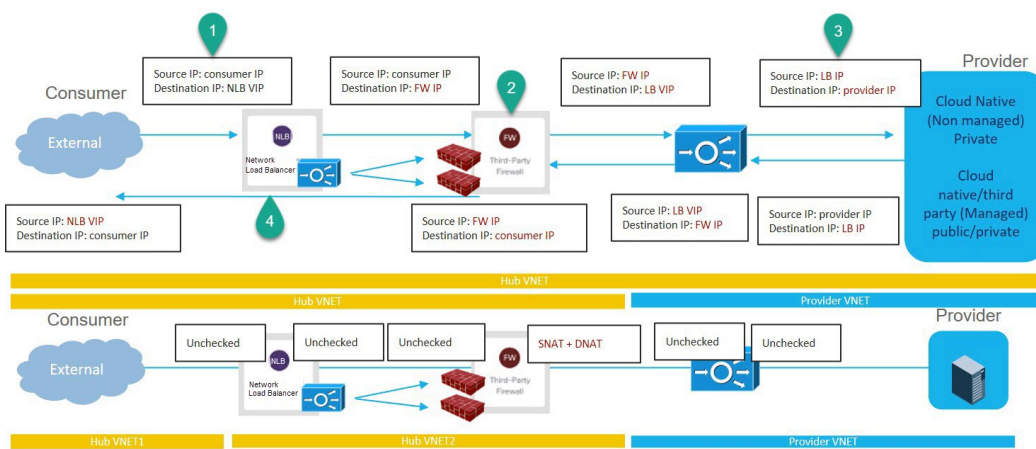
- 最初のサービス デバイス: ハブ VNet のネットワーク ロードバランサ
- 2番目のサービス デバイス: ハブ VNet のファイアウォール
- サードサービス デバイス: ハブ VNet またはスポーク VNet 内のサードパーティのロードバランサ

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 はプロバイダーであり、外部 EPG はコンシューマー側で構成されます。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. コンシューマー側で外部 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 \(65 ページ\)](#) 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)]** 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。
 - 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 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)]** 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 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)
 - サードパーティのロードバランサ (ハブまたはプロバイダー 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](#)」と「[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。

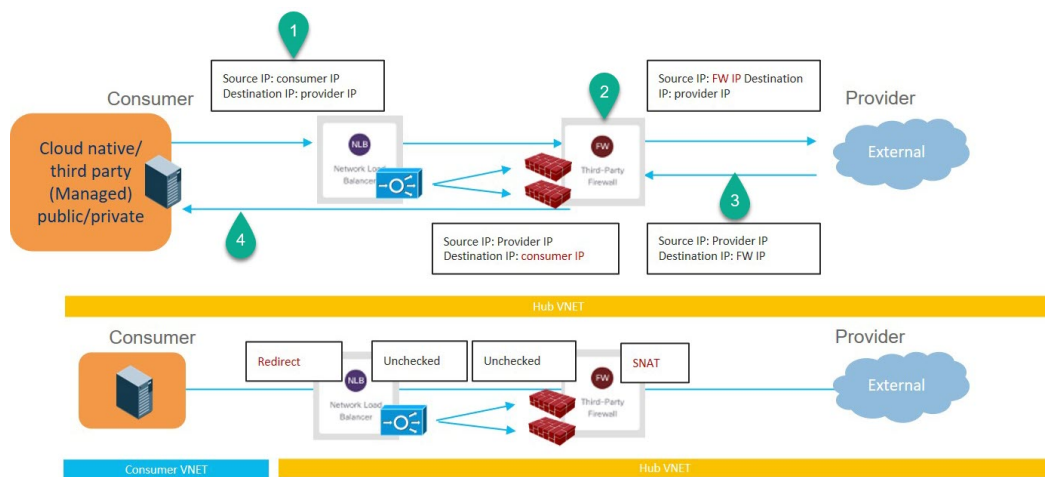
このユースケースでは、サービス EPG はコンシューマであり、外部 EPG はプロバイダー側で構成されます。



- (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、リターン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. プロバイダー側で外部 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。
 - `0.0.0.0/0` サブネット で外部 EPG を構成しないでください。
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、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 \(65 ページ\)](#) 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、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。

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。

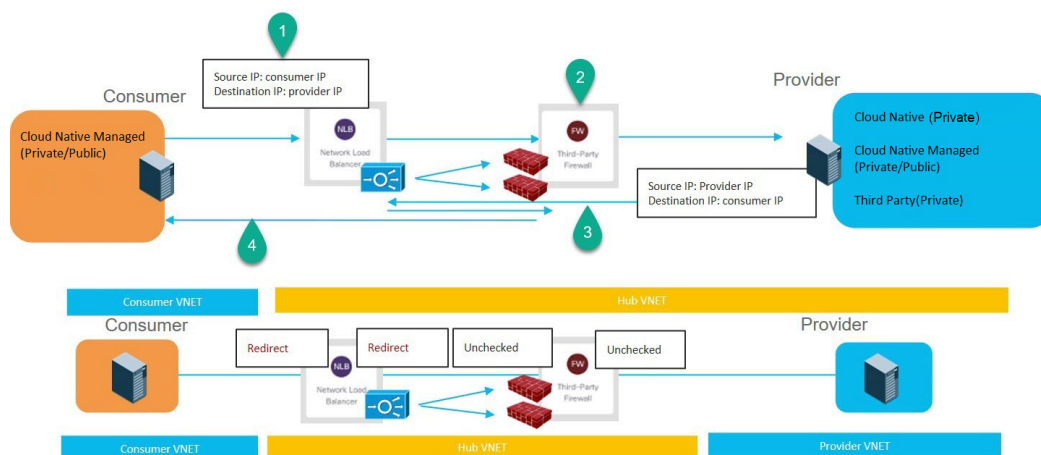
East-West の 2 ノード サービス グラフ

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ー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ーはクラウド 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ーのサービス 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、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
- プロバイダーとしてのサービス 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、Cloud Native 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
 - **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 \(65 ページ\)](#) 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)]** 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。

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。

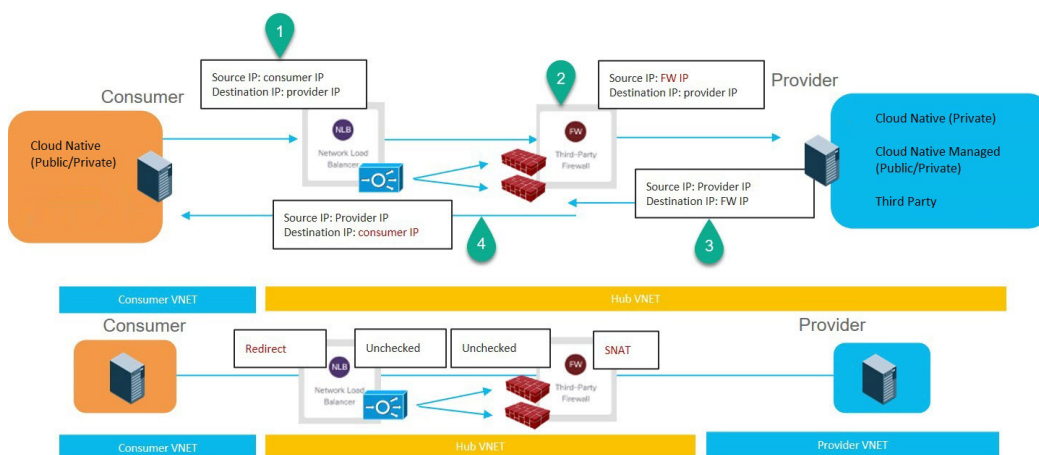
SNAT オプションを使用した East-West の 2 ノード サービス グラフ

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ーはクラウド 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、リターン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ーのサービス 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、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

- プロバイダーとしてのサービス 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、Cloud Native 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
 - **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（65 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、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。

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。

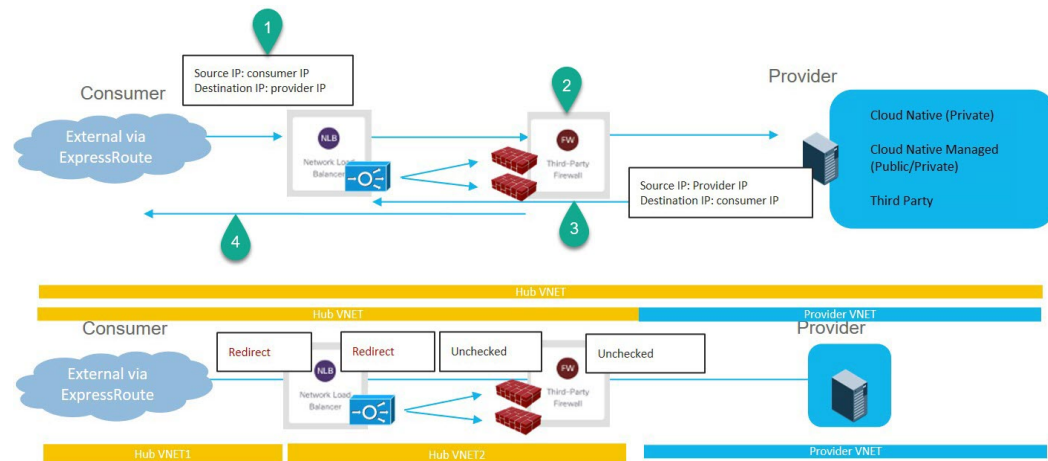
エクスプレスルート ゲートウェイ経由の受信トラフィックの2ノード サービス グラフ

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ー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 がプロバイダーであり、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 Active Directory Domain 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

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](#)を使用したエクスプレス ルート ゲートウェイの展開 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（65 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、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。
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。

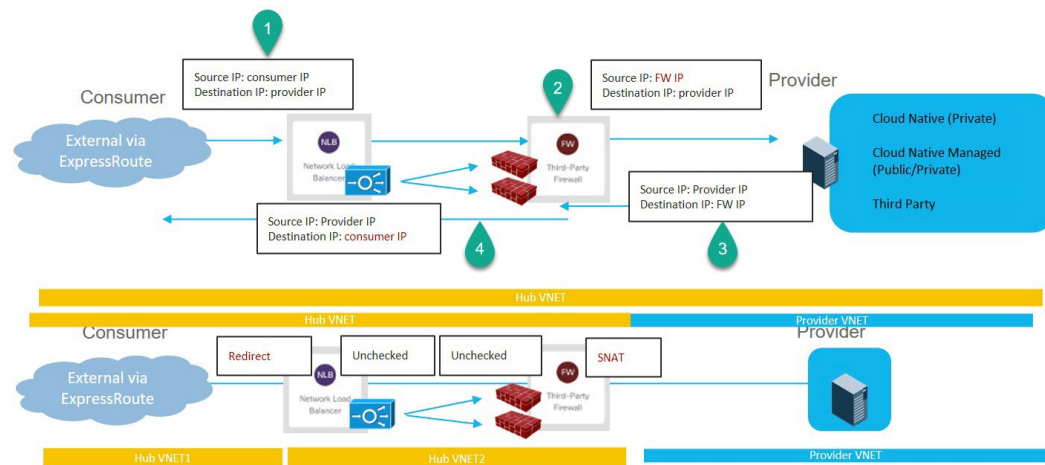
SNATオプションを使用したエクスプレスルートゲートウェイ経由のインバウンドトラフィックの2ノードサービスグラフ

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 はプロバイダーであり、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、リターン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、Redis Cache 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

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たエクスプレス ルート ゲートウェイの展開](#)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 \(65 ページ\)](#)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、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。

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。

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。

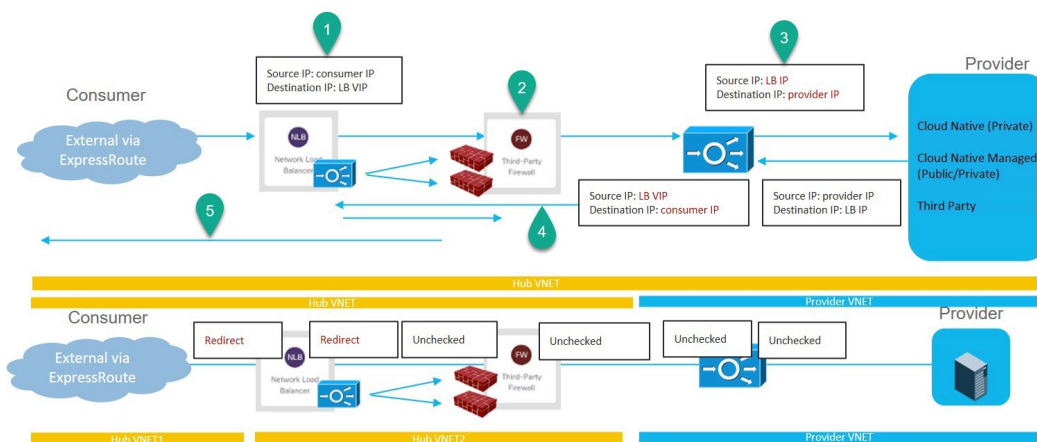
- 最初のサービス デバイス: ハブ VNet のネットワーク ロードバランサ
- 2番目のサービス デバイス: ハブ VNet のファイアウォール
- 3番目のサービス デバイス: ハブまたはスポーク VNet のアプリケーション ロードバランサ

このユースケースでは、コンシューマ側とプロバイダー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 はプロバイダーです。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3番目のサービス デバイスであるアプリケーション ロードバランサに移動します。
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

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たエクスプレス ルート ゲートウェイの展開](#)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（65 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)] 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 [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)] 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 (プロバイダー 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。

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 とプロバイダー 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 がプロバイダー EPG である場合、コンシューマ EPG とプロバイダー 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 とプロバイダー 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 とプロバイダー 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にプロバイダー 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 とプロバイダー 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ーの 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ー EPG のリージョンに展開する必要があります。プロバイダー 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。
- プロバイダーとしての外部 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 とプロバイダー 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、プロバイダー EPG3 がプロバイダー VNet にある場合、EPG1 と EPG3 間のコントラクト、および EPG2 と EPG3 間のコントラクト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ーがユーザ定義ルートの特
定の接続先に対して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。

サービスチェーン オプション	スポークツースポーク		スポークツ-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	サポート対 象外	サポート対 象外	サポート対 象	サポート対 象
FW (SNAT なし) ²	サポート対 象外	サポート対 象	サポート対 象外	サポート対 象外	サポート対 象外	サポート対 象外

サービスチェーンオプション	スポークツースポーク		スポークツ―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) 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	サポート対象外	サポート対象外
<ul style="list-style-type: none"> • NLB²-FW(no SNAT)¹ • NLB²-FW(no SNAT)¹-NLB/ALB¹ • NLB²-FW(no SNAT)¹-LB(SNAT)¹ 	サポート対象外	サポート対象	サポート対象外	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	サポート対象外	サポート対象	サポート対象	サポート対象	サポート対象外	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	サポート対象外	サポート対象外	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	サポート対象外	サポート対象外	サポート対象	サポート対象

¹ Unchecked on both consumer and provider connector or options are not applicable for ALB.

² Redirect is enabled on both consumer and provider connector.

³ 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 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。プロバイダー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。プロバイダー コネクタで SNAT が有効になっています。

⁶ Unchecked on consumer connector. プロバイダー 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 \(63 ページ\)](#) 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)] エリアに [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 (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** [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)] エリアに [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)] フィールドに入力します。
- 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)] エリア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) [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)] エリアに [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、予期される正しい動作です。

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. フィルタとのコントラクト

GUI を使用したサービス 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 Dialog 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 \(65 ページ\)](#) 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 \(67 ページ\)](#) 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	

[プロパティ (Properties)]	説明
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。 <ol style="list-style-type: none"> 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 タイプ	デバイス タイプを選択します。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 標準 • Standard V2
[VM インスタンス数 (VM Instance Count)]	[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 (VM Instance Size)]	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。

[プロパティ (Properties)]	説明
スキーム	<p>[インターネット向け] または [内部] を選択します。</p> <ul style="list-style-type: none"> • [インターネット向け (Internet Facing)]: 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 (Internal)]: 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。 <ul style="list-style-type: none"> • [ダイナミック (Dynamic)]: Azure によってダイナミック IP アドレスが割り当てられます。ダイナミック 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。 <p>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。</p>
サブネット	<p>サブネットを選択するには:</p> <ol style="list-style-type: none"> 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「チェック」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	

[プロパティ (Properties)]	説明
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。 <ul style="list-style-type: none"> ネットワーク ロード バランサ
[すべてのトラフィックを許可 (Allow All Traffic)]	<p>[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。</p> <p>[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のオプションについて (9 ページ)」を参照してください。</p> <p>(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。</p> <ul style="list-style-type: none"> 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)] エリアで、[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)] エリアで、[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。

[プロパティ (Properties)]	説明
スキーム	<p>[インターネット向け] または [内部] を選択します。</p> <ul style="list-style-type: none"> • [インターネット向け (Internet Facing)]: 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 (Internet Facing)] 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 (Internet Facing)] 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 (Internal)]: 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。 • [ダイナミック (Dynamic)]: Azure によってダイナミック IP アドレスが割り当てられます。ダイナミック IP アドレスは、VM が起動するたびに変更されます。 • [静的 (Static)]: 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。 <p>(注) Cloud APIC は、標準の SKU NLB のみを作成します。</p>
[カスタムリソースグループ (Custom Resource Group)]	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。

[プロパティ (Properties)]	説明
Subnets	<p>サブネットを選択するには:</p> <ol style="list-style-type: none"> 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、左側の列のリージョン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	<p>下矢印をクリックして、[詳細設定 (Advanced Settings)] エリアを展開します。次のエントリが表示されます。</p>

[プロパティ (Properties)]	説明
[フロントエンドIP 名 (Frontend IP Names)]	

[プロパティ (Properties)]	説明
	<p>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。</p> <ul style="list-style-type: none"> 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 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 アドレスの構成について (6 ページ) を参照してください。 <p>このエリアにフロントエンド 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のが Azure に通知されます。このエリア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。</p> <p>このエリアのパブリック 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。</p> <ol style="list-style-type: none"> [+ 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。 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。 [+ 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。 <p>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。</p> <ul style="list-style-type: none"> 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
	<p>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：</p> <ol style="list-style-type: none"> 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。 <p>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。</p>

- 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	<p>テナントを選択します。</p> <ol style="list-style-type: none"> 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	<p>デバイス タイプを選択します。</p> <ul style="list-style-type: none"> • サードパーティ ロード バランサ
[作成モード (Creation Mode)]	<p>[セレクタ (Selectors)]を選択します。</p> <p>[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。</p>

[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 (Interface)]	<p>[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。</p> <ol style="list-style-type: none"> [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。 [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。 [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。 [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。 <ul style="list-style-type: none"> [キー (Key)]: 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 (Operator)]: これは、equal、notequals、in、notin、keyあり、またはkeyなしのいずれかです。 [値 (Value)]: 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。 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。 [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。 <p>[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。</p> <p>(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。</p>

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。 <ul style="list-style-type: none">• サードパーティ ファイアウォール <p>(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。</p>
VRF	VRF を選択するには、次の手順を実行します。 <ol style="list-style-type: none">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	<p>[インターフェイスの追加 (Add Interface)] をクリックします。</p> <p>[設定] ページが表示されます。</p> <ol style="list-style-type: none"> [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。 [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。 <ul style="list-style-type: none"> [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のオプションについて (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。 <ul style="list-style-type: none"> 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)] エリアで、[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)] エリアで、[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。 [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。 インターフェイス セレクタの名前を入力します。 [一致式 (Match Expressions)] をクリックして選択します。 <ul style="list-style-type: none"> [キー (Key)]: 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 (Operator)]: 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 (Value)]: 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。 [追加 (Add)] をクリックします。 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。[さあ、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	<p>テナントを選択します。</p> <ol style="list-style-type: none"> [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。 左側の列から、クリックしてテナントを選択します。 [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	<p>デバイスを選択します。</p> <ol style="list-style-type: none"> [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。 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。 [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	<p>テナントを選択します。</p> <ol style="list-style-type: none"> [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。 左側の列から、クリックしてテナントを選択します。 [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 (Application Load Balancer)]	<ol style="list-style-type: none"> 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。
[サードパーティの ファイアウォール (Third Party Firewall)]	<ol style="list-style-type: none"> 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ー側でユーザ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)] オプションの隣のボックスにチェックを入れます。 5. [プロバイダー 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 (Add)] 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 (Network Load Balancer)]	<ol style="list-style-type: none"> 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ー側でユーザ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)] オプションの隣のボックスにチェックを入れます。 5. [追加 (Add)] をクリックします。
[サードパーティロードバランサ (Third Party Load Balancer)]	<ol style="list-style-type: none"> 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イスを選択します。 4. [プロバイダー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 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) [**プロバイダー 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ー 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) [**EPG 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 Listener)] 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 Listener)] 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 (Add Cloud Load Balancer Listener)] 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	アプリケーション ゲートウェイの場合は、[HTTP] または [HTTPS] をクリックして選択します。
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 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): <ol style="list-style-type: none"> [SSL 証明書の追加] をクリックします。 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。 キーリングを選択してください: <ol style="list-style-type: none"> [キーリングの選択] をクリックします。[キーリングの選択 (Select Key Ring)] ダイアログが表示されます。 [キーリングの選択 (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。[キーリングの選択 (Select Key Ring)] ダイアログボックスが閉じます。 [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。 <p>(注) リスナーは複数の証明書を持つことができます。</p>
ルールの追加 (Add Rule)	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
	<p>[ルール設定 (Rule Settings)] ペインで、次のオプションを設定します。</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 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: <ol style="list-style-type: none"> 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。 <ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> 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)	<p>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正常性チェックを実行します。これは、正常性チェックで構成できます。</p> <ul style="list-style-type: none"> [プロトコル (Protocol)]: [HTTP] または [HTTPS] をクリックして選択します。 [パス (Path)]: パスを入力します。デフォルトは / です [ポート (Port)]: 正常性チェックを実行するポートを入力します。 [詳細設定 (Advanced Settings)] <ul style="list-style-type: none"> [異常なしきい値 (Unhealthy Threshold)]: 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アダプタイズされるタイミングを決定します。 [タイムアウト (Timeout)]: 正常性チェックのタイムアウトの値を入力します。 [間隔 (Interval)]: 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 (Success Code)]: 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 (Use host from rule)]: 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 (Host)]: [ルールからホストを使用 (Use host from rule)] がチェックされていない場合は、正常性チェックに使用するホスト名を指定します。 <p>完了したら、[ルールの追加] をクリックします。</p>

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 (Add Cloud Load Balancer Listener)] 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。

[プロパティ (Properties)]	説明
プロトコル (Protocol)	[TCP] または [UDP] をクリックして選択します。
[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。
[フロントエンド IP 名 (Frontend IP Name)]	<p>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。</p> <ul style="list-style-type: none"> • [デフォルト IP を使用 (Use default IP)] : 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 (65 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。 <p>詳細については、Azure 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 アドレスの構成について (6 ページ) を参照してください。</p>
ルール設定	<p>[ルール設定 (Rule Settings)] ペインで、次のオプションを設定します。</p> <ul style="list-style-type: none"> • 名前 : 規則の名前を入力します。 • [アクションタイプ (Action Type)] : 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 (Port)] : バックエンドプール サーバー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 (Protocol)] : [TCP] または [UDP] をクリックして選択します。 • [EPG] : Web サーバーがトラフィックを処理する EPG。

[プロパティ (Properties)]	説明
正常性チェック (Health Checks)	<p>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 ターゲットで正常性チェックを実行します。ここで構成できます。</p> <ul style="list-style-type: none"> • [プロトコル (Protocol)]: [TCP]、[HTTP] または [HTTPS] をクリックして選択します。 • [ポート (Port)]: 正常性チェックを実行するポートを入力します。 • [詳細設定 (Advanced Settings)] <p>[異常なしきい値 (Unhealthy Threshold)]: 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アダプタイズされるタイミングを決定します。</p> • [間隔 (Interval)]: 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。 <p>終了したら、[Add] をクリックします。</p>

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>
```

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

```
</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のオプションについて（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、次のようになります。

- 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 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" />
  <cloudLIIf name="provider">
    <cloudEPSelector name="east" matchExpression="IP=='{(eastus_FwUntrustSubnet)}'" status="" />
  </cloudLIIf>
  <cloudLIIf name="consumer">

```

REST API を使用したサードパーティ ロードバランサの作成

```

    <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のオプションについて (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 を使用したサービス 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。

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 を使用したサービス グラフの作成

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" deviceLIIfName="external"/>
<vnsAbsFuncConn attNotify="no" name="provider" deviceLIIfName="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/cloudcomp/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"/>

```

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

```

</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>
</polUni>

```



```

</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}}"/>
      </cloudLB>
    </fvTenant>
  </polUni>

```

ステップ3 プロバイダー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/cloudddomp/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/cloudddomp/provp-azure/region-[[{region}]]/zone-default"/>
        </cloudSubnet>
        <cloudSubnet ip="{{BackALBSubnet}}" name="BackALBSubnet" status="">
          <cloudRsZoneAttach status=""
tDn="uni/cloudddomp/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>
</vnsAbsNode>
    <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、プロバイダー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 アプリケーション ゲートウェイのサービス 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 ロード バランシングのサービス 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、次のようになります。

- `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 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/nToHLnmDBq2BfLimx/zNJQC9bGuzr8Mj7dm0
XuHfQYgV0h1PtL4Pdx5f5qjB0NbhJAVB1Gw8cDiErEgAXy9Km27ySo2foKryNqCre
Ginn/CgF75QPied568eScNDZPt/eMeHAuRX/PykKUatWwncGanjvHqc+SOLPF6TD
gQ5nwOHFVvYm2DY8bdfYwRwMgsO7JqZzbPMptA2QWblILsSoIrdkIgf6ZfYy/EN
bH+nYN2rJt8lZysxz0YmR0oRQHTiN2NiDY/ZV63yxCXfLg9qpNZCuD8KOfdCZPEq
8taklWBxiR5/HRPscWAdWQsoiKgG1k4NEbFA9QIDAQABAoIBAQQQA9IslYrdtqN
q6mZ3s2BNfF/4kgb7gn0Dws+9EJJLCJNZVhFEo2ZxxypPp6HRnjYS50W83/E1and
+GdlbSucTuxqfWQVh7r1ebYZIwK+NYSjr5yNVxux8U2hCNNV8WVWqkJjKcUqICB
Bm47FKj53LV46zE0gyCaibFrYxZJ9+farGneyBdnoV+3thmez7534Kci0t3J3Eri
lgSY3ql6hPXb2ZXAP4jdAoLgWdu4I1M6QoiWopZM/QYIE/WtPYyJ0QzNCXObtc5
FboDcvedsgd4x5G1fv2A4xTBQMCTZUZJ9fYAcFogTZXD+UVqxorh47tf/mz+1fjq
f1XphEd1AoGBAPV1vKfGW46qqRnYovfryxxz4OMlsvSgcJpQTQtBQi2koJ8OwEZJ
2s+CX0r+oDqpW23go/QEVYVkcic9RGkJBNGel+dm/bTjzgmQYtqSCNtecTsZD5JN
y1jkciiZznDkjCjReS2Zk3dGXIBriYk7ezp2z7EKfDrHe5x5ouGMgCnAoGBAOnh
buDEohv8KJaB+DiUfhtoa3aKNPBO+zWPCHP0HFGjPXshJcIYZc1GcycmuDKVnNdD
MxhE/yOnQHowi4T9FMLpz5yh5zucUVqOBgB1P6MzbC5t5MtLrEYr/AqFN11CqyXQ
cVcT6iCW1OAFJRw3c/OiESwLMzchsl8RnbwOi6kDAoGBANv1zmPb07zB3eGTCU0t
KGiqwFLncUkVaDZZRFZYpNwiRkoe73j9brkNbgCqxW+NLP5UjoeFry0N6y106q/
ZA4I7FnXryLBw2HYuw41Vixl+XOZ/HeO3RmFN1z717dGmaGbv43aKIB9x+X5n8wF
6z1NtBHmBk7yNwom1IRag1sbAoGAXOp4cJ/tJNXSe7AswHDQCL68uimJdDfZ5nKG
k83nE+Qc0qQozDJAmCiSfmuSNRnSep3FiafjBFX0X4h+mdbJcc7bagRnI92Mh0X
mOwsp4P2GdywkZwdbuHQ6UBp1Ferf9aztzTn+as6xKOUATEezy9DK9zMWzQhhtay
m9yZTp0CgYEAlUtcpWjAzQbXODJGmxGdAAakPpeiKw/Da3MccrTdgJt88ezM1Oej
Pdoab0G2PfcgJzTSGk7N4XArVKeq7pgz0kwcYash06A2Hal+D1z/bGoZP+kmD/x
Ny82phxYOXCncE5Vv921U59+j7e067UFLAYJe6fu+oFImvofRnP4DIQ=
-----END RSA PRIVATE KEY-----" cert="-----BEGIN CERTIFICATE-----
MIIElTCCA32gAwIBAgIJAKWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBACTCFNhb3NlMRlweAYDVQQK
Ew1NeUNvbXBhbnkxDjAMBGNVBAStBU15T3JnMRgwFgYDVQDDFA8qLmFtYXpvcjYy
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY2lzY28uY29tMB4XDTE4MTAw
MjIwIjEwNTMwNVV0XDE5MTAwMjIwIjEwNTMwNVV0YXZzZm9uYXZzZm9uYXZzZm9u
YXZzZm9uYXZzZm9uYXZzZm9uYXZzZm9uYXZzZm9uYXZzZm9uYXZzZm9uYXZzZm9u
EwJdQTERMA8GA1UEBxMIU2FuIEpvc2UxejAQBGNVBAoTCU15Q29tcGFueTEOMAwG
A1UECXMFTXlPcmcxGDAWBgNVBAMUyouYWLhem9uYXdzLmNvbTEGMB4GCSqGSIb3
DQEJARYRcmFtc2hhaEBjaXNjby5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQQDgMbfFor5Ee/+dOgcueYMGryF8uKaBf/M01AL1sa7OvwyPt2bRe4d9B
ga/SHU+0vg93F/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXv1A8h53nrX5Jw0Nk+394x4c5Ff8/KQpRq1ZadwZqe08epz5I4s8XpMOBDmfA
4ccW/IzYNjxt9lhataYaw7smpnNs8ym0DZBZuUguxKgit2QgiB/pl9jL8Q1sf6dg
3aslPyXNizHPRiZHSFAoI3Y2INj91XrflEJd8uD2qk1kK4Pwo590Jk8Sry1qSj
YHGJh8de+xxYB1ZCyIqAbWTg0RsUD1AgMBAAGjgfUwgfiwHQYDVR0OBBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMGbowgbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIGNMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNV
BACTCFNhb3NlMRlweAYDVQQKEw1NeUNvbXBhbnkxDjAMBGNVBAStBU15T3Jn
MRgwFgYDVQDDFA8qLmFtYXpvcjYycy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY2lzY28uY29tggkApY2On/9qsGwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAE/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iur84mQzhoT
nx5CN109xu5ml5baCYZsSnn6D7usC092bPA/kRCGxt29gkjpWA74tJHqIhVWgBM
mOrLisShoelewv+wRl0oVRChlTfKtXO68Tuk6vrqpW76hKfOHia7b2h1IIMdq6VA/
+A5FQ0xqYfKdVd2RaINpzI8mqZiszqw+7E6j1PL5k4tftWEaYpfpPlVesFEyJEL
gHBUiPt8TIbamyI8qUQmB/emnLXekQ5PrxdRnleA3h8jfq3D1CQRTLjMDL3tpFwg
qopM6et5ZKqShX4T87BsgZIoiquzXqsuHg==
-----END CERTIFICATE-----">
  </pkiKeyRing>

  <pkiTP status="" name="lbTP" certChain="-----BEGIN CERTIFICATE-----
```

REST API を使用した HTTPS サービス ポリシーの作成

```

MIElTCCA32gAwIBAgIJAkWNjp//arBsMA0GCSqGSIb3DQEBCwUAMIGNMQswCQYD
VQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBACtCFNhb3NlMRlWEAYDVQQK
Ew1NeUNvbXBhbnkxDjAMBGNVBAStBU15T3JnMRgwFgYDVQQDFA8qLmFtYXpvc2F3
cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNoYWhAY21zY28uY29tMB4XDTE4MTAw
MjIwNTMwNV0XDTE5MTAwMjIwNTMwNV0wY0x0c2ZAJBgNVBAYTA1VTRQswCQYDVQQL
EwJDRTERMA8GA1UEBxMIU2FuIEpvc2UxU2EjAQBgNVBAoTCU15Q29tcGFueTEOMAwG
A1UEC3R1PmcmcGDABWBgNVBAMUDyouYW1hem9uYXdzLmNvbTEgMB4GCSqGSIb3
DQEJARYRcmFtc2hhaEBjaXNjby5jb20wggeiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQQDgMbfFor5Ee/+dOgcueYMGrYF8uKaBf/M01AL1sa7OvwyPt2bRe4d9B
ga/SHU+0vg93F/mqMHQ1seMBUHUbDxwOISsSABfL0qbbvJKjZ+gqvI2oJF4aKef8
KAXv1A8h53nrx5Jw0Nk+394x4cC5Ff8/KQpRq1ZadwZqe08epz5I4s8XpMOBDMfA
4ccW/IzYNjxt91hataYaw7smpnNs8ym0DZBZuUguxKgit2QgiB/pl9jL8Q1sf6dg
3aslPyXNizHPRiZSHsFAAdOI3Y2INj91XrLEJd8uD2qk1kK4Pwo590Jk8Sry1qSJ
YHGJHn8dE+xxYB1ZCyiIqAbWTg0RsUD1AgMBAAGjgfUwgfIwHQYDVR0OBBYEFBYq
K3b39+1oOr4IBSsePwcOpML7MIHCBgNVHSMGjbogwbeAFBYqK3b39+1oOr4IBSse
PwcOpML7oYGTpIGQMIgNMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNV
BACtCFNhb3NlMRlWEAYDVQQKEw1NeUNvbXBhbnkxDjAMBGNVBAStBU15T3Jn
MRgwFgYDVQQDFA8qLmFtYXpvc2F3cy5jb20xIDAeBgkqhkiG9w0BCQEWEXJhbXNo
YWhAY21zY28uY29tggkApY2On/9qsGwwDAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAE/RuzCheLIbHbrurGet6eaVx9DPYydNiKVBSAKO+5iuR84mQzhoT
nx5CN109xu5m15baCYZsSnn6D7usc092bPA/kRCGxt29gkjpWA74tJHqIhVWgbM
mOrLiSHoeleWv+wR10oVRCh1TfKtXO68TUk6vrqpw76hKfOHIA7b2h1IIMdq6VA/
+A5FQ0xqYfqKdVd2RaINpzI8mqZisZqw+7E6j1PL5k4tftWEaYpfGf1VesFEyJEL
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。