ポリシー ベース リダイレクトの設定

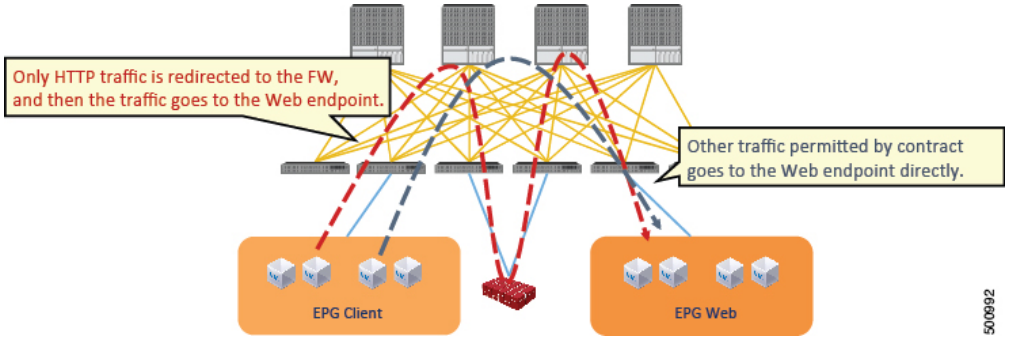
ポリシーベースのリダイレクトについて

Cisco Application Centric Infrastructure(ACI) ポリシーベース リダイレクト（PBR）により、レイヤ 4 ーレイヤ 7 パッケージなしで、ファイアウォールやロード バランサなどのサービス アプライアンスを管理対象ノードまたは非管理対象ノードとしてプロビジョニングできます。一般的な使用例としては、プールしてアプリケーション プロファイルに合わせて調整すること、また容易にスケーリングすることができ、サービス停止の問題が少ないサービス アプライアンスのプロビジョニングがあります。PBR により、プロビジョニングするコンシューマおよびプロバイダー エンドポイント グループをすべて同じ仮想ルーティングおよび転送（VRF）インスタンスに含めることで、サービス アプライアンスの展開をシンプル化できます。PBR の導入は、ルート リダイレクト ポリシーおよびクラスタのリダイレクト ポリシーの設定と、ルーティングとクラスタ リダイレクト ポリシーを使用するサービス グラフ テンプレートの作成から構成されます。サービス グラフ テンプレートを展開した後は、サービス グラフ プロバイダーの

エンドポイントグループを利用するためにエンドポイントグループを有効にすることにより、サービスアプライアンスを使用します。これは、vzAnyを使用することにより、さらに簡素化し、自動化できます。パフォーマンスの要件が、専用のサービスアプライアンスをプロビジョニングするかどうかを決定するものとなるのに対し、PBRを使用すれば、仮想サービス アプライアンスの展開も容易になります。

次の図は、ファイアウォールへのトラフィックに固有の、リダイレクトの使用例を示しています:

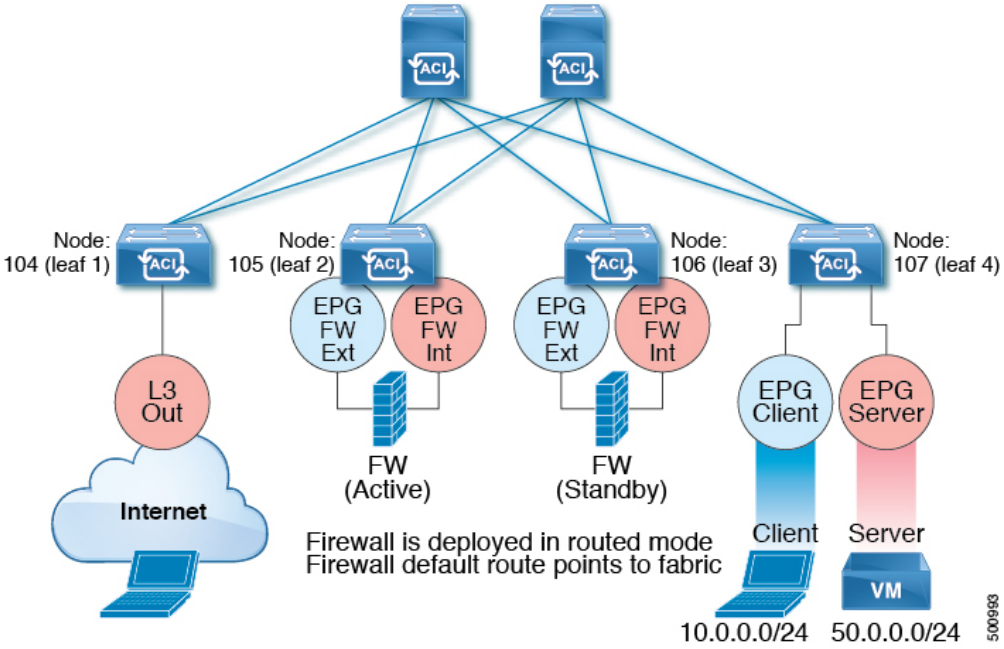
図 *1*: 使用例: ファイアウォール特有のトラフィックのリダイレクト



この使用例では、2つの情報カテゴリを作成する必要があります。最初の情報カテゴリはHTTPトラフィックを許可します。その後このトラフィックはファイアウォールにリダイレクトされます。トラフィックはファイアウォールを通過してから、Webエンドポイントに送られます。2番目の情報カテゴリはすべてのトラフィックを許可します。これは最初の情報カテゴリではリダイレクトされなかったトラフィックをキャプチャします。トラフィックはそのままWebエンドポイントに送られます。

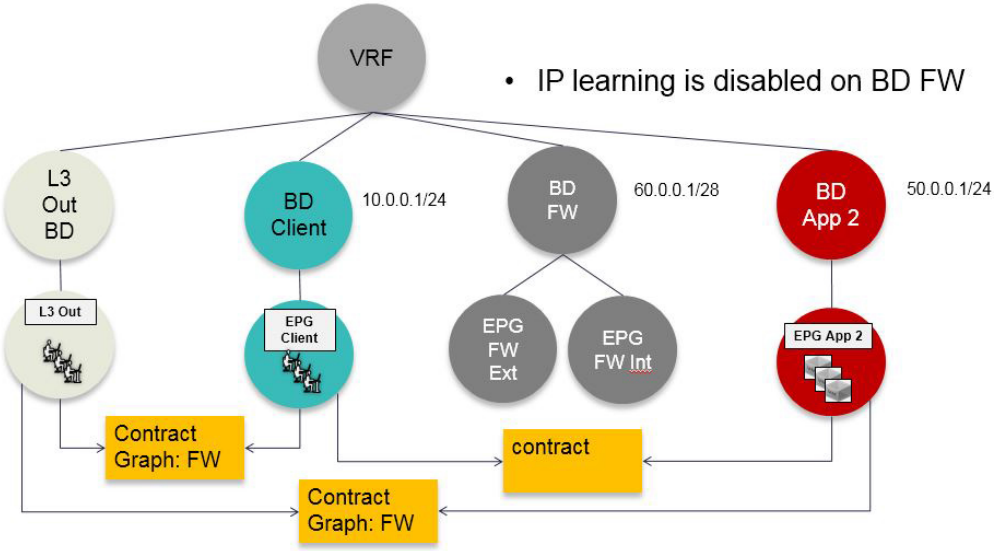
次の図は、ACI PBR物理トポロジのサンプルを示しています:

図 *2*:サンプルの *ACI PBR* 物理トポロジ



次の図は、ACI PBR 論理トポロジのサンプルを示しています:

図 *3*:サンプルの *ACI PBR* 論理トポロジ



これらの例はシンプルな導入ですが、 ACI PBR は、ファイアウォールやサーバのロード バランサなどのような、複数のサービスのために物理および仮想サービス アプライアンスの両方を混在させたものにスケールアップすることを可能にします。

複数ノード ポリシー ベースのリダイレクトについて

複数ノード ポリシー ベースのリダイレクトは、1 つのサービス チェーンで最大 3 つのノードをサポートすることにより、PBR を強化します。どのサービス ノードのコネクタがトラフィックの終端になるかは設定することができ、この設定に基づいて、サービス チェーンの送信元および宛先クラス ID が決定されます。複数のノード PBR 機能では、ポリシー ベースのリダイレクトはサービス ノード コネクタのコンシューマ側、プロバイダ側、またはその両方で有効にすることができます。これは、転送方向にも、または逆方向にも設定できます。サービス ノードのコネクタで PBR ポリシーを設定した場合、そのコネクタがトラフィックを終端することはありません。

対称ポリシー ベースのリダイレクトについて

対称ポリシー ベースのリダイレクト (PBR) 構成により、サービス アプライアンスのプールをプロビジョニングできるため、コンシューマとプロバイダーのエンドポイント グループ トラフィックがポリシー ベースになります。トラフィックは、送信元および宛先 IP 等価コスト マルチパス ルーティング (ECMP) プレフィックス ハッシュに応じて、プール内のサービス ノードの 1 つにリダイレクトされます。

（注） 対称 PBR 構成には 9300-EX ハードウェアが必要です。

対称 PBR REST のサンプルの例を以下に示します。

```
Under fvTenant svcCont

<vnsSvcRedirectPol name="LoadBalancer_pool">
          <vnsRedirectDest name="lb1" ip="1.1.1.1" mac="00:00:11:22:33:44"/>
          <vnsRedirectDest name="lb2" ip="2.2.2.2" mac="00:de:ad:be:ef:01"/>
          <vnsRedirectDest name="lb3" ip="3.3.3.3" mac="00:de:ad:be:ef:02"/>
</vnsSvcRedirectPol>

<vnsLIfCtx name="external">
          <vnsRsSvcRedirectPol tnVnsSvcRedirectPolName="LoadBalancer_pool"/>
          <vnsRsLIfCtxToBD tDn="uni/tn-solar/bd-fwBD">
</vnsLIfCtx>

<vnsAbsNode name="FW" routingMode="redirect">
```

対称 PBR NX-OS スタイルの CLI コマンドの例を次に示します。

テナント スコープの下の次のコマンドは、サービス リダイレクト ポリシーを作成します。

```
apic1(config-tenant)# svcredir-pol fw-external
apic1(svcredir-pol)# redir-dest 2.2.2.2 00:11:22:33:44:56
```

次のコマンドは PBR を有効にします。

```
apic1(config-tenant)# l4l7 graph FWOnly contract default
apic1(config-graph)# service FW svcredir enable
```

次のコマンドは、デバイス選択ポリシー コネクタの下にリダイレクト ポリシーを設定します。

```
apic1(config-service)# connector external
apic1(config-connector)# svcredir-pol tenant solar name fw-external
```

ポリシーベースのリダイレクトとハッシュアルゴリズム

（注） この機能は、APIC リリース 2.2(3x) リリースおよび APIC リリース 3.1 (1) でさせてで使用できます。APIC Release 3.0(x) ではサポートされていません。

Cisco APIC、リリース 2.2(3x) では、ポリシー ベースのリダイレクト機能 (PBR) は、次のハッシュ アルゴリズムをサポートします。

- 送信元 IP アドレス
- 宛先 IP アドレス
- ソース IP アドレス、宛先 IP アドレスおよびプロトコル タイプ (着信も、対称) に基づいてアルゴリズムが以前のリリースでサポートされます。

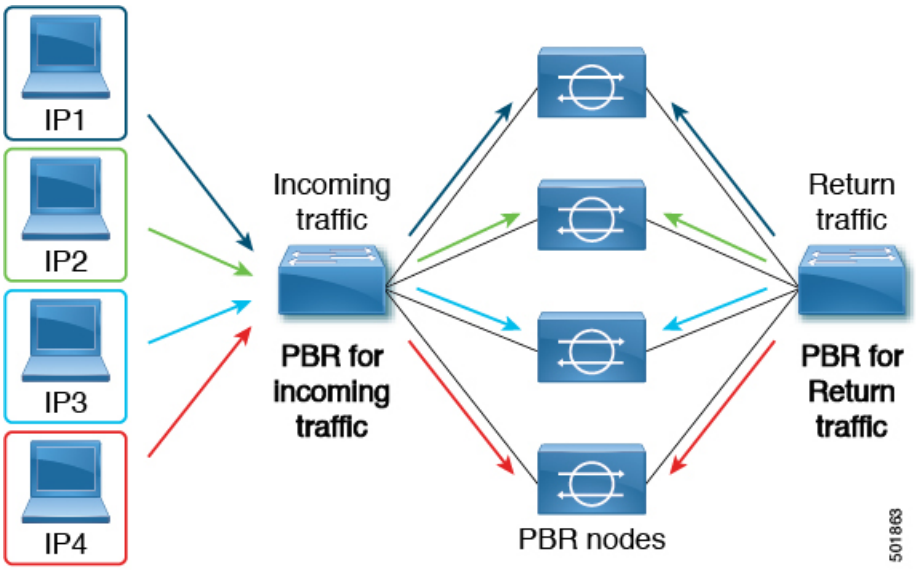
ポリシーベースのリダイレクトの修復性のあるハッシュ

対称 PBR では、着信と戻りユーザ トラフィックは、ECMP グループで同じ PBR ノードを使用します。ただし、PBR ノードのいずれかがダウンするか、障害を起こした場合には、既存のトラフィック フローは別のノードに送られて再ハッシュされます。これは、機能しているノードの既存のトラフィックが、現在の接続情報を持っていない他の PBR ノードに負荷分散のために送られるといったような問題の原因となります。トラフィックがステートフルファイアウォールを通過する場合には、接続がリセットされることにもつながります。

修復性のあるハッシュは、トラフィック フローを物理ノードへマッピングするプロセスで、障害の発生したノードからのフロー以外のトラフィックが再ハッシュされるのを避けられるようにします。障害を起こしたノードからのトラフィックは、「バックアップ」ノードに再マッピングされます。「バックアップ」ノード上の既存のトラフィックは移動できません。

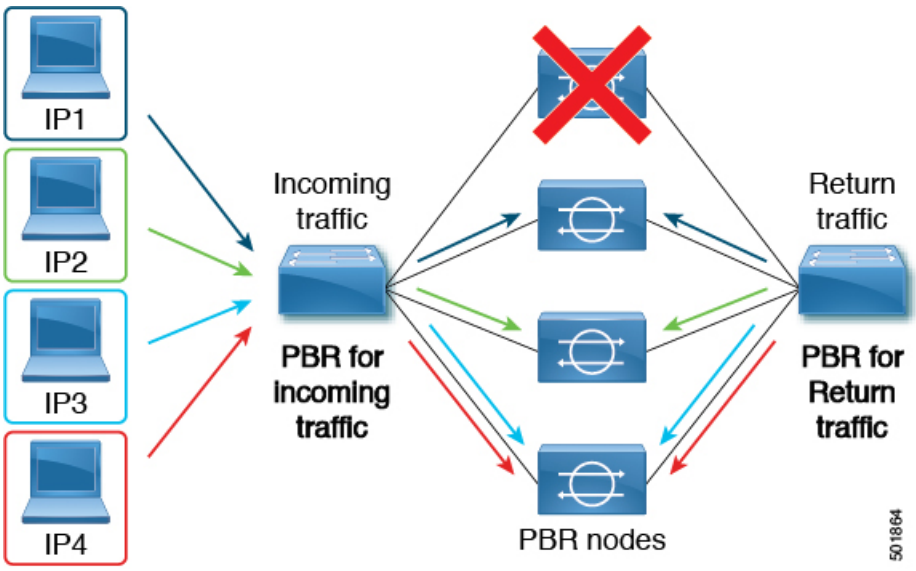
次の図は、着信と戻りユーザ トラフィックが同じ PBR ノードを使用している、対称 PBR の基本的な機能を示しています。

図 *4*: 対称 *PBR*



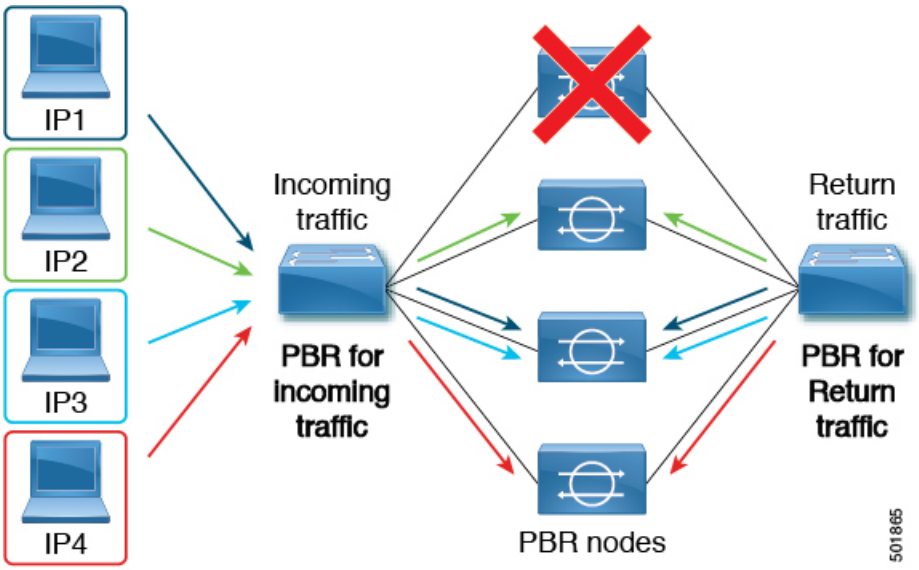
次の画像は、PBR ノードのいずれかが無効か、障害が発生したときに何が生じるかを示しています。IP1 のトラフィックは隣のノードへ再ハッシュされ、IP2 および IP3 のトラフィックがもう 1 つの PBR ノードに負荷分散されます。このことは、前述のように、他の PBR ノードが IP2 および IP3 トラフィックの現在の接続情報を持っていない場合、接続の中断や遅延という問題につながることがあり得ます。

図 *5*: 修復性のあるハッシュがない場合の無効化された/障害の発生した *PBR* ノード



最後の図は、修復性のあるハッシュが有効になっている場合に、この同じ使用例がどのように対処されるかを示しています。無効化された/障害の発生したノードからのユーザ トラフィックだけが移動されます。その他のすべてのユーザ トラフィックは、それぞれの PBR ノードに残ります。

図 *6* : 修復性のあるハッシュがある場合の無効化された/障害の発生した *PBR* ノード



ノードがサービス可能状態に戻ると、障害の発生したノードからアクティブなノードに再ハッシュされたトラフィック フローは、再度アクティブ化されたノードに戻ります。

（注） ECMP グループの PBR ノードを追加または削除すると、すべてのトラフィック フローが再ハッシュされる原因となることがあります。

L4 ～ L7 のポリシー ベース リダイレクトで復元力のあるハッシュを有効にする

始める前に

このタスクでは、L4-7 ポリシー ベースのリダイレクト ポリシーが作成されたことを前提としています。

ステップ 1 メニュー バーで、**Tenants** > **All Tenants** の順に選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ウィンドウで、**Tenant** ***tenant_name*** > **Policies** > **Protocol** > **L4-L7 Policy Based Redirect** > ***L4-L7_PBR_policy_name*** を選択します。

ステップ 4 Work ペインで、**Resilient Hashing Enabled** チェック ボックスをオンにします。

ステップ 5 [Submit] をクリックします。

コンシューマとプロバイダブリッジドメイン内のサービス ノードへの PBR によるサポート

Cisco APIC 3.1(1) リリース以降、コンシューマやプロバイダを含むブリッジ ドメイン (BD) は、サービス ノードもサポートするようになりました。したがって今後は、別の PBR ブリッジ ドメインをプロビジョニングする必要はありません。

Cisco Nexus 9300-EX と 9300-FX プラットフォームのリーフ スイッチは、この機能をサポートします。

ポリシーベースのリダイレクトを設定する際の注意事項と制約事項

ポリシーベースのリダイレクトを行うサービス ノードを計画する際には、次の注意事項と制約事項に従ってください:

- Cold Standby のアクティブ/スタンバイ導入では、サービス ノードにアクティブな導入の MAC アドレスを設定します。Cold Standby のアクティブ/スタンバイ導入では、アクティブ ノードがダウンすると、スタンバイ ノードがアクティブ ノードの MAC アドレスを引き継ぎます。
- ネクスト ホップ サービス ノードの IP アドレスと仮想 MAC アドレスを指定する必要があります。
- ポリシー ベースのリダイレクト ブリッジ ドメインでは、エンドポイント データプレーンの学習を無効にする必要があります。
- 別のブリッジ ドメイン サービスにアプライアンスをプロビジョニングします。Cisco Application Policy Infrastructure Controller（Cisco APIC）リリース 3.1(x) 以降、別のブリッジ ドメインでのサービス アプライアンスのプロビジョニングは必須ではなくなりました。そのためには、Cisco Nexus 9300-EX と 9300-FX プラットフォームのリーフ スイッチが必要です。
- Cisco APIC リリース 3.1 ソフトウェアからダウングレードすると、内部コードが、ポリシーベースのリダイレクト ブリッジ ドメインがコンシューマまたはプロバイダと同じブリッジ ドメインを使用しているかのチェックを行います。その場合にはダウングレード中にエラーが出されます。そのような設定は Cisco APIC の以前のバージョンではサポートされないからです。
- サービス アプライアンス、送信元、およびブリッジ ドメインは、同じ VRF に存在できます。
- Cisco N9K-93128TX、N9K-9396PX、N9K-9396TX、N9K-9372PX、および N9K-9372TX スイッチでは、サービス アプライアンスを、送信元または宛先のいずれかのエンドポイント

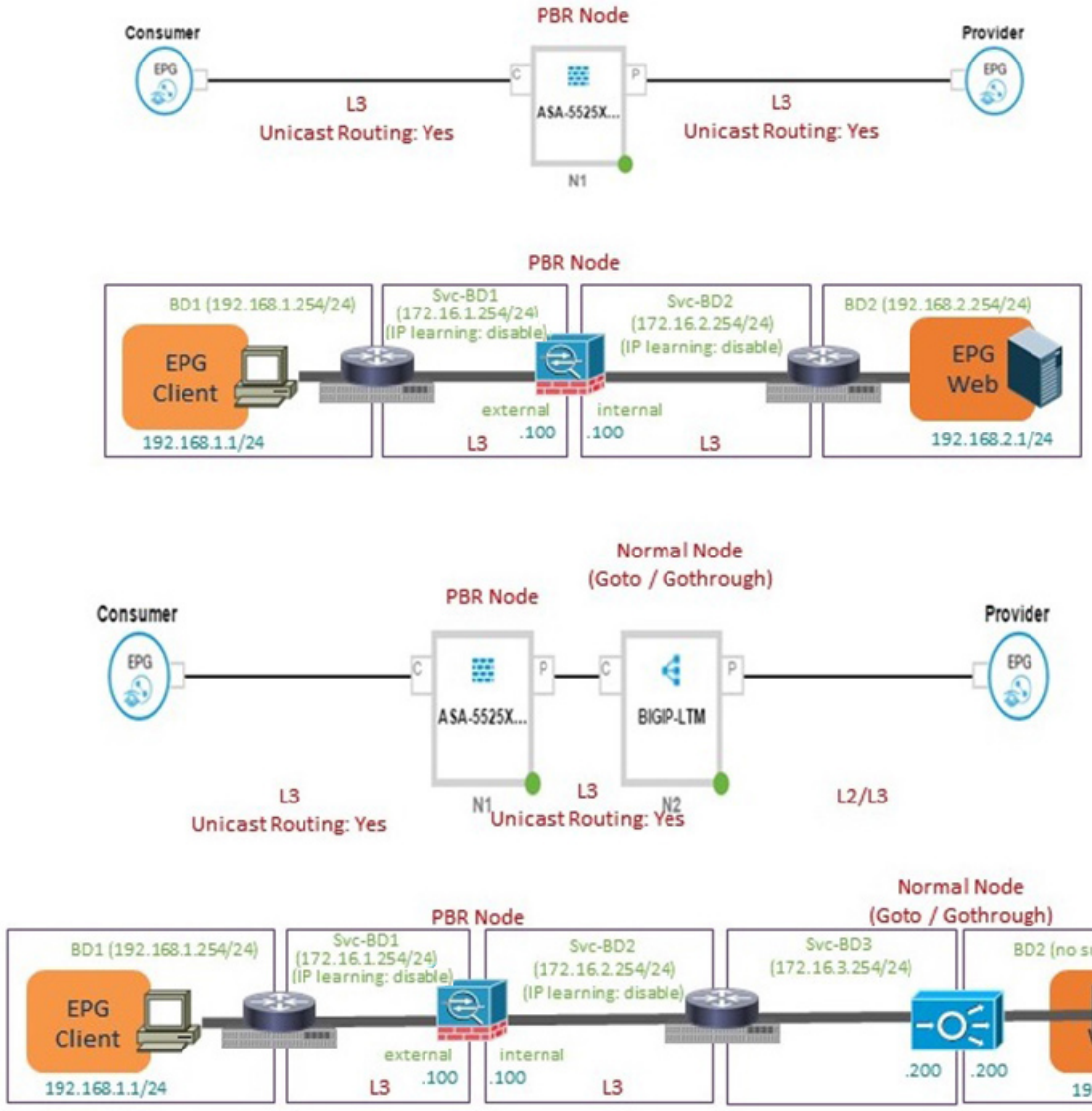
グループと同じリーフ スイッチに配置することはできません。Cisco N9K-C93180YC-EX および N9K-93108TC-EX スイッチでは、サービス アプライアンスを、送信元または宛先のいずれかのエンドポイント グループと同じリーフ スイッチに配置することができます。

- サービス アプライアンスは、通常のブリッジ ドメインにのみ配置できます。
- サービス アプライアンスのプロバイダのエンドポイント グループによって提供される契約は `allow-all` に設定できますが、トラフィックを Cisco Application Centric Infrastructure (Cisco ACI) ファブリックでルーティングすることはできません。
- Cisco APIC リリース 3.1(1) 以降では、Cisco Nexus 9300-EX と 9300-FX プラットフォームのリーフ スイッチを使用する場合、ポリシー ベースのリダイレクト ブリッジ ドメインでエンドポイント データプレーン学習を無効にする必要はありません。サービス グラフの導入時には、ポリシーベースのリダイレクト ノード EPG の場合にのみ、エンドポイント データプレーンの学習は自動的に無効にされます。非 EX および非 FX プラットフォーム リーフ スイッチを使用する場合は、ポリシー ベースのリダイレクト ブリッジ ドメインでエンドポイント データプレーンの学習を無効にする必要があります。
- 複数のノードのポリシー ベースのリダイレクト (複数ノード PBR):
  - ポリシー ベース ルーティングを設定できるサービス チェーンでは、最大 3 つのノードをサポートしています。
  - ロード バランサの複数ノード PBR L3 宛先についての注意事項:
    - L3 宛先のアップグレード: L3 Destination (VIP) パラメータは、アップグレード後にはデフォルトで有効になります。このことで問題は発生しません。PBR ポリシーは特定のサービス ノードで設定されていたわけではなく (3.2(1) より前)、ノード コネクタが L3 宛先として扱われており、新しい Cisco APIC バージョンでも引き続き同様だからです。
    - トラフィックは、必ずしもコンシューマ/プロバイダを宛先とする必要はありません。
    - 転送方向では、トラフィックはロード バランサを宛先とします。
    - 逆方向では、SNAT が有効になっている場合、トラフィックの宛先はロード バランサの内部レッグになります。
    - 両方向では、論理インターフェイス コンテキストの L3 宛先 (VIP) を有効にします (チェックします)。
    - 両方向で L3 宛先 (VIP) を有効にする (チェックする) と、内部側で設定された PBR ポリシーにより、ロード バランサ内部で SNAT から 非 SNAT への切り替えを行うことができます。
    - SNAT が無効の場合:
      - 逆方向トラフィックは、ロードバランサの内部レッグではなく、コンシューマを宛先とします (内部レッグで PBR ポリシーが有効にされている)

- PBR ポリシーが適用されるため、この状況では L3 宛先 (VIP) は適用されません。

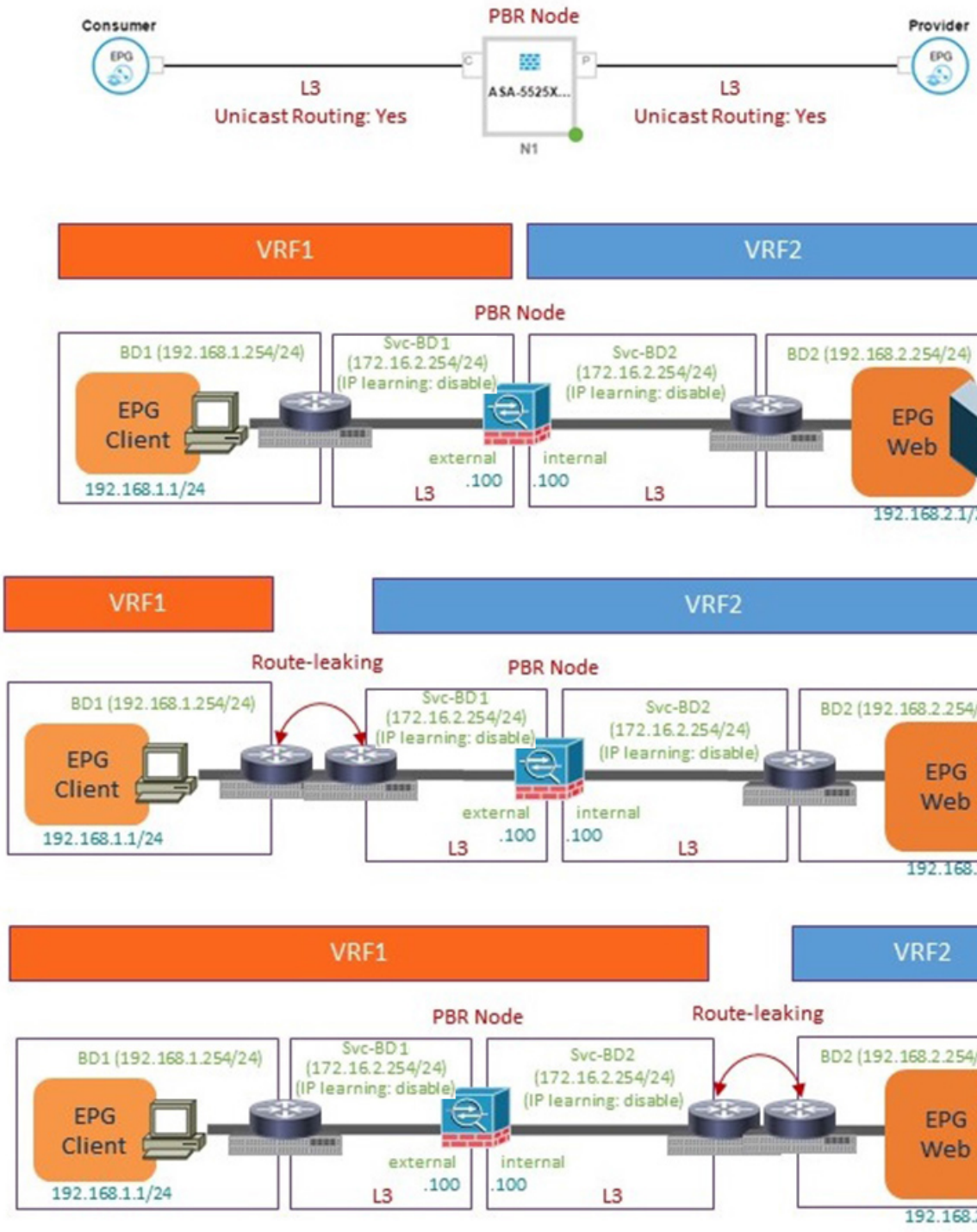
- マルチキャストおよびブロードキャスト トラフィック リダイレクションはサポートされていません。
- 透過的なサービスへのリダイレクションはサポートされていません。
- リダイレクト ポリシーの宛先を別のグループに変更した場合、Cisco APIC は変更に対してエラーを発生し、ポリシーの動作状態は無効になります。ポリシーを再度有効にするには、エラーをクリアする必要があります。
- 同じ VRF インスタンス内でサポートされているポリシーベースのリダイレクトの設定には、次のものが含まれます:

図 *7*: 同じ *VRF* インスタンス内でサポートされるポリシー ベースのリダイレクトの設定



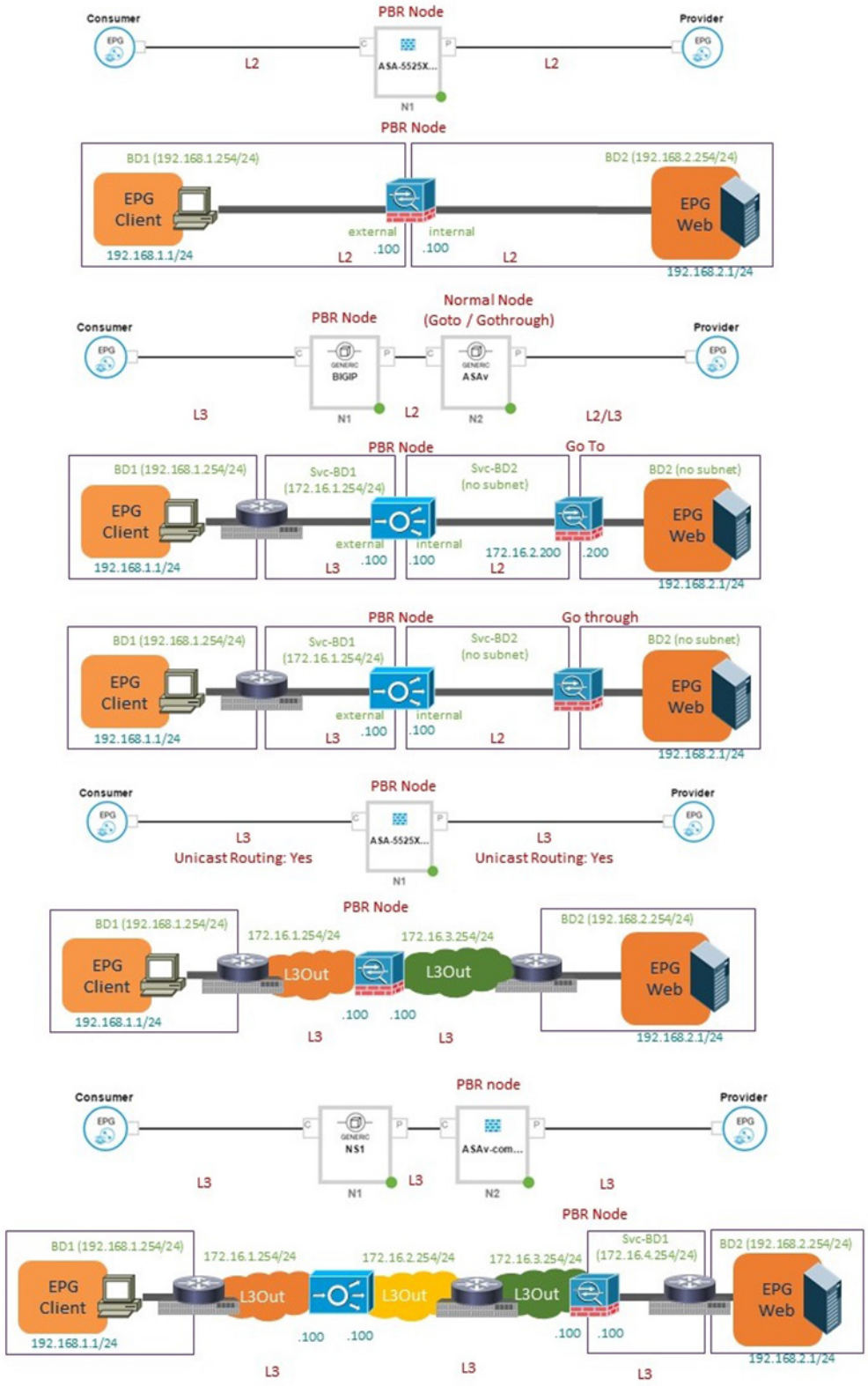
- 別の VRF インスタンス内でサポートされるポリシーベースのリダイレクトの設定には、次のものが含まれます:

図 *8* : 別の ***VRF*** インスタンス内でサポートされるポリシーベースのリダイレクトの設定



- サポートされていないポリシー ベースのリダイレクト設定は次のとおりです:

図 *9:* サポートされていないポリシー ベースのリダイレクト設定



GUI を使用したポリシー ベース リダイレクトの設定

次の手順では、GUI を使用してポリシー ベース リダイレクト (PBR) を設定します。

（注） ポリシー ベースのリダイレクトの機能は、GUI では「policy-based routing」と呼ばれます。

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [Navigation] ウィンドウで、**Tenant** *tenant_name* > **Services** > **L4-L7** > **Devices** を選択します。

ステップ 4 作業ウィンドウで、 **Actions** > **Create L4-L7 Devices** を選択します。

ステップ 5 **Create L4-L7 Devices** ダイアログボックスで、必要に応じてフィールドに入力します。

General セクションの **Service Type** は、**Firewall** または **ADC** にできます。

ステップ 6 ナビゲーション ウィンドウで、**Tenant** *tenant_name* > **Services** > **L4-L7** > **Service Graph Templates** を選択します。

ステップ 7 作業ウィンドウで、**Action** > **Create L4-L7 Service Graph Template** を選択します。

ステップ 8 **Create L4-L7 Service Graph Template** ダイアログボックスで、次の操作を実行します:

a) **Graph Name** フィール小渡に、サービス グラフ テンプレートの名前を入力します。

b) **Graph Type** ラジオ ボタンで、**Create A New Graph** をクリックします。

c) **Device Clusters** ペインで作成したデバイスを、コンシューマ エンドポイント グループとプロバイダ エンドポイント グループの間にドラッグ アンド ドロップします。これで、サービス ノードが作成されます。

APIC リリース 3.2(1) においては、オプションとしてステップ c PBR を繰り返すことで、PBR をサポートするには、最大 3 つのサービス ノードのデバイスを含めることができます。

d) デバイスのサービスの種類に基づいて、以下を選択します:

ファイアウォールの場合には、**Routed** を選択して、次の手順を続けます。

ADC の場合には、**One-Arm** または **Two-Arm** を選択して、次の手順を続けます。

e) **Profile** ドロップダウンリストで、デバイスに適した機能プロファイルを選択します。プロファイルが存在しない場合は、 「GUI を使用した機能プロファイルの作成」の手順に従って作成します。

f) **Route Redirect** チェックボックスをオンにします。

g) [Submit] をクリックします。

新しいサービス グラフ テンプレートが [Service Graph Templates] テーブルに表示されます。

ステップ 9 ナビゲーション ウィンドウで、**Tenant** *tenant_name* > **Policies** > **Protocol** > **L4-L7 Policy Based Redirect** を選択します。

ステップ 10 作業ウィンドウで、**Action** > **Create L4-L7 Policy Based Redirect** を選択します。

ステップ 11 **Create L4-L7 Policy Based Redirect** ダイアログボックスで、必要に応じてフィールドに入力します。このポリシーベースのリダイレクト ポリシーは、コンシューマ コネクタ用のものです。

ステップ 12 プロバイダ コネクタ用には、別のポリシー ベースのリダイレクト ポリシーを作成します。

ステップ 13 ナビゲーション ウィンドウで、**Tenant** ***tenant_name*** **> Services > L4-L7 > Service Graph Templates >** ***service_graph_template_name*** を選択します。

作成したサービス グラフ テンプレートを選択します。

ステップ 14 サービス グラフ テンプレートを右クリックして、**Apply L4-L7 Service Graph Template** を選択します。

ステップ 15 **Apply L4-L7 Service Graph Template to EPGs** ダイアログボックスで、次の操作を実行します:

a) **Consumer EPG/External Network** ドロップダウンリストで、コンシューマ エンドポイント グループを選択します。

b) **Provider EPG/External Network** ドロップダウンリストで、プロバイダ エンドポイント グループを選択します。

c) **Contract** オプション ボタンの **Create A New Contract** をクリックします。

d) **Contract Name** フィールドに、契約の名前を入力します。

e) **No Filter (Allow All Traffic)** チェック ボックスはオンにしないでください。

f) **Filter Entries** テーブルで **+** をクリックしてエントリを追加します。

g) 新しいフィルタ エントリで、名前として [IP] を入力し、**IP** を **Ether Type** として選択して、**Update** をクリックします。

h) **Next** をクリックします。

i) コンシューマ コネクタの **BD** ドロップダウンリストで、コンシューマ エンドポイント グループに接続している外部ブリッジ ドメインを選択します。ブリッジ ドメインでは、**Enable Dataplane Learning** チェックボックスをオフにする必要があります。

j) コンシューマ コネクタの **Redirect Policy** ドロップダウンリストで、コンシューマ コネクタ用に作成したリダイレクト ポリシーを選択します。

k) コンシューマ コネクタの **Cluster Interface** ドロップダウンリストで、コンシューマ クラスタ インターフェイスを選択します。

l) プロバイダ コネクタの **BD** ドロップダウンリストで、コンシューマ エンドポイント グループに接続している内部ブリッジ ドメインを選択します。ブリッジ ドメインでは、**Enable Dataplane Learning** チェックボックスをオフにする必要があります。

m) プロバイダ コネクタの **Redirect Policy** ドロップダウンリストで、プロバイダ コネクタ用に作成したリダイレクト ポリシーを選択します。

n) プロバイダ コネクタの **Cluster Interface** ドロップダウンリストで、プロバイダ クラスタ インターフェイスを選択します。

o) **Next** をクリックします。

p) パラメータをデバイスでの必要に合わせて設定します。

q) **Finish** をクリックします。

NX-OS スタイルの CLI を使用したポリシー ベース リダイレクトの設定

この手順のコマンド例にはには、ルート リダイレクト、クラスタのリダイレクト、およびグラフの導入が含まれます。デバイスはテナント T1 の下に作成されます。デバイスは管理対象モードの Cisco ASA 仮想デバイスになります。アンマネージド モードのデバイスだけが CLI で設定できます。

ステップ 1 デバイス クラスタを作成します。

例：

```
l417 cluster name ifav-asa-vm-ha type virtual vlan-domain ACIVswitch service FW function go-to
    cluster-device Device2 vcenter ifav108-vcenter vm "ASAv_HA1"
    cluster-device Device1 vcenter ifav108-vcenter vm "ASAv_HA"
    cluster-interface provider
      member device Device1 device-interface GigabitEthernet0/1
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 3"
        exit
      member device Device2 device-interface GigabitEthernet0/1
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 3"
        exit
      exit
    cluster-interface failover_link
      member device Device1 device-interface GigabitEthernet0/8
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 10"
        exit
      member device Device2 device-interface GigabitEthernet0/8
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 10"
        exit
      exit
    cluster-interface consumer
      member device Device1 device-interface GigabitEthernet0/0
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 2"
        exit
      member device Device2 device-interface GigabitEthernet0/0
        interface ethernet 1/45 leaf 102
        vnic "Network adapter 2"
        exit
      exit
    exit
exit
```

ステップ 2 テナント PBRv6_ASA_HA_Mode の下に、PBR サービス グラフ インスタンスを展開します。

例：

```
tenant PBRv6_ASA_HA_Mode
  access-list Contract_PBRv6_ASA_HA_Mode_Filter
    match ip
    exit
```

ステップ 3 フィルタが IP プロトコルに一致する PBR 用の契約を作成します。情報カテゴリの下で、レイヤ 4 ～ レイヤ 7 サービス グラフ名を指定します。

サービス アプライアンスのプロバイダ エンドポイント グループによって提供される契約は、`allow-all` 設定では構成できません。

例：

```
contract Contract_PBRv6_ASA_HA_Mode
  scope tenant
  subject Subject
    access-group Contract_PBRv6_ASA_HA_Mode_Filter both
    l4l7 graph PBRv6_ASA_HA_Mode_Graph
    exit
  exit
vrf context CTX1
  exit
vrf context CTX2
  exit
```

ステップ 4 クライアントとサーバのエンドポイント グループ用にブリッジ ドメインを作成します。クライアントとサーバの両方が同じ VRF インスタンスに属します。

例：

```
bridge-domain BD1
  arp flooding
  l2-unknown-unicast flood
  vrf member CTX1
  exit
bridge-domain BD2
  arp flooding
  l2-unknown-unicast flood
  vrf member CTX1
  exit
```

ステップ 5 ファイアウォールの内部および外部レッグ用には、別のブリッジ ドメインを作成します。

PBR では、リモート リーフ スイッチの送信元 VTEP の学習が無効になっている必要があります。これは、**no ip learning** コマンドで行います。

例：

```
bridge-domain External-BD3
  arp flooding
  no ip learning
  l2-unknown-unicast flood
  vrf member CTX1
  exit
bridge-domain Internal-BD4
  arp flooding
  no ip learning
  l2-unknown-unicast flood
  vrf member CTX1
  exit
```

ステップ 6 アプリケーションプロファイルを作成し、エンドポイント グループを指定します。

例：

```
application AP1
  epg ClientEPG
    bridge-domain member BD1
```

```
        contract consumer Contract_PBRv6_ASA_HA_Mode
        exit
      epg ServerEPG
        bridge-domain member BD2
        contract provider Contract_PBRv6_ASA_HA_Mode
        exit
      exit
```

ステップ 7 ブリッジ ドメインのデフォルト ゲートウェイを指定します。

例：

```
    interface bridge-domain BD1
      ipv6 address 89:1:1:1::64/64
      exit
    interface bridge-domain BD2
      ipv6 address 99:1:1:1::64/64
      exit

 interface bridge-domain External-BD3
      ipv6 address 10:1:1:1::64/64
      exit
    interface bridge-domain Internal-BD4
      ipv6 address 20:1:1:1::64/64
      exit
```

ステップ 8 テナント T1 からデバイスをインポートします。

例：

```
l4l7 cluster import-from T1 device-cluster ifav-asa-vm-ha
```

ステップ 9 サービス リダイレクト ポリシーを使用してサービス グラフを作成します。

例：

```
l4l7 graph PBRv6_ASA_HA_Mode_Graph contract Contract_PBRv6_ASA_HA_Mode
      service N2 device-cluster-tenant T1 device-cluster ifav-asa-vm-ha mode FW_ROUTED svcredir
enable
      connector consumer cluster-interface consumer_PBRv6
          bridge-domain tenant PBRv6_ASA_HA_Mode name External-BD3
          svcredir-pol tenant PBRv6_ASA_HA_Mode name External_leg
          exit
      connector provider cluster-interface provider_PBRv6
          bridge-domain tenant PBRv6_ASA_HA_Mode name Internal-BD4
          svcredir-pol tenant PBRv6_ASA_HA_Mode name Internal_leg
          exit
        exit
    connection C1 terminal consumer service N2 connector consumer
    connection C2 terminal provider service N2 connector provider
    exit
```

ステップ 10 外部および内部レッグのサービス リダイレクトのポリシーを作成します。IPv6 アドレスは次の例で使用されます。同じコマンドを使用して IPv4 アドレスを指定することもできます。

例：

```
svcredir-pol Internal_leg
    redir-dest 20:1:1:1::1 00:00:AB:CD:00:11
    exit
svcredir-pol External_leg
    redir-dest 10:1:1:1::1 00:00:AB:CD:00:09
```

```
    exit
exit
```

NX-OS スタイルの CLI を使用したポリシー ベースのリダイレクト設定を確認する

ポリシー ベースのリダイレクトを設定した後は、NX-OS スタイル CLI を使用して設定を確認できます。

ステップ 1 テナントの実行設定を表示します。

例：

```
apic1# show running-config tenant PBRv6_ASA_HA_Mode svcredir-pol
# Command: show running-config tenant PBRv6_ASA_HA_Mode svcredir-pol
# Time: Wed May 25 00:57:22 2016
  tenant PBRv6_ASA_HA_Mode
    svcredir-pol Internal_leg
      redir-dest 20:1:1:1::1/32 00:00:AB:CD:00:11
      exit
    svcredir-pol External_leg
      redir-dest 10:1:1:1::1/32 00:00:AB:CD:00:09
      exit
    exit
```

ステップ 2 テナントとそのサービス グラフの実行設定を表示します。

例：

```
apic1# show running-config tenant PBRv6_ASA_HA_Mode l4l7 graph PBRv6_ASA_HA_Mode_Graph
# Command: show running-config tenant PBRv6_ASA_HA_Mode l4l7 graph PBRv6_ASA_HA_Mode_Graph
# Time: Wed May 25 00:55:09 2016
  tenant PBRv6_ASA_HA_Mode
    l4l7 graph PBRv6_ASA_HA_Mode_Graph contract Contract_PBRv6_ASA_HA_Mode
      service N2 device-cluster-tenant T1 device-cluster ifav-asa-vm-ha mode FW_ROUTED svcredir
enable
        connector consumer cluster-interface consumer_PBRv6

          bridge-domain tenant PBRv6_ASA_HA_Mode name External-BD3

          svcredir-pol tenant PBRv6_ASA_HA_Mode name External_leg

          exit

        connector provider cluster-interface provider_PBRv6

          bridge-domain tenant PBRv6_ASA_HA_Mode name Internal-BD4
          svcredir-pol tenant PBRv6_ASA_HA_Mode name Internal_leg
          exit
        exit
      connection C1 terminal consumer service N2 connector consumer
      connection C2 terminal provider service N2 connector provider
      exit
    exit
```

ステップ 3 サービス グラフ設定を表示します。

例：

```
apic1# show l4l7-graph graph PBRv6_ASA_HA_Mode_Graph
Graph           : PBRv6_ASA_HA_Mode-PBRv6_ASA_HA_Mode_Graph
Graph Instances : 1

Consumer EPg     : PBRv6_ASA_HA_Mode-ClientEPG
Provider EPg     : PBRv6_ASA_HA_Mode-ServerEPG
Contract Name    : PBRv6_ASA_HA_Mode-Contract_PBRv6_ASA_HA_Mode
Config status    : applied
Service Redirect : enabled

Function Node Name : N2
 Connector   Encap       Bridge-Domain  Device Interface      Service Redirect Policy
 ----------  ----------  ----------     --------------------  -----------------------
 consumer    vlan-241    PBRv6_ASA_HA_  consumer_PBRv6        External_leg
                         Mode-
                         External-BD3
 provider    vlan-105    PBRv6_ASA_HA_  provider_PBRv6        Internal_leg
                         Mode-
                         Internal-BD4
```

ポリシー ベースのリダイレクトとサービス ノードのトラッキング

（注） この機能は、APIC リリース 2.2(3x) リリースおよび APIC リリース 3.1 (1) でさせてで使用できます。APIC Release 3.0(x) ではサポートされていません。

Cisco APIC、リリース 2.2(3x) とポリシー ベースのリダイレクトとサービス ノードの追跡 (PBR) のサポートが機能します。

宛先ノードのサポート デュアル IP スタックをリダイレクトします。したがって、IPv4 と IPv6 の両方のアドレスは、同時に設定できます。

スイッチは、トラッキング PBR をサポートするのに Cisco IP SLA モニタリング機能を内部的に使用します。トラッキング機能では、サービス ノードに到達できない場合に、リダイレクト宛先ノードがマークされます。トラッキング機能は、サービス ノードの接続を再開するかどうかリダイレクト宛先ノードを示します。サービス ノードがマークダウンときに送信または、トラフィックのハッシュを使用できません。代わりに、トラフィックを送信またはリダイレクト宛先ノードのクラスタ内の異なるサービス ノードにハッシュがされます。

一方向のトラフィックのブラック holing を避けるためには、リダイレクト正常性ポリシー サービス ノードの入力と出力をリダイレクト宛先ノードを関連付けることができます。これによりを入力または出力のいずれかのリダイレクト宛先ノードがダウンしている場合、その他のリダイレクト宛先ノードもマークダウンされます。したがって、入力と出力トラフィックの両方のは、リダイレクト宛先ノードのクラスタ内の異なるサービス ノードにハッシュを取得します。

しきい値設定

サービス ノードを追跡するため PBR ポリシーを設定するとき、次のしきい値の設定を使用できます。

- しきい値の有効化または無効化：しきい値が有効になっているとき、最小および最大のしきい値のパーセンテージを指定します。リダイレクト先グループを完全に無効にして、リダイレクトを防止したい場合は、有効になっているしきい値は必須です。リダイレクトがないときに、トラフィックがコンシューマとプロバイダ間で直接送信されます。
- 最小しきい値：指定した最小しきい値のパーセンテージ。トラフィックが最小パーセンテージを下回る場合、リダイレクトではなくパケットが許可されます。デフォルト値は 0 です
- 最大しきい値：指定された最大しきい値のパーセンテージ。最小しきい値に達すると、操作状態に戻すため最大パーセンテージに最初に到達する必要があります。デフォルト値は 0 です

例として、ポリシーに 3 つのリダイレクト先があると仮定してみましょう。最小しきい値が 70% に指定されており、最大しきい値が 80% に指定されています。3 つのリダイレクト先ポリシーのいずれかがダウンすると、 1/3、つまり最小しきい値以下の 33% 可用性パーセンテージが下がります。その結果、リダイレクト先グループの最小しきい値のパーセンテージがダウンし、トラフィックがリダイレクトではなく許可の取得を開始します。同じ例で続けると、最大しきい値が 80% の場合、リダイレクト ポリシー先グループを操作状態に戻すため、最大しきい値のパーセンテージ以上のパーセンテージに最初に達する必要があります。

ポリシー ベース リダイレクトとトラッキング サービス ノードについての注意事項と制約事項

PBR トラッキングおよびサービス ノードを利用するときに、これらの注意事項と制約事項に従います。

- リリース 4.0(1) 以降では、システムレベルのグローバル GIPo が有効になっている場合に限り、リモート リーフ設定で PBR トラッキングがサポートされます。「*GUI* を使用してリモート リーフのグローバル *GIPo* を構成する」を参照してください。
- リリース 4.0(1) 以降では、リモート リーフ設定で PBR の復元力のあるハッシュがサポートされています。
- マルチポッド ファブリック設定はサポートされています。マルチサイト セットアップはサポートされていません。
- コンシューマとプロバイダ Epg のレイヤ 3 Out はサポートされます。
- リダイレクト宛先ノードの追跡では、TCP または ICMP プロトコル タイプが使用されます。

- ポリシー ベース リダイレクトでサポートされる追跡可能 IP アドレスの最大数は、リーフ スイッチで 100、ACI ファブリックでは 200 です。
- ACI ファブリックでのグラフ インスタンスの最大数は、ファブリックあたり 1000 です。
- グラフ インスタンスの最大数は、デバイスあたり 100 です。
- PBR を設定できるサービス ノードの最大数は、ポリシーあたり 40 です。
- 1 つのサービス チェーンでサポートされるサービス ノードの最大数は 3 です。
- PBR トラッキングでは、共有サービスがサポートされています。
- 許可アクションまたは拒否アクションはサポートされています。

PBR を設定し、GUI を使用してサービス ノードのトラッキング

ステップ 1 メニュー バーで [Tenant] > **テナント名**をクリックします。[Navigation] ペインで、[Policies] > [Protocol] > [L4-L7 Policy Based Redirect] をクリックします。

ステップ 2 右クリックして **L4 ~ L7 ポリシー ベースのリダイレクト** をクリックします **作成 L4 ~ L7 ポリシー ベースのリダイレクト** 。

ステップ 3 **Create L4–L7 Policy Based Redirect** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに PBR ポリシーの名前を入力します。

b) ダイアログボックスでは、ハッシュ アルゴリズムの、IP SLA モニタリング ポリシー、およびその他の必要な値を設定する適切な設定を選択します。

c) しきい値の設定フィールドでは、必要に応じて設定を指定し、必要な場合。

d) [Destinations] を展開して [Create Destination of Redirected Traffic] を表示します。

e) **リダイレクト トラフィックの宛先の作成** ダイアログボックスなどの適切な詳細を入力します **IP** アドレス、および **MAC アドレス** フィールド。

IP アドレスおよび 2 番目の IP アドレス（IPv4 アドレス/IPv6 アドレス）を指定できるフィールドが表示されます。

（注） このフィールドは必須ではありません。L4-L7 デバイスに複数の IP アドレスがあり、ACI でそれらの両方を確認する必要がある場合に使用します。

[IP] と [Second IP] の両方のパラメータを設定した場合、PBR 宛先が「UP」とマーキングされるには、両方がアップ状態である必要があります。

f) **ヘルス グループのリダイレクト** フィールドで、既存のヘルス グループに関連付けるまたは必要に応じて、新しいヘルス グループを作成します。[OK] をクリックします。

g) **Create L4–L7 Policy Based Redirect** ダイアログボックスで **Submit** をクリックします。

L4 L7 ポリシー ベースのリダイレクトとサービス ノードのトラッキング L4 L7 PBR ポリシーおよびリダイレクト宛先グループを追跡するための設定にリダイレクト ヘルス グループ ポリシーが有効になっているバインディングの後に設定されます。

GUI を使用したインポート ポリシーの設定

ステップ 1 メニュー バーで、**Tenant** > **Tenant_name** をクリックします。**Navigation** ウィンドウで、**Networking** > **Protocol Policies** > **L4-L7 Redirect Health Groups** をクリックします。

ステップ 2 **L4 –L7 Redirect Health Groups** を右クリックし、**Create L4–L7 Redirect Health Group** をクリックします。

ステップ 3 **Create L4–L7 Redirect Health Group** ダイアログボックスで、次の操作を実行します。

a) **Name** フィールドに、 リダイレクト正常性ポリシーの名前を入力します。

b) 適切であれば、**Description** フィールドに追加の情報を入力し、**Submit** をクリックします。

L4 ～ L7 リダイレクト正常性ポリシーが設定されます。

GUI を使用した IP SLA モニタリング ポリシーの設定

ステップ 1 メニューバーで、**Tenant**>**Tenant_name** をクリックします。**Navigation** ウィンドウで、**Policies**>**Protocol**>**IP SLA Monitoring Policies** をクリックします。

ステップ 2 **IP SLA Monitoring Policies** を右クリックして、**Create IP SLA Monitoring Policy** をクリックします。

ステップ 3 **Create IP SLA Monitoring Policy** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、 IP SLA モニタリング ポリシーの名前を入力します。

b) **SLA Frequency** フィールドに、インターバル プローブ時間を秒単位で入力します。最小のインターバル時間は 1 秒です。

c) **SLA Type** フィールドで、SLAタイプを選択します。[Submit] をクリックします。

（注） 現在のところ、**SLA Type** としては、tcp だけがサポートされています。

SLA タイプとしては TCP または ICMP が可能です。ICMP がデフォルト値です。

これで IP SLA モニタリング ポリシーが設定されます。

GUI を使用してリモート リーフのグローバル GIPo を構成する

このタスクを実行すると、リモート リーフ設定で PBR トラッキングを機能させることができます。

（注） リモート リーフで PBR トラッキングを機能させるには、この設定を行う必要があります。この設定を行わないと、メイン データセンターが到達可能でも、リモート リーフで PBR トラッキングは機能しません。

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。

ステップ 2 [System Settings] ナビゲーション ウィンドウで [System Global GIPo] をクリックします。

ステップ 3 [System Global GIPo Policy] 作業ウィンドウで [Enabled] をクリックします。

ステップ 4 [Policy Usage Warning] ダイアログで、GIPo ポリシーを使用する可能性があるノードとポリシーを確認し、必要に応じて [Submit Changes] をクリックします。

REST API を使用したサービス ノードのトラッキングのサポートをする PBR の設定

トラッキング サービス ノードをサポートする PBR を設定します。

例：

```
<polUni>
    <fvTenant name="coke" >
    <fvIPSLAMonitoringPol name="tcp_Freq60_Pol1" slaType="tcp" slaFrequency="60" slaPort="2222" />
    <vnsSvcCont>
        <vnsRedirectHealthGroup name="fwService1"/>
          <vnsSvcRedirectPol name="fwExt" hashingAlgorithm="sip" thresholdEnable="yes"
minThresholdPercent="20" maxThresholdPercent="80">
            <vnsRedirectDest ip="40.40.40.100" mac="00:00:00:00:00:01">
              <vnsRsRedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-fwService1"/>

            </vnsRedirectDest>
            <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-tcp_Freq60_Pol1"/>
          </vnsSvcRedirectPol>
         <vnsSvcRedirectPol name="fwInt" hashingAlgorithm="sip" thresholdEnable="yes"
minThresholdPercent="20" maxThresholdPercent="80">
            <vnsRedirectDest ip="30.30.30.100" mac="00:00:00:00:00:02">
              <vnsRsRedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-fwService1"/>

            </vnsRedirectDest>
            <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-tcp_Freq60_Pol1"/>
          </vnsSvcRedirectPol>
        </vnsSvcCont>
    </fvTenant>
</polUni>
```

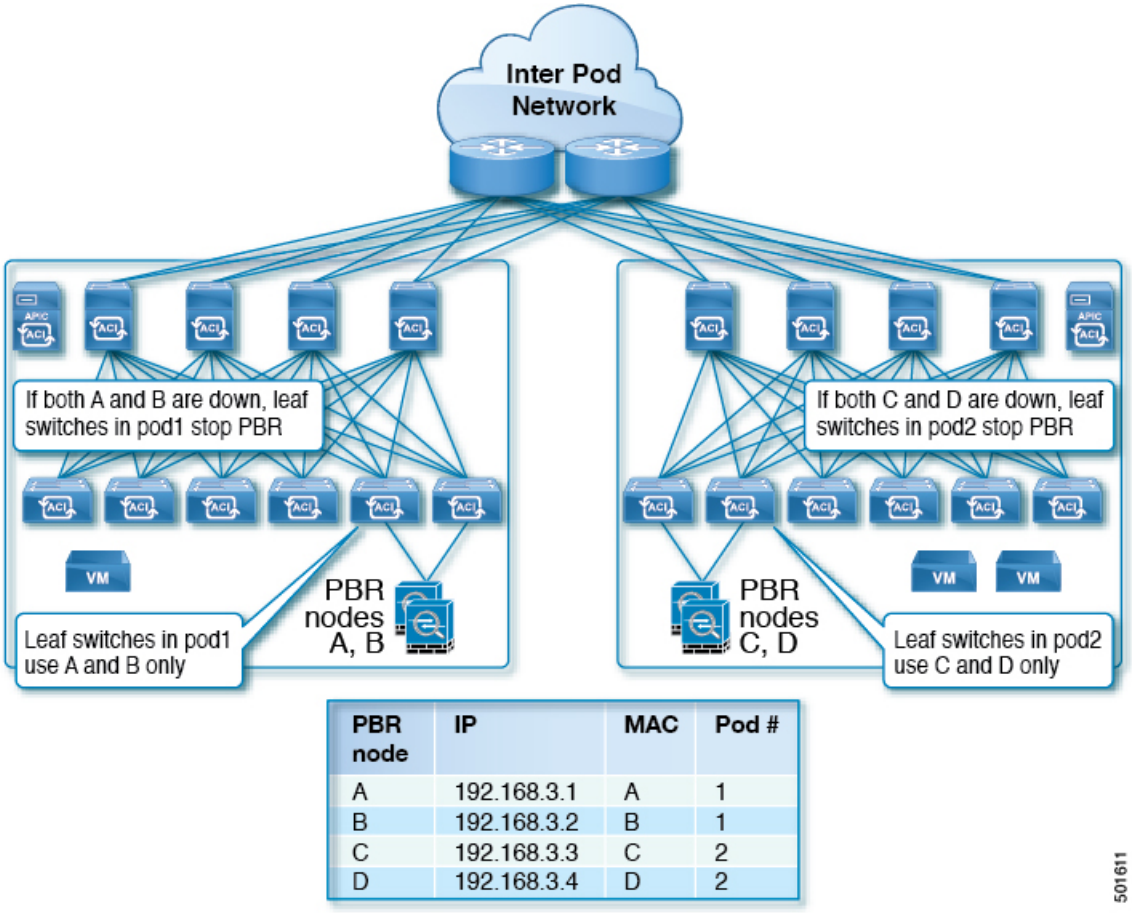
ベースリダイレクトの場所に対応したポリシーについて

ロケーション対応ポリシー ベースのリダイレクト (PBR) はサポートされています。この機能は、multipod 設定シナリオに役立ちます。ここでは、ポッド認識サポートされ、優先ローカル PBR ノードを指定できます。ロケーション対応のリダイレクトを有効にすると、ポッド Id が指定されて、レイヤ 4 ~ レイヤ 7 PBR ポリシー内のすべてのリダイレクト宛先はポッド認識必

要があります。リダイレクト宛先は、特定のポッドにあるリーフ スイッチでのみプログラムされます。

次の図は、2 個のポッドの例を表示します。ポッド 1 で PBR ノード A と B、C と D PBR ノードがポッド 2 では。ポッド 1 のリーフ スイッチが A、B、PBR ノードを使用する prefer し、ポッド 2 のリーフ スイッチ C と D で PBR ノードの使用場所に対応した PBR 設定を有効にするとPBR ノード A と B ポッド 1 では、ダウンは、[ポッド 1 のリーフ スイッチと開始 PBR ノード C と D を使用するには同様に、PBR ノード C と D ポッド 2 では、ダウンが、ポッド 2 のリーフ スイッチと開始 PBR ノード A および B を使用するには

図 *10 : 2* 個のポッドのロケーション対応 *PBR* 設定の例



PBR node	IP	MAC	Pod #
A	192.168.3.1	A	1
B	192.168.3.2	B	1
C	192.168.3.3	C	2
D	192.168.3.4	D	2

ロケーション認識型 PBR の注意事項

ロケーション認識型 PBR を活用する際はこれらの注意事項に従ってください。

- Cisco Nexus 9300（Cisco Nexus 9300 EX および 9300 FX を除く）プラットフォーム スイッチは、ロケーション認識型 PBR 機能をサポートしていません。
- GOLF ホスト アドバタイズメントと北南ファイアウォール連携にロケーション認識型 PBR を使用します。

GUI を使用したロケーション認識型 PBR の設定

この機能を有効にするための 2 つの項目をプログラムする必要があります。ポッド ID 認識リダイレクトを有効にし、特定のポッドにあるリーフ スイッチで、リダイレクト宛先をプログラムして、優先 PBR ノードにポッド ID を関連付けます。

ステップ 1 メニュー バーで [Tenant] > **テナント名**をクリックします。[Navigation] ペインで、[Policies] > [Protocol] > [L4-L7 Policy Based Redirect] をクリックします。

ステップ 2 右クリックして **L4 ~ L7 ポリシー ベースのリダイレクト** をクリックします **作成 L4 ~ L7 ポリシー ベースのリダイレクト** 。

ステップ 3 **Create L4–L7 Policy Based Redirect** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに PBR ポリシーの名前を入力します。

b) **[ポッド ID 認識リダイレクトの有効化]** チェック ボックスをオンにします。

c) ダイアログ ボックスでハッシュ アルゴリズム、IP SLA モニタリング ポリシー、およびその他の必要な値を構成するため、適切な設定を選択します。

d) しきい値の設定フィールドでは、必要に応じて設定を指定し、必要な場合。

e) [Destinations] を展開して [Create Destination of Redirected Traffic] を表示します。

f) **リダイレクト トラフィックの宛先の作成** ダイアログボックスなどの適切な詳細を入力します **IP** アドレス、および **MAC アドレス** フィールド。

IP アドレスと 2 番目の IP アドレスのフィールドでは、IPv4 アドレスと IPv6 あれドレスを指定できます。

g) **[ポッド ID]** フィールドに、ポッド ID 値を入力します。

h) **[リダイレクト ヘルス グループ]** フィールドで、既存のヘルス グループに関連付けるか、適切であれば、新しいヘルス グループを作成します。[OK] をクリックします。

必要に応じて別のポッド ID にリダイレクトされたトラフィックの他の宛先を作成します。

i) **Create L4–L7 Policy Based Redirect** ダイアログボックスで **Submit** をクリックします。

L4-L7 ロケーション認識型 PBR が設定されています。

REST API を使用して設定の場所に対応した PBR

2 つ設定する必要があります項目の場所に対応した PBR を有効にして、プログラムが特定のポッドにあるリーフ スイッチ内の送信先をリダイレクトします。次の例の場所に対応した PBR を有効にするよう設定されている属性が: programLocalPodOnly と podId 。

ロケーション対応 PBR を設定します。

例：

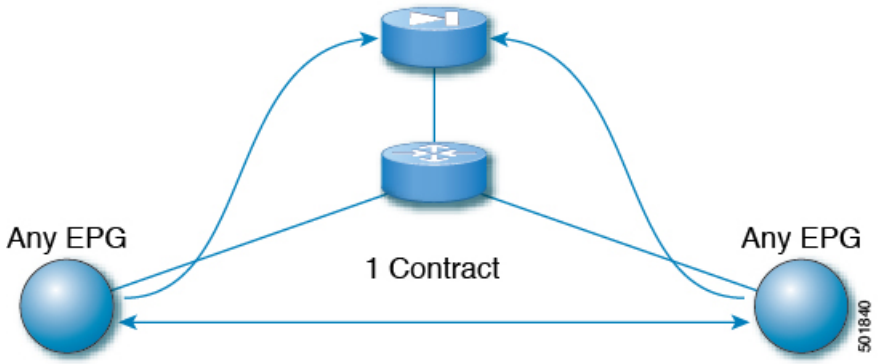
```
<polUni>
```

```
    <fvTenant name="coke" >
    <fvIPSLAMonitoringPol name="icmp_Freq60_Pol1" slaType="icmp" slaFrequency="60"/>
    <vnsSvcCont>
        <vnsRedirectHealthGroup name="fwService1"/>
          <vnsSvcRedirectPol name="fwExt" hashingAlgorithm="sip" thresholdEnable="yes"
minThresholdPercent="20" maxThresholdPercent="80" programLocalPodOnly="yes">
            <vnsRedirectDest ip="40.40.40.100" mac="00:00:00:00:00:01" podId="2">
              <vnsRsRedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-fwService1"/>

            </vnsRedirectDest>
            <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-icmp_Freq60_Pol1"/>
          </vnsSvcRedirectPol>
          <vnsSvcRedirectPol name="fwInt" hashingAlgorithm="dip" thresholdEnable="yes"
minThresholdPercent="20" maxThresholdPercent="80">
            <vnsRedirectDest ip="30.30.30.100" mac="00:00:00:00:00:02">
              <vnsRsRedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-fwService1"/>

            </vnsRedirectDest>
            <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-icmp_Freq60_Pol1"/>
          </vnsSvcRedirectPol>
        </vnsSvcCont>
    </fvTenant>
</polUni>
```

同じVRFインスタンス内のすべてのEPG-EPGにトラフィックをリダイレクトするには、ポリシーベースのリダイレクトとサービス グラフ

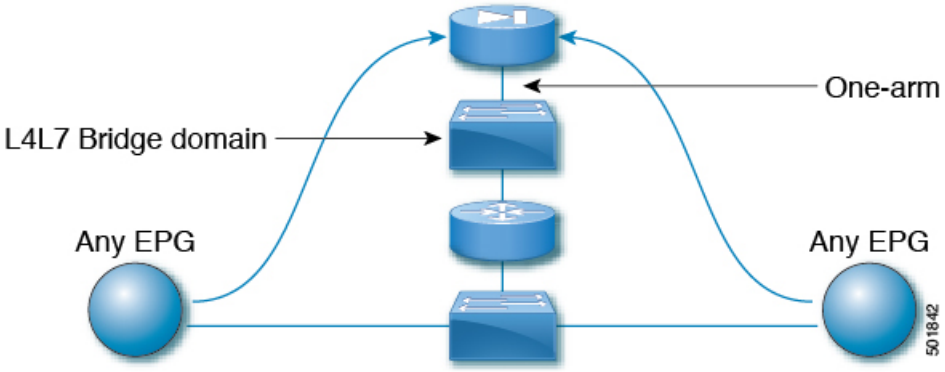
設定できる Cisco Application Centric Infrastructure (Cisco ACI) サービス グラフ リダイレクト vzAny と vzAny の設定によって、デバイスはすべてのエンドポイントを表す構築をレイヤ 7 にレイヤ 4 で同じ:VRF インスタンス内の他のエンドポイント グループをすべてのエンドポイント グループからのすべてのトラフィックを転送するには。同じVRFインスタンスでグループ。vzAny は「any EPG」と呼ばれることがあります。

図 *11 : vzAny* トポロジ



同じ VRF インスタンスの下にある任意のエンドポイント グループ ペア間のトラフィックは、ファイアウォールなどのレイヤ 4 からレイヤ 7 デバイスにリダイレクトできます。また、同じブリッジ ドメイン内のトラフィックをファイアウォールにリダイレクトすることもできます。ファイアウォールは、次の図に示すように、任意の一対のエンドポイント グループ間のトラフィックをフィルタリングできます。

図 *12*：任意の *EPG* ペア間のトラフィックをフィルタリングするファイアウォール

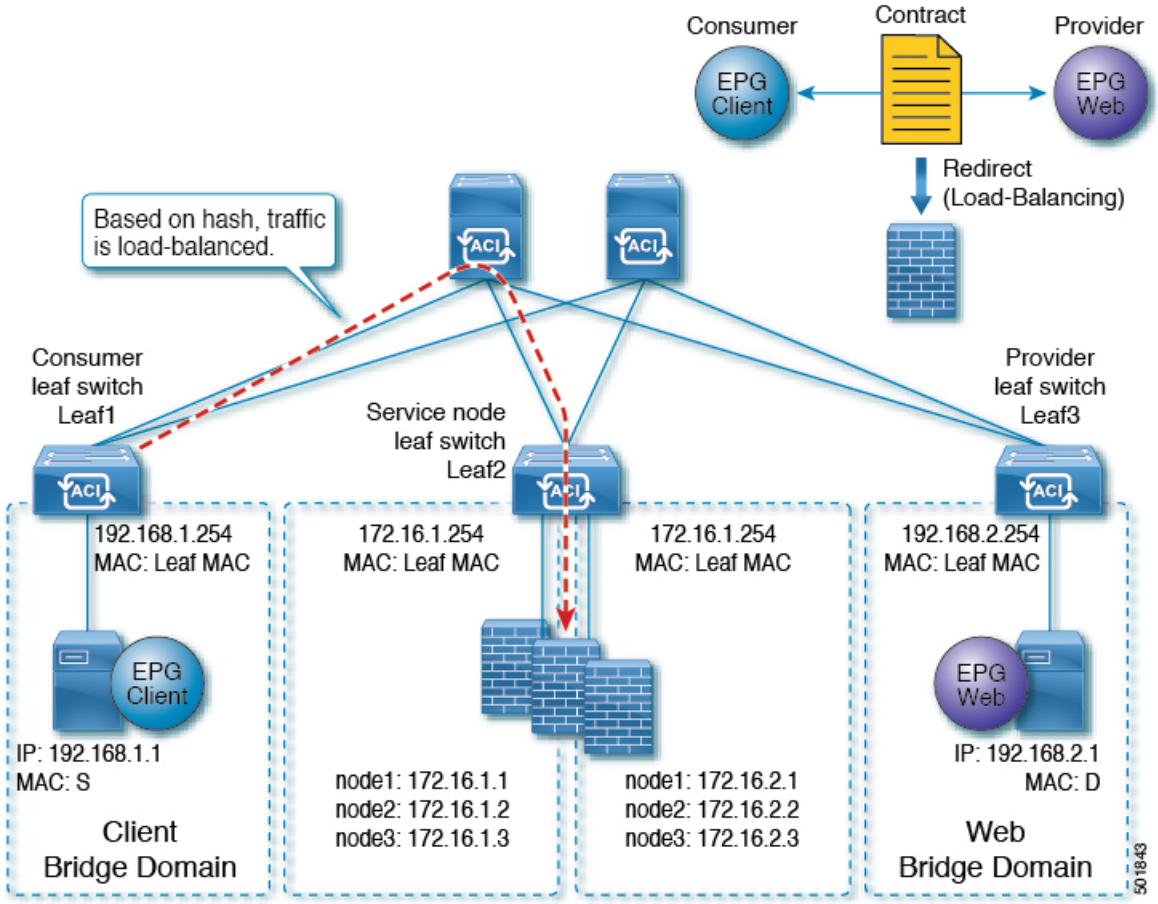


この機能の 1 つの使用例は、Cisco ACI をデフォルト ゲートウェイとして使用することですが、ファイアウォールを通るトラフィックをフィルタリングすることもそうです。vzAny とポリシー ベースのリダイレクト ポリシーにより、セキュリティ管理者は ACL ルールを管理し、ネットワーク管理者はルーティングとスイッチングを管理します。この設定の利点には、エンドポイント トラッキング、ARP インスペクションによるファースト ホップ セキュリティ、IP アドレス ソース ガードなどの Cisco Application Policy Infrastructure Controller (Cisco APIC) ツールを使用できることが含まれます。

ポリシー ベースのリダイレクト ポリシーを使用してサービス グラフを適用すると、次の機能も有効になります。

- ファイアウォール クラスタリング
- ファイアウォールの健全性追跡
- 位置認識リダイレクション

図 *13* : ファイアウォール クラスタリング



Cisco APIC 3.2 のリリースより前に、vzAny を契約のコンシューマとして使用することができました。Cisco APIC 3.2 のリリースから、vzAny を契約のプロバイダとして使用することもできます。この拡張により、以下の構成が可能になります。

- プロバイダとしての vzAny、コンシューマとしての vzAny (ワンアームのみのポリシーベースのリダイレクト)
- プロバイダとしての vzAny、およびコンシューマとしての通常のエンドポイント グループ (ポリシーベースのリダイレクトおよび非ポリシーベースのリダイレクトの場合)

vzAny を使用してトラフィックをリダイレクトするポリシー ベースのリダイレクト ポリシーを使用してサービス グラフを適用した後、2 つのサーバ間のデータ バックアップ トラフィックなどのトラフィックがファイアウォールをバイパスするようにする場合には、エンドポイント グループ間でより具体的な契約を作成することができます。たとえば、2 つのエンドポイント グループは、特定のポート上でトラフィックを相互に直接送信できます。より具体的なルールは、「任意のEPGから任意のEPGへ」リダイレクト ルールに優先します。

同じ VRF インターフェイス内のすべての EPG 間トラフィックをリダイレクトするために、ポリシーベースのリダイレクトポリシーをサービス グラフとともに設定する際の注意事項と制約事項

次の注意事項と制約事項は、同じ VRF インターフェイス内のすべての EPG 間トラフィックをリダイレクトするために、ポリシーベースのリダイレクト ポリシーをサービス グラフとともに設定する際に適用されます。

- レイヤ 4 ～ 7 デバイスと vzAny は、同じ VRF インスタンスに属している必要があります。
- レイヤ 4 ～ 7 デバイスはワンアーム モードで展開する必要があります。
- 複数ノードのサービス グラフで設定された vzAny も機能する可能性はありますが、この設定は試験されておらず、サポートされません。自身のリスクにおいて使用してください。
- レイヤ 4 ～ 7 デバイスは、アンマネージド モードでのみ展開できます。
- VRF リーキングと組み合わせた使用は、実装されていません。VRF インスタンスの vzAny に、他の VRF インスタンスの vzAny の契約の提供または利用を行わせることはできません。
- 異なるテナントのエンドポイント グループと vzAny の間で契約を設定することは、 VRF インスタンスがテナント **Common** にある場合のように、同じ VRF に属している限りにおいて可能です。
- マルチポッド環境では、 vzAny をプロバイダおよびコンシューマとして使用できます。
- Cisco ACI マルチサイト環境では、vzAny をサイト間でのプロバイダおよびコンシューマとして使用することはできません。

同じ VRF インターフェイス内のすべての EPG 間トラフィックをリダイレクトするために、ポリシーベースのリダイレクトポリシーをサービス グラフとともに設定する

次の手順では、同じ VRF インスタンス内のすべての EPG-EPG にトラフィックをリダイレクトするサービス グラフでポリシー ベースのリダイレクト ポリシーで設定します。

ステップ 1 レイヤ 4 レイヤ 7 デバイスへの接続を割り当てるはサービス ブリッジ ドメインを作成します。

ブリッジ ドメインの作成については、*Cisco APIC* ベーシック コンフィギュレーション ガイド を参照してください。

ステップ 1 > メイン 画面。

a) **VRF** ドロップダウンリスト、エンドポイントのグループが含まれている:VRF インスタンスを選択します。
b) **転送** ドロップダウンリスト、選択した場合 **カスタム** 、次に、 **L2 不明なユニキャスト** ドロップダウンリストを選択できます **フラッド** 必要かどうか。

ステップ 2 > L3 設定 画面。

a) チェックがあることを確認します **ユニキャスト ルーティング** チェック ボックス。
b) **サブネット** テーブルで、サブネットを作成します。

ゲートウェイ IP アドレスは、レイヤ 7 デバイス インターフェイスをレイヤ 4 に与えるは IP アドレスと同じサブネット内にする必要があります。

c) チェックを外し、 **エンドポイント データ ラーニング** チェック ボックス。

ステップ 2 リダイレクト ポリシーを作成します。

a) **[Navigation]** ウィンドウで、**[Tenanttenant_name] > [Networking] > [Policies] > [Protocol] > [L4-L7 Policy Based Redirect]** を選択します。
b) 右クリックして **L4 L7 ポリシー ベースのリダイレクト**] を選択します **作成 L4 L7 ポリシー ベースのリダイレクト** 。
c) [Name] フィールドにポリシーの名前を入力します。
d) **宛先** テーブルで、をクリックして + 。
e) **リダイレクト トラフィックの宛先の作成** ダイアログ ボックスで、次の情報を入力します。

- **IP** : IP アドレスを入力レイヤ 7 デバイスにレイヤ 4 に割り当てるされます。ブリッジ ドメインに支えられている IP アドレスと同じサブネットの IP アドレスがあります。
- **MAC** : レイヤ 7 デバイスにレイヤ 4 に割り当てるが MAC アドレスを入力します。レイヤ 7 デバイスにレイヤ 4 のフェールオーバー時にも有効な MAC アドレスを使用する必要があります。たとえば、ASA ファイアウォール時これと呼ばれる、「仮想 mac です。」

f) その他の適切な値を入力し、クリックして **OK** 。
g) **作成 L4 L7 ポリシー ベースのリダイレクト** ダイアログ ボックスで、他の適切な値を入力し、クリックして **Submit** 。

ステップ 3 1 つの具体的なインターフェイスを 1 つの論理インターフェイス レイヤ 7 デバイスにレイヤ 4 を作成します。

レイヤ 7 デバイスにレイヤ 4 の作成についてを参照してください。 GUI を使用したレイヤ 4 ～ レイヤ 7 デバイスの作成 。

ステップ 4 ルート リダイレクトを有効になっていると、サービス グラフ テンプレートを作成します。

a) **Navigation** ウィンドウで、**Tenant tenant_name > Services > L4-L7 > Service Graph Template** を選択します。
b) 右クリックして **サービス グラフ テンプレート**] を選択します **サービス グラフ テンプレートの作成** します。
c) **Name** フィールドに、サービス グラフの名前を入力します。
d) 以前を作成していないレイヤ 7 デバイスにレイヤ 4 の場合、 **デバイス クラスタ**] ペインで、デバイスを作成します。

e) ドラッグ アンド ドロップ レイヤ 4 からレイヤ 7 デバイス、 **デバイス クラスタ** され、中間 EPG コンシューマとプロバイダー EPG にウィンドウ。
f) **L4L7** ラジオ ボタンをクリックします **ルーテッド** 。
g) チェック マークを残します、 **リダイレクト ルーティング** チェック ボックス。
h) [Submit] をクリックします。

ステップ 5 サービス グラフ vzAny (AnyEPG) エンドポイント グループに適用されます。

ステップ 1 > 契約 画面。

a) **Navigation** ウィンドウで、**Tenant tenant_name** > **Services** > **L4-L7** > **Service Graph Template** > ***service_graph_name*** を選択します。

service_graph_name は、作成したサービス グラフ テンプレートです。

b) サービス グラフ テンプレートを右クリックし、選択 **L4 L7 サービス グラフ テンプレートの適用** 。
c) **コンシューマ EPG/外部ネットワーク** ドロップダウンリスト、選択、 **AnyEPG** テナントに対応するリスト項目とのこれを使用する VRF インスタンス使用例。

たとえば、テナントは、「tenant1」:VRF インスタンスは「vrf1」で、選択 **tenant1/vrf1/AnyEPG** .

d) **プロバイダー EPG 内部ネットワーク/** ドロップダウンリスト、同じ選択 **AnyEPG** コンシューマ EPG 用に選択したリスト項目。
e) **Contract Name** フィールドに、契約の名前を入力します。
f) [Next] をクリックします。

ステップ 2 > グラフ 画面。

a) 両方の **BD**] ドロップダウン リスト、ステップ 1 で作成したレイヤ 7 サービス ブリッジ ドメインをレイヤ 4 を選択します。
b) 両方の **リダイレクト ポリシー**] ドロップ ダウン リストでは、この使用例用に作成したリダイレクト ポリシーを選択します。
c) コンシューマ コネクタの **クラスタ インターフェイス** ドロップダウンリスト、ステップ 3 で作成したクラスタ インターフェイス (論理インターフェイス) を選択します。
d) プロバイダー コネクタの **クラスタ インターフェイス** ドロップダウンリスト、ステップ 3 で作成した同じクラスタ インターフェイス (論理インターフェイス) を選択します。
e) [Finish] をクリックします。