



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 \(1 ページ\)](#)
- [複数ノード ポリシー ベースのリダイレクトについて \(18 ページ\)](#)
- [対称ポリシー ベースのリダイレクトについて \(18 ページ\)](#)
- [重みベースの対称ポリシーベースのリダイレクトについて \(19 ページ\)](#)
- [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 \(21 ページ\)](#)
- [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 \(21 ページ\)](#)
- [PBR バックアップポリシーについて \(24 ページ\)](#)
- [バイパスアクションについて \(28 ページ\)](#)
- [L3Out によるポリシーベースリダイレクト \(32 ページ\)](#)
- [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 \(42 ページ\)](#)
- [レイヤ 1/レイヤ 2 ポリシーベースリダイレクトについて \(42 ページ\)](#)
- [ポリシーベースリダイレクトとサービスノードのトラッキング \(53 ページ\)](#)
- [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 \(59 ページ\)](#)
- [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 \(62 ページ\)](#)
- [レイヤ 3 ポリシーベースリダイレクト先の動的 MAC アドレス検出 \(68 ページ\)](#)

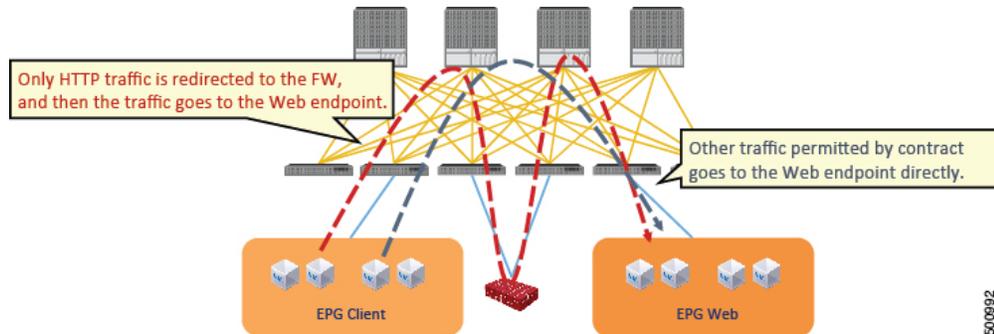
ポリシーベースのリダイレクトについて

Cisco Application Centric Infrastructure (ACI) ポリシーベースリダイレクト (PBR) により、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、また容易にスケールアップすることができ、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:

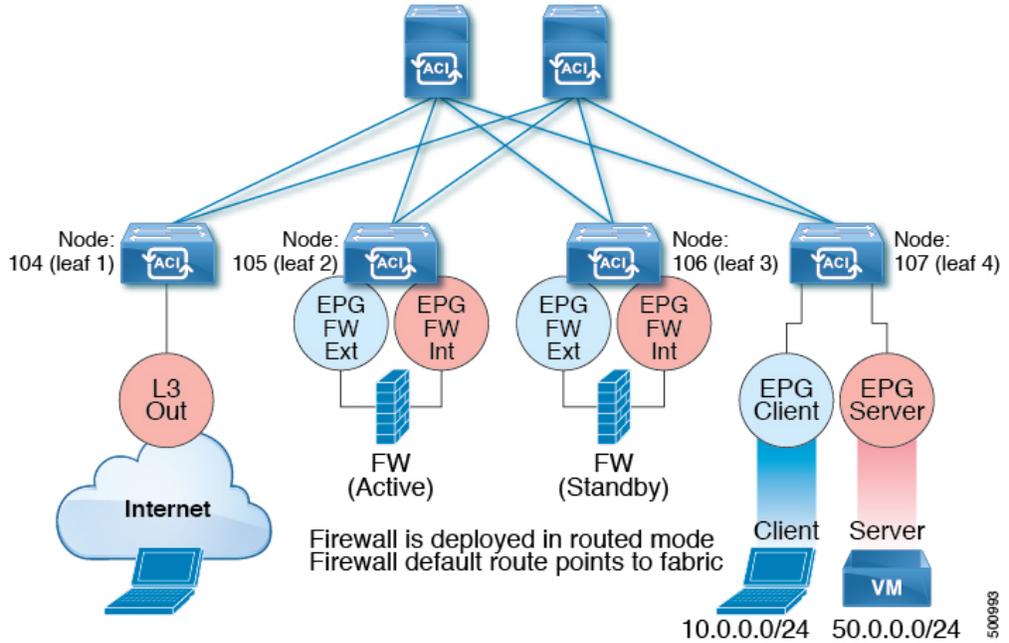
図 1: 使用例: ファイアウォール特有のトラフィックのリダイレクト



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。

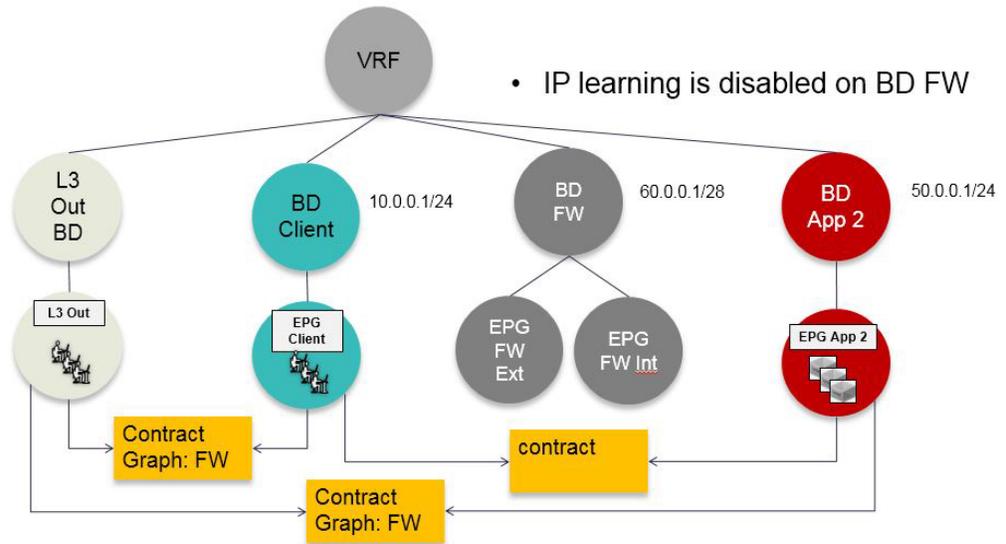
次の図は、ACI PBR 物理トポロジのサンプルを示しています:

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。

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

ポリシーベースリダイレクト(PBR)サービスノードを計画するときは、次の注意事項と制限事項に従ってください。

- ファブリック内の PBR でパケットをルーティングする必要があるため、パケットの送信元 MAC アドレスが書き換えられる可能性があります。IP アドレスヘッダーの存続可能時間(TTL)フィールドは、ファブリック内でパケットがルーティングされる回数だけ減少します。
- 両方のサービスレッグに同じアクションを選択します。つまり、内部サービスレッグの拒否アクションを選択した場合は、外部サービスレッグの拒否アクションも選択する必要があります。
- L3Out EPG と通常の EPG は、コンシューマー EPG またはプロバイダー EPG にできます。
- L2Out EPG は、コンシューマー EPG またはプロバイダー EPG にすることはできません。
- 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 アドレスを指定する必要があります。
- 5.2(1) より前のリリースでは、仮想 MAC アドレスを指定する必要があります。5.2(1) 以降のリリースでは、オプションで仮想 MAC アドレスを提供せず、代わりに Cisco Application Policy Infrastructure Controller (Cisco APIC) にアドレスを動的に検出できます。
- 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 APIC 3.1(1) 以降のリリースでは、サービスアプライアンスを別のブリッジドメインにプロビジョニングすることは必須ではありません。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 からダウングレードする場合、ポリシーベースのリダイレクトブリッジドメインが同じブリッジドメインをコンシューマーまたはプロバイダーとして使用しているかどうかを内部コードで確認します。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。
- 5.2(1) 以降のリリースから 5.2(1) より前のリリースにダウングレードする場合は、5.2 リリースからの PBR 関連の機能を含むすべての PBR 関連の設定を削除し、関連するサービスグラフを削除する必要があります。次に例を示します。
 - L3Out で PBR 接続先を使用するデバイス選択ポリシーを削除します。
 - 拡張 LAG ポリシーを使用するレイヤ 4 ~ レイヤ 7 サービスデバイスを削除します。
 - HTTP SLA タイプを使用する IP SLA モニタリングポリシーを削除します。
 - 接続先 MAC アドレスが設定されていない PBR 接続先を削除します。

- サービスアプライアンス、ソース、ブリッジドメインは、同じ VRF インスタンスに配置できます。
- 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。
- PBR ノードインターフェイスは、FEX ホストインターフェイスではサポートされていません。PBR ノードインターフェイスは、FEX ホストインターフェイスではなく、リーフダウンリンクインターフェイスの下に接続する必要があります。コンシューマーとプロバイダーのエンドポイントは、FEX ホストインターフェイスで接続できます。
- サービスアプライアンスは、ブリッジドメインにのみ存在できます。
- サービスアプライアンスのプロバイダー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) 以降のリリースでは、Cisco Nexus 9300-EX および 9300-FX プラットフォーム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。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。
- Cisco APIC リリース 4.0(1) 以降のリリースでは、PBR を使用してサービスグラフをコントラクト対象に付加できます。サービスグラフとの EPG 内コントラクトは、EPG 間コントラクトとして同時に使用することはできません。リダイレクトが有効になっているサービスグラフで使用する場合は、EPG 間および EPG 内の通信に別々のコントラクトを使用する必要があります。
- Cisco APIC リリース 4.2(3) 以降のリリースでは、サービスグラフテンプレートでコントラクトからのフィルタ (`filters-from-contract`) オプションが利用可能になり、ソースまたは接続先にコンシューマー EPG クラス ID を含まないゾーニングルールに対して、デフォルトのフィルタの代わりにサービスグラフが付加されているコントラクト対象の特定のフィルタを使用できるようになりました。ソースまたは接続先としてコンシューマー EPG クラス ID を持つゾーニングルールでは、オプションに関係なく特定のフィルタを使用します。
- マルチノードポリシーベースのリダイレクト (マルチノード PBR) :
 - ポリシーベースリダイレクト用に構成できるサービスグラフで最大 5 つの機能ノードをサポートします。

- マルチノード PBR サービスチェーンを使用する場合、すべてのサービスデバイスはローカルリーフスイッチにあるか、リモートリーフスイッチに接続されている必要がありますが、両方に分散することはできません。
 - サポートされるトポロジ：

このトポロジでは、*RL* はリモートリーフスイッチを意味し、*LL* はリモートリーフスイッチの下ではなく、メインロケーションの下にあるローカルリーフスイッチを意味します。

 - *N1(LL)--N2(LL)--N3(LL)* : すべてのデバイスは、メインロケーションとリモートリーフスイッチに分散されていないローカルリーフスイッチに接続されています。
 - *N1(RL)-N2(RL)--N3(RL)* : すべてのデバイスがリモートリーフスイッチに接続されています。
 - サポートされていないトポロジ：
 - *N1(LL)--N2(RL)--N3(LL)* : サービスデバイスは、ローカルリーフスイッチとリモートリーフスイッチに分かれます。
- ロードバランサ向けのマルチノード PBR レイヤ 3 接続先ガイドライン：
 - レイヤ 3 接続先アップグレード : レイヤ 3 接続先 (VIP) パラメータは、アップグレード後にデフォルトで有効になります。特定のサービスノードで PBR ポリシーが設定されていない場合 (3.2(1) より前のリリース)、ノードコネクタはレイヤ 3 の接続先として扱われ、新しい Cisco APIC リリースでも引き続き使用されるため、このことによる問題は発生しません。
 - トラフィックは、必ずしもコンシューマー/プロバイダーのみが接続先であ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の VIP アドレスに送信されます。
 - 逆方向では、SNAT が有効になっている場合、トラフィックはロードバランサの内部レッグに送信されます。
 - 両方向で、論理インターフェイス コンテキストでレイヤ 3 接続先 (VIP) を有効 (チェック) します。
 - 両方向でレイヤ 3 接続先 (VIP) を有効 (チェック) し、内部側で PBR ポリシーを構成することにより、ロードバランサ内部で SNAT から No-SNAT に切り替えられるようにします。
 - SNAT が無効の場合:
 - 逆方向のトラフィックはコンシューマーに送られますが、ロードバランサの内部レッグには送られません (内部レッグで PBR ポリシーを有効にします)。

- この場合は PBR ポリシーが適用されるため、レイヤ 3 接続先 (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。
- 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。
- PBR を使用する EPG 内または外部内の EPG コントラクトは、EPG 間コントラクトには使用できません。
- 非 PBR EPG から PBR EPG にエンドポイントを移行する場合、接続先リーフスイッチのリモートエンドポイントは、古い非 PBR EPG の `sclass` の詳細を持つリモートエンドポイントをクリアしません。この問題は、リモートエンドポイントを持つ接続先リーフスイッチが、製品 ID に `-EX`、`-FX`、または `-GX` サフィックスが付いているスイッチの場合に発生します。この問題は、製品 ID に `-FX2`、`-GX2`、またはそれ以降のサフィックスが付いているスイッチでは発生しません。

この問題が発生した場合、次の CLI コマンドを使用して、リモートエンドポイントを手動でクリアできます。

```
vsh -c "clear system internal epm endpoint key vrf vrf_name ip ip_name"
```

- サポートされているポリシーベースのリダイレクト設定には、次のものがあります。

図 4: 同じ VRF インスタンスのポリシーベースリダイレクト

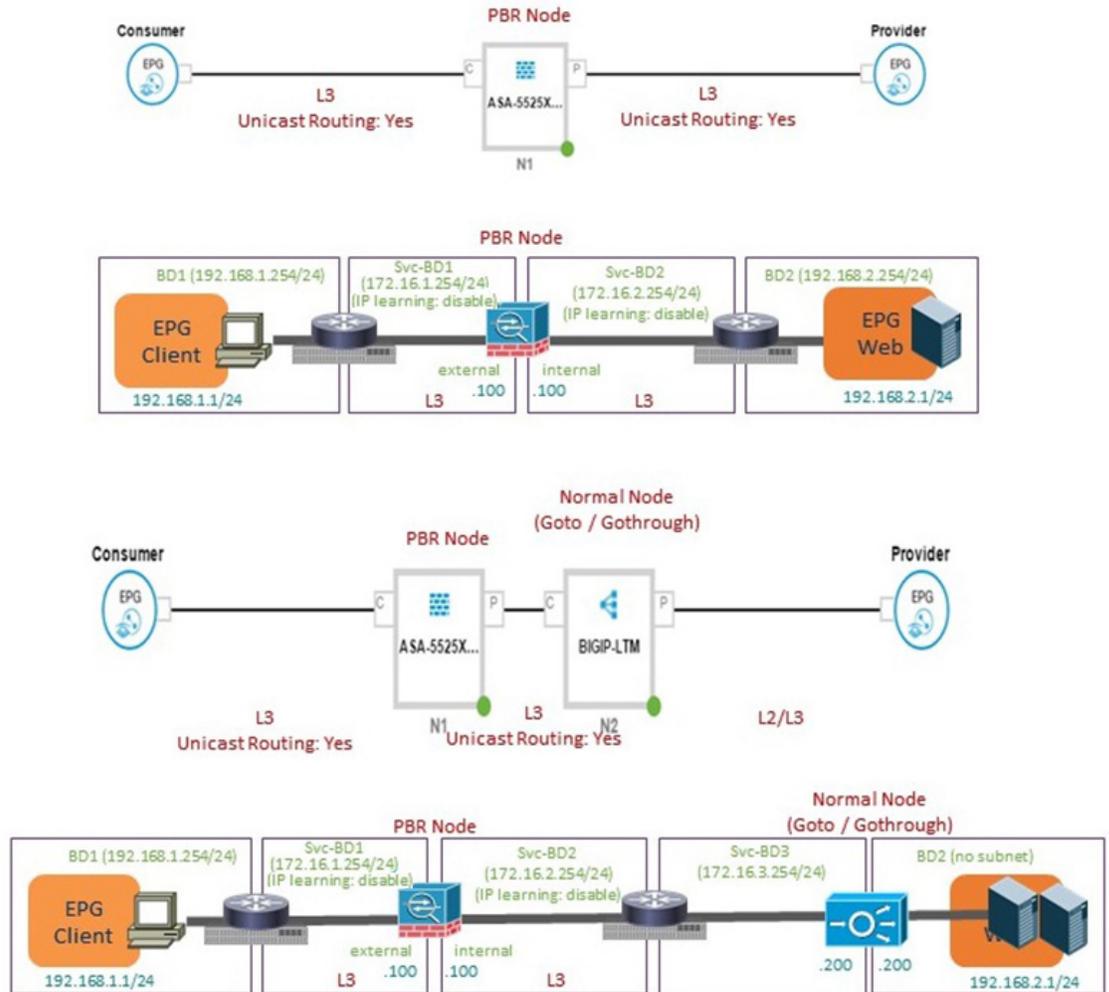


図 5:異なる VRFインスタンスのポリシーベースリダイレクト

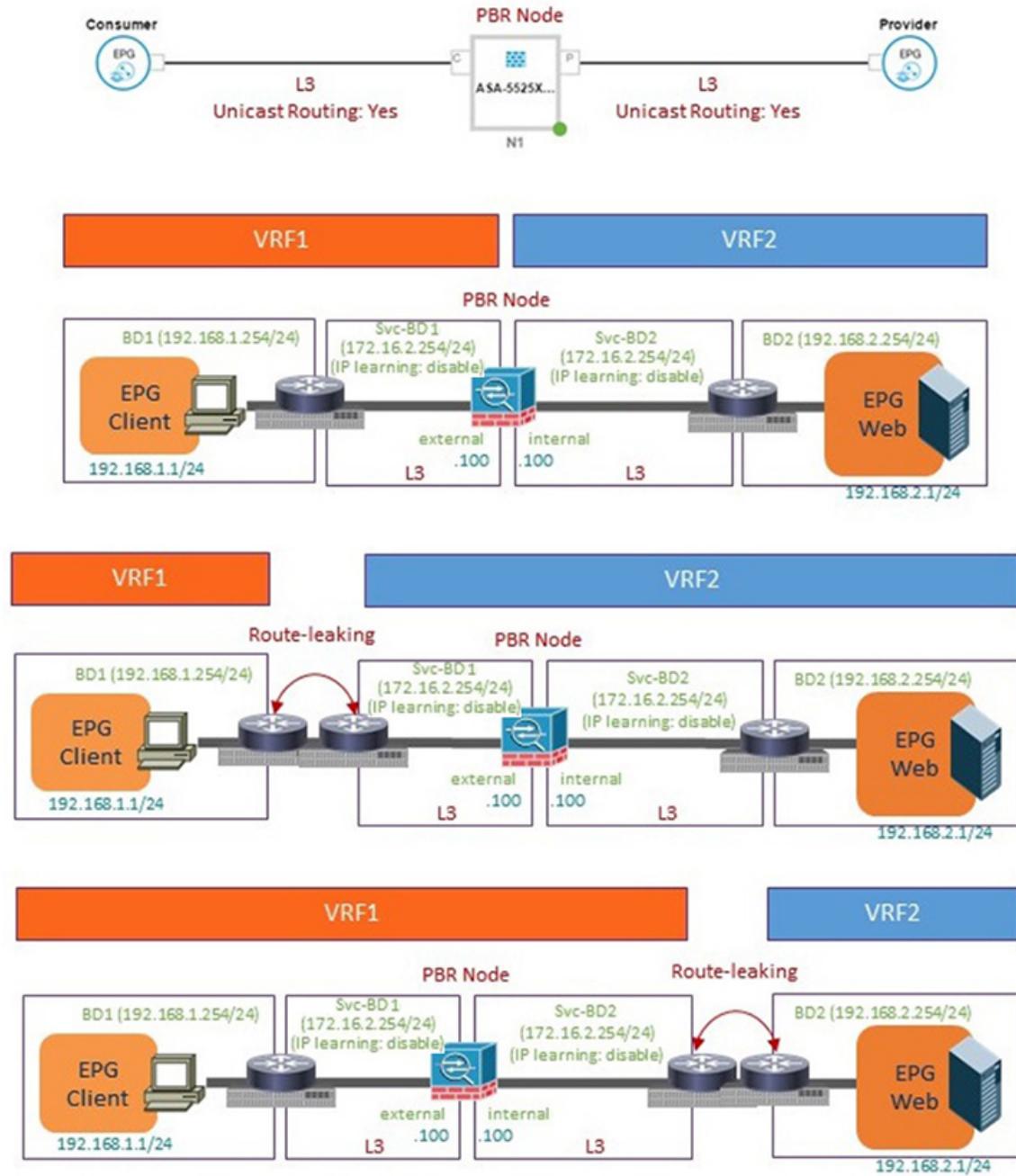
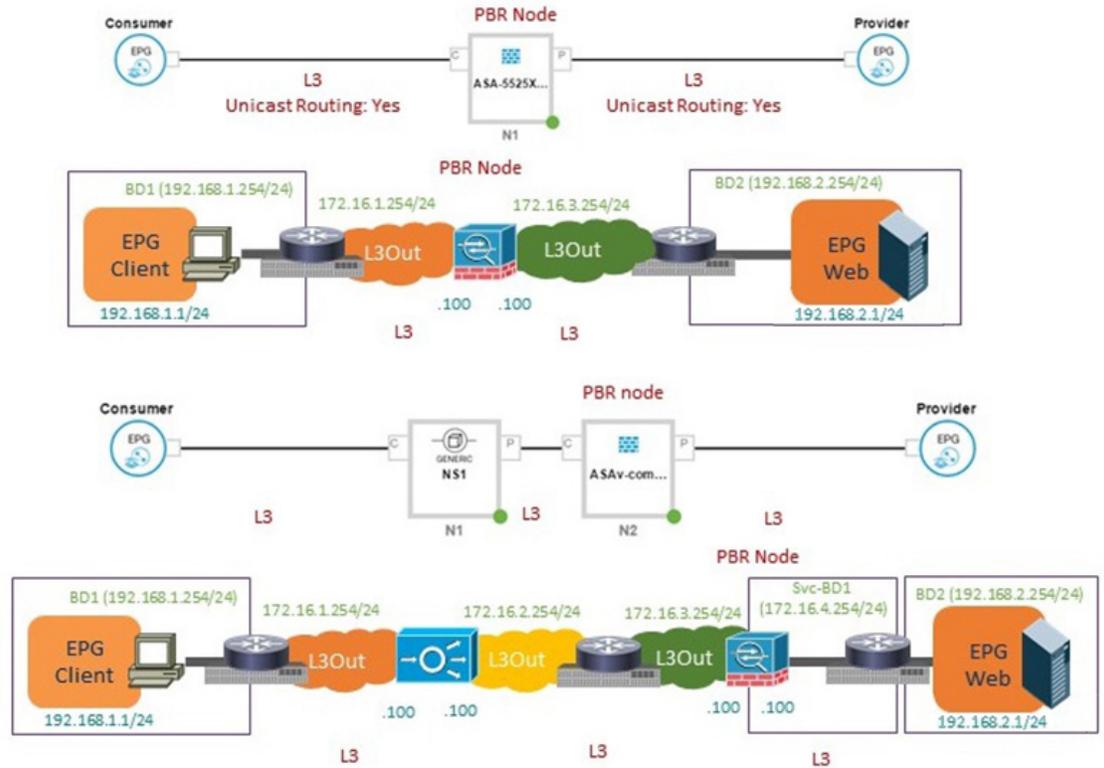
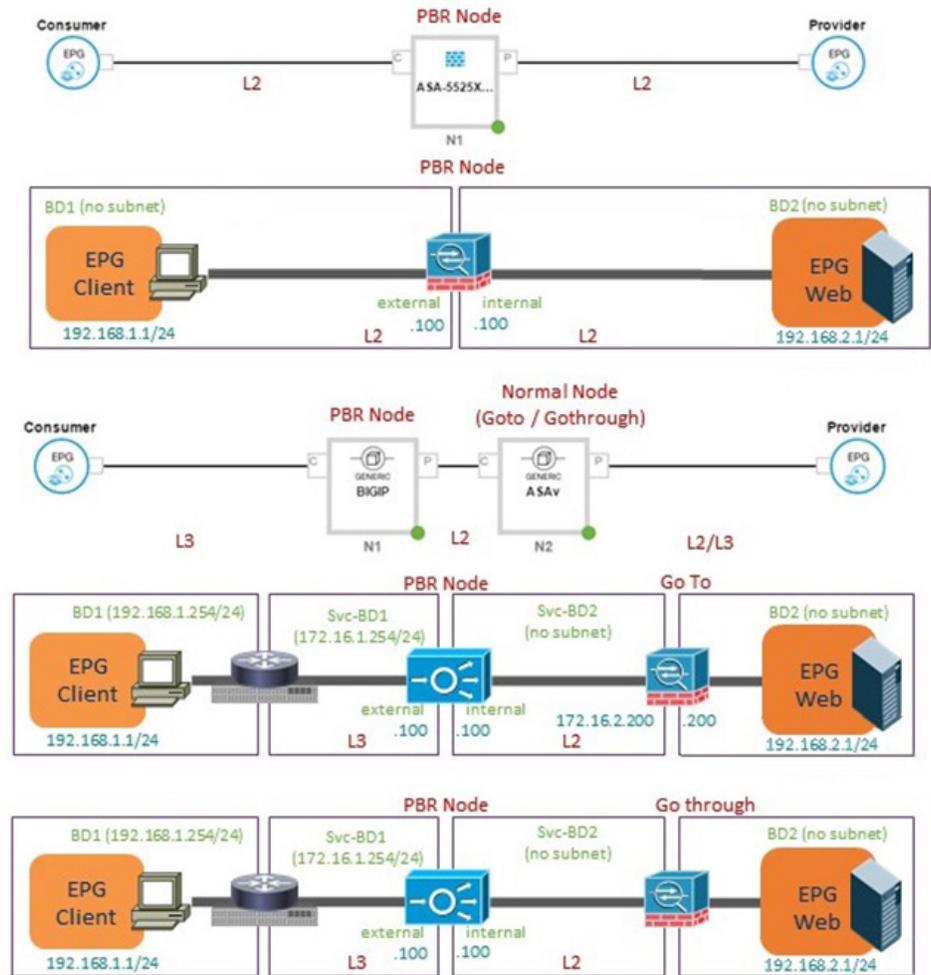


図 6 : L3Out 接続先を使用したポリシーベースリダイレクト



- 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 7: 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。

- 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。

[全般 (General)] セクションでは、[サービスタイプ (Service Type)] には [ファイアウォール (Firewall)]、[ADC]、[その他 (Other)] を選択できます。

(注) レイヤ1/レイヤ2 PBR 設定の場合、レイヤ4～レイヤ7サービスデバイスを作成し、次の手順を実行します。

1. [その他 (Other)] として、[サービスタイプ] を選択します。
2. [デバイスタイプ (Device Type)] には、[物理 (Physical)] を選択します (クラウド/仮想はサポートされていません)。
3. 物理ドメインを選択します。
4. 必要に応じて、[機能タイプ (Function Type)] [L1] または [L2] を選択します。
5. 外部および内部の具象インターフェイスを作成し、対応するリーフにポート接続を作成します。
6. 事前に作成した具象インターフェイスを選択し、クラスタインターフェイスを作成します。このインターフェイスを作成するときは VLAN カプセル化を指定する必要があります。カプセル化はサービス デバイスにプッシュされます。

(注) 静的VLAN構成の場合、外部レッグと内部レッグがレイヤ2に対して異なるVLANを持つことを確認します。それ以外は、レイヤ1に対して同じVLANになります。

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** フィールドに、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。

Cisco Application Policy Infrastructure Controller (APIC) リリース 4.2(1) 以降のリリースでは、オプションで手順 c を繰り返すことで、最大で 5 つのサービスノード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) **Route Redirect** チェックボックスをオンにします。
- f) [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 [サービスグラフテンプレート (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:
- 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。
 - 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。
 - Contract** オプション ボタンの **Create A New Contract** をクリックします。
 - Contract Name** フィールドに、契約の名前を入力します。
 - 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。
 - Filter Entries** テーブルで + をクリックしてエントリを追加します。
 - 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。
 - Next** をクリックします。
 - 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。
 - 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。
 - 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。
 - 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。
 - 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。

- ステップ 1** デバイス クラスタを作成します。

例 :

```
1417 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
  1417 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
```

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

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：

```
1417 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：

```
1417 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 svcredirect
  enable
  connector consumer cluster-interface consumer_PBRv6
    bridge-domain tenant PBRv6_ASA_HA_Mode name External-BD3
    svcredirect-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
    svcredirect-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：

```
svcredirect-pol Internal_leg
  redir-dest 20:1:1:1::1 00:00:AB:CD:00:11
  exit
svcredirect-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 svcredirect-pol
# Command: show running-config tenant PBRv6_ASA_HA_Mode svcredirect-pol
# Time: Wed May 25 00:57:22 2016
tenant PBRv6_ASA_HA_Mode
  svcredirect-pol Internal_leg
    redir-dest 20:1:1:1::1/32 00:00:AB:CD:00:11
  exit
  svcredirect-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 1417 graph PBRv6_ASA_HA_Mode_Graph
# Command: show running-config tenant PBRv6_ASA_HA_Mode 1417 graph PBRv6_ASA_HA_Mode_Graph
# Time: Wed May 25 00:55:09 2016
tenant PBRv6_ASA_HA_Mode
  1417 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 1417-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_Mode-External-BD3
           consumer_PBRv6  External_leg
provider   vlan-105  PBRv6_ASA_HA_Mode-Internal-BD4
           provider_PBRv6  Internal_leg

```

複数ノードポリシーベースのリダイレクトについて

マルチノードポリシーベースリダイレクトは、サービスグラフで最大5つの機能ノードをサポートすることで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リダイレクト(PBR)構成により、サービスノードのプールをプロビジョニングできるため、ポリシーに基づき、コンシューマーとプロバイダーのエンドポイントグループ間のトラフィックを負荷分散できます。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以降の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)# 1417 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。

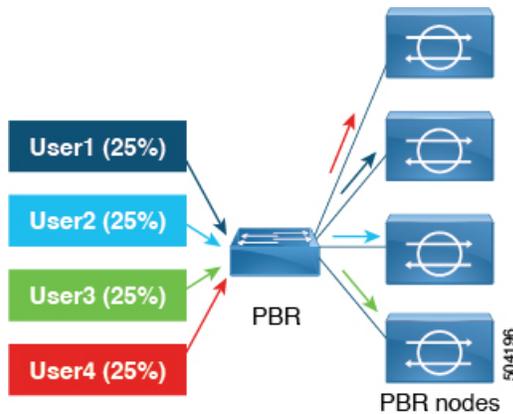
```
apicl(config-service)# connector external
apicl(config-connector)# svcredir-pol tenant solar name fw-external
```

重みベースの対称ポリシーベースのリダイレクトについて

Cisco APIC リリース 6.0(1) より前のリリースでは、各 PBR 接続先の重みを指定するオプションはありませんでした。PBR 接続先（サービスノード）のキャパシティは考慮されておらず、各接続先の重みは同じでデフォルト値の 1 です。次の例では、4 つの接続先を考えます。トラフィックのロードバランスの重みが同じであるため、各接続先では約 25% とほぼ同じ量のトラフィックを受信できます。

表 1: PBR 接続先へのトラフィック（デフォルト設定の対称 PBR、重みは「1」）

Destination	重量	Traffic %-age (おおよその)
接続先 1	1	25
接続先 2	1	25
接続先 3	1	25
接続先 4	1	25

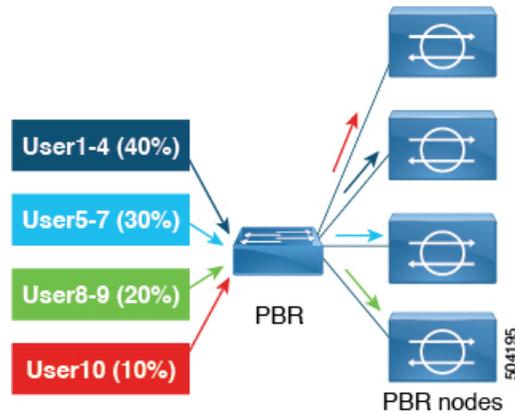


Cisco APIC リリース 6.0(1) 以降のリリースでは、トラフィックをより効率的に処理する重みベースの対称 PBR がサポートされています。重みベースの対称 PBR では、管理者はサービスノードのキャパシティに基づいて PBR 接続先の重みを設定し、設定された重みに基づいて負荷分散できます。1 つのサービスノードは複数のポリシーに属することができ、異なるポリシーで異なる重みを持てます。

容量の異なる4つのPBR接続先について考察します。すべての接続先に同じ量のトラフィックは送信されず、接続先のPBR設定は重みベースです。1から10までの重みを付けることができます。重みが付いていない場合、デフォルト値は1です。重みによって、接続先に送信されるトラフィックが決まります。トラフィックの重みベースの分散の例を以下に示します。

表 2: PBR 接続先へのトラフィック (重みベースの対称 PBR)

Destination	重量	Traffic %-age (おおよその)
接続先 1	4	40
接続先 2	3	30
接続先 3	2	20
接続先 4	1	10



(注) 上記に示すトラフィックのパーセンテージ (25%、30%、10% など) の数値は示唆的なものであり、明確なものではありません。

サービス付加の対称 PBR を維持するには、各サービスノードがコンシューマーコネクタとプロバイダーコネクタの2つのインターフェイスを持ち、両方向、つまりコンシューマーからプロバイダーおよびプロバイダーからコンシューマーに同じ重みを設定するようにします。

重みベースの PBR の制限事項

ブリッジドメインの PBR 接続先では、PBR ポリシーごとの最大の重みは 128 です。L3Out の PBR 接続先の場合、PBR ポリシーごとの最大の重みは 64 です。

システム障害は、次の条件下で発生します。

- プライマリとバックアップの接続先の重みの合計が 128 (または L3Out の場合は 64) を超える場合の動作障害。

- プライマリ接続先の重みの合計が 128（または L3Out の場合は 64）を超える場合の設定障害。
- バックアップ接続の重みの合計が 128（または L3Out の場合は 64）を超える場合の設定障害。

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) で使用できません。APIC リリース 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
- 送信元 IP アドレス、接続先 IP アドレス、プロトコル番号（デフォルト構成）。

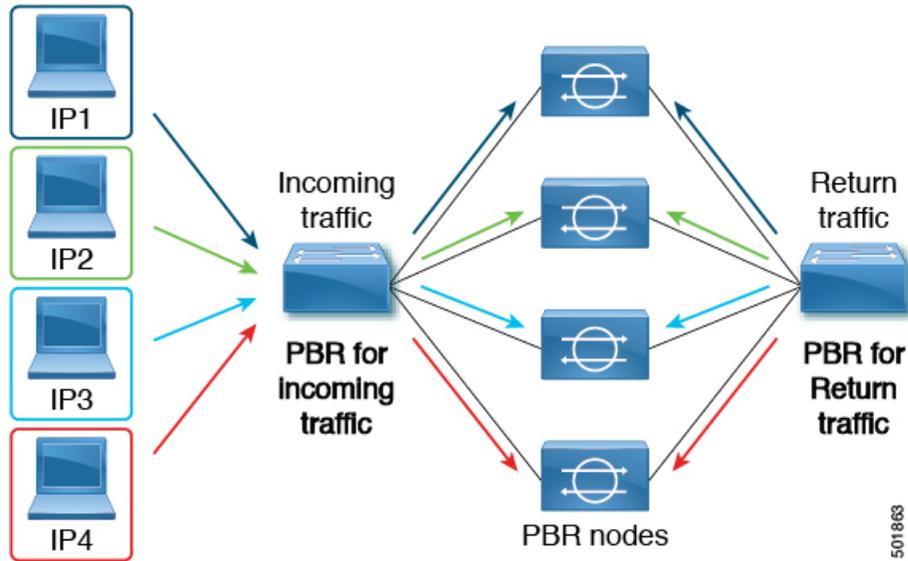
ポリシーベースのリダイレクトの修復性のあるハッシュ

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。

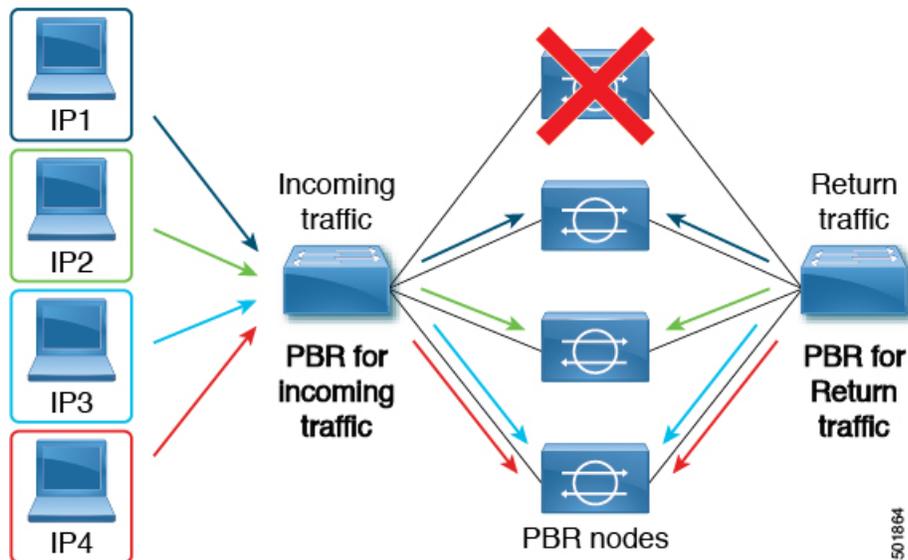
次の図は、着信と戻りユーザトラフィックが同じ PBR ノードを使用している、対称 PBR の基本的な機能を示しています。

図 8: 対称 PBR



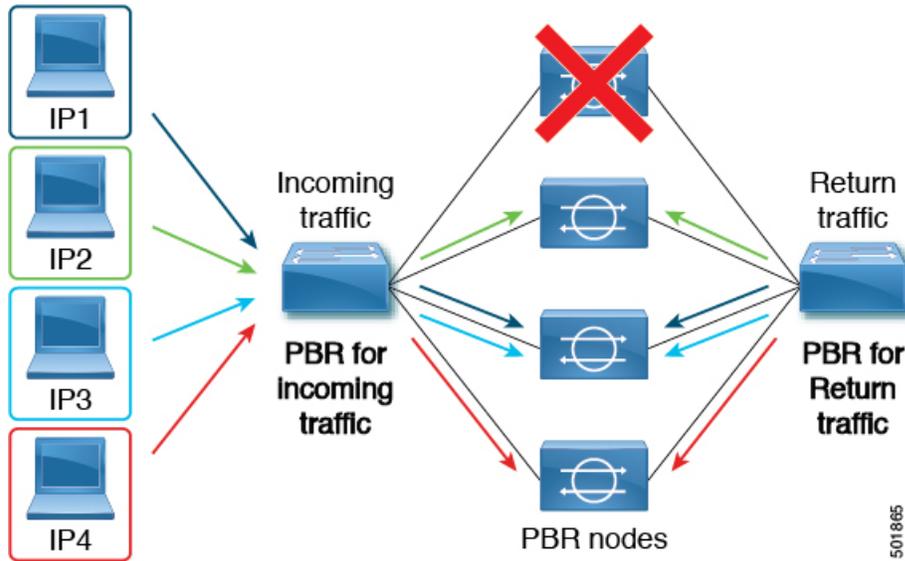
次の画像は、PBR ノードのいずれかが無効か、障害が発生したときに何が起きるかを示しています。IP1 のトラフィックは隣のノードへ再ハッシュされ、IP2 および IP3 のトラフィックがもう 1 つの PBR ノードに負荷分散されます。このことは、前述のように、他の PBR ノードが IP2 および IP3 トラフィックの現在の接続情報を持っていない場合、接続の中断や遅延という問題につながる可能性があります。

図 9: 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ー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ートラフィックは、それぞれの PBR ノードに残ります。

図 10: 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

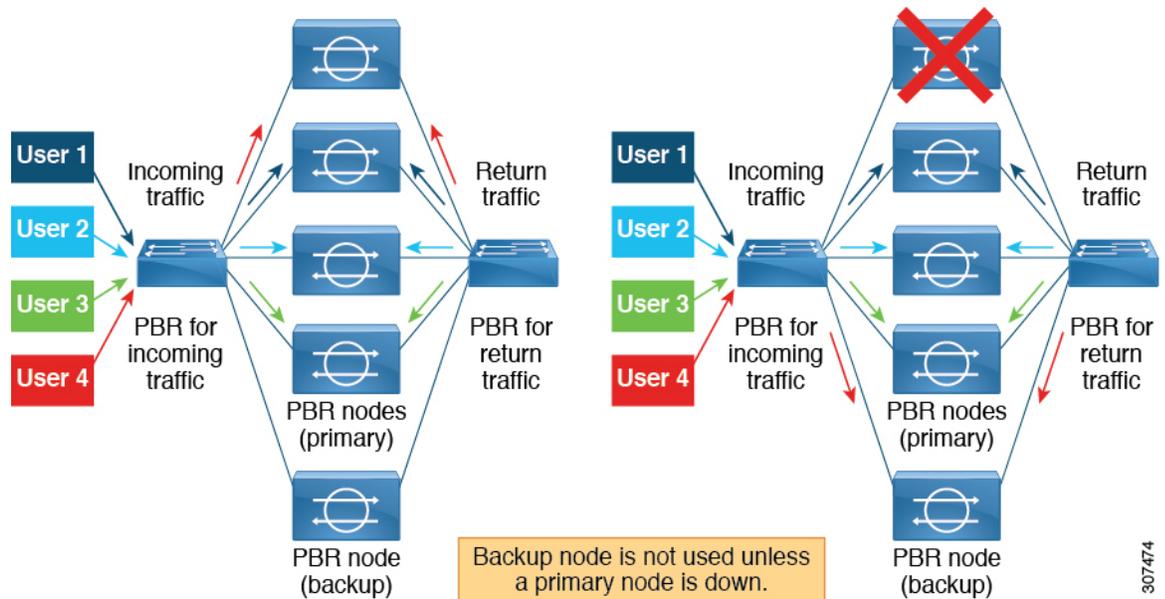
このタスクでは、L4-7 ポリシーベースのリダイレクトポリシーが作成されたことを前提としています。

- 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 [送信 (Submit)] をクリックします。

PBR バックアップポリシーについて

Cisco APIC リリース 4.2(1) より前のリリースでは、PBR ポリシー内のすべてのポリシーベースリダイレクト (PBR) 接続先は、PBR 接続先が機能している限り使用されます。PBR ノードの1つで障害が発生すると、既存のトラフィックフローが再ハッシュされます。これにより、たとえば、データベースがステートフルファイアウォールを通過している場合に、接続がリセットされる可能性があります。復元力のあるハッシュの PBR では、障害が発生したノードを通過したトラフィックのみが使用可能なノードの1つに転送されるため、新しく共有されるノードのトラフィックが過負荷になる可能性があります。使用可能なノードの1つを共有する代わりに、グループ内のバックアップノードを構成して使用して、トラフィックの負荷を吸収することができます。PBR バックアップポリシーごとに複数のバックアップ PBR 接続先を構成できます。

Cisco APIC リリース 4.2(1) 以降のリリースでは、新しい PBR バックアップポリシー オプションが利用できます。



復元力のあるハッシュでは、障害が発生したノードを通過したトラフィックのみが、使用可能なノードの1つに再ルーティングされます。復元力のあるハッシュと PBR バックアップポリシーを使用すると、障害が発生したプライマリノードを通過したトラフィックは、使用可能なバックアップノードの1つに再ルーティングされます。

バックアップポリシーの注意事項と制限事項

PBR バックアップポリシー オプションについては、次の注意事項と制限事項に従ってください。

- PBR バックアップポリシー オプションは、新世代リーフスイッチでのみサポートされません。これらのスイッチモデルでは、スイッチ名の最後に「-EX」、「-FX」、「-FX2」が付きます。
- 復元力のあるハッシュを有効にする必要があります。
- Cisco APIC リリース 5.0(1) 以降のリリースでは、レイヤ 1/レイヤ 2 PBR もバックアップポリシーをサポートしています。
- 接続先は、PBR 接続先またはバックアップ PBR 接続先として使用できますが、両方は使用できません（同じまたは異なる PBR ポリシーでは、プライマリ PBR 接続先を PBR ポリシーでバックアップ PBR 接続先としては使用できません）。

- 1 つのバックアップ PBR ポリシーは、1 つの PBR ポリシーでのみ使用できます。PBR ポリシーに 2 番目のバックアップポリシーを追加しようとすると、構成が拒否されます。

複数の PBR ポリシーに同じバックアップ PBR 接続先を使用する場合は、同じバックアップ PBR 接続先を使用して 2 つの異なるバックアップ PBR ポリシーを作成します。これらの両方のポリシーの接続先には、同じヘルスグループが構成されている必要があります。

- Cisco APIC リリース 6.0(1) 以降のリリースでは、バックアップノードで重みベースの PBR を設定できます。プライマリノードがダウンしている場合、（障害が発生した）プライマリノードと同等またはそれ以上の重みを持つバックアップが使用されます。たとえば、プライマリノードの重みを 5 と考えると、プライマリノードの障害後に有効なバックアップノードの重みは 5 以上である必要があります。
- 復元力のあるハッシュと PBR バックアップポリシーの使用：

- 障害が発生したノードを通過したトラフィックは、IP アドレスが小さい順に、PBR バックアップポリシーのバックアップノードに送信されます。複数のプライマリノードに障害が発生し、すべてのバックアップノードが使用されている場合、障害が発生したノードを通過したトラフィックは、プライマリノードとバックアップノードを含む使用可能なノードの 1 つに、IP アドレスの低い順にルーティングされます。たとえば、4 つのプライマリノード（192.168.1.1 ~ 192.168.1.4）と 2 つのバックアップノード（192.168.1.5 および 192.168.1.6）があるとします。

- IP アドレス 192.168.1.1 のプライマリノードに障害が発生した場合、このノードを通過したトラフィックは、最小の IP アドレス 192.168.1.5 で使用できるバックアップノードにルーティングされます。
- IP アドレス 192.168.1.1 と 192.168.1.2 の 2 つのプライマリノードに障害が発生した場合、192.168.1.1 を通過したトラフィックはバックアップノード 192.168.1.5 に、192.168.1.2 を通過したトラフィックはバックアップノード 192.168.1.6 にルーティングされます。
- IP アドレス 192.168.1.1、192.168.1.2、192.168.1.3 の 3 つのプライマリノードに障害が発生し、192.168.1.5 のバックアップノードが 1 つだけ使用可能な場合、最初に障害が発生したノード 192.168.1.1 を通過したトラフィックは、バックアップノード 192.168.1.5 にルーティングされます。

- 2 番目に障害が発生したプライマリノード 192.168.1.2 の場合、バックアップノードが使用されている IP アドレス 192.168.1.1 と使用可能なプライマリノード 192.168.1.4 の IP アドレスを比較すると、192.168.1.1 は、最初に使用可能なプライマリノード 192.168.1.4 より小さいため、障害ノード 192.168.1.2 を通過したトラフィックは、バックアップノード 192.168.1.5 に再ルーティングされます。
 - 3 番目に障害が発生したノード 192.168.1.3 では、バックアップノードがすでに使用されているため、3 番目に障害が発生したノードを通過したトラフィックは、使用可能なプライマリノード 192.168.1.4 にルーティングされます。
- ポッド認識 PBR が有効な場合、障害が発生したプライマリノードでは、障害が発生したノードを通過したトラフィックは、最初に使用可能なローカルバックアップノードに送られます。バックアップノードが使用できない場合は、ローカルプライマリノードが優先されます。すべてのローカルプライマリノードとローカルバックアップノードに障害が発生し、ローカルノードを使用できない場合、障害が発生したノードを通過したトラフィックは、リモートプライマリノードから、リモートバックアップノードに送られます。次に例を示します。
- プライマリノードとバックアップノードの両方が同じポッドにあり、ポッド認識 PBR が有効な場合、ローカルポッドのプライマリノードで障害が発生すると、障害が発生したノードを通過したトラフィックは同じローカル Pod のバックアップノードに送られます。
 - ローカルプライマリノードとローカルバックアップノードがあり、ポッド認識 PBR が有効な場合、ローカルプライマリノードおよびローカルバックアップノードで障害が発生すると、障害が発生したノードを通過したトラフィックは、別のポッド内の異なるプライマリノードに移動します。

PBR バックアップポリシーの作成

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、**[テナント (Tenant)] > [テナント名 (tenant_name)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [L4 ~ L7 ポリシーベースリダイレクトバックアップ (L4-L7 Policy Based Redirect Backup)]** の順に選択します。

ステップ 4 **[L4 ~ L7 ポリシーベースリダイレクトバックアップ (L4-L7 Policy Based Redirect Backup)]** を右クリックし、**[L4 ~ L7 ポリシーベースリダイレクトバックアップの作成 (Create L4-L7 Policy Based Redirect Backup)]** を選択します。

[PBR バックアップポリシーの作成 (Create PBR Backup Policy)] ダイアログが表示されます。

ステップ 5 **[名前 (Name)]** フィールドに、バックアップポリシーの一意の名前を入力します。

ステップ6 [L3 接続先 (L3 Destinations)] テーブルで、[+] をクリックします。

[リダイレクトされたトラフィックの接続先の作成 (Create Destination of Redirected Traffic)] ダイアログが表示されます。

- a) [IP] フィールドに、レイヤ3 接続先ノードの IP アドレスを入力します。
- b) [MAC] フィールドに、レイヤ3 接続先ノードの MAC アドレスを入力します。
- c) オプション: [追加の IPv4/IPv6] フィールドに、レイヤ3 接続先ノードのセカンダリ IP アドレスを入力します。
- d) [ポッド ID (Pod ID)] フィールドに値を入力します。デフォルト値は 1 です。
- e) [重み (Weight)] フィールドに値を入力します。デフォルト値は 1 です。指定できる範囲は 1 ~ 10 です。

プライマリノードに障害が発生すると、重みに基づいてバックアップノードが割り当てられます。

- f) [リダイレクトヘルスグループ (Redirect Health Group)] フィールドで、既存のヘルスグループを選択するか、新しいヘルスグループを作成します。

新しいリダイレクトヘルスグループ作成の詳細については、「[GUI を使用したリダイレクトヘルスグループの設定 \(58 ページ\)](#)」を参照してください。

- g) [OK] をクリックします。

オプション: 手順 a から手順 e を繰り返して、さらにレイヤ3 接続先を追加します。

ステップ7 [送信 (Submit)] をクリックします。

PBR バックアップポリシーの有効化

始める前に

このタスクは、レイヤ4 ~ レイヤ7 ポリシーベースリダイレクト (PBR) ポリシーが作成されている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、[テナント (Tenant)] > [テナント名 (tenant_name)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [L4 ~ L7 ポリシーベースリダイレクト (L4-L7 Policy Based Redirect)] > [L4 ~ L7 PBR ポリシー名 (L4-L7_PBR_policy_name)] の順に選択します。

ステップ4 [接続先タイプ (Destination Type)] フィールドで、[L3] を選択します。

ステップ5 [IP SLA モニタリングポリシー (IP SLA Monitoring Policy)] フィールドで、既存のポリシーを選択するか、モニタリング中に使用されるプローブを定義する新しい IP SLA モニタリングポリシーを作成します。

新しい IP SLA モニタリングポリシーの作成の詳細については、「[Cisco APIC Layer 3 ネットワーキング設定ガイド](#)」を参照してください。

ステップ6 [復元力のあるハッシュの有効化 (Resilient Hashing Enabled)] チェックボックスをオンにします。

ステップ7 [バックアップポリシー (Backup Policy)] フィールドで、既存のポリシーを選択するか、新しいバックアップポリシーを作成します。

新しいバックアップポリシー作成の詳細については、「[PBRバックアップポリシーの作成 \(26ページ\)](#)」を参照してください。

ステップ8 **L3 接続先**または**L1/L2 接続先**テーブルに少なくとも1つのアクティブなPBR接続先が表示され、リダイレクトヘルスグループで構成されていることを確認します。

新しいリダイレクトヘルスグループ作成の詳細については、「[GUIを使用したリダイレクトヘルスグループの設定 \(58ページ\)](#)」を参照してください。

ステップ9 [送信 (Submit)] をクリックします。

バイパスアクションについて

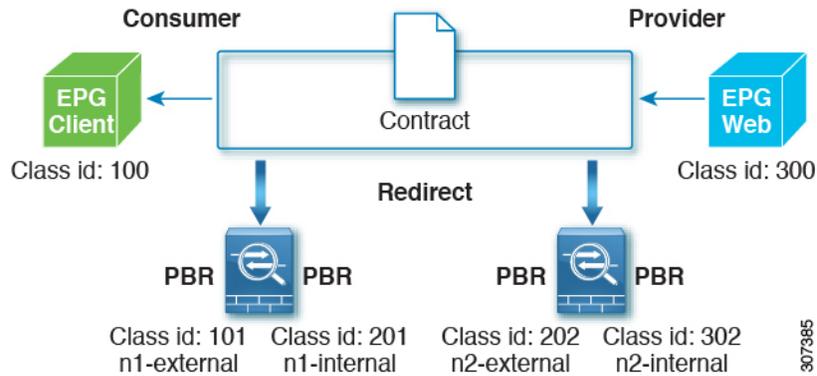
Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1(2) より前のリリースでは、レイヤ4～レイヤ7サービスのポリシーベースリダイレクトを作成する場合にしきい値の有効化を選択すると、**拒否アクション**または**許可アクション**の2つのオプションしか使用できませんでした。

これらの2つのオプションを使用すると、マルチノードポリシーベースリダイレクトグラフで、1つのノードがしきい値の下限を下回ると、選択した2つのオプションに応じて、次のアクションが発生します。

- **拒否アクション**：このノードでのトラフィックがドロップされます。
- **許可アクション**：トラフィックは接続先に直接送信され、残りのサービスチェーンはスキップされます。

Cisco APIC リリース 4.1(2) 以降のリリースでは、新しい**バイパスアクション**オプションが利用可能になりました。このオプションを使用すると、マルチノードポリシーベースリダイレクトグラフで、1つのノードがしきい値下限を下回っても、トラフィックは稼働しているかバイパスできない残りのサービスチェーンを介して通過できます。

次のセクションでは、この2ノードのポリシーベースリダイレクトグラフの例を使用して、これら3つのオプションによってトラフィックを処理する方法をそれぞれ説明します。



両方のノードが稼働している場合、この2ノードのポリシーベースリダイレクトは次のように動作します。

送信元 EPG	宛先 EPG	Action
100	300	PBR から n1-external
201	300	PBR から n2-external
302	300	permit
300	100	PBR から n2-internal
202	100	PBR から n1-internal
101	100	permit

次のセクションでは、[しきい値ダウンアクション (Threshold Down Action)]フィールドで選択したオプションに基づいて、最初のノードがダウンしたときに2ノードのポリシーベースリダイレクトがどのように動作するかについて説明します。

拒否(deny action)

上記の設定例で、[しきい値ダウンアクション (Threshold Down Action)]フィールドで拒否アクションを選択し、最初のノードがダウンすると、次の表のように最初のノードを使用するPBRポリシーが「ドロップ (Drop)」に更新され、クライアント EPG と Web EPG 間の通信がドロップします。

送信元 EPG	宛先 EPG	Action
100	300	削除 (Drop)
201	300	PBR から n2-external
302	300	permit
300	100	PBR から n2-internal
202	100	削除 (Drop)

送信元 EPG	宛先 EPG	Action
101	100	permit

許可(permit action)

上記の設定例で、[しきい値ダウンアクション (Threshold Down Action)] フィールドで許可アクションを選択し、最初のノードがダウンすると、最初のノードを使用する PBR ポリシーが「許可」に更新されます。クライアント EPG から Web EPG (100 から 300) へのトラフィックは、サービスノードを介さずに直接通過します。Web EPG からクライアント EPG (300 から 100) へのリターントラフィックは、次の表に示すように、n2-internal にリダイレクトされます。ただし、非対称フローであるため、2 番目のノードはパケットがドロップされる可能性があります。

送信元 EPG	宛先 EPG	Action
100	300	Permit
201	300	PBR から n2-external
302	300	permit
300	100	PBR から n2-internal
202	100	Permit
101	100	permit

バイパス (bypass action)

Cisco APIC リリース 4.1(2)以降のリリースでは、[しきい値ダウンアクション (Threshold Down Action)] フィールドで新しいバイパスアクション オプションを選択し、最初のノードがダウンすると、最初のノードを使用する PBR ポリシーが「PBR から次のデバイス (PBR to next device)」に更新されます。この場合、次のようになります。

- クライアント EPG から Web EPG (100 から 300) へのトラフィックは、n2-external にリダイレクトされます。
- Web EPG からクライアント EPG (300 から 100) へのリターントラフィックは、n2-internal にリダイレクトされます。
- n2-external からコンシューマーへのリターントラフィックは「許可」に設定されます。

送信元 EPG	宛先 EPG	Action
100	300	PBR から n2-external
201	300	PBR から n2-external
302	300	permit

送信元 EPG	宛先 EPG	Action
300	100	PBR から n2-internal
202	100	Permit
101	100	permit

ガイドラインと制約事項

バイパスアクション オプションの注意事項と制限事項は次のとおりです。

- バイパスアクション オプションは、新世代 ToR スイッチでのみサポートされます。これらのスイッチモデルでは、スイッチ名の最後に「EX」、「FX」、「FX2」が付きます。
- バイパスアクション オプションは、1 ノードサービスグラフでは必要ありません。この場合、バイパスが設定されていれば転送アクションは許可アクションと同じになります。
- L3Out EPG と通常の EPG は、コンシューマー EPG またはプロバイダー EPG にできます。
- NAT が有効のサービスノードは、トラフィックフローが中断するためバイパスできません。
- 5.0(1) 以降のリリースでは、レイヤ 1/レイヤ 2 PBR はバイパスアクションをサポートしています。
- 次の場合、バイパスアクション オプションはサポートされません。
 - ワンアームモードのレイヤ 4～レイヤ 7 デバイス。
 - リモートリーフスイッチ。
- バイパスアクションが有効の場合は、複数のサービスグラフで同じ PBR ポリシーを使用しないでください。Cisco APIC では、バイパスアクションを持つ同じ PBR ポリシーが複数のサービスグラフで使用されている場合、設定は拒否されます。これを回避するには、同じ PBR 接続先 IP アドレス、MAC アドレス、ヘルスグループを使用する異なる PBR ポリシーを設定します。

ポリシーベースリダイレクトでのしきい値ダウンアクションの設定

始める前に

このタスクは、レイヤ 4～レイヤ 7 サービス ポリシーベースリダイレクト (PBR) ポリシーが作成されている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、[テナント (Tenant)] > [テナント名 (tenant_name)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [L4 ~ L7 ポリシーベースリダイレクト (L4-L7 Policy Based Redirect)] > [L4 ~ L7 PBR ポリシー名 (L4-L7_PBR_policy_name)] の順に選択します。
- ステップ 4** [接続先タイプ (Destination Type)] フィールドで、[L3] を選択します。
- ステップ 5** [IP SLA モニタリングポリシー (IP SLA Monitoring Policy)] フィールドで、既存のポリシーを選択するか、モニタリング中に使用されるプローブを定義する新しいIP SLA モニタリングポリシーを作成します。
- 新しい IP SLA モニタリングポリシーの作成の詳細については、「Cisco APIC Layer 3 ネットワーキング設定ガイド」を参照してください。
- ステップ 6** [しきい値有効 (Threshold Enable)] チェックボックスをオンにします。
- 次のフィールドが表示されます。
- 最小しきい値のパーセンテージ (%)
 - 最大しきい値のパーセンテージ (%)
 - しきい値ダウン時のアクション
- ステップ 7** 最小しきい値および最大しきい値をパーセンテージ (%) で指定します。
- 最小しきい値と最大しきい値の詳細については、「サービスノードをトラッキングするためのポリシーベースリダイレクトとしきい値の設定 (55 ページ)」を参照してください。
- ステップ 8** [しきい値ダウン時のアクション (Threshold Down Action)] エリアで、しきい値ダウン時のアクションを選択します。
- 次のオプションがあります。
- バイパス (bypass action)
 - 拒否 (deny action)
 - 許可 (permit action)
- ステップ 9** [送信 (Submit)] をクリックします。

L3Out によるポリシーベースリダイレクト

Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1(2) 以降のリリースでは、L3Out を使用して、サービスグラフの一部であるレイヤ 4 ~ レイヤ 7 サービスデバイスに接続できます。ポリシーベースリダイレクト (PBR) サービスグラフの一部として L3Out を使用するには、複数の方法があります。

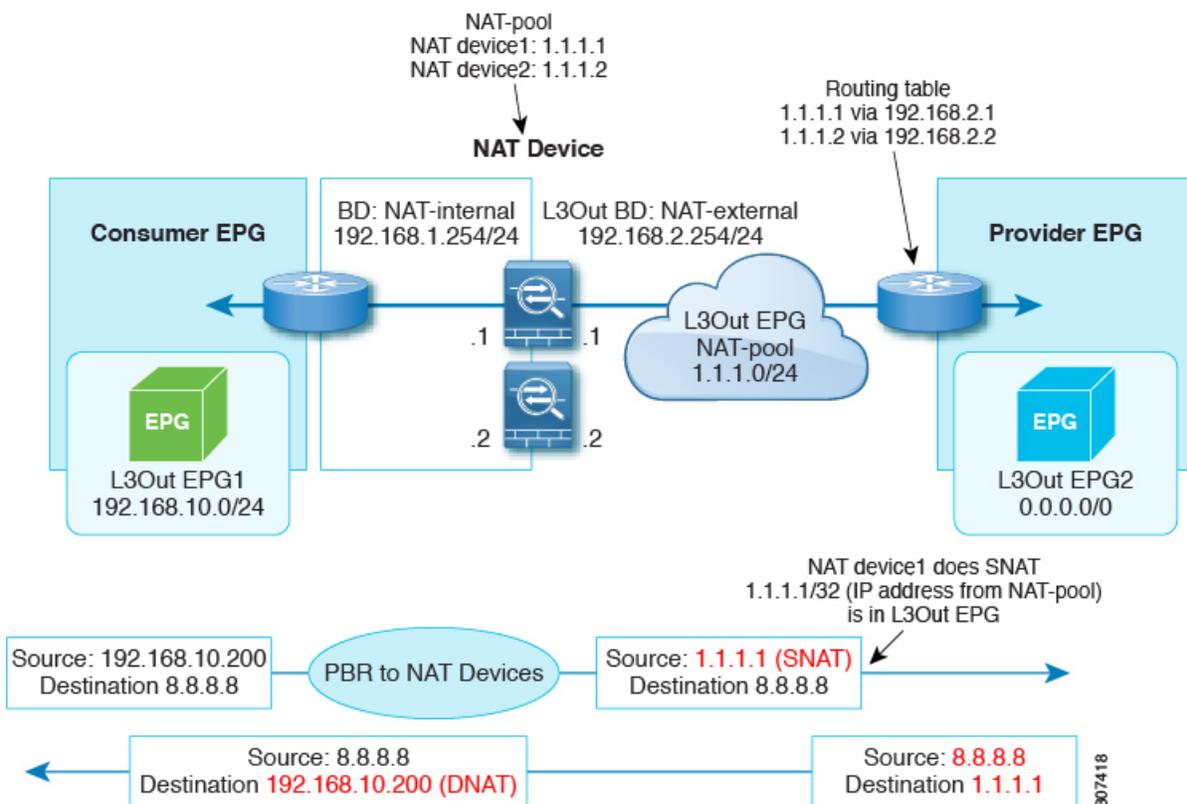
- PBR を使用すると、レイヤ 4 ~ レイヤ 7 サービスデバイスのコンシューマーインターフェイスのみにリダイレクトし、レイヤ 4 ~ レイヤ 7 サービスデバイスのプロバイダーインターフェイスは L3Out に接続します。これは、PBR がトラフィックの一方向に対してのみ

実行されるため、「単方向」PBRと呼ばれます。このオプションはCisco APICリリース4.1(2)で導入されました。

- PBRを使用すると、レイヤ4～レイヤ7サービスデバイスのプロバイダーインターフェイスのみにリダイレクトし、レイヤ4～レイヤ7サービスデバイスのコンシューマーインターフェイスはL3Outに接続します。このオプションはCisco APICリリース5.0(1)で導入されました。これも単方向PBR設計であり、前に箇条書きで説明したものの対称設計です。
- PBRを使用して、L3Outに接続されているレイヤ4～レイヤ7サービスデバイスインターフェイスにリダイレクトします。このオプションはCisco APICリリース5.2(1)で導入されました。

これらのユースケースについては、以下のテキストで詳しく説明されています。

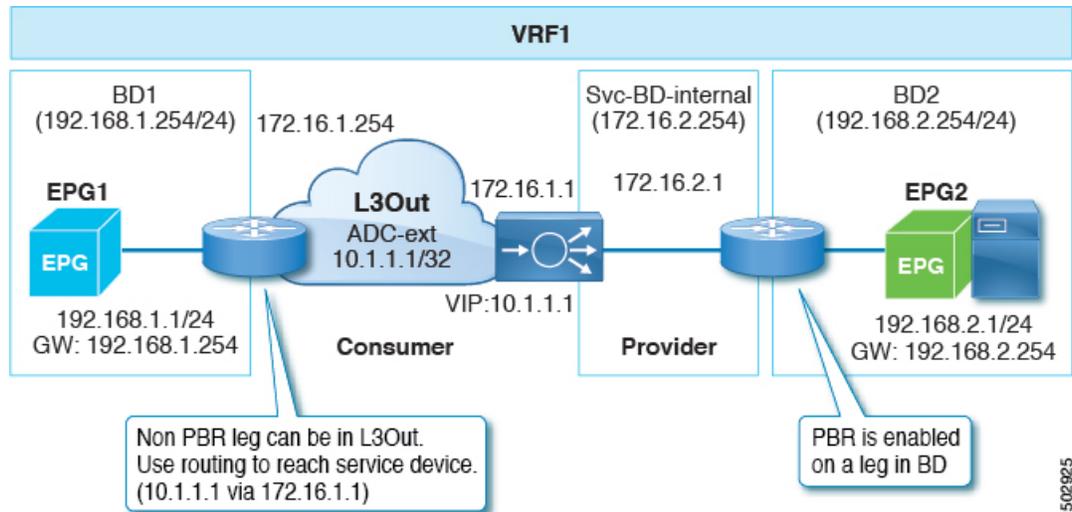
最初の箇条書きで述べたように、Cisco APICリリース4.1(2)以降のリリースでは、次の図に示すように、コンシューマーインターフェイスに単方向PBRを設定し、プロバイダーインターフェイスをL3Outに接続できます。



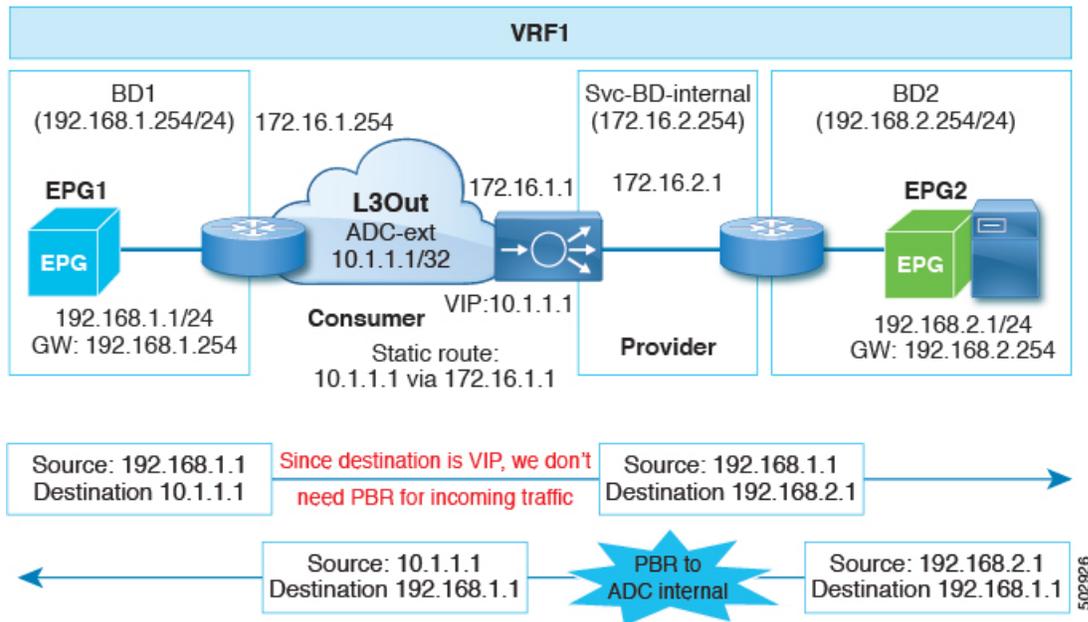
この例では、ブリッジドメインのコンシューマーコネクタでPBRが有効になっていますが、L3OutのプロバイダーコネクタではPBRが有効になっていません。この設計は、L3Outが最後のサービスノードのプロバイダーコネクタである場合にのみサポートされます。Cisco APIC 4.1(2)より前のリリースでは、トラフィックをサービスグラフのノードにリダイレクトするようにPBRが設定されていると、単方向PBRの場合でもレイヤ4～レイヤ7サービスデバイス

のコンシューマーコネクタとプロバイダーコネクタの両方がブリッジドメインに存在する必要がありました。

Cisco APIC リリース 5.0(1) 以降のリリースでは、L3Out がプロバイダーコネクタまたはコンシューマーコネクタであるかどうか、L3Out が最後のノードであるかどうかにかかわらず、単方向PBRはL3Out内の他のコネクタでサポートされます。これには、次の図に示すようにロードバランサがサービスノードのコンシューマー側のローカルサブネットの外部にVIPアドレスを持っている場合も含まれます。

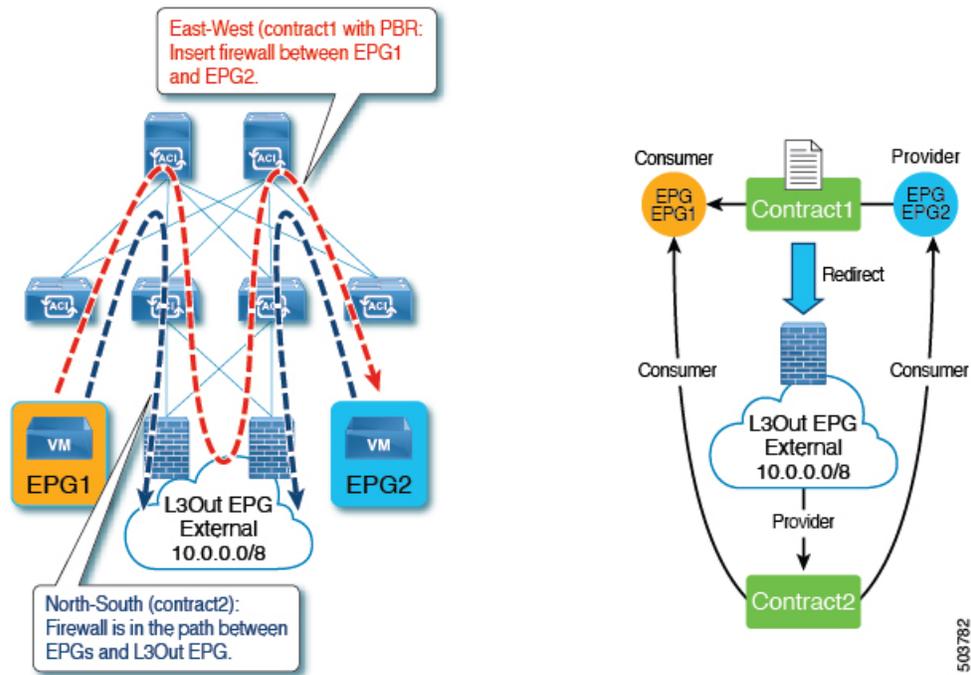


次の図の例では、コンシューマーエンドポイントからVIPアドレスへの着信トラフィックは、ルーティングテーブルに基づいて、L3Outに接続されているロードバランサに転送されます。次に、トラフィックはプロバイダーのエンドポイントに転送されます。プロバイダーエンドポイントからコンシューマーエンドポイントへのリターントラフィックは、PBRにより、サービスノードのプロバイダー側にリダイレクトされます。

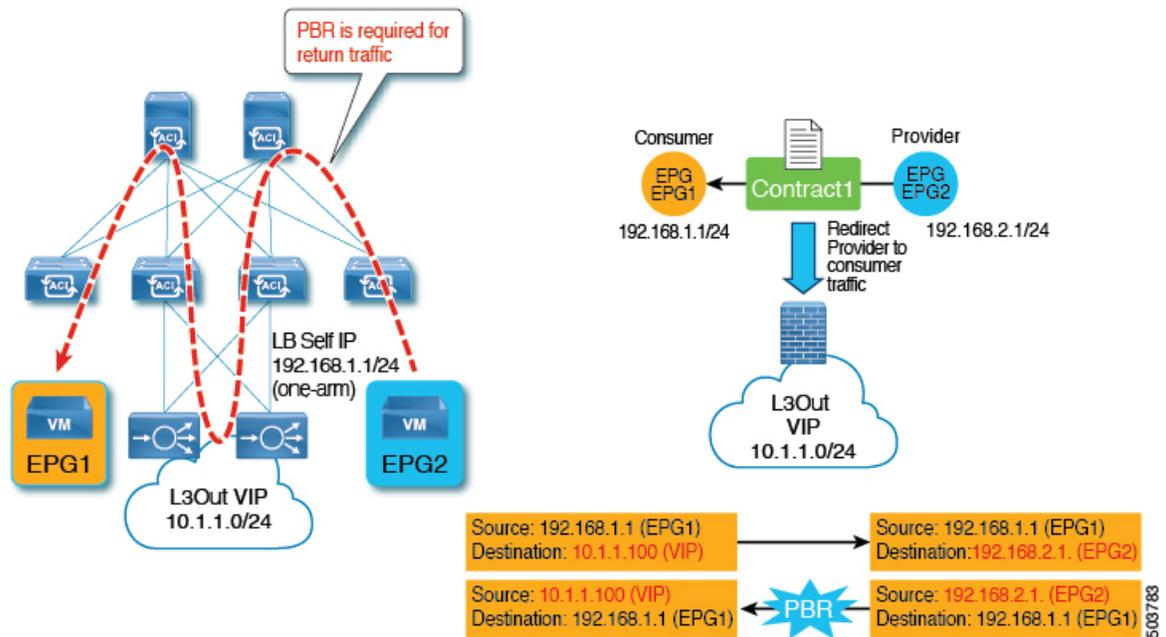


Cisco APIC リリース 5.2(1)以降のリリースでは、PBR ポリシーの接続先として使用されるレイヤ4～レイヤ7サービスデバイスは、L3Outにインターフェイスを持つことができます。これより前のリリースでは、PBR ポリシーの接続先インターフェイスはブリッジドメインのみでありました。一般的な導入例には次のものもあります。

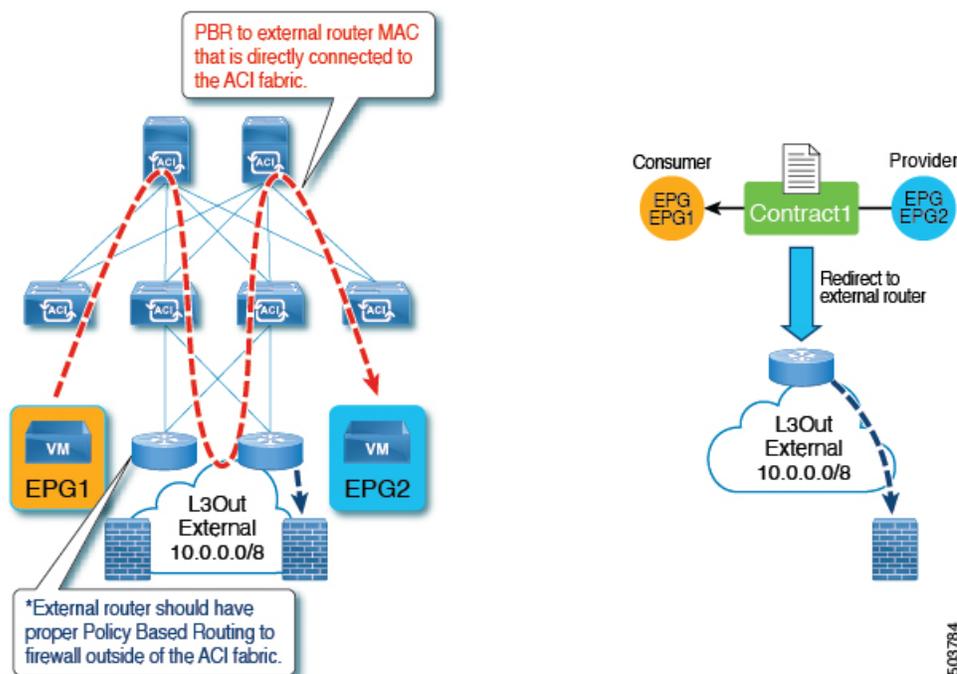
- 水平方向のトラフィックと垂直方向のトラフィックの両方に同じファイアウォールを使用できます。この場合、ファイアウォールの内部レッグは Cisco Application Centric Infrastructure (ACI) ファブリックに接続されていますが、ファイアウォールの外部レッグは Cisco ACI ファブリックの外部にあります。



- ローカルサブネットの外部にあるVIPアドレスを持つワンアームロードバランサを持てます。この場合、VIPアドレスは、ロードバランサのセルフIPアドレスサブネットの外部にあります。ロードバランサはソースネットワークアドレス変換 (SNAT) を実行しないため、リターントラフィックにはPBRが必要です。



- 外部ファイアウォールなど、Cisco ACI に直接接続されていないデバイスにトラフィックを再ルーティングできます。



L3Outによるポリシーベースリダイレクトの注意事項と制限事項

次の注意事項と制限事項は、L3Outを使用したポリシーベースリダイレクト (PBR) に関するものです。

- ワンアームモードとツーアームモードの両方がサポートされています。
- ブリッジメインの PBR とサービスグラフの同じ機能ノードの L3Out の PBR を混在させることはできません。次に例を示します。
 - N1 のコンシューマーコネクタを BD1 (PBR は有効) に構成し、N1 のプロバイダーコネクタを L3Out1 (PBR は有効) に構成することはできません。
 - ただし、N1 のコンシューマーコネクタを BD1 (PBR は無効) に構成し、N1 のプロバイダーコネクタを L3Out1 (PBR は無効) に構成できます。
- スイッチ仮想インターフェイス (SVI)、ルーテッドサブインターフェイス、またはルーテッドインターフェイスを使用した L3Out がサポートされています。
- PBR 接続先にフローティング SVI を使用するインフラ L3Out、GOLF L3Out、SDA L3Out、L3Out を使用することはできません。
- 同じ VRF インスタンスに他の L3Out EPG がある場合は、特定の L3Out EPG サブネットを使用します。そうしないと、他の L3Out が誤って EPG の分類に使用される可能性があります。

- 0.0.0.0/0 または 0::0 の L3Out EPG は、PBR 接続先の L3Out EPG には使用できません。これは、水平方向のトラフィックを自動的に作成されたサービス EPG で分類する必要があるためです。したがって、L3Out EPG が 0.0.0.0/0 で設定されている場合、水平方向のトラフィックは外部からのトラフィックとして分類されます。
- サービスデバイスが ツーアームモードで、サービスデバイスコネクタの L3Out の 1 つが 0.0.0.0/0 または 0::0 を学習する場合、両方のアームを同じリーフスイッチまたは同じ vPC ペアに接続する必要があります。
- コンシューマー/プロバイダー EPG が L3Out EPG の場合、PBR 接続先の L3Out が存在するサービスリーフスイッチの下に配置することはできません。これはハードウェアの制限です。
 - リーフスイッチは、特定の L3Out EPG サブネットを使用している場合でも、パケットがコンシューマー/プロバイダー L3Out EPG からのものか、サービスデバイスから戻ったものなのかを判断できません。
 コンシューマー/プロバイダー EPG が L3Out EPG ではなく通常の EPG の場合、コンシューマー、プロバイダー、サービスデバイスの L3Out は同じリーフスイッチの下に配置できます。
- L3Out の背後のサービスデバイスを使用してツーアームモードで PBR を展開し、ネクストホップ接続に OSPF または EIGRP プロトコルを使用する場合、両方のアームを同じサービスリーフスイッチに展開することはサポートされていません。各アームを異なるサービスリーフスイッチに展開することができます。
- ツーアームモードで PBR を展開し、OSPF、EIGRP、BGP プロトコルを使用してサービスノード L3Out を展開する場合、各アームでサービスデバイスのネクストホップを適切に制御する必要があります。
- 次の表に、サポートされるコンシューマー/プロバイダー EPG タイプの組み合わせをまとめます。

表 3: サポートされるコンシューマー/プロバイダー EPG タイプの組み合わせ

コンシューマー/プロバイダー	EPG	L3Out	ESG
EPG	サポート対象	サポート対象	サポート対象外 ¹
L3Out	サポート対象	サポート対象	サポート対象
ESG	非対応	サポートあり	サポート対象

¹ EPG 間のコントラクトは、サービスグラフがなくてもサポートされません。

- PBR を使用した EPG/ESG/L3Out EPG 内コントラクトがサポートされています。
 - リリース 5.2(1) 以降のリリースでは、L3Out EPG 内コントラクトがサポートされています。

- ブリッジドメインでPBRでサービスグラフを使用する場合、Cisco ACIではサービスEPGと呼ばれる非表示のEPGが自動的に作成されます。Cisco ACIは、サービスEPGとユーザーが作成したEPGの間のコントラクトを設定して、サービスグラフによって定義されたトラフィックパスを許可します。レイヤ4～レイヤ7サービスデバイスインターフェイスをL3Outに接続し、このインターフェイスをサービスグラフのPBR接続先として使用すると、Cisco ACIによってサービスEPGが自動的に作成されますが、管理者はサービスEPGに加えてL3Out EPGも作成する必要があります。一部のトラフィックはPBRを使用してレイヤ4～レイヤ7インターフェイスに転送されますが、ロードバランサによるキープアライブなどの他のトラフィックは、通常のトラフィック転送（ルーティング）を使用して送信する必要があります。ロードバランサのキープアライブの場合に必要なように、レイヤ4～レイヤ7サービスデバイスで使用されるL3Out EPGとエンドポイントがあるEPG間の通信を有効にするには、**ダイレクトコネクト**を設定し、L3Out EPGとサーバーがあるEPG間のコントラクトも設定する必要があります。
- コンバージェンスを向上させるため、L3OutのPBR接続先にはトラッキングが必須です。
- ブリッジドメインのPBR接続先にも適用できるワンアームモードでは、バイパス機能はサポートされていません。
- マルチノードPBRがサポートされています。
- アクティブ/アクティブ対称PBRがサポートされています。
- トラッキング、しきい値ダウンアクションがサポートされています。
- 復元力のあるハッシュがサポートされています。
- N+M冗長性がサポートされています。
- 単一のポッド、Cisco ACI マルチポッド、リモートリーフスイッチがサポートされています。
- Cisco ACI マルチサイトはサポートされていません。
- エンドポイントセキュリティグループ(ESG)のないVRF間コントラクトで、PBR L3Outの接続先がプロバイダーVRFインスタンスにある場合：
 - サービスデバイスによって使用されるL3Out EPGサブネットをコンシューマーVRFインスタンスにリークする必要があります。そうしないと、コンシューマーVRFインスタンスにはPBR接続先へのルートがなく、プロバイダーVRFインスタンスにはプロバイダーVRFインスタンスのPBR接続先からコンシューマーEPGへのトラフィックに対する許可ルールがありません。PBR接続先がブリッジドメインにある場合、PBR接続先のサービスブリッジドメインをコンシューマーVRFインスタンスにリークする必要はありません。
- PBRの有無によるESGからL3Out、ESG間に対するESGによるVRF内コントラクト：
 - コンシューマーESGまたはL3OutサブネットをプロバイダーVRFインスタンスにリークし、プロバイダーESGまたはL3OutサブネットをコンシューマーVRFインスタンスにリークする必要があります。さらに、PBRを使用している場合：

- PBR 接続先がブリッジドメインにある場合、サービスデバイスサブネットをリークする必要はありません。
- L3Out の PBR 接続先が L3Out EPG がコンシューマーまたはプロバイダー VRF インスタンスにあるかどうかにかかわらず、サービスデバイスが使用する L3Out EPG サブネットを他の VRF インスタンスにリークする必要があります。
- L3Out EPG サブネットをリークするには、サブネットのプロパティを変更し、**共有ルート制御サブネット**と**共有セキュリティインポートサブネット**を有効にします。また、必要に応じて**集約共有ルート**を有効にします。
- 内部 VRF インスタンスは、PBR 接続先への L3Out を持つボーダーリーフスイッチ上に作成されます（VRF は同じテナントの下に作成されます）。内部 VRF インスタンスは、PBR ポリシーの PBR 接続先ごとに作成されます。
 - たとえば、PBR-policy1 に 3 つの接続先がある場合、PBR ポリシーに 3 つの VRF インスタンスが作成されます。複数のコントラクトで PBR-policy1 を再利用する場合、3 つの VRF インスタンスのみが作成されます。
 - コンシューマー/プロバイダーのリーフスイッチには VRF スケールの影響はありません。
- L3Out がコンシューマーまたはプロバイダーのいずれかの VRF インスタンスに属していることを確認します。

GUI を使用した L3Out によるポリシーベースリダイレクトの設定

L3Out を使用したポリシーベースリダイレクト (PBR) の構成手順は、一部の相違点を除き、通常のポリシーベースリダイレクト構成とほとんど同じです。

始める前に

必要なテナント、VRF インスタンス、EPG、EPG のブリッジドメイン、サービスブリッジドメインを作成します。

ステップ 1 レイヤ 4 ~ レイヤ 7 デバイスの作成 PBR の接続先が L3Out にある場合、具象インターフェイスの場合、パスは L3Out 論理インターフェイスで使用されるパスと一致する必要があります。

「[GUI を使用したレイヤ 4 ~ レイヤ 7 サービスデバイスの設定](#)」を参照してください。

L3Out とピアリングするレイヤ 4 ~ レイヤ 7 のサービス仮想アプライアンスと組み合わせて L3Out で PBR を使用する場合、具体的なデバイス構成の一部として仮想化ホストインターフェイスのパスを構成する必要があります。レイヤ 4 ~ レイヤ 7 サービスの具象デバイス設定で使用されるパスと、L3Out 設定で使用されるパスは一致する必要があります。これは、フローティング L3Out 機能がまだサービスグラフに統合されていないためです。したがって、Cisco Application Centric Infrastructure (ACI) にはパス情報を設定する必要があります。

ステップ2 サービス グラフ テンプレートを作成します。

[GUIでサービスグラフテンプレートを構成する](#)を参照してください。

ステップ3 IP SLA モニタリング ポリシーの設定

次のサイトで、「Cisco APIC Layer 3 ネットワーキング設定ガイド」のIP SLAに関する章を参照してください。

<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

ステップ4 PBR ポリシーを作成します。

「[GUIを使用したポリシーベースリダイレクトの設定 \(11 ページ\)](#)」を参照してください。

トラッキングを有効にするには、リダイレクトヘルスグループを設定する必要があります。「[GUIを使用したリダイレクトヘルスグループの設定 \(58 ページ\)](#)」を参照してください。

ステップ5 L3Out と L3Out EPG (または外部 EPG) を作成します。

0.0.0.0/0 は使用せず、ファイアウォールまたはロードバランサのサブネットアドレスと、外部トラフィックのサブネットを必ず含めてください。

次のサイトで、「Cisco APIC Layer 3 ネットワーキング設定ガイド」を参照してください。

<https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html>

ステップ6 デバイス選択ポリシーを作成します。

「[GUIを使用したデバイス選択ポリシーの作成](#)」を参照してください。

手順に従って、次のサブステップを必要に応じて置き換えます。

- a) [関連付けられたネットワーク (Associated Network)] ボタンで、[ブリッジドメイン (Bridge Domain)] または [L3Out] を選択します。

PBR ポリシーの接続先が L3Out のインターフェイスである場合は、[L3Out] を選択する必要があります。

- b) [ブリッジドメイン (Bridge Domain)] を選択した場合は、[ブリッジドメイン (Bridge Domain)] ドロップダウンリストで、ターゲットインターフェイスのブリッジドメインを選択します。[L3Out] を選択した場合は、[L3Out] ドロップダウンリストで、ターゲットインターフェイスの L3Out EPG を選択します。

- c) 必要に応じて、[L4 ~ L7 ポリシーベースリダイレクト (L4-L7 Policy-Based Redirect)] ドロップダウンリストで、適切な PBR ポリシーを選択します。

PBR ポリシーの接続先が L3Out のインターフェイスである場合は、PBR ポリシーを選択する必要があります。

- d) 必要に応じて、デバイス選択ポリシーの残りの部分を設定します。

ステップ7 サービスグラフをコントラクトに付加したサービスグラフを適用します。

「[GUIを使用したエンドポイントグループへのサービスグラフテンプレートの適用](#)」を参照してください。

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。

レイヤ1/レイヤ2ポリシーベースリダイレクトについて

レイヤ1デバイスの使用は、通常、インラインモードまたは有線モードと呼ばれ、サービスデバイスがレイヤ2またはレイヤ3転送に関与していないセキュリティ機能を実行することが予想される場合、ファイアウォールと侵入防御システム(IPS)に使用されます。

レイヤ2デバイスの使用は、通常、透過モードまたはブリッジモードと呼ばれ、ファイアウォールおよびIPSに使用されます。

レイヤ3デバイスの使用は、通常、ルーテッドモードと呼ばれ、ルータファイアウォールおよびロードバランサに使用されます。

Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1 より前のリリースでは、PBRは、レイヤ3デバイス(Go-To)モードでのみ設定されたレイヤ4～レイヤ7サービスデバイスにトラフィックをリダイレクトするように設定できました。レイヤ4～レイヤ7サービスデバイスが、透過ファイアウォールなどのレイヤ1またはレイヤ2デバイスである場合、PBRは使用できませんでした。サービスグラフを使用し、レイヤ4～レイヤ7サービスデバイスを**透過(Go-Through)**モードで定義することで、レイヤ1またはレイヤ2モードで動作するレイヤ4～レイヤ7サービスデバイスのみを展開できました。

Cisco APIC リリース 4.1 以降のリリースでは、レイヤ1/レイヤ2デバイスモードで設定されたレイヤ4～レイヤ7サービスデバイスにトラフィックをリダイレクトするようにPBRを設定することもできます。PBRは、ルーテッドモードのファイアウォールに加えて、インラインIPSまたは透過ファイアウォールで使用できます。

レイヤ1/レイヤ2PBR機能の一部として、Cisco APICは、リンクレイヤをトラッキングするためにレイヤ2 ping パケットを使用してレイヤ4～レイヤ7サービスデバイスがトラフィックを転送しているかどうかを確認できます。

非IPアドレストラフィックも転送できる**透過(Go-Through)**モードとは異なり、レイヤ1/レイヤ2PBRはIPアドレストラフィックにのみ適用されます。

レイヤ1/レイヤ2 PBR 設定の概要

次のリストは、主要なレイヤ1/レイヤ2 PBR 設定の概念の一部をまとめたものです。

- デバイスレイヤ1/レイヤ2 PBR でレイヤ4～レイヤ7サービスデバイスを展開する場合、コンシューマー側とプロバイダー側の2つのブリッジドメインを設定する必要がありますが、通常の PBR とは異なり、これらのブリッジドメインはエンドポイント（コンシューマーまたはプロバイダー）に設定されているブリッジドメインと同じにできません。
- サービスブリッジドメインは、ユニキャストルーティングが有効になっている必要があります。
- 物理レイヤ4～レイヤ7サービスデバイスは、個々のリンクまたは VPC を使用してリーフスイッチに接続できます。
- レイヤ1 デバイスでは、コンシューマー側の VLAN とプロバイダー側の VLAN は同じですが、ブリッジドメインが異なります。したがって、レイヤ4～レイヤ7サービスデバイスのコンシューマー側とプロバイダー側は、異なる物理リーフに接続する必要があります。
- レイヤ4～レイヤ7サービスデバイスがレイヤ1またはレイヤ2デバイスとして設定されている場合、トラフィックを送受信するインターフェイスに IP アドレスがないため、接続先のリーフ/ポートおよび VLAN を入力することによってリダイレクトポリシーを定義します。
- リダイレクトポリシーの設定には、リーフ/ポートと VLAN の定義のみが必要で、MAC アドレスの入力はオプションです。MAC フィールドが空白の場合、Cisco Application Centric Infrastructure (ACI) は動的に1つの MAC アドレスを生成します。この MAC アドレスは、サービスブリッジドメイン上のレイヤ4～レイヤ7サービスデバイスに送信する際に、接続先 MAC アドレスを書き換えるために使用されます。これらの MAC アドレスは、レイヤ4～レイヤ7サービスデバイスの MAC アドレスではありません。これらは、Cisco ACI がトラフィックの接続先 MAC アドレスを書き換えるために使用する仮想 MAC アドレスです。
- レイヤ4～レイヤ7サービスデバイスがレイヤ2モードで展開されている場合、PBR がトラフィックを転送するために使用する MAC アドレスを、レイヤ4～レイヤ7サービスデバイスに転送するように静的に設定する必要があります。1つの MAC アドレスは、サービスブリッジドメインで使用されるコンシューマーからプロバイダーへの接続先 MAC アドレスを識別し、もう1つの MAC アドレスは、他のサービスブリッジドメインで使用されるプロバイダーからコンシューマーへの接続先 MAC アドレスを定義します。

これらの MAC アドレスは、リダイレクトポリシー定義の一部としてユーザーが APIC に手動で入力するか、フィールドが空のままの場合は自動生成されます。管理者は、これらの MAC アドレスをレイヤ4～レイヤ7サービスデバイスの MAC アドレステーブルに追加し、コンシューマーからプロバイダーへの方向で使用される MAC アドレスのプロバイダー側のポートと、プロバイダーからコンシューマーへの方向で使用されるコンシューマー側のポートに関連付ける必要があります。

- 中間スイッチがリーフと、レイヤ1/レイヤ2モードで展開されたレイヤ4～レイヤ7サービスデバイスの間にある場合、中間スイッチは、書き換えられた接続先 MAC 宛てのトラフィックを転送する必要もあります。
- レイヤ1/レイヤ2 PBR は、リーフ/ポート/VLAN への転送に基づいているため、VMM ドメインではなく、物理ドメインでのみ展開できます。仮想アプライアンスでレイヤ1/レイヤ2 PBR を展開する必要がある場合は、物理ドメインで構成する必要があります。
- ハイアベイラビリティの観点から、レイヤ4～レイヤ7サービスデバイスはアクティブ/スタンバイモードで展開され、Cisco ACIでは、どのパス（リーフ/ポート）がアクティブか、スタンバイかを確認するためにトラッキングを実行する必要があります。トラッキングは、レイヤ4～レイヤ7サービス論理デバイスクラスタ内の複数のサービスデバイスに必須です。
- レイヤ1/レイヤ2 PBR トラッキングには、レイヤ2 ping が使用されます。IP SLA タイプはレイヤ2 ping です。
- レイヤ2 ping の ethertype 0x0721 は、サービスデバイスを通るリーフノード間で交換されます。したがって、レイヤ1/レイヤ2デバイスでは ethertype 0x0721 を許可する必要があります。
- レイヤ1/レイヤ2 ポリシーベースリダイレクトは、CLI ではサポートされていません。
- レイヤ1/レイヤ2 PBR アクティブ/アクティブ PBR 接続先は、カプセル化のフラグメントがリモートリーフスイッチでサポートされていないため、リモートリーフスイッチには接続できません。プロバイダーおよびコンシューマーのサービスノードは、引き続きリモートリーフスイッチに接続できます。
- アクティブ/スタンバイモード（ハイアベイラビリティ）で構成されたレイヤ1/レイヤ2対称 PBR の場合、重みベースの対称 PBR はサポートされません。アクティブおよびスタンバイ PBR の接続先には重みを設定しないことをお勧めします。
- アクティブ/アクティブモードで設定されたレイヤ1/レイヤ2対称 PBR の場合、重みベースの対称 PBR がサポートされます。
- 動的な VLAN 割り当てはサポートされていません。

アクティブ/スタンバイレイヤ1/レイヤ2 PBR 設計の概要

Cisco Application Policy Infrastructure Controller (APIC) リリース 4.1 以降のリリースでは、レイヤ1/レイヤ2ポリシーベースリダイレクト (PBR) およびアクティブ/スタンバイ PBR 設計がトラッキングでサポートされています。

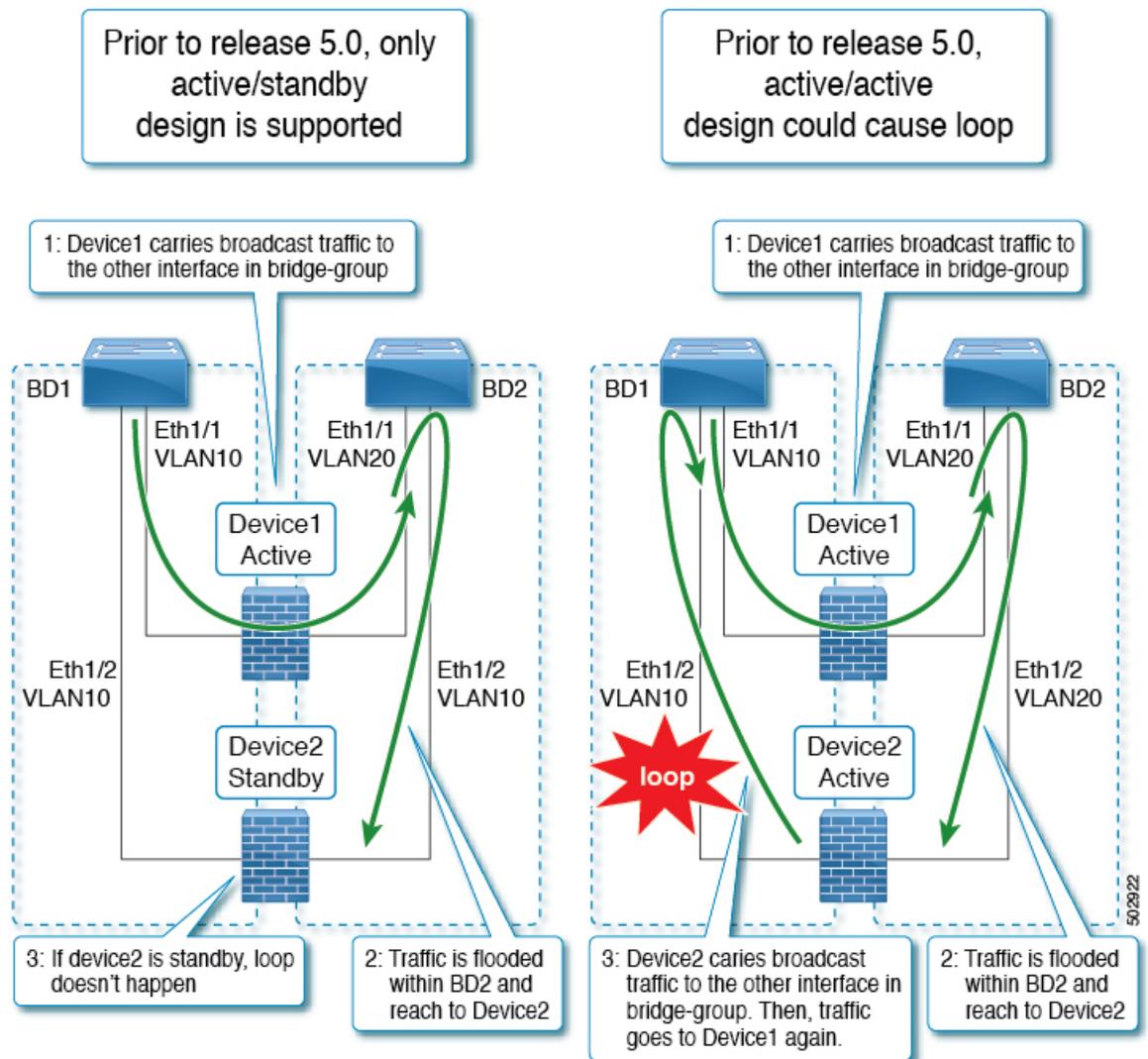
レイヤ1/レイヤ2 PBR の場合、レイヤ2 ping の送信元および接続先 MAC アドレスは PBR 接続先 MAC アドレスです。PBR ノードが稼働してトラフィックを伝送している場合、レイヤ2 ping は正常に Cisco Application Centric Infrastructure (ACI) ファブリックに戻るようになります。その後、Cisco ACI ファブリックは PBR 接続先が使用可能であることを認識します。レイヤ1/レイヤ2 PBR を使用して挿入するアクティブおよびスタンバイのハイアベイラビリティレイヤ1/レイヤ2サービスノードがあり、トラッキングが有効になっている2つの PBR 接続先が

ある場合、スタンバイデバイスはトラフィックを転送しないため、アクティブノードに接続されているパスの1つのみが稼働することになります。その結果、トラフィックはアクティブノードに接続されているインターフェイスにリダイレクトされます。

フェールオーバーが発生し、スタンバイがアクティブロールを引き継ぐ場合、トラッキングステータスに変化し、トラフィックは新しいアクティブノードに接続されているインターフェイスにリダイレクトされます。

Cisco APIC リリース 5.0(1) より前のリリースでは、次の図に示すように、同一のサービスブリッジドメインペアに複数のレイヤ1/レイヤ2 デバイスがアクティブ/スタンバイ設計で存在する場合、ブリッジドメイン内でトラフィックがフラッディングされ、トラフィックが2番目のレイヤ4～7サービスデバイスに到達しても、この2番目のレイヤ4～7サービスデバイスがスタンバイモードであるため、ループは発生しません。

Cisco APIC リリース 5.0(1) より前のリリースでアクティブ/スタンバイ設計がサポートされない理由は、アクティブ/スタンバイ設計で、同じサービスブリッジドメインペアに複数のレイヤ1/レイヤ2 デバイスがある場合、2番目のデバイスがレイヤ4～レイヤ7サービスデバイスはトラフィックを他のブリッジドメインの他のインターフェイスに転送し、トラフィックは最初のデバイスに到達してループが発生するためです。



アクティブ/アクティブレイヤ1/レイヤ2対称PBR設計の概要

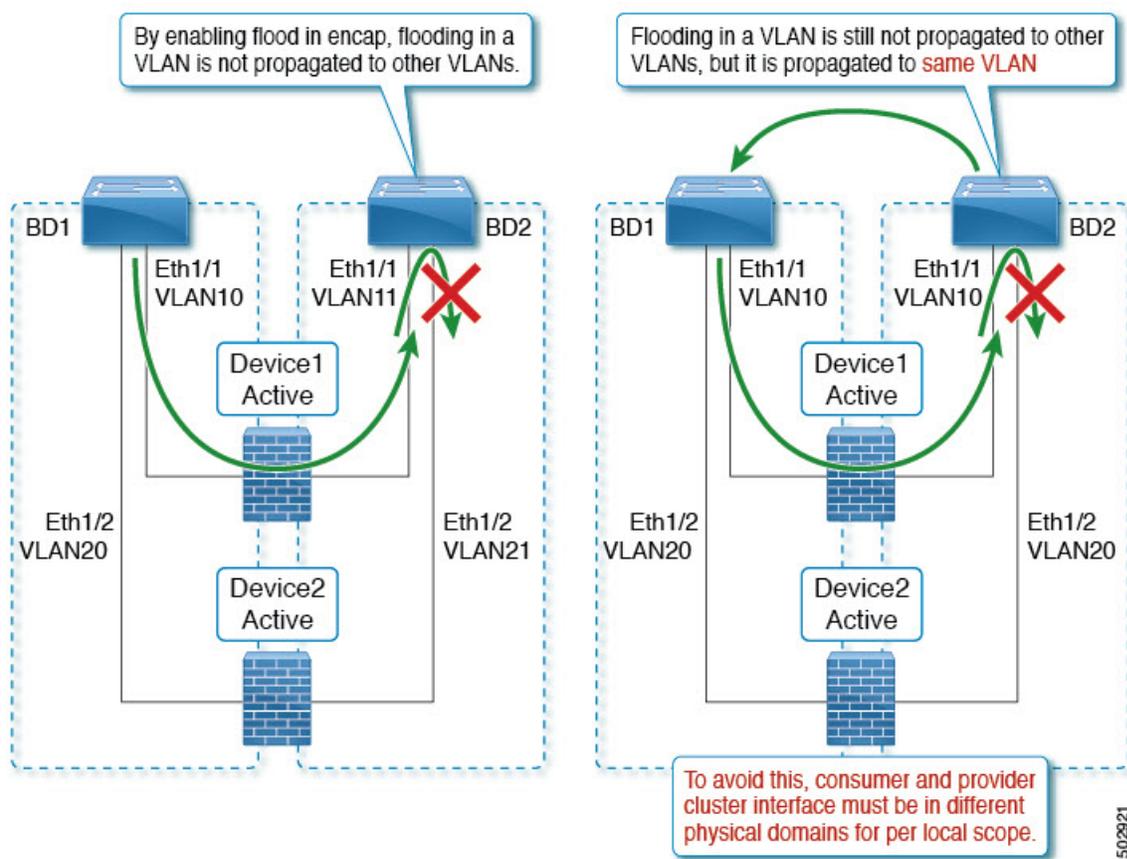
Cisco APIC リリース 5.0(1) 以降のリリースでは、サービスチェーン内のレイヤ1/レイヤ2 デバイスは、アクティブ/アクティブの対称PBR設計で動作できます。対称PBRは、ハッシュに基づいて個々のデバイスへのトラフィックを分散するために使用されます。

このモードでは、トラフィックフローのハイアベイラビリティと効率的な分散が実現できます。APIC リリース 5.0(1) では、対称PBR 関連機能として、しきい値、ダウンアクション、バックアップPBR ポリシー (N+M ハイアベイラビリティ) などがサポートされています。レイヤ1 PBR アクティブ/アクティブモードの場合、コンシューマーコネクタとプロバイダコネクタは異なる物理ドメインにある必要があります。

レイヤ1/レイヤ2のアクティブ/アクティブ設計を展開するには、レイヤ4～レイヤ7論理デバイス クラスタでアクティブ/アクティブモードを有効にする必要があります。クラスタ内の具象デバイスインターフェイスごとにカプセル化する必要があります。

例：同じブリッジドメインペアで、カプセル化が有効なフラッディングを使用すると、フラッディングは VLAN 内で伝達され、他の VLAN には伝達されません。そのため、同じブリッジドメイン内の複数のアクティブデバイスを接続できます。

レイヤ1 アクティブ/アクティブモードの場合、外部コネクタと内部コネクタは同じカプセル化を持っています。アクティブノードごとに異なる VLAN を使用する場合、カプセル化が有効なフラッディングだけでは、ループを防止するには不十分です。この問題を回避するには、デバイスの両レッグを異なる物理ドメインと異なる VLAN 名前空間に関連付ける必要があります（実際の VLAN の範囲はそのままにできます）。これにより、レッグごとに異なる fabEncap が生成され、トラフィックループを防止します。



GUI を使用したレイヤ1/レイヤ2デバイスの設定

始める前に

- Cisco APIC GUI を使用してレイヤ1/レイヤ2デバイスを作成し、具象デバイスインターフェイスを作成します。

ステップ1 メニューバーで、[テナント (Tenants)] > [すべてのテナント (ALL Tenants)] の順に選択します。 >

- ステップ2** ナビゲーションウィンドウで、[テナント (Tenant)]/[テナント名 (tenant_name)]>[サービス (Services)]>[L4-L7]の順に選択します。
- ステップ3** 右クリックで、[デバイス (Devices)]>[L4 ~ L7 デバイスの作成 (Create L4-L7 Devices)]の順に選択します。
- ステップ4** [L4 ~ L7 デバイスの作成 (Create L4-L7 Devices)]ダイアログボックスに、次のフィールドを入力にします。
- [名前 (Name)]フィールドで、レイヤ4～レイヤ7デバイスクラスタの名前を指定します。
 - [サービスタイプ (Service Type)]領域で、[Other (その他)]を選択します。
 - [デバイスタイプ (Device Type)]で[物理 (Physical)]を選択します。
 - [物理ドメイン (Physical Domain)]で、[物理ドメイン名 (physical domain name)]を選択します。
 - [コンテキスト認識 (Context Aware)]で[単一 (Single)]を選択します。
 - [機能タイプ (Function Type)]で、[L1]または[L2]を選択します。
 - チェックボックスをオンにして、**アクティブ/アクティブモード**を有効にします。
- ステップ5** 具象デバイスインターフェイスを作成します。レイヤ1またはレイヤ2の**アクティブ/アクティブモード**の場合は、右側の作業ペインの[デバイス (Devices)]モードで[+]をクリックします。[具象デバイスの作成 (Create Concrete Device)]ダイアログボックスが表示されます。
- [名前 (Name)]フィールドに、デバイス名を入力します。
 - [+]をクリックして、具象デバイスインターフェイスにカプセル化を作成します。名前と具象インターフェイス名を入力します。
- レイヤ1/レイヤ2 PBRはツーアーム設計のみをサポートするため、[+]をもう一度クリックして、別の具象インターフェイスを作成します。名前、インターフェイスパス、カプセル化を入力します。[更新 (Update)]>[OK]の順にクリックします。
- アクティブデバイスをさらに追加するには、手順5aと手順5bを繰り返します。
- クラスタで、[+]をクリックしてコンシューマークラスターインターフェイスを作成し、コンシューマー具象インターフェイスを選択します。レイヤ1モードの場合、物理ドメインを選択します。
- [+]をもう一度クリックしてプロバイダークラスターインターフェイスを作成し、プロバイダー具象インターフェイスを選択します。レイヤ1モードの場合は、別の物理ドメインを選択します。
- (注) レイヤ1アクティブ/アクティブデバイスの場合、2つの異なるVLANプールにマッピングされた2つの物理ドメインを作成しますが、同じVLAN範囲を維持します。レイヤ2アクティブ/アクティブデバイスの場合、物理ドメインは手順4eで選択されます。
- ステップ6** [Finish]をクリックします。
-

APIC GUI を使用したレイヤ 1/レイヤ 2 PBR の設定

始める前に

- レイヤ 1/レイヤ 2 機能タイプを使用して、L4 ~ L7 デバイスおよびサービスグラフを作成します。詳細は、「GUI を使用したポリシーベースリダイレクトの設定の設定手順」を参照してください。

-
- 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** 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 3** 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 4** [L4 ~ L7 ポリシーベースリダイレクトの作成 (Create L4-L7 Policy Based Redirect)] ダイアログボックスで、次のフィールドを入力します。
- [名前 (Name)] フィールドに、名前を入力します。
 - [接続先タイプ (Destination Type)] フィールドで、[L1] または [L2] を選択します。
 - IP SLA モニタリングポリシーで、L2 ping モニタリングポリシーを作成します。
 - [名前 (Name)] フィールドに、名前を入力します。
 - [SLA タイプ (SLA Type)] で、[L2Ping] を選択します。
 - [SLA 頻度 (SLA Frequency)] はオプションです。
 - [L1 ~ L2 接続先 (L1-L2 Destination)] で、[+] をクリックして接続先を追加します。
名前、リダイレクトヘルスグループ、具象インターフェイスを入力します。MAC アドレスの構成はオプションです。
 - [OK] をクリックします。
(注) 実際のインターフェイスの MAC アドレスは入力しないでください。APIC が自動的に MAC を生成するように空白のままにするか、外部 PBR ポリシー MAC A および内部 PBR ポリシー MAC B にダミーの MAC アドレスを入力します。これらの MAC アドレスはファイアウォール設定で使用されることに注意してください。
- ステップ 5** [送信 (Submit)] をクリックします。
- ステップ 6** ナビゲーションウィンドウで、[サービス (Services)] > [L4 ~ L7 (L4-L7)] > [デバイス選択ポリシー (Device Selection Policies)] > [論理デバイスコンテキスト名 (Logical Device Context_name)] の順に選択します。
- ステップ 7** 論理デバイスを展開し、コンシューマーまたはプロバイダーの [L4 ~ L7 ポリシーベースリダイレクト (L4-L7 Policy-Based Redirect)] フィールドにレイヤ 1/レイヤ 2 PBR ポリシーを適用します。
- ステップ 8** [送信 (Submit)] をクリックします。
-

CLI を使用したレイヤ1/レイヤ2 PBR の ASA の設定

始める前に

- 一般的な構成の場合、サービスデバイスはレイヤ2 ping トラッキングパケットを転送できる必要があります。

レイヤ2 ping、ethertype 0x0721 がトラッキングに使用されます。レイヤ2 ping は、サービスデバイスを通するリーフノード間で交換されます。したがって、レイヤ1/レイヤ2 デバイスでは ethertype 0x0721 を許可する必要があります。

- 静的 MAC 構成が必要です。
- 次に、ASA がレイヤ2 モードで L4 ~ L7 デバイスとして使用される ASA 設定の例を示します。

ステップ1 ASA インターフェイス（サービスレッグ）は、同じブリッジグループで設定する必要があります。

例：

```
interface GigabitEthernet0/0
nameif externalIf
brdige-group 1

interface GigabitEthernet0/1
nameif internalIf
bridge-group 1
```

ステップ2 ASA は、レイヤ2 ping トラフィックの送信元 MAC アドレスを学習します。レイヤ2 ping トラフィックは同じ送信元 MAC を使用してコンシューマーとプロバイダーの方向をトラッキングするため、ASA で作成されるエントリが競合するのを避けるために、MAC 学習を無効にすることをお勧めします。

次の例では、**externalIf** は、レイヤ1/レイヤ2 サービスノードのコンシューマーコネクタとして使用される ASA のインターフェイス名で、**internalIf** は、レイヤ1/レイヤ2 サービスノードのプロバイダーコネクタとして使用される ASA のインターフェイス名です。**externalIf** および **internalIf** で MAC 学習を無効にします。L2 ping は、外部レッグと内部レッグの両方をトラッキングする場合に同じソース MAC を使用します。

レイヤ2 ping が同じ送信元 MAC を使用して外部と内部をトラッキングするため、ASA で競合するエントリが作成されるのを避けるために、MAC 学習は無効になっています。

例：

```
mac-learn externalIf disable
mac-learn internalIf disable
```

ステップ3 L2 ping カスタム EtherType を許可するように ASA ルールを設定します。

例：

```
access-list Permit-Eth ethertype permit any
access-group Permit-Eth in interface externalIf
access-group Permit-Eth in interface internalIf
```

ステップ4 リダイレクトされたトラフィックとレイヤ2 (Layer2) ping パケットは PBR 接続先 MAC を使用し、ASA はコンシューマー インターフェイスとプロバイダー インターフェイスをブリッジします。ASA 透過モードは、一般に不明な接続先 MAC をフラッディングしますが、L2 PBR では、PBR 接続先 MAC が実際にはネットワークに存在しないため、この方法は使用できません。したがって、レイヤ2 ping および PBR トラフィックが ASA によってすべてのケースで適切にブリッジされるように静的 MAC エントリを使用することを勧めします。

例：

```
mac-address-table static externalIf (MAC B)
mac-address-table static internalIf (MAC A)
```

(注) ASA などのサービスデバイスの設定とは別に、リーフとサービスデバイスの中に中間スイッチがある場合、中間スイッチによってトラフィックを伝送できるようにする必要があります。中間スイッチで静的 MAC 構成または無差別モード構成が必要になる場合があります。

CLI を使用したリーフのレイヤ1/レイヤ2 PBR ポリシーの確認

この手順のコマンド例では、レイヤ1およびレイヤ2のポリシーベースリダイレクトノードを設定します。

ステップ1 スイッチに PBR グループと接続先情報が設定されているかを確認します。

例：

```
sdk74-leaf4# show service redir info
GrpID Name                destination                operSt
=====
1    destgrp-1             dest-[50.50.50.1]-[vxlan-2719744]]  enabled
2    destgrp-2             dest-[20.20.20.1]-[vxlan-2719744]]  enabled
Name                vrfEncap                operSt                bdVnid                ip                vMac                vrf
=====
dest-[20.20.20.1]-[vxlan-2719744]]  vxlan-16514958  20.20.20.1  00:00:14:00:00:01  coke1:cokectx1
vxlan-2719744  enabled
dest-[50.50.50.1]-[vxlan-2719744]]  vxlan-16711542  50.50.50.1  00:00:3C:00:00:01  coke1:cokectx1
vxlan-2719744  enabled
```

ステップ2 正しいアクションとグループ情報でゾーニングルールが構成されているかを確認します。

例：

```
sdk74-leaf4# show zoning-rule | grep redir
4103          49155          49154          18          enabled          2719744
redir(destgrp-2)  fully_qual(6)
4106          49154          49155          17          enabled          2719744
redir(destgrp-1)  fully_qual(6)
```

ステップ3 PBR の Aclqos サブコマンド：

例：

```
module-1# show system internal aclqos services redir ?
<CR>
```

REST API を使用したレイヤ 1/レイヤ 2 PBR の設定

```

dest    Dest related info
group   Group related info

module-1# show system internal aclqos services redir group 1

Flag Legend :
0x1: In SDK
0x10: In local DB
0x20: Delete pending
0x40: Dummy adj

***** Service key redir-group(1) *****
Service flags: 0x11
Num of reference: 0x1
Num of path: 1
path 0 key: redir-dest-ipv4(vrf vnid vxlan-2719744 prefix-50.50.50.1)

module-1# show system internal aclqos services redir dest 2719744 50.50.50.1
Flag Legend :
0x1: In SDK
0x10: In local DB
0x20: Delete pending
0x40: Dummy adj
***** Service key redir-dest-ipv4(vrf vnid vxlan-2719744 prefix-50.50.50.1) *****
Service flags: 0x10
Num of reference: 0x1
Num of path: 1
Ifindx: 0x18010007
Bd_vnid: 16711542
Vmac: 00:00:3c:00:00:01

```

ステップ 4 ゾーニングルールコマンド:

例:

```

module-1# show system internal aclqos zoning-rules 4106
ASIC type is Sug
=====
Rule ID: 4106 Scope 3 Src EPG: 49154 Dst EPG: 49155 Filter 17
Redir group: 1

Curr TCAM resource:
=====
unit_id: 0
=== Region priority: 1539 (rule prio: 6 entry: 3)===
sw_index = 44 | hw_index = 44
=== SDK Info ===
Result/Stats Idx: 81876
30
Tcam Total Entries: 1
HW Stats: 0

```

REST API を使用したレイヤ 1/レイヤ 2 PBR の設定

レイヤ 1/レイヤ 2 ポリシーベースリダイレクト構成:

例:

```

<polUni>
  <fvTenant name="coke" >

    <!--If L1/L2 device in active-active mode -- >
    <vnsLDevVip name="N1" activeActive="yes" funcType="L1" managed="no">
    </vnsLDevVip>
    <!--If L1/L2 device in active-standby mode -- >
    <vnsLDevVip name="N1" activeActive="no" funcType="L1" managed="no">
    </vnsLDevVip>

    <vnsAbsGraph descr="" dn="uni/tn-coke/AbsGraph-WebGraph" name="WebGraph" ownerKey=""
ownerTag="" uiTemplateType="UNSPECIFIED">

      <!--For L2 device -- >
      <vnsAbsNode descr="" funcTemplateType="OTHER" funcType="L2" isCopy="no" managed="no" name="N1"
ownerKey="" ownerTag="" routingMode="Redirect" sequenceNumber="0" shareEncap="no">
      </vnsAbsNode>

      <!--For L1 device -- >
      <vnsAbsNode descr="" funcTemplateType="OTHER" funcType="L1" isCopy="no" managed="no" name="N1"
ownerKey="" ownerTag="" routingMode="Redirect" sequenceNumber="0" shareEncap="no">
      </vnsAbsNode>

    </vnsAbsGraph>

    <fvIPSLAMonitoringPol name="Pol2" slaType="l2ping"/>
  <vnsSvcCont>
  <vnsRedirectHealthGroup name="2" />
    <vnsSvcRedirectPol name="N1Ext" destType="L2">
      <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-Pol2"/>
    <vnsL1L2RedirectDest destName="1">
      <vnsRsL1L2RedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-2"/>
      <vnsRsToCIf tDn="uni/tn-coke/lDevVip-N1/cDev-ASA1/cIf-[Gig0/0]"/>
    </vnsL1L2RedirectDest>
  </vnsSvcRedirectPol>

    <vnsSvcRedirectPol name="N1Int" destType="L2">
      <vnsRsIPSLAMonitoringPol tDn="uni/tn-coke/ipslaMonitoringPol-Pol2"/>
    <vnsL1L2RedirectDest destName="2">
      <vnsRsL1L2RedirectHealthGroup tDn="uni/tn-coke/svcCont/redirectHealthGroup-2"/>
      <vnsRsToCIf tDn="uni/tn-coke/lDevVip-N1/cDev-ASA1/cIf-[Gig0/1]"/>
    </vnsL1L2RedirectDest>
  </vnsSvcRedirectPol>
  </vnsSvcCont>
</fvTenant>
</polUni>

```

ポリシーベースリダイレクトとサービスノードのトラッキング

Cisco Application Policy Infrastructure Controller (APIC) 2.2(3) および 3.1(1) リリース (ただし、3.0 リリースを除く) 以降のリリースでは、ポリシーベースリダイレクト機能 (PBR) は、サービスノードをトラッキングする機能をサポートしています。トラッキングにより、ダウンしているサービスノードへのトラフィックのリダイレクトを防ぐことができます。サービスノード (PBR 接続先) がダウンした場合、PBR ハッシュはポリシーで使用可能な PBR 接続先の選択を開始

できます。この機能を使うには、Cisco Nexus 9300-EX、-FX、またはそれ以降のプラットフォーム リーフスイッチが必要です。

サービスノードは、デュアル IP アドレススタッキングをサポートできます。したがって、この機能には、IPv4 アドレスと IPv6 アドレスの両方を同時にトラッキングできます。IPv4 アドレスと IPv6 アドレスの両方が「up (動作中)」の場合、PBR 接続先は「up (動作中)」とマークされます。

スイッチでは、Cisco IP SLA モニタリング機能を内部的に使用して、PBR トラッキングをサポートします。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、リダイレクト接続先ノードを「ダウン (down)」としてマークします。トラッキング機能では、サービスノードが接続を再開すると、リダイレクト先をノード「動作中 (up)」としてマークします。サービスノードが「ダウン (down)」とマークされている場合、そのノードはトラフィックの送信またはハッシュに使用されません。代わりに、トラフィックはリダイレクト先ノードのクラスタ内の別のサービスノードに送信またはハッシュされます。

一方向のトラフィックのブラックホール化を避けるために、サービスノードの入力および出力のリダイレクト接続先ノードをリダイレクトヘルスポリシーに関連付けることができます。そうすることで、入力または出力のリダイレクト接続先ノードがダウンした場合、もう一方のリダイレクト接続先ノードも「ダウン (down)」としてマークされます。したがって、入力トラフィックと出力トラフィックの両方が、リダイレクト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されます。

トラッキングには次のプロトコルを使用できます。

- ICMP (レイヤ 3 PBR の場合)
- TCP (レイヤ 3 PBR の場合)
- L2ping (レイヤ 1/2 PBR の場合)
- HTTP URI (レイヤ 3 PBR の場合、5.2(1) 以降のリリース)

ポリシーベースリダイレクトとヘルスグループによるサービスノードのトラッキング

ポリシーベースリダイレクト (PBR) サービスノードトラッキングを使用すると、障害が発生した PBR ノードへのトラフィックのリダイレクトを防止できます。PBR ノードのコンシューマーコネクタまたはプロバイダーコネクタがダウンした場合、障害が発生したノードを通過したトラフィックがブラックホールになる可能性があります。トラフィックがブラックホール化されるのを防ぐために、Cisco Application Centric Infrastructure (ACI) では両方向のトラフィックに PBR ノードを使用しないようにします。レイヤ 4 からレイヤ 7 へのサービスデバイスには、別のインターフェイスがダウンした場合にインターフェイスを停止できるものもあります。これを使用して、トラフィックのブラックホール化を防ぐことができます。PBR ノードにこの機能がない場合、コンシューマーコネクタまたはプロバイダーコネクタのいずれかがダウンしている場合は、ヘルスグループ機能を使用してノードの PBR を無効にする必要があります。

各 PBR 接続先 IP と MAC アドレスは、ヘルスグループに含めることができます。たとえば、2つの PBR ノードの接続先があるとします。1つは、Health-group1 にあり、コンシューマーコネクタとして 172.16.1.1 を持ち、プロバイダーコネクタとして 172.16.2.1 を持っています。もう1つは、Health-group2 にあり、コンシューマーコネクタとして 172.16.1.2 を持ち、プロバイダーコネクタとして 172.16.2.2 を持っています。同じヘルスグループ内の PBR 接続先のいずれかがダウンしている場合、そのノードは PBR に使用されません。

サービスノードをトラッキングするためのポリシーベースリダイレクトとしきい値の設定

サービスノードをトラッキングするためのポリシーベースリダイレクト(PBR)ポリシーを構成する場合、次のしきい値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、パケットはリダイレクトされずに許可されます。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1つがダウンすると、アベイラビリティのパーセンテージは3つのうちの1つ（または 33%）が低下し、最小しきい値を下回ります。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、最大しきい値が 80% の場合、リダイレクトポリシーの接続先グループを動作状態に戻すには、最大しきい値のパーセンテージよりも大きいパーセンテージにする必要があります。

重みベースの PBR の場合、しきい値は使用可能な PBR 接続先のすべての重みの合計を、設定された PBR 接続先のすべての重みの合計で割った値になります。以下の例では、すべての接続先が稼働している場合、しきい値は 100% になります。接続先 1 がダウン（重み 4）で、しきい値が 60% であるとしてみます。

Destination	重量	Traffic %-age (おおよその)
接続先 1	4	40
接続先 2	3	30

Destination	重量	Traffic %-age (おおよその)
接続先 3	2	20
接続先 4	1	10

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限事項

サービスノードでポリシーベースリダイレクト(PBR)トラッキングを使用する場合は、次の注意事項と制限事項に従ってください。

- 接続先を共有する接続先グループには、同じヘルスグループと IP SLA モニタリングポリシーが設定されている必要があります。
- リリース 4.0(1) 以降のリリースでは、リモートリーフスイッチ設定は PBR トラッキングをサポートしますが、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です。「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) 以降のリリースでは、リモートリーフスイッチ設定は PBR の復元力のあるハッシュをサポートします。
- Cisco ACI マルチポッドファブリックセットアップがサポートされています。
- Cisco ACI マルチサイトセットアップはサポートされていますが、PBR の接続先を別のサイトにすることはできません。
- L3Out は、コンシューマー EPG およびプロバイダー EPG でサポートされています。
- PBR は、リーフスイッチで最大 100 のトラッキング可能な IP アドレスをサポートし、Cisco Application Centric Infrastructure (ACI) ファブリックで 400 のトラッキング可能な IP アドレスをサポートします。
- Cisco ACI ファブリック内のサービスグラフィンスタンスの最大数については、お客様がお使いのリリース向けの『Cisco APIC の検証済みスケーラビリティガイド』を参照してください。
- デバイスごとのサービスグラフィンスタンスの最大数については、お客様がお使いのリリース向けの『Cisco APIC の検証済みスケーラビリティガイド』を参照してください。
- PBR ポリシーごとに最大 40 のサービスノードを設定できます。
- サービスチェーンごとに最大 3 つのサービスノードを設定できます。
- 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。
- 次のしきい値ダウン時のアクションがサポートされています。

- バイパス (bypass action)
 - 拒否(deny action)
 - 許可(permit action)
- 複数のPBRポリシーが同じVRFインスタンスに同じPBR接続先IPアドレスを持つ場合、そのポリシーはPBR接続先に対して同じIP SLAポリシーとヘルスグループを使用する必要があります。

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。ナビゲーションウィンドウで、[ポリシー (Policies)] > [プロトコル (Protocol)] > [L4 ~ L7 ポリシーベースリダイレクト (L4-L7 Policy Based Redirect)] の順に選択します。
- 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:
- [名前 (Name)] フィールドに、ポリシーベースリダイレクト (PBR) ポリシーの名前を入力します。
 - 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適切に設定します。

(注) 接続先を共有する接続先グループには、同じIP SLA モニタリングポリシーが設定されている必要があります。
 - 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。
 - [L3 接続先 (L3 Destinations)] の場合は、[+] をクリックして、[リダイレクトされたトラフィックの接続先の作成 (Create Destination of Redirected Traffic)] を表示します。
 - [リダイレクトされたトラフィックの接続先の作成 (Create Destination of Redirected Traffic)] ダイアログボックスに、適切な値を入力します。

[IP] および [追加の IPv4/IPv6 (Additional IPv4/IPv6)] フィールドが提供され、IPv4 または IPv6 アドレスを指定できます。

(注) [追加の IPv4/IPv6 (Additional IPv4/IPv6)] フィールドは必須ではありません。レイヤ4 ~ レイヤ7サービスデバイスに複数のIPアドレスがあり、Cisco Application Centric Infrastructure(ACI) でそれらの両方を確認する場合は、このフィールドを使用します。

[IP] と [追加の IPv4/IPv6 (Additional IPv4/IPv6)] パラメータの両方が設定されている場合、PBR 接続先を「稼働中」としてマークするには、両方が稼働している必要があります。
 - [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。

(注) 接続先を共有する接続先グループには、同じヘルスグループが設定されている必要があります。

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。

レイヤ4～レイヤ7 PBR とサービスノードのトラッキングは、リダイレクトヘルスグループポリシーを PBR ポリシーにバインドし、リダイレクト接続先グループをトラッキングする設定を有効にした後で行います。

GUI を使用したリダイレクトヘルスグループの設定

ステップ1 メニューバーで、[テナント (Tenant)] > [テナント名 (Tenant_name)] をクリックします。ナビゲーションウィンドウで、[ポリシー (Policies)] > [プロトコル (Protocol)] > [L4～L7 リダイレクトヘルスグループ (L4-L7 Redirect Health Groups)] の順に選択します。

ステップ2 [L4～L7 リダイレクトヘルスグループ (L4-L7 Redirect Health Groups)] を右クリックし、[L4～L7 リダイレクトヘルスグループの作成 (Create L4-L7 Redirect Health Group)] を選択します。

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。
- レイヤ4～レイヤ7サービスのリダイレクトヘルスポリシーが設定されています。

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：

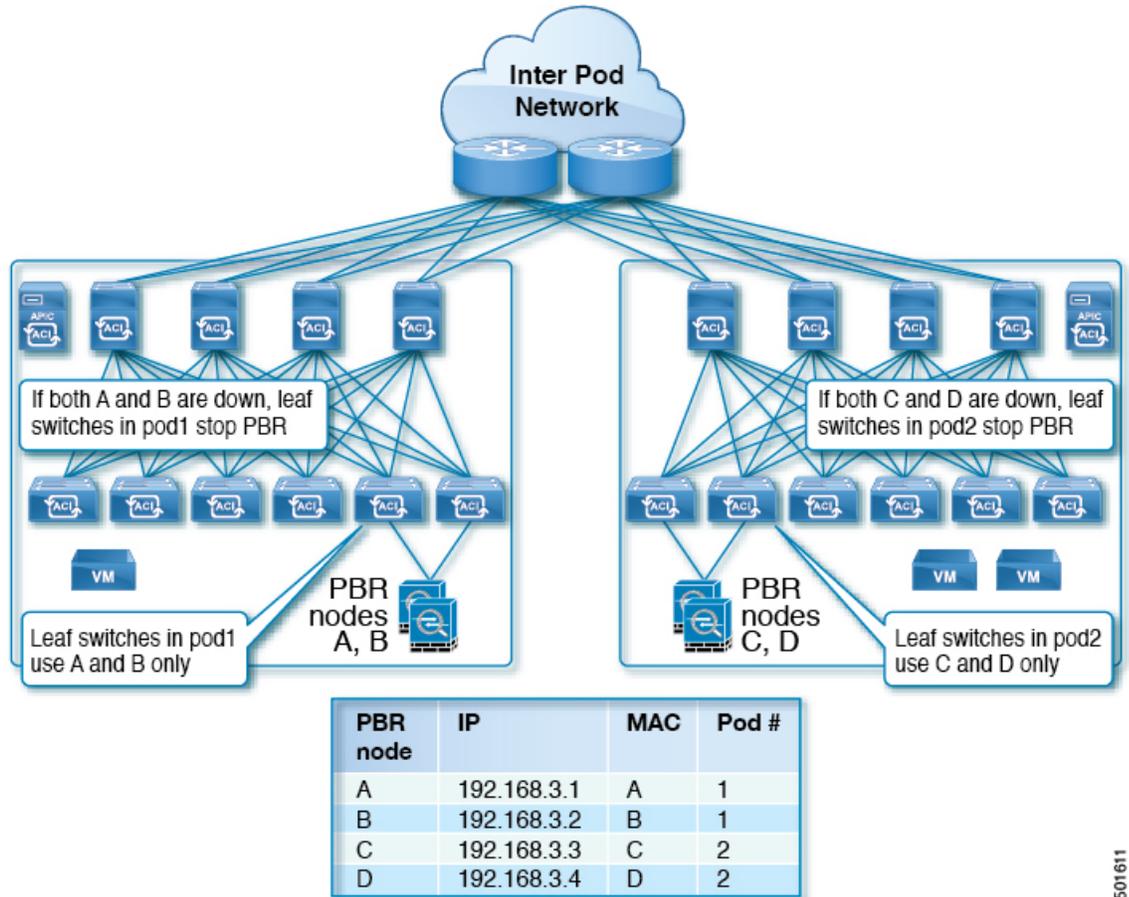
```
<polUni>
  <fvTenant name="t1" >
    <fvIPSLAMonitoringPol name="tcp_Freq60_Poll" slaType="tcp" slaFrequency="60" slaPort="2222" />
    <vnsSvcCont>
      <vnsRedirectHealthGroup name="fwService1"/>
      <vnsSvcRedirectPol name="fwExt" hashingAlgorithm="sip" thresholdEnable="yes"
        minThresholdPercent="20" maxThresholdPercent="80">
        <vnsRedirectDest ip="40.40.40.100" mac="00:00:00:00:01">
          <vnsRsRedirectHealthGroup tDn="uni/tn-t1/svcCont/redirectHealthGroup-fwService1"/>
        </vnsRedirectDest>
        <vnsRsIPSLAMonitoringPol tDn="uni/tn-t1/ipslaMonitoringPol-tcp_Freq60_Poll"/>
      </vnsSvcRedirectPol>
      <vnsSvcRedirectPol name="fwInt" hashingAlgorithm="sip" thresholdEnable="yes"
        minThresholdPercent="20" maxThresholdPercent="80">
        <vnsRedirectDest ip="30.30.30.100" mac="00:00:00:00:02">
          <vnsRsRedirectHealthGroup tDn="uni/tn-t1/svcCont/redirectHealthGroup-fwService1"/>
        </vnsRedirectDest>
        <vnsRsIPSLAMonitoringPol tDn="uni/tn-t1/ipslaMonitoringPol-tcp_Freq60_Poll"/>
      </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 11:2個のポッドのロケーション対応 PBR 設定の例



501611

ロケーション認識型 PBR の注意事項

ロケーション認識 PBR を使用する場合は、次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 ホストアダプ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。

外部 EPG から EPG へのトラフィックの VRF 内コントラクトや、EPG 間のトラフィックの VRF 内コントラクトなど、着信トラフィックとリターントラフィックが同じリーフノードに適用されるコントラクトには、ロケーション認識 PBR を使用します。それ以外の場合では、トラフィックの対称性が失われる可能性があります。

- 複数の PBR ポリシーで同じ VRF に同じ PBR 接続先 IP アドレスを持つ場合、すべてのポリシーでポッド ID 認識リダイレクトを有効にするか、ポッド ID 認識リダイレクトを無効にする必要があります。同じ (VRF、IP アドレス) ペアは、有効の Pod ID 認識リダイレ

クトポリシーと無効のPod ID認識リダイレクトポリシーで同時に使用することはできません。たとえば、次の構成はサポートされていません。

- PBR-policy1には、VRF AのPBR接続先192.168.1.1があり、Pod ID認識リダイレクションが有効で、POD 1に192.168.1.1が設定されています。
- PBR-policy2では、VRF AにPBR接続先192.168.1.1があり、Pod ID認識リダイレクションが無効になっています。

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ア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) **[重み (Weight)]** フィールドに値を入力します。デフォルト値は1です。指定できる範囲は1~10です。

このフィールドは、**[ポッドID認識リダイレクトを有効にする (Enable Pod ID Aware Redirection)]** チェックボックスがオンになっている場合にのみ表示されます。
 - i) **[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。
 - j) **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 :

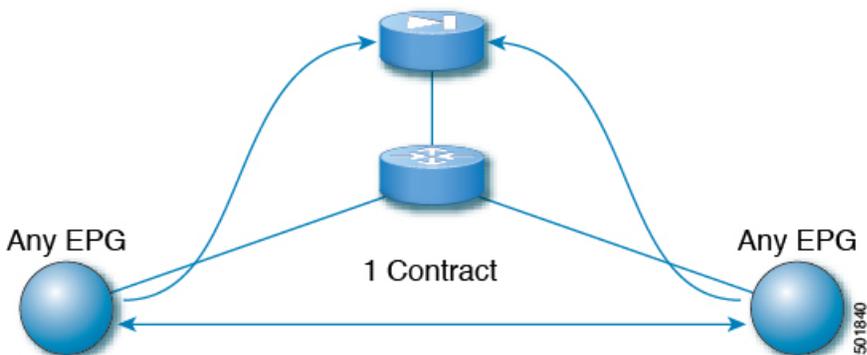
```
<polUni>
  <fvTenant name="coke" >
    <fvIPSLAMonitoringPol name="icmp_Freq60_Pol1" slaType="icmp" slaFrequency="60"/>
    <vnsSvcCont>
      <vnsRedirectHealthGroup name="fwService1"/>
      <vnsSvcRedirectPol name="fwExt" hashingAlgorithm="sip" thresholdEnable="yes"
minThresholdPercent="20" maxThresholdPercent="80" 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

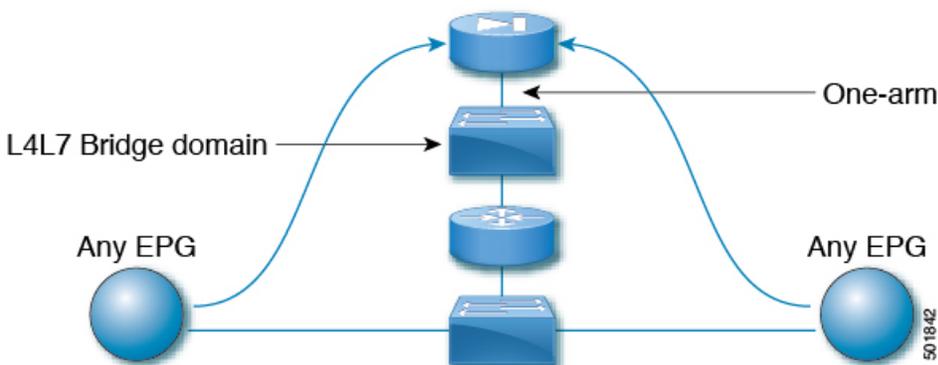
トグループからのすべてのトラフィックを転送するには、同じ VRF インスタンスでグループ。vzAny は「any EPG」と呼ばれることがあります。

図 12: 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、任意の一对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 13: 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。

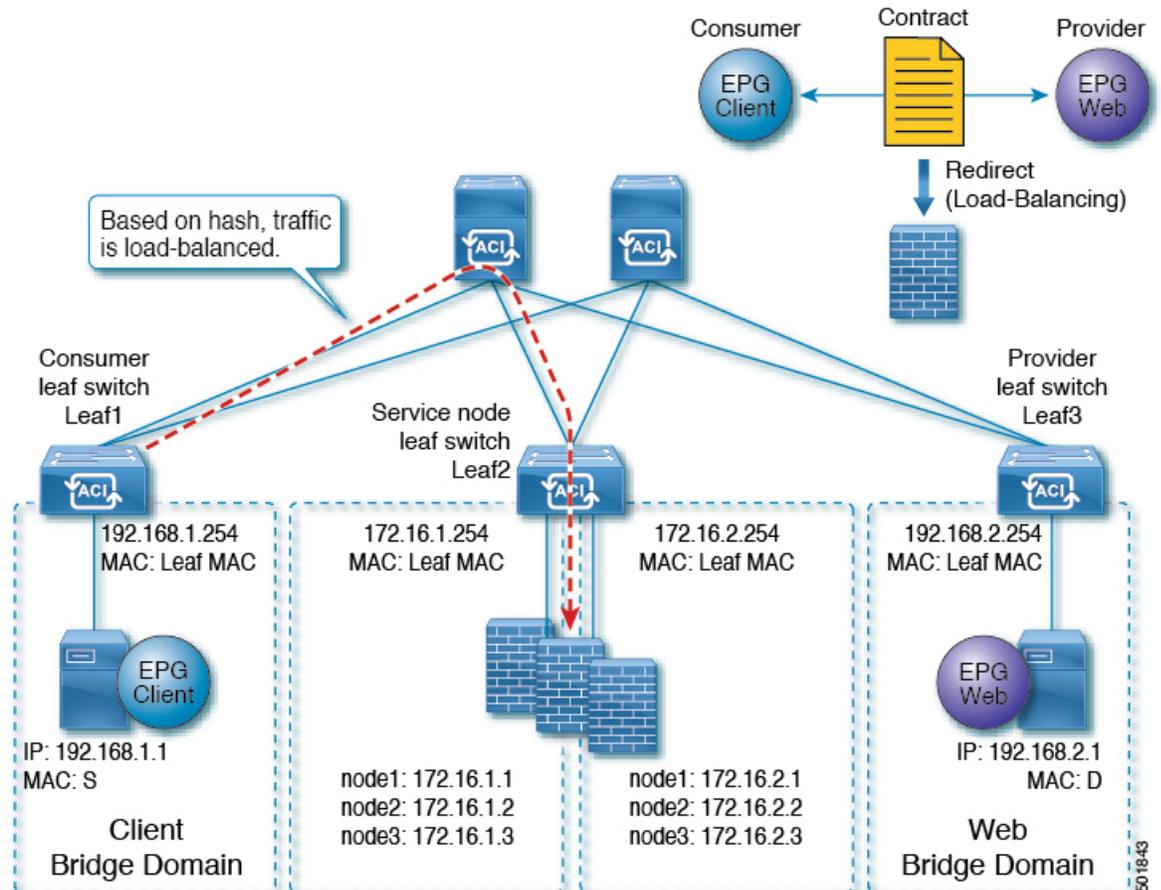
ポリシーベースのリダイレクトポリシーを使用してサービスグラフを適用すると、次の機能も有効になります。

- ファイアウォールクラスタリング

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

- 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 14: 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

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～レイヤ 7 サービスデバイスと 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～レイヤ 7 サービスデバイスは、ワンアームモードで展開する必要があります。
- 一般的な場合、多くの EPG が同じコントラクトを消費して提供する代わりに、vzAny コントラクトを使用して、多くの EPG から多くの EPG トラフィックへの PBR を有効にすることをお勧めします。ただし、同じ EPG で、コンシューマーコントラクトとプロバイダーコントラクトの両方としてサービスグラフが付加されているコントラクトを持たないでください。

この推奨事項は、多くのプロバイダーおよびコンシューマー EPG を持つコントラクトの設定変更に影響を与える可能性があるために設けられています。Cisco Application Policy Infrastructure Controller (APIC) の 1 つの構成変更が同時に複数のゾーニングルール変更に関連する場合、Cisco APIC では、特定のリーフノードのハードウェアのプログラミングを完了するのに時間が必要です。

- 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。
- 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、サイト間で vzAny をプロバイダーおよびコンシューマー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

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) **ナビゲーション** ウィンドウで、[テナント (Tenant)] [テナント名 (tenant_name)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [L4 ~ L7 ポリシーベースリダイレクト (L4-L7 Policy Based Redirect)] の順に選択します。
- 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) **[L3 接続先 (L3 Destinations)]** テーブルで、[+] をクリックします。
- 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 に割り当てられます。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** (オプション)。レイヤ 4 ~ レイヤ 7 デバイスに割り当て 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 ファイアウォールの場合、これは仮想 MAC と呼ばれます。MAC アドレスを指定しない場合、アドレスは動的に検出されます。

- 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サービスデバイスの設定](#)。

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 クラスター**]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 クラスター** 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。

レイヤ3ポリシーベースリダイレクト先の動的MACアドレス検出

Cisco Application Policy Infrastructure Controller (APIC) 5.2(1) 以降のリリースでは、MACアドレスを指定せずにレイヤ3ポリシーベースリダイレクト (PBR) の接続先を設定できます。PBR接続先の一例として、サービスグラフの一部であるレイヤ4～レイヤ7デバイスがあります。この機能を設定することで、リーフスイッチは Address Resolution Protocol (ARP) を使用して、PBRネクストホップのMACアドレスを決定します。これにより、各PBR接続先のMACアドレスを確認する必要がなく、アクティブ/スタンバイ HA ペアでフローティングMACアドレスを使用する必要がないという利点があります。

レイヤ3ポリシーベースリダイレクト先の動的MACアドレス検出の注意事項と制限事項

レイヤ3ポリシーベースリダイレクト (PBR) 接続先の動的MACアドレス検出を設定するための注意事項と制限事項を次に示します。

- MACアドレスを指定しなかった接続先に対しては、トラッキングを有効にする必要があります。
- すべてのレイヤ3 PBR Equal Cost Multipath (ECMP : 等コストマルチパス) 機能と、IPv4 および IPv6 の接続先を使用できます。
- 同じ PBR ポリシーで、MACアドレスを設定した接続先と MACアドレスを設定していない接続先を一緒に持つことができます。
- MACアドレスが変更された場合、トラッキング間隔によっては、新しいMACアドレスを検出して、コンシューマーおよびプロバイダーのリーフスイッチでPBR接続先MACアドレスを更新するのに時間がかかります。
- リーフスイッチごとに100の接続先、ファブリックごとに1,500の接続先を持つことができます。

GUIを使用したレイヤ3ポリシーベースリダイレクト先の動的MACアドレス検出の設定

次の手順では、レイヤ3ポリシーベースリダイレクト (PBR) 接続先の動的MACアドレス検出を設定します。

- ステップ1 メニューバーで、[テナント (Tenants)] > [すべてのテナント (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 ナビゲーションウィンドウで、[テナント (Tenant)]/[テナント名 (*tenant_name*)] > [ポリシー (Policies)] > [プロトコル (Protocol)] > [L4 ~ L7 ポリシーベースリダイレクト (L4-L7 Policy-Based Redirect)] の順に選択します。
- ステップ4 [L4 ~ L7 ポリシーベースリダイレクト (L4-L7 Policy-Based Redirect)] を右クリックし、[L4 ~ L7 ポリシーベースリダイレクトの作成 (Create L4-L7 Policy-Based Redirect)] を選択します。
- ステップ5 [L4 ~ L7 ポリシーベースリダイレクトの作成 (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 (次に指定されているものは除く)。
 - a) [接続先タイプ (Destination Type)] で、まだ選択されていない場合は [L3] を選択します。
 - b) [IP SLA モニタリングポリシー (IP SLA Monitoring Policy)] ドロップダウンリストで、既存のIP SLA モニタリングポリシーを選択するか、新しいポリシーを作成します。
 - c) [L3 接続先 (L3 Destinations)] セクションで、[+] をクリックします。
 - d) [リダイレクトされたトラフィックの接続先の作成 (Create Destination of redirected traffic)] ダイアログボックスの [MAC] フィールドに、00:00:00:00:00:00 と入力するか、値を空のままにします。

どちらの方法でも、動的MACアドレス検出が有効になります。値を空のままにした場合、ポリシーの作成が完了すると値は 00:00:00:00:00:00 になります。
 - e) [リダイレクトヘルスグループ (Redirect Health Group)] で、必要に応じて、既存のヘルスグループを選択するか、新しいヘルスグループを作成します。
 - f) 必要に応じて、残りのフィールドに値を入力します。
 - g) [OK] をクリックします。
 - h) [送信 (Submit)] をクリックします。

REST API を使用したレイヤ3ポリシーベースリダイレクト先の動的MACアドレス検出の設定

次の REST API の例では、MAC アドレスに 00:00:00:00:00:00 を指定することで、レイヤ3ポリシーベースリダイレクト先の動的MACアドレス検出を有効にします。

```
<vnsSvcRedirectPol AnycastEnabled="no" destType="L3"
  dn="uni/tn-t0/svcCont/svcRedirectPol-TEST-PBR-POL" hashingAlgorithm="sip-dip-prototype"
  maxThresholdPercent="0" minThresholdPercent="0" name="TEST-PBR-POL"
  programLocalPodOnly="no" resilientHashEnabled="no" srcMacRewriteEnabled="no"
```

```
thresholdDownAction="permit" thresholdEnable="no" userdom=":all:common:">
  <vnsRsIPSLAMonitoringPol tDn="uni/tn-t0/ipslaMonitoringPol-l3ping"
    userdom=":all:common:"/>
  <vnsRedirectDest ip="11.2.2.100" ip2="0.0.0.0" mac="00:00:00:00:00:00" podId="1"
    userdom=":all:common:">
    <vnsRsRedirectHealthGroup tDn="uni/tn-t0/svcCont/redirectHealthGroup-Test-HG"
      userdom=":all:common:"/>
  </vnsRedirectDest>
</vnsSvcRedirectPol>
```

または、mac に空の値を指定できます。

```
<vnsRedirectDest ip="11.2.2.100" ip2="0.0.0.0" mac="" podId="1" userdom=":all:common:">
```

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。