ACI ファブリックの PBR を使用する Nexus Dashboard Orchestrator サイト間中継ルーティング 、リリース 4.3.x

目次

PBR を使用したサイト間中継ルーティング

次のセクションでは、Multi-Site ドメインでのポリシーベース リダイレクト（PBR）を使用したサイト間トランジット ルーティングの使用例のガイドライン、制限事項、および構成手順について説明します。

次のセクションは、PBR を使用したサイト間中継ルーティング（L3Out-to-L3Out）にのみ適用されます。PBR を使用した L3Out から EPG へのサイト間通信については、「PBR を搭載したサイト間 L3Out」の章を参照してください。 PBR を使用しない単純なサイト間 L3Out の使用例については、「サイト間L3Out」を参照してください。
次のセクションで説明する PBR を使用したサイト間トランジット ルーティングは、VRF 間シナリオと VRF 内シナリオの両方でサポートされます。

構成ワークフロー

次のセクションで説明する使用例は、基本的なサイト間 L3Out PBR の使用例の拡張であり、基本的なサイト間 L3Out（PBR なし）構成の拡張です。この機能を構成するには、次の手順を実行します。

1. 各サイトの基本的な外部接続（L3Out）を構成します。

   以下のセクションで説明される PBR 構成を持つサイト間 L3Out は、各サイトの既存の外部接続（L3Out）の上部で構築されます。各サイトで L3Out を構成していない場合、次のセクションに進む前に、「外部接続（L3Out）」の章で説明されている方法で 1 つ作成し、展開します。

2. PBR を使用しないユースケースの場合と同様に、異なるサイトに展開された L3Out に関連付けられている 2 つの外部 EPG 間にコントラクトを作成します。
3. 以下のセクションで説明するように、以前に作成したコントラクトにサービス チェーンを追加します。これには、以下が含まれます。
   - サービス デバイス テンプレートを作成し、サイトに割り当てます。

     サービス デバイス テンプレートは、PBR を使用したサイト間トランジット ルーティングを有効にするサイトに割り当てる必要があります。

   - サービス デバイス テンプレートにサイトレベル構成を提供します。

     各サイトは、異なる高可用性モデル（アクティブ/アクティブ、アクティブ/スタンバイ、独立サービス ノードなど）を含む独自のサービス デバイス構成を持つことができます。

   - 定義したサービス デバイスを、前の手順で展開したサイト間 L3Out のユース ケースで使用するコントラクトに関連付けます。

Cisco ACI コントラクトと PBR の用語を理解するには、『*ACI コントラクト ガイド*』と「*ACI PBR ホワイトペーパー*」を参照してください。

トラフィック フロー

このセクションでは、異なるサイトの 2 つの外部 EPG 間のトラフィック フローを要約します。

2 サイトに展開された独立 FW サービスによる非対称なトラフィック フローを避けるため、
双方向のトラフィック フローは両方のファイアウォールを経由してリダイレクトされます。

コンシューマからプロバイダへのトラフィック フロー

分類のために接続先の外部 EPG に関連付けられている IP プレフィックスは、コンシューマ リーフ スイッチで（そのクラス ID を使用して）自動的にプログラムされるため、リーフ スイッチは常に接続先の外部 EPG のクラス ID を解決でき、PBR ポリシーのローカル FW へのトラフィックのリダイレクトを適用します。

コンシューマ サイトのファイアウォールがセキュリティ ポリシーを適用した後、トラフィックはファブリックに返送され、外部の接続先に接続するプロバイダー ボーダー リーフ ノードに向けてサイト間で転送されます。Site1 から発信されたトラフィックを受信するボーダー リーフノードは、PBR ポリシーを適用し、トラフィックをローカル ファイアウォール ノードにリダイレクトします。ファイアウォールがローカル セキュリティ ポリシーを適用した後、トラフィックはボーダー リーフ ノードに送り返されます。ボーダー リーフ ノードは、外部の接続先にトラフィックを転送するだけです。

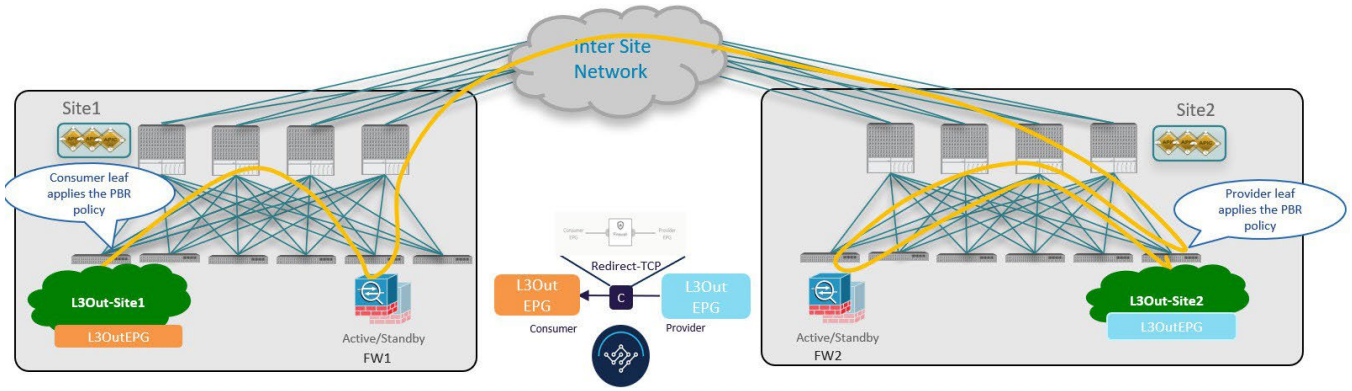


図 1. コンシューマからプロバイダへのトラフィック フロー

プロバイダからコンシューマへのトラフィック フロー

コンシューマからプロバイダーへのスイッチと同様に、プロバイダー リーフ スイッチは常に接続先の外部 EPG のクラス識別子を解決でき、反対方向のローカル FW にトラフィックをリダイレクトする PBR ポリシーを適用します。

その後、トラフィックはコンシューマ サイトに送信され、外部の接続先に転送される前にローカル ファイアウォールに送られます。

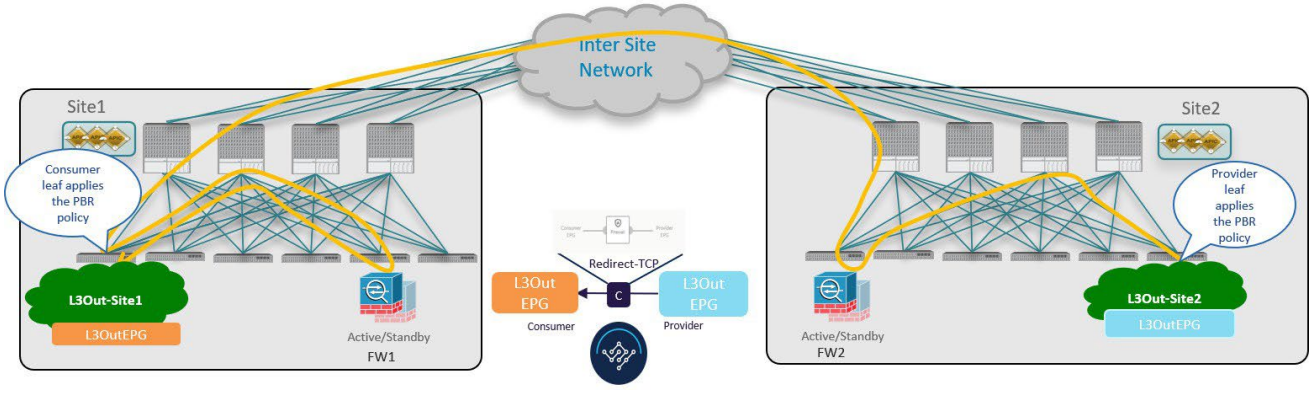


図 2 プロバイダからコンシューマへのトラフィック フロー

PBR を使用したサイト間転送ルーティングに関する注意事項と制約事項

マルチサイトで PBR を使用して vzAny 内にサイト間中継ルーティングを展開する場合は、次の注意事項と制約事項が適用されます。

- vzAny PBR を使用したサイト間トランジット回送は、ワンアーム インターフェイスのシングルノード ファイア ウォールでのみサポートされます。

  この使用例は、Cisco APIC リリース 6.0（4）以降を実行しているサイトでサポートされています。

  - これらのユース ケースのアプリケーション テンプレートで定義されている既存のサービス グラフ オブジェクトを使用するとき、リリース 4.2（3）で導入された新しいサービス チェーン ワークフローを使用し、サービス デバイス テンプレートでポリシーを定義してコントラクトに関連付けることで、新しいサービス グラフを暗黙的に作成することを推奨します。

    次のセクションで説明する手順では、新しいサービス デバイス テンプレートを使用して、サポートされているユース ケースを有効にしますが、該当する場合は特有の違いについて説明します。

    アプリケーション テンプレートのサービス グラフ オブジェクトの構成は、今後のリリースで廃止されます。

- L3Out VRF は、ストレッチ（VRF 内の使用例の場合）またはサイトローカル（VRF 間の使用例の場合）にすることができます。

  次のセクションでは、各サイトに VRF と L3Out がすでに設定されていることを前提としています。

  この章で説明する L3Out-to-L3Out の使用例を有効にするには、vzAny VRF に対して [サイト対応ポリシーの適用（Site-Aware Policy Enforcement）] オプションと [L3 マルチキャスト（L3 Multicast）] オプションを有効にする必要があることに注意してください。

  VRF がまだない場合は、通常どおりにアプリケーション テンプレートで VRF を作成できます。VRF 構成の詳細については、「VRF の構成」を参照してください。

- 新しい L3Out-to-L3Out の使用例を有効にするには、VRF で [サイト認識ポリシー適用モード（Site-Aware Policy Enforcement Mode）] 設定を有効にする必要があります。[サイト認識ポリシー適用モード（Site-Aware Policy Enforcement Mode）] オプションを有効または無効にすると、リーフ スイッチでゾーン分割ルールを更新する必要があるため、短時間のトラフィックの中断（EPG 間の既存のコントラクトを含む）が発生します。この操作はメンテナンス期間中に実行することを推奨します。[サイト認識ポリシー適用モード（Site-Aware Policy Enforcement Mode）] を有効にすると、既存のコントラクトのリーフ スイッチでの TCAM 使用率が増加します。コントラクト許可ロギングをこのオプションと組み合わせて使用することはできません。
- サービス デバイス インターフェイスにアタッチするサービス BD は、L2 ストレッチとして構成する必要があります（BUM 転送はオプションで、無効にしておくべきです）。

  サービス BD がまだない場合は、アプリケーション テンプレートで作成できます。BD 構成の詳細については、「ブリッジ ドメインの構成」を参照してください。

- コンシューマ、プロバイダー、およびサービス BD は、ハードウェア プロキシ モードで構成する必要があります。
- vzAny PBR は、L3Out ではなく、ストレッチされたサービス BD に接続する必要があります。

- しきい値ダウン拒否アクションと sip-dip-protocol ハッシュのみがサポートされます。
- PBR 接続先は、コンシューマ VRF またはプロバイダー VRF のいずれかにある必要があります。たとえば、
  「*Cisco Application Centric Infrastructure におけるポリシーベース リダイレクト サービス グラフの設計に関するホワイトペーパー*」を参照してください。

この使用例では、以下はサポートされていません。

- 特定のリモート リーフ スイッチ構成。

  リモート リーフ ノードを利用するマルチサイト展開には、特定の考慮事項が適用されます。異なるサイトに属するリモート リーフ ノードに展開されているエンドポイント（コンシューマまたはプロバイダー）間の通信を目的とした、PBR を使用したサイト間中継ルーティングは、vzAny PBR および L3Out-to L3Out ではサポートされません。

- 各 VRF は、vzAny-to-vzAny、L3OutEPG-to-L3OutEPG、および vzAny-To-L3OutEPG PBR のワンアーム構成で 1 つのデバイスのみを使用するように制限されます。この制限は、 APICの特別な ACL により適用されます。
- vzAny-to-vzAny/L3OutEPG-to- L3OutEPG のリダイレクト、および vzAny-to-EPG、EPG-to-EPG、EPG-to-L3OutEPG などの他の使用例では、それらが同じ VRF にある場合、異なるファイアウォール VLAN インターフェイスを使用する必要があります。
- PBR を使用した vzAny が、新しくサポートされたユースケース（vzAny-to-vzAny、vzAny-to-L3OutEPG、L3OutEPG-to-L3OutEPG）のノースサウス通信に適用される場合、ストレッチ サブネットに対して入力トラフィックの最適化を有効にする必要があります。
- L3 PBR 接続先を持つ 1 つのノード サービス チェーンのみがサポートされます。
- コントラクト許可ロギングは、サイト認識ポリシー適用モードが有効になっている VRF ではサポートされません。このモードは vzAny PBR および L3OutEPG-to-L3OutEPG PBR では必要です。
- PBR を使用したポッド対応 vzAny はサポートされていません。

サービス デバイス テンプレートの作成

始める前に：

- 「サイト間中継ルーティングの注意事項および 制限事項」で説明されているように、要件を読んで満たしていることを確認します。
- このセクションで定義するサービス ノードで使用する拡張サービス ブリッジ ドメイン（BD）を作成しておく必要があります。

  サービス BD がまだない場合は、通常どおりにアプリケーション テンプレートで作成できます。BD 構成の詳細については、「ブリッジ ドメインの構成」を参照してください。

次の手順では、サイト間トランジット ルーティングの使用例に使用するサービス ノードとその設定を使用してサービス デバイス テンプレートを作成する方法について説明します。

1. Nexus Dashboard Orchestrator の GUI にログインします。
2. 左のナビゲーション ペインから、**[構成（Configure）] > [テナント テンプレート（Tenant Template）]** を選択します。
3. （オプション）テナント ポリシー テンプレートと IP-SLA モニタリング ポリシーを作成します。

   トラフィック リダイレクションの IP-SLA ポリシーを構成することを推奨します。これにより、以下の手順 7 で説明する PBR ポリシーの構成が簡素化されます。IP-SLA ポリシーがすでに定義されている場合は、この手順をスキップできます。それ以外の場合は、次の手順を実行します。

   a. **[テナント ポリシー（Tenant Policies）]** タブを選択します。
   b. **[テナント ポリシー（Tenant Policy）]**ページ内で**[テナント ポリシー テンプレートの作成（Create Tenant Policy Template）]**をクリックします。
   c. **[テナント ポリシー（Tenant Policies）]** ページの右のプロパティ サイトバーにテンプレートの **[名前（Name）]** を入力し、
   [テナントの選択（Select a Tenant）] を選択します。
   d. **[テンプレート プロパティ（Template Properties）]** ページで、**[アクション（Actions）] > [サイトの追加/削除（Add/Remove** Sites）] を選択し、両方のサイトにテンプレートを関連付けます。
   e. メインペインで、 **[オブジェクトの作成（Create Object）] > [IP SLA** モニタリング ポリシー（**IP SLA Monitoring Policy**）] を選択します。
   f. ポリシーの **[名前（Name）]** を指定し、その設定を定義します。
   g. **[保存（Save）]** をクリックして、テンプレートを保存します。
   h. **[テンプレートの展開（Deploy）]** をクリックして、展開します。
4. サービス デバイス テンプレートを作成し、テナントおよびサイトに関連付けます。
   a. **[構成（Configure ）] > [テナント テンプレート（Tenant Templates）]** から、**[サービス デバイス（Service Device）]** タブを選択します。
   b. **[サービス デバイス テンプレートの作成（Create Service Device Template）]** をクリックします。
   c. 開くテンプレート　プロパティ サイドバーで、テンプレートの **[名前（Name）]** を入力し、**[テナントの選択（Select a Tenant）]** を選択します。
   d. **[テンプレート プロパティ（Template Properties）]** ページで、**[アクション（Actions）] > [サイトの追加/削除（Add/Remove** Sites）] を選択し、両方のサイトにテンプレートを関連付けます。
   e. **[保存（Save）]** をクリックして、テンプレートを保存します。

5. デバイス クラスタを作成して構成します。

   a. [テンプレート プロパティ（**Template Properties**）] ページ（テンプレート レベル の構成）で、[オブジェクトの作成（**Create Object**）] > [サービス デバイス クラスタ（**Service Device Cluster**）] を選択します。

   デバイス クラスタは、トラフィックをリダイレクトするサービスを定義します。このリリースでは、active/standby、active/active、または複数の独立したノードのクラスタの 3 つの異なる冗長モデルで展開できるファイアウォール サービス ノードへのリダイレクションがサポートされています。これらのさまざまなオプションのプロビジョニングについては、以下の手順 7 で説明します。サイトレベルでファイアウォール展開モデルを選択でき、同じ Multi-Site ドメインの一部であるさまざまなファブリックにさまざまなオプションを展開できることに注意してください。

   b. **[<cluster-name>]** サイドバーで、クラスタの **[名前（Name）]**を入力します。

   [デバイスの場所（Device Location）] と **[デバイス モード（Device Mode）]** は、現在サポートされている使用例に基づいて事前に入力されています。デバイスの場所 は ACI として、 デバイス モード は L3として事前に構成する必要があります。

   c. **[デバイスタイプ（Device Type）]** で、[ファイアウォール（Firewall）] を選択します。

   d. **[デバイス モード（Device Mode）]** では、[L3] を選択します。

   e. **[接続モード（Connectivity Mode）]** の場合、[One Arm] を選択します。

   このリリースでは、ワン アーム モードで接続されたサービス デバイスのみサポートされます。

   デバイス接続モードを ワン アーム、ツー アーム、および詳細モードの間で変更すると、プロセスでデバイス インターフェイスの名前が変更される場合があります。警告メッセージはユーザーに警告し、インターフェイスを変更しようとすることは、
   そのインターフェイスが現在コントラクトによって使用されている場合、制限されます。

   以前に使用していたインターフェイス名を保持し、
   展開された構成の中断を回避することを望む場合は、変更プロセス中に名前の変更を上書きすることを選択できます。

   検証は、ワン アーム モードとツー アーム モードでのみ実行されます。
   [詳細（Advanced）] モードでは、検証は実行されません。
   このモードを選択すると、ユーザーはエキスパートであると見なされます。

   f. **[インターフェイス名（Interface Name）]** を入力します。

   g. **[インターフェイス タイプ（Interface Type）]** で、[BD] を選択します。

   h. **[BD の選択（Select BD）]** をクリックして、このデバイスを接続するサービス ブリッジ ドメインを選択します。

   これは、「vzAny with PBR を使用した vzAny の 注意事項と制限事項」の一部として作成した拡張サービス BD です。

   i. **[リダイレクト（Redirect）]** オプションで、[はい（Yes）] を選択します。

   PBR の使用例では、リダイレクトの有効化を選択する必要があります。[はい（Yes）] を選択すると、**[IP SLA モニタリング ポリシー（IP SLA Monitoring Policy）]** オプションが使用可能になります。

   j. （オプション）**[IP SLA モニタリング ポリシーの選択（Select IP SLA Monitoring Policy）]** を

クリックし、前の手順で作成した IP SLA ポリシーを選択します。

k. （オプション）サービス クラスタの追加設定を指定する場合は、**[詳細設定（Advanced Settings）]** エリアで **[有効（Enable）]** を選択します。

次の詳細設定を構成できます。

- **[QoS ポリシー（QoS Policy）]**：リダイレクトされたトラフィックに ACI ファブリック内で特定の QoS レベルを割り当てることができます。
- **[優先グループ（Preferred Group）]**：このサービス デバイス インターフェイスクラスタが優先グループの一部であるかどうかを指定します。
- **[ロード バランシング ハッシュ（Load Balancing Hashing）]**：PBR ロード バランシングのハッシュ アルゴリズムを指定できます。

vzAny-to-vzAny、vzAny-to- ExtEPG、および ExtEPG-to-ExtEPG 使用例ではデフォルト構成のみをサポートしているため、デフォルト値のままにする必要があります。他の使用例（EPG から EPG、ExtEPG から EPG、および vzAny から EPG）の負荷バランシングハッシュを変更できます。

詳細については、*「ACI ポリシーベースのリダイレクト サービス グラフの設計」*を参照してください。

- **[ポッド対応リダイレクション（Pod Aware Redirection）]**：優先 PBR ノードを指定する場合は、マルチポッド構成で構成できます。ポッド対応リダイレクションを有効にすると、ポッド ID を指定でき、リダイレクトは指定された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。
- **[送信元 MACの書き換え（Rewrite Source MAC）]**：PBR ノードが IP ベースの転送ではなく「送信元 MAC ベースの転送」を使用している場合に、送信元 MAC アドレスを更新します。

詳細については、*「ACI ポリシーベースのリダイレクト サービス グラフの設計」*を参照してください。

- **[高度なトラッキング オプション（Advanced Tracking Options）]**：サービス ノード トラッキングのさまざまな詳細設定を構成できます。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*」を参照してください。

l. **[OK]** をクリックして保存します。

サービス デバイス クラスタを作成すると、**[テンプレート プロパティ（Template Properties）]**（テンプレート レベルの構成）ページで赤色で強調表示されることに注意してください。この時点で、ファイアウォール サービスへのリダイレクトを定義しましたが、やはりサイトローカル レベルで使用するファイアウォール情報とリダイレクト ポリシーを指定する必要があります。

6. 前の手順で作成したサービス デバイス クラスタのサイトローカル構成を指定します。

a. **[サービスデバイステンプレート（Service Device Template）]** 画面で、**[<site-name>]** タブをクリックします。

b. サイト レベルで、作成したサービス デバイス クラスタを選択します。

c. プロパティのサイドバーで、**[ドメイン タイプ（Domain Type）]** を選択します。

このサイトのファイアウォールデバイスが物理または VMM（仮想であり、VMM ドメインの一部であるハイパーバイザによってホストされる）のいずれであるかを選択できます。

d. **[ドメインの選択（Select Domain）]** をクリックして、このファイアウォール デバ

イスが属するドメインを選択します。物理ドメインまたは仮想ドメインのいずれか

を選択できます。

- 物理ドメインを選択した場合は、次の情報を入力します。
  - **[VLAN]**：ファブリックとファイアウォール デバイス間のトラフィックに使用される VLAN ID を指定する必要があります。
  - [ファブリックからデバイスへの接続（Fabric to Device Connectivity）]：ファイアウォール デバイスへのファブリックの接続に関するスイッチ ノードとインターフェイス情報を提供します。
- VMM ドメインを選択した場合は、追加のオプションを指定します。
  - [トランキング ポート（Trunking Port）]：**L4-L7 VM** のタグ付きトラフィックを有効にするために使用されます。

    デフォルトで、ACI サービス グラフ構成では、アクセスモード ポート グループが作成され、L4-L7 VM の vNIC に自動的に接続されます。

  - **[無差別モード（Promiscuous Mode）]**：L4-L7 仮想アプライアンスが、VM が所有する vNIC MAC 以外の MAC アドレス宛のトラフィックを受信する必要がある場合に必要です。
  - **[VLAN]**：VMM ドメインのオプション構成であり、指定されていない場合は、ドメインに関連付けられたダイナミック VLAN プールから割り当てられます。
  - [拡張 LAG オプション（Enhanced LAG Option）]：ハイパーバイザとファブリック間のポートチャネルに拡張 **LACP** を使用している場合。
  - **[VM 名（VM Name）]**：この VMM ドメインと、ファイアウォール トラフィックで使用されるインターフェイス（**VNIC**）で使用可能なすべての VM のリストから、ファイアウォールの VM を選択します。

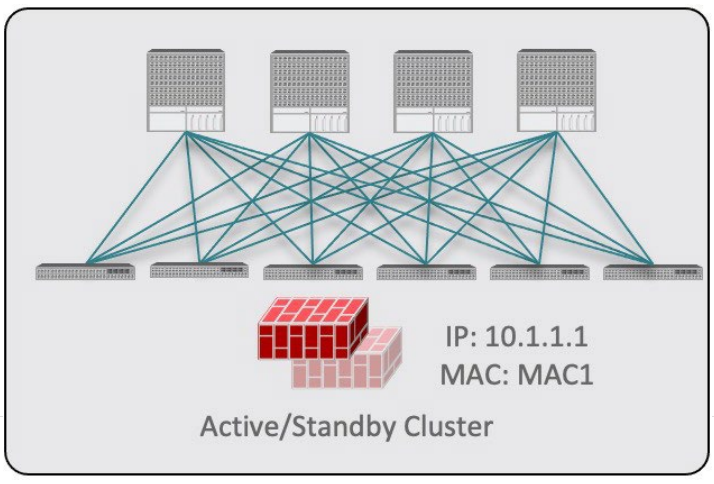
    展開するデバイス クラスタの種類に応じて、**[+ VM 情報の追加（+Add VM information）]** をクリックして
    追加のクラスタ ノードを指定します。

7. FW デバイス情報と PBR 宛先 IP アドレスを指定します。

   前述のように、このリリースでは、高可用性 FW クラスタの 3 つの展開オプション（active/standby クラスタ、active/active クラスタ、独立アクティブ ノード）がサポートされています。3 つのすべての展開オプションで、IP SLA ポリシー（手順 3 で説明）を使用すると、ファイアウォール ノードの IP アドレスのみを指定でき、対応する MAC アドレスが自動的に検出されます。

   異なるサイトに異なる設計を展開できます。

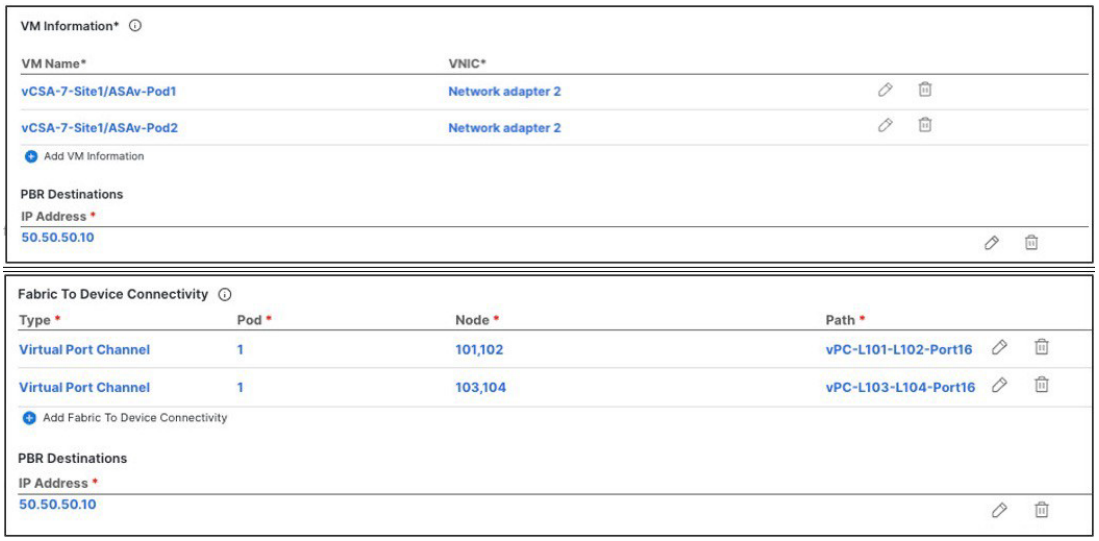
   - Active/standby クラスタは、単一の MAC/IP ペアによって識別されます。



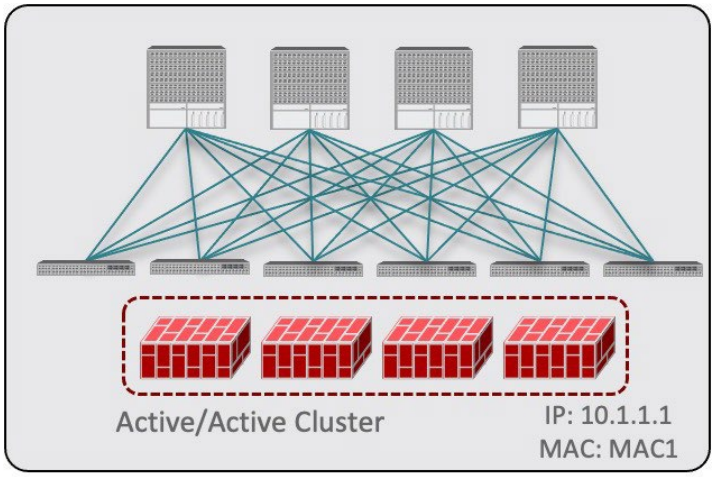
この場合、アクティブなファイアウォール ノードを識別する単一の PBR 宛先 IP アドレスを指定し、クラスタ内のすべてのノードに関する情報も含める必要があります。

たとえば、2 ノードの active/standby クラスタの場合は、次のように指定します。

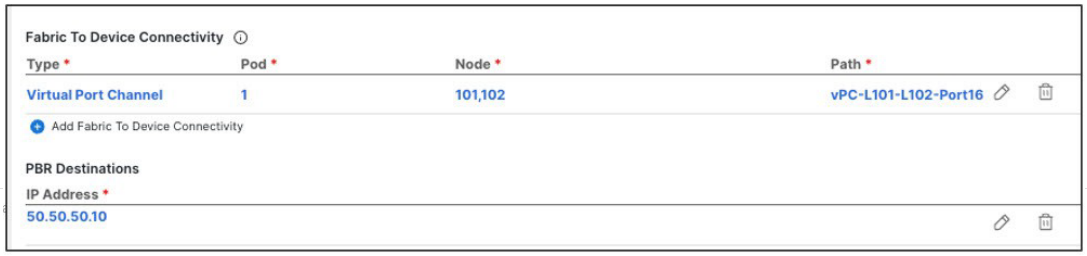
- 仮想ファイアウォール クラスタの場合、アクティブ ファイアウォール ノードとスタンバイ ファイアウォール ノードを表す VM と、PBR の宛先としてのアクティブ ファイアウォールの IP アドレスを表します。
- 物理ファイアウォール クラスタの場合、アクティブ ファイアウォール ノードおよびスタンバイ ファイアウォール ノードをファブリックのリーフ スイッチに接続するために使用されるインターフェイス（以下の具体例では vPC インターフェイス）と、PBR の宛先となるアクティブ ファイアウォールの IP アドレス。



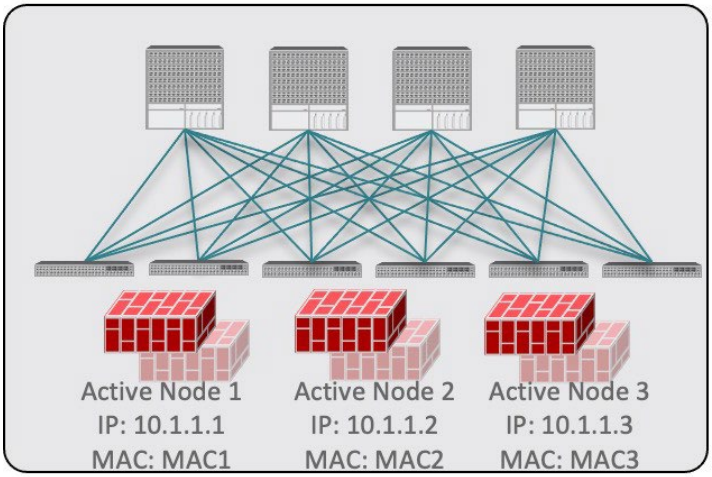
- Active/active クラスタは、単一の MAC/IP ペアによっても識別されます。



Cisco ファイアウォール（ASA または FTD モデル）の場合、単一の MAC/IP ペアを持つアクティブ/アクティブ クラスタは物理フォーム ファクタでのみサポートされます。すべてのクラスタ ノードは同じ MAC/IP アドレスを所有し、ACI リーフ スイッチのペアに展開された同じ vPC 論理接続に接続されている必要があります。次の図は、その結果として、単一の vPC インターフェイスと単一の PBR 接続先 IP アドレスを NDO で構成する方法を示しています。ここでは、前のユースケースで説明した IP SLA ポリシーを使用すると、MAC アドレスが動的に検出されます。



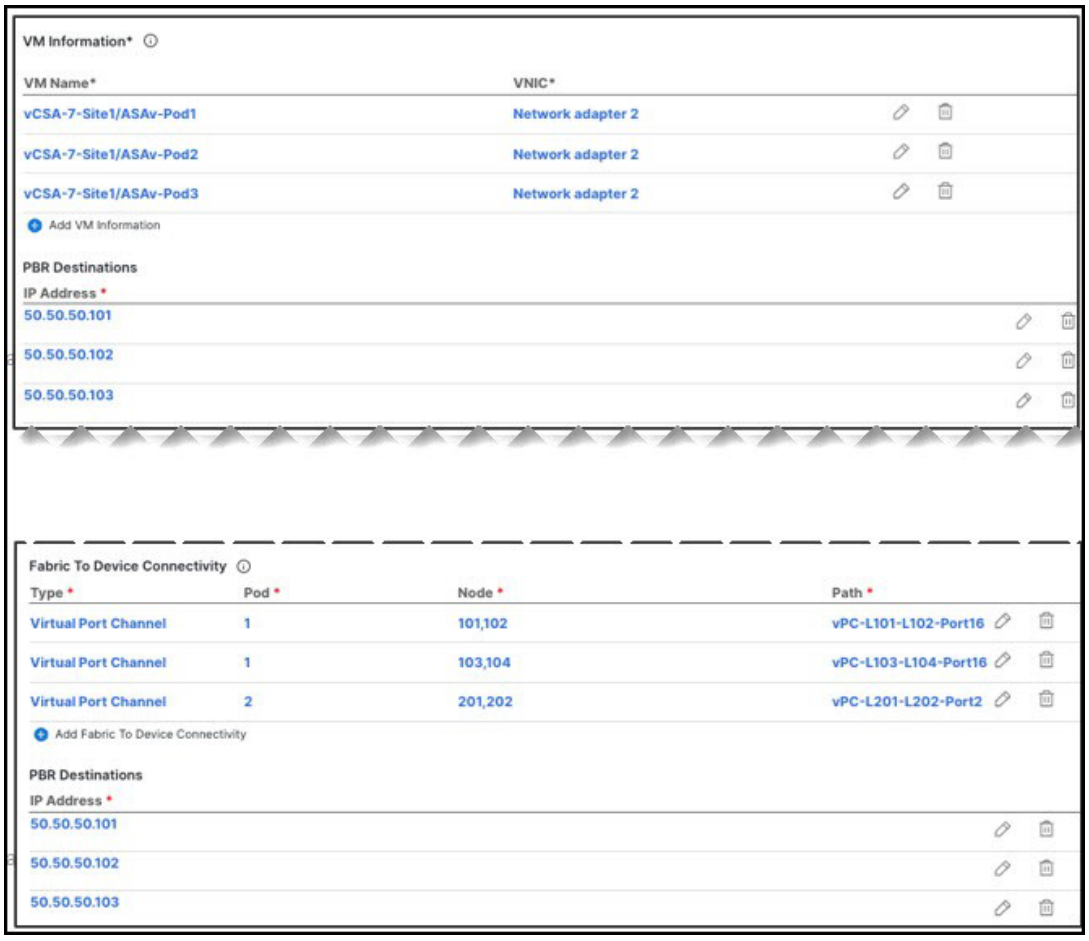
- 独立したアクティブ ノード構成の場合、各アクティブ ノードは一意の MAC/IP アドレス ペアによって識別されます。
  対称 PBR により、トラフィックは両方向で同じアクティブ ノードによって処理されることに注意してください。



この場合、NDO 構成で、各アクティブ ノードの個々の PBR 接続先 IP アドレスと各ノードの情報を指定する必要があります。

たとえば、3 つの独立したファイアウォール ノードを展開する場合は、次のように指定します。

- 仮想ファイアウォール フォーム ファクタの場合、3 つのファイアウォール ノードを表す VM と、PBR 宛先としての一意の IP アドレス。
- 物理ファイアウォールのフォーム ファクタの場合、各ファイアウォール ノードをファブリックのリーフ スイッチに接続するために使用されるインターフェイス（以下の具体例では vPC インターフェイス）と、PBR の宛先となる各ファイアウォール ノードの固有 IP アドレス。



a. [デバイス接続にファブリックを追加（Add Fabric To Device Connectivity）]（物理ドメイン）または [VM 情報を追加（Add VM **Information**）]（**VMM** ドメイン）をクリックします。

前の手順で物理ドメインと VMM ドメインのどちらを選択したかに応じて、ファイアウォール VM またはファイアウォール デバイスへの物理ファブリック接続のいずれかの情報を指定します。

物理ドメインの場合は、ポッド、スイッチノード、およびインターフェイス情報を指

定します。VMM ドメインの場合は、VM 名と vNIC 情報を指定します。

b. **[PBR 宛先の追加（Add PBR Destination）]** をクリックして、サービス ブリッジ ドメインに接続されているファイアウォール上のインターフェイスの IP アドレスを指定します。

展開するデバイス クラスタの種類によっては、1 つ以上の PBR 宛先 IP アドレスを指定する必要があります。

これにより、ファイアウォールのインターフェイスに IP アドレスがプロビジョニングされるのではなく、その IP アドレスへのトラフィックのリダイレクトが構成されるだけです。特定のファイアウォール構成は NDO から展開されないため、個別にプロビジョニングする必要があります。

c. **[OK]** をクリックして、指定した構成を保存します。

d. テンプレートを関連付けた他のサイトに対してこの手順を繰り返します。

8. テンプレートを保存して展開します。

a. **[サービス デバイス テンプレート（Service Device Template）]** レベルで、**[保存（Save）]** をクリックしてテンプレート構成を保存します。

b. **[テンプレート プロパティ（Template Properties）]** タブを選択し、**[テンプレートの展開（Deploy Template）]** をクリックして構成をサイトにプッシュします。

c. （オプション）構成がサイトレベルで作成されたことを確認します。

L4-L7 デバイスが APIC で構成されていることを確認するには、APIC GUI で **[<tenant-name>] > [サービス（Services）] > [L4-L7] > [デバイス（Devices）] > [<cluster-name>]** に移動します。これにより、デバイスクラスタが、前の手順で指定したすべての構成とともに表示されます。

PBR ポリシーが APIC で構成されたことを確認するには、**[<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）]** に移動し、ステップ *5j で選択した IP SLA モニタリング ポリシーと手順 7d* で提供した IP アドレスで定義された **<cluster- name>-one-arm** リダイレクトが表示されるはずです。

次に行う作業：

サービス デバイス構成を展開したら、「コントラクトの 作成とサービス チェーンの追加」の説明に従って、アプリケーション テンプレート、外部 EPG、およびサービス チェーンを関連付けるコントラクトを作成します。

コントラクトの作成とサービスチェーンの追加

始める前に：

- 「外部接続（L3Out）」の説明に従って、各サイトで外部接続（L3Out）構成を作成して展開しておく必要があります。
- 「サービス デバイス テンプレートの作成」の説明に従って、デバイス構成を含むサービス デバイス テンプレートを作成して展開しておく必要があります。

サービス デバイス テンプレートを作成して展開し、各サイトの L3Outs の外部 EPG を使用してアプリケーション テンプレートを作成した後、外部 EPG 間のコントラクトを作成し、前のセクションで作成したサービス デバイスとコントラクトを関連付けて、ポリシーベース リダイレクトを使用したサイト間のトランジットを可能にします。

1. L3Outs の外部 EPG と外部 EPG 間のコントラクトを作成するアプリケーション テンプレートに移動します。通常は、各サイトに関連付けられた異なるサイト ローカル テンプレートで外部 EPG を定義します。
2. 2 つの外部 EPG を作成し、各サイトの L3Out をサイトレベルで外部 EPG に関連付けます。

   これは、ファブリックの外部接続を作成するときに通常使用するプロセスと同じです。L3Out テンプレートと外部 EPG の詳細については、「外部接続（L3Out）」を参照してください。

3. 通常どおり、両方のサイトに関連付けられたストレッチ テンプレートにコントラクトを作成し、コンタクトを両方の外部 EPG に関連付けます。

   この場合、外部 EPG の 1 つは consumer になり、もう 1 つは provider になります。

4. 作成したコントラクトを選択します。
5. **[**サービス チェーン（**Service Chaining**）**]** エリアで、**[+** サービス チェーン（**+Service Chaining**）**]** をクリックします。

   これらの手順は、「サービス デバイス テンプレートの作成」で説明されているように、リリース 4.2(3) で導入された新しいサービス デバイス テンプレート ワークフローを使用して、この使用例の新しいサービス デバイスを構成していることを前提としています。アプリケーション テンプレートでサービス グラフがすでに定義されている場合は、代わりに [サービス グラフ（Service Graph）] を選択し、既存のサービス グラフを選択します。ただし、[サービス グラフ（Service Graph）] オプションは将来のリリースで廃止されることに注意してください。

6. **[**デバイス タイプ（**Device Type**）**]** で、[ファイアウォール（Firewall）] を選択します。

   このリリースでは、ワン アーム モードで接続されたサービス デバイスのみサポートされます。

7. **[**デバイス（**Device**）**]** ドロップダウンから、前の手順で作成した FW デバイス クラスタを選択します。
8. **[**コンシューマ コネクタ タイプのリダイレクト（**Consumer Connector Type Redirect**）**]** が有効になっていることを確認します。
9. **[**プロバイダ コネクタ タイプのリダイレクト（**Provider Connector Type Redirect**）**]** が有効になっていることを確認します。
10. **[**追加（**Add**）**]** をクリックして続行します。
11. **[**保存（**Save**）**]** をクリックして、テンプレートを保存します。

12. **[**テンプレートの展開（**Deploy**）**]** をクリックして、展開します。

初版：2024 年 3 月 1 日
最終更新日：2024 年 3 月 1 日

米国本社
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax：408 527-0883