PBR を使用したサイト間 L3Out

PBR を使用したサイト間 L3Out

Cisco Application Centric Infrastructure（ACI）ポリシーベース リダイレクト（PBR）は、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、および侵入防御システム（IPS）のトラフィック リダイレクションを可能にします。一般的な使用例としては、プールしてアプリケーション プロファイルに合わせて調整すること、また容易にスケーリングすることができ、サービス停止の問題が少ないサービス アプライアンスのプロビジョニングがあります。PBR により、コンシューマとプロバイダ エンドポイントの間のコントラクトに基づくサービス アプライアンスの挿入は簡素化されます。このことは、それらすべてが同じ仮想ルーティングおよびフォワーディング（VRF）インスタンスに存在する場合でも成り立ちます。

PBR の展開には、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、これらの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が含まれます。サービスグラフ テンプレートを展開した後、EPG 間のコントラクトにアタッチして、そのコントラクトに従うすべてのトラフィックが、作成した PBR ポリシーに基づいてサービス グラフ デバイスにリダイレクトされるようにすることができます。これにより、同じ2つのEPG間のどのタイプのトラフィックをL4-L7デバイスにリダイレクトし、どのタイプのトラフィックを直接許可するかを選択できます。

サービス グラフおよびPBRに固有の詳細情報については、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』を参照してください。

構成ワークフロー

次のセクションで説明するユース ケースは、基本的なサイト間 L3Out（PBR なし）のユース ケースの拡張であり、各サイトの基本的な外部接続（L3Out）構成の拡張です。サポートされるユース ケースを構成するワークフローは同じですが、オブジェクトを同じ VRF で作成する

か、異なる VRF で作成するか（VRF 間と VRF 内）、およびオブジェクトを展開する場所（拡張か非拡張か）のみが異なります。

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。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） で説明されるように 1 つ作成し展開します。

2. PBR を**使用せず**にサイト間 L3Out の使用例を構成します。

   サービス チェーンを追加する前に、ポリシーベースのリダイレクションを使用しない単純なサイト間 L3Out の使用例を構成することをお勧めします。これは、サイト間 L3Out 章で詳細を説明しています。

3. 以下のセクションに説明されるように、L3Out 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。

   - サイト間 L3Out が展開されている各サイトの各ポッドに外部 TEP プールを追加します。
   - 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、他の構成オブジェクトを含む L3Out およびアプリケーション テンプレートと同じ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（active/active、active/standby、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基本的なサイト間 L3Out の使用例に使用するコントラクトに関連付けます。

サポートされる使用例

次の図は、アプリケーション EPG の ACI 内部エンドポイントと、サポートされているサイト間 L3Out with PBR 使用例の別のサイトの L3Out を経由する外部エンドポイント間のトラフィック フローを示しています。

VRF 内と VRF 間

アプリケーション EPG と外部 EPG を作成および設定する場合、アプリケーション EPG のブリッジドメインと L3Out に VRF を提供する必要があります。同じ VRF（intra-VRF）を使用するか、異なるVRF（inter-VRF）を使用するかを選択できます。

EPG 間のコントラクトを確立する場合は、1 つの EPG をプロバイダとして指定し、もう 1 つの EPG をコンシューマとして指定する必要があります。

- 両方の EPG が同じ VRF にある場合、どちらか一方がコンシューマまたはプロバイダになることができます。

- EPG が異なる VRF にある場合は、外部 EPG がプロバイダーであり、アプリケーション EPG がコンシューマである必要があります。

ストレッチ EPG への L3Out

この使用例は、2 つのサイト間で拡張される単一のアプリケーション EPG と、1 つのサイトでのみ作成される単一の L3Out を示しています。アプリケーション EPG のエンドポイントが L3Out と同じサイトにあるか、他のサイトにあるかに関係なく、トラフィックは同じ L3Out を通過します。ただし North-South トラフィックの場合、PBR ポリシーは常にコンピューティング リーフ ノードにのみ適用されるため（境界リーフ ノードには適用されない）、トラフィックは常にエンドポイントのサイトに対してローカルなサービス ノードを通過します。

（注） 外部 EPG が拡張され、各サイトに独自の L3Out があるが、トラフィックの発信元または宛先であるサイトの L3Out がダウンしている場合も、同じフローが適用されます。

図 *1*: インバウンド トラフィック

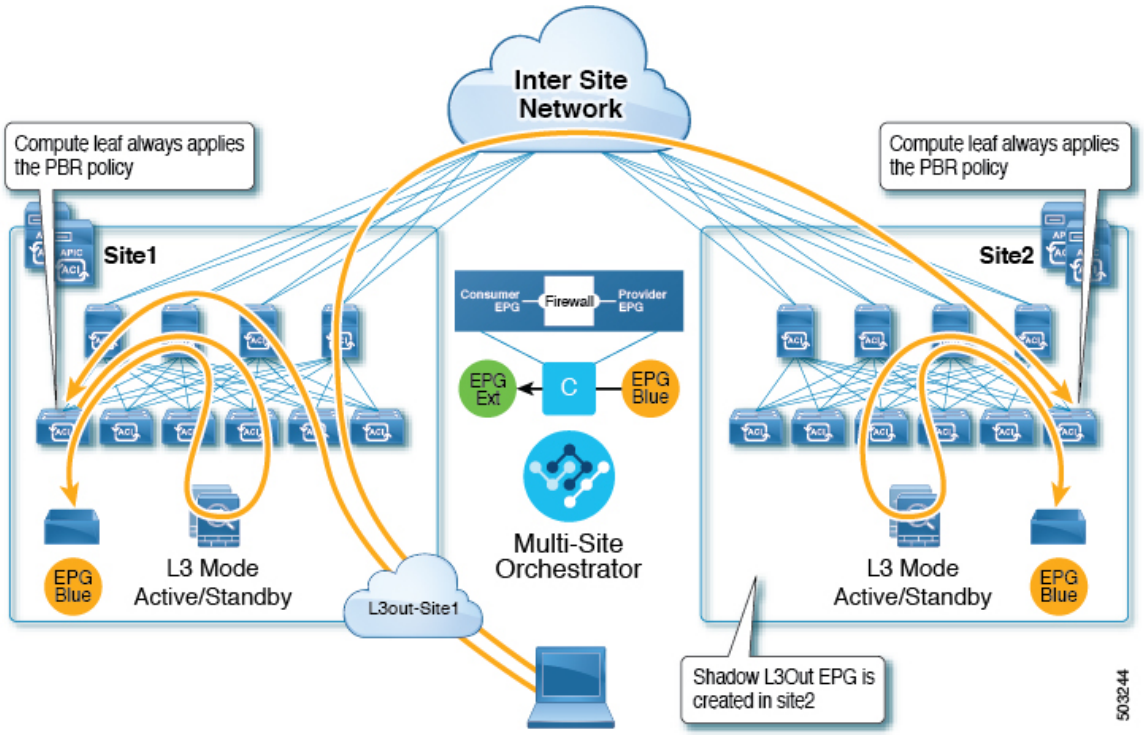
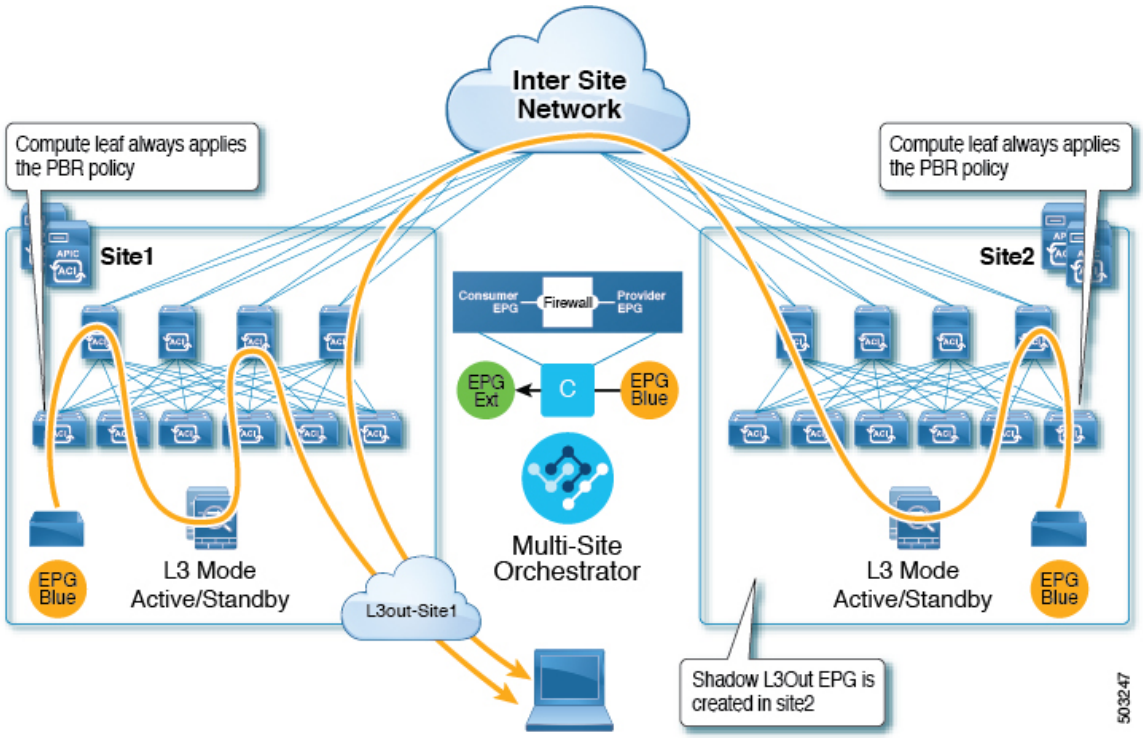


図 *2:* アウトバウンド トラフィック



サイトローカル EPG への L3Out

この使用例は、North-South トラフィックに他のサイトの L3Out を使用するサイトローカル アプリケーション EPG を示しています。前の例と同様に、すべてのトラフィックは EPG のサイトローカル サービス グラフ デバイスを使用します。

（注） 外部 EPG が拡張され、各サイトに独自の L3Out があり、EPG のローカル L3Out がダウンしている場合も、同じフローが適用されます。

図 *3:* インバウンド トラフィック

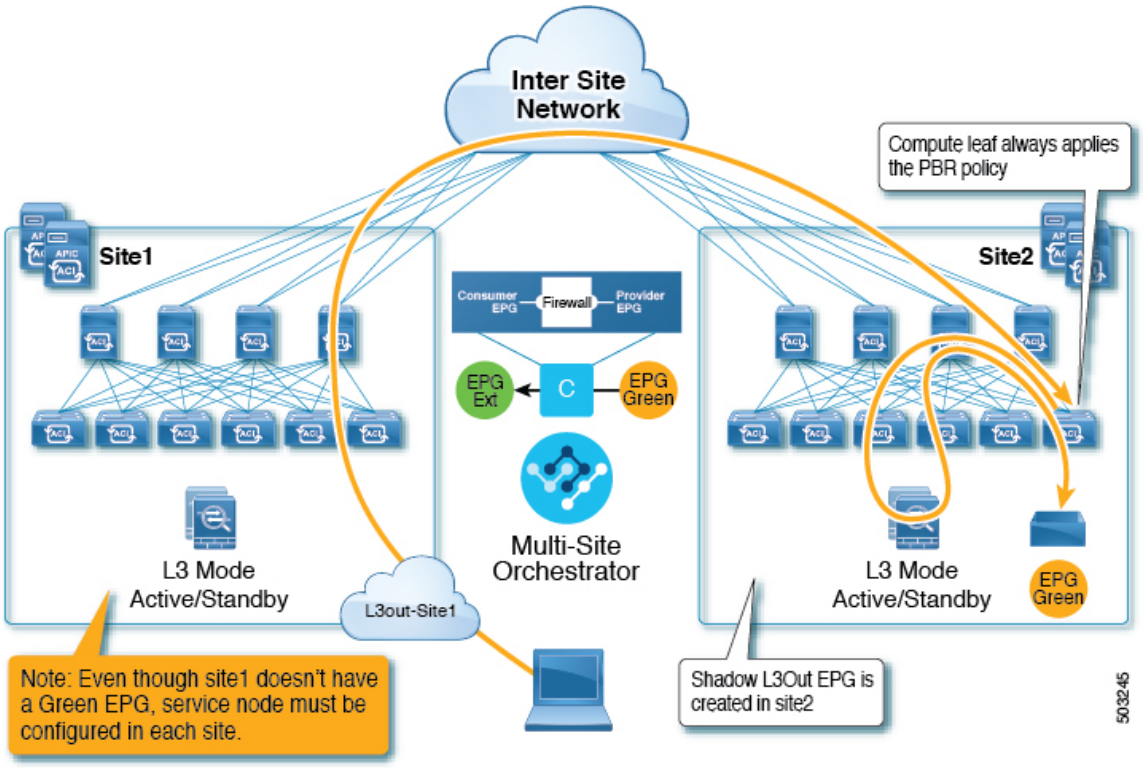
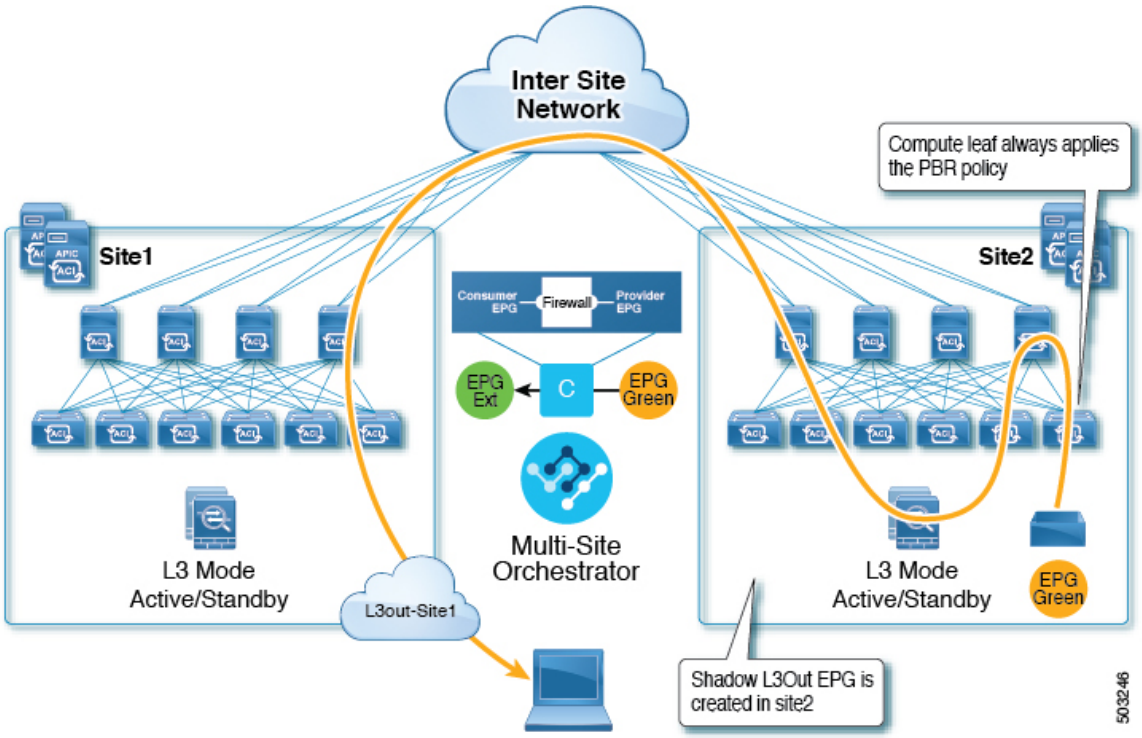


図 *4:* アウトバウンド トラフィック



注意事項と制約事項

サイト間 L3Out を設定する際には次の制約事項が適用されます。

- PBR を使用したサイト間 L3Out では、次の使用例がサポートされています。
  - アプリケーション EPG をコンシューマとする Inter-VRF サイト間 L3Out。

    VRF 間コントラクトの場合、L3Out へ関連付けられている外部 EPG がプロバイダである必要があります。

    この使用例は、Cisco APIC リリース 4.2(5) 以降またはリリース 5.1(x) を実行しているサイトでサポートされていますが、APIC リリース 5.0(x) ではサポートされていません。

  - アプリケーション EPG がプロバイダまたはコンシューマのいずれかである VRF 内サイト間 L3Out

    この使用例は、Cisco APIC リリース 4.2(5) 以降またはリリース 5.1(x) を実行しているサイトでサポートされていますが、APIC リリース 5.0(x) ではサポートされていません。

  - ファイアウォール ノード専用の PBR を使用したサイト間中継ルーティング（L3Out-to-L3Out）

ロードバランサへのトラフィックのリダイレクトはサポートされていません。

この使用例は、Cisco APIC リリース 6.0(3) 以降を実行しているサイトでサポートされています。

- EPG-to-L3Out のユース ケースでは、アプリケーション EPG をストレッチまたはサイト ローカルにすることができます。
- EPG-to-L3Out のユース ケースでは、ワンアームとツーアームの両方の導入モデルがサポートされています。 L3Out-to-L3Out の使用例では、ワンアーム ファイアウォール デバイスのみがサポートされます。

  ワンアーム展開では、サービス グラフの内部インターフェイスと外部インターフェイスの両方が同じブリッジ ドメインに接続されます。ツーアーム展開では、サービス グラフ インターフェイスは個別の BD に接続されます。
- EPG-to-L3Out ユース ケースについては、PBR を使用してロード バランサを構成する場合、ロード バランサと仮想 IP（VIP）の実サーバは同じサイトに存在する必要があります。PBR がディセーブルの場合、ロードバランサと実サーバは異なるサイトに存在できます。

  L3Out-to-L3Out の場合は、ロードバランサをサポートしていません。
- 1 つのサイトの L3Out と別のサイトの EPG 間、または異なるサイトの 2 つの L3Out 間ですでに構成されているコントラクトでサービス チェーンを有効にして、サービス デバイスを挿入する前に、サイト間 L3Out の基本的なユース ケースを構成しておく必要があります。

  PBR を使用しないサイト間 L3Out の展開に関する詳細な手順については、「サイト間 L3Out」の章を参照してください。

サービス デバイス テンプレートの作成

- 注意事項と制約事項 （6 ページ） 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。

ここでは、サービスグラフの1つ以上のデバイスを設定する方法について説明します。

ステップ 1 Nexus Dashboard Orchestrator の GUI にログインします。

ステップ 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。

ステップ 3 **[サービスノード（Service Nodes）]** タブを選択します。

ステップ 4 サービス デバイス テンプレートを作成し、サイトに関連付けます。

a) **[テナント テンプレートの** > **構成 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、それら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。

ステップ 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設定）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、トラフィックのリダイレクト先であるサービスを定義します。このリリースでは、サービス クラスタは、アクティブ/アクティブ クラスタ、アクティブ/スタンバイ クラスタ、または上記に示す複数の独立したノードのクラスタ内の、単一ノード ファイアウォール デバイスで構成する必要があります。

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ユースケースに基づいて事前に入力されています。

c) **[デバイス タイプ（Device Type）]** を選択します。

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

e) **[接続モード（Connectivity Mode）]** を選択します。

（注） L3Out-to-L3Out の使用例を構成する場合は、`[ワンアーム（One Arm）]` を使用する必要があります。

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。

vzAny の使用例の場合、このリリースでは、ブリッジ ドメインへのサービス デバイスの接続のみがサポートされます。

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、前のセクションで作成した拡張サービス BD です（例：`[FW 外部（FW-external）]`）。

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、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）]** 領域で **[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**：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**：このサービス 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**：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。

  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**：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**：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**：サービス ノード トラッキングのさまざまな詳細設定を設定できます。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。

コントラクトへのサービス チェーンの追加

基本のサイト間 L3Out ユースケースとサービス デバイス テンプレートを展開した後、L3Out とアプリケーション EPG または別の L3Out の間で作成したコントラクトにサービスチェーンを追加することで、ポリシーベースのリダイレクションを追加できます。

ステップ 1 コントラクトを定義したアプリケーション テンプレートに戻ります。

ステップ 2 コントラクトを選択します。

ステップ 3 **[サービス チェーン（Service Chaining）]** 領域で、**[+ サービス チェーン（+Service Chaining）]** をクリックします。

ステップ 4 **[デバイス タイプ（Device Type）]** を選択します。

（注） L3Out-to-L3Out の使用例を構成している場合、この使用例はファイアウォール デバイスのみをサポートします。

ステップ 5 **[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。

ステップ 6 **[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。

ステップ 7 **[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。

ステップ 8 **[追加（Add）]** をクリックして続行します。

ステップ 9 **[保存（Save）]** をクリックして、テンプレートを保存します。

ステップ 10 **[テンプレートの展開（Deploy）]** をクリックして、再展開します。

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。