Cisco Multi-Site 導入ガイド、ACI ファブリック

Contents

表 1.　　マニュアルの変更履歴

日付	バージョン	変更
2021 年 10 月 3 日	1.0	• 初期バージョン
2021 年 10 月 14 日	2.0	• 「ACI マルチポッドと ACI マルチサイトの統合」の追加 • いくつかのタイプミスとその他の小さな編集を修正しました

概要

このドキュメントの主な目的は、複数の Cisco ACI Multi-Site の使用例に固有の導入および構成情報を提供することです。ACI Multi-Site は、地理的に分散したデータセンターを相互接続し、一貫したエンドツーエンドのポリシー適用とともに、これらのロケーション間のレイヤ 2 およびレイヤ 3 接続を拡張するために広く使われるシスコのアーキテクチャです。

Cisco Multi-Site アーキテクチャの機能コンポーネント、データ プレーン通信の仕組み、および ACI ファブリック間の到達可能性情報の交換に使用されるコントロール プレーン プロトコルの詳細については、このホワイトペーパーでは説明しません。この導入ガイドを最大限に活用するための前提条件として、次のリンクにある ACI Multi-Site アーキテクチャ全体とその主な機能を説明するホワイトペーパーに目を通しておいてください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html

このガイドはさまざまなセクションに分かれており、それぞれが特定の導入面に対応しています。

- サイト間ネットワーク接続のプロビジョニング：このセクションでは、さまざまな ACI ファブリックを相互接続するために使用される ISN インフラストラクチャを構築するネットワークデバイスに必要な特定の設定について説明します。
- 特定の Multi-Site ドメインへの ACI ファブリックの追加：このパートでは、同じ Multi-Site ドメインに異なる ACI ファブリックを追加するために Cisco Nexus Dashboard Orchestrator NDO（以前は Cisco Multi-Site Orchestrator – MSO）で実行された必要なインフラストラクチャ設定について説明します。

  注：このペーパーに記載されている考慮事項のほとんどは、元の仮想 NDO クラスタ（ソフトウェア リリース 3.1(1) まで使用可能）を利用した導入にも適用されます。ただし、Orchestrator は Cisco Nexus Dashboard コンピューティング プラットフォーム上で有効なサービスとしてのみサポートされるため、このドキュメントの残りの部分では、Nexus Dashboard Orchestrator（NDO）の導入についてのみ説明します。
- Nexus Dashboard Orchestrator のスキーマとテンプレートの定義：このセクションでは、特定のテナントポリシーをプロビジョニングするためのスキーマとテンプレートの設定方法について説明します。Nexus Dashboard Orchestrator は設計上、これらのポリシー要素を定義する方法に多くの柔軟性を提供していますが、目標はベスト プラクティスである推奨事項を提供すること です。
- サイト間（イーストウェスト）のエンドポイント接続の確立：このセクションでは、異なるファブリックに EPG/BD を導入し、それらの間にレイヤ 2 およびレイヤ 3 のサイト間接続を確立する方法に焦点を当てます。セキュリティの観点から、EPG 間の特定のポリシーをセキュリティ コントラクトを使用して定義する方法について説明します。また、優先グループと vzAny を使用して最初にポリシーの側面を削除することで、接続の確立を簡素化する方法についても説明します。
- 外部ネットワーク ドメイン（ノースサウス）とのエンドポイント接続の確立：このパートでは、異なるファブリックの ACI リーフ ノードに接続されたエンドポイントが、ローカル L3Out t またはリモートを介して到達可能な外部リソースと通信できるようにするための L3Out 設定の導入に焦点を当てます。L3Out 接続（サイト間 L3Out）。
- ネットワーク サービスの統合：ここでは、サービス グラフと PBR を活用します。同じファブリックまたは別のファブリックに属する EPG 通信の間（イーストウェスト）、または ACI と外部ネットワーク ドメインの間（ノースサウス）に、通信ネットワーク サービスを挿入する方法を特に学びます。

上記のさまざまな使用例のプロビジョニングに使用されるトポロジは、次の図 1 のとおりです。

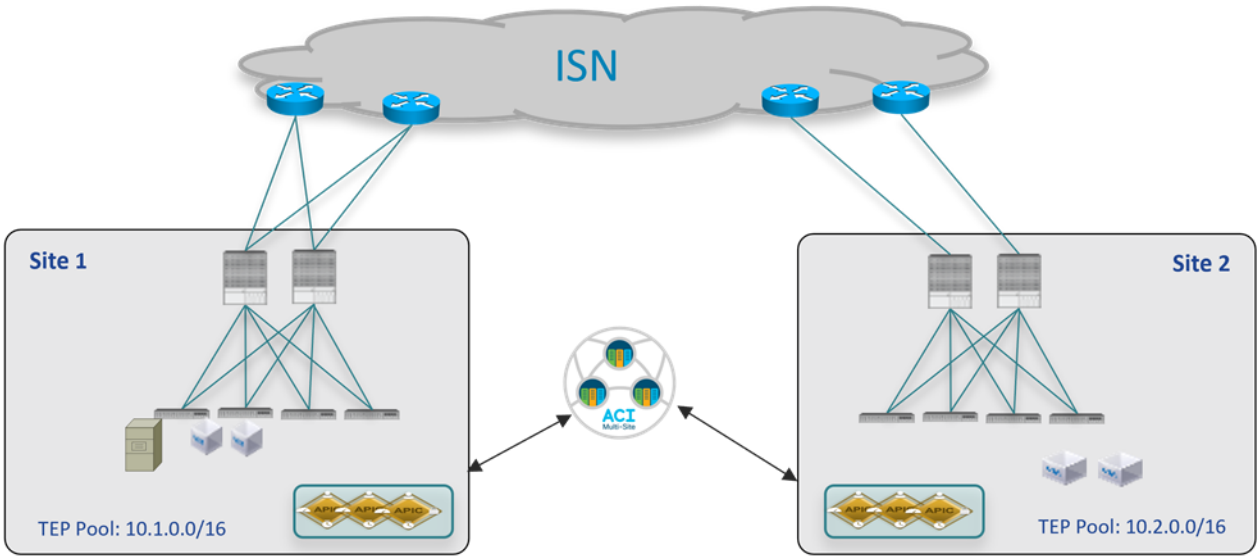


図 1.
2 つのファブリックへの Multi-Site の導入

ACI ファブリックは、異なるファブリックのエンドポイント間で発生する VXLAN 通信のトランスポートを表すサイト間ネットワーク（ISN）ルーテッド ドメインを介して接続されます。念のため、同じ Multi-Site ドメインの異なる ACI ファブリック部分の間に遅延の制限はありません。遅延に関する唯一の考慮事項は次のとおりです。

- 最大 150 ミリ秒の RTT は、Orchestrator サービスが有効になっている Nexus ダッシュボード クラスタ ノード間でサポートされる遅延です。
- 最大 500 ミリ秒の RTT は、各 Nexus Dashboard Orchestrator ノードと Multi-Site ドメインに追加された APIC コントローラ ノード間の遅延です。つまり、Multi-Site アーキテクチャは、世界中に地理的に分散できる ACI ファブリックを管理できるようにゼロから設計されています。

このホワイトペーパーで説明するすべての使用例は、このホワイトペーパーの作成時点で入手可能な最新の ACI および Nexus Dashboard Orchestrator ソフトウェア リリースを使用して検証されています。具体的には、2 つの ACI ファブリックは ACI 5.1(1) コードを使用していますが、Nexus Dashboard Orchestrator では 3.5(1) リリースを使用しています。ただし、Nexus Dashboard Orchestrator リリース 2.2(1) 以降、Nexus Dashboard Orchestrator リリースと ACI ソフトウェア リリースの間に相互依存関係はなく、Nexus Dashboard Orchestrator リリース 3.2(1) 以降を使用した Multi-Site 展開では、同じ Multi-Site ドメインの一部であるソフトウェア リリース（ACI 4.2(4) 以降）が混在するファブリックを使用できます。

注： この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFP のドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

サイト間ネットワーク接続のプロビジョニング

Multi-Site ドメインを作成する最初の手順は、異なる ACI ファブリックを相互接続し、VXLAN トラフィックを伝送してサイト間でレイヤ 2 およびレイヤ 3 接続を確立するために使用されるネットワークインフラストラクチャのプロビジョニングを行うことです。ISN は APIC または Orchestrator サービスによって管理されないため、各ファブリックを ISN インフラストラクチャに接続するには、スパイン ノードの設定を開始する前に個別に事前プロビジョニングを行う必要があります。

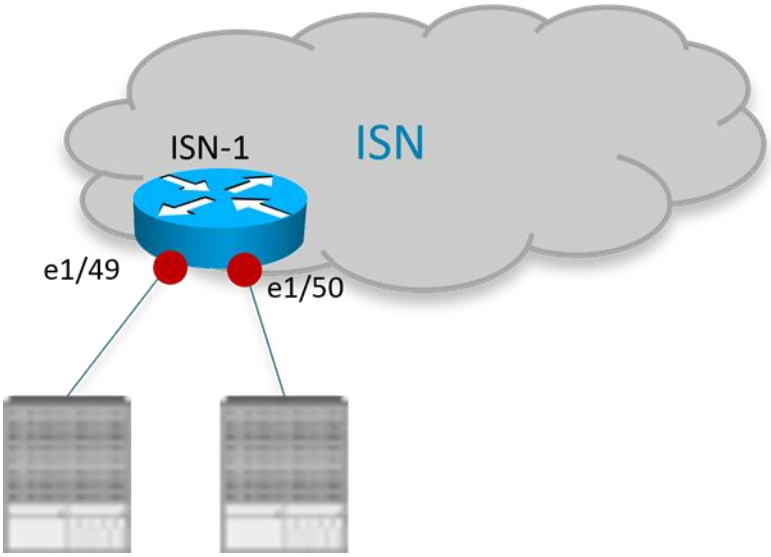


図 2.
スパイン ノードに接続する ISN ルータ

各ファブリックのスパイン ノードに接続する ISN デバイスのインターフェイスは、異なるファブリックのスパイン ノード間でインフラストラクチャ（アンダーレイ）プレフィックスを交換できるように、ルーティング隣接関係を確立するポイントツーポイント L3 リンクとして展開する必要があります。次の設定例は、ローカル ACI ポッドのスパイン ノードに接続するために図 2 の ISN ルータで定義されたインターフェイスの特定の例を示しています（他のルータのインターフェイスも同様に設定されます）。

注： 次の構成は、ISN ノードとしての Nexus 9000 スイッチの展開に適用されます。異なる HW プラットフォームを使用する場合は、特定の CLI コマンドをわずかに変更する必要があります。

ISN-1 ルータ：

```
interface Ethernet1 / 49.4
  description L3 Link to Pod1-Spine1
  mtu 9150
  encapsulation dot1q 4
  vrf member
  ip address 192.168.1.1/31
  ip ospf network point-to-point
  ip router ospf ISN area 0.0.0.0
  no shutdown
!
interface Ethernet1/50.4
```

```
description L3 Link to Pod1-Spine2
mtu 9150
encapsulation dot1q 4
vrf member
ip address 192.168.1.5/31
ip ospf network point-to-point
ip router ospf ISN area 0.0.0.0
no shutdown
```

- 上記のように、ルータをスパイン ノードに接続する物理リンク上にサブ インターフェイスを作成する必要があります。これは、リーフ ノードとスパイン ノードが常に dot1q タグ付きトラフィックを生成するように要求する特定の ACI 実装のためです（外部 ISN インフラストラクチャに接続する場合、特定の VLAN タグ 4 が常に ACI スパイン ノードによって使用されます）。これらのインターフェイスは、別の IP サブネットの一部としてアドレス指定する必要があるポイントツーポイント レイヤ 3 リンクのままであることに注意してください（/30 または /31 マスクの使用が一般的に推奨されます）。これは、ISN ルータの主な要件は、異なるローカル リンクに設定されたサブ インターフェイスで同じ VLAN タグ 4 を使用できるようにすることです。最新のスイッチおよびルータのほとんどは、この機能を備えています。
- インターフェイスの MTU は、VXLAN トラフィック（50 バイト）の余分なオーバーヘッドを考慮する必要があります。上記の設定例に示す 9150B の値は、外部 ISN インフラストラクチャに接続するスパイン サブ インターフェイスのデフォルト MTU と一致します。これにより、OSPF 隣接関係が正常に確立されます。ただし、必要な最小値は主に ACI ファブリックに接続されたエンドポイントによって生成されるトラフィックの MTU に依存するため、ISN ルータでこのような大規模な MTU をサポートする必要はありません。詳細については、『ACI Multi-Site』の「サイト間ネットワーク（ISN）の導入に関する考慮事項」セクションを参照してください。

  https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html#IntersiteNetworkISNdeploymentconsiderations
- ISN ルータのインターフェイスは、専用 VRF の一部として、またはグローバル テーブルに展開できます。 可能な場合は、専用 VRF を使用することを強く推奨します。これは、運用の簡素化の観点からも、マルチサイト コントロールおよびデータ プレーンに厳密に必要な数よりも多くのプレフィックスをスパイン ノードに送信しないようにするためにも（ISN インフラストラクチャが他の接続サービスを提供するためにも共有されます）。
- ACI リリース 5.2(3) および Nexus Dashboard Orchestrator リリース 3.5(1) から、スパインと ISN デバイス間のアンダーレイ隣接を確立するために BGP を導入することもできます。ただし、このホワイトペーパーでは、OSPF の使用に焦点を当てています。ACI Multi-Site アーキテクチャの導入以降、広く展開されているからです。

ISN ネットワークのコアを構築するデバイス間で、特にそのインフラストラクチャが地理的に分散した場所にまたがる場合は、異なるルーティング プロトコル（通常は BGP）が使用されることがよくあります。これは、同じ Multi-Site ドメインの一部のファブリック間で交換する必要がある特定のプレフィックスを OSPF から BGP に再配布する必要があることを意味します。これにより、サイト間で交換されるプレフィックスをかなりの程度選択的に制御できます。「Nexus Dashboard Orchestrator Sites Infra Configuration」のセクションで詳しく説明しますが、サイト間制御とデータ プレーン接続を確立するために必要なプレフィックスは、次に示すとおりわずかです。

- 各スパイン ノードの BGP EVPN ルータ ID。リモート スパイン ノードへの MP-BGP EVPN 隣接関係を確立します。

- リモート サイトとのユニキャスト レイヤ 2 およびレイヤ 3 データ プレーン接続に使用される、同じ ACI ファブリックの各ポッド部分のオーバーレイ ユニキャスト TEP（O-UTEP）エニーキャスト アドレス。
- リモート サイトから発信されたレイヤ 2 ブロードキャスト/不明なユニキャスト/マルチキャスト（BUM）トラフィックを受信するために使用される、同じ ACI ファブリックのすべてのポッド部分で共有されるオーバーレイ マルチキャスト TEP（O-MTEP）エニーキャスト アドレス。
- 1 つ（または複数）の外部 TEP プールを使用して、リモート サイトとのサイト間 L3Out 接続を有効にします。

各ファブリックの起動に使用される元のインフラ TEP プール（図 1 の例では 10.1.0.0/16 と 10.2.0.0/16）は、サイト間で交換する必要がないため、プロトコル間で再配布されません。次の例は、上記のいくつかのプレフィックスの交換を可能にする再配布の例を示しています（この設定は ISN デバイスとして導入された Nexus 9000 スイッチに適用されます）。

- IP プレフィックス リストとルート マップを定義して、ローカル プレフィックスをリモート サイトにアドバタイズします。

```
ip prefix-list LOCAL-MSITE-PREFIXES seq 5 permit <BGP-EVPN-RID Site1-Spine1>
ip prefix-list LOCAL-MSITE-PREFIXES seq 10 permit <BGP-EVPN-RID Site1-Spine2>
ip prefix-list LOCAL-MSITE-PREFIXES seq 5 permit <BGP-EVPN-RID Site1-Spine1>
ip prefix-list LOCAL-MSITE-PREFIXES seq 20 permit <O-MTEP-Site1>
ip prefix-list LOCAL-MSITE-PREFIXES seq 25 permit <EXT-TEP-POOL-Site1>
!
route-map MSITE-PREFIXES-OSPF-TO-BGP permit 10
  match ip address prefix-list LOCAL-MSITE-PREFIXES
```

- IP プレフィックス リストとルート マップを定義して、リモート サイトから受信するプレフィックスを指定します。

```
ip prefix-list REMOTE-MSITE-PREFIXES seq 5 permit <BGP-EVPN-RID Site2-Spine1>
ip prefix-list REMOTE-MSITE-PREFIXES seq 10 permit <BGP-EVPN-RID Site2-Spine2>
ip prefix-list REMOTE-MSITE-PREFIXES seq 15 permit <O-UTEP-Pod1-Site2>
ip prefix-list REMOTE-MSITE-PREFIXES seq 20 permit <O-MTEP-Site2>
ip prefix-list REMOTE-MSITE-PREFIXES seq 25 permit <EXT-TEP-POOL-Site2>
!
route-map MSITE-PREFIXES-BGP-TO-OSPF permit 10
  match ip address prefix-list REMOTE-MSITE-PREFIXES
```

- OSPF と BGP 間でプレフィックスを再配布するためにルート マップを適用します（逆も同様）。

```
router bgp 3
vrf ISN
  address-family ipv4 unicast
    redistribute ospf ISN route-map MSITE-PREFIXES-OSPF-TO-BGP
!
router ospf ISN
  vrf ISN
    redistribute ospf ISN route-map MSITE-PREFIXES-OSPF-TO-BGP
```

Multi-Site ドメインへの ACI ファブリックの追加

ここでは、Multi-Site ドメインの一部であるファブリックを Nexus Dashboard Orchestrator に追加する方法について説明します。

Nexus Dashboard Orchestrator への ACI ファブリックのオンボーディング

ISN の設定がプロビジョニングされれば、ACI ファブリックを Nexus Dashboard Orchestrator にオンボードし、必要なインフラ設定を実行して、各サイトを ISN に正しく接続し、必要なコントロールプレーンピアリングを確立できます。具体的には、各スパインは、直接接続されたファーストホップ ISN ルータとの OSPF 隣接関係、およびリモートサイトのスパイン ノードとの MP-BGP EVPN ピアリングを確立します。

Multi-Site Orchestrator リリース 3.1(1) までは、サイトのオンボーディング手順を MSO で直接実行する必要がありました。リリース 3.2(1) 以降では、Nexus Dashboard Orchestrator は、Nexus Dashboard コンピューティングクラスタで実行されるサービスとしてのみサポートされます。その場合、サイトのオンボーディング手順を Nexus ダッシュボードで直接実行する必要があります（そして、サイトがホストされたサービスで利用可能になります。 これは、特定の例の Nexus Dashboard Orchestrator の場合と同様です）。「Nexus Dashboard Orchestrator サイトのインフラ設定」のセクションで説明されている必要なインフラ設定手順は、古い MSO リリースを利用する導入でも有効です。

図 3 は、ACI ファブリックを Nexus ダッシュボードにオンボードするプロセスを開始する方法を示しています。

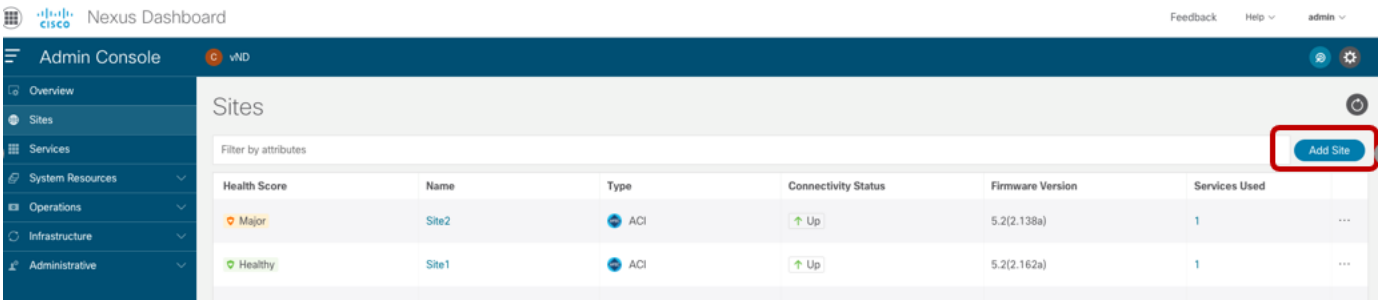


図 3.
NDO 3.1(1) へのサイトの追加

[サイトの追加 (Add Site)] を選択すると、次の画面が開き、NDO にオンボーディングする必要がある ACI ファブリックの情報を指定できます。

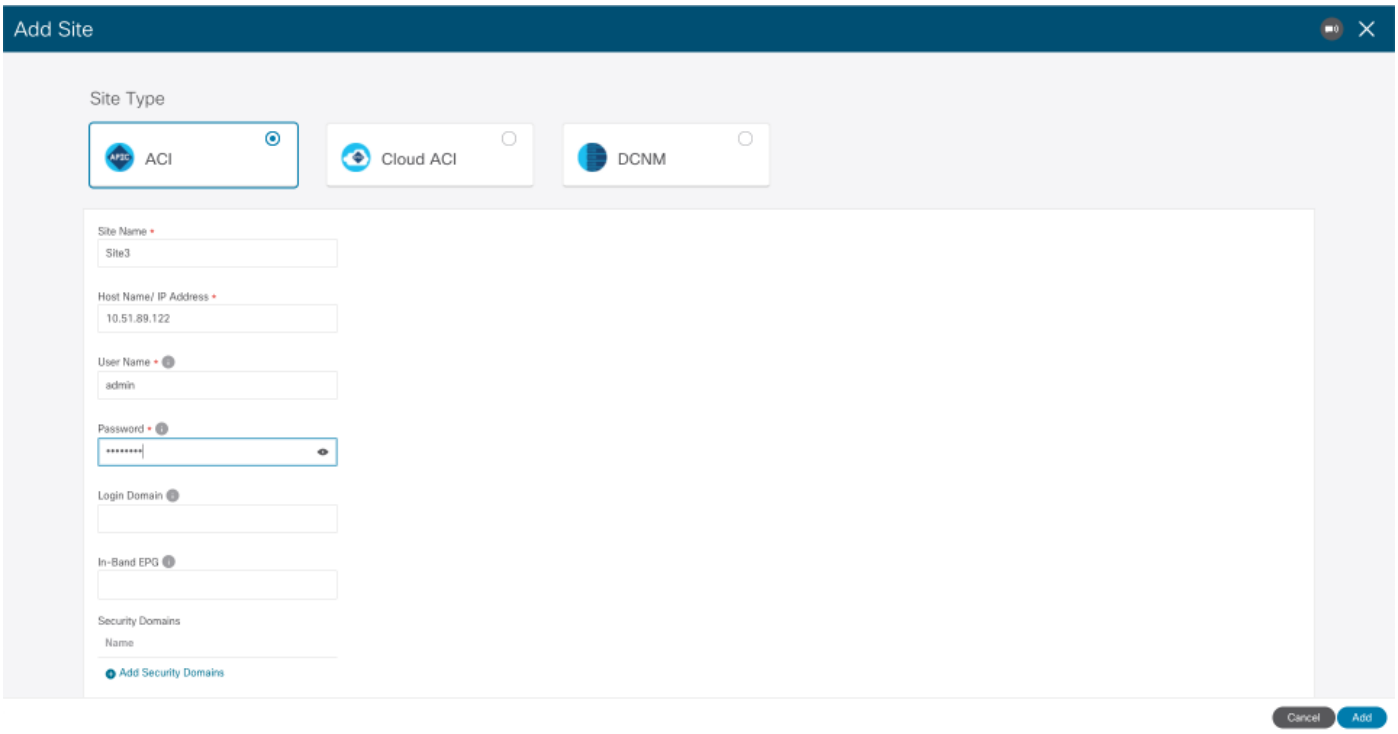


図 4.
ACI ファブリック情報の指定

ACI ファブリックを Nexus ダッシュボードにオンボードするには、次の情報が必要です。

- [サイト名 (Site Name)]：Nexus ダッシュボードで ACI ファブリックを参照するために使用される名前。
- [ホスト名/IP アドレス (Host Name / IP Address)]：追加するファブリックを管理する APIC クラスタ ノードの 1 つの IP アドレス。このドキュメントの執筆時点で、Nexus ダッシュボード上で Orchestrator サービスのみを実行している場合は、ここで APIC のアウトオブバンド（OOB）またはインバンド（IB）アドレスを指定できます。同じ ND クラスタ（Insights など）で他のサービスを有効にする場合は、代わりに IB アドレスのみを使用してファブリックをオンボードする必要があります。詳細については、特定のサービス インストール ガイドを参照してください（cisco.com から入手可能）。
- [ユーザー名 (User Name)] と [パスワード (Password)]：Nexus ダッシュボード、およびシングル サインオン機能を介して Nexus ダッシュボードでホストされているサービスの UI に接続するために使用されるクレデンシャル。
- [ログイン ドメイン (Login Domain)]：デフォルトでは、ユーザーは Nexus ダッシュボードでローカルに認証されます。代わりに、特定のログイン ドメイン（Radius、TACACS など）を使用する場合は、ドメイン名を Nexus ダッシュボードで定義し、このフィールドで指定できます。
- [インバンド EPG (In-Bad EPG)]：Nexus Dashboard 上のホスティング サービス（Insight など）が、このサイトからのデータ ストリーミングにインバンド接続を使用している場合にのみ必要です。
- セキュリティ ドメイン：

ACI ファブリック オンボーディング プロセスの最後のオプションの手順では、この特定のファブリックの地理的位置を表すために、マップ上のサイトのピンをドロップします。

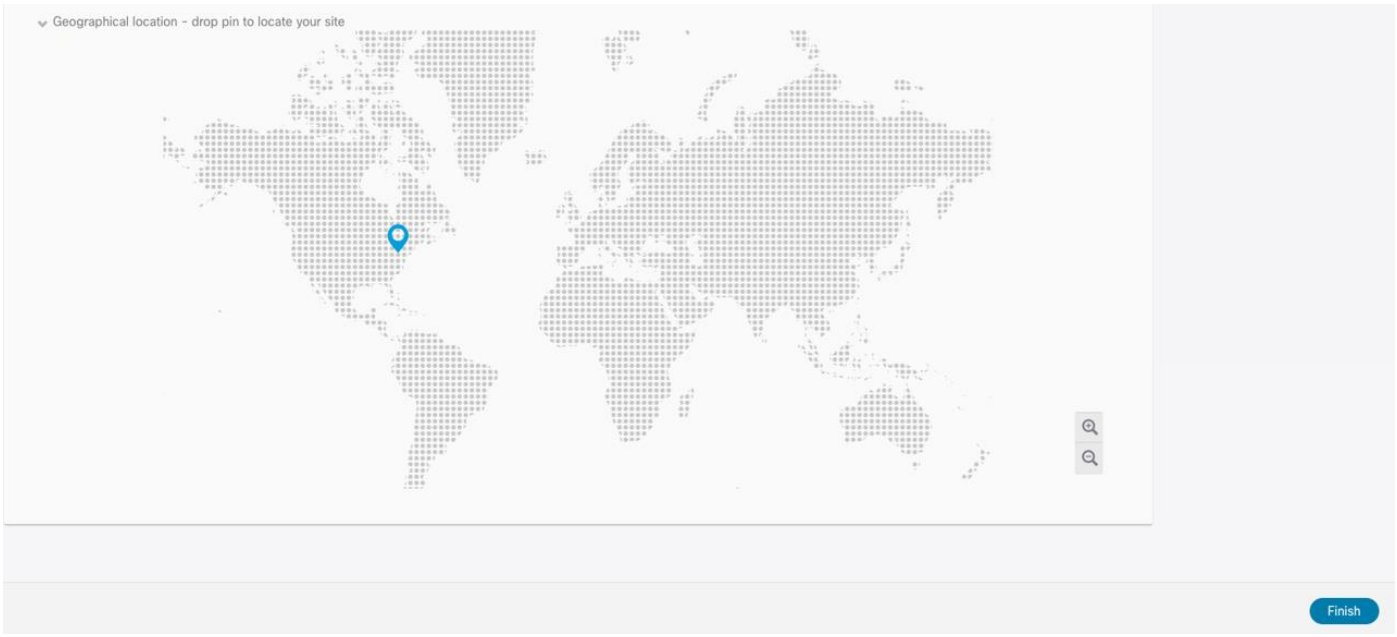


図 5.
サイト上のピンをマップにドロップする

Nexus ダッシュボードにオンボードする必要があるすべてのファブリックに対して、同じ手順を繰り返します。最後に、これらすべてのサイトが「管理対象外」状態で Nexus Dashboard Orchestrator UI に表示されます。ユーザーは、同じ ACI Multi-Site ドメインの一部となるファブリックを選択的に「管理対象」として設定できます。

サイトが [管理対象 (Managed)] に設定されている場合、ユーザーは特定のサイト ID を入力するよう求められます。これは、そのサイトを一意に識別する必要があります。

注： サイト ID は、APIC レベルで設定されているファブリック ID とは異なります。同じファブリック ID で設定されたファブリックは、一意のサイト ID が割り当てられている限り、同じマルチサイトドメインの一部になることができます。

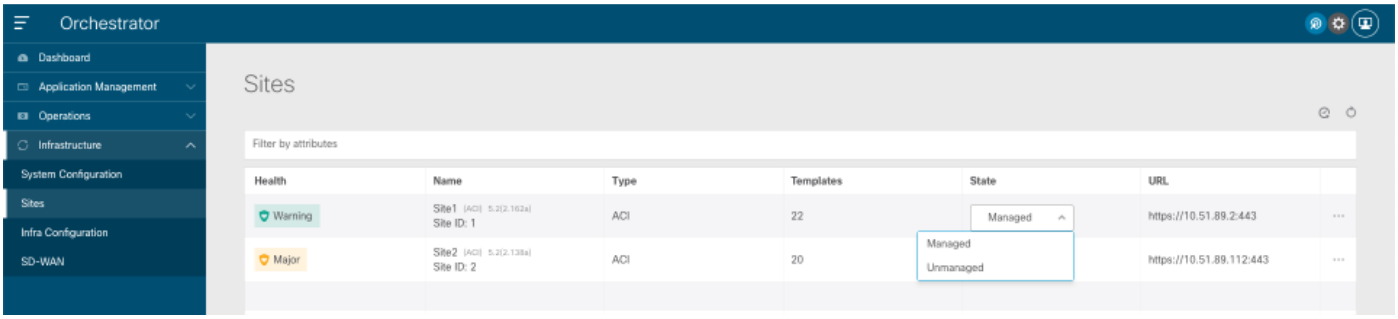


図 6.
NDO UI でのサイトの表示

ファブリックが「管理対象」になると、NDO ダッシュボードに表示されます。

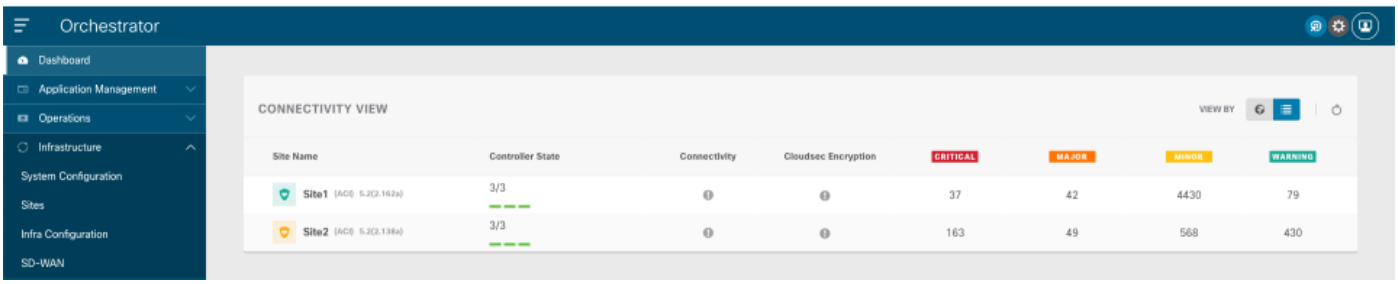


図 7.
NDO ダッシュボードの接続ビュー

上記のように、Orchestrator サービスは、オンボードされたサイトの各 APIC コントローラ ノードの健全性と、各 APIC ドメインで発生した特定の障害（関連する重大度）を収集できます。ファブリックが Orchestrator Service にオンボーディングされたが、各サイトを外部 ISN に接続するためのインフラ設定手順がまだ実行されていないという単純な理由により、サイト間の接続には警告サインが表示されます。

Nexus Dashboard Orchestrator サイト インフラストラクチャ設定

ファブリックが Nexus ダッシュボードにオンボーディングされ、Orchestrator サービスで「Managed」として設定された後、各サイトを ISN に接続できるように特定のインフラストラクチャ設定を実行する必要があります。これは、各ファブリックのスパインが直接接続された ISN ルータとの OSPF 隣接関係を最初に確立し、サイト間コントロール プレーンとデータ プレーンの接続を正常に確立するために必要な「アンダーレイ」ネットワーク情報を交換するために必要です。

次の表 1 に、インフラ設定を開始する前に利用できる特定の情報を示します。これらのさまざまな IP プレフィックスの意味の詳細については、ACI Multi-Site ペーパーの「サイト間ネットワーク（ISN）の導入に関する考慮事項」のセクションを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html#IntersiteNetworkISNdeploymentconsiderations

サイト	ノード	ISN へのインターフェイス	ISN へのインターフェイスの IP アドレス	BGP-EVPN ルータ ID	O-UTEP	O-MTEP
1	Spine-1101	e1/63 e1/64	192.168.1.0/31 192.168.1.2/31	172.16.100.1	172.16.100.100	172.16.100.200
1	Spine-1102	e1/63 e1/64	192.168.1.4/31 192.168.1.6/31	172.16.100.2	172.16.100.100	172.16.100.200
2	Spine-2101	e1/63 e1/64	192.168.2.0/31 192.168.2.2/31	172.16.200.1	172.16.200.100	172.16.200.200
2	Spine-2102	e1/63 e1/64	192.168.2.4/31 192.168.2.6/31	172.16.200.2	172.16.200.100	172.16.200.200

表 2.　　サイトのインフラ設定の IP アドレス情報

インフラストラクチャ設定ワークフローは、Nexus Dashboard Orchestrator の左側のタブで [インフラストラクチャ (Infrastructure)]→[インフラストラクチャ設定 (Infra Configuration)] オプションを選択して開始します。

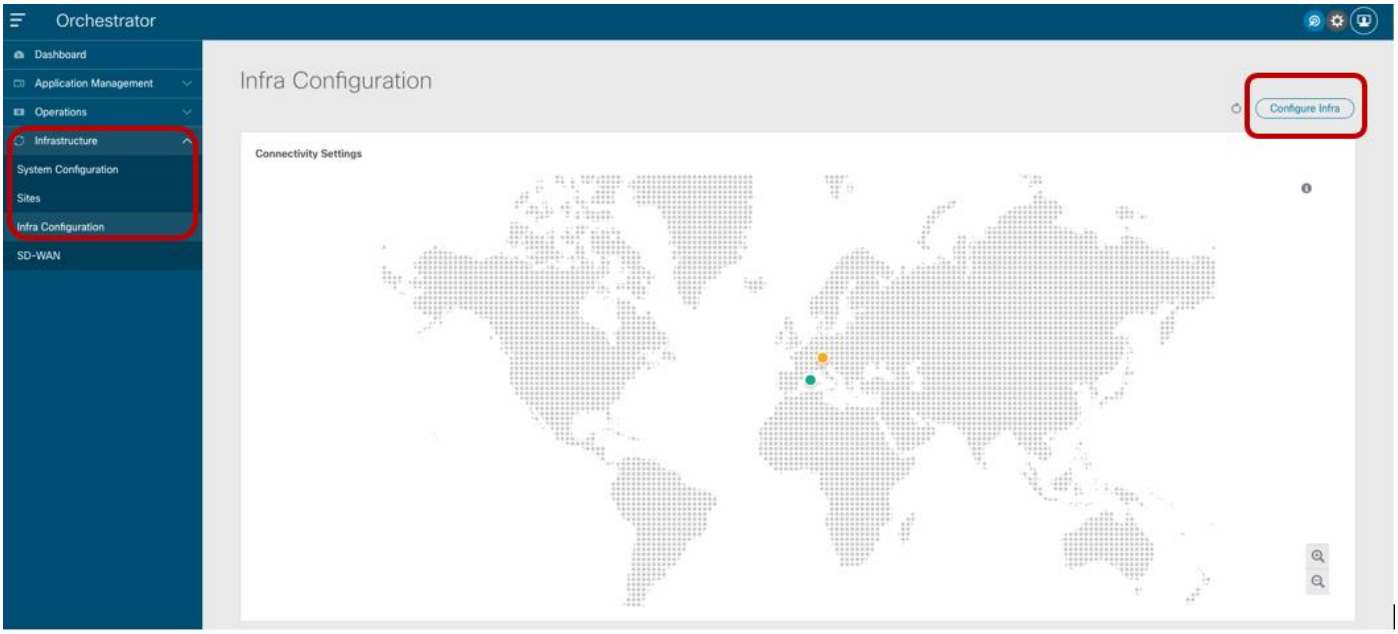


図 8.
サイト インフラストラクチャ設定プロセスの開始

[インフラの構成 (Configure Infra)] を選択すると、[ファブリック接続インフラ (Fabric Connectivity Infra)] ページがユーザーに表示されます。

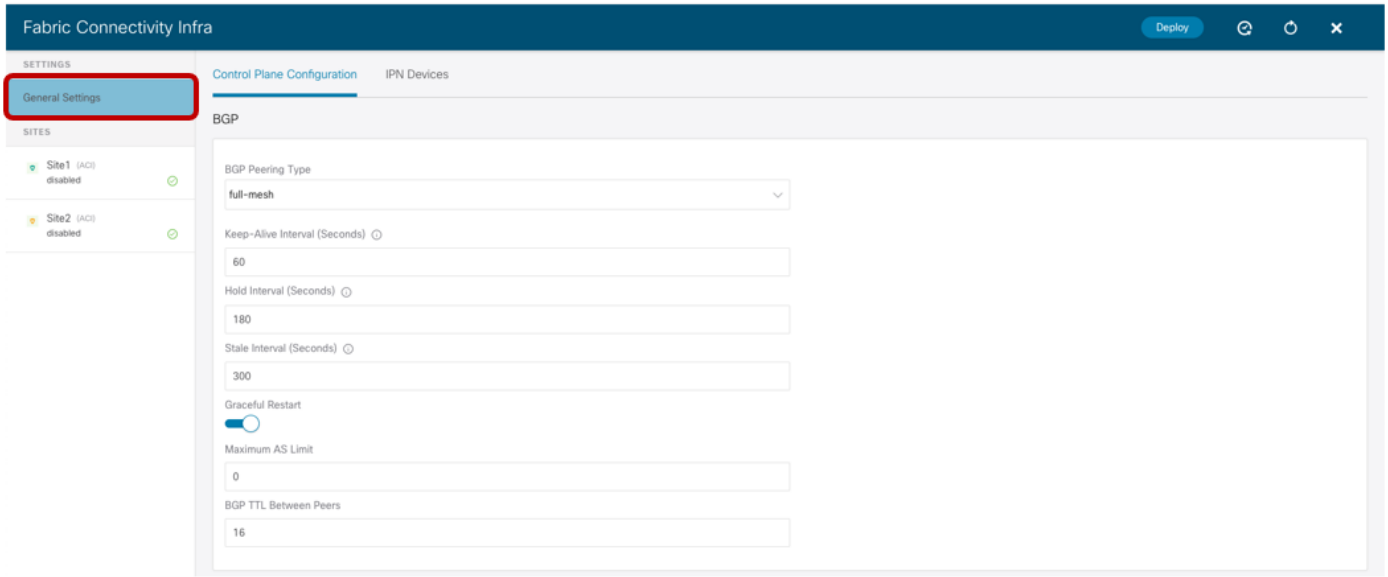


図 9.
インフラの構成の一般設定

[一般設定 (General Settings)] タブには [コントロール プレーンの構成 (Control Plane Configuration)] セクションがあり、必要に応じて、異なるファブリックに属するスパイン間で使用される MP-BGP EVPN コントロール プレーンに使用されるいくつかのデフォルト パラメータを調整できます。ほとんどの導入シナリオでは、これらのパラメータのデフォルト値を維持することを推奨します。これは、[BGP ピアリング タイプ (BGP Peering Type)] オプションにも適用されます。デフォルトでは、[フルメッシュ (full-mesh)] に設定されます。

これは、異なるサイトに展開されたスパイン ノードが、それらの間にフルメッシュの MP-BGP EVPN 隣接関係を確立することを意味します。これは、異なるサイトが同じ BGP 自律システム番号（ASN）の一部であるかどうかに関係なく発生します。代替オプションは、[ルート リフレクタ (route-reflector)] を選択することです。これは、ファブリックが同じ ASN の一部である場合にのみ有効です。また、[グレースフル ヘルパー (Graceful Helper)] ノブがデフォルトでオンになっていることにも注意してください。これは、BGP グレースフル リスタート機能（IETF RFC 4724 に記載）を有効にして、BGP スピーカーが BGP リスタート イベント中にフォワーディング ステートを維持できることを示すことができるようにするためです。

代わりに、特定のファブリックに関連付けられた左側のタブを選択して、サイト インフラストラクチャ設定を開始します。

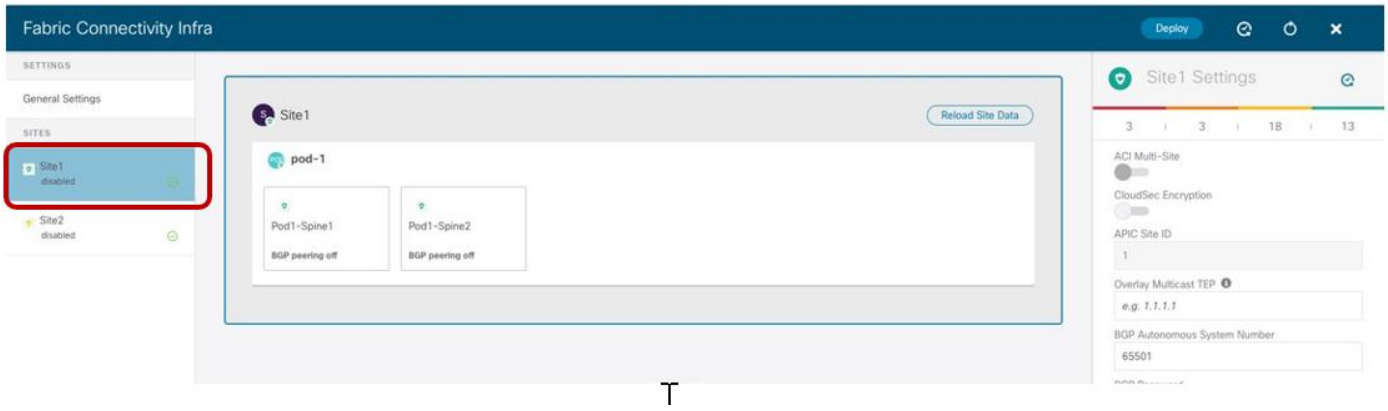


図 10.
特定のサイト インフラストラクチャ設定の開始

設定は、Nexus Dashboard Orchestrator UI で選択されている内容に応じて、サイト レベル、ポッド レベル、スパイン ノード レベルの 3 つの異なる手順で実行されます。

サイト レベルの設定

ACI サイト全体を識別するメイン ボックスをクリックすると、図 11 に示すパラメータを設定する機能が Orchestrator Service に提供されます。

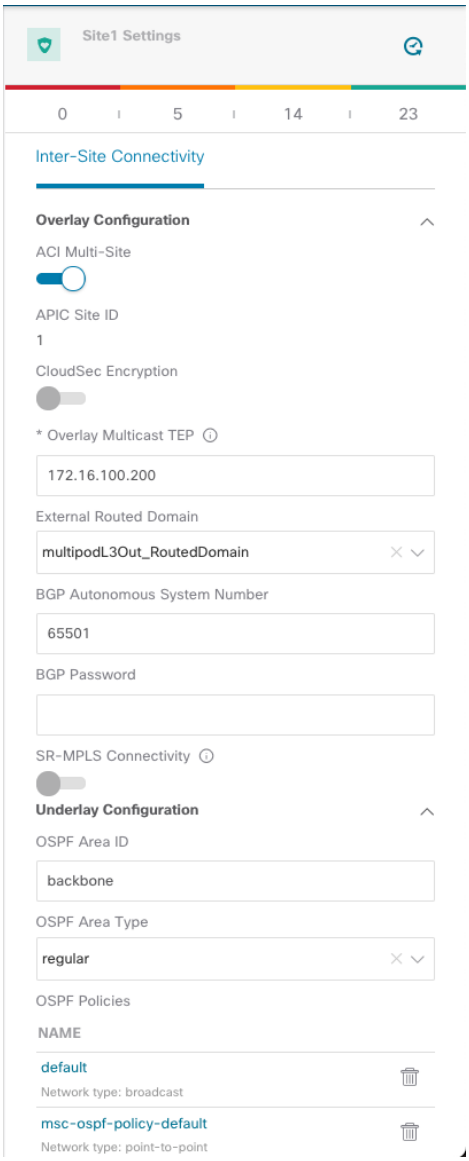


図 11.
サイト レベルの設定

- [ACI マルチサイト (ACI Multi-Site)] ノブ：これをオンにすると、ファブリックで Multi-Site が有効になり、他のサイトとのコントロール プレーンおよびデータ プレーンの接続を確立できます。これは、Nexus Dashboard Orchestrator が各接続サイトにローカルにポリシーを提供するためだけに導入されたものなので、ISN を介したサイト間通信が必要ない場合は必要ありません（この特定のシナリオでは ISN は必要ありません）。
- オーバーレイ マルチキャスト TEP：すべてのローカル スパイン ノードに展開され、リモート サイトから発信された BUM（またはレイヤ 3 マルチキャスト）トラフィックを受信するために使用されるエニーキャスト TEP アドレス。単一の O-MTEP アドレスは、単一のポッドまたはマルチポッド ファブリックであるかに関係なく、ACI ファブリックに関連付けられます。
- 外部ルーテッド ドメイン：これは、スパイン ノードを ISN に接続するためのファブリック アクセス ポリシーの一部として APIC で定義されます。Nexus Dashboard Orchestrator でのこのパラメータの指定

は厳密には必須ではありませんが、APIC レベルで定義されたスパインのアクセス ポリシーを持つことをお勧めします。

- [BGP 自律システム番号 (BGP Autonomous System Number)]：APIC から動的に取得されるローカル ASN 値。
- [OSPF 設定（OSPF 設定）（エリア ID、エリア タイプ、ポリシー）：これらは、スパインと直接接続された ISN ルータ間の OSPF 隣接関係を確立するために必要な OSPF パラメータです。

ポッドレベルの設定

ポッドを識別するボックスを選択すると、ポッドの固有の設定にアクセスできます。これらは、同じマルチポッド ファブリックの一部であるすべてのポッドに個別に適用される設定です（この例では、単一のポッドファブリックがあります）。

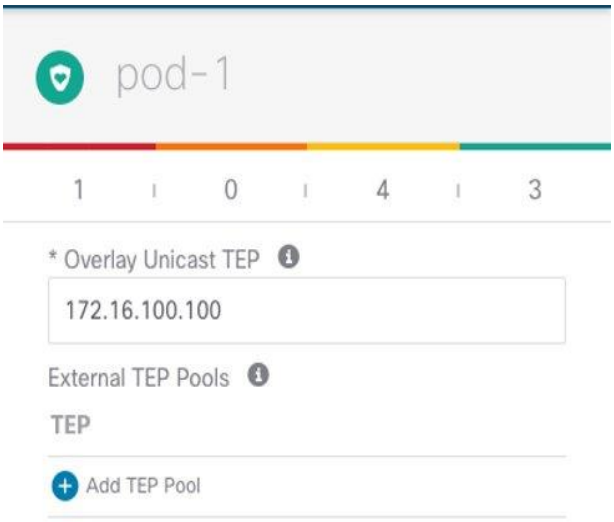


図 12.
ポッドレベルの設定

- オーバーレイ ユニキャスト TEP：ポッド内のすべてのローカル スパイン ノードに展開され、レイヤ 2 およびレイヤ 3 ユニキャスト トラフィック フローの送受信に使用されるエニーキャスト TEP アドレス。同じマルチポッド ファブリックの各ポッド部分は、一意の TEP アドレスを定義します。
- [外部 TEP プール (External TEP Pools)]：サイト間 L3Out 機能を有効にするときに必要なプレフィックス（「サイト間 L3Out の導入」を参照）。

スパインレベルの設定

最後に、特定のスパイン ノードごとに固有の設定を適用する必要があります。

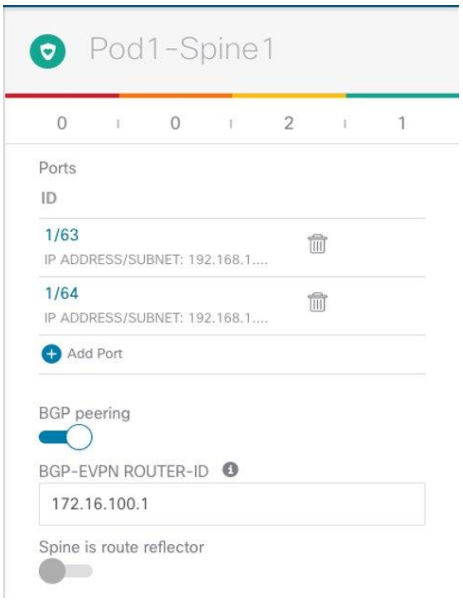


図 13.
スパイン レベルの設定

- ポート：ISN インフラストラクチャへの接続に使用されるローカル スパインのインターフェイスを指定します。インターフェイスごとに、次のパラメータを指定する必要があります。

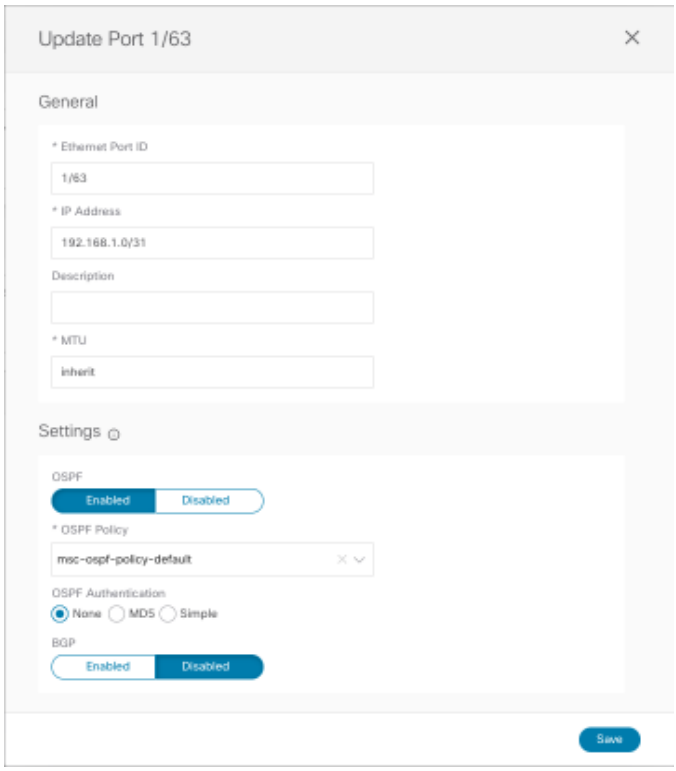


図 14.
ポート設定

- イーサネット ポート ID：ISN に接続されている特定のインターフェイス。ISN との間で送受信アンダーレイ トラフィックを伝送するために、サブ インターフェイスがプロビジョニングされます。

- IP アドレス：サブインターフェイスの IP アドレス。
- 説明：この特定のインターフェイスに関連付けるオプションの説明。
- MTU：サブインターフェースの MTU 値[継承（Inherit)] はデフォルト値の 9150B を保持しますが、ユーザーは必要に応じて別の値を指定できます。

```
Spine1011-Site1# show int e1/63.63
Ethernet1/63.63 is up
admin state is up, Dedicated Interface, [parent interface is Ethernet1/63
Hardware: 10000/100000/40000 Ethernet, address: 0000.0000.0000 (bia 780c.f0a2.039f)
Internet Address is 192.168.1.0/31
MTU 9150 bytes, BW 40000000 Kbit, DLY 1 usec
```

  ここで使用する値が ISN ルータで設定された MTU と一致することを推奨します（「サイト間ネットワーク接続のプロビジョニング」のセクションを参照）。
- OSPF ポリシー：サイト レベルの設定時に作成/選択された特定のポリシーを参照します。通常、これらが OSPF ポイントツーポイント インターフェイスであることを指定する必要があります。
- OSPF 認証：認証を有効にします（デフォルトでは無効）。

  注：OSPF が無効になっている場合、OSPF パラメータは表示されず、スパインと ISN デバイス間のアンダーレイ ピアリングに BGP を使用できるようにすると、異なる BGP パラメータが表示されます。
- BGP ピアリング：このノブを有効にして、スパインがリモート ファブリックのスパインと MP-BGP EVPN ピアリングを確立するようにします。ファブリックごとに少なくとも 2 つのスパインを（冗長性のため）このノブを有効にして設定する必要があります。他のローカル スパインは「フォワーダ」の役割を引き受けます。つまり、本質的には、リモート ACI に展開されたスパインではなく、「BGP ピアリング」がオンになっている同じ ACI ファブリックの他のポッドのスパインとのみ MP-BGP EVPN 隣接関係を確立します。ファブリック。これにより、サイト間ピアリングの全体的な冗長性を損なうことなく、地理的な BGP 隣接関係の数を減らすことができます。

  注： 2 つのスパインを持つシングルポッド ファブリックの特定の例では、スパインの障害シナリオでリモート プレフィックスが学習され続けるように、両方のスパインの [BGP ピアリング (BGP Peering)] ノブを有効にする必要があります。同じポッドに 3 つ以上のスパインが展開されている場合は、2 つのスパインでのみノブを有効にする必要があります。他の 2 つの「フォワーダ」スパインは、COOP コントロール プレーンを介してローカル BGP 対応スパインからリモート エンドポイント情報を学習します。
- BGP-EVPN ROUTER-ID：各スパインに展開され、ローカル「フォワーダ」スパインおよびリモート サイトに展開された BGP 対応スパインとの MP-BGP EVPN ピアリングを確立するために使用される一意のループバック インターフェイス。ベスト プラクティスの推奨事項は、マルチサイト EVPN ピアリング専用の IP アドレスを使用することです。これは、ISN インフラストラクチャでルーティング可能です。

  重要な注意：スパイン ノードに指定されたルータ ID は、ファブリックの起動時に内部 TEP プールから割り当てられた元のルータ ID を置き換えます。これにより、スパイン RR とリーフ ノード間に確立された MP-BGP VPNv4 セッションがリセットされ、ローカル L3Out 接続で学習された外部プレフィックスがファブリック内に伝播され、その結果、ノースサウス トラフィック フローが一時的に停止します。そのため、このインフラストラクチャ設定タスクは、一度に 1 つのスパインで実行することをお勧めします。できれば、メンテナンス期間中に実行することをお勧めします。Nexus Dashboard Orchestrator からファブリックを切り離す必要がある場合、サイトの削除シナリオにも同じ考慮事項が適用されます。Nexus Dashboard Orchestrator からサイトを削除するだけでは infra L3Out 設定が削除されないため、

NDO で以前に割り当てられたルータ ID が引き続き使用されることに注意してください。ただし、infra L3Out を APIC で直接削除すると、ルータ ID は TEP プールの元の 1 つの部分に変更されます。これにより、BGP VPNv4 セッションがリセットされて、ノースサウストラフィックが一時的に使用できなくなります。

- 最後のノブは、Multi-Site ドメイン内のファブリックがすべて同じ BGP ASN の一部であり、スパインをルート リフレクタとして設定する必要がある場合にのみ必要です。同じ Multi-Site ドメインでサポートされるファブリックの最大数を導入する場合でも、スケーラビリティの問題はないため、ベストプラクティスの推奨事項は、フルメッシュ ピアリングを作成するデフォルトの動作を維持することです。

サイト間制御およびデータ プレーン接続の確認

Nexus Dashboard Orchestrator にオンボードされたすべての ACI ファブリックについて、前のセクションで説明した設定手順を完了して展開すると、MP-BGP EVPN の隣接関係がサイト間で確立され、VXLAN データ プレーンも正常な状態になります。これは、NDO UI のダッシュボード タブで確認できます。

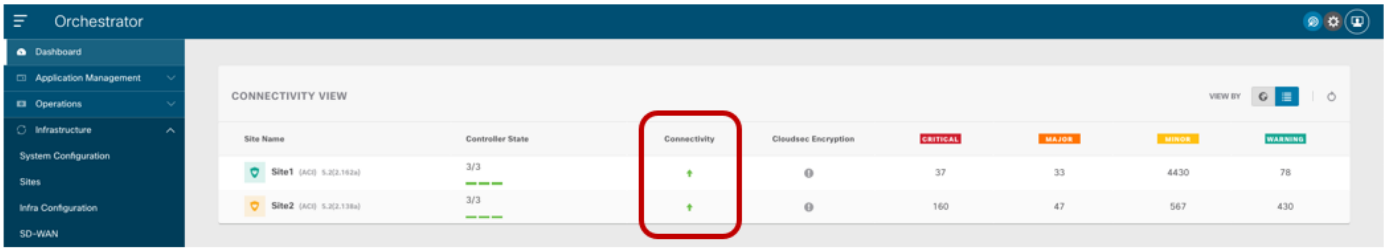


図 15.
NDO ダッシュボード

接続が正常でない状態で表示された場合、コントロール プレーンの隣接関係の確立に問題があるか、正常でない VXLAN データ プレーン、またはその両方の情報が UI から提供されます。この情報は、次の図に示すように、[インフラの構成 (Infra Configuration)] セクションの一部として各サイトで取得できます。

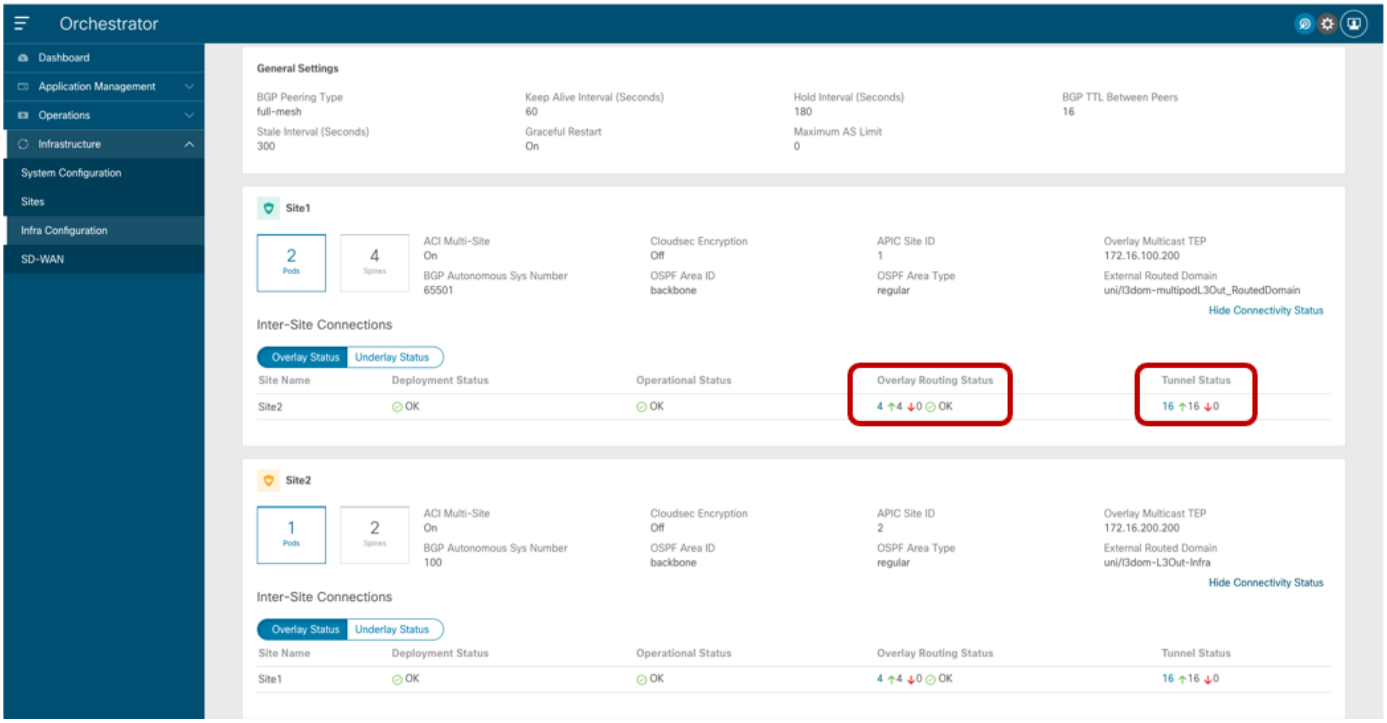


図 16.
各サイトの接続ステータスの表示

上記のように、各ファブリックの [オーバーレイ ステータス (Overlay Status)] と [アンダーレイ ステータス (Underlay Status)] の両方が詳細に表示されます。ユーザーは、ルーティング隣接またはトンネル隣接を強調表示する特定の値をクリックすることで、より詳細にドリルダウンすることもできます。次の図は、たとえば「オーバーレイ ルーティング ステータス」の詳細情報を示しています。

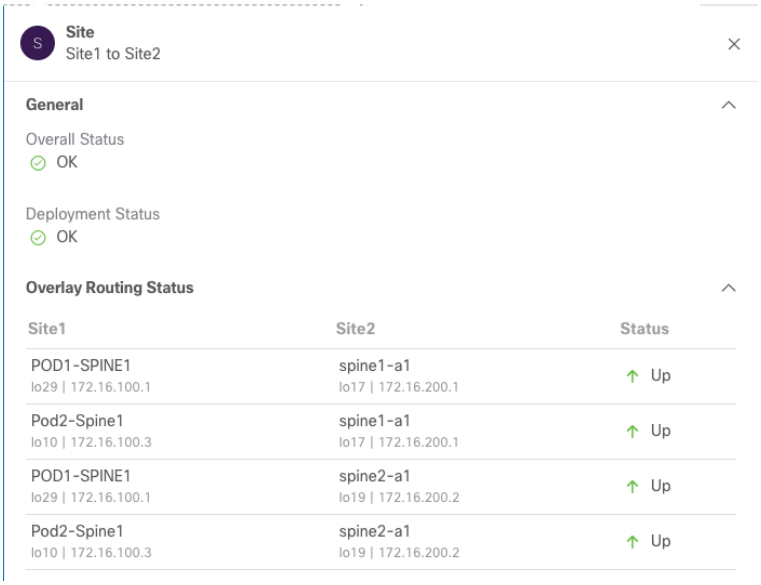


図 17.
オーバーレイ ルーティング ステータスの詳細情報

通常、コントロール プレーンまたはデータ プレーンの接続の確立の問題は、ファブリック間の到達可能性情報の正常な交換を許可しない ISN の設定エラーが原因です。したがって、最初に必要な手順は、サイト内のスパ

イン ノードがリモート サイトからIP プレフィックス（BGP EVPN ルータ ID、O-UTEP、およびO-MTEP）を受信することを確認し、その逆も確認することです。これは、次のようにSite1 のスパイン ノードの 1 つに接続することで実行できます。

Spine 1101 Site1

```
Spine1011-Site1# show ip route vrf overlay-1
IP Route Table for VRF "default"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
<snip>
172.16.100.1/32, ubest/mbest: 2/0, attached, direct
    *via 172.16.100.1, lo16, [0/0], 01w02d, local, local
    *via 172.16.100.1, lo16, [0/0], 01w02d, direct
172.16.100.2/32, ubest/mbest: 4/0
    *via 10.1.0.64, eth1/34.69, [115/3], 06:36:58, isis-isis_infra, isis-l1-int
    *via 10.1.0.67, eth1/61.72, [115/3], 06:36:58, isis-isis_infra, isis-l1-int
    *via 10.1.0.68, eth1/33.71, [115/3], 06:36:58, isis-isis_infra, isis-l1-int
    *via 10.1.0.69, eth1/57.70, [115/3], 06:36:58, isis-isis_infra, isis-l1-int
172.16.100.100/32, ubest/mbest: 2/0, attached, direct
    *via 172.16.100.100, lo21, [0/0], 06:36:59, local, local
    *via 172.16.100.100, lo21, [0/0], 06:36:59, direct
172.16.100.200/32, ubest/mbest: 2/0, attached, direct
    *via 172.16.100.200, lo20, [0/0], 06:36:59, local, local
    *via 172.16.100.200, lo20, [0/0], 06:36:59, direct
172.16.100.2/32, ubest/mbest: 4/0
    *via 192.168.1.3, eth1/64.64, [110/4], 01w02d, ospf-default, intra
172.16.200.2/32、ubest / mbest：1/0
    *via 192.168.1.1, eth1/63.63, [110/4], 01w02d, ospf-default, intra
172.16.200.100/32, ubest/mbest: 2/0
    *via 192.168.1.1, eth1/63.63, [110/4], 06:37:51, ospf-default, intra
    *via 192.168.1.3, eth1/64.64, [110/4], 00:00:35, ospf-default, intra
172.16.200.200/32, ubest/mbest: 2/0
    *via 192.168.1.1, eth1/63.63, [110/4], 06:37:46, ospf-default, intra
    *via 192.168.1.3, eth1/64.64, [110/4], 00:00:35, ospf-default, intra
```

注： 前提条件は、必要なIP プレフィックスだけがサイト間で交換されるように、ファーストホップISN ルータで適切なフィルタリングが実行されることです。必要な設定の詳細については、「サイト間ネットワーク接続のプロビジョニング」セクションを参照してください。

Nexus Dashboard Orchestrator テナント、スキーマ、およびテンプレート定義

サイトのオンボーディングとインフラストラクチャの設定手順が完了すると、異なる ACI ファブリックに接続されたエンドポイント間のセキュアな通信の確立を開始できます。これを行うには、まずテナントを作成し、サイト間接続を必要とするすべてのファブリックにテナントを展開する必要があります。デフォルトでは、2 つのテナント（infra および common）のみが Nexus Dashboard Orchestrator で事前定義され、以前は「Managed」として設定されていたすべてのサイトに自動的に関連付けられます。

デフォルトでは、これらのテナントに関連付けられているスキーマがないため、APIC でデフォルトで通常使用できる common/infra ポリシーの一部を利用する場合は、異なる APIC ドメインから Nexus Dashboard Orchestrator にこれらのオブジェクトをインポートする必要があります。APIC ドメインからの既存のポリシーのインポートについては、このホワイトペーパーでは説明しません。

このセクションの残りの部分では、新しいテナントのポリシーの作成と、Multi-Site ドメインの一部であるファブリック全体のプロビジョニングに焦点を当てます。そのための最初のステップは、新しいテナントを作成し、それを導入する必要があるすべてのサイトに関連付けることです（図 18）。

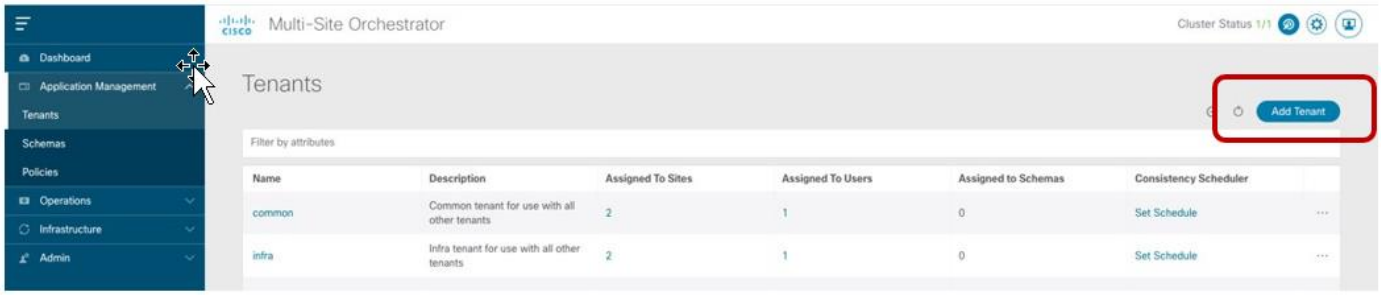


図 18.
新しいテナントの追加

[テナントの追加 (Add Tenant)] オプションを選択すると、テナントの情報を設定し、テナントを作成するサイトを指定できます。図 19 の例では、新しく作成されたテナントは、以前に Orchestrator Service にオンボーディングされていた両方のサイトにマッピングされます。

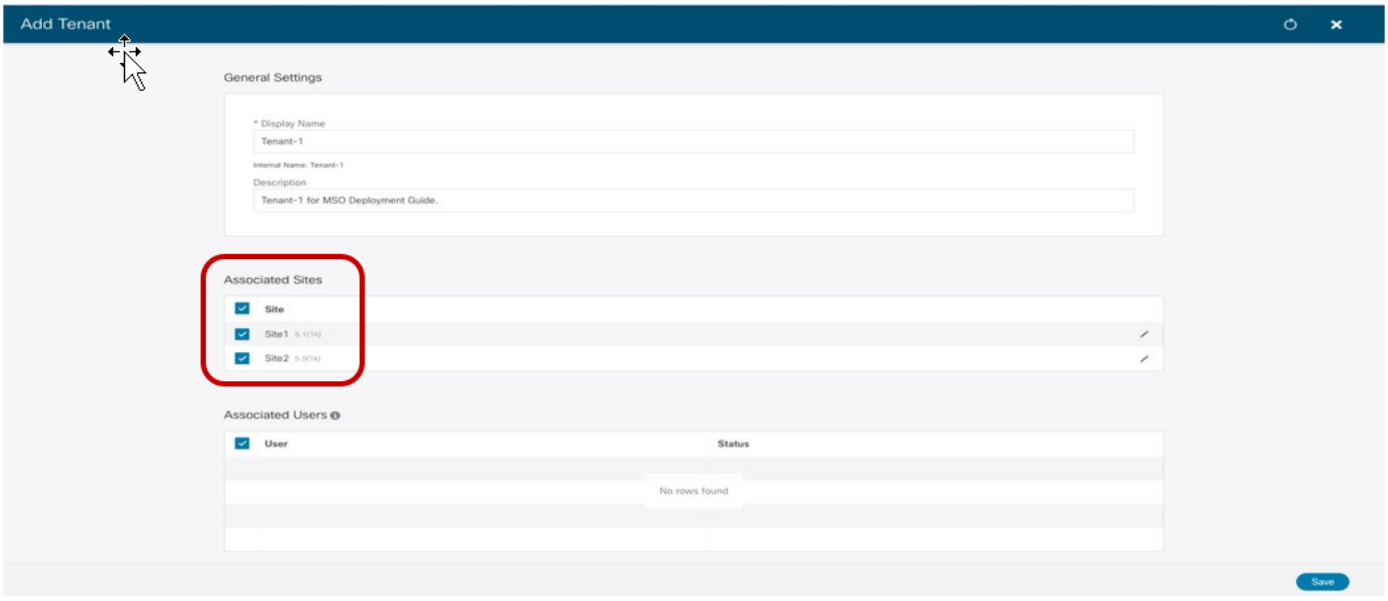


図 19.
異なるファブリックへのテナントのマッピング

また、上記の画面では、特定のユーザーをこの新しく作成されたテナントに関連付けて、テナントの設定を管理できるようになっています（デフォルトでは、管理者ユーザーのみがテナントに関連付けられています）。サポートされるユーザーロールと設定の詳細については、次のリンクにある設定ガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/dcn/ndo/3x/configuration/cisco-nexus-dashboard-orchestrator-configuration-guide-aci-341.html

上記の設定の結果、テナント 1 が Site1 と Site2 の両方に作成されます。ただし、これはまだ「空の貝殻」です。これは、このテナントでファブリックにプロビジョニングされるポリシーがまだ定義されていないためです。テナントポリシーの定義には、「スキーマ」および「テンプレート」と呼ばれる特定の設定構造の作成が必要です。これらの構成要素が表す内容と関連する導入ガイドラインの詳細については、以下のペーパーの「Cisco ACI Multi-Site Architecture」のセクションを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html#CiscoACIMultiSitearchitecture

この例では、テナント 1 に関連付けられたすべてのテンプレートのリポジトリとして使用される特定のスキーマ（「Tenant-1 Schema」という名前）を定義します。

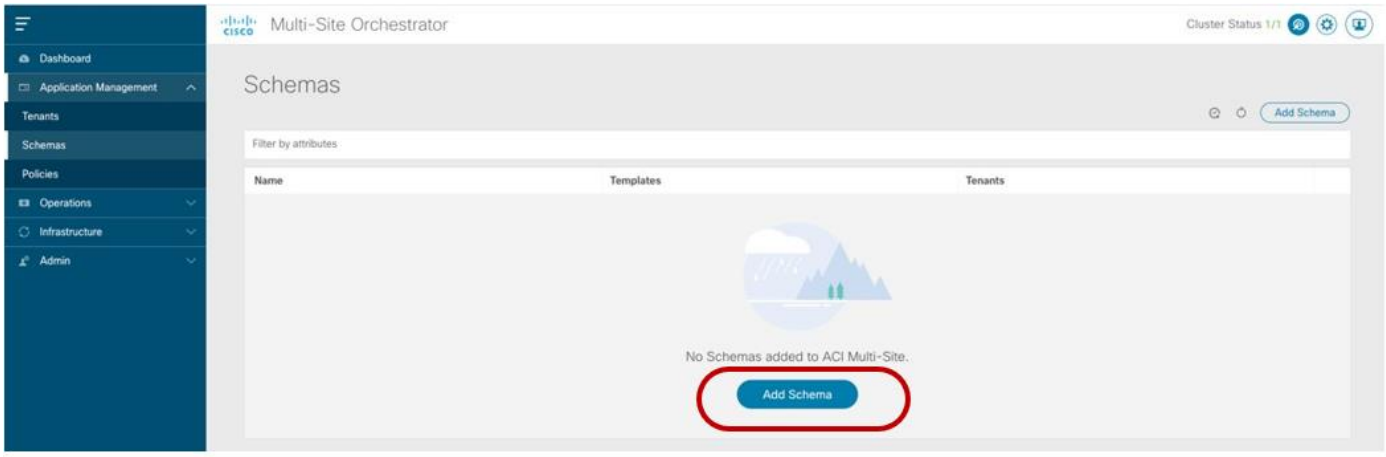


図 20.
新しいスキーマの作成

図 21.
スキーマへの名前の割り当て

このホワイトペーパーの残りの部分で説明する使用例では、各サイトでローカルに使用でき、両方のサイトに共通するポリシー（つまり、「拡張」ポリシー）を展開する必要があるため、以下の 3 つのテンプレートを使用します。

- Template-Site1 は、Site1 にのみローカルにポリシーを展開します。
- Template-Site2 は、Site2 にのみローカルにポリシーを展開します。
- Site1 と Site2 に共通のポリシーを展開するためのテンプレート拡張（拡張ポリシー）。

注： 同じ名前を持つ同じ ACI Multi-Site ドメインの異なるファブリック部分に置く必要があるオブジェクトは、常にすべてのサイトに関連付けられたテンプレートからのみプロビジョニングする必要があることに注意してください。唯一の例外は、異なるアプリケーションプロファイルの一部として展開された EPG で、名前が重複している可能性があります。この場合でも、運用の簡素化のために、サイトローカル EPG を一意の名前でプロビジョニングすることを推奨します。

図 22 に示すように、上記の各テンプレートを Tenant-1 テナントに関連付ける必要があります。

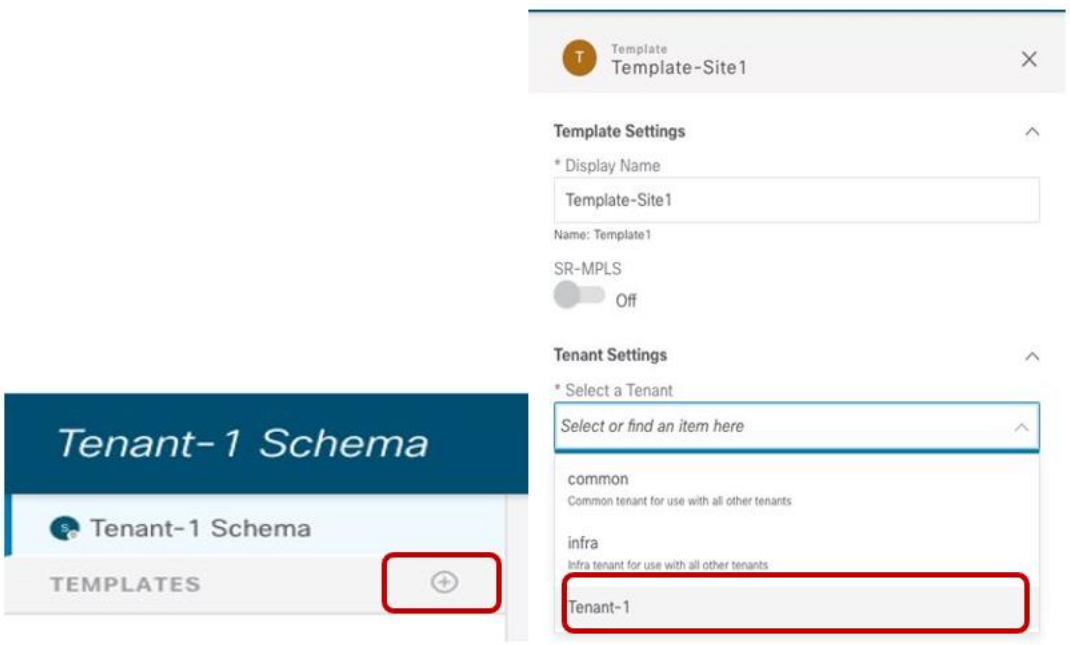


図 22.
テナント 1 にマッピングされたテンプレートの作成

他のテンプレートに対して同じ操作が完了したら、各テンプレートを対応する ACI サイトに関連付けることができます。

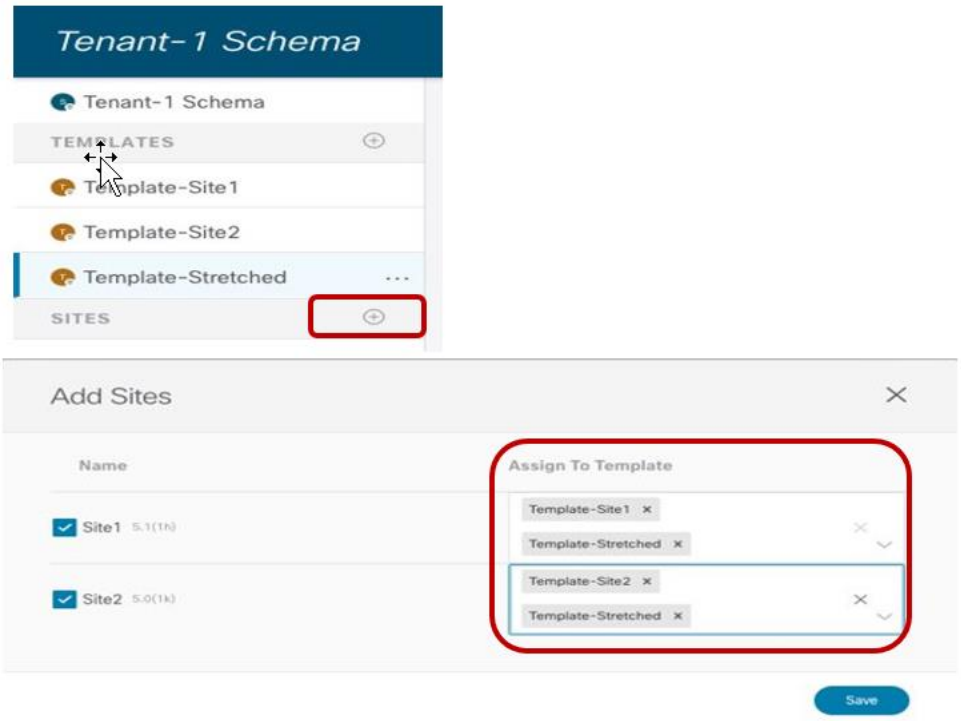


図 23.
テンプレートを ACI サイトに関連付ける

この最後の手順が完了すると、次のセクションで説明するさまざまな使用例を実装するために、さまざまなサイトにプッシュする特定の設定ポリシーの定義を開始できます。

エンドポイント間のサイト間接続

検討している最初の 2 つの使用例は、別々のファブリックに接続されたエンドポイント間で EPG 内および EPG 間の接続を確立できるようにするものです。通常、これらの使用例は「イーストウェスト」接続と呼ばれます。

サイト間の EPG 内接続

サイト間で EPG 内接続を確立するには、Template-Stretched でオブジェクトを定義する必要があります。これにより、これらの項目を両方のファブリックでレンダリングできます。展開できるシナリオはいくつかあります。1 つ目は図 24 に示すもので、EPG はストレッチされた BD にマッピングされ、BD に関連付けられた IP サブネットもサイト間でストレッチされます。これは、この場合、異なるサイトに接続されたエンドポイント間でサブネット内通信を有効にできることを意味します。

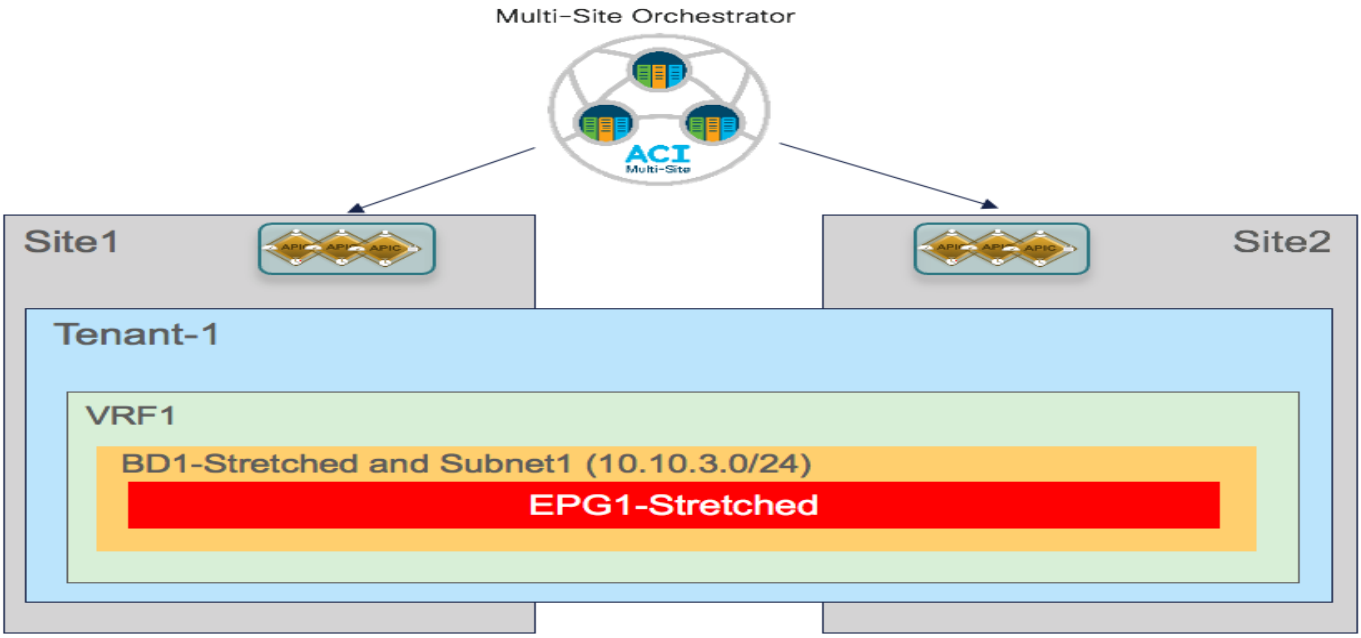


図 24.
ストレッチ EPG、ストレッチ BD、ストレッチ サブネット

代わりに、2 番目のシナリオを図 25 に示します。この場合、EPG はサイト全体にストレッチされますが、BD とサブネットは引き延ばされません。これは、別のサイトに接続されたエンドポイント間の EPG 内通信が、レイヤ 2 ではなくレイヤ 3 であることを意味します（前のケース）。

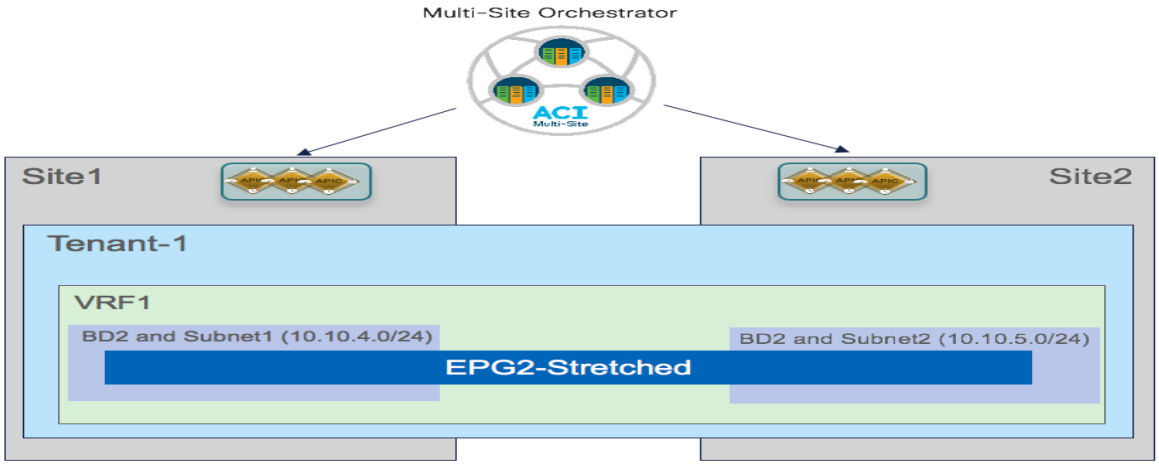


図 25.
BD およびサブネットをストレッチしない EPG のストレッチ

次のセクションでは、上記の 2 つの通信パターンを有効にするために必要なポリシーをプロビジョニングするために必要な特定の設定手順について説明します。

ストレッチ VRF の作成

サイト間の EPG 内通信を有効にするための最初のステップは、EPG（BD であればなおよい）が関連付けられている VRF を作成して展開することです。この VRF は、両方の ACI ファブリックでプロビジョニングする必要があるため、Template-Stretched の一部として設定する必要があります。

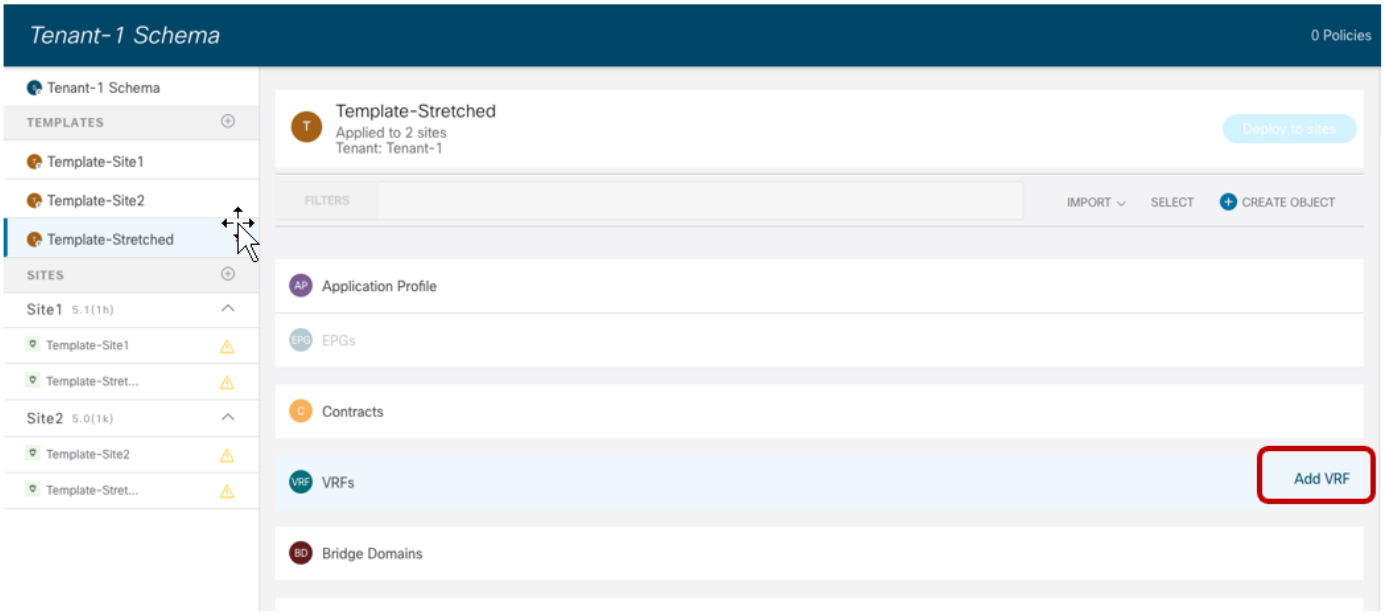


図 26.
Template-Stretched での新しい VRF の作成

図 27 は、NDO GUI で新しい VRF を作成するときに使用できるさまざまな設定パラメータを示しています。

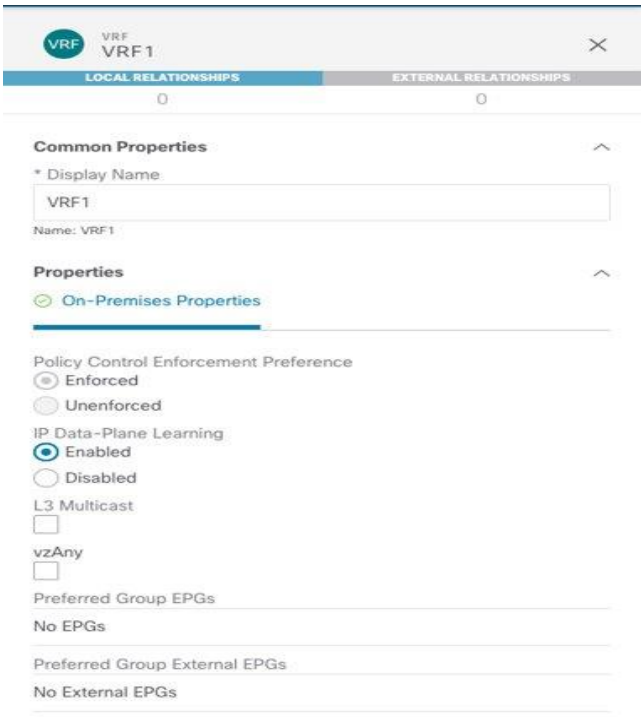


図 27.
VRF 設定パラメータ

[ポリシー制御適用設定 (Policy Control Enforcement Preference)] は、マルチサイトでサポートされる唯一の VRF 設定であるため、常に適用されてグレー表示されます。ノブを公開する唯一の理由は、VRF 設定が APIC

から Nexus Dashboard Orchestrator にインポートされるブラウンフィールドシナリオの場合です。 APIC の VRF が「非エンフォース」として設定されている場合、ユーザーは NDO で設定を「Enforced」に直接変更したり、そのような設定ではサイト間通信を確立したりはできないことを明確に理解した上で「非エンフォース」に維持することができます。サポートされている他の機能（優先グループまたは vzAny の使用）があり、EPG 間通信のポリシー適用を削除できます。これについては、「サイト間の EPG 間接続」のセクションで詳しく説明します。

新しく作成された VRF のもう 1 つのデフォルト設定は、[IP データプレーンの学習 (IP Data-Plane Learning)] です。この設定を変更する必要がある特定のシナリオがあります。通常は、IP アドレスが異なる MAC アドレス（アクティブ/アクティブ サーバー NIC チーミング オプション、アプリケーション クラスタ サービス、特定の FW/SLB クラスタ オプションなど）に関連付けられる場合があります。詳細については、次のリンクから入手可能な ACI 設計ガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/cisco-application-centric-infrastructure-design-guide.html

VRF の設定が完了したら、テンプレートを展開して、VRF が Template-Stretched に関連付けられている両方の APIC ドメインで作成されるようにします。

図 28.
APIC ドメインで VRF を作成するためのテンプレート拡張の展開

設定が APIC ドメインにプッシュされる前に、NDO GUI によって作成されるオブジェクトの概要が表示されます（この場合、Site1 と Site2 の両方で VRF1 のみ）。

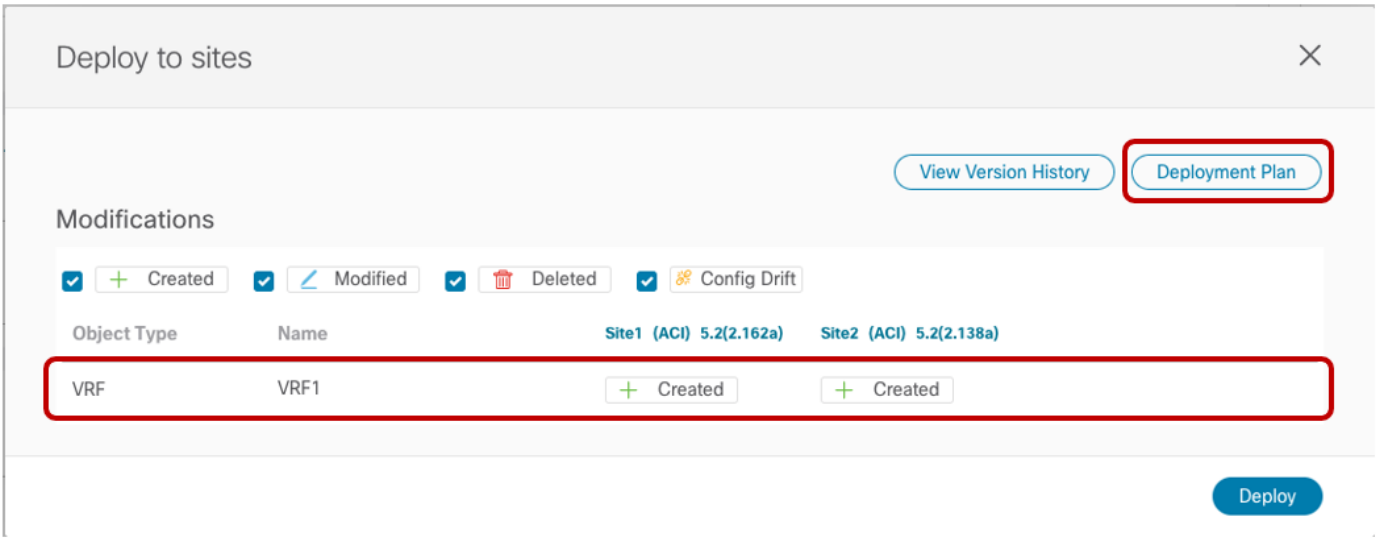


図 29.
Site1 および Site2 にプッシュされる VRF1

NDO リリース 3.4(1) から、「テンプレート展開プラン（Template Deployment Plan）」という名前の新しい機能が使用可能になりました。上の図に示す対応するボタンを選択すると、グラフィカル（およびXML ベース）情報が表示され、テンプレートの展開の結果として、Orchestrator によってプロビジョニングされたオブジェクト（およびどのサイトでか）が詳細に表示されます。この単純なシナリオでは、展開プランには、両方のサイトでVRF が作成されていることが示されます（導入されるテンプレートは両方のサイトに関連付けられているため）。

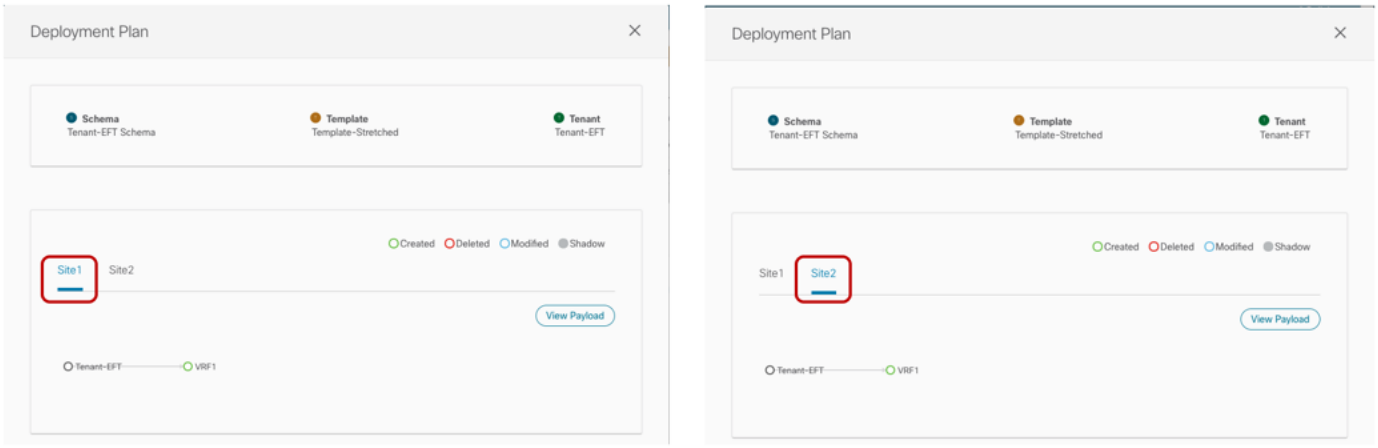


図 30.
テンプレート展開プラン（グラフィカルビュー）

上記の [ペイロードの表示 (View Payload)] オプションを選択すると、テンプレートの展開の結果として Orchestrator が各サイトの APIC コントローラに対して行う REST API コールの XML 形式を表示できます。

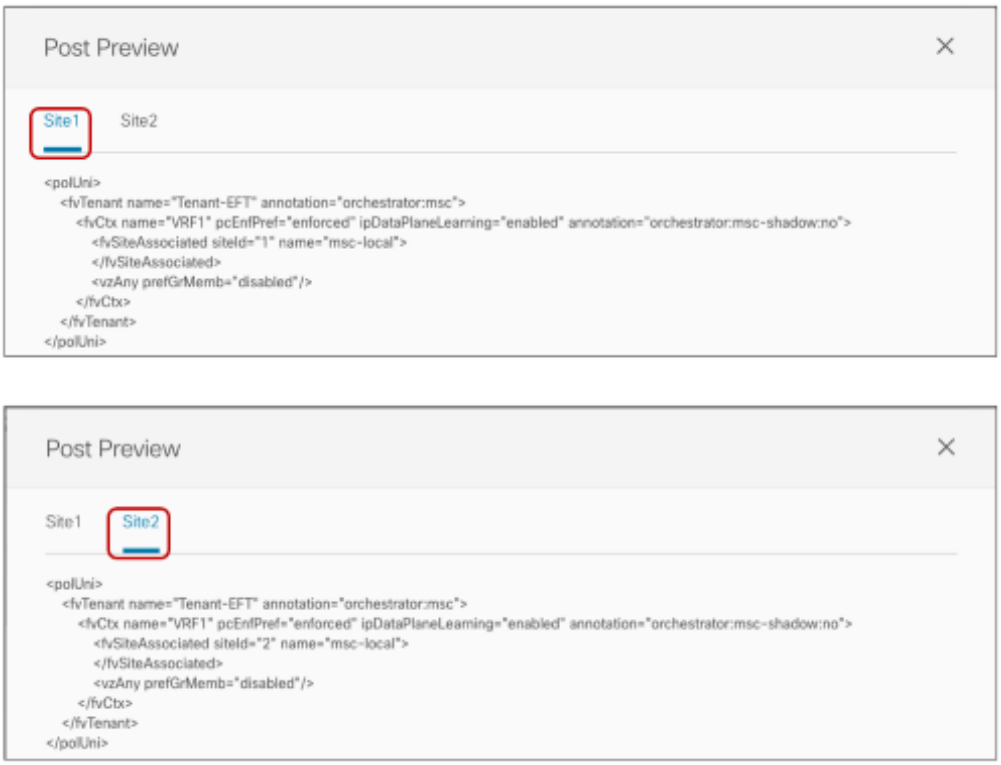


図 31.
展開プラン (XML ビュー)

ストレッチブリッジドメインとストレッチサブネットの作成

前の図 24 に示した使用例の実装に必要なストレッチ BD は、Template-Stretched 内で定義する必要があります。

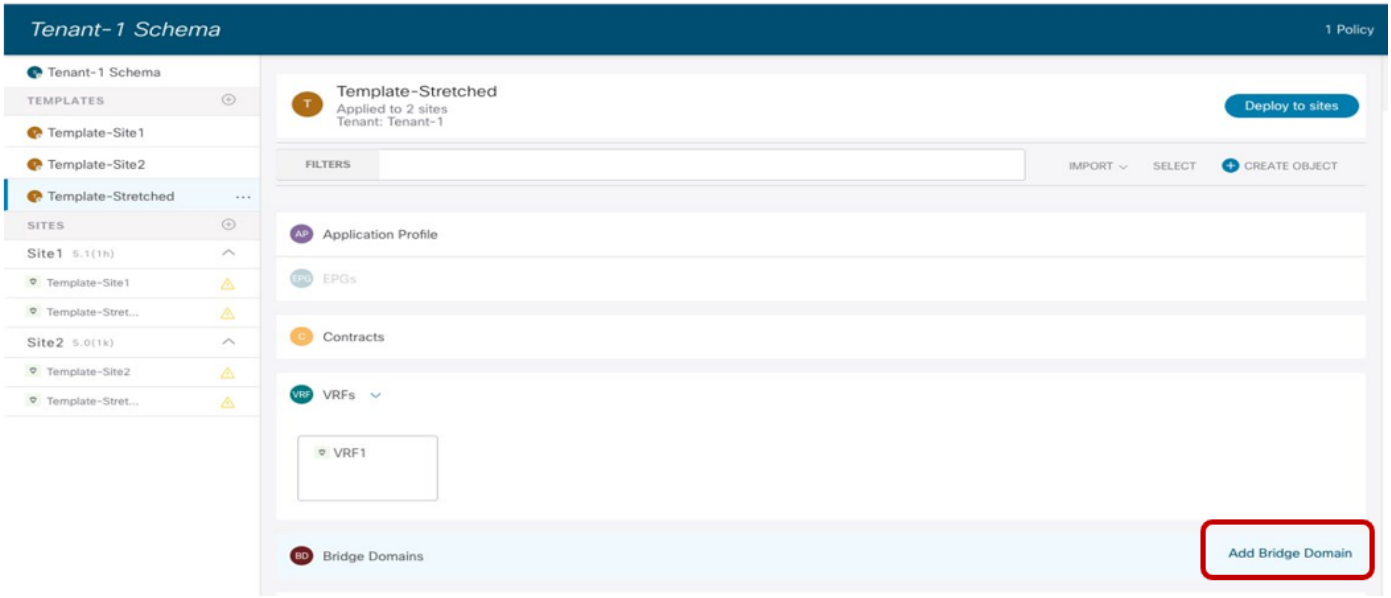


図 32.
Template-Stretched でのストレッチ BD の作成

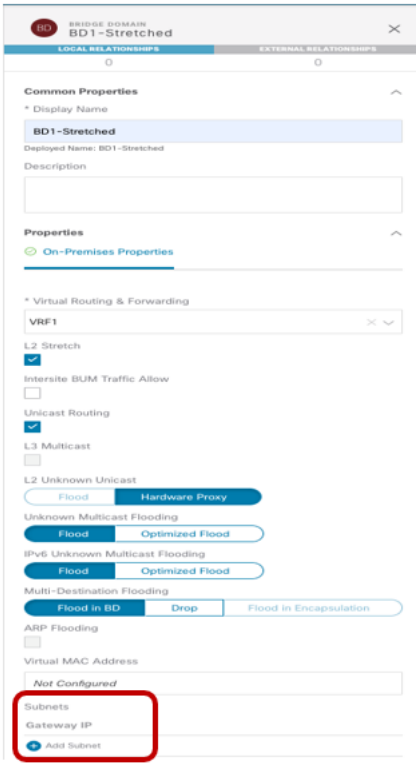


図 33.
ストレッチ BD（設定パラメータ）

- 上記の図 33 に示すように、BD は以前に定義したストレッチ VRF1 に関連付ける必要があります。
- BD は、[L2 ストレッチ (L2 Stretch)] ノブを設定することでストレッチされます。ほとんどの使用例では、サイト間フラッディングを有効にする必要がある特定のシナリオでのみ必要なため、[サイト間 BUM トラフィック許可 (Intersite BUM Traffic Allow)] ノブを無効のままにすることを推奨します。これは、たとえば、レガシーから ACI への移行の使用例（エンドポイントのデフォルト ゲートウェイが ACI に移行されるまで）や、サイト間で L2 マルチキャスト ストリームを送信する必要がある場合です。フラッディングを制御する他のノブは、通常はデフォルト値のままにできます。
- BD は拡張されているため、BD サブネットはテンプレート レベルでも定義されます。これは、BD サブネットもサイト全体に拡張する必要があるためです。

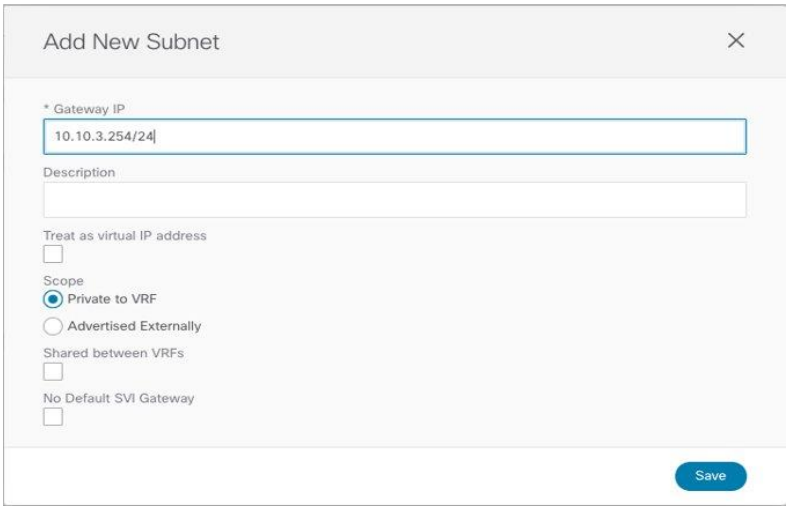


図 34.
BD のサブネット IP アドレスの定義

BD の設定が完了すると、Template-Stretched を ACI ファブリックに展開できます。

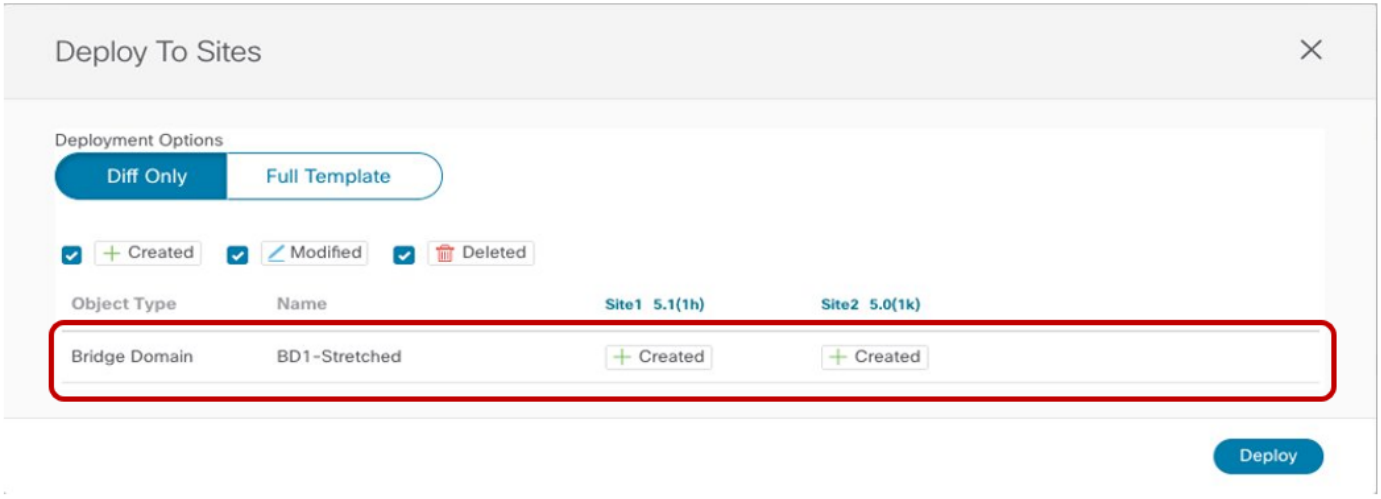


図 35.
ストレッチ BD の Site1 および Site2 への展開

その結果、両方の APIC ドメインで BD が作成され、VRF1 が展開されているすべてのリーフ ノードで同じエニーキャスト ゲートウェイ 10.10.3.254/24 が定義されます。

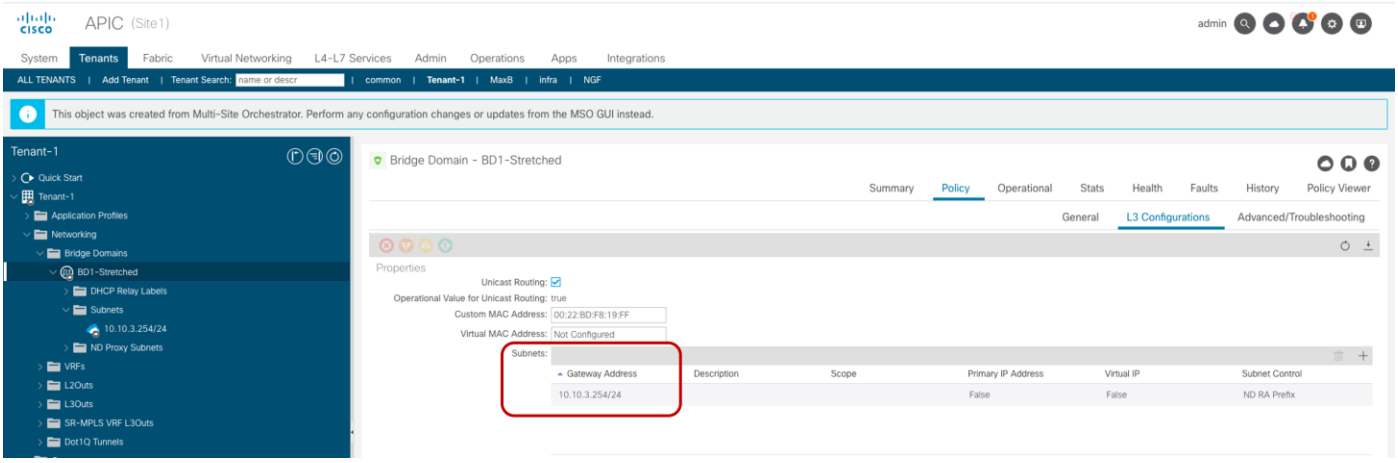


図 36.
Site1 の APIC で作成されたストレッチ サブネットによる BD ストレッチ

ストレッチされていないサブネットを持つストレッチされていないブリッジ ドメインの作成

この特定の設定は、図 25 に示した使用例を実装するために必要です。この場合、EPG は拡張されますが、BD は拡張されません。EPG は単一の BD にのみ関連付けることができるため、BD の転送動作が非ストレッチであっても、両方のサイトで同じ BD オブジェクトが作成されるようにする必要があります。これは、Stretched-Template 内に BD を展開し、図 37 に示すように設定することで実現できます。

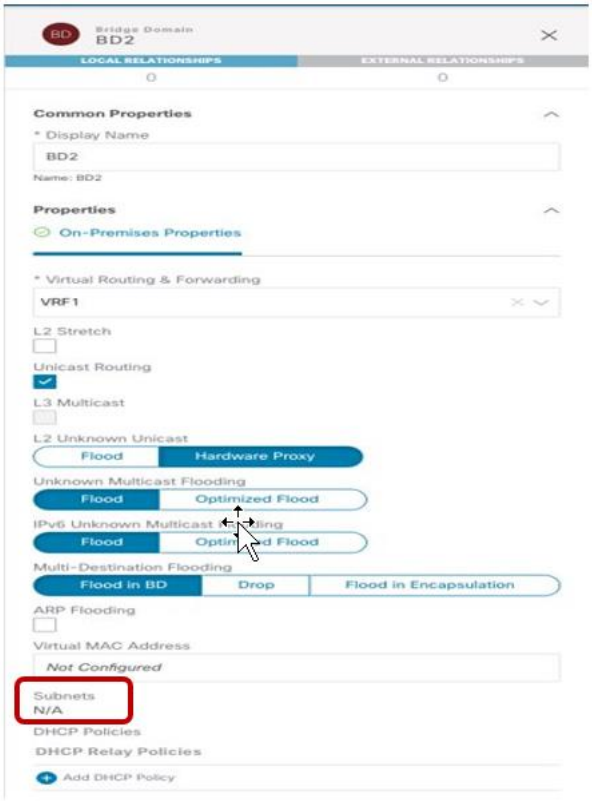


図 37.
サイト間で展開された非ストレッチ BD2（設定パラメータ）

- BD は、以前に定義された同じストレッチ VRF1 に関連付けられます。
- BD サブネットを拡張したり、サイト間の L2 通信を許可したりしないため、[L2 ストレッチ (L2 Stretch)] ノブを無効にして BD を設定する必要があります。
- BD のサブネット フィールドはテンプレート レベルでグレー表示されます。これは、この特定の使用例では、各サイトに配置された BD に個別の IP サブネットを提供することが目的であるためです。したがって、図 38 と図 39 に示すように、サブネットは（Template-Stretched が関連付けられているサイトごとに）サイト レベルで設定されます。

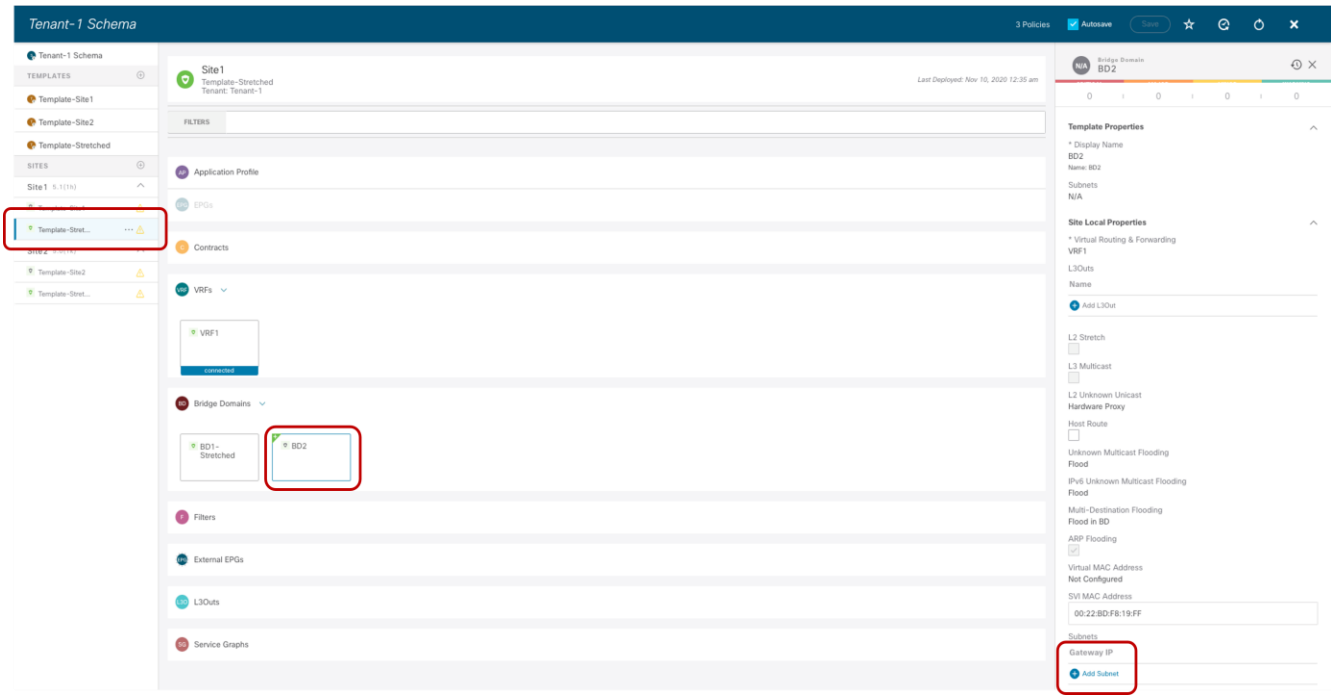


図 38.
Site1 レベルでの BD のサブネットの定義

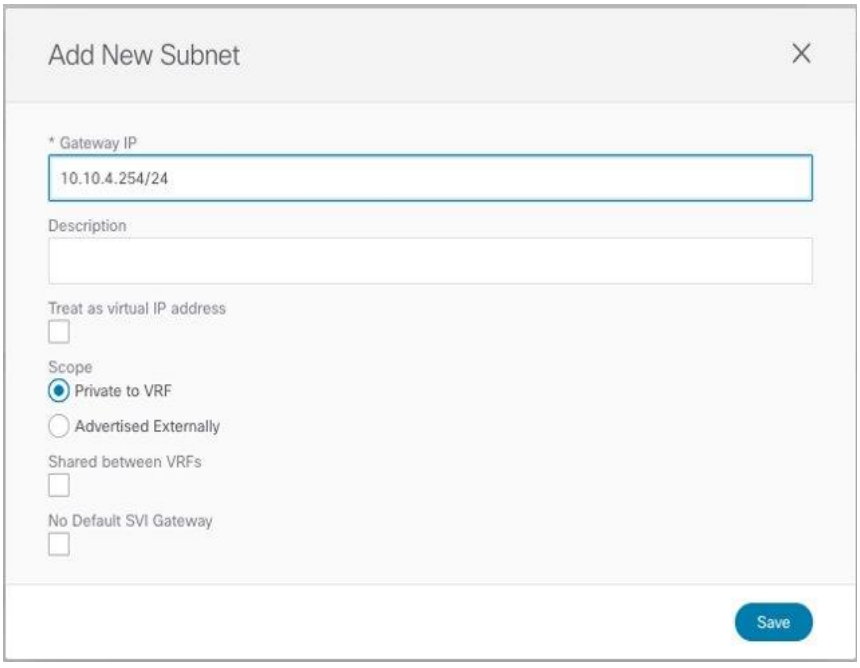


図 39.
Site1 に接続されたエンドポイントの BD のサブネット

同じ設定を Site2 レベルの同じ BD に適用する必要があります。これにより、Site2 に接続されたエンドポイントに使用する別の IP サブネットを設定できます（図 40）。

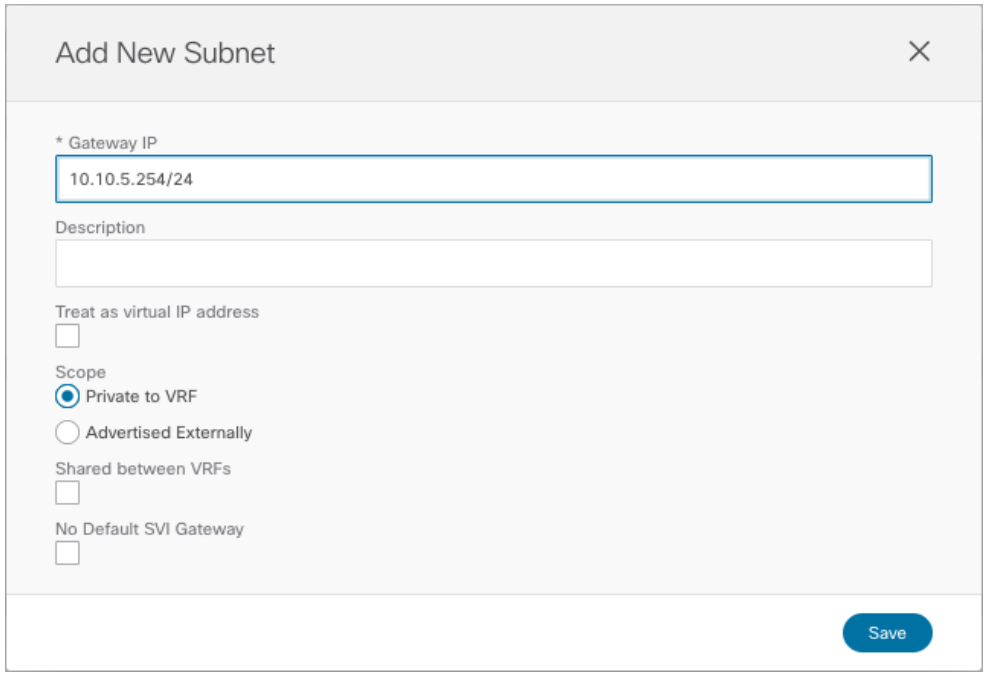


図 40.
Site2 に接続されたエンドポイントの BD のサブネット

各 ACI ファブリックのサイト レベルで特定のサブネットがプロビジョニングされ、テンプレートが展開されると、設定の結果を APIC ドメインで直接確認できます。図 41 に示すように、Site1 の BD は両方の IP サブネットで設定されていますが、Nexus Dashboard Orchestrator（10.10.4.0/24）の Site1 レベルで設定された特定のサブネットのみがエンドポイントのデフォルト ゲートウェイ サービスを提供するために使用されます。他の IP サブネット（10.10.5.0/24）（「シャドウ サブネット」とも呼ばれます）は、「デフォルト SVI ゲートウェイなし」パラメータで自動的にプロビジョニングされます。これは、Site1 のリーフ ノードにのみインストールされ、同じ EPG のエンドポイント部分が通信するサイト（「ストレッチ EPG の作成」セクションのリーフ ノード ルーティング テーブルを参照）。

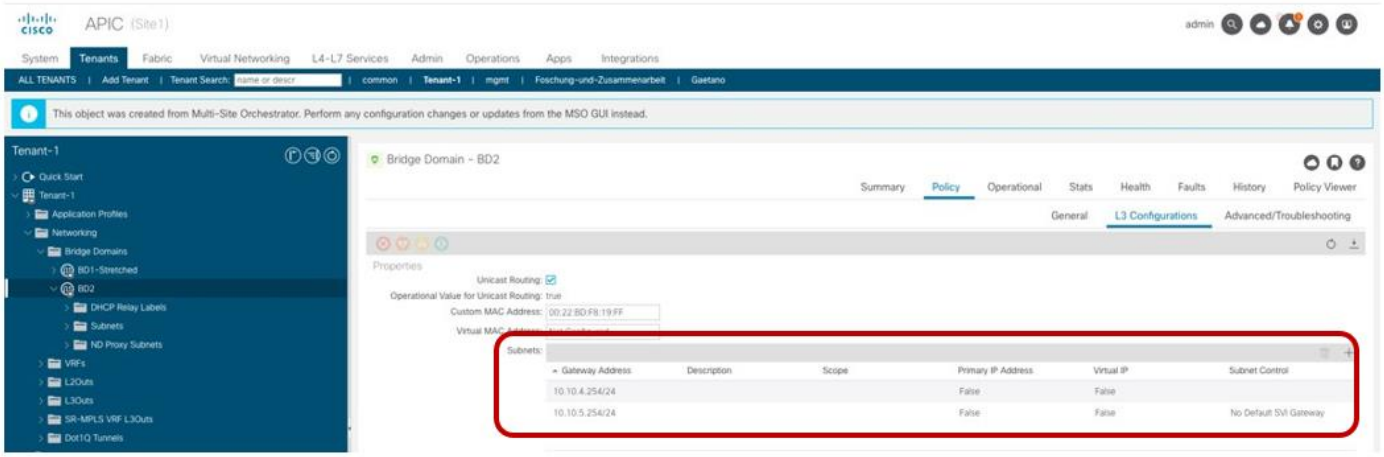


図 41.
Site1 の APIC で設定された BD のサブネット

代わりに、以下の図 42 で強調表示されているように、Site2 の APIC ノードに展開された同じ BD に対しては、まったく逆の考慮事項が有効です。

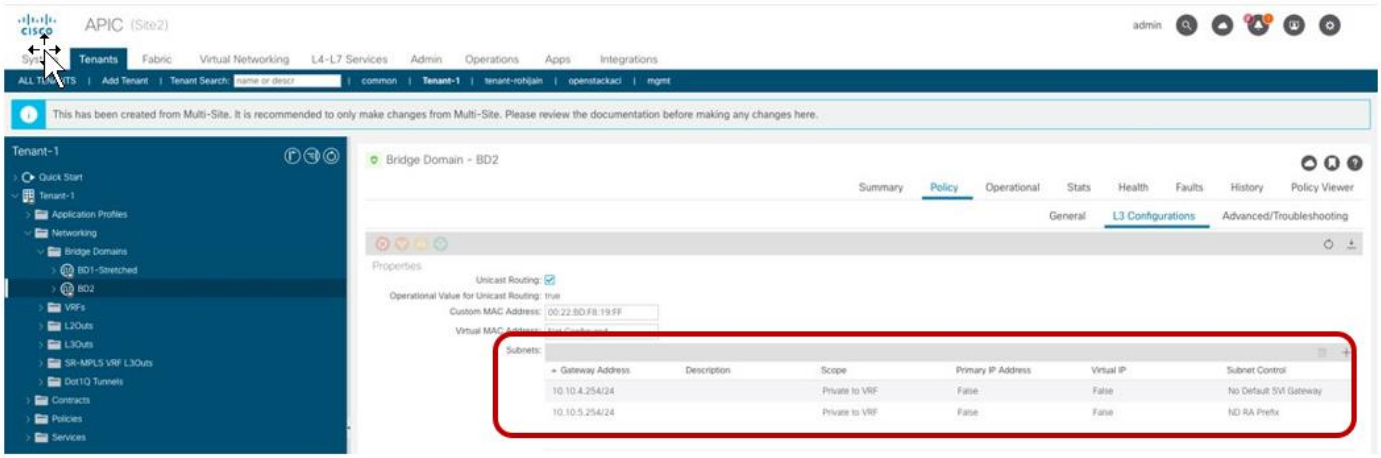


図 42.
サイト 1 の APIC で設定された BD のサブネット

注： [シャドウ サブネット (Shadow Subnet)] は、元のサイトで同じサブネットが設定されていた特定の設定とは別に、[プライベートから VRF (Private to VRF)] スコープで常にプロビジョニングされます。つまり、インスタンス化されたサイトの L3Out から「Shadow Subnet」プレフィックスをアドバタイズすることはできません。異なるサイトの L3Out から BD サブネットをアドバタイズするには、「L2 Stretch」フラグを設定して BD を展開する必要があります。

ストレッチ EPG の作成

最後の手順は、図 24 と図 25 に示した 2 つの EPG（EPG1-Stretched と EPG2-Stretched）を作成することです。これらはストレッチ オブジェクトであるため、Template-Stretched で定義され、両方の ACI サイトにプッシュされます。

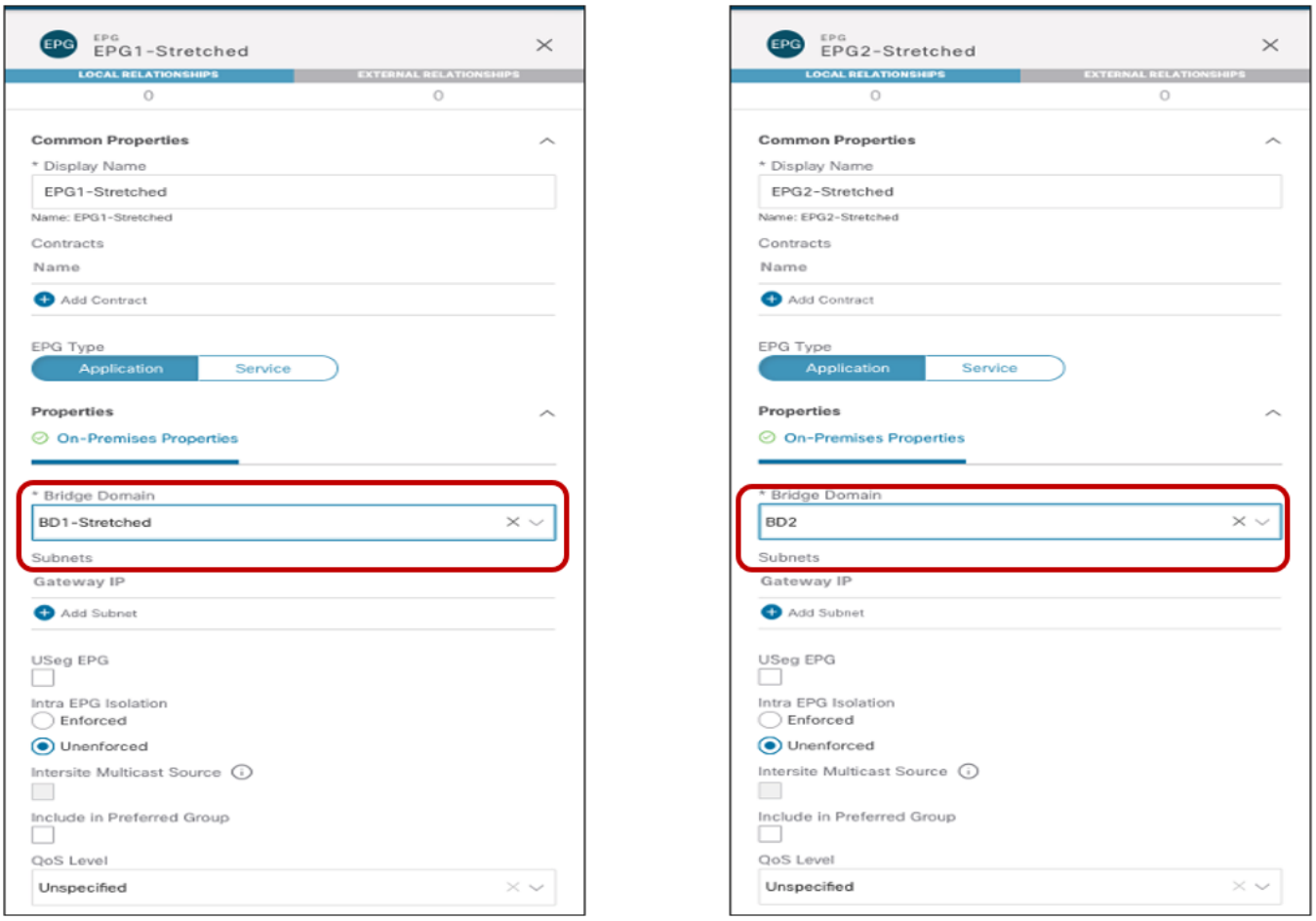


図 43.
ストレッチ EPG の作成

上記のように、各 EPG は、実装が必要な特定の使用例に応じて、以前に作成された BD にマッピングされます。EPG が作成されたら、次の論理ステップは、それらの EPG の一部になるエンドポイントのタイプを指定することです。ACI では、ベアメタル サーバー、仮想マシン、コンテナなど、性質の異なる同じ EPG エンドポイントに接続できます。使用するエンドポイントのタイプは、EPG を特定のドメイン（物理ドメイン、VMM ドメインなど）にマッピングすることで指定します。これらのドメインは、Multi-Site ドメインの一部である各ファブリックの APIC レベルで作成されますが、その後、Orchestrator サービスに公開されるため、EPG ドメインマッピングは Orchestrator サービスを介して直接プロビジョニングできます（サイト固有のレベルでは、各ファブリックは独自にローカルに定義されたドメインを公開できるため）。

注： APIC でドメインを作成する方法は、このペーパーの範囲外です。詳細については、以下の『ACI 設定ガイド』を参照してください。

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

図 44 に、Site1 の物理ドメインへの EPG2-Stretched のマッピングと、それらの物理エンドポイントに必要な対応するスタティック ポート設定の例を示します。この設定は、APIC ドメインでローカルに定義された物理ドメインを具体的に参照するため、サイト レベルで実行する必要があります。

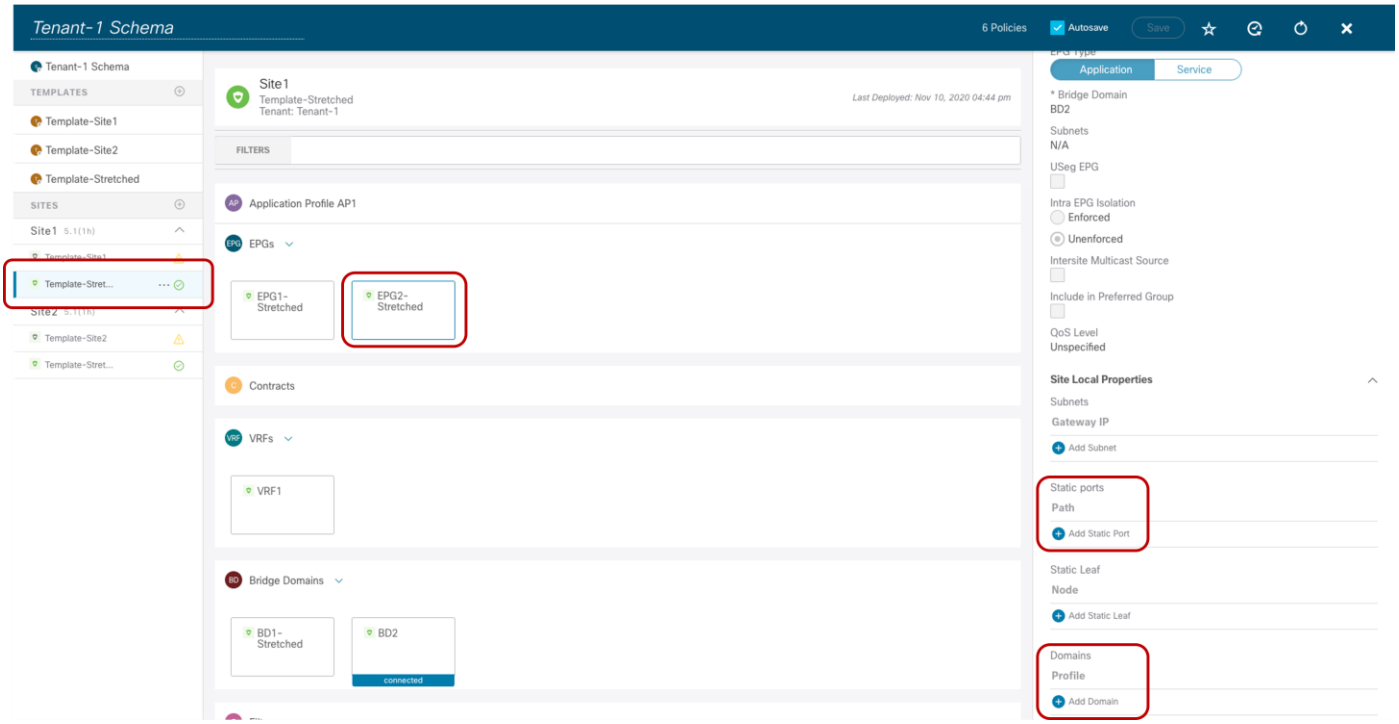


図 44.
EPG2 ストレッチのスタティック ポートおよび物理ドメインの設定

[ドメインの追加 (Add Domain)] を選択した後、この EPG をマッピングする特定の物理ドメインを指定できます。「展開の即時性」と「解決の即時性」に関係するものを選択するためのさまざまなオプションがあります。これらのオプションの意味の詳細については、上記の ACI 設定ガイドを参照してください。

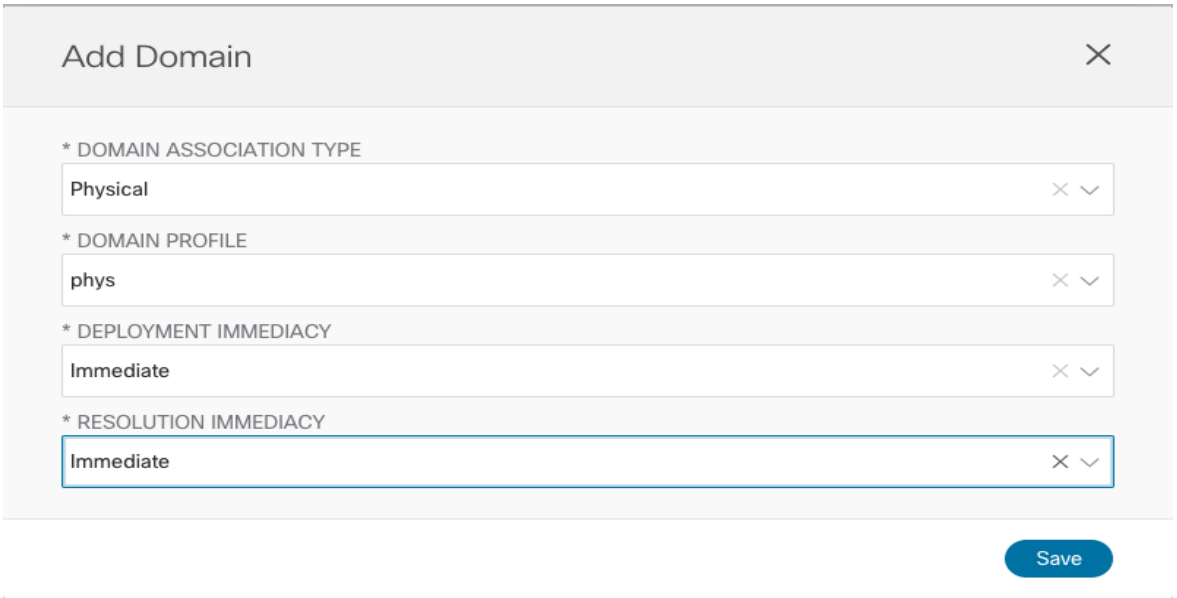


図 45.
物理ドメインへの EPG2 ストレッチのマッピング

スタティック ポート設定では、特定のポート（vPC1）と VLAN カプセル化（VLAN 100）を指定して、物理エンドポイントを ACI ファブリックに接続し、EPG2 ストレッチグループの一部にすることができます。

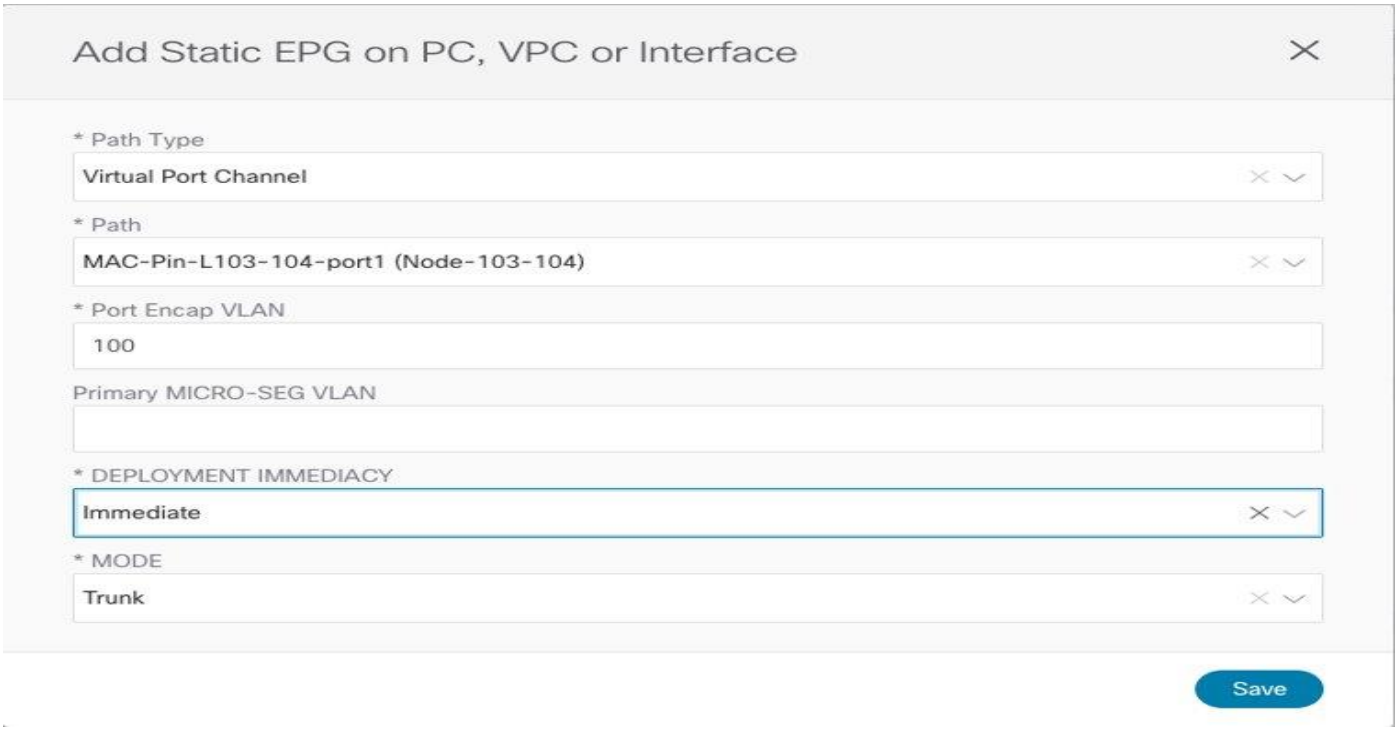


図 46.
物理エンドポイントのスタティック ポート設定

最後に、物理ドメインマッピング設定が APIC Site1 にプッシュされる前に、Nexus Dashboard Orchestrator GUI に、[導入 (Deploy)] をクリックしたときに適用される特定の変更が表示されます。

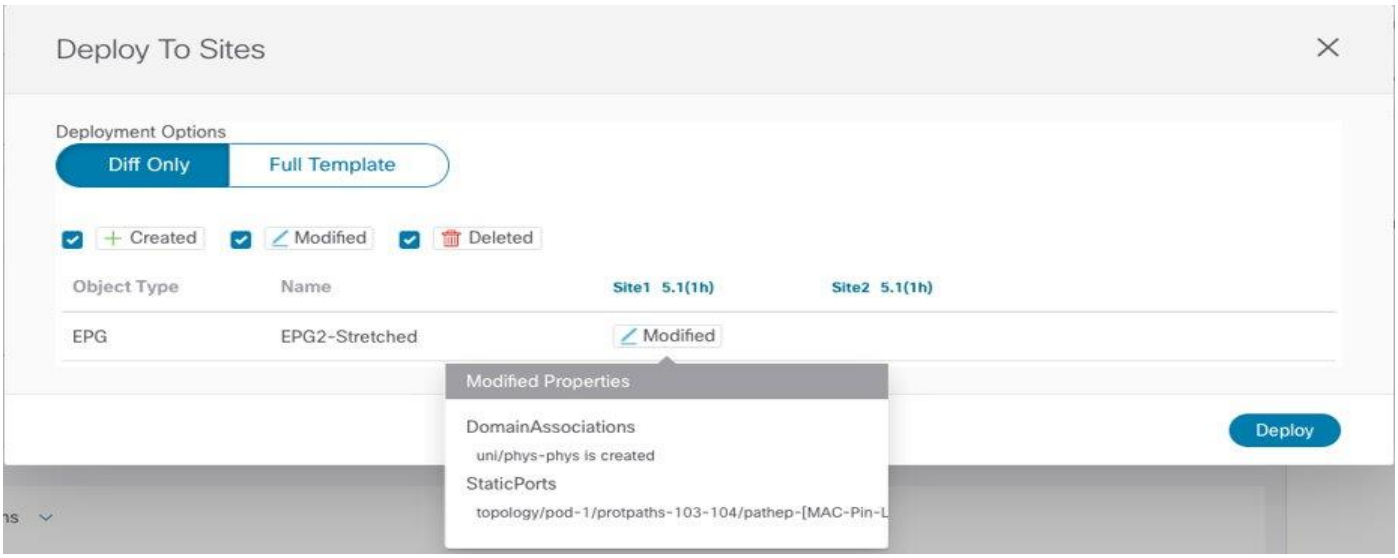


図 47.
Site1 に展開する変更の確認

同様の手順に従って、EPG2-Stretched を Site2 の特定のドメイン（VMM ドメインなど）にマッピングできます。そうすることで、Stretched-EPG2 のエンドポイント部分を表す仮想マシンが接続できるように、APIC と

ピア接続されている VSphere サーバーによって管理される ESXi ホスト上で対応するポート グループが自動的にプロビジョニングされます。

EPG 内通信の確認

エンドポイントが接続されると、リーフ ノードによってローカルに検出されます。

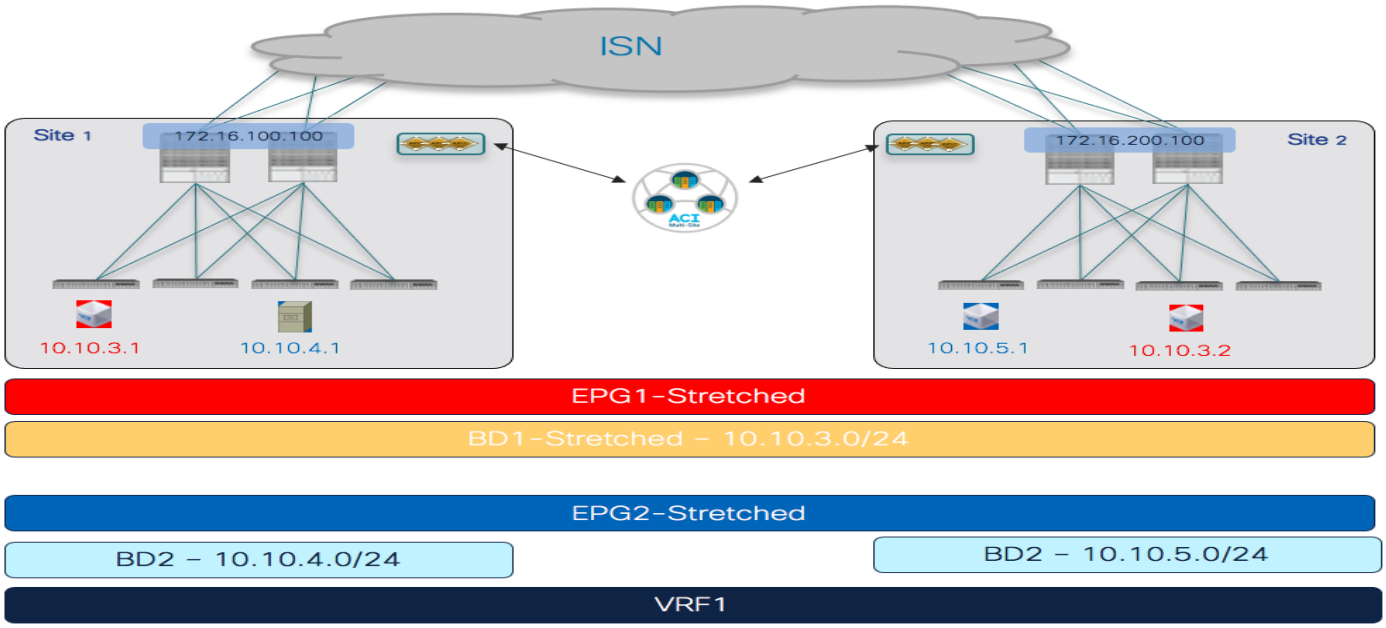


図 48.
ストレッチ EPG に接続されたエンドポイント

この情報は、各サイトの APIC から直接（EPG の操作タブの一部として）取得できます。また、Site1 と Site2 の場合は、特定のリーフ ノードの CLI からも取得できます。

Leaf 103 Site1

```
Leaf103-Site1# show endpoint vrf Tenant-1:VRF1
凡例：
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
 L - local            E - shared-service
+------------------------------+--------------+----------------+-------------+---------
----+
      VLAN/                           Encap            MAC Address       MAC
Info/       Interface
      Domain                          VLAN             IP Address        IP Info
+ ------------------------------ + -------------- + ----------------- + ------------- +
------------ +
10                                      vlan-100     0050.56b9.3e72
LV                        po1
Tenant-1:VRF1                           vlan-100         10.10.4.1
LV                        po1
```

Leaf 301 Site2

```
Leaf301-Site2# show endpoint vrf Tenant-1:VRF1
凡例：
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
 L - local            E - shared-service
+------------------------------+--------------+----------------+-------------+---------
----+
      VLAN/                           Encap           MAC Address       MAC
Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+ ------------------------------ + -------------- + ----------------- + ------------- +
------------ +
42                                      vlan-
136    0050.5684.48b0 LpV                       po2
Tenant-1:VRF1                           vlan-
136         10.10.5.1 LpV                        po2
```

これらのエンドポイント間の通信は、同じ EPG2 ストレッチグループの一部であるため、サイト間で自由に確立できます。エンドポイントが接続されているリーフ ノードのルーティング テーブルを調べると、ローカル エンドポイントの IP サブネットが（対応するエニーキャスト ゲートウェイ アドレスを使用して）ローカルにインスタンス化され、リモート サイトのエンドポイントの IP サブネットは、ネクストホップ（10.1.112.66）としてローカル スパインのプロキシ VTEP アドレスをポイントしてローカルにインスタンス化されることがわかります。

Leaf 103 Site1

```
Leaf103-Site1# show endpoint vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
10.10.4.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    * via 10.1.112.66%overlay-1、[1/0]、00:09:58、static、tag 4294967294
10.10.4.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 10.10.4.254, vlan10, [0/0], 00:09:58, local, local
10.10.5.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.1.112.66%overlay-1, [1/0], 00:09:58, static, tag 4294967294
```

これは、APIC にプッシュされ、前の図 41 に示されている設定の結果です（反対の設定は、Site2 のリーフ ノードでプロビジョニングされます）。ルーティング テーブルのサブネットエントリは、リーフ ノードがデータ プレーンの学習によってリモート エンドポイントの特定の IP アドレスを学習できるようになるまで、ルーティングされたトラフィックをサイト間で転送するために使用されます。

次の CLI 出力は、Site2 のリモート エンドポイントのデータ プレーン学習が行われた後の Site1 のリーフ ノードのエンドポイント テーブルを示しています（Site2 のリーフ ノードでも同様の出力が得られます）。リモート エンドポイントに到達する VXLAN トンネルのネクストホップは、リモート ファブリックの O-UTEP アドレス（172.16.200.100）で表されます。

Leaf 103 Site1

```
Leaf103-Site1# show endpoint vrf Tenant-1:VRF1
凡例：
 S - static s - arp L - local O - peer-attached
 V - vpc-attached a - local-aged p - peer-aged M - span
 B - bounce H - vtep R - peer-attached-rl D - bounce-to-proxy
 E - shared-service m - svc-mgr
+----------------------------------+--------------+-----------------+-------------+------
-------+
      VLAN/ Encap MAC Address MAC Info/ Interface
      Domain VLAN IP Address IP Info
+----------------------------------+--------------+-----------------+-------------+------
-------+
Tenant-EFT:VRF1 10.10.5.1 tunnel39
13 vlan-883 0050.56b9.1beeLV po1
Tenant-EFT:VRF1 vlan-883 10.10.4.1 LV po1
```

Leaf 103 Site1

```
Leaf103-Site1#show interface tunnel 39
Tunnel39 is up
    MTU 1500 bytes, BW 1000000 Kbit
    Transport protocol is in VRF "overlay-1"
    Tunnel protocol/transport GRE/IP
    Tunnel source 10.1.0.68/32 (lo0)
    Tunnel destination 172.16.200.100/32
```

同様に、EPG1-Stretched グループに接続されたエンドポイント間では通信を自由に行うことができます。唯一の違いは、これらのエンドポイントが、サイト間で拡張されている同じ IP サブネット（10.10.3.254/24）の一部であることです。したがって、レイヤ 3 ルーティングではなくレイヤ 2 ブリッジングを使用すると、次のエンドポイント テーブルを確認することができます。

Leaf 101 Site1

```
Leaf101-Site1# show endpoint vrf Tenant-1:VRF1
凡例：
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
 L - local            E - shared-service
+------------------------------+--------------+----------------+-------------+---------
----+
      VLAN/                          Encap           MAC Address       MAC
Info/       Interface
```

```
      Domain                              VLAN            IP Address        IP Info
+ ------------------------------- + --------------- + ----------------- + -------------- +
------------- +
1/Tenant-1:VRF1                     vxlan-
16154555    0050.56a2.380f                        tunnel26
3                                        vlan-886    0050.56b9.54f3
LV                          po1
```

この場合、VXLAN トンネル（tunnel26）を介して到達可能であるという情報とともに、リモートエンドポイントの MAC アドレスだけがローカル リーフ ノードで学習されます。当然のことながら、この場合もローカル リーフ ノードの VTEP と Site2 の O-UTEP アドレス（172.16.200.100）の間に VXLAN トンネルが確立されます。

Leaf 101 Site1

```
Leaf101-Site1# show interface tunnel 26
Tunnel26 is up
    MTU 9000 bytes, BW 0 Kbit
    Transport protocol is in VRF "overlay-1"
    Tunnel protocol/transport is ivxlan
    Tunnel source 10.1.0.68/32 (lo0)
    Tunnel destination 172.16.200.100/32
```

お気づきかもしれませんが、同じ EPG のエンドポイント間の通信を有効にするために特定のセキュリティ ポリシーは必要ありませんでした。これは ACI のデフォルトの動作で、常に無料の EPG 内通信を許可します。ACI によって提供されるゼロ トラスト セキュリティ アプローチのため、EPG1-Stretched と EPG2-Stretched のエンドポイント部分間の通信は、デフォルトでは許可されません。「サイト間 EPG 接続」セクションでは、この通信を許可する方法について詳しく説明します。

ストレッチ オブジェクトのネームスペース変換情報の確認

ACI Multi-Site アーキテクチャでは、ポリシーが異なる APIC クラスタによってローカルにインスタンス化されるため、まったく異なる名前空間を表すサイトを相互接続できます。つまり、特定のリソース（BD の L2VLAN ID、VRF の L3VLAN ID、EPG の Class-ID など）が各 APIC コントローラによって割り当てられると、オブジェクトがサイト間で拡張されていても、その値は各サイトで異なります（したがって、同じ論理項目を表します）。

サイト間通信を確立するために使用される VXLAN トラフィックは、VXLAN ヘッダーでこのタイプの情報を伝送するため、変換（または名前空間の正規化）機能を受信スパインで実行して、エンドツーエンド通信および一貫性のあるポリシー アプリケーションを正しく実施する必要があります。

注： 名前空間の正規化機能は、ストレッチされたオブジェクトだけでなく、異なるサイトで定義されたローカル オブジェクト間の関係を作成する場合にも必要です。詳細については、以下のペーパーの「Cisco ACI Multi-Site アーキテクチャ」セクションを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html#CiscoACIMultiSitearchitecture

サイト間 EPG 内通信の特定のシナリオでは、リモート サイトから VXLAN トラフィックを受信するスパイン ノードで変換エントリが適切に設定されていることを確認できます。図 49 は、Site1 の APIC ドメインで作成されたストレッチ オブジェクトに割り当てられた特定の値を示しています。

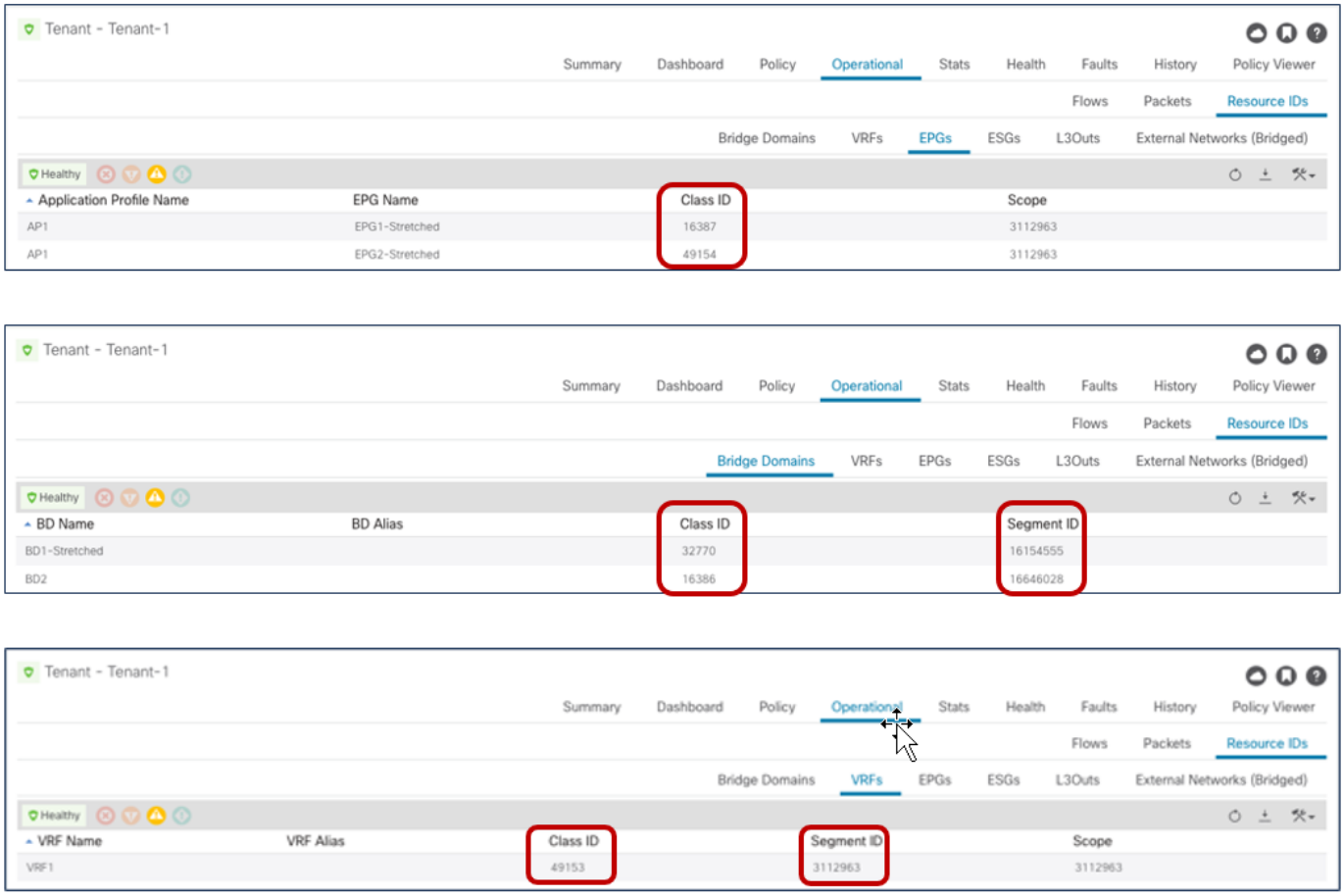
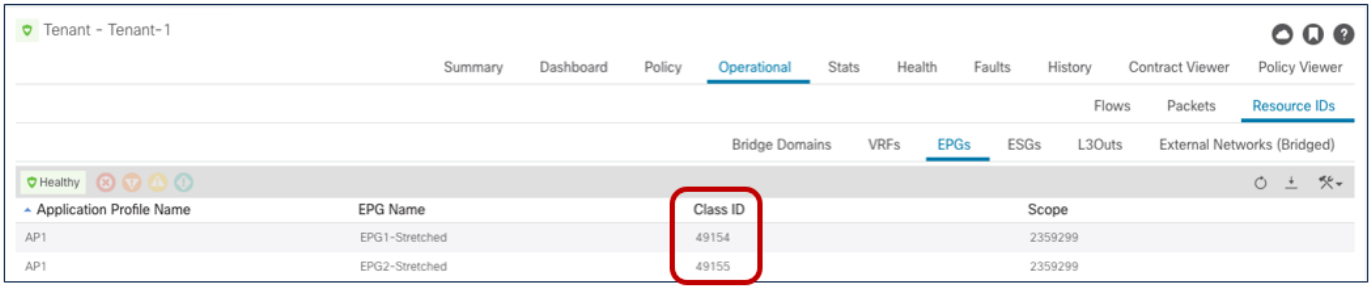


図 49.
Site1 で作成されたオブジェクトのクラス ID、セグメント ID、およびスコープ

図 50 は、代わりに、Site2 の APIC コントローラによって割り当てられた同じオブジェクトの値を示しています。



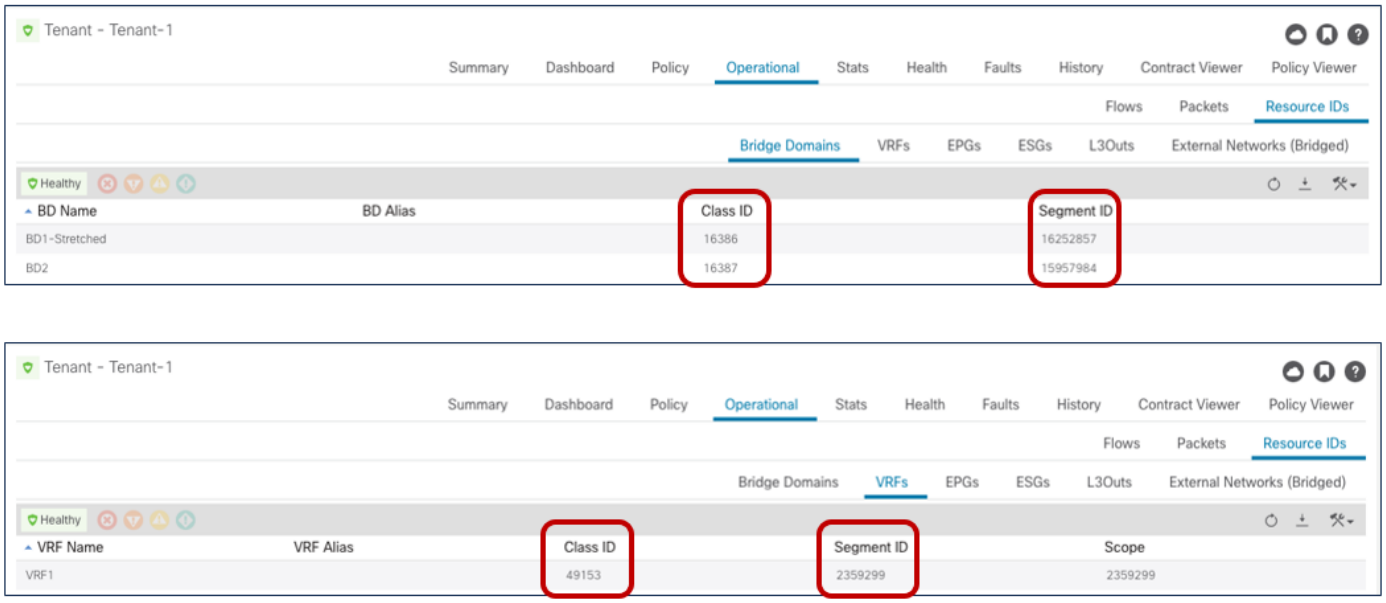


図 50.
Site2 で作成されたオブジェクトのクラス ID、セグメント ID、およびスコープ

上記の 2 つの図の情報を比較すると簡単にわかるように、Site1 のストレッチされたオブジェクト（EPG、BD、または vRF）に割り当てられた値は、Site2 でプロビジョニングされた値とは異なります。ここで、スパインによって実行される変換機能がこれらの値を「正規化」します。これにより、サイト間のデータ プレーン接続を成功させます。

次の出力は、Site1 のスパインと Site2 のスパインのエントリを示しています。これらのエントリは、サイト間でストレッチされている BD と VRF のセグメント ID とスコープを変換できます。VRF1 と BD1-Stretched はストレッチされたオブジェクトであるため、それらの変換マッピングどのように作成されるかを確認できます。しかし、「L2 stretched」ではない BD2 についてはそうではありません。

Spine 1101 Site1

```
Spine1101-Site1# show dcimgr repo vnid-maps
------------------------------------------------------------
     Remote              |           Local
site Vrf Bd | Vrf Bd Rel-state
------------------------------------------------------------
2 2359299 | 3112963 [formed]
  2   2359299  16252857 |   3112963  16154555  [formed]
```

Spine 401 Site2

```
APIC-Site2# fabric 401 show dcimgr repo vnid-maps
------------------------------------------------------------------
 Node 401 (spine1-a1)
------------------------------------------------------------------
------------------------------------------------------------
     Remote              |           Local
```

```
site Vrf Bd | Vrf Bd Rel-state
------------------------------------------------------------
1 3112963 | 2359299 [formed]
  1   3112963  16154555 |   2359299  16252857  [formed]
```

次の出力では、代わりに、VRF、BD、および EPG のポリシー情報（つまり、クラス ID）の Site1 および Site2 のスパイン ノードの変換エントリが表示されます。あるケース（VRF1 の場合）で、ローカルとリモートのクラス ID の値が実際には同じであることに注意してください（49153）。それ以外の場合は、同じクラス ID 値が 2 つのファブリックで異なる目的で使用されます。たとえば、49154 は、Site1 の EPG2-Stretched のクラス ID と、Site2 の EPG1-Stretched のクラス ID を表します。これにより、各 APIC ドメインがローカルで重要な値を割り当てるため、サイト間通信を成功させるために名前空間の正規化機能が必要になります。

Spine 1101 Site1

```
Spine1101-Site1# show dcimgr repo sclass-maps
------------------------------------------------------------
     Remote            |        Local
site Vrf PcTag | Vrf PcTag Rel-state
------------------------------------------------------------
  2   2916358   16386  |  2129927   32770   [formed]
  2   2818056   16387  |  2916360   16386   [formed]
  2   2359299   49155  |  3112963   49154   [formed]
  2   2359299   49153  |  3112963   49153   [formed]
  2   2359299   49154  |  3112963   16387   [formed]
```

Spine 401 Site2

```
Spine401-Site2# show dcimgr repo sclass-maps
------------------------------------------------------------
     Remote            |        Local
site Vrf PcTag | Vrf PcTag Rel-state
------------------------------------------------------------
  1   3014657   32770  |  2326532   16386   [formed]
  1   2916360   16386  |  2818056   16387   [formed]
  1   3112963   49154  |  2359299   49155   [formed]
  1   3112963   16387  |  2359299   49154   [formed]
  1   3112963   49153  |  2359299   49153   [formed]
```

サイト間 EPG 間接続（VRF 内）

異なる EPG に接続されたエンドポイント間のサイト間接続を確立するために考慮する最初の使用例は、図 51 に示すもので、VRF 内シナリオに適用されます。

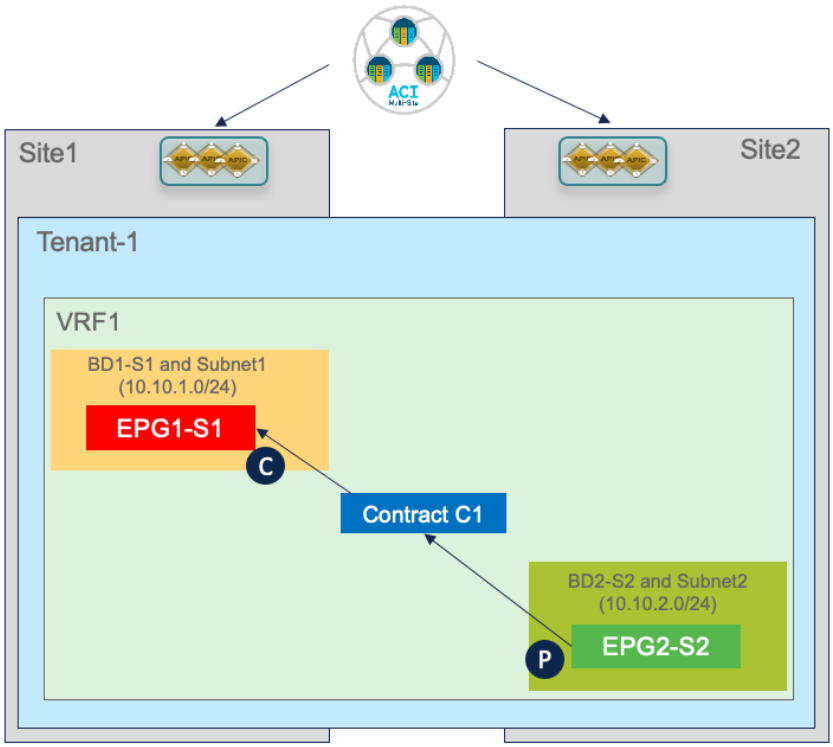


図 51.
サイト間 EPG 間接続（VRF 内）の使用例

前述の拡張 EPG の使用例とは異なり、この場合、EPG/BD オブジェクトは各サイトでローカルにプロビジョニングされるので、許可される通信のタイプを指定する特定のセキュリティ ポリシー（つまり、コントラクト）を作成して、それらの間の接続を確立する必要があります。EPG 間の接続の確立には、ローカルに展開または拡張されているという事実とは別に、次のセクションで説明する内容と同様の考慮事項が適用されることに注意してください（図 52）。

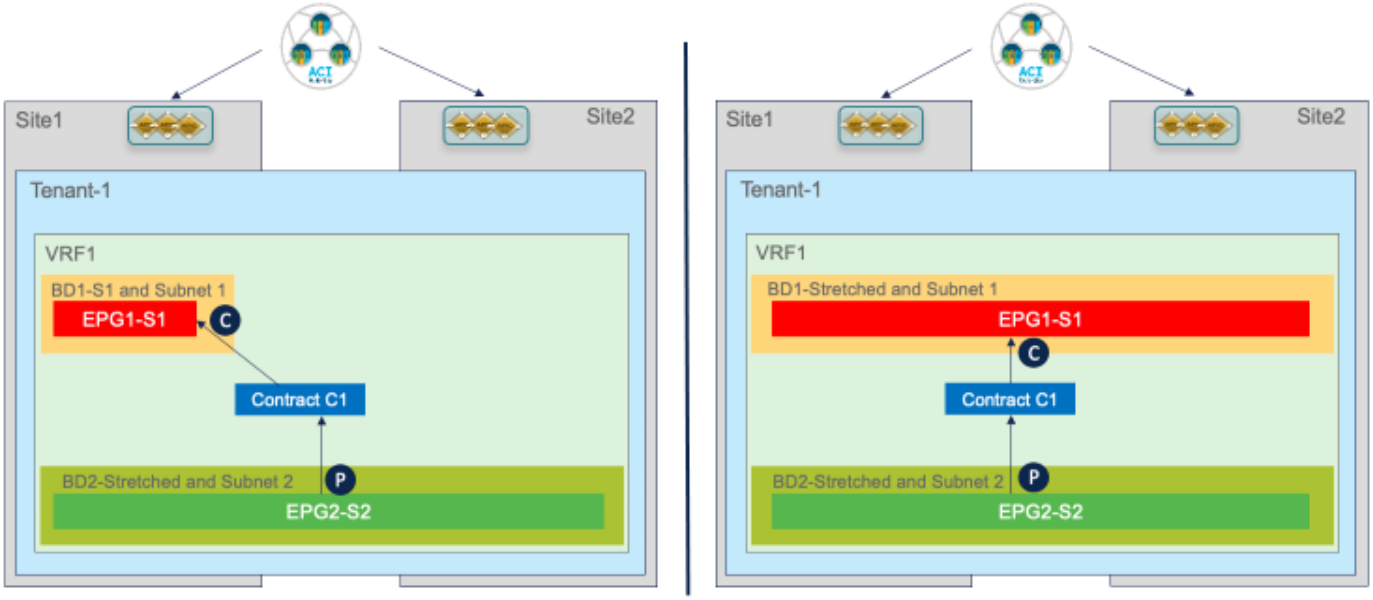


図 52.
ローカルまたはストレッチ EPG 間の EPG 間通信

サイトローカル EPG/BD の作成

サイト ローカル EPG/BD の作成は、拡張 EPG の使用例で説明したものと同様です。主な違いは、これらのオブジェクトは、ポリシーをプロビジョニングする特定の ACI ファブリックにのみ関連付けられているテンプレートで定義する必要があることです。図 53 に、Site1 にのみプロビジョニングする必要がある EPG1-S1 と BD1-S1 の作成を示します（ローカル EPG/BD オブジェクトの Site2 に関連付けられたテンプレートで同様の設定が必要です）。

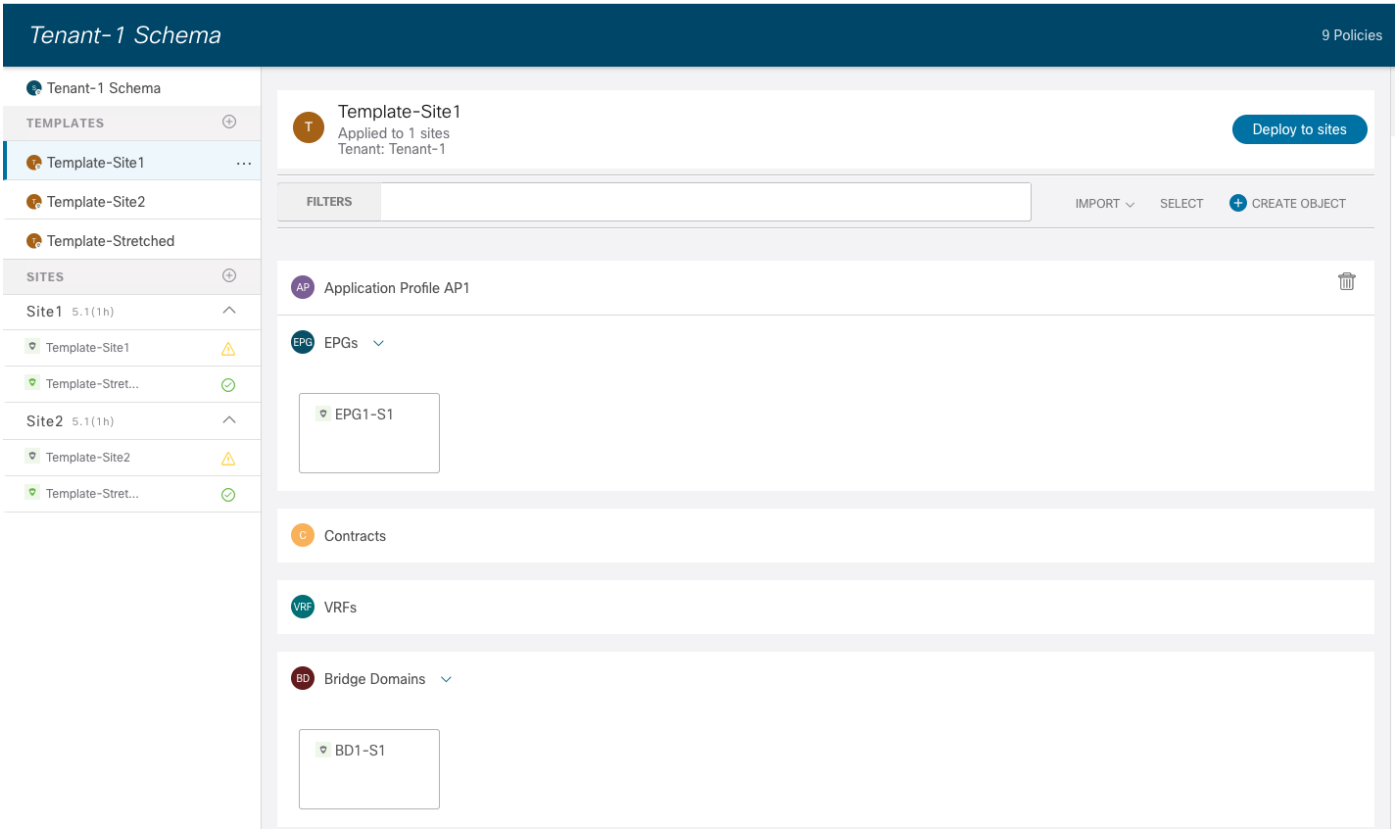


図 53.
サイト固有のテンプレートで定義された EPG/BD

したがって、以前に展開されたストレッチ VRF にローカル BD をマッピングする場合などには、テンプレート間参照が必要になります。Nexus Dashboard Orchestrator では、同じスキーマで定義されたテンプレート間、または異なるスキーマ間でオブジェクトを相互参照できます。

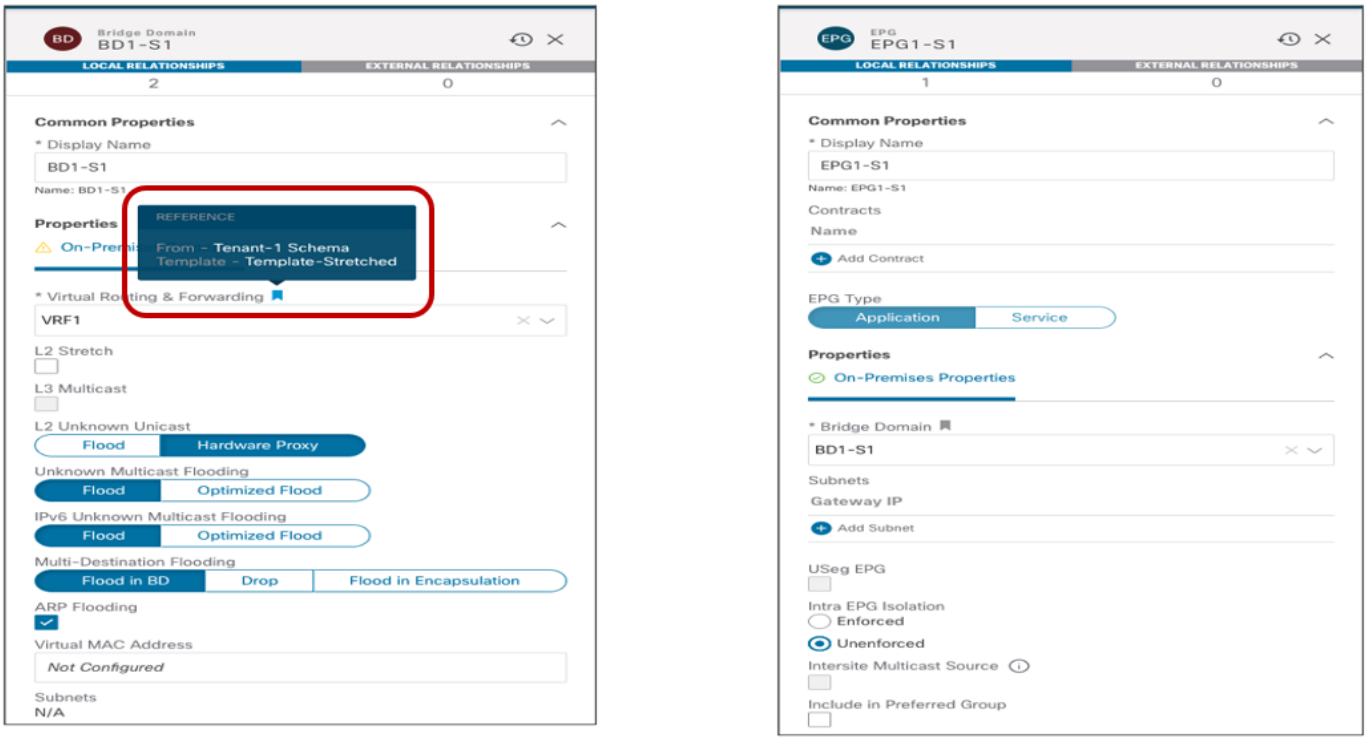


図 54.
ローカル BD および EPG の設定

EPG と BD ローカル オブジェクトを定義した後は、ストレッチ EPG の使用例で説明したのと同じサイトローカル設定を実行する必要があります。BD サブネットはサイトローカル レベルで割り当てられ（BD がローカライズされるため）、ローカル EPG をローカルドメイン（物理、VMM など）にマッピングすることが要求されます。

EPG 間のセキュリティ コントラクトの適用

ローカル EPG/BD オブジェクトが各ファブリックに作成されると、それらの間の通信を確立するために、すべてのトラフィックまたは特定のプロトコルを許可するセキュリティ ポリシー（コントラクト）を適用する必要があります。コントラクトと関連するフィルタは、両方のファブリックで使用できるように Template-Stretched で定義できます。

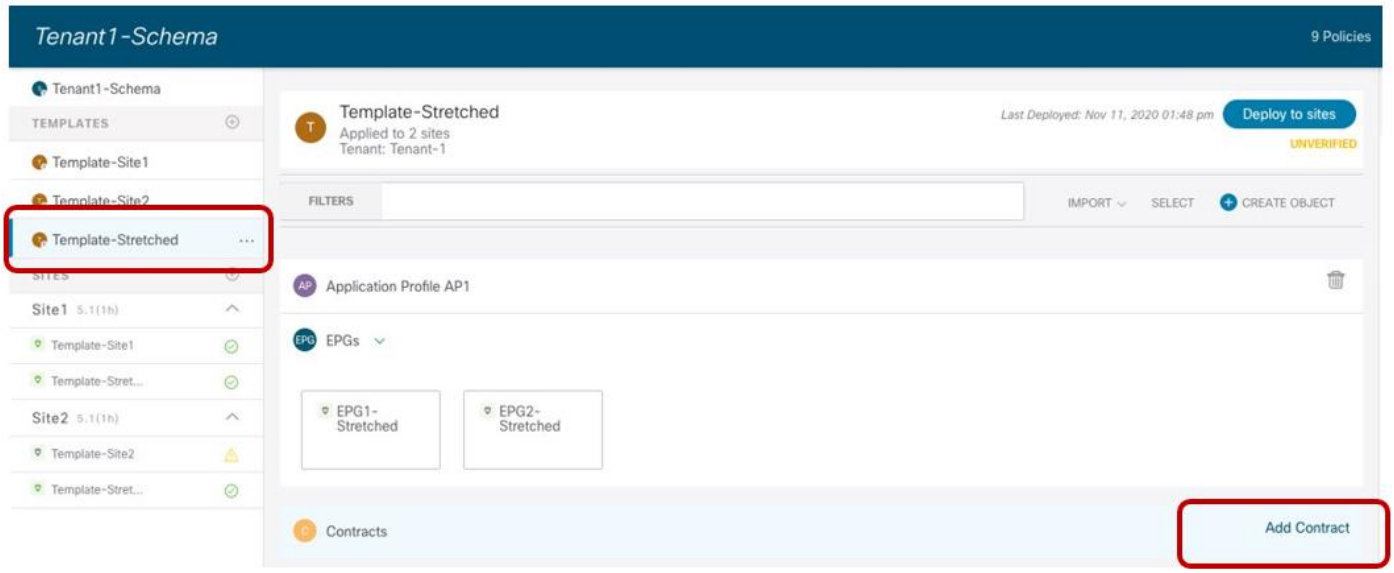


図 55.
Template-Stretched でのコントラクトの作成

コントラクトでは、許可するトラフィックを指定するために使用される 1 つ以上のセキュリティフィルタを参照する必要があります。「拒否 (Deny)」エントリを使用してフィルタを作成することが可能である点にも注意してください（以前のリリースでは「Permit (許可)」が唯一のオプションでした）。

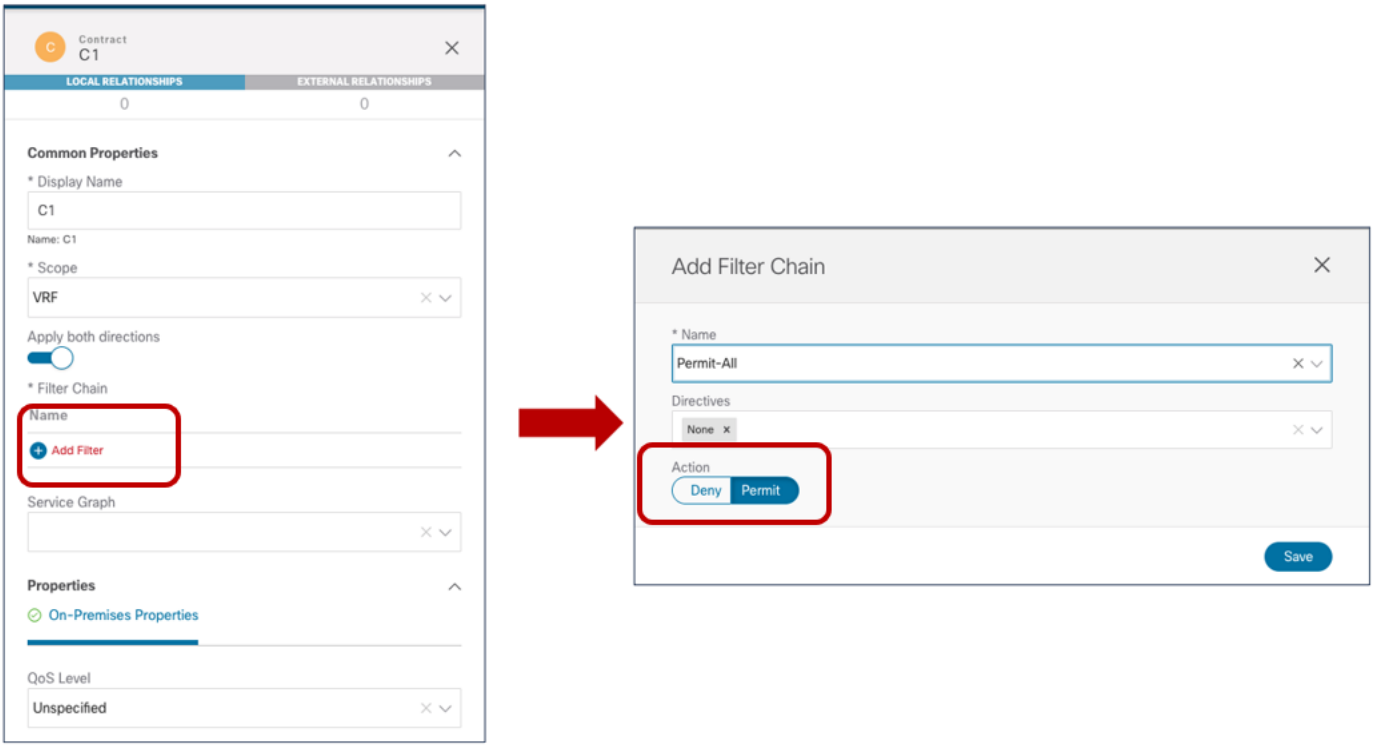


図 56.
コントラクトに関連付けられた拒否/許可フィルタの定義

最後の手順は、許可（または拒否）されるトラフィック フローを定義するために使用される特定のフィルタのエントリを作成することです。次の図 57 の特定の例では、すべてのトラフィックに一致するように変換するデフォルト設定を使用しています。

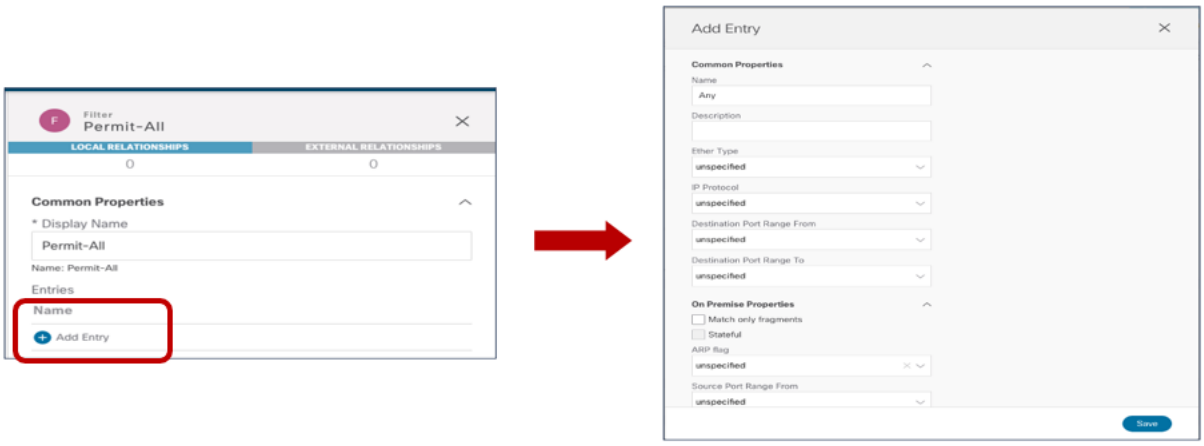


図 57.
トラフィックの拒否/許可に対するフィルタのエントリの作成

関連付けられたフィルタとのコントラクトが準備できたら、コントラクトを「提供」する EPG と、それを「消費」する EPG を定義できます。ACI Multi-Site でコントラクトを使用する場合のベストプラクティスの推奨事項は、使用するすべてのコントラクトのプロバイダー側とコンシューマー側を常に明確に識別することです。これは、「サービス ノードと ACI マルチサイトの統合」のセクションで詳しく説明されているように、目標がサービス グラフをコントラクトにアタッチすることである場合に特に重要です。ACI コントラクトの使用に関する詳細については、以下のドキュメントを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743951.html

EPG 間のサイト間通信の確認

コントラクトが適用されると、異なる EPG のエンドポイント間のサイト間接続を確立できます。エンドポイントが相互に通信を開始する前に、次の出力に示すように、エンドポイントは接続先のリーフ ノードでローカルに学習されます。

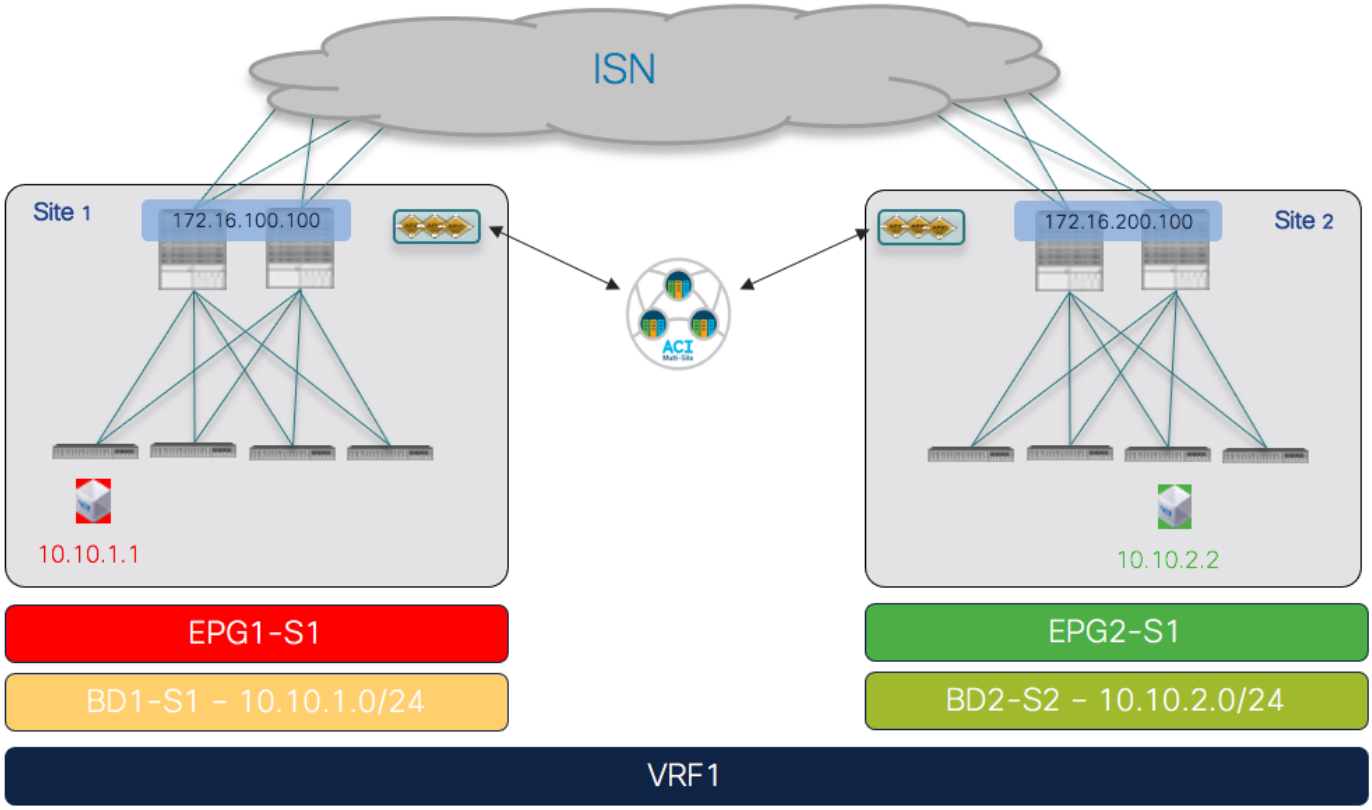


図 58.
ローカル EPG に接続されたエンドポイント

Leaf 101 Site1

```
Leaf101-Site1# show endpoint vrf Tenant-1:VRF1
凡例：
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
 L - local            E - shared-service
+------------------------------+--------------+----------------+-------------+---------
----+
      VLAN/                           Encap            MAC Address       MAC
Info/       Interface
      Domain                          VLAN             IP Address        IP Info
+ ------------------------------ + -------------- + ----------------- + -------------- +
------------ +
55                                      vlan-
819    0050.56b9.1bee LpV                       po1
```

```
Tenant-1:VRF1                           vlan-
819         10.10.1.1 LpV                       po1
```

Leaf 303 Site2

```
Leaf303-Site2# show endpoint vrf Tenant-1:VRF1
凡例：
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
 L - local            E - shared-service
+------------------------------+--------------+----------------+-------------+---------
----+
      VLAN/                           Encap           MAC Address       MAC
Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+ ------------------------------ + --------------- + ----------------- + -------------- +
------------- +
34                                      vlan-118    0050.56b3.e41e
LV                        po4
Tenant-1:VRF1                           vlan-118         10.10.2.2
LV                        po4
```

リーフ ノードのルーティング テーブルには、コントラクトの結果として、ローカル スパイン ノードでプロビジョニングされたプロキシ TEP アドレスを指すリモート EPG に関連付けられた IP サブネットもインストールされます。この逆は、Site2 のリーフ ノードで発生します。

Leaf 101 Site1

```
Leaf101-Site1# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.1.112.66%overlay-1, [1/0], 01:01:38, static, tag 4294967294
10.10.1.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 10.10.1.254, vlan54, [0/0], 01:01:38, local, local
10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.1.112.66%overlay-1, [1/0], 00:04:51, static, tag 4294967294
Leaf 303 Site2
Leaf303-Site2# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
```

```
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.136.66%overlay-1, [1/0], 00:06:47, static, tag 4294967294
10.10.2.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.136.66%overlay-1, [1/0], 00:06:47, static, tag 4294967294
10.10.2.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 10.10.2.254, vlan33, [0/0], 00:06:47, local, local
```

エンドポイント間の接続が確立されると、各サイトのリーフ ノードは、データ プレーン アクティビティを介してリモート エンドポイントの特定の情報を学習します。次の出力は、たとえばSite1 のリーフ ノードのエンドポイント テーブルを示しています。

Leaf 101 Site1

```
Leaf101-Site1# show endpoint vrf Tenant-1:VRF1
凡例：
 s - arp              H - vtep             V - vpc-attached     p - peer-aged
 R - peer-attached-rl B - bounce           S - static           M - span
 D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
 L - local            E - shared-service
+------------------------------+--------------+----------------+-------------+---------
----+
      VLAN/                          Encap           MAC Address       MAC
Info/       Interface
      Domain                         VLAN            IP Address        IP Info
+ ------------------------------ + -------------- + ----------------- + ------------- +
------------ +
Tenant-
1:VRF1                                              10.10.2.2                      tunnel26
55                                    vlan-
819    0050.56b9.1bee LpV                     po1
Tenant-1:VRF1                         vlan-
819         10.10.1.1 LpV                      po1
```

リモート エンドポイント10.10.2.2 は、VXLAN tunnel26 経由で到達可能として学習されます。予想どおり、このようなトンネルの宛先はSite2 の O-UTEP アドレス（172.16.200.100）です。

Leaf 101 Site1

```
Leaf101-Site1# show interface tunnel 26
Tunnel26 is up
    MTU 9000 bytes, BW 0 Kbit
    Transport protocol is in VRF "overlay-1"
    Tunnel protocol/transport is ivxlan
```

```
Tunnel source 10.1.0.68/32 (lo0)
Tunnel destination 172.16.200.100/32
```

名前空間変換情報の確認

ストレッチ EPG の使用例で説明したように、VXLAN データパスを使用してサイト間通信を確立する必要が生じるたびに、スパインに変換エントリを作成する必要があります。各ファブリックにローカルに展開された EPG/BD 間の EPG 間接続の特定の使用例では、それらの間にセキュリティポリシーを作成すると、リモートサイトの APIC ドメインでいわゆる「シャドウオブジェクト」（図 59）が作成されます。

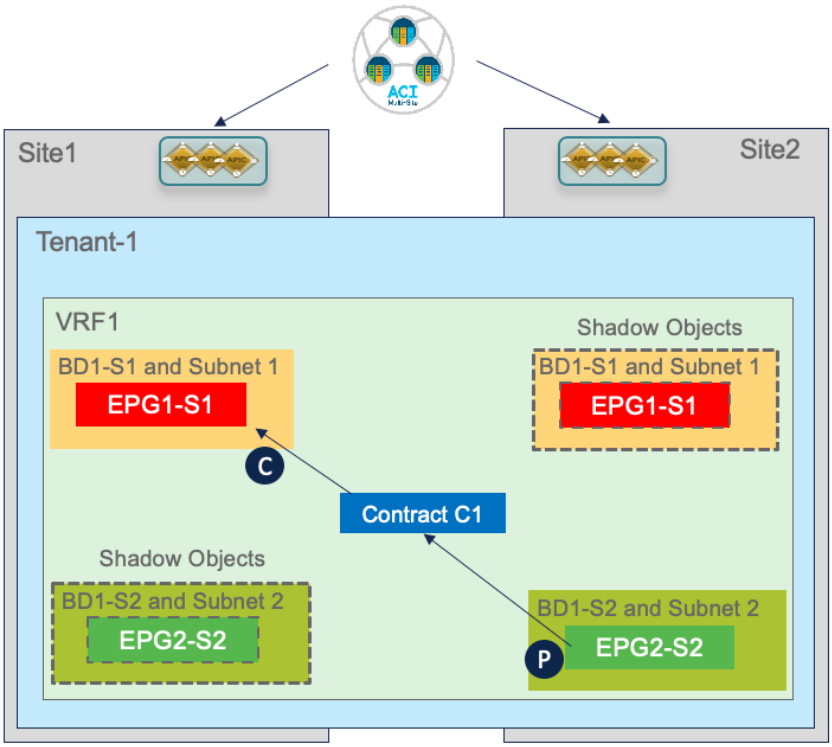


図 59.
シャドウオブジェクトの作成

ACI リリース 5.0(2) 以降、シャドウオブジェクトは APIC においてデフォルトで非表示になっています。表示を有効にするには、図 60 に示す [非表示のポリシーを表示 (Show Hidden Policies)] オプションのフラグをオンにする必要があります。

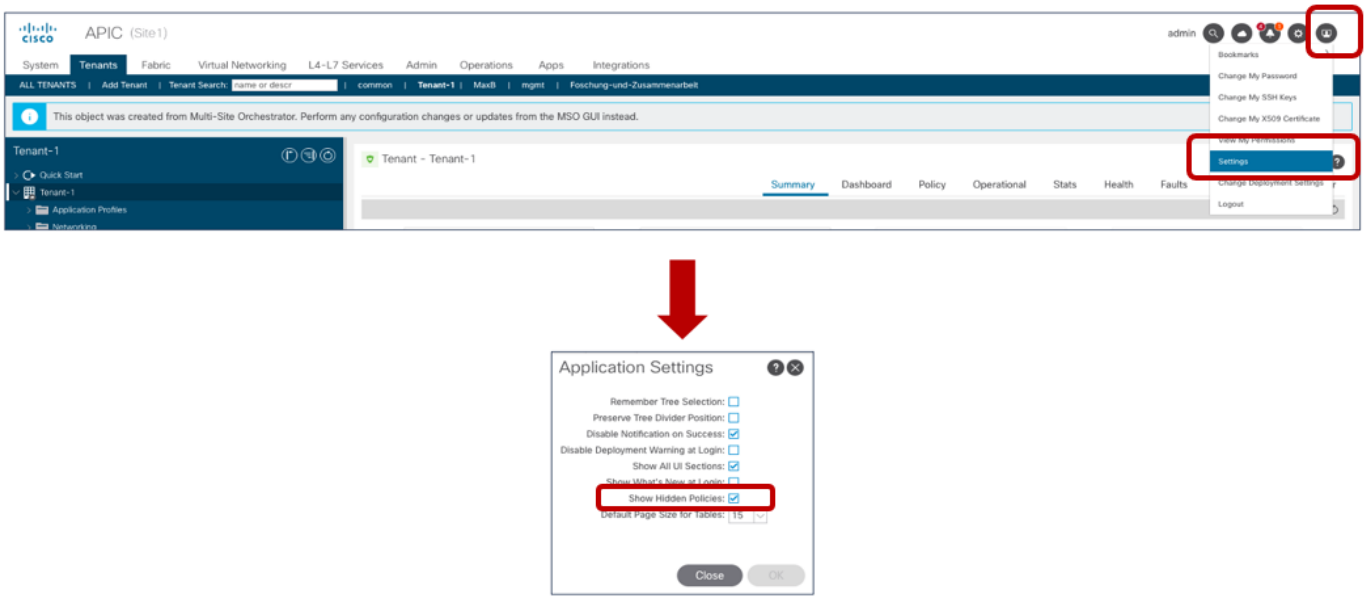


図 60.
シャドウ オブジェクトの表示の有効化

Nexus Dashboard Orchestrator リリース 3.4(1) 以降で使用可能な「テンプレート展開プラン」機能は、作成されたオブジェクトとその場所に関する情報を明確に提供できるため、非常に興味深い機能です。この例では、Site1 の EPG1-S1 によって提供されるコントラクトを消費するように Site2 の EPG2-S2 を設定すると（図 61 の [サイトに展開 (Deploy to sites)] ウィンドウで提供される情報）、展開プランはこれらのシャドウ オブジェクトの作成を強調表示します（図 62）。

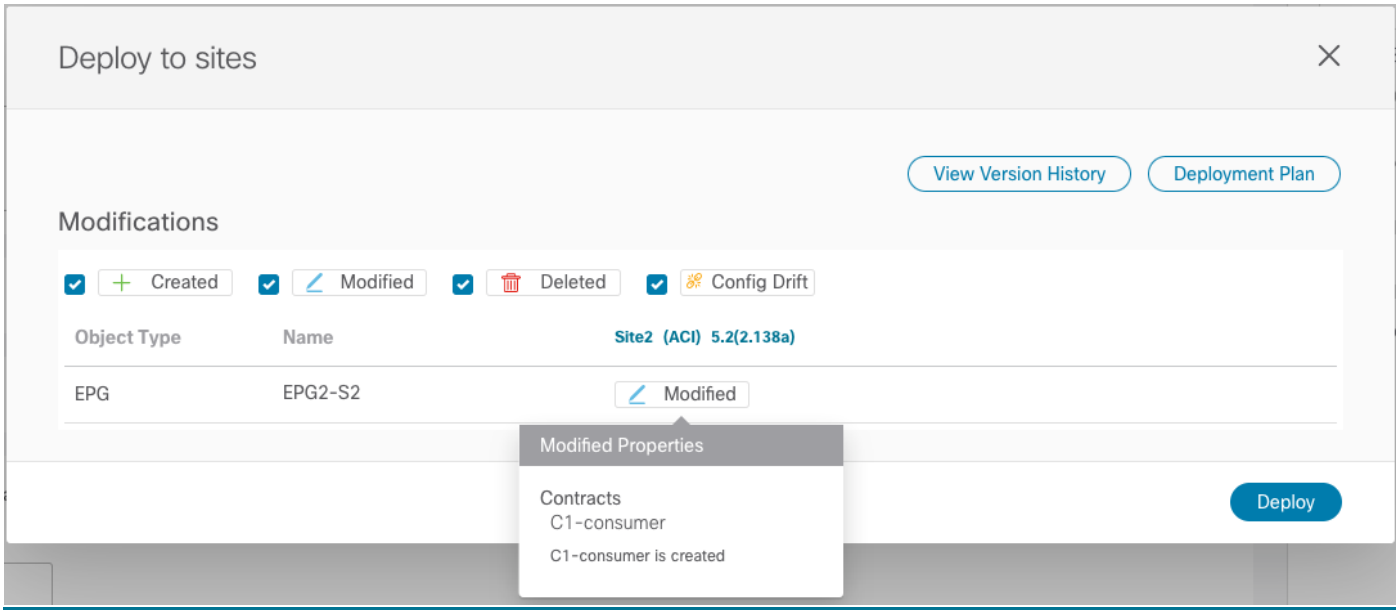


図 61.
消費されるコントラクトの EPG-S2 への追加

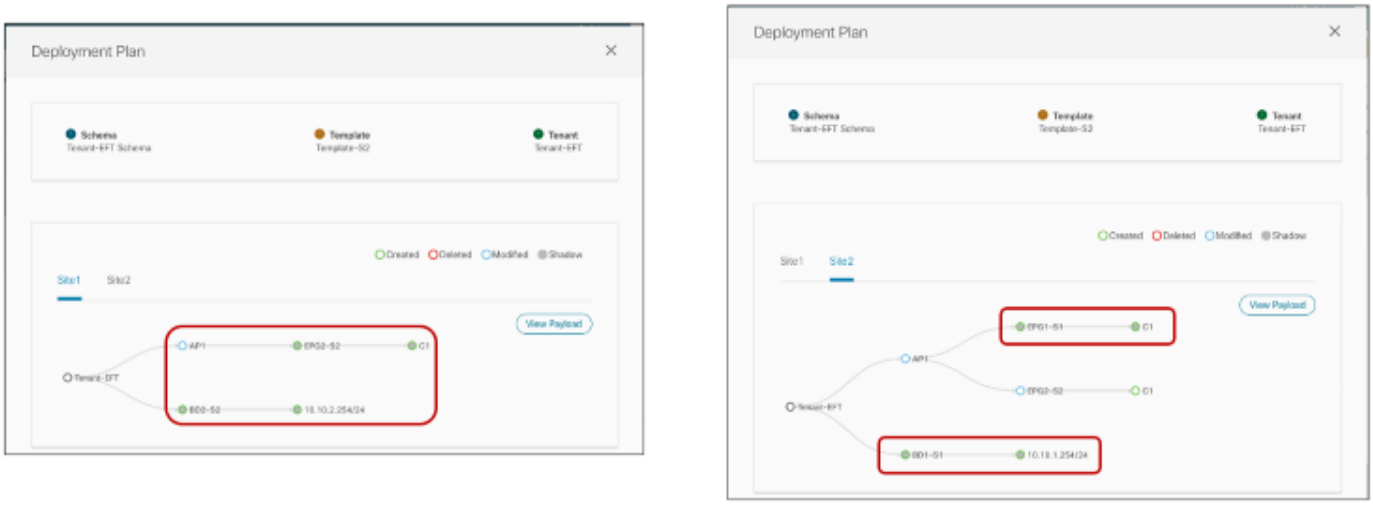


図 62.
展開プランで強調表示されるシャドウ オブジェクトの作成

シャドウ オブジェクトの作成では、サイト間データ プレーン通信を正常に行うために、スパインの変換テーブルで設定する必要がある特定のリソース（セグメント ID、クラス ID など）の割り当てが可能である必要があります。

たとえば、Site2 の APIC を見ると、Site2 でローカルに定義された EPG と BD がシャドウ オブジェクトとして表示されていることがわかります。

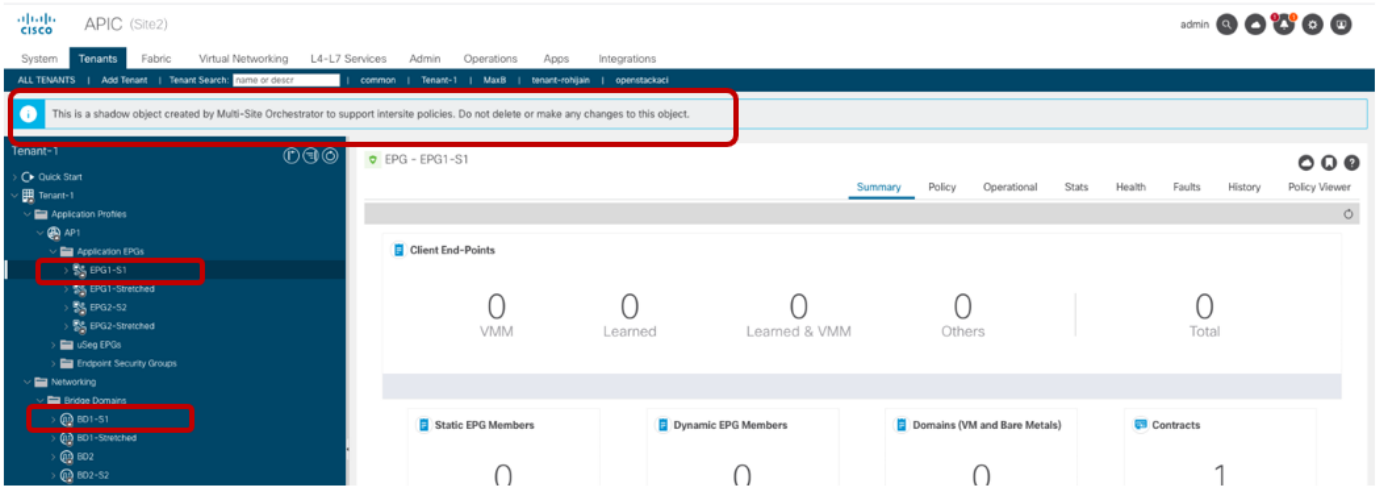


図 63.
APIC でのシャドウ オブジェクトの表示

EPG1-S1 および BD1-S1 は、Site1 でのみローカルに作成されたオブジェクトです（サイト ローカル オブジェクトを表すため）。ただし、EPG1-S1 と EPG2-S2 間のセキュリティ ポリシーの確立により、Site2 を管理する APIC でもこれらのオブジェクトが作成されました。EPG2-S2 と BD2-S2 でも同じ動作が見られます。図 64 と図 65 に、これらのオブジェクトに割り当てられた特定のセグメント ID とクラス ID の値を示します（エントリは図 49 と図 50 に示したものと同じであるため、VRF は示されていません）。

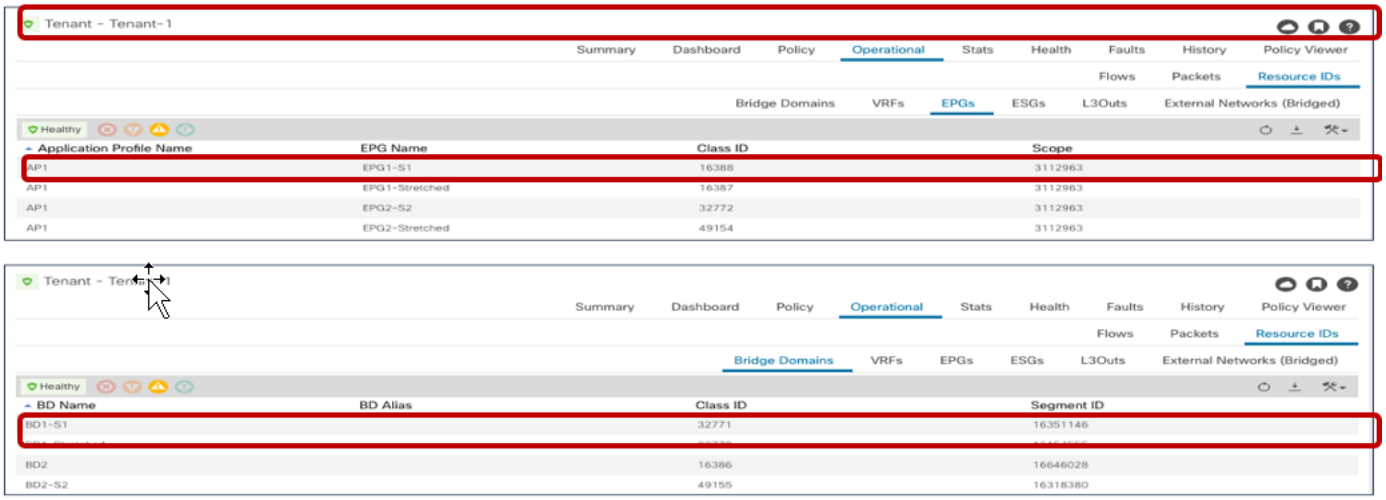


図 64.
Site1 のローカルおよび シャドウ オブジェクトのセグメント ID とクラス ID

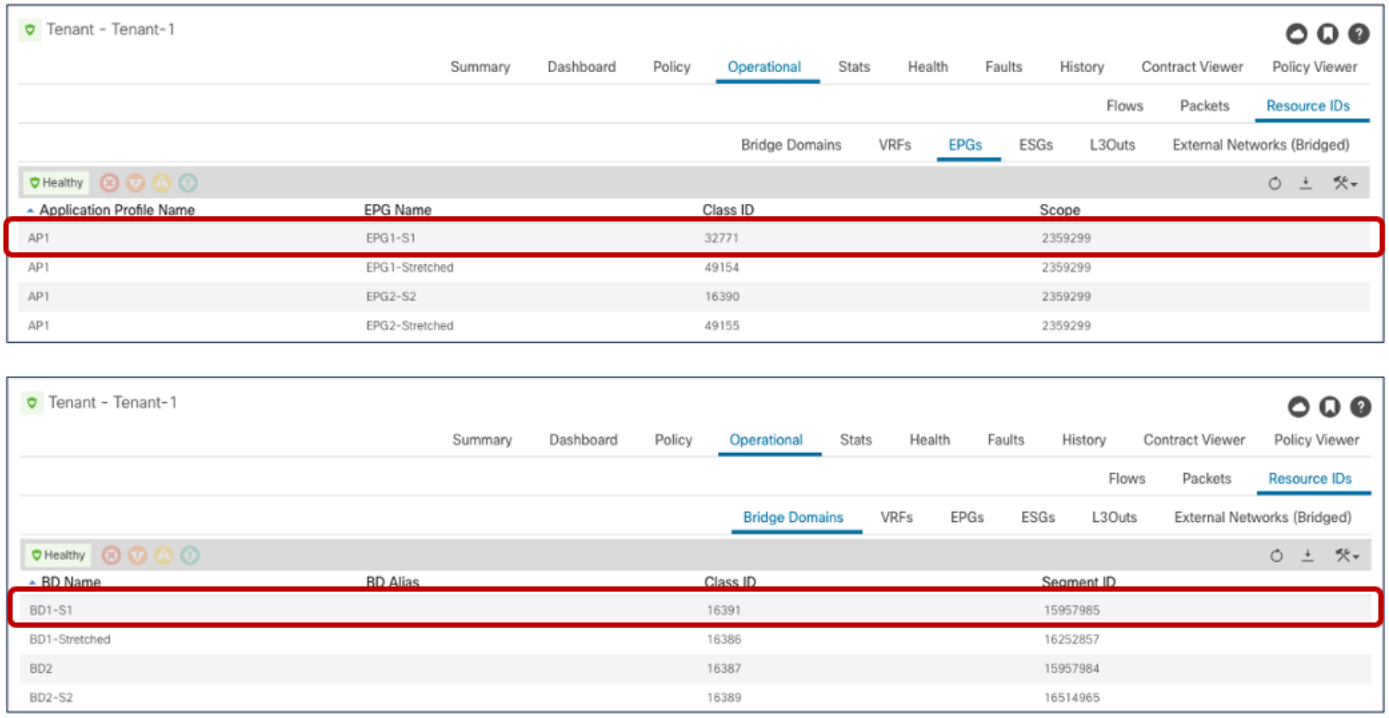


図 65.
Site2 のローカルおよび シャドウ オブジェクトのセグメント ID とクラス ID

これらの値は、EPG1-S1 の Site1 部分のエンドポイントと EPG2-S2 の Site2 部分のエンドポイント間でトラフィックが交換されるときに、適切な変換機能を実行できるように、スパインの変換テーブルにプログラムされます。

セグメント ID に関係するのは、VRF のエントリだけです。これは、サイト間でルーティングを行う場合、VRF L3 VNID 値が VXLAN ヘッダーに挿入され、受信側サイトが正しいルーティング ドメインでレイヤ 3 ルックアップを実行できるようにするためです。BD に関連付けられたセグメント ID のトランスレーション エントリを

インストールする必要はありません（VXLAN ヘッダーでこれらの値を伝送するサイト間トラフィックが存在しないためです）。

Spine 1101 Site1

```
Spine1101-Site1# show dcimgr repo vnid-maps
------------------------------------------------------------
     Remote             |           Local
site Vrf Bd | Vrf Bd Rel-state
------------------------------------------------------------
2 2359299 | 3112963 [formed]
```

Spine 401 Site2

```
Spine401-Site2# show dcimgr repo vnid-maps
------------------------------------------------------------
     Remote             |           Local
site Vrf Bd | Vrf Bd Rel-state
------------------------------------------------------------
1 3112963 | 2359299 [formed]
```

代わりに、EPG およびシャドウ EPG のクラス ID が次の出力に表示されます。

Spine 1101 Site1

```
Spine1101-Site1# show dcimgr repo sclass-maps
------------------------------------------------------------
     Remote             |        Local
site Vrf PcTag | Vrf PcTag Rel-state
------------------------------------------------------------
2 2359299 | 3112963 [formed]
2 2359299 | 3112963 [formed]
```

Spine 401 Site2

```
Spine401-Site2# show dcimgr repo sclass-maps
------------------------------------------------------------
     Remote             |        Local
site Vrf PcTag | Vrf PcTag Rel-state
------------------------------------------------------------
1 3112963 32772 | 2359299 16390 [formed
1 3112963 16388 | 2359299 32771 [formed]
```

スパインの変換エントリのプログラミングに加えて、シャドウ EPG へのクラス ID の割り当ても、コントラクトに関連付けられたセキュリティ ポリシーを適切に適用できるようにするために重要です。「EPG から EPG へのサイト間通信の確認」のセクションですでに説明したように、VRF 内サイト間トラフィック フローが確立

されると、リモート エンドポイント情報がローカル リーフ ノードで学習されます。これにより、フローの両方向の入力リーフ ノードでコントラクトを常に適用できます。

次の出力は、EPG1-S1 のエンドポイント部分がローカルに接続されている Site1 のリーフ 101 にプログラムされたセキュリティ ルールを示しています。お気づきのように、16388（EPG1-S1 のクラス ID）と32772（シャドウ EPG2-S2 のクラス ID）の間の通信には、コントラクト C1 に関連付けられた許可エントリがあります。リターン フローのエントリもあります。これは、何らかの理由で、Site2 のリモートリーフ ノードの入力方向にポリシーを適用できない場合にのみ使用されます。

Leaf 101 Site1

```
Leaf101-Site1# show zoning-rule scope 3112963
+ --------- + -------- + -------- + ---------- + ---------- ------ + --------- + --------- +
------------ + --------- -+ ---------------------- +
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+---------------+---------+---------+-------------+-
---------+----------------------+
| 4151 | 0 | 0 | implicit | uni-dir | enabled | 3112963 | | deny,log | any_any_any(21) |
| 4200 | 0 | 0 | implarp | uni-dir | enabled | 3112963 | | permit | any_any_filter (17) |
| 4198 | 0 | 15 | implicit | uni-dir | enabled | 3112963 | | deny,log | any_vrf_any_deny(22)
|
| 4213 | 0 | 32771 | implicit | uni-dir | enabled | 3112963 | | permit | any_dest_any(16) |
| 4219 | 16388 | 32772 | default | uni-dir-ignore | enabled | 3112963 | Tenant-1:C1 | permit
| src_dst_any(9) |
| 4220 | 32772 | 16388 | default | bi-dir | enabled | 3112963 | Tenant-1:C1 | permit |
src_dst_any(9) |
| 4203 | 0 | 32770 | implicit | uni-dir | enabled | 3112963 | | permit | any_dest_any(16) |
+---------+--------+--------+----------+---------------+---------+---------+-------------+-
---------+----------------------+
```

同様の出力は、EPG2-S2 のエンドポイント部分がローカルに接続されているサイト 2 のリーフ 303 にあります。ここで使用されるクラス ID の値は、シャドウ EPG1-S1（32771）およびローカル EPG2-S2（16390）の Site2 でプログラムされたものであることに注意してください。

Leaf 303 Site2

```
Leaf303-Site2# show zoning-rule scope 2359299
+ --------- + -------- + -------- + ---------- + ---------- ------ + --------- + --------- +
------------ + --------- -+ ---------------------- +
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+---------------+---------+---------+-------------+-
---------+----------------------+
| 4183 | 0 | 0 | implicit | uni-dir | enabled | 2359299 | | deny,log | any_any_any(21) |
| 4182 | 0 | 0 | implarp | uni-dir | enabled | 2359299 | | permit | any_any_filter(17) |
| 4181 | 0 | 15 | implicit | uni-dir | enabled | 2359299 | | deny,log | any_vrf_any_deny(22)
|
| 4176 | 0 | 16387 | implicit | uni-dir | enabled | 2359299 | | permit | any_dest_any(16) |
| 4190 | 0 | 16386 | implicit | uni-dir | enabled | 2359299 | | permit | any_dest_any(16) |
| 4176 | 0 | 16387 | implicit | uni-dir | enabled | 2359299 | | permit | any_dest_any(16) |
```

```
| 4207 | 16390 | 32771 | default | bi-dir | enabled | 2359299 | Tenant-1:C1 | permit |
src_dst_any(9) |
| 4206 | 32771 | 16390 | default | uni-dir-ignore | enabled | 2359299 | Tenant-1:C1 | permit
| src_dst_any(9) |
+---------+--------+--------+----------+----------------+---------+---------+-------------+-
---------+----------------------+
```

サイト間接続を有効にするための優先グループの使用

VRF 内での EPG 間通信を可能にするコントラクトの使用に対する代替アプローチは、優先グループ機能の使用です。

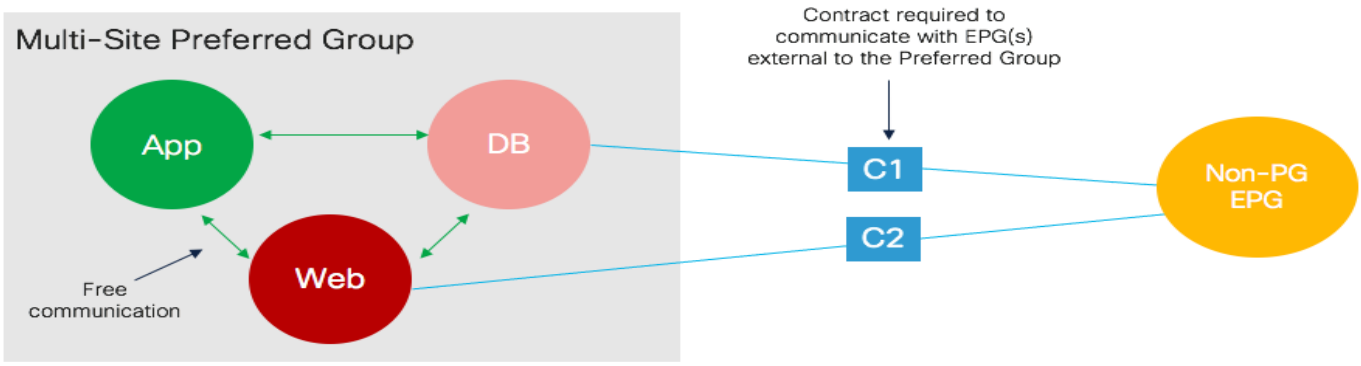


図 66.
EPG 間のフリーな VRF 内通信での優先グループの使用

定義された VRF ごとに 1 つの優先グループがサポートされ、EPG を選択的に追加できます。優先グループに属する EPG は、コントラクトを使用せずに相互に通信できます。優先グループの一部ではない EPG との通信では、セキュリティ ポリシーの定義が必要です（図 66）。

APIC の優先グループは、機能がアクティブになるようにグローバルに有効にする必要があります。図 67 で強調表示されているように、このノブはデフォルトで無効になっています。

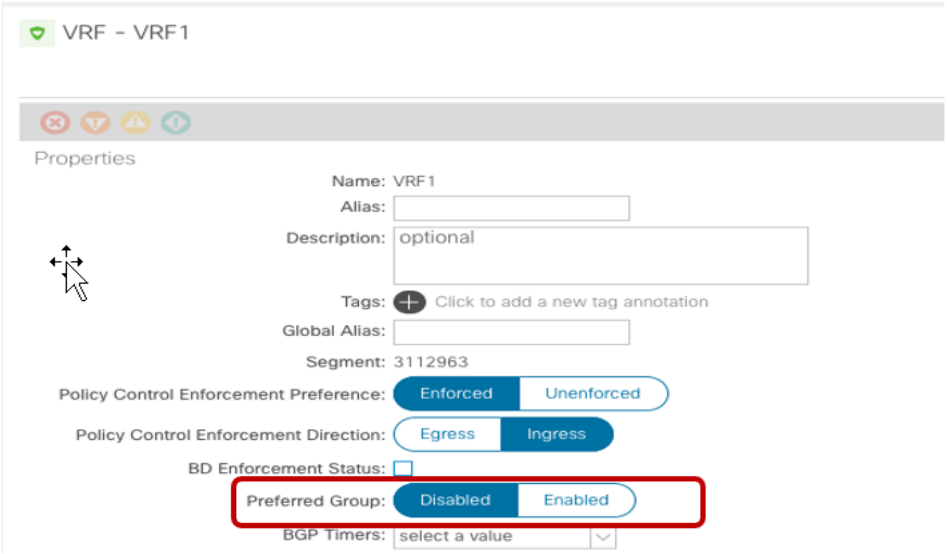


図 67.
APIC のグローバル優先グループ ノブ

グローバル ノブを無効にすると、優先グループ内の EPG が相互に自由に通信できなくなります。ただし、グローバル VRF レベル ノブは Nexus Dashboard Orchestrator には表示されません。Nexus Dashboard Orchestrator でのみ優先グループに EPG を追加/削除する場合の動作は次のとおりです。

- NDO の優先グループに最初の EPG を追加すると、NDO は vRF レベルでグローバル ノブを有効にします。
- NDO の優先グループから最後の EPG を削除すると、NDO は vRF レベルでグローバル ノブを無効にします。

優先フィールドがすでに APIC レベルでグローバルに有効になっているブラウンフィールドシナリオでは、動作が少し異なります（たとえば、優先グループ機能は、NDO が設計に統合される前に APIC に展開されているため）。このような状況では、NDO の優先グループへの EPG の追加を開始する前に、VRF オブジェクトを APIC から NDO にインポートすることを強くお勧めします。これにより、優先グループがすでに有効になっている（APIC レベルで）情報が NDO に提供されます。これにより、NDO の優先グループから最後の EPG を削除するときに、NDO がグローバル ノブを無効にして、EPG 間の通信に影響を与えないようにします。優先グループの一部であり、NDO によって管理されていない（つまり、APIC で直接設定され、NDO にインポートされていない EPG）。

NDO の優先グループに EPG を追加する設定は非常に簡単で、図 68 に示すとおりです。サイト内でローカルに定義された EPG、または複数のロケーションにまたがる EPG に適用できます。

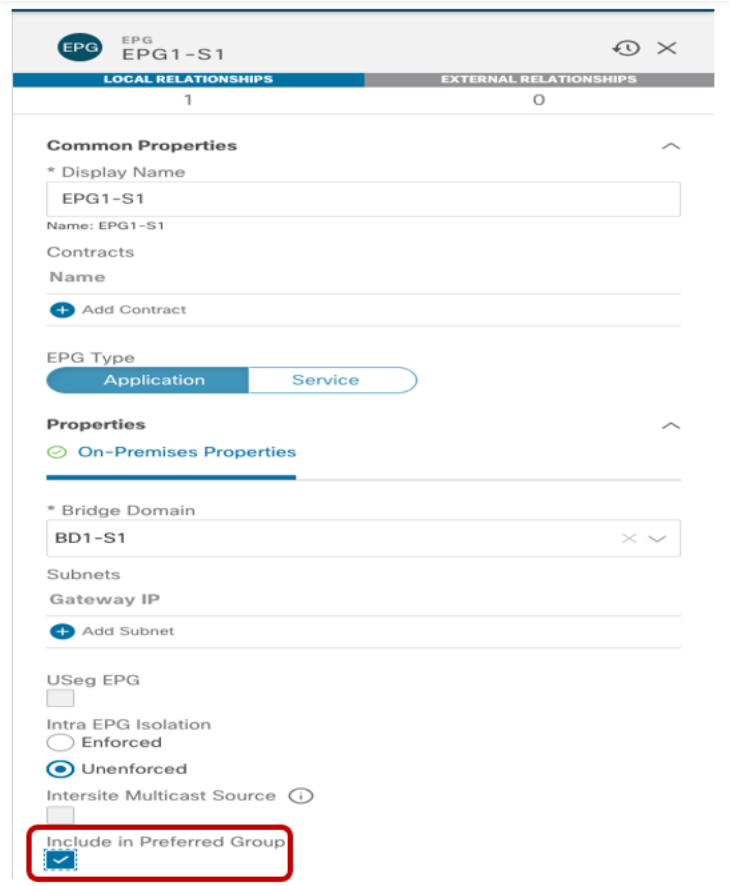


図 68.
NDO の優先グループへの EPG の追加

設定が展開されると、変換エントリとシャドウ オブジェクトが自動的に作成され、優先グループに属するすべての EPG 間でサイト間接続を確立できるようになります。マルチサイト展開で優先グループの一部として展開できる EPG の最大数の詳細については、ACI スケーラビリティガイドを参照してください。

次の出力は、有効化の結果としてACI リーフ ノードにプログラムされたセキュリティ ルールを示しています。

Leaf 101 Site1

```
Leaf101-Site1# show zoning-rule scope 3112963
+---------+--------+--------+----------+---------+---------+---------+------+----------+----
-----------------+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+---------+---------+---------+------+----------+----
-----------------+
| 4151 | 0 | 0 | implicit | uni-dir | enabled | 3112963 | | deny,log | any_any_any(21) |
| 4200 | 0 | 0 | implarp | uni-dir | enabled | 3112963 | | permit | any_any_filter(17) |
+---------+--------+--------+----------+---------+---------+---------+------+----------+----
-----------------+
```

注： SrcEPG および DstEPG が「0」のエントリは、優先グループ設定のために追加される暗黙の許可ルールです（優先グループにない EPG が追加されると、暗黙の拒否ルールが追加されます）。優先グループの詳細については、以下のペーパーを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743951.html#Preferredgroup

vzAny の使用

EPG の VRF レベルで使用できるもう 1 つの興味深い機能は、vzAny です。 vzAny は、特定の VRF 内に展開されているすべての EPG を表す論理グループ構造です（つまり、EPG は vRF の一部である BD にマッピングされます）。vzAny を使用すると、セキュリティ ポリシーの適用を簡素化して、2 つの特定の使用例（多対 1 接続モデルの作成と Any-to-any 接続モデルの作成）を実装できます。

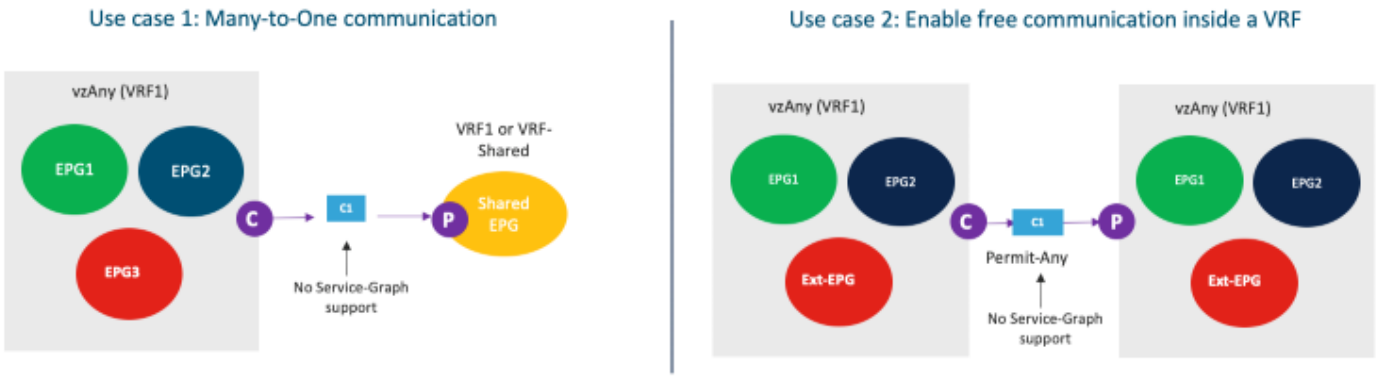


図 69.
vzAny の使用例

マルチサイト展開での VzAny の使用に適用されるいくつかの制限を強調することが重要です。

- Nexus Dashboard Orchestrator 3.5(1) リリースでは、vzAny にアタッチされたサービス グラフを使用したり、コントラクトを提供したりすることはできません。これには、APIC およびスイッチング レベルでも実装を変更する必要があるため、今後サポートされる予定です。

- 上の図に示すように、vzAny は共有サービス シナリオのコントラクトのコンシューマーになることができます（つまり、プロバイダーは異なる VRF の EPG です）。ただし、コンシューマーが別の VRF の EPG にある場合、vzAny をコントラクトのプロバイダーにすることはできません（これは、ACI 単一ファブリック設計にも適用される制限です）。

2 番目の使用例は、セキュリティ ポリシーの適用を削除し、ACI Multi-Site を使用してファブリック間のネットワーク接続を確立することを目的とする場合の優先グループの代替アプローチです。プロビジョニングの観点からは、必要な設定は非常に単純で、「全許可」フィルタに関連付けられたコントラクトを定義するだけで済みます（前の図 56 と図 57 を参照）。コントラクトが作成されると、VRF レベルで VzAny に適用できます（図 70 を参照）。

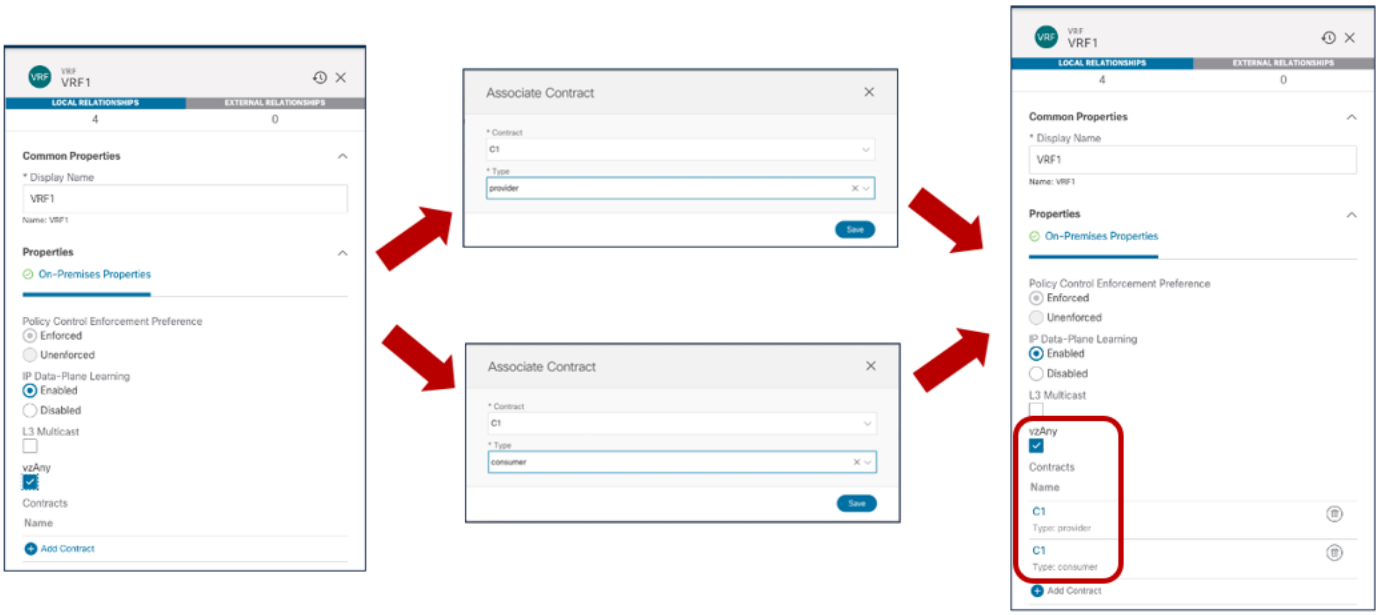


図 70.
vzAny が「全許可」コントラクトのプロバイダー/コンシューマーになるように設定

上記の設定の結果、変換エントリとシャドウ オブジェクトが両方の APIC ドメインで作成され、すべての VRF 内通信が自由に行われるようになります。機能的な観点から、この設定は、VRF のポリシー制御適用設定を「非エンフォース」に設定することに似ています。この「VRF 非エンフォース」オプションは、Multi-Site ではサポートされておらず、シングル ファブリック展開でもベスト プラクティスとは見なされません。したがって、ここで説明する VzAny 設定を使用して同じ目的を達成することを推奨します。

注： Nexus Dashboard Orchestrator リリース 3.5(1) では、vzAny の設定は優先グループ機能の使用と相互に排他的です。したがって、特定の要件に応じて、どのアプローチを採用するかを事前に決定することが重要です。

サイト間の EPG 間接続（VRF 間 – 共有サービス）

「共有サービス」は、異なる VRF の一部である EPG 間のサイト間接続を確立するための固有の使用例です。図 69 では、すでに VzAny のコンテキストで共有サービスの概念が導入されていますが、同じ機能を特定の EPG 間に導入できます。

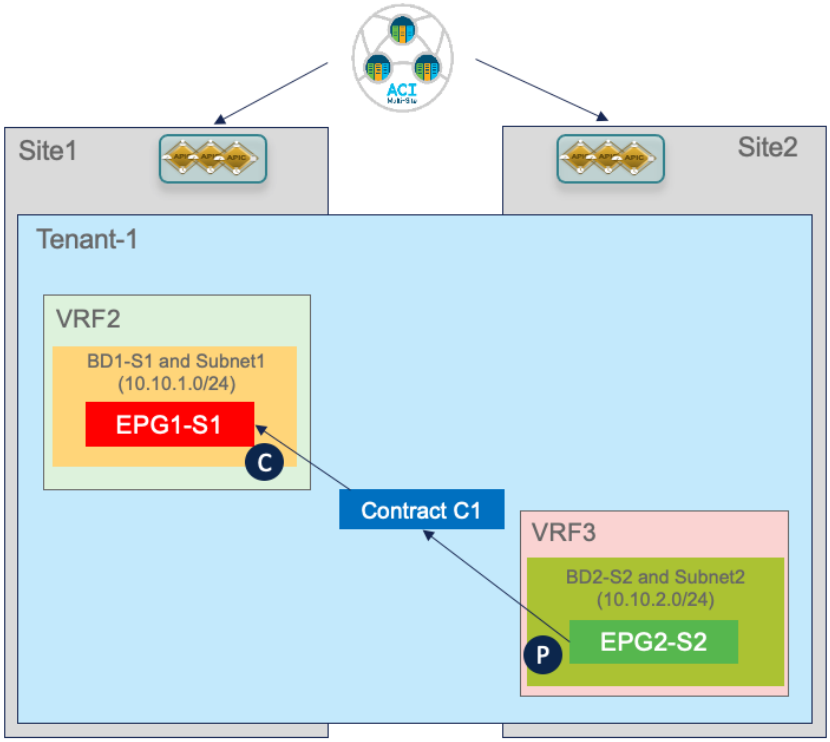


図 71.
共有サービスの使用例

高レベルの観点からは、VRF 内シナリオの「EPG 間のセキュリティ コントラクトの適用」の一部としてすでに説明した考慮事項と同じです。異なる EPG のエンドポイント間の接続を確立するには、エンドポイント間のコントラクトを作成する必要があります。ただし、次のセクションで説明するように、VRF 間でこの接続を作成する必要がある場合、追加の考慮事項はほとんどありません。

「共有サービス」設定のプロビジョニング

図 71 で強調表示されている共有サービスの使用例のプロビジョニングには、いくつかの特定の手順が必要です。

- 新しい VRF3 を定義し、それに BD2-S2 を関連付けます。
- コントラクトの適切な範囲の定義：新しく作成されたコントラクトのデフォルトの範囲は「VRF」です。これは、同じ VRF の一部であるが共有サービス シナリオでの通信を許可しない EPG 間に適用された場合にのみ有効であることを意味します。したがって、VRF が同じテナントの一部であるか、またはテナント間で定義されているかによって、スコープを「テナント」または「グローバル」に適切に変更する必要があります。

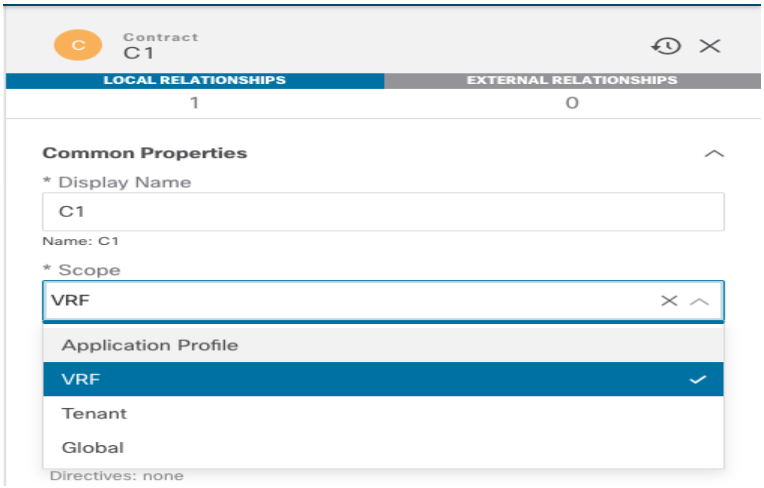


図 72.
コントラクトの適切な範囲の設定

ルーティングの観点からは、異なる VRF を使用することで、個別のルーティング ドメイン間の論理的な分離が保証されます。したがって、共有サービスの使用例では、異なるルーティング ドメイン間で接続を確立できるように、異なる VRF に適切なプレフィックス情報を入力する必要があります。この機能は通常、「ルートリーク」と呼ばれます。VRF 間のルートのリークを有効にするための最初の要件は、図 73 で強調表示されているように、BD に関連付けられた IP サブネットの [VRF 間の共有 (Shared between VRFs)] オプションを設定することです。

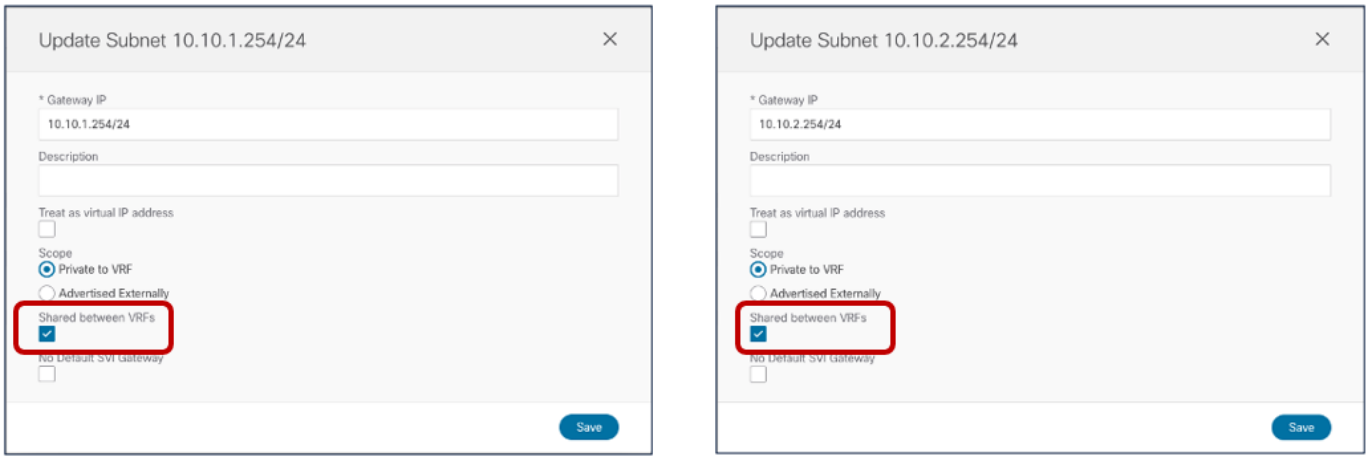


図 73.
VRF 間でリークされる BD サブネットの設定

ACI では、VRF 間でのプレフィックスのリークは、考慮される特定の方向（コンシューマーからプロバイダー、またはプロバイダーからコンシューマー）に応じて異なります。

コンシューマー VRF2（BD1-S1）の BD に関連付けられた IP サブネットは、EPG 間のコントラクトの設定に基づいてプロバイダー VRF3 にリークされます。反対方向（プロバイダー VRF3 からコンシューマー VRF2）へのリークは、代わりにプロバイダー EPG2-S2 に適用された特定の設定の結果です。

図 74 に示すように、以前に BD2-S2（プロバイダー EPG の BD）で設定した同じプレフィックスを EPG2-S2 自体で設定する必要があります。BD に適用される同じフラグは、「デフォルト SVI ゲートウェイなし」オプシ

ョンを追加してここでも設定する必要があります。この設定は、ルートをリークし、セキュリティポリシーを適用できるようにします（次のセクションで説明します）。

注： プロバイダー EPG でサブネットのプレフィックスを指定するという要件により、複数の EPG が同じ BD で定義されている場合（特定の IP サブネットに関連付けられている場合）、ルートリークのプロビジョニングが困難になります。同じ IP サブネット範囲からアドレス指定されているにもかかわらず、各 EPG の一部として展開された特定のエンドポイント。

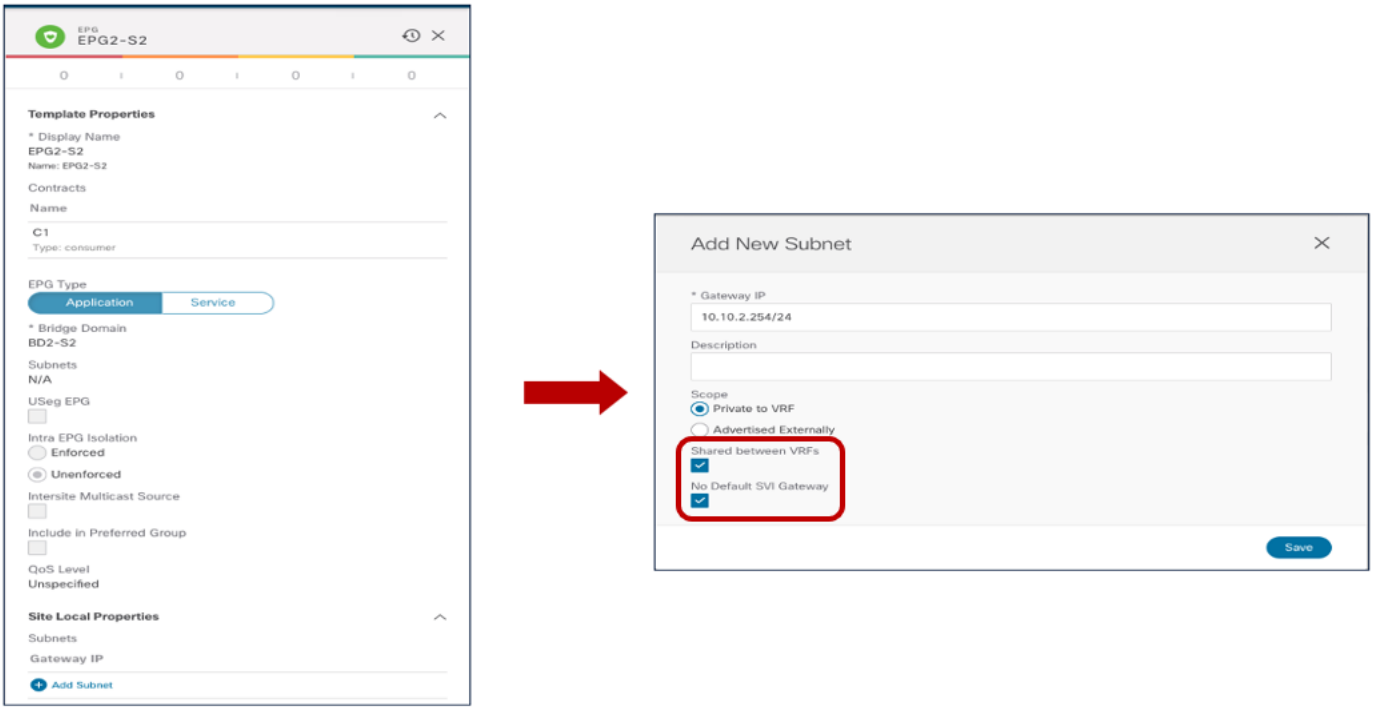


図 74.
プロバイダー EPG でのプレフィックスの設定

共有サービスのサイト間通信の確認

次の図 75 は、共有サービスの使用例でプロビジョニングしたシナリオを示しています。

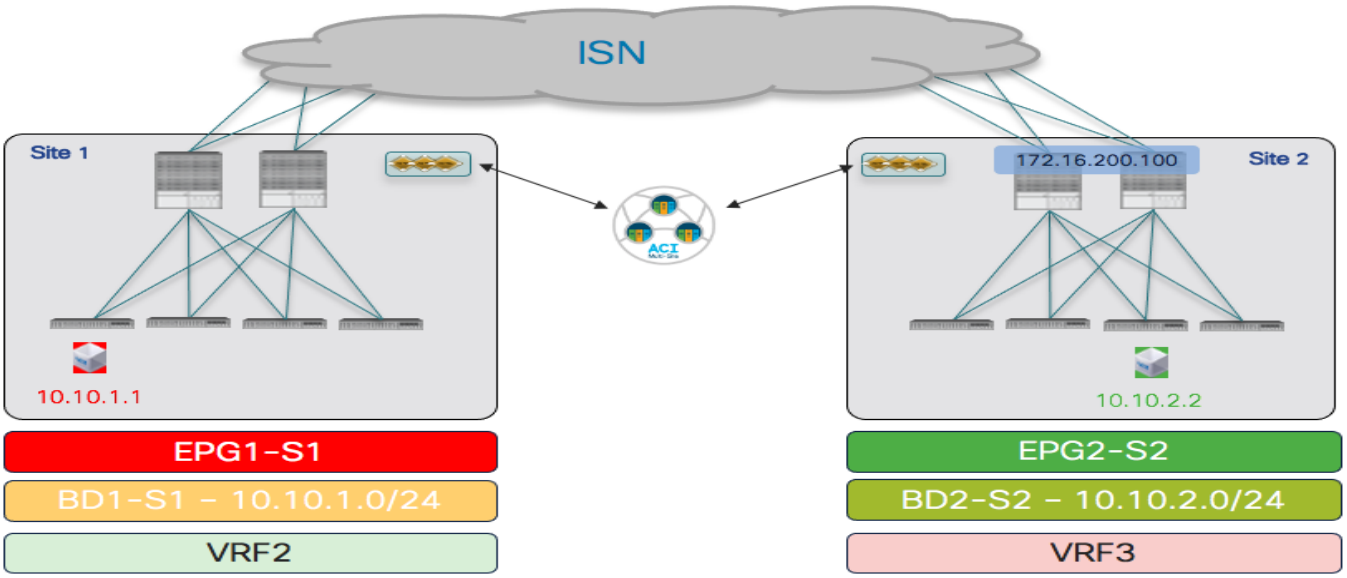


図 75.
個別の VRF のローカル EPG に接続されたエンドポイント（共有サービスの使用例）

各サイトでローカルに定義された EPG と異なる VRF の一部との間でコントラクトを適用すると、反対側のサイトでシャドウ オブジェクトの作成が生成されます。EPG と BD に加えて、VRF もシャドウ オブジェクトとしてインスタンス化されます。

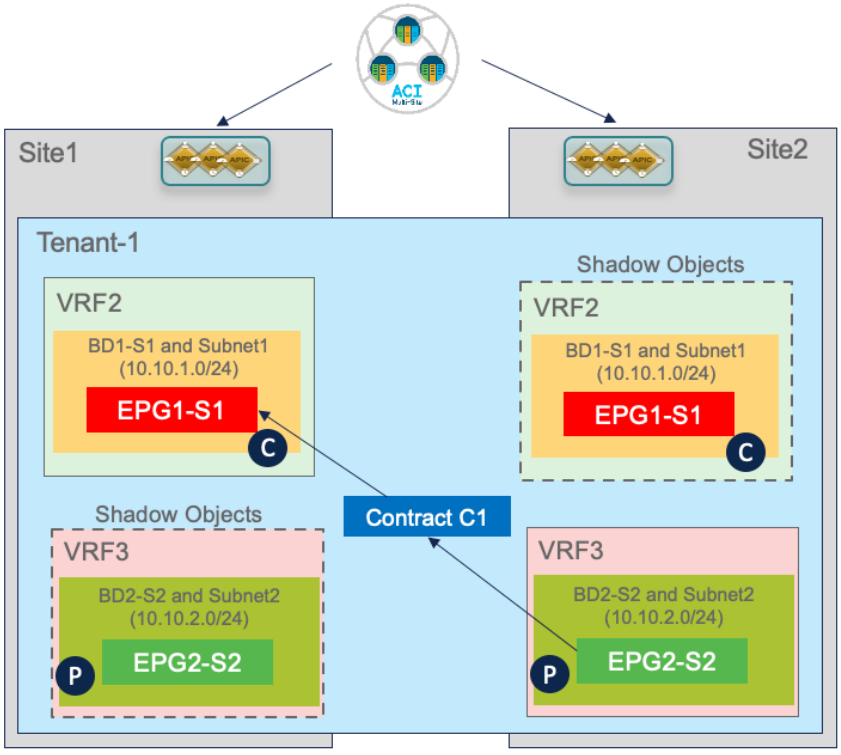


図 76.
共有サービスの使用例のシャドウ オブジェクトの作成

これは、通常どおり APIC とスパインで確認できます。シャドウ オブジェクトを表示し、スパインの変換テーブルで設定された値を取得する方法の詳細については、前のセクションを参照してください。次の図 77 と図 78 は、各 APIC ドメインのローカル オブジェクトとシャドウ オブジェクトに関連付けられたセグメント ID とクラス ID を示しています。

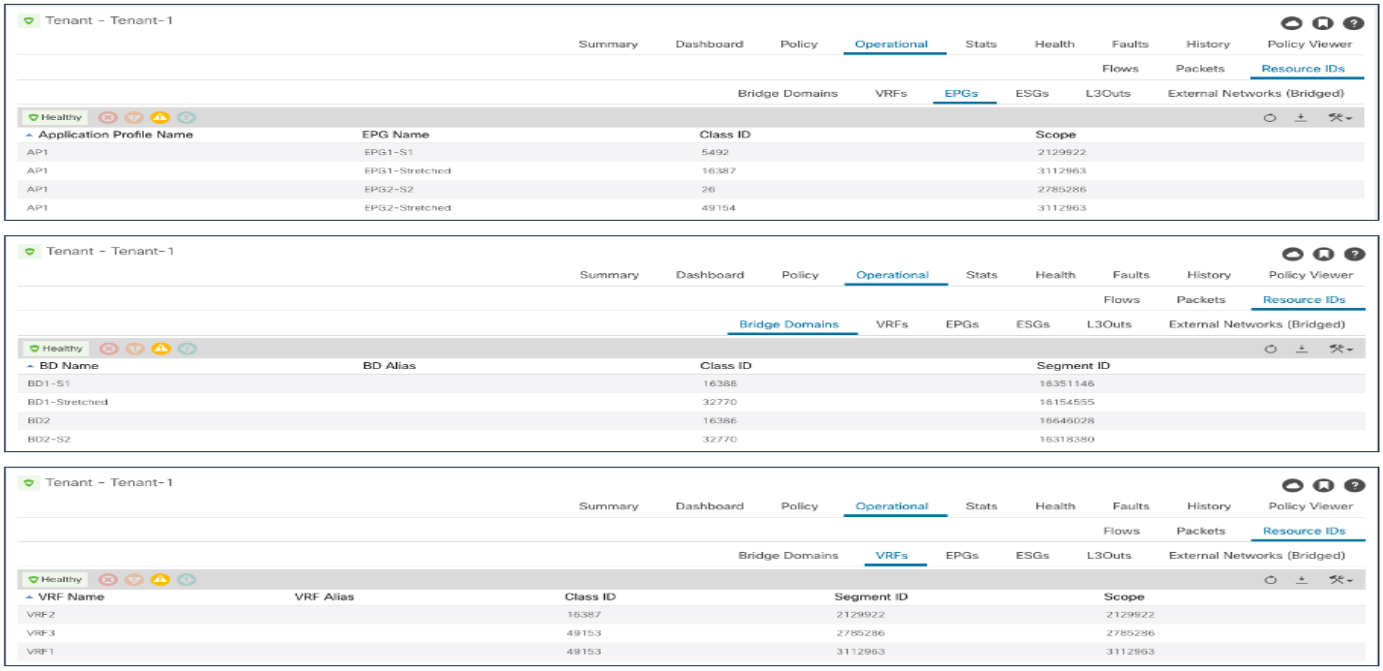


図 77.
Site1 のローカルおよび シャドウ オブジェクトのセグメント ID とクラス ID

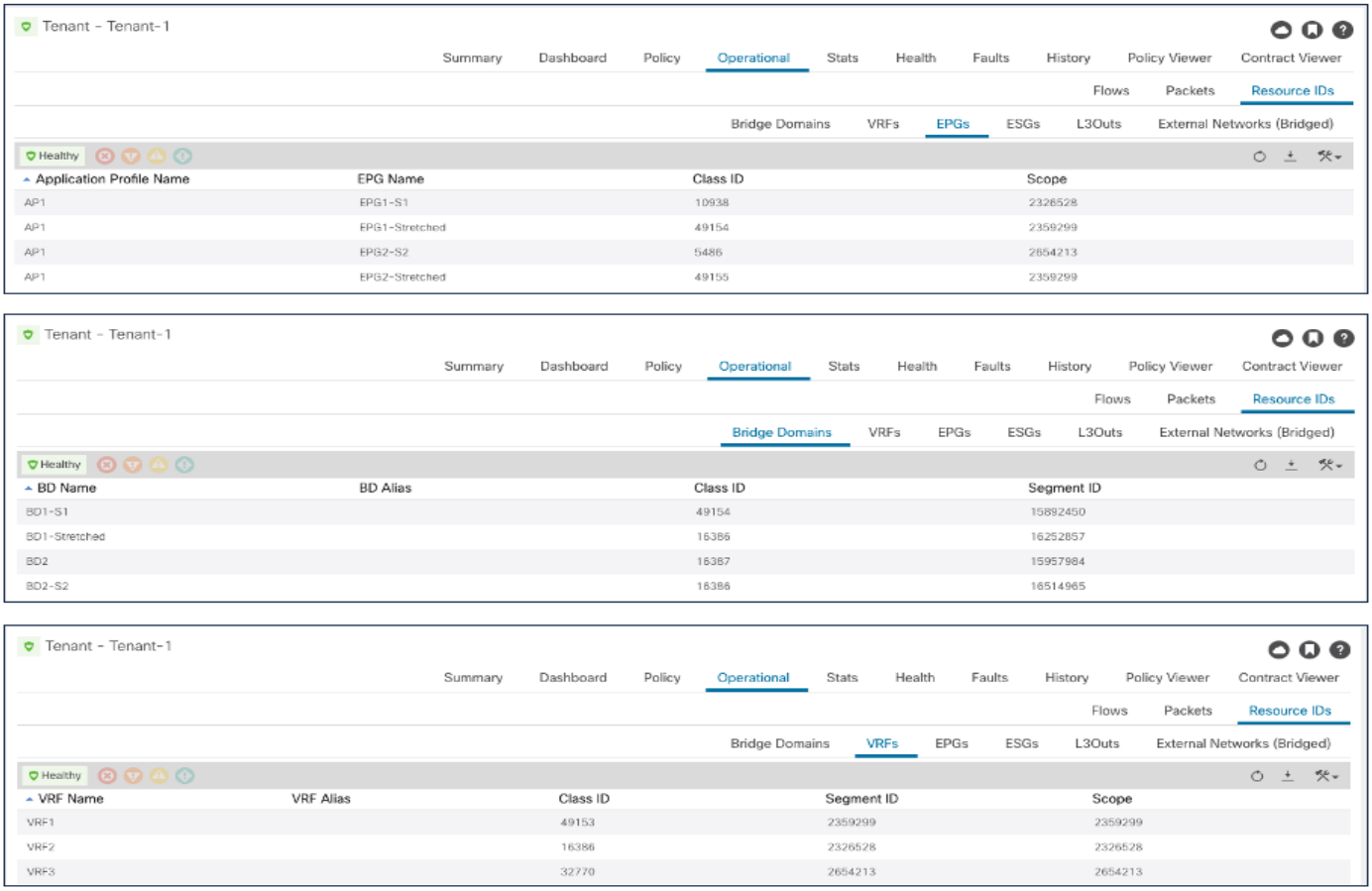


図 78.
Site2 のローカルおよびシャドウ オブジェクトのセグメント ID とクラス

プロバイダー EPG でのコントラクトと IP プレフィックス設定の作成の結果、BD1-S1 と BD2-S2 のサブネットが VRF 間でリークされます（次の出力を参照）。

Leaf 101 Site1

```
Leaf101-S1# show ip route vrf Tenant-1:VRF2
IP Route Table for VRF "Tenant-1:VRF2"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
*via 10.1.112.66%overlay-1, [1/0], 00:04:51, static, tag 4294967294
10.10.1.254/32, ubest/mbest: 1/0, attached, pervasive
* via 10.10.1.254、vlan13、[0/0]、00:08:31、local、local
10.10.2.0/24, ubest/mbest: 1/0, attached, direct, pervasive
*via 10.1.112.66%overlay-1, [1/0], 00:08:31, static, tag 4294967294, rwVnid: vxlan-2785286
```

Leaf 303 Site2

```
Leaf303-Site2# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF2"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
*via 10.1.112.66%overlay-1, [1/0], 00:08:31, static, tag 4294967294, rwVnid: vxlan-2785286
10.10.2.0/24, ubest/mbest: 1/0, attached, direct, pervasive
*via 10.0.136.66%overlay-1, [1/0], 00:35:33, static, tag 4294967294, rwVnid: vxlan-2654213
10.10.2.254/32, ubest/mbest: 1/0, attached, pervasive
*via 10.10.2.254, vlan33, [0/0], 00:06:47, local, local
```

上記の出力は、リークされた各ルートに、宛先へのトラフィックをカプセル化するときに使用されるセグメント ID の特定の情報がどのように含まれているかを示しています。Site1 では、vxlan-2785286 はローカル シャドウ VRF3 インスタンスに割り当てられたセグメント ID を表します。同様に、Site2 の Vxlan-2326528 は、ローカル シャドウ VRF2 インスタンスに割り当てられたセグメント ID を表します。リモート接続先が接続されている VRF のセグメント ID を使用して入力リーフのトラフィックをカプセル化すると、リモート サイトの受信リーフが正しいルーティング ドメインで適切にルックアップを実行できるようになります。

セキュリティ ポリシーが常に安定した状態で入力リーフ ノードに適用される VRF 内使用例とは異なり、共有サービス シナリオでは、セキュリティ ポリシーが常にコンシューマー リーフ ノードに適用される必要があります。これは、多くのコンシューマー EPG が共通の共有リソースにアクセスしようとすると、プロバイダー リーフの TCAM プログラミングのスケーラビリティの問題を回避するために行われます。

これを確実にするために、次の 2 つのことが行われています。

- エンドポイント情報のデータ プレーン学習は行われません。これは、プロバイダー リーフでのポリシーの適用を引き起こすクラス ID 情報の学習を回避するためです。
- プロバイダー EPG のクラス ID は、前述のプロバイダー EPG での IP プレフィックス設定の結果として、すべてのコンシューマー リーフ ノードで静的にプログラムされます。図 75 に示す特定のシナリオでは、次のコマンドを使用して、10.10.2.0 /24 サブネットのクラス ID が Site1 のコンシューマー リーフに設定されていることを確認できます。

Leaf 101 Site1

```
Leaf101-Site1# moquery -d sys/ipv4/inst/dom-Tenant-1:VRF2/rt-[10.10.2.0/24]
Total Objects shown: 1

# ipv4.Route
prefix : 10.10.2.0/24
childAction :
ctrl : pervasive
descr :
dn : sys/ipv4/inst/dom-Tenant-1:VRF2/rt-[10.10.2.0/24]
```

```
flushCount : 1
lcOwn : local
modTs : 2020-11-13T22:14:20.696+00:00
monPolDn :
name :
nameAlias :
pcTag : 26
pref : 1
rn : rt-[10.10.2.0/24]
sharedConsCount : 0
status :
tag : 4294967294
trackId : 0
```

注： 前の図 77 に示すように、pcTag 26 は Site1 の APIC コントローラにインストールされたシャドウ EPG2-S2 のクラス ID を表します。

その結果、次のセキュリティ ルールが Site1 のコンシューマー リーフにインストールされ、ポリシーを適用できるようになります。

Leaf 101 Site1

```
Leaf101-Site1# show zoning-rule scope 2129922
+---------+--------+--------+----------+----------------+---------+---------+-------------+-
---------+------------------------+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+----------------+---------+---------+-------------+-
---------+------------------------+
| 4223 | 0 | 0 | implicit | uni-dir | enabled | 2129922 | | deny,log | any_any_any(21) |
| 4224 | 0 | 0 | implarp | uni-dir | enabled | 2129922 | | permit | any_any_filter(17) |
| 4225 | 0 | 15 | implicit | uni-dir | enabled | 2129922 | | deny,log | any_vrf_any_deny(22)
|
| 4228 | 0 | 16388 | implicit | uni-dir | enabled | 2129922 | | permit | any_dest_any(16) |
| 4206 | 32771 | 16390 | default | uni-dir-ignore | enabled | 2359299 | Tenant-1:C1 | permit
| src_dst_any(9) |
| 4226 | 26 | 0 | implicit | uni-dir | enabled | 2129922 | | deny,log |
shsrc_any_any_deny(12) |
| 4213 | 16397 | 26 | default | bi-dir | enabled | 2129922 | Tenant-1:C1 | permit |
src_dst_any(9) |
+---------+--------+--------+----------+----------------+---------+---------+-------------+-
---------+------------------------+
```

プロバイダー EPG が共有サービスの使用例（Site1 のこの例では 26）の特別なクラス ID を取得していることに注目してください。この値は、展開されたすべての VRF でグローバル一意性を持つプールから取得されます。これは、割り当てられたクラス ID が各 VRF でローカルに有効である VRF 内使用例とは異なります。

最後に、目標が異なるテナントの一部である VRF 間の通信を確立する場合にも、上記と同じ考慮事項（およびプロビジョニング手順）を適用できます（図 79）。

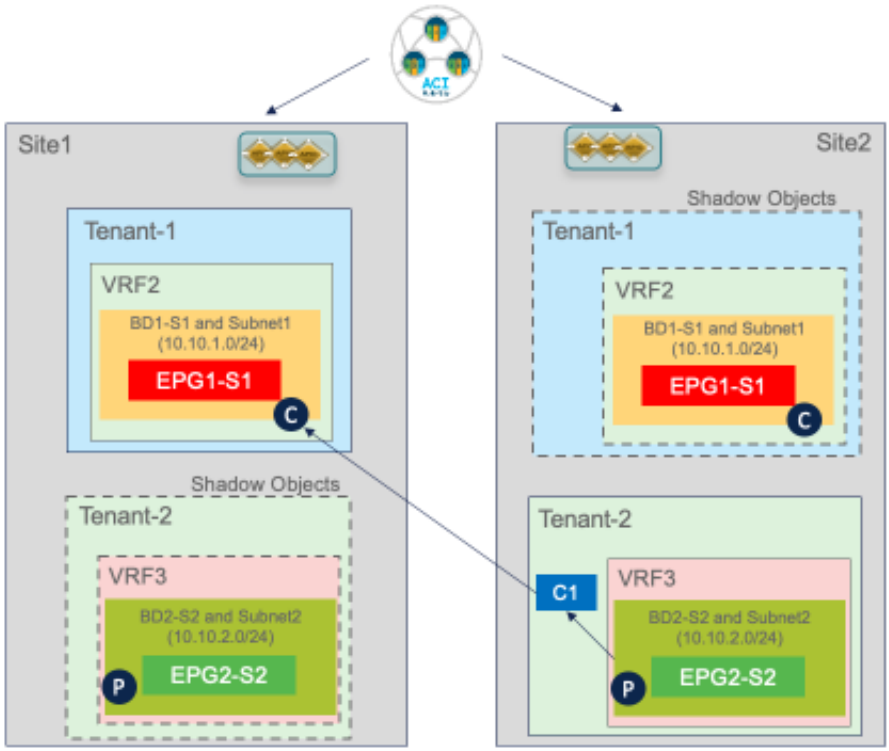


図 79.
テナント間共有サービスの使用例

展開モデルに適用される、唯一の固有の考慮事項は以下のとおりです。

- コントラクトは、「Global」の範囲でプロビジョニングされ、プロバイダー テナント（上記の例ではテナント 2）で定義されている必要があります。
- 別々の VRF とテナントの一部である EPG 間のコントラクトを作成すると、テナントが各サイトにローカルにのみ展開されるシナリオで「シャドウ テナント」のインスタンス化が発生します。

最後に、プロバイダーテナントで定義されたコントラクトは、「コントラクト インターフェイス」としてコンシューマー テナントにエクスポートする必要があります。ただし、これは、異なるテナントの一部である EPG 間にコントラクトが適用されると、Orchestrator サービスによって自動的に実行されます（そのため、プロビジョニングは Orchestrator の観点からは、図 76 に示す使用例と同じです）。

外部レイヤ 3 ドメインへの接続

前のセクションで説明した使用例では、同じ Multi-Site ドメインの一部である ACI サイト間でのレイヤ 2 およびレイヤ 3 接続の確立を扱いました。通常は「イーストウェスト」接続と呼ばれます。このセクションでは、外部のレイヤ 3 ネットワーク ドメインから DC リソースへのアクセスを提供する複数の使用例について説明します。これは一般に「サウス-ノース」接続と定義されています。

使用例1：外部リソースとの通信へのサイト ローカル L3Out 接続（Intra-VRF）

図 80 に示す最初の使用例では、各サイトに展開されたローカル L3Out 接続からの外部リソースの共通セットにアクセスします。

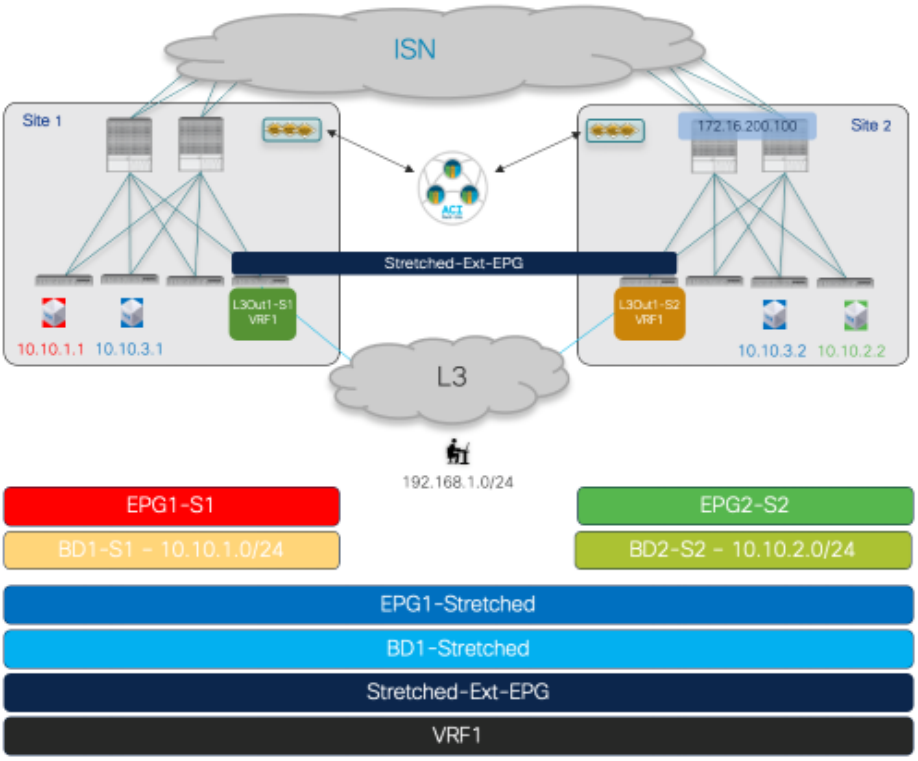


図 80.
外部リソースの共通セットへのアクセスを提供するサイトローカル L3Out

同じ VRF1 ルーティングドメインの一部である EPG および BD（サイトローカルオブジェクトとストレッチオブジェクトの混合）は、前述の使用例に合わせてすでにプロビジョニングされています。したがって、最初に必要な設定手順は、各ローカルサイトで L3Out を作成することです。図 81 は、ファブリック 1 で定義された L3Out1-S1 の Nexus Dashboard Orchestrator でこれを行う方法を示しています。同じことが、Site2 に関連付けられたテンプレートで L3Out1-S2 を定義するために実行できます。各サイトで L3Out を一意の名前で定義することをお勧めします。これにより、多くの使用例のプロビジョニングの柔軟性が向上します（以下のセクションで説明します）。

注： 図 80 に示す図は、各ファブリックで単一の BL ノードを使用しているため、通常、冗長性のために少なくとも 1 組の BL ノードを活用する実際の実稼働環境を表すものではありません。

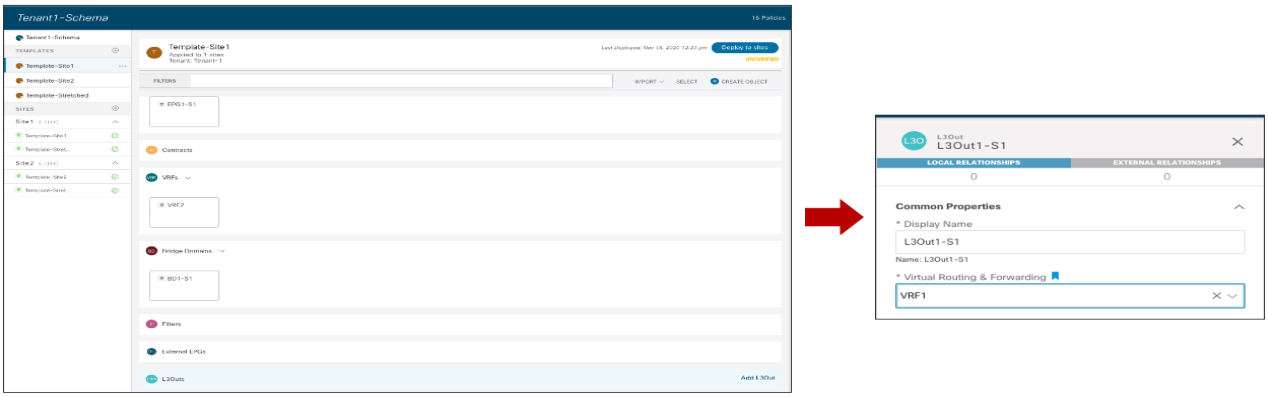


図 81.
Site1 でのローカル L3Out の作成

現在の Nexus Dashboard Orchestrator 3.5(1) リリースでは、NDO からのみ L3Out オブジェクトを作成できますが、論理ノード、論理インターフェイス、ルーティング プロトコルなどの設定は特定の APIC ドメイン レベルで処理されます。APIC で L3Out を作成する方法の詳細については、このペーパーの範囲外です。詳細については、以下のペーパーを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/guide-c07-743150.html

各サイトの L3Out がプロビジョニングされると、L3Out に関連付けられた外部 EPG の作成に進むことができます。ベスト プラクティスとして、L3Out 接続が外部リソースの共通セットへのアクセスを提供する場合は、単一の外部 EPG を導入する必要があります。次の図 82 に示す「拡張」外部 EPG を使用すると、ノースサウス接続の確立に必要なセキュリティ ポリシーの定義が簡素化されます。

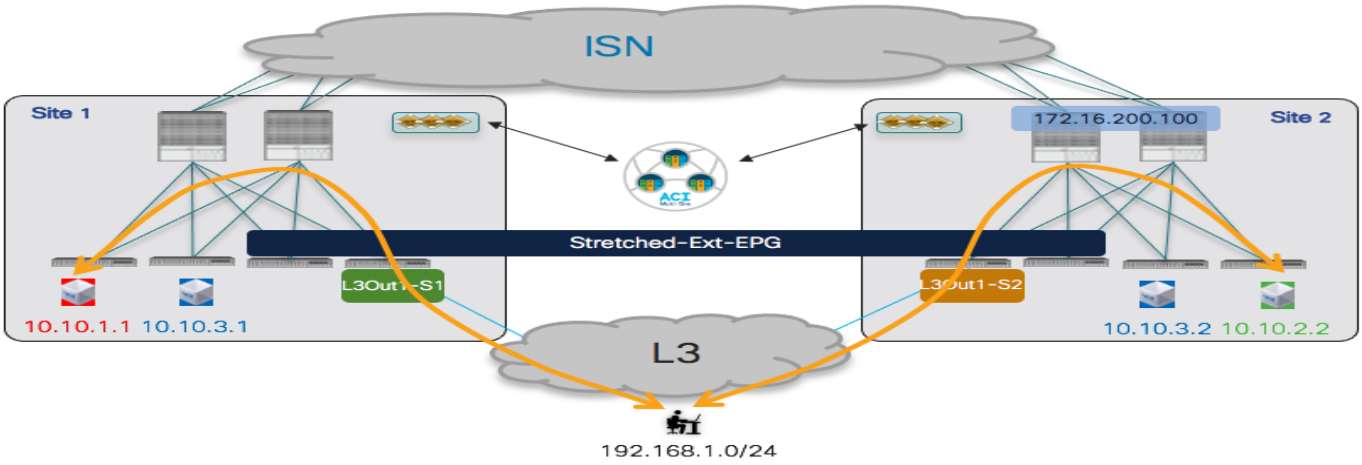


図 82.
「ストレッチ」外部 EPGの使用

同じ外部 EPG を両方のファブリックに展開する必要があるため、両方のサイトに関連付けられている Template-Stretched の一部として設定する必要があります。

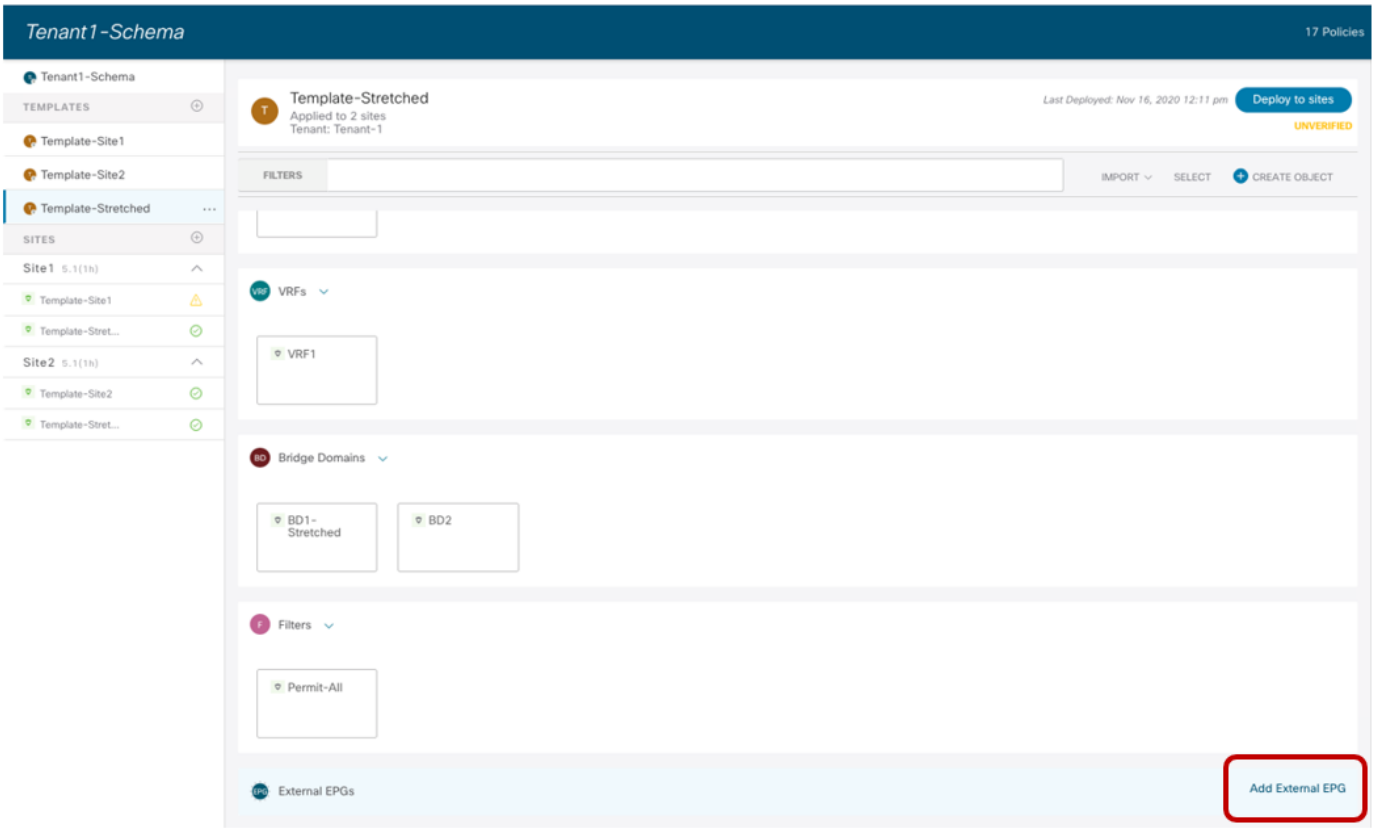


図 83.
「ストレッチ」外部 EPGの作成

外部 EPG には、EPG の一部として外部リソースを分類できるように 1 つ以上の IP プレフィックスが定義されている必要があります（内部 EPG でセキュリティ ポリシーを適用できるようにするため）。図 84 の例では、すべての外部リソースをこの特定の外部 EPG の一部として確実に分類できるように、「キャッチ-オール」0.0.0.0/0 プレフィックスを使用する一般的なアプローチが示されています。

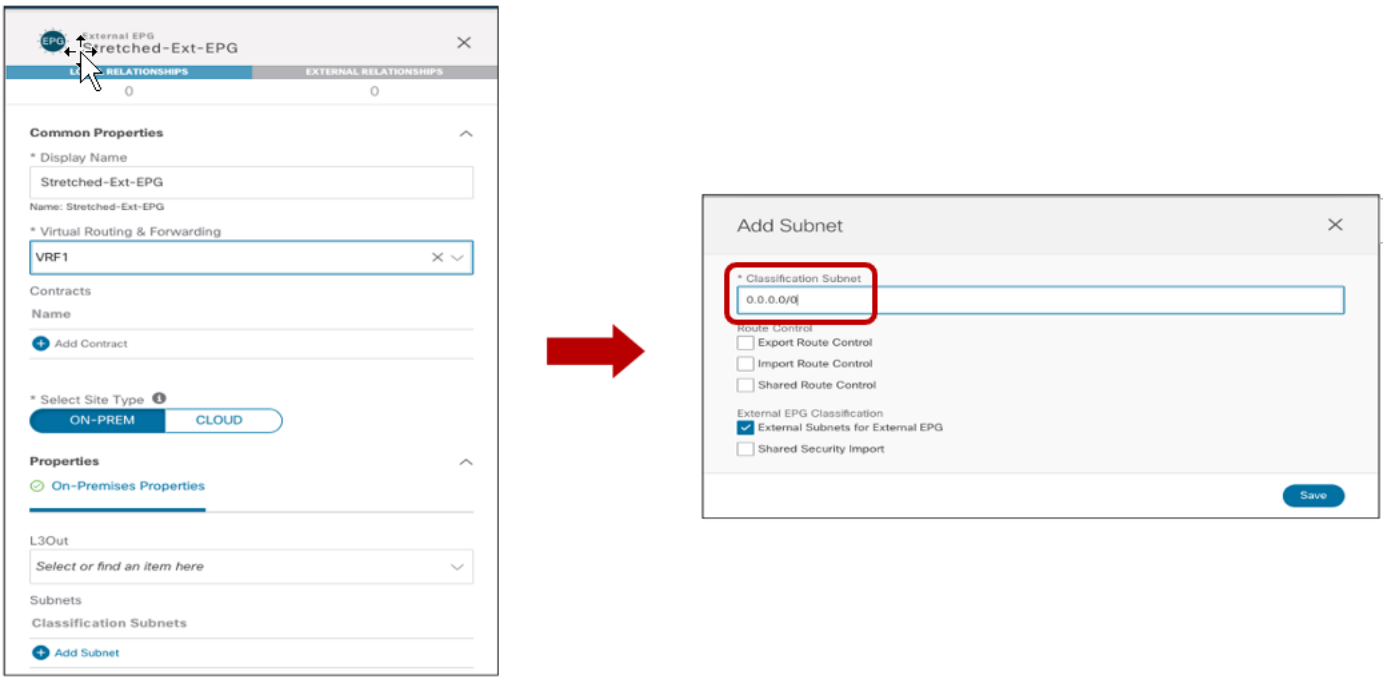


図 84.
「キャッチ-オール」分類サブネットの定義

外部 EPG を定義したら、それをサイト レベルで、各ファブリックに対して以前に定義したローカル L3Out オブジェクトにマッピングする必要があります。図 85 に、Site1 で定義された L3Out への Ext-EPG の関連付けを示します。同様のマッピングが Site2 の L3Out にも必要です。

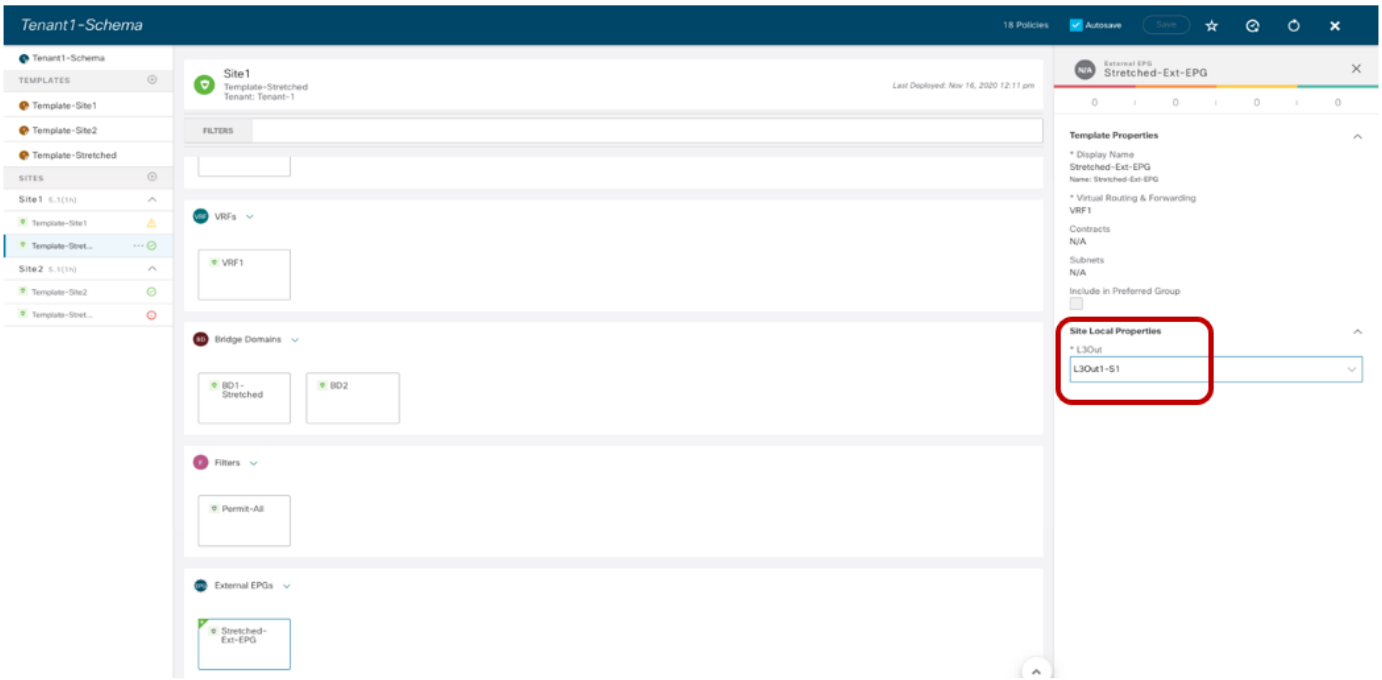


図 85.
外部 EPG のローカル L3Out 接続へのマッピング

注： NDO GUI には、グローバルテンプレート レベルで外部 EPG を L3Out にマッピングする機能もあります。ただし、この使用例で説明したシナリオでは、各ファブリックで個別の L3Out 接続が作成されるため、サイト レベルでマッピングを作成する必要があります。

外部 EPG がプロビジョニングされ、ローカル L3Out にマッピングされたら、図 82 に示すように、NS 接続を確立するために 2 つの最終手順が必要です。

- 内部 EPG と外部 EPG 間のセキュリティ ポリシーを確立します。これは、VRF 内 EPG から EPG への接続に以前使用したものと同じコントラクト C1 を使用できます。コントラクトの方向に関係するものについては、Ext-EPG がコントラクトを提供し、内部 EPG がコントラクトを使用しているかどうか、またはその逆の場合は関係ありません。

  また、優先グループまたは vzAny 機能を使用して、コントラクトを適用する代わりに、無料のノースサウス接続を許可することもできます。Ext-EPG に優先グループを使用する場合は、特定の考慮事項が適用されます。この場合、外部ソースから発信されたすべてのトラフィックを分類するために 0.0.0.0/0 はサポートされません。同じアドレス空間をカバーするための推奨設定は、図 86 に示すように、範囲を 2 つの部分に分割することです。

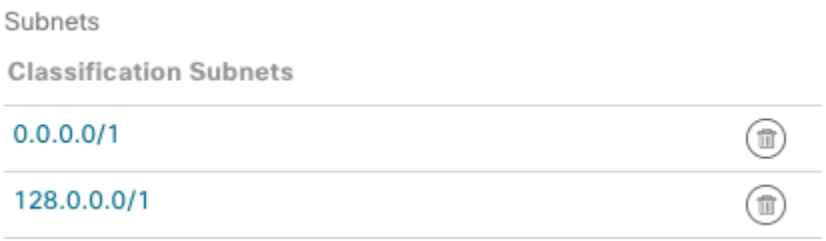


図 86.
外部 EPG を優先グループに追加する場合の分類サブネット

- 内部 BD サブネットを外部ネットワーク ドメインに向けてアナウンスします。これを実現するには、まず、図 87 に示すように、BD に関連付けられた IP サブネットに「外部アトバタイズ (Advertised Externally)」フラグを設定する必要があります。

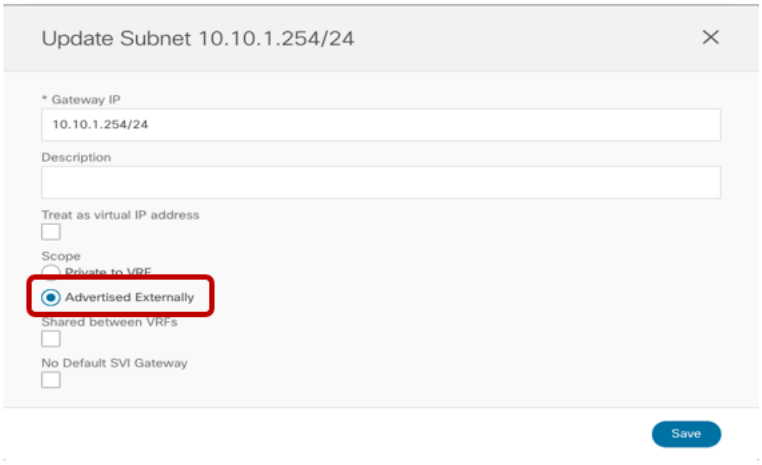


図 87.
BD サブネットを外部ネットワークに向けてアナウンスするには、「外部アトバタイズ (Advertised Externally)」フラグを設定します。

2 番目のステップとして、どの L3Out から BD サブネットプレフィックスをアドバタイズするかを指定する必要があります。これは通常、Nexus Dashboard Orchestrator でサイト レベルで BD にL3Out を関連付けることによって実現されます。図 88 に、Site1 にローカルに展開された BD1-S1 に必要な設定を示します。サイトにまたがる BD の場合は、代わりに BD を各サイトでローカルに定義された L3Out にマッピングする必要があります。

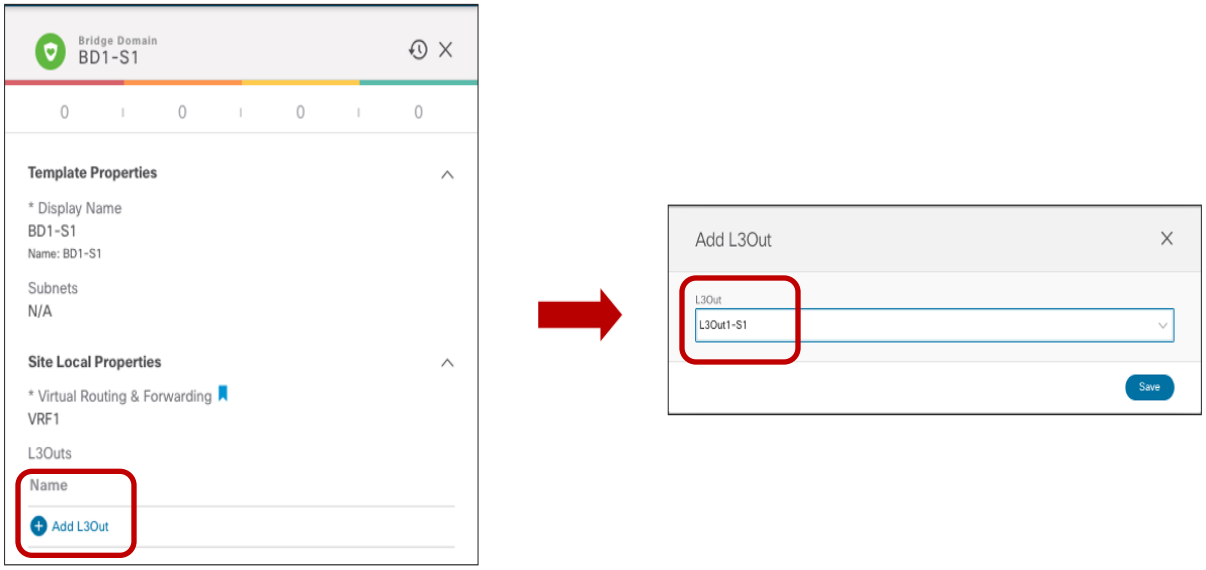


図 88.
BD への L3Out のマッピング

注： 各サイトで一意の名前の L3Out 接続を使用することは、上の図で実行されたマッピングに基づいて BD のサブネットを通知する場所を厳密に制御するために非常に重要です。

ユース ケース 1 確認

前述の設定を完全にプロビジョニングすると、ノースサウス接続を正常に確立できます。内部 EPG が拡張外部 EPG とセキュリティ コントラクトを確立する場合でも（前述の図 82 を参照）、VRF 内シナリオでは、各サイトでローカルに定義された IP サブネットのプレフィックス情報のみがローカル L3Out 接続に送信されます。これにより、着信トラフィックは常に、サブネットがローカルに定義されているファブリックに向けられます。ストレッチされた BD の場合、ストレッチされた IP サブネットは両方のサイトで定義された L3Outs からデフォルトでアドバタイズされます。つまり、着信トラフィックは「間違った」サイトで受信される可能性があり、ISN 全体での再ルーティングが必要になります。（図 89）。

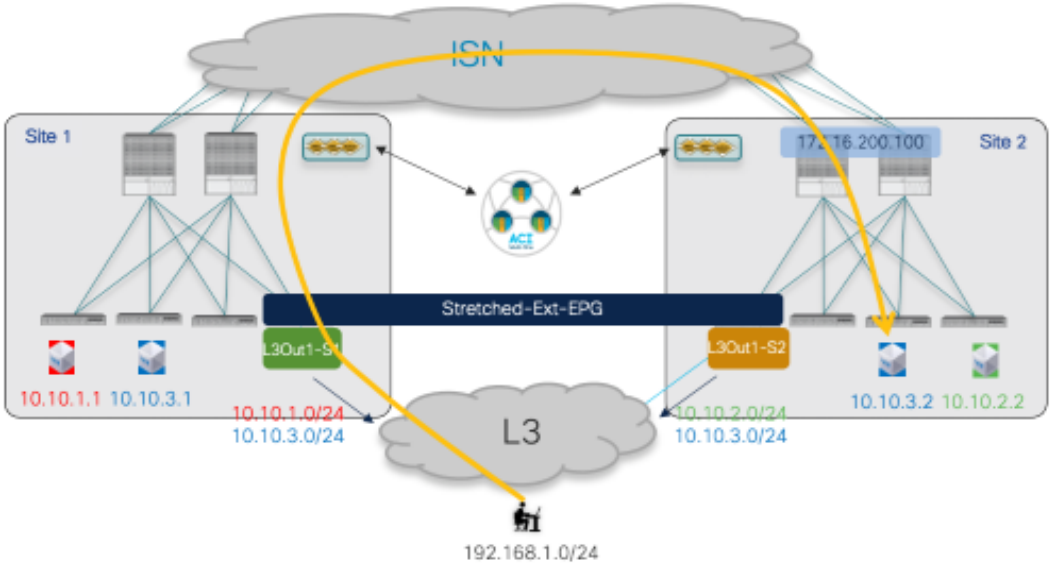


図 89.
準最適な着信トラフィック パス

ストレッチ EPG/BD に属するエンドポイントを宛先とする着信トラフィック フローは、ホストベースのルーティング機能を設定することで最適化できます。これにより、ローカル サイトで検出されたエンドポイントの特定の /32 プレフィックスを各 L3Out からアドバタイズできます。

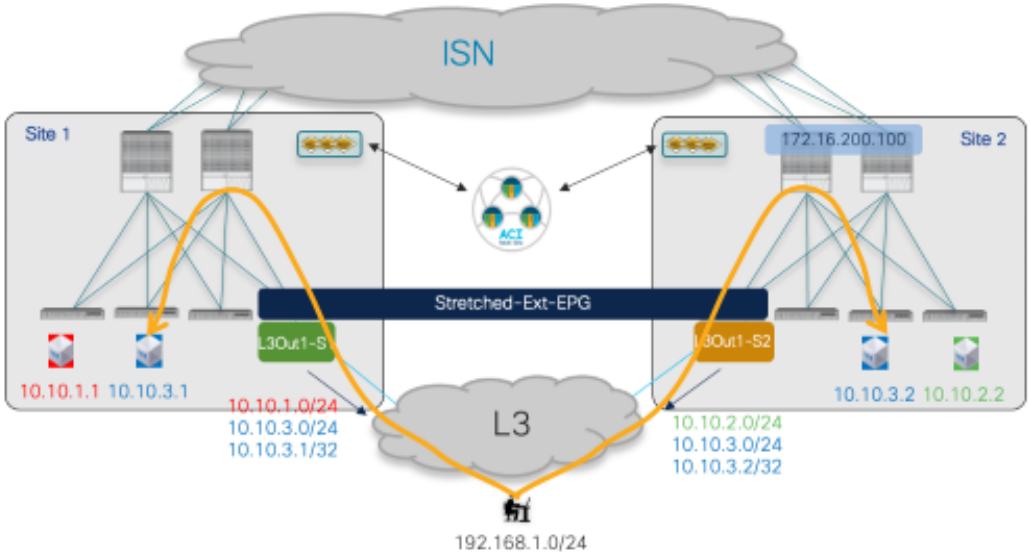


図 90.
着信トラフィック最適化のためのホストベース ルーティング アドバタイズメント

ホストベースのルーティング情報のアドバタイズメントは、各 BD の NDO で有効にできます。また、サイト全体に拡張された BD に対してのみアドバタイズする必要があります。図 91 で強調表示されているように、「ホスト ルート (Host Route)」フラグは BD1-Stretched に対して有効になっており、これはサイト レベルで実行されます。

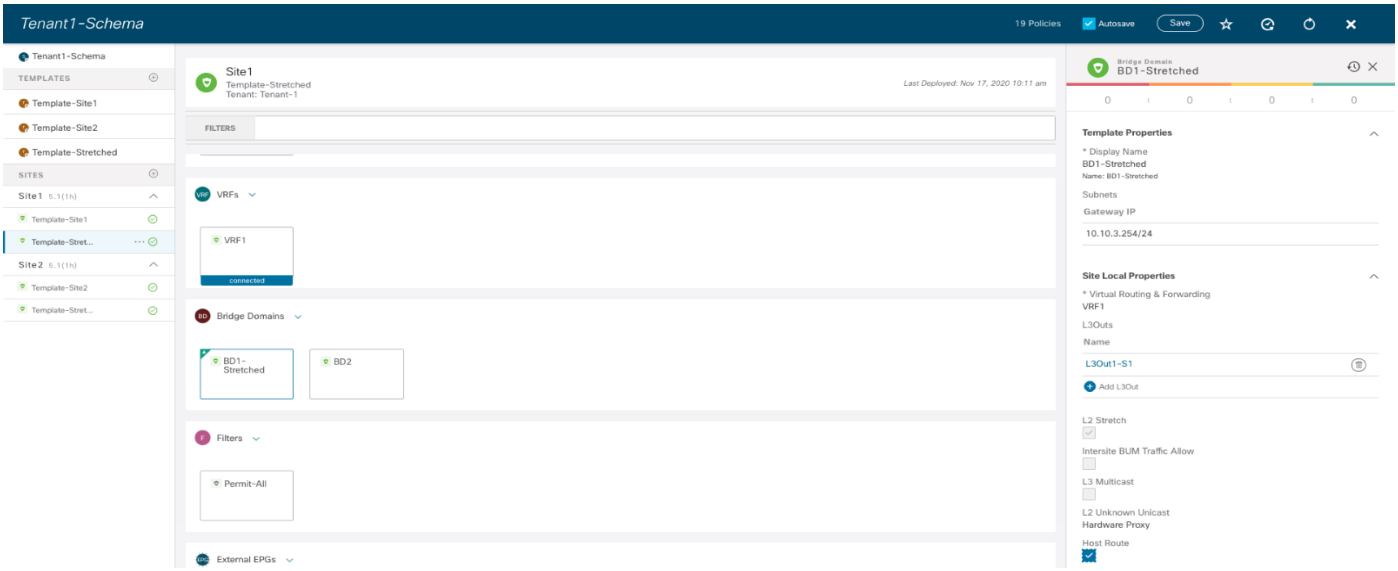


図 91.
NDO でのホストベース ルーティングの有効化

発信トラフィック フローに関係するものについては、各ファブリックのコンピューティング リーフ ノードの観点から、外部 IP プレフィックス 192.168.1.0/24 への唯一のパスは、常にローカル ボーダー リーフ（BL）ノードを経由します。これは、Site1 の L3Out 接続で学習された外部プレフィックスが、Site2 に MP-BGP コントロール プレーンを使用してデフォルトでSite2 にアドバタイズされないためです（サイト間 L3Out 機能が有効になっていない場合）（これについては、詳細については、「サイト間 L3Out の導入」のセクションを参照してください）。

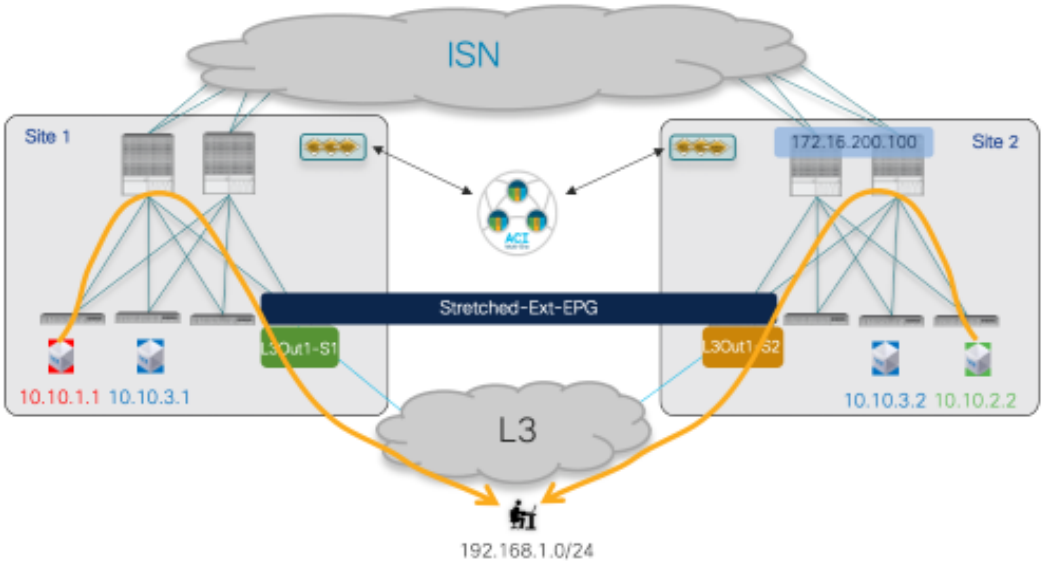


図 92.
常にローカル L3Out を使用するアウトバウンド通信

次の出力では、10.1.0.69 は Site1 の ボーダー リーフ ノードの TEP アドレスを表し、10.0.224.96 は Site2 の ボーダー リーフ ノードの TEP アドレスです。

```
Leaf 101 Site1
```

```
Leaf101-Site1# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
*via 10.1.112.66%overlay-1, [1/0], 00:04:51, static, tag 4294967294
10.10.1.254/32, ubest/mbest: 1/0, attached, pervasive
*via 10.10.1.254, vlan43, [0/0], 03:04:11, local, local
10.10.2.0/24, ubest/mbest: 1/0, attached, direct, pervasive
*via 10.1.112.66%overlay-1, [1/0], 00:46:04, static
10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
*via 10.1.112.66%overlay-1, [1/0], 00:47:38, static
10.10.1.254/32, ubest/mbest: 1/0, attached, pervasive
*via 10.10.1.254, vlan43, [0/0], 03:04:11, local, local
192.168.1.0/24, ubest/mbest: 1/0
*via 10.1.0.69%overlay-1, [200/0], 03:02:43, bgp-65501, internal, tag 3
```

Leaf 303 Site2

```
Leaf303-Site2# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.2.0/24, ubest/mbest: 1/0, attached, direct, pervasive
*via 10.0.136.66%overlay-1, [1/0], 02:03:12, static
10.10.2.254/32, ubest/mbest: 1/0, attached, pervasive
*via 10.10.2.254, vlan16, [0/0], 04:21:10, local, local
10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
*via 10.0.136.66%overlay-1, [1/0], 02:03:12, static
10.10.3.254/32, ubest/mbest: 1/0, attached, pervasive
*via 10.10.1.254, vlan43, [0/0], 03:04:11, local, local
192.168.1.0/24, ubest/mbest: 1/0
*via 10.0.224.96%overlay-1, [200/0], 00:19:39, bgp-100, internal, tag 30
```

セキュリティ ポリシーの観点から（優先グループが使用されていない場合）、VRF 内のノースサウス トラフィック フローでは、コントラクト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ます（境界リーフ ノードには適用されません）。これは、コントラクトの方向（つまり、誰がプロバイダーで誰がコンシューマー

か）とは無関係に当てはまりますが、これはVRF の「ポリシー制御適用方向 (Policy Control Enforcement Direction)」は常にデフォルトの「入力 (Ingress)」値に維持されるということを前提としています。

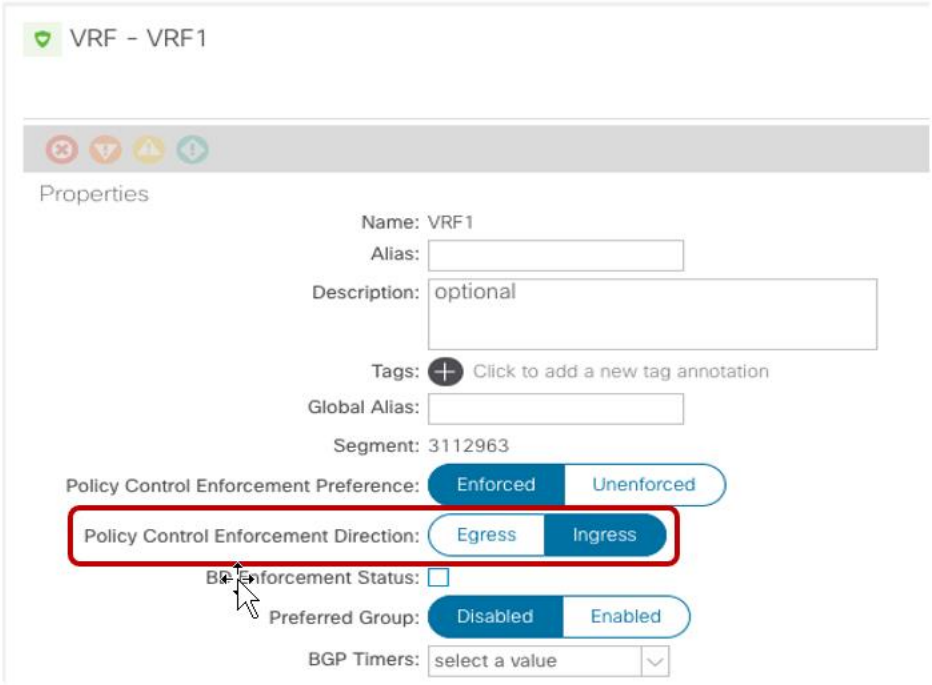


図 93.
デフォルト VRF の設定

注： サービス グラフとPBR をノースサウス トラフィック フローに適用できるようにするため、この設定をデフォルト値のままにすることを強く推奨します。詳細については、「ACI Multi-Siteとのサービス ノード統合」セクションを参照してください。

次の出力は、Site1 の ボーダー リーフ ノードのゾーン分割ルール設定を示しています。16388 は内部 EPG1-S1 のクラス ID を表し、49153は vRF1 のクラス ID です。分類のために 0.0.0.0/0 プレフィックスを使用して設定された外部 EPG を持つ L3Out でトラフィックを受信すると、外部 EPG の特定のクラス ID の代わりに、（L3Out の）VRF のクラス ID が割り当てられます（このセクションで後述するように、外部 EPG については、より具体的な分類サブネットを使用します）。したがって、次の表の最後のエントリ（ルール ID 4225）を確認すると、着信トラフィックのセキュリティ ポリシーを境界リーフ ノード104 に適用できると結論付けることができます。

Leaf 104 Site1

```
Leaf104-Site1# show zoning-rule scope 3112963
+---------+--------+--------+----------+---------+---------+---------+------------+--------
--+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+---------+---------+---------+------------+--------
--+----------------------+
| 4148 | 0 | 0 | implicit | uni-dir | enabled | 3112963 | | deny,log | any_any_any(21) |
| 4153 | 0 | 0 | implarp | uni-dir | enabled | 3112963 | | permit | any_any_filter(17) |
| 4199 | 0 | 15 | implicit | uni-dir | enabled | 3112963 | | deny,log | any_vrf_any_deny(22)
|
```

```
| 4156 | 0 | 16386 | implicit | uni-dir | enabled | 3112963 | | permit | any_dest_any(16) |
| 4206 | 0 | 32770 | implicit | uni-dir | enabled | 3112963 | | permit | any_dest_any(16) |
| 4216 | 0 | 32771 | implicit | uni-dir | enabled | 3112963 | | permit | any_dest_any(16) |
| 4213 | 16387 | 15 | default | uni-dir | enabled | 3112963 | Tenant-1:C1 | permit |
src_dst_any(9) |
| 4218 | 49153 | 16387 | default | uni-dir | enabled | 3112963 | Tenant-1:C1 | permit |
src_dst_any(9) |
| 4145 | 16388 | 15 | default | uni-dir | enabled | 3112963 | Tenant-1:C1 | permit |
src_dst_any(9) |
| 4225 | 49153 | 16388 | default | uni-dir | enabled | 3112963 | Tenant-1:C1 | permit |
src_dst_any(9) |
+---------+--------+--------+----------+---------+---------+---------+-------------+--------
--+----------------------+
```

これはこの場合には正しくありません。リーフ 104 は外部発信トラフィック フローの宛先のクラス ID（この例では EPG1-S1 の内部エンドポイント部分を表す10.10.1.1）を決定する方法を認識していないからです。これは、ノースサウス通信を行っても、内部エンドポイント情報がBL ノードで学習されないためです。さらに、EPG1-S1（10.10.1.0/24）に関連付けられた特定の IP サブネットも、特定のクラス ID 情報なしでローカルにインストールされます（「pcTag」行の「any」値を参照）。

Leaf 104 Site1

```
Leaf104-Site1# moquery -d sys/ipv4/inst/dom-Tenant-1:VRF1/rt-[10.10.1.0/24]
Total Objects shown: 1


# ipv4.Route
prefix : 10.10.1.0/24
childAction :
ctrl : pervasive
descr :
dn : sys/ipv4/inst/dom-Tenant-1:VRF2/rt-[10.10.2.0/24]
flushCount : 0
lcOwn : local
modTs : 2020-11-16T20:24:29.023+00:00
monPolDn :
name :
nameAlias :
pcTag : any
pref : 1
rn : rt-[10.10.2.0/24]
sharedConsCount : 0
status :
tag : 0
trackId : 0
```

次の出力は、内部エンドポイント 10.10.1.1 が接続されているコンピューティング リーフ上のゾーン分割ルール エントリを示しています。これにより、外部クライアント 192.168.1.1 を使用した着信および発信フローのセキュリティ ポリシーを適用できます。

Leaf 101 Site1

```
Leaf101-Site1# show zoning-rule scope 3112963
+---------+--------+--------+----------+---------+---------+---------+------------+----------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir     | operSt  | Scope   | Name       | Action   | Priority             |
+---------+--------+--------+----------+---------+---------+---------+------------+----------+----------------------+
| 4151    | 0      | 0      | implicit | uni-dir | enabled | 3112963 |            | deny,log | any_any_any(21)      |
| 4200    | 0      | 0      | implarp  | uni-dir | enabled | 3112963 |            | permit   | any_any_filter(17)   |
| 4198    | 0      | 15     | implicit | uni-dir | enabled | 3112963 |            | deny,log | any_vrf_any_deny(22) |
| 4203    | 0      | 32770  | implicit | uni-dir | enabled | 3112963 |            | permit   | any_dest_any(16)     |
| 4228    | 0      | 32771  | implicit | uni-dir | enabled | 3112963 |            | permit   | any_dest_any(16)     |
| 4210    | 16387  | 15     | default  | uni-dir | enabled | 3112963 | Tenant-1:C1 | permit   | src_dst_any(9)       |
| 4199    | 49153  | 16387  | default  | uni-dir | enabled | 3112963 | Tenant-1:C1 | permit   | src_dst_any(9)       |
| 4224    | 16388  | 15     | default  | uni-dir | enabled | 3112963 | Tenant-1:C1 | permit   | src_dst_any(9)       |
| 4223    | 49153  | 16388  | default  | uni-dir | enabled | 3112963 | Tenant-1:C1 | permit   | src_dst_any(9)       |
+---------+--------+--------+----------+---------+---------+---------+------------+----------+----------------------+
```

着信フローの場合、パケットは vXLAN ヘッダー（49153）で VRF クラス ID を伝送するため、上記のルール 4223 では、EPG1-S1 のローカルに接続されたエンドポイント部分（クラス ID 16388 で識別される）にポリシーを適用できます。発信フローの場合は、エントリ 4224 が適用されます。これは、分類に 0.0.0.0/0 を使用する外部 EPG を介して到達可能なすべての外部宛先が、特定のクラス ID 値 15 で識別されるためです。同じエントリがボーダー リーフ ノードでも使用できますが、発信フローには影響を及ぼしません。コンピューティング ノードがボーダー リーフ ノードに送信されるパケットの VXLAN ヘッダーに特定のビットを設定して、ポリシーがすでに適用されたことを示すからです。

代わりに、外部 EPG の 0.0.0.0/0 分類サブネットが、より具体的なエントリ（具体例では外部クライアントのサブネットと一致する 192.168.1.0/24）に置き換えられた場合、次の出力に示すように、コンピューティング リーフ ノードのゾーニング テーブルが変更されます。この場合、特定のルール ID 4194 および 4219 により、EPG1-S1（クラス ID 16388）と外部 EPG（クラス ID 32773）間の着信および発信信の通信にセキュリティ ポリシーを適用できます。

Leaf 101 Site1

```
Leaf101-Site1# show zoning-rule scope 3112963
+ --------- + -------- + -------- + ---------- + ---------- ------ + --------- + --------- + ------------ + --------- -+ ---------------------- +
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+---------------+---------+---------+------------+----------+----------------------+
```

```
| 4151 | 0 | 0 | implicit | uni-dir | enabled | 3112963 | | deny,log | any_any_any(21) |
| 4200 | 0 | 0 | implarp | uni-dir | enabled | 3112963 | | permit | any_any_filter (17) |
| 4198 | 0 | 15 | implicit | uni-dir | enabled | 3112963 | | deny,log | any_vrf_any_deny(22)
|
| 4203 | 0 | 32770 | implicit | uni-dir | enabled | 3112963 | | permit | any_dest_any(16) |
| 4228 | 0 | 32771 | implicit | uni-dir | enabled | 3112963 | | permit | any_dest_any(16) |
| 4219 | 16388 | 32773 | default | uni-dir-ignore | enabled | 3112963 | Tenant-1:C1 | permit
| src_dst_any(9) |
| 4194 | 32773 | 16388 | default | bi-dir | enabled | 3112963 | Tenant-1:C1 | permit |
src_dst_any(9) |
| 4225 | 16387 | 32773 | default | uni-dir-ignore | enabled | 3112963 | Tenant-1:C1 | permit
| src_dst_any(9) |
| 4217 | 32773 | 16387 | default | bi-dir | enabled | 3112963 | Tenant-1:C1 | permit |
src_dst_any(9) |
+---------+--------+--------+----------+----------------+---------+---------+-------------+-
---------+----------------------+
```

使用例 2：外部リソースとの通信に対するサイトローカル L3Out 接続（同じテナント内の VRF 間/共有サービス）

考慮すべき 2 番目の使用例は、L3Out 接続が内部 EPG/BD とは異なる VRF の一部であり、通常「共有サービス」と呼ばれるシナリオです。この使用例では、L3Out VRF（VRF 共有）は、内部 EPG/BD が属する同じテナントで定義されます。

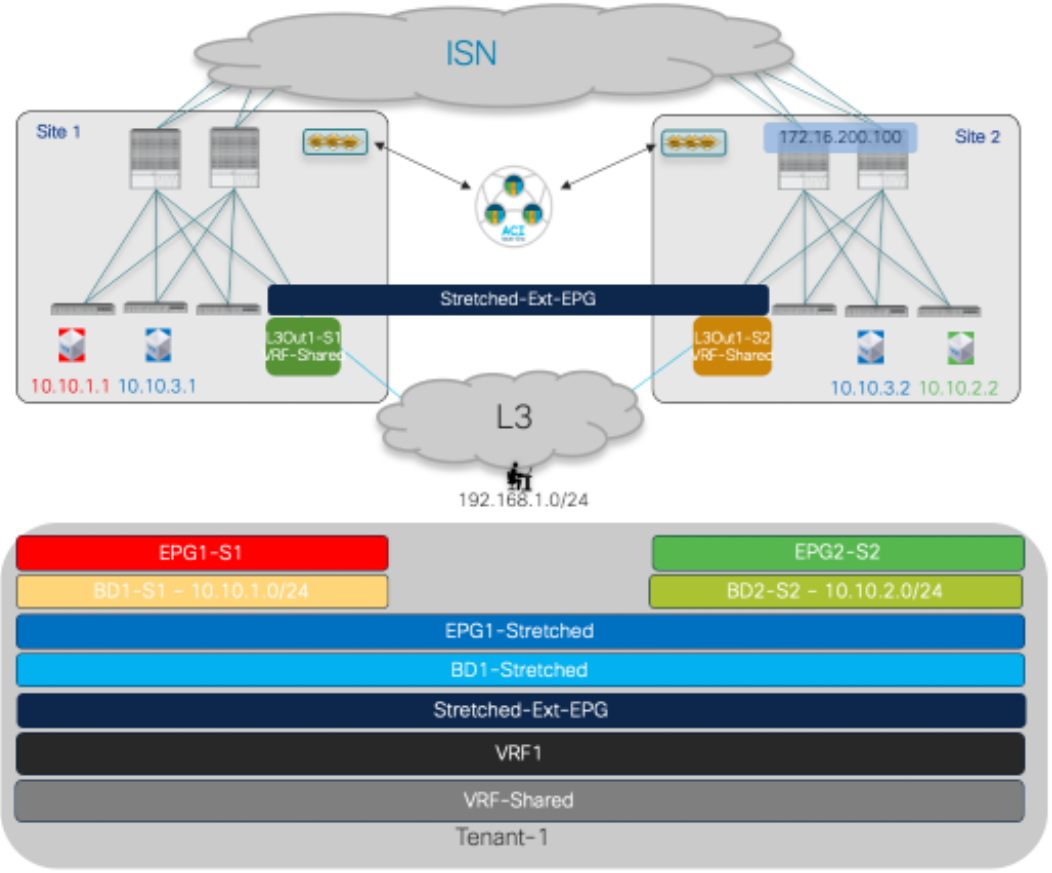


図 94.
VRF 間のノースサウス接続

前述の VRF 内の使用例と異なる唯一のプロビジョニング手順は次のとおりです。

- スコープ「Tenant」でコントラクトを設定します。
- 内部 EPG と外部 EPG 間のコントラクトを適用します。VRF 内使用例1 とは異なり、セキュリティ ポリシーが適用されるリーフ ノードは、「使用例」で説明されているように、特定のプロバイダー側とコンシューマー側に依存します。「使用例 2 検証」セクションを参照してください。
- ローカル L3Out の外部にアドバタイズできるように内部 BD サブネットを設定します。VRF 全体でこれを行うには、BD を L3Out にマッピングする必要はありません（「VRF 内」の使用例のように）。「外部アトバタイズ (Advertised Externally)」に加えて「VRF 間共有 (Shared between VRFs)」フラグを選択するだけです。図 95 を参照してください。

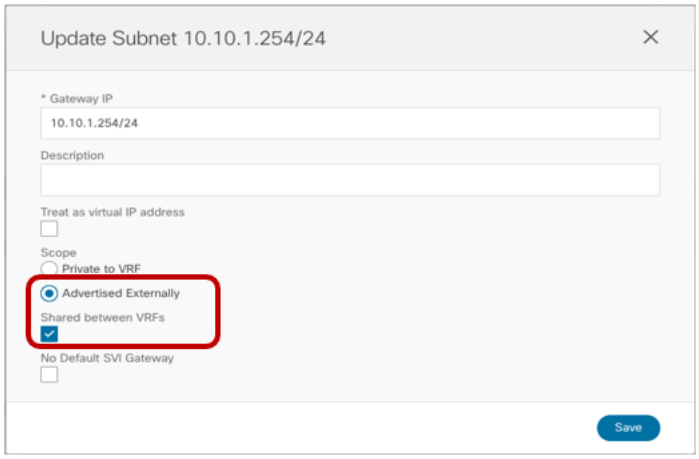


図 95.
BD のサブネットを別の VRF にリークする設定

- 内部 EPG がコントラクトのプロバイダーである場合、BD に関連付けられた同じサブネットも EPG 自体で定義する必要があります。

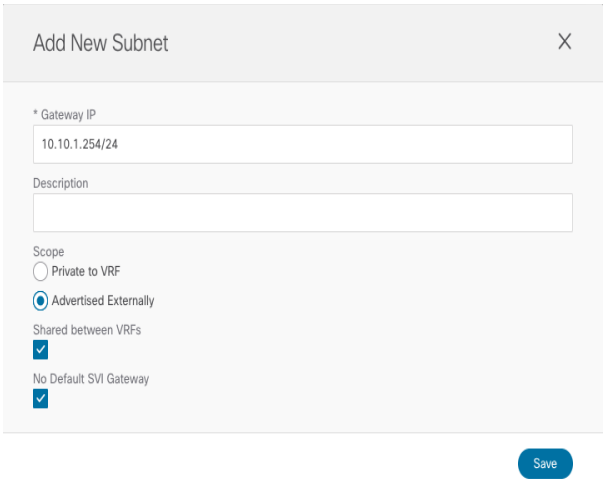


図 96.
プロバイダー EPG でのサブネットの設定

すでに BD に使用されているのと同じフラグを EPG のサブネットにも設定する必要があることに注意してください（そうしなかった場合、Nexus Dashboard Orchestratorはテンプレートの展開を妨げます）。上記の設定は、VRF 間のルートのリークを有効にするためにのみ必要であるため、「デフォルト ゲートウェイがデフォルト ゲートウェイが特定の BD の設定の結果としてすでにインスタンス化されているため」というフラグを追加で設定する必要があります。

- 外部 EPG に関連付けられたサブネットを正しく設定して、VRF 間 NS 接続を確立できるようにします。これには、図 97 に示す設定を実行する必要があります。

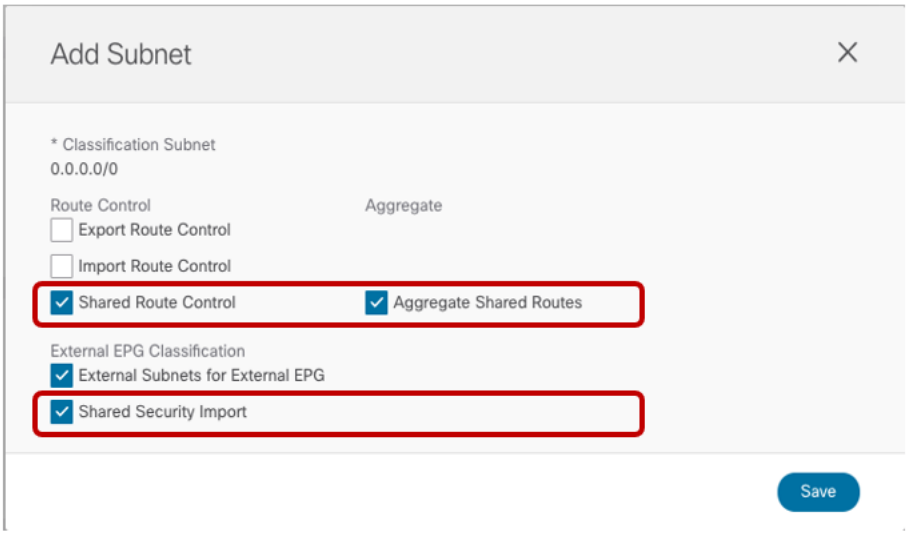


図 97.
VRF 間ノースサウス接続に必要な外部 EPG の設定

上記の例では、外部 EPG で0.0.0.0/0 が定義されているため、図で設定されているさまざまなフラグによって次の動作が発生します。

- 「外部 EPG の外部サブネット (External Subnets for External EPG)」：この外部 EPG にマッピングします（つまり、対応するクラス ID に関連付けられます）。前述のように、特定の 0.0.0.0/0 の場合、すべての着信トラフィックに関連付けられるクラス ID は、実際には vRF クラス ID です（外部 EPG クラス ID ではありません）。
- 「集約共有ルート (Aggregate Shared Routes)」を使用した「共有ルート制御 (Shared Route Control)」：外部ルータから学習した（またはスタティック ルートとしてローカルに設定された）すべてのプレフィックスを内部 VRF にリークできます。「共有集約ルート (Aggregate Shared Routes)」フラグが設定されていない場合、0.0.0.0/0 ルートのみが外部ルータから受信された場合にのみリークされます。0.0.0.0/0 以外のプレフィックスを設定する場合も、同じ考慮事項が適用されます。

「共有セキュリティ インポート (Shared Security Import)」：これは、内部 VRF が関連付けられたクラス ID で展開されているコンピューティング リーフ ノードにプレフィックス 0.0.0.0/0（キャッチオール）がインストールされていることを確認するために必要です。これにより、コンピューティング リーフは、ローカルに接続されたエンドポイントから発信され、外部ネットワーク ドメインを宛先とするフローにセキュリティ ポリシーを適切に適用できます。

注： より具体的な IP サブネット（たとえば192.168.1.0/24）を指定する場合、L3Out で学習される可能性のある /24 サブネットのより具体的なプレフィックス部分をリークするには、「集約共有ルート」を使用する

必要があります。フラグが設定されていない場合、外部ルータから受信した場合、/24 プレフィックスだけがリークされます。

VRF 間使用例の重要な考慮事項の 1 つは、L3Out に関連付けられた外部 EPG の展開方法に関連しています。前述のように、この使用例では、BD のサブネットは、前述のフラグの特定の使用に基づいて外部ネットワークドメインにアドバタイズされ、BD を L3Out に明示的にマッピングする必要はありません。これは、ストレッチされた外部 EPG を導入する場合（図 82 で前述）、どの L3Out から BD のサブネットがアナウンスされるかを制御することはできず、デフォルトでサイトにのみ存在する IP サブネットだけが、リモートサイトの L3Out からもアドバタイズされることを意味しています（図 98）。

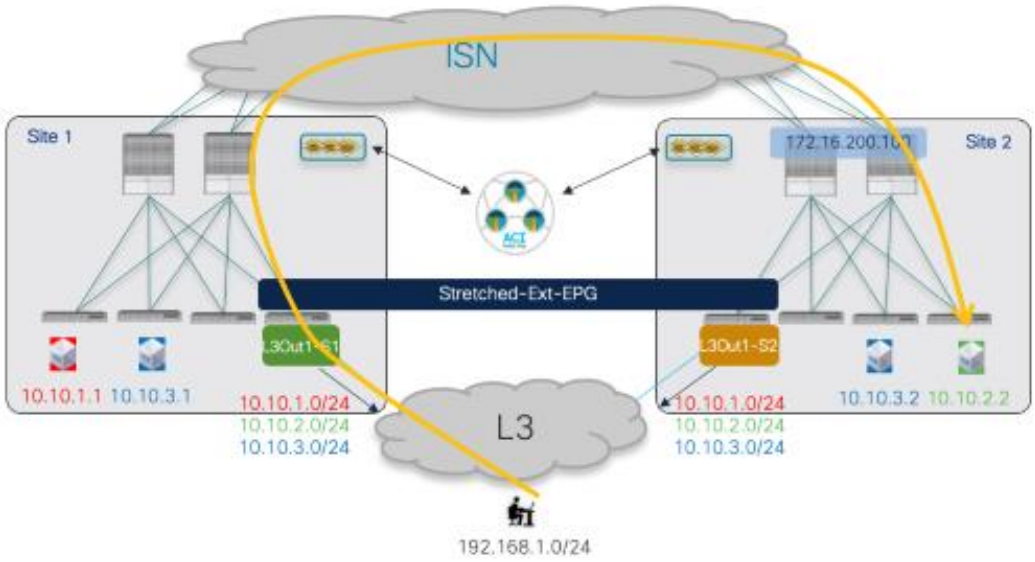


図 98.
共有サービスの使用例での BD サブネットのアドバタイズ

上記のシナリオでは、デフォルトの動作を変更し、ローカル L3Out からアドバタイズされたルーティング情報がローカルに定義されたサブネットに適していることを確認できます（ただし、ストレッチされたサブネットではホストベースのルーティングを有効にできます）。最も一般的な EBGP 隣接関係は外部ルータと確立されるため、これを実現する簡単な方法は、たとえば、AS-Path プリペンド機能を使用することです。

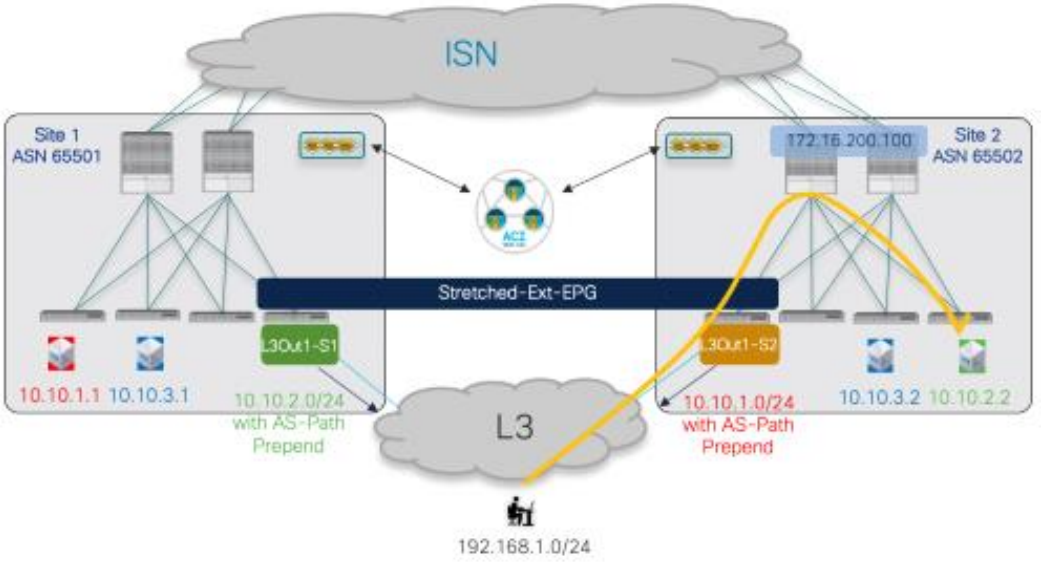


図 99.
AS パス プリペンドを使用した着信トラフィックの最適化

図 100、図 101、および図 102 に、この設定に必要な手順を示します。L3Out へのルート マップの作成と適用は、現在 APIC でのみサポートされており、Nexus Dashboard Orchestrator ではサポートされていないことに注意してください。

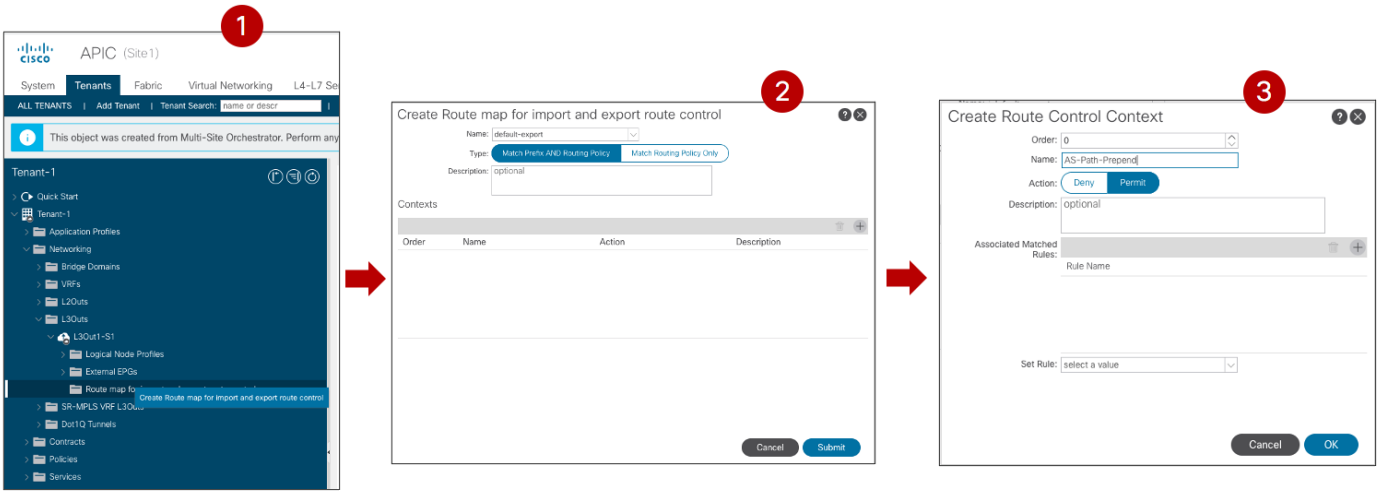


図 100.
L3Out に関連付けられた「デフォルト エクスポート」ルート マップの作成

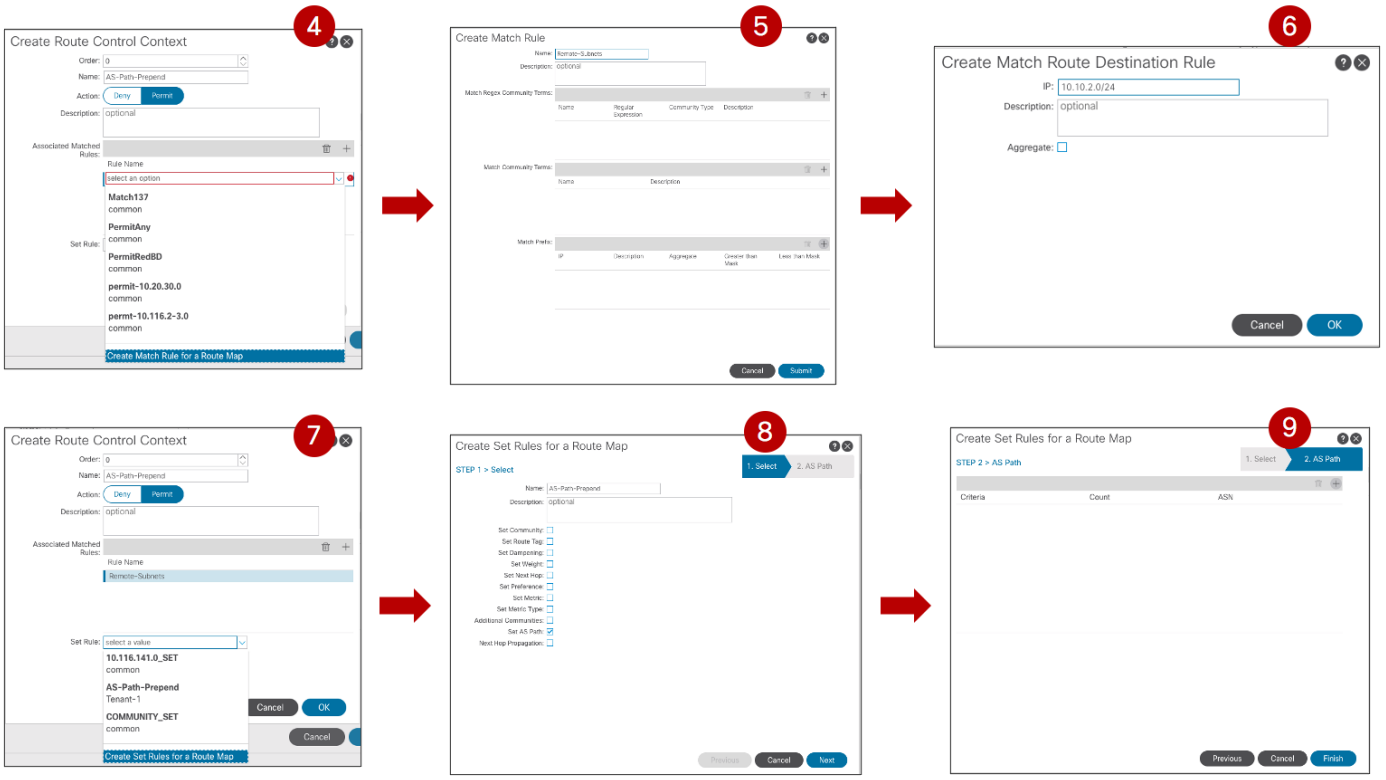


図 101.
ルート制御コンテキストコンフィギュレーション（一致およびプレフィックスの設定）

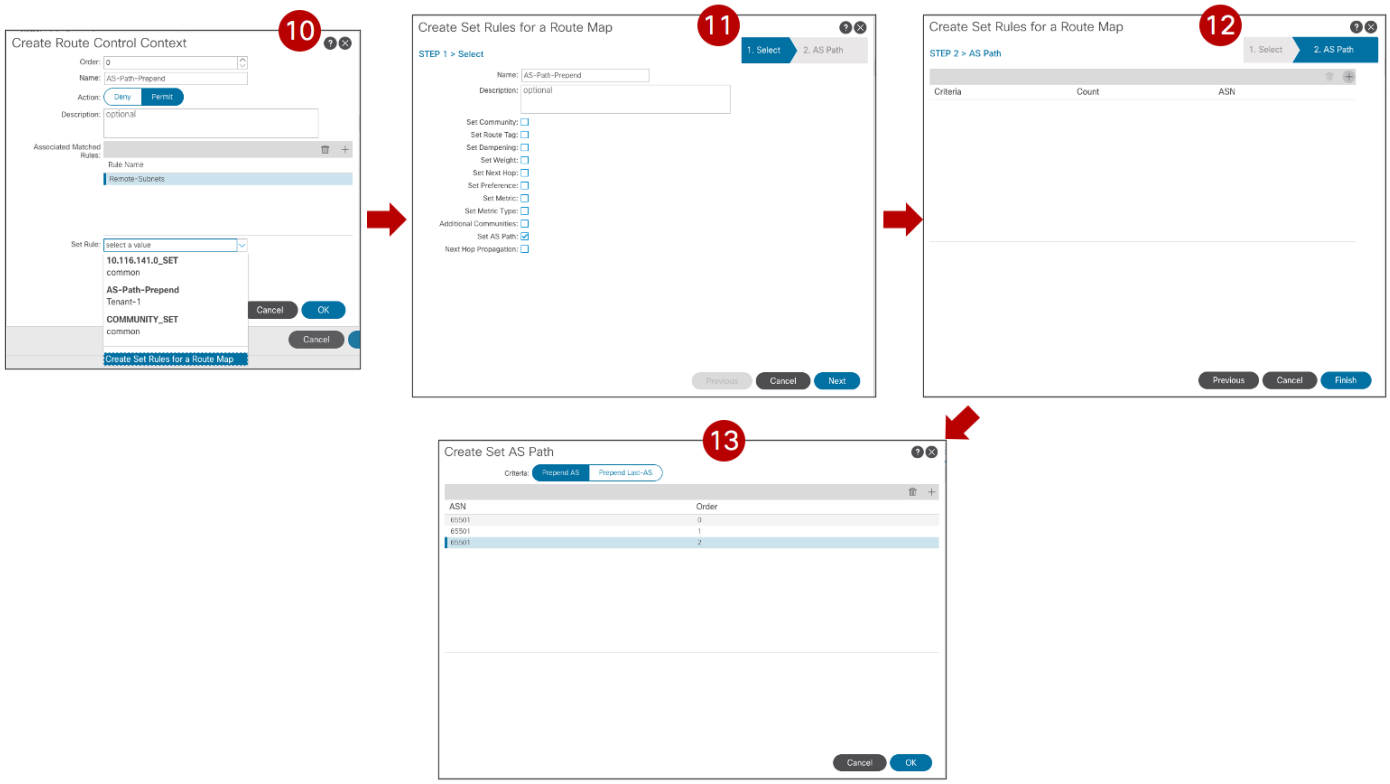


図 102.
ルート制御コンテキストセットプレフィックスの完了

注： 拡張されていないサブネットのホストベース ルーティングを有効にすることは、スケーラビリティの問題がないことを前提として、着信トラフィック パスを最適化する代替アプローチです。

使用例2検証

内部 EPG/BD と外部ネットワーク ドメイン間の接続については、図 89、図 90、および図 91 で行ったのと同じ考慮事項が、この使用例にも適用されます。つまり、最適な着信ルーティングは、特定の BD レベルでホストベースのルーティング機能を有効にすることで影響を受けますが、アウトバウンド通信は常にローカル L3Out 接続を介して流れます。

図 100 は、特定のノースサウス VRF 間使用例に必要なVRF の展開を示しています。気づいたように、両方の VRF は BL ノードに展開されますが、通常は内部 VRF のみがコンピューティング リーフ ノードに存在します。

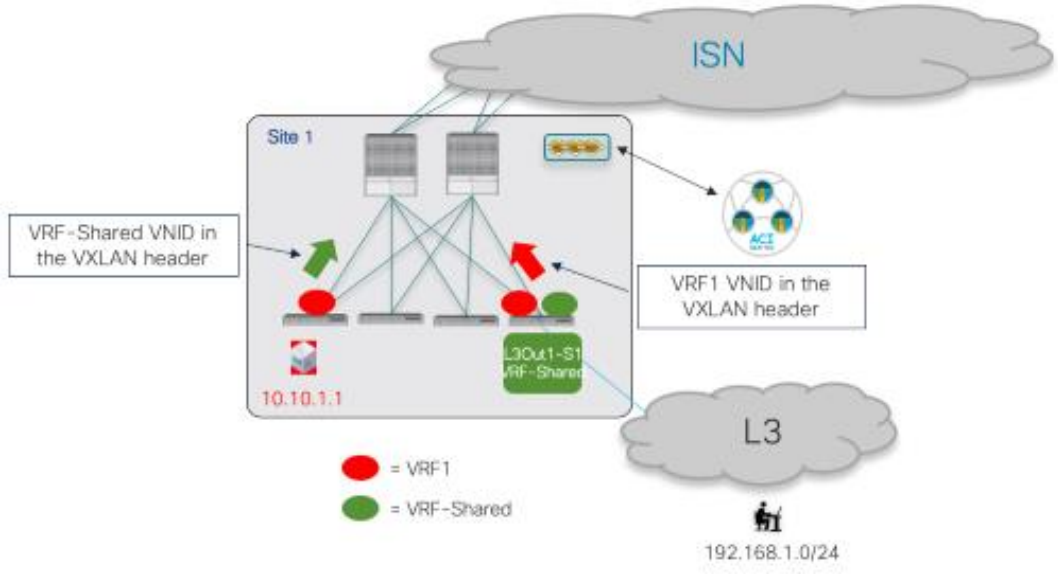


図 103.
VXLAN カプセル化トラフィックの VRF 展開と VNID

さらに、コンピューティング リーフでカプセル化されたアウトバウンド トラフィック VXLAN は、ヘッダーの VRF 共有 VNID を使用するため、トラフィックを受信する BL ノードは、外部ドメインにトラフィックを送信する前に VRF 共有ドメインで L3 ルックアップを実行できます。次の出力は、コンピューティング リーフ ノードと BL ノードのルーティング テーブルの内容を示しています。コンピューティング リーフ 101 では、外部プレフィックス 192.168.1.0/24 が VRF1 ルーティング テーブルにリークされ、VXLAN ヘッダーの VNID を 2293765 に書き換えます（Site1 の VRF 共有の VNID を表します）。BL ノード104 では、代わりに内部サブネット 10.10.1.0/24 が VRF 共有ルーティング テーブルにリークされ、VXLAN ヘッダーの VNID を 3112963 に書き換えます（Site1 の VRF1 の VNID を表します）。

Leaf 101 Site1

```
Leaf101-Site1# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
```

```
10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.1.112.66%overlay-1, [1/0], 00:21:25, static, rwVnid: vxlan-3112963
10.10.1.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 10.10.1.254, vlan43, [0/0], 3d16h, local, local
192.168.1.0/24, ubest/mbest: 1/0
    *via 10.1.0.69%overlay-1, [200/0], 00:27:33, bgp-65501, internal, tag 3, rwVnid: vxlan-2293765
```

Leaf 104 Site1

```
Leaf104-Site1# show ip route vrf Tenant-1:VRF-Shared
IP Route Table for VRF "Tenant-1:VRF-Shared"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>
10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.1.112.66%overlay-1, [1/0], 00:23:32, static, tag 4294967292, rwVnid: vxlan-3112963
192.168.1.0/24, ubest/mbest: 1/0
    *via 172.16.1.1%Tenant-1:VRF-Shared, [20/0], 1d20h, bgp-65501, external, tag 3
```

Inter-VRF シナリオでは、内部 EPG と外部 EPG 間のコントラクトを使用するときにセキュリティ ポリシーの適用が適用されるリーフ ノードは、コントラクトのプロバイダーとコンシューマーが誰であるかによって異なります。

Ext-EPG がコンシューマーであり、内部 EPG がコントラクトのプロバイダーである場合（外部クライアントがデータセンターにトラフィックを送信して、そこでホストされているアプリケーションによって提供されるサービスを「消費」する場合）、セキュリティ ポリシーはトラフィックを受信した最初のリーフに適用されます。これは、着信トラフィックの場合は BL ノードで、アウトバウンド トラフィックの場合はコンピューティング リーフで、内部エンドポイントが展開されているサイトとは無関係に有効であることを意味します。

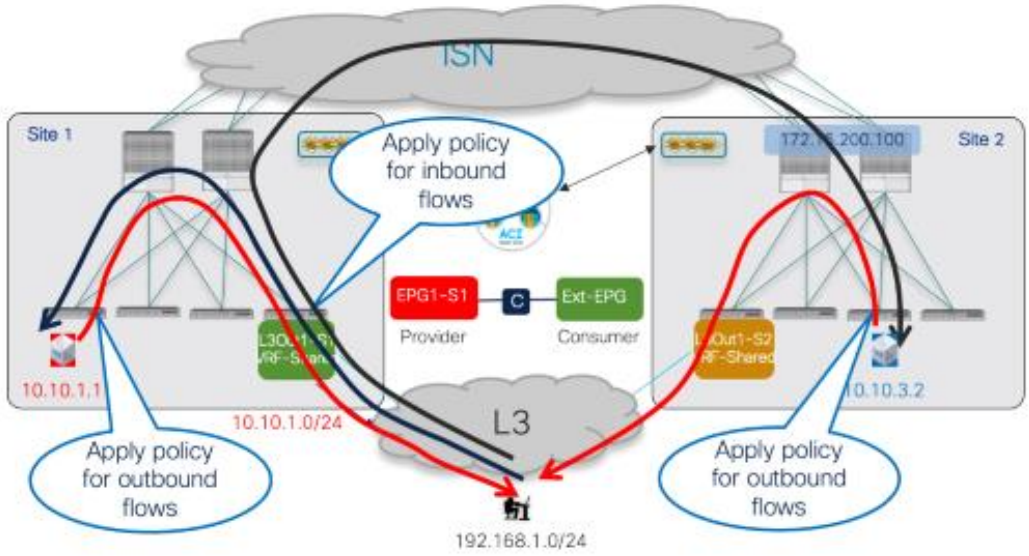


図 104.
Ext-EPG がコンシューマーである場合のセキュリティ ポリシーの適用

代わりに、コントラクトの方向が逆になり、外部 EPG がコントラクトのプロバイダーとして設定されている場合（通常は、外部サービスに接続するためにデータセンターから開始される通信用）、セキュリティ ポリシーは両方のレッグのコンピューティング リーフ ノードに一貫して適用されます。

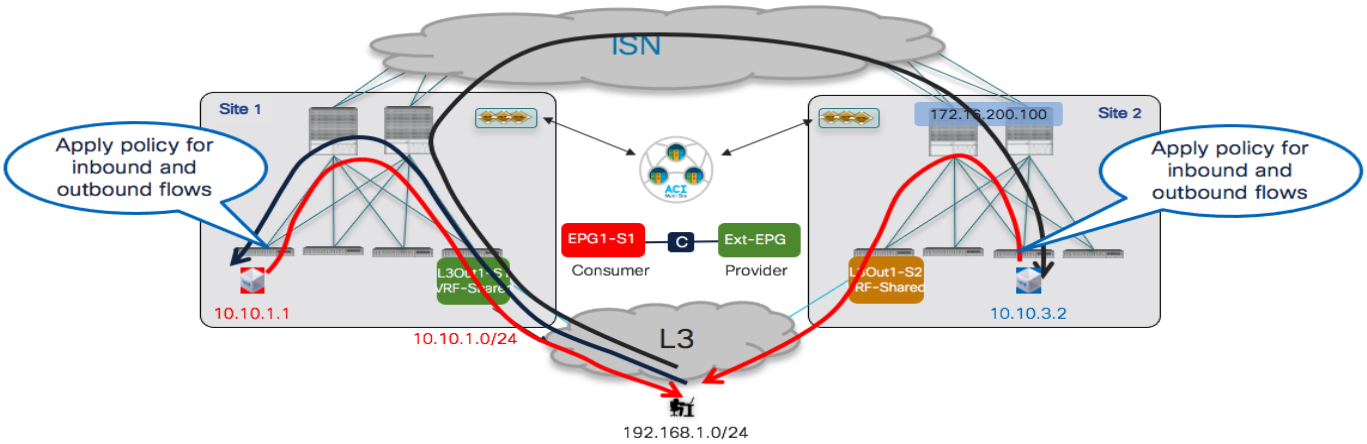


図 105.
Ext-EPG がプロバイダーである場合のセキュリティ ポリシーの適用

使用例 3：外部リソースとの通信へのサイト ローカル L3Out 接続（異なるテナント間の Inter-VRF/共有サービス）

この共有サービスの使用例では、内部 EPG/BD の VRF と L3Out の VRF は異なるテナントで定義されます。前の使用例で行った設定手順と導入時の考慮事項は、ここでも引き続き適用されますが、次の違いがあります。

- コントラクトの範囲を「グローバル」に設定する必要があります。

- コントラクトは、「プロバイダー」テナントに関連付けられたテンプレートで定義する必要があります。この設定を Nexus Dashboard Orchestrator に自動的に適用すると、図 106 および図 107 に示すように、APIC では「コンシューマー」テナントに向けてコントラクトがエクスポートされます。

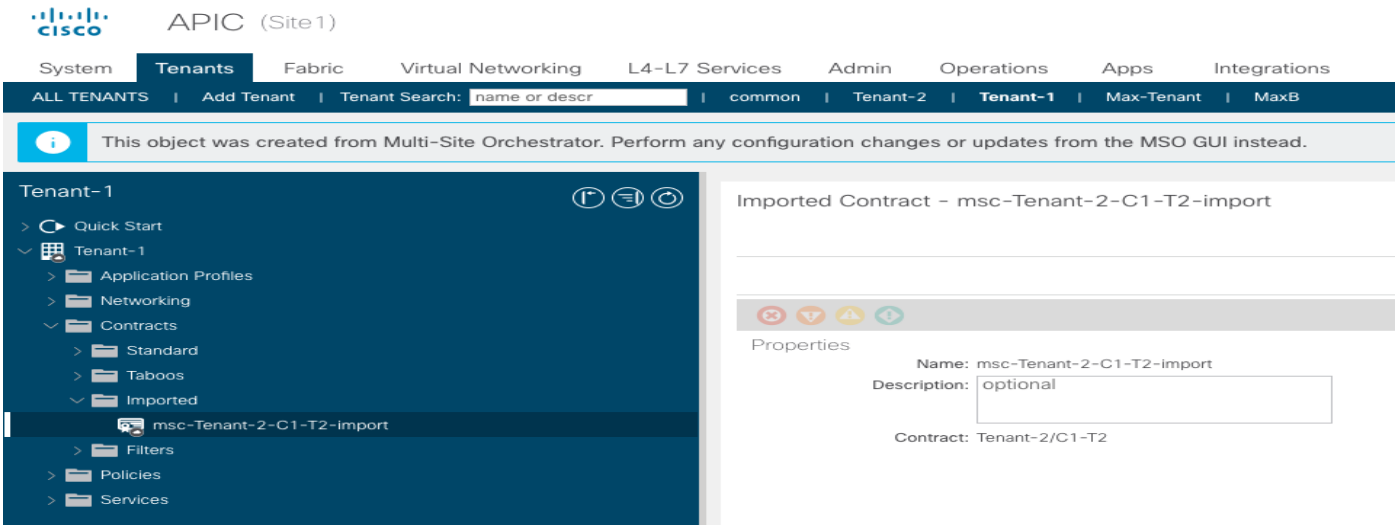


図 106.
コンシューマーテナントにインポートされたコントラクト

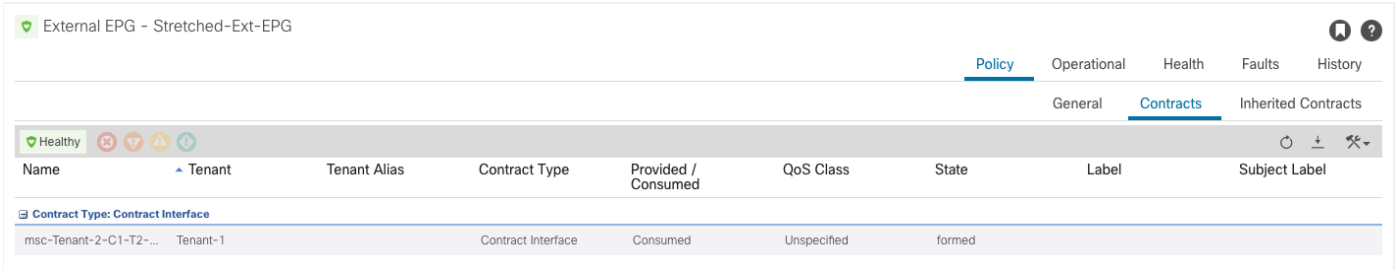


図 107.
コンシューマーテナントで作成されたコントラクトインターフェイス

外部ネットワークへの BD サブネットのアドバタイズメントを含むその他のすべての考慮事項は、前の使用例 2 とまったく同じです。

サイト間 L3Out の展開

前述のすべての使用例では、外部リソースとのアウトバウンド通信のために、Multi-Site ドメインの各ファブリック パーツでローカル L3Out 接続を使用できることが常に要件でした。ACI Multi-Site 展開でのこのデフォルトの動作では、特定のファブリックにのみ展開されている L3Out 接続を介してアクセス可能なリソースと通信する必要があるいくつかの特定のシナリオをカバーできません。

最初のシナリオは、図 108 に示すように、サイトに接続された内部エンドポイントとリモートサイトに展開された L3Out 接続との間にノースサウス接続を確立することです。

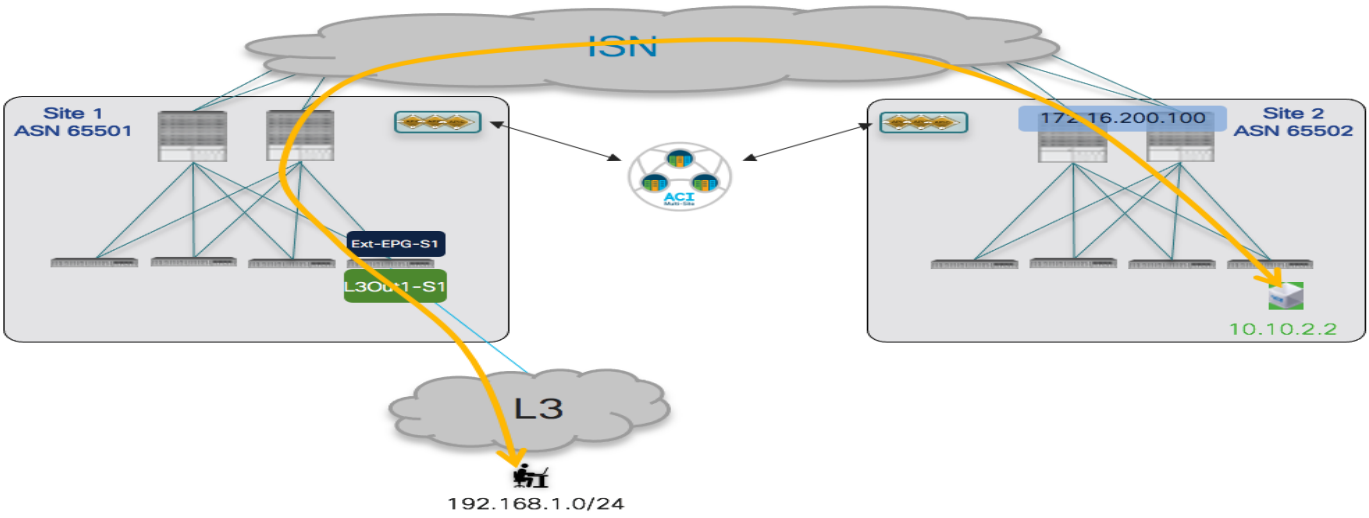


図 108.
サイト間ノースサウス接続シナリオ

2 番目のシナリオは、図 106 に示すように、異なるサイトに導入された L3Out 接続間での中継ルーティングの有効化です。

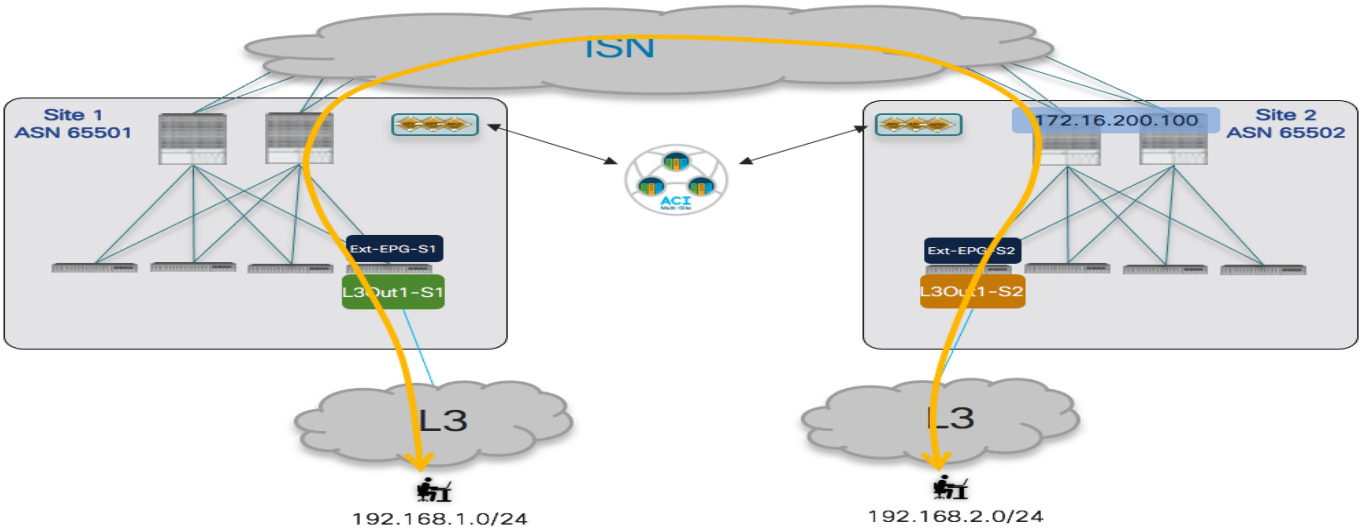


図 109.
サイト間トランジット ルーティングのシナリオ

ACI リリース4.2(1) および MSO リリース 2.2(1) は、「サイト間 L3Out」機能のサポートを導入しました。これにより、上記の図に示す 2 つの使用例、VRF 内および VRF間の両方（さらにはテナント間）の導入シナリオに対応できるように、デフォルトのマルチサイトの動作を変更できます。

ACI リリース 5.2(3) およびNDO リリース 3.5(1) では、サイト間 L3Out が優先グループまたは vzAny の使用と組み合わせてサポートされないことに注意してください。したがって、個別のサイトで定義された EPG と Ext-EPG 間（または Ext-EPG 間）に特定のコントラクトを適用する必要があります。

注： サイト間 L3Out 機能の導入を必要とする特定の使用例、およびコントロールとデータ プレーンの動作の技術的側面に関する詳細については、以下の ACI Multi-Site のペーパーを参照してください（このドキュメントでは、主にこの機能の導入方法に焦点を当てています）） ：

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html#ConnectivitytotheexternalLayer3domain

サイト間ノースサウス接続（VRF 内）

ここで考慮される最初のシナリオは、図 110 に示す、サイト間ノースサウス接続のイントラ VRF の確立に関するものです。

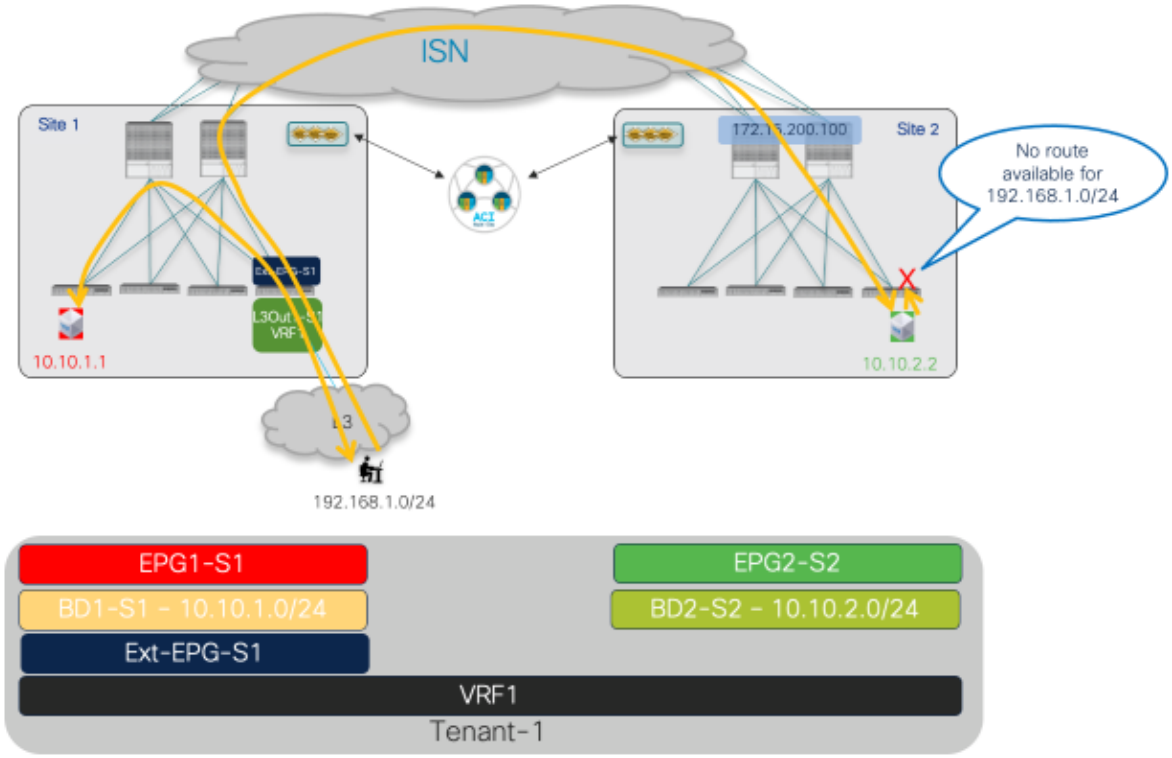


図 110.
ノースサウス接続（VRF 間）のサイト間 L3Out

上記のように、BD とコントラクトが適切に設定されると（EPG1-S1 と Ext-EPG-S1 の間、および EP2-S2 と Ext-EPG-S1 の間の接続が可能になります）、L3Out 接続（Site1 の EPG1-S1）で同じファブリックに接続されているエンドポイントでのみ、双方向のノースサウス通信がデフォルトで確立されます。EPG2-S2 のリモート エンドポイントは、着信トラフィック フローを受信することもできます（ISNを介した VXLAN データ プレーン接続の活用）。ただし、外部プレフィックス 192.168.1.0/24 はサイト間でアドバタイズされないため、リターン通信はできません。ACI Multi-Site のこのデフォルト動作は、「サイト間 L3Out」機能を有効にすることで変更できます。Nexus Dashboard Orchestrator で実行される次の設定手順は、EPG2-S2 の Site2 部分のエンドポイントと外部ネットワーク 192.168.1.0/24 間の双方向のノースサウス通信を実現するために必要です。

1. IP サブネットを L3Out-S1からアドバタイズするように BD2-S2 を適切に設定します。これには、IP サブネットを「外部アトバタイズ (Advertised Externally)」にし、BD をリモートL3Out にマッピングする必要があります。BD は Site2 でローカルに定義されているため、両方のアクションがサイト レベルで実行されます。SIte2 で定義された BD2-S2 を L3Out-S1 に関連付けるには、NDO テンプレートで L3Out オブジェクトを定義する

必要があります。L3Out が最初に APIC で作成された場合、L3Out オブジェクトを NDO にインポートできます。

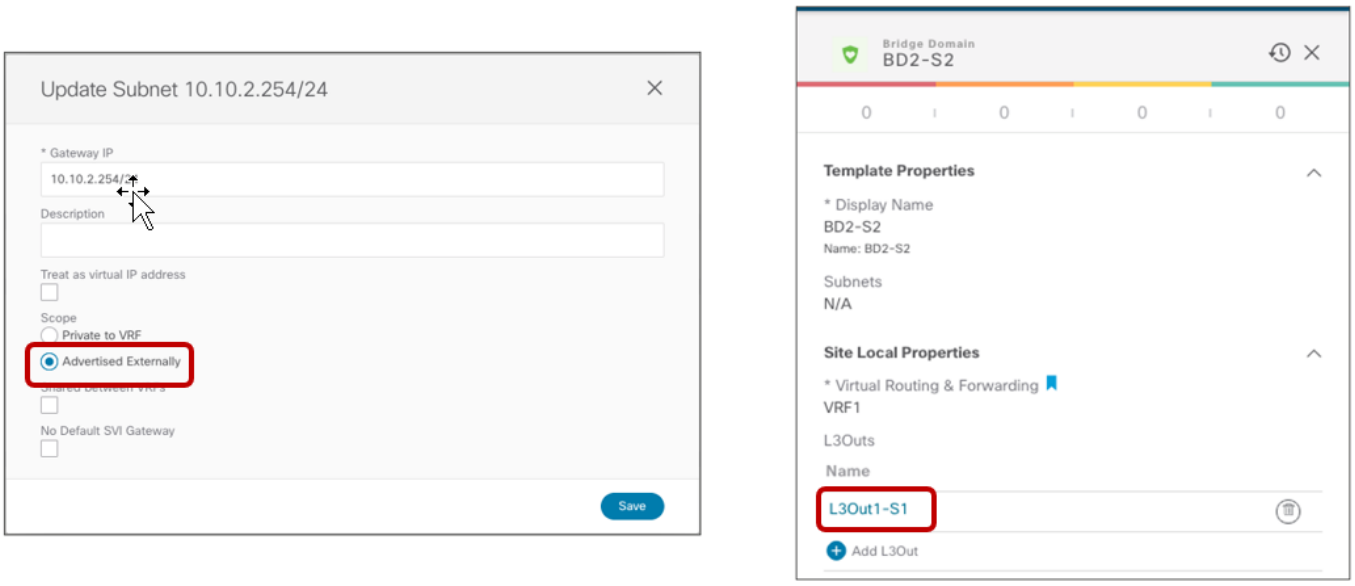


図 111.
L3Out1-S1から BD2-S2 のサブネットをアドバタイズするための設定

2. 着信トラフィックを適切に分類するように Ext-EPG-S1 を設定します。このドキュメントで前述したように、L3Out がすべての外部宛先へのアクセスを提供する場合、「キャッチオール」0.0.0.0/0 プレフィックスの使用は非常に一般的ですが、この特定の使用例では、L3Out が特定の外部リソースへのアクセスを提供するので、より具体的なプレフィックスを構成できます。

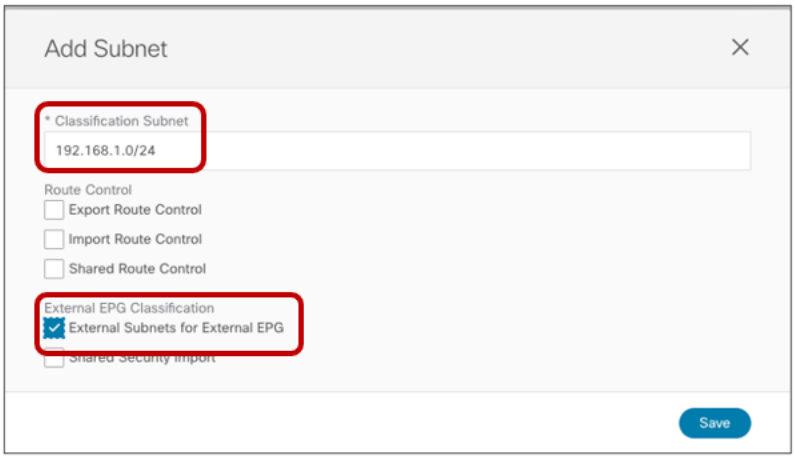


図 112.
Ext-EPG-S1 で設定された分類サブネット

3. 前述の ACI Multi-Site ペーパーで詳細に説明されているように、サイト間 L3Out 接続は、内部エンドポイントが接続されているコンピューティング リーフ ノードと外部リソースに接続されている BL ノード間に VXLAN トンネルを直接作成することで実現されます。これを可能にするには、まず、L3Out が展開されている Multi-Site ドメインの ACI ファブリック部分の外部 TEP プールを定義する必要があります。これにより、そのファブリック内の各境界リーフ ノードの TEP アドレス（指定された外部 TEP プールの一部）をプロビジョニングして、リモート コンピューティング リーフ ノードから直接 VXLAN トンネルを確立できるようになります（デフ

ォルトで割り当てられたすべての TEP アドレスファブリックリーフおよびスパイン ノードは、ファブリック起動操作中に設定された元の TEP プールの一部であり、そのようなプールはサイト間でルーティングできない場合があります）。技術的には、外部 TEP プールが L3Out が展開されているファブリックにのみ必要な場合でも、マルチサイト ドメインの各ファブリック部分に 1 つを提供することをお勧めします（後ほどローカル L3Out が作成されたときにすぐに通信が機能するようにするためのみ）。

図 113 に示すように、外部 TEP プールの設定は、NDO ドメインのファブリック部分の各ポッドの「インフラ設定」ワークフローの一部として NDO で実行できます。

注： NDO ドメインのファブリック部分がマルチポッド ファブリックとして展開されている場合、ファブリックの各ポッド部分に個別の外部 TEP プールを指定する必要があります。外部 TEP プールの範囲は、/22～/29 プレフィックスです。

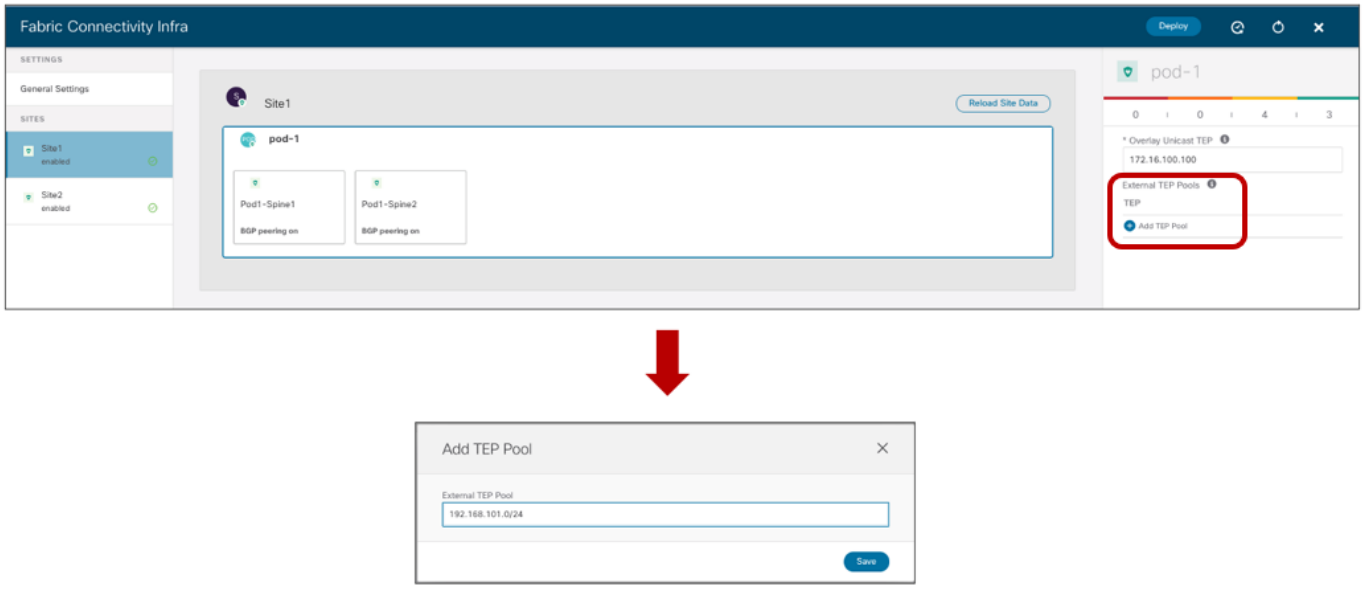


図 113.
各ポッドの外部 TEP プールの設定

外部 TEP プール設定がファブリックにプッシュされると、最初に BL ノードでの専用ループバック インターフェイスのプロビジョニングが行われます。これは、リモート サイトのコンピューティング ノードから開始された VXLAN トンネルの宛先として使用される、そのノードに割り当てられた外部 TEP アドレスを表します。これは、たとえば次の出力の Site1 の BL ノードで確認できます。

Leaf 104 Site1

```
Leaf104-Site1# show ip int bri vrf overlay-1
IP Interface Status for VRF "overlay-1"(4)
Interface            Address              Interface Status
eth1/49              unassigned           protocol-up/link-up/admin-up
eth1/49.6            unnumbered           protocol-up/link-up/admin-up
                     (lo0)
eth1/50              unassigned           protocol-up/link-up/admin-up
eth1/50.7            unnumbered           protocol-up/link-up/admin-up
                     (lo0)
```

```
eth1/51              unassigned          protocol-down/link-down/admin-up
eth1/53              unassigned          protocol-down/link-down/admin-up
eth1/54              unassigned          protocol-down/link-down/admin-up
vlan8                10.1.0.30/27        protocol-up/link-up/admin-up
lo0                  10.1.0.69/32        protocol-up/link-up/admin-up
lo1                  10.1.232.65/32      protocol-up/link-up/admin-up
lo4                  192.168.101.232/32  protocol-up/link-up/admin-up
lo1023               10.1.0.32/32        protocol-up/link-up/admin-up
```

4. 外部 TEP プールのプロビジョニングは、サイト間で外部プレフィックスの交換をトリガーするには不十分です。これは、前の図 110 に示す発信フローを Site1 の BL ノードに送信できるようにするために必要です。そのためには、Site2 の EPG2-S2 と Site1 の L3Out に関連付けられた Ext-EPG の間にコントラクトを適用する必要もあります。

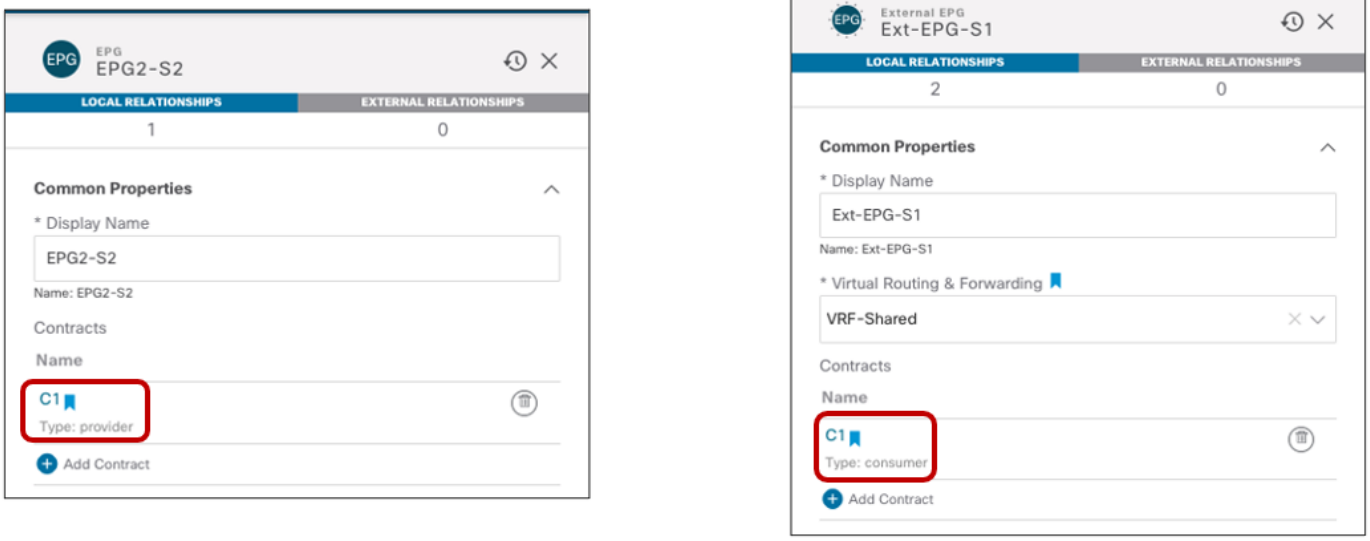


図 114.
EPG2-S2 と Ext-EPG-S1 間のコントラクトの適用

そのコントラクト関係が確立されると、VPNv4/VPNv6 プレフィックス交換がスパイン間でトリガーされ、外部プレフィックス 192.168.1.0/24 を Site2 にアドバタイズできます。これにより、発信通信が正常に確立されます。これは、Site2 のコンピューティング リーフのルーティング テーブルを確認することで確認できます。

Leaf 304 Site2

```
Leaf304-Site2# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.2.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.136.66%overlay-1, [1/0], 03:32:38, static, rwVnid: vxlan-2359299
```

```
10.10.2.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 10.10.2.254, vlan41, [0/0], 1d01h, local, local
192.168.1.0/24, ubest/mbest: 1/0
    *via 192.168.101.232%overlay-1, [200/0], 00:00:02, bgp-100, internal, tag
65501, rwVnid: vxlan-3112963
```

上記のように、外部プレフィックスのネクストホップは、Site1 の BL ノードに割り当てられた外部 TEP プールアドレスです。また、ルーティング テーブルには、外部宛先 192.168.1.0/24 宛てのすべてのトラフィックをヘッダーの VXLAN ID 3112963 を使用してカプセル化する必要があるという情報が表示されます。この値は、次の出力に示すように、Site1 の L3Out VRF（VRF1）の VXLAN ID を表します。

Leaf 104 Site1

```
Leaf104-Site1# show vrf Tenant-1:VRF1 detail
VRF-Name: Tenant-1:VRF1, VRF-ID: 41, State: Up
    VPNID: unknown
    RD: 103:3112963
```

この VXLAN ID 値は vXLAN ヘッダーに追加され、受信側の BL ノードが宛先に対してレイヤ 3 ルックアップを実行するための情報を取得できるようにします。VXLAN トンネルは BL ノードで直接終端されるため、Site1 のスパインで変換は行われず、その結果、コンピューティング リーフ ノードは Site の VRF1 を表す正しい VXLAN ID を認識する必要があります。

この VXLAN ID 値は vXLAN ヘッダーに追加され、受信側の BL ノードが宛先に対してレイヤ 3 ルックアップを実行するための情報を取得できるようにします。VXLAN トンネルは BL ノードで直接終端されるため、Site1 のスパインで変換は行われず、その結果、コンピューティング リーフ ノードは Site1 の VRF1 を表す正しい VXLAN ID を認識する必要があります。したがって、この情報は、Site2 のコンピューティング リーフ ノードの BGP ルーティング テーブルで確認できるため、EVPNコントロール プレーン更新の一部としてSite1 から Site2 に伝達されます。

Leaf 304 Site2

```
Leaf304-Site2# show ip bgp 192.168.1.0/24 vrf Tenant-1:VRF1
BGP routing table information for VRF Tenant-1:VRF1, address family IPv4 Unicast
BGP routing table entry for 192.168.1.0/24, version 30 dest ptr 0xa2262588
Paths: (1 available, best #1)
Flags: (0x08001a 00000000) on xmit-list, is in urib, is best urib route, is in HW
  vpn: version 218279, (0x100002) on xmit-list
Multipath: eBGP iBGP
  Advertised path-id 1, VPN AF advertised path-id 1
  Path type: internal 0xc0000018 0x80040 ref 0 adv path ref 2, path is valid, is best path,
remote site path
             Imported from 103:19890179:192.168.1.0/24
  AS-Path: 65501 3 , path sourced external to AS
    192.168.101.232 (metric 63) from 10.0.0.66 (172.16.200.1)
      Origin IGP, MED not set, localpref 100, weight 0 tag 0, propagate 0
      Received label 0
      Received path-id 2
      Extcommunity:
          RT:65501:19890179
```

```
SOO:65501:33554415
COST:pre-bestpath:166:2684354560
COST:pre-bestpath:168:3221225472
VNID:3112963
```

サイト間ノースサウス接続（VRF 間）

このシナリオの唯一の違いは、L3Out が内部エンドポイント（VRF1 の一部）とは異なる VRF（VRF 共有）の一部であることです。

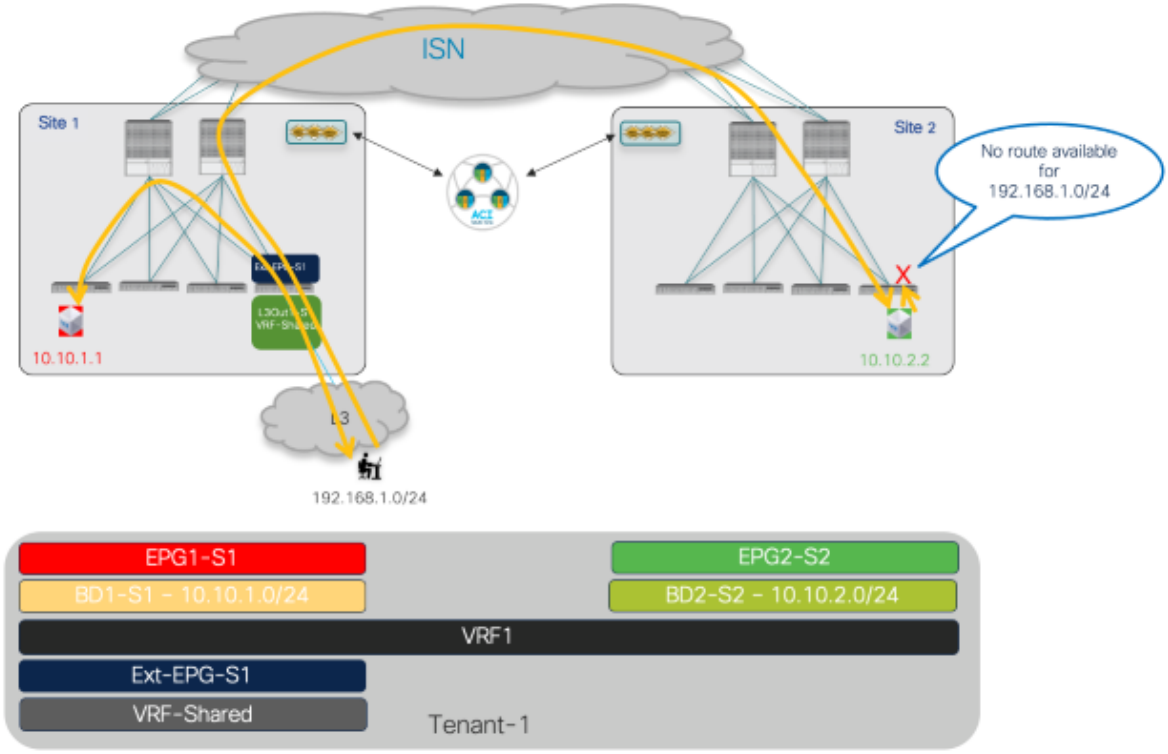


図 115.
ノースサウス接続用のサイト間 L3Out（VRF 間）

上記の設定手順 3 と 4 は同じままです（ただし、適用されるコントラクトの範囲が少なくとも「テナント」になっていることを確認する必要があります）。現在変更されているのは、VRF 間のルートをリークし、ポリシーを適切に適用できるようにするために必要な設定です。「使用例 2：外部リソースと通信するためのサイトローカル L3Out 接続（同じテナント内の VRF 間/共有サービス）」と同じ考慮事項がここでも適用されます。図 116 に、BD および EPG で定義されたサブネットに必要な設定（EPG1-S1 がコントラクトのプロバイダーである場合、EPG でのサブネットは不要）と、Ext-EPG-S1 でのサブネット設定を示します。

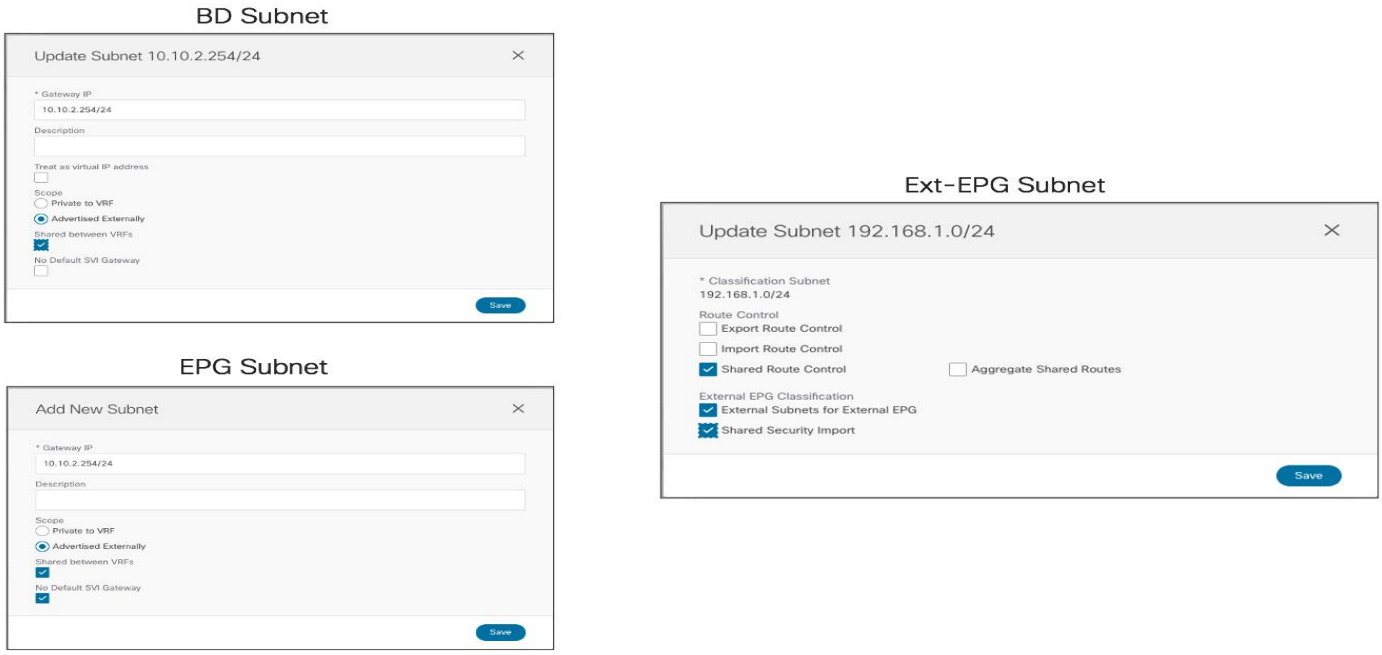


図 116.
サイト間ノースサウス VRF 間使用の設定のプロビジョニング

VRF が個別のテナントで定義されている場合、このセクションで前述した使用例では、同じ設定を NDO から事前にプロビジョニングする必要があることに注意してください。唯一の違いは、このような場合、コントラクトの範囲は「グローバル」である必要があり、プロバイダーテナントで定義する必要があることです。詳細については、「使用例 3：外部リソースと通信するためのサイトローカル L3Out 接続（異なるテナント間の VRF 間/共有サービス）」セクションを参照してください。

サイト間中継ルーティング接続（VRF 間）

以前の使用例では、エンドポイントと外部リソース間のサイト間通信を可能にするために、サイト間 L3Out 機能が導入されました。サイト間 L3Out が便利な特定の使用例は、ACI Multi-Site が個別の外部ネットワークドメインを相互接続する「分散型コア」の役割を果たしている場合です。この導入モデルはサイト間中継ルーティングと呼ばれ、図 115 に示すように、両方の L3Out 接続が同じ VRF1 ルーティングドメインの一部です。

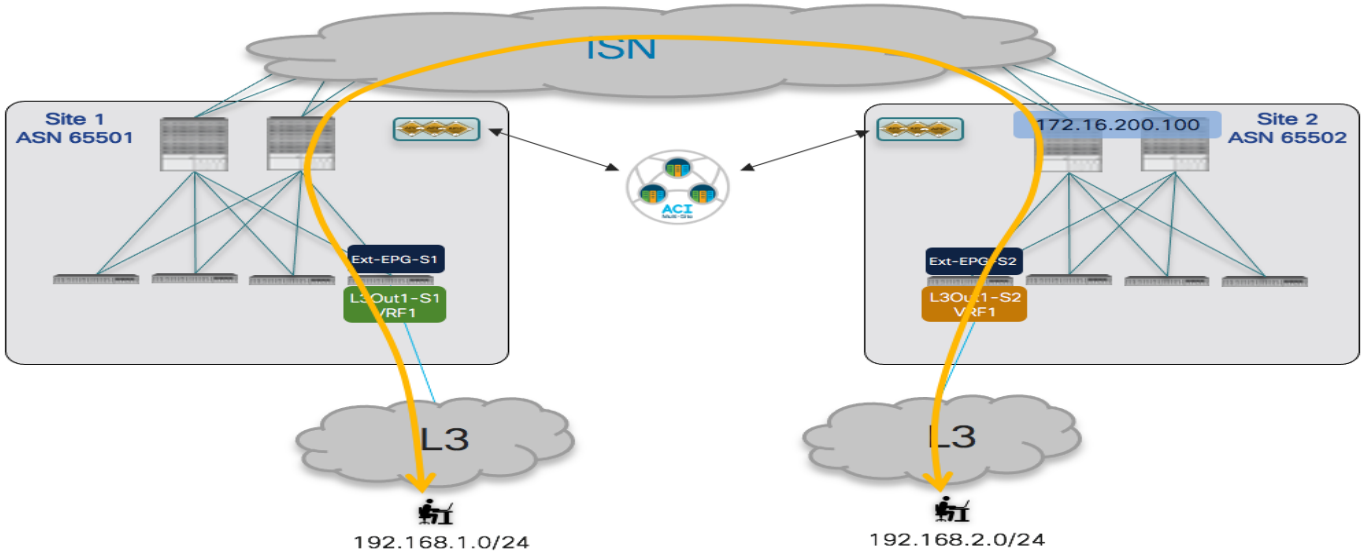


図 117.
サイト間中継ルーティング接続（VRF 間）

この場合、L3Out 接続ごとに、個別の外部 EPG が定義されます。相互に通信する必要がある異なる外部ルーテッド ドメインへの接続を提供するためです。このシナリオを実装するために必要なプロビジョニング手順は次のとおりです。

- Ext-EPG に関連付ける 1 つ以上のプレフィックスを定義して、着信トラフィックを適切に分類できるようにします。展開された L3Out のみが上記の図に示されている L3Out である場合、単純な 0.0.0.0/0 プレフィックスを両方に使用できます。ただし、実際のシナリオでは、他のすべての外部リソースへのアクセスを提供するために異なる L3Out 接続を使用するのが一般的です。そのため、サイト間中継ルーティングを可能にする L3Out 接続の Ext-EPG には、より具体的なプレフィックスが指定されます。

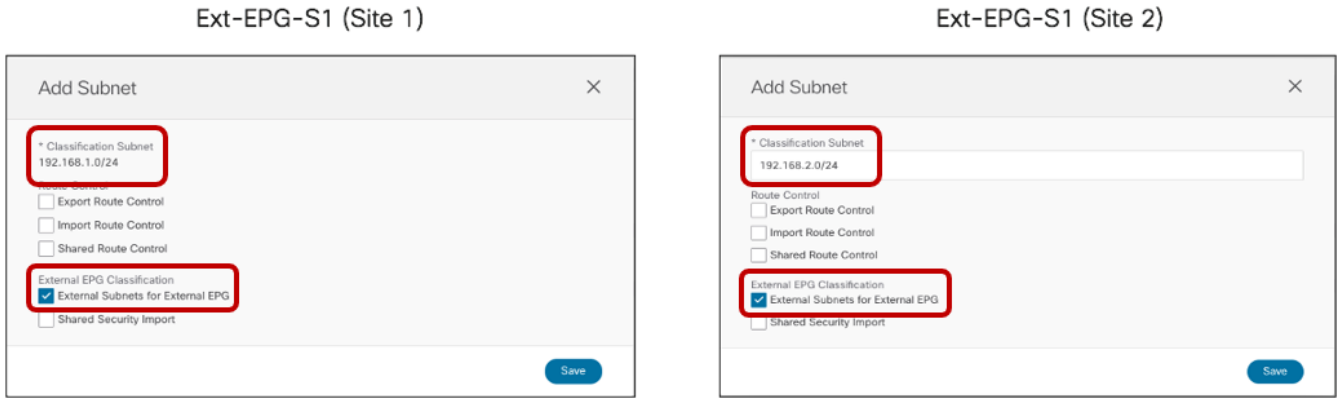


図 118.
Site1 および 2 の Ext-EPG での分類サブネットの設定

- 各 L3Out で学習したプレフィックスをリモート L3Out からアドバタイズできることを確認します。このセクションで説明する特定の例では、IP プレフィックス 192.168.1.0/24 が Site1 の L3Out で受信され、Site2 の L3Out からアドバタイズされる必要があります。また、192.168.2.0 /24 プレフィックスの場合も同様です。

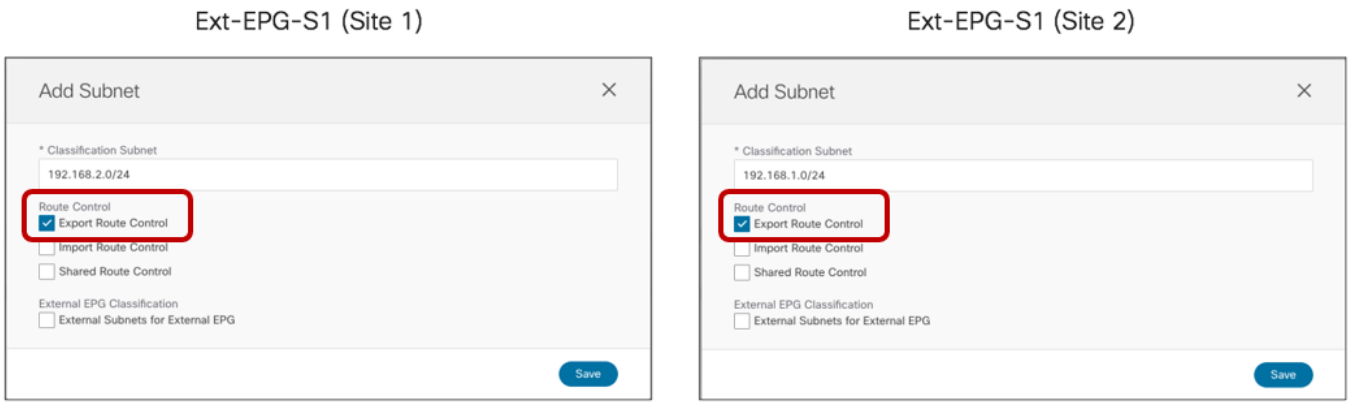


図 119.
各サイトの L3Out からの特定のプレフィックスのアナウンス

- サイト間中継ルーティングを正常に有効にするための最後の手順は、異なるサイトに展開された L3Out に関連付けられた Ext-EPG 間のセキュリティ ポリシーを作成することです。図 120 の例では、Site1 の Ext-EPG-S1 がコントラクト C1 を提供し、それが Site2 の Ext-EPG-S2 によって消費されます。

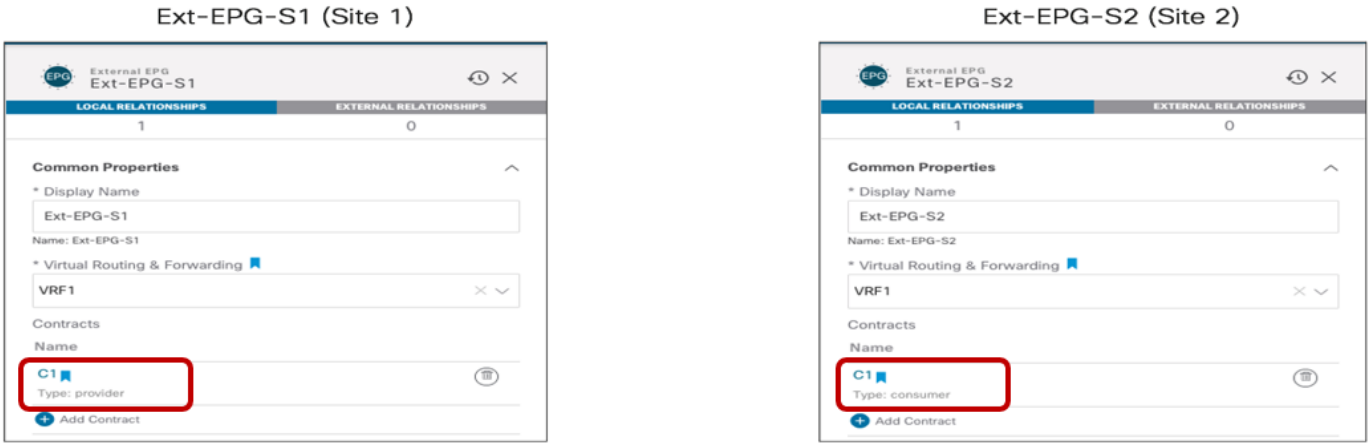


図 120.
Ext-EPG 間のセキュリティ ポリシーの適用

上記のプロビジョニング手順を Site1 と Site2 の APIC ドメインに展開すると、サイト間中継接続を確立できます。各サイトの BL ノードで、リモート外部プレフィックスが実際に受信されていることを確認できます。

Leaf 104 Site1

```
Leaf104-Site1# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.1.0/24, ubest/mbest: 1/0
    *via 172.16.1.1%Tenant-1:VRF1, [20/0], 00:35:20, bgp-65501, external, tag 3
192.168.1.0/24, ubest/mbest: 1/0
    *via 192.168.101.232%overlay-1, [200/0], 00:00:02, bgp-100, internal, tag
65501, rwVnid: vxlan-3112963
```

Leaf 201 Site2

```
Leaf201-Site2# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.1.0/24, ubest/mbest: 1/0
    *via 192.168.101.232%overlay-1, [200/0], 00:03:02, bgp-100, internal, tag
65501, rwVnid: vxlan-3112963
```

```
192.168.2.0/24, ubest/mbest: 1/0
    *via 172.16.2.1%Tenant-1:VRF1, [20/0], 00:38:25, bgp-100, external, tag 30
```

上記のように、プレフィックス 192.168.2.0/24 は、スパイン間で確立され、ローカル BL ノードにインストールされた、VPNv4 コントロールプレーン セッションを経由して、Site1 で学習されます。このローカル BL ノードは、Site2 で BL ノードに割り当てられた外部 TEP アドレス（192.168.103.229）を表すネクストホップを持ち、Site2 で VRF1 を表す固有の VXLAN ID（vxlan-2359299）を使用するようになっています。同様の考慮事項が、Site1 から Site2 にアドバタイズされる 192.168.1.0/24 にも適用されます。

ポリシー適用の観点から、コントラクトは常に外部ネットワークからトラフィックを受信する BL ノードに着信で適用されます（図 121）。

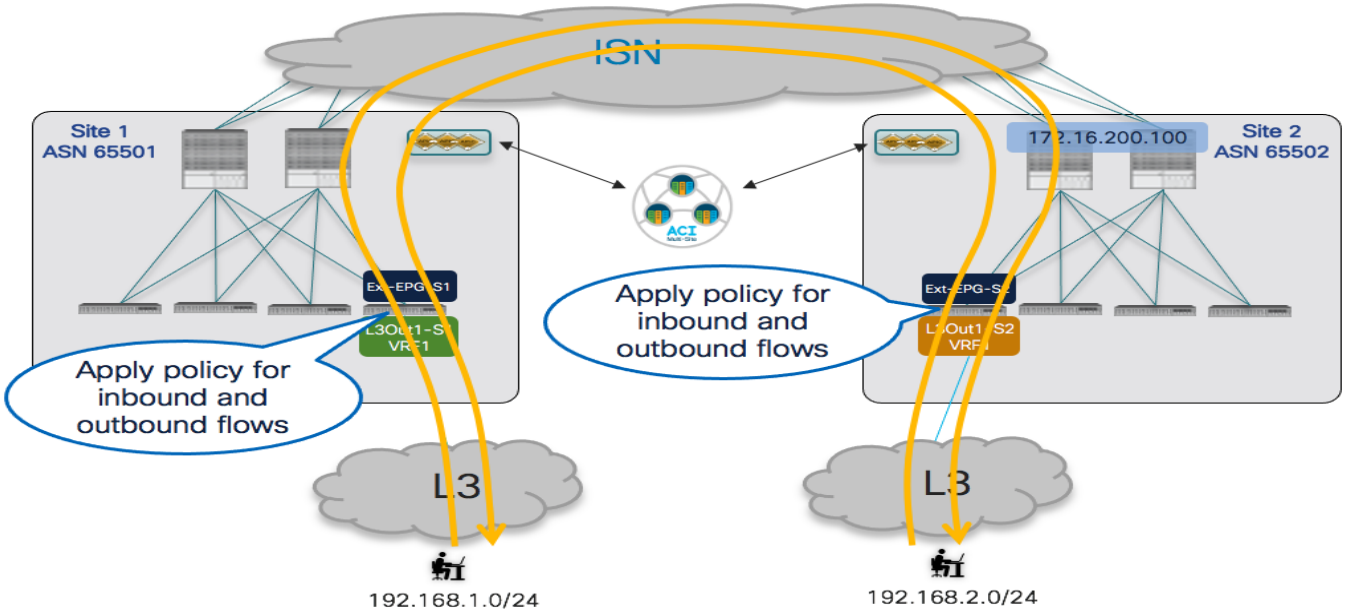


図 121.
BL ノードで常に着信に適用されるセキュリティ ポリシー

これを可能にするには、次のコマンドを使用して確認できるように、各 BL ノードがローカルおよびリモートの外部プレフィックスのクラス ID を認識している必要があります。

Leaf 104 Site1

```
Leaf104-Site1# vsh -c 'show system internal policy-
mgr prefix'
Vrf-Vni VRF-Id Table-Id Table-State  VRF-
Name                    Addr                                Class Shared Remote Complete
======= ======  ========== =======  ============================
================================ ====== ====== ====== ========
3112963 41      0x29           Up      Tenant-
1:VRF1                                    192.168.1.0/24  49156   True   True   False
3112963 41      0x29           Up      Tenant-
1:VRF1                                    192.168.2.0/24  16392   True   True   False
```

Leaf 201 Site2

```
Leaf201-Site2# vsh -c 'show system internal policy-mgr prefix'
```

```
Vrf-Vni VRF-Id Table-Id Table-State  VRF-
Name                    Addr                                  Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2359299 31      0x1f           Up      Tenant-
1:VRF1                                      192.168.2.0/24  49161   False  True   False
2359299 31      0x1f           Up      Tenant-1:VRF1
```

上記のように、プレフィックスのクラスIDはサイトごとに異なり、ローカルExt-EPGに関連付けられた値と、コントラクト関係の確立の結果として作成されるシャドウExt-EPGに対応します。

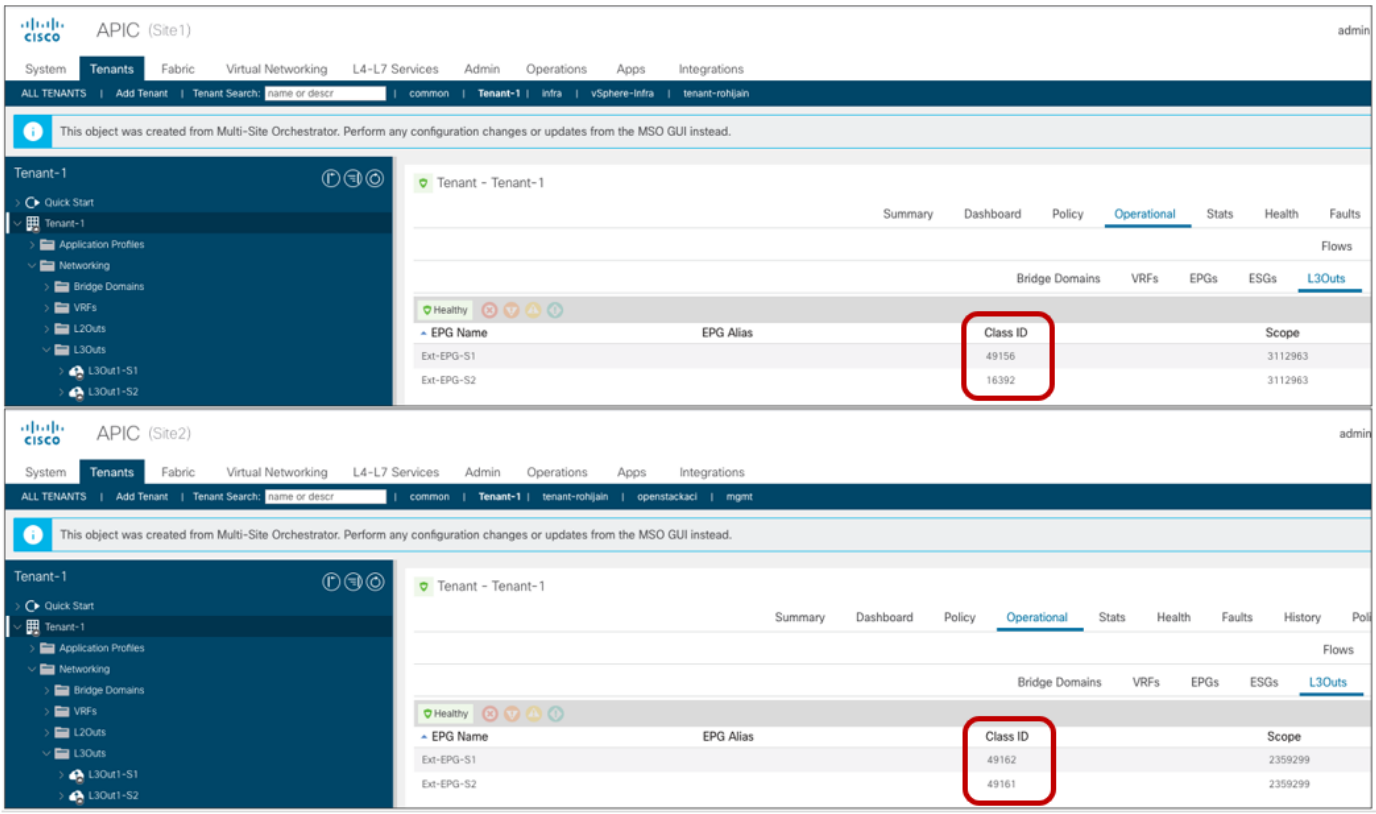


図 122.
各サイトのローカルおよびシャドウExt-EPGのクラスID値

上記に示すように、Ext-EPG 間のコントラクトの確立により、各リモートAPIC ドメインで、関連付けられたExt-EPGを含む、シャドウL3Out全体がインスタンス化されます（L3Out-S2はSite1のAPICのシャドウ オブジェクトで、L3Out-S1はSite2のAPICのシャドウ オブジェクトです）。これらのシャドウEPGオブジェクトを作成すると、Ext-EPGで設定された特定のIPプレフィックスを適切なClass-ID値にマッピングできます。

リモート外部プレフィックスを正しいClass-ID値に関連付けられることは、BLノードに着信ポリシーを適用するために重要です。これは、Site1とSite2のBLノードのゾーン分割ルールテーブルを確認することで確認できます。

Leaf 104 Site1

```
Leaf104-Site1# show zoning-rule scope 3112963
+ --------- + -------- + -------- + ---------- + ---------- ------ + --------- + --------- +
------------ + --------- -+ ---------------------- +
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+---------------+---------+---------+-------------+-
---------+----------------------+
|   4156  |   0    |   0    | implicit |    uni-dir    | enabled | 3112963
|            | deny,log |   any_any_any(21)    |
|   4232  |   0    |   0    | implarp  |    uni-dir    | enabled | 3112963
|            |  permit  |  any_any_filter(17)  |
|   4127  |   0    |   15   | implicit |    uni-dir    | enabled | 3112963
|            | deny,log | any_vrf_any_deny(22) |
|   4124  |   0    | 49154  | implicit |    uni-dir    | enabled | 3112963
|            |  permit  |   any_dest_any(16)   |
|   4212  |   0    | 49153  | implicit |    uni-dir    | enabled | 3112963
|            |  permit  |   any_dest_any(16)   |
|   4234  |   0    | 32771  | implicit |    uni-dir    | enabled | 3112963
|            |  permit  |   any_dest_any(16)   |
|   4199  | 49156  | 16392  | default  | uni-dir-ignore | enabled | 3112963 | Tenant-1:C1
|  permit  |    src_dst_any(9)    |
|   4213  | 16392  | 49156  | default  |     bi-dir    | enabled | 3112963 | Tenant-1:C1
|  permit  |    src_dst_any(9)    |
+---------+--------+--------+----------+---------------+---------+---------+-------------+-
---------+----------------------+
```

注： 3112963は、Site1 の VRF1 のセグメント ID 値です（この情報は、「show vrf<VRF_name> detail」コマンドで取得できます）。

Leaf 201 Site2

```
Leaf201-Site2# show zoning-rule scope 2359299
+ --------- + -------- + -------- + ---------- + ---------- ------ + --------- + --------- +
------------ + --------- -+ ---------------------- +
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+---------------+---------+---------+-------------+-
---------+----------------------+
| 4183 | 0 | 0 | implicit | uni-dir | enabled | 2359299 | | deny,log | any_any_any(21) |
|   4108  |   0    |   0    | implarp  |    uni-dir    | enabled | 2359299
|            |  permit  |  any_any_filter(17)  |
|   4213  |   0    |   15   | implicit |    uni-dir    | enabled | 2359299
|            | deny,log | any_vrf_any_deny(22) |
|   4214  |   0    | 32772  | implicit |    uni-dir    | enabled | 2359299
|            |  permit  |   any_dest_any(16)   |
|   4212  |   0    | 32771  | implicit |    uni-dir    | enabled | 2359299
|            |  permit  |   any_dest_any(16)   |
|   4201  |   0    | 16392  | implicit |    uni-dir    | enabled | 2359299
|            |  permit  |   any_dest_any(16)   |
|   4109  | 49161  | 49162  | default  |     bi-dir    | enabled | 2359299 | Tenant-1:C1
|  permit  |    src_dst_any(9)    |
```

```
|    4182   | 49162   | 49161   | default   | uni-dir-ignore | enabled | 2359299 | Tenant-1:C1
|  permit   |     src_dst_any(9)     |
+---------+-------+--------+---------+---------------+---------+---------+-------------+-
---------+----------------------+
```

注： 2359299 は、Site2 の VRF1 のセグメント ID 値です。

サイト間中継ルーティング接続（VRF 間）

図 123 に示す共有サービス シナリオでは、サイト間中継ルーティング通信も可能です。この場合、各サイトに展開された L3Out は異なる VRF の一部です。

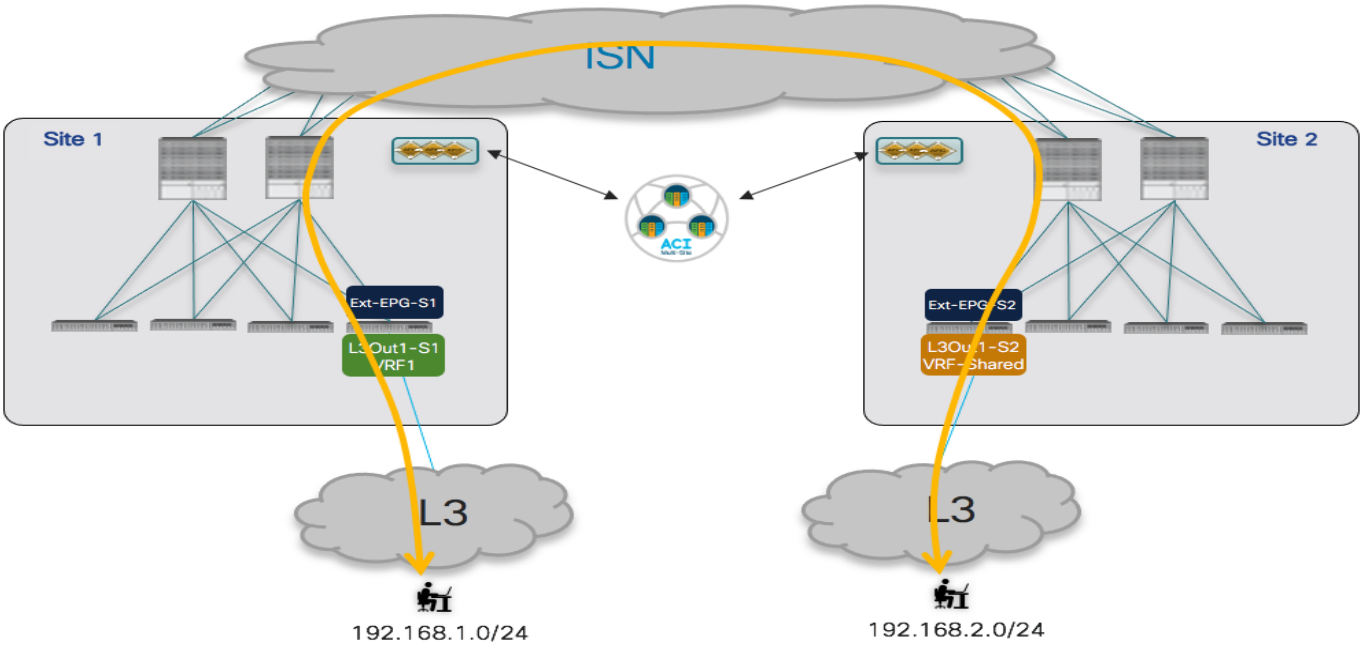


図 123.
サイト間中継ルーティング接続（VRF 間）

必要なプロビジョニング手順は、前述の VRF 内シナリオとよく似ています。

- トラフィックの分類に使用される IP プレフィックスに関連付けられた Ext-EPG のフラグを適切に設定します。これらのフラグの設定は、VRF 間の IP プレフィックスをリークし、リモートBL ノードにこれらのプレフィックスのクラス ID 値を適切にインストールするために必要です。

Ext-EPG-S1 (Site 1)

Ext-EPG-S2 (Site 2)

図 124.
ルートリークおよびクラス IDインストールのフラグの設定

- 各 L3Out で学習したプレフィックスをリモート L3Out からアドバタイズできることを確認します。これには、図 119 に示す VRF 内の使用例とまったく同じ設定が必要です。
- Ext-EPG 間にセキュリティ コントラクトを適用します。これは、図 120 に示されているのと同じ設定で実行できます。ただし、VRF が同じテナントの一部であるか、または個別のテナントで定義されているかによって、コントラクト C1 の範囲を「テナント (Tenant)」または「グローバル (Global)」に設定する必要がある点が異なります。

図 125 に示すように、Site1 の BL ノードが Site2 のリモートBL ノードへのトラフィックをカプセル化するという事実を利用して、サイト間中継ルーティング通信がファブリック全体で確立されます。その際、リモートファブリックの共有 VRF を表す VRF セグメントID を使用します。またこの逆も成り立ちます。

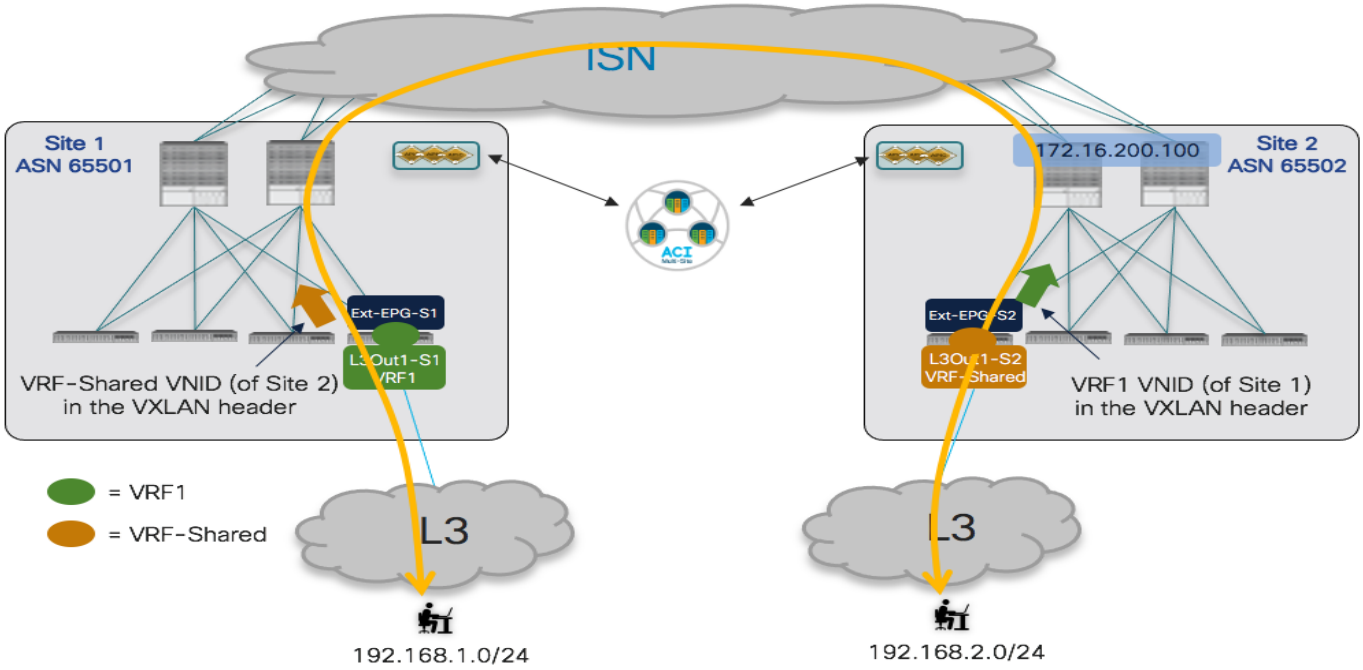


図 125.
リモート サイトへのトラフィック送信時のリモート VRF セグメント ID の使用

このことは以下の出力により確認できます。

```
Leaf 104 Site1
Leaf104-Site1# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.1.0/24, ubest/mbest: 1/0
    *via 172.16.1.1%Tenant-1:VRF1, [20/0], 00:35:20, bgp-65501, external, tag 3
192.168.2.0/24, ubest/mbest: 1/0
```

```
    *via 192.168.103.229%overlay-1, [200/0], 01:12:10, bgp-65501, internal, tag
100, rwVnid: vxlan-2097156
```

注： 2097156 は、Site2 の VRF 共有のセグメント ID 値です（この情報は、「show vrf<VRF_name> detail」コマンドを使用して取得できます）。

Leaf 201 Site2

```
Leaf201-Site2# show ip route vrf Tenant-1:VRF-Shared
IP Route Table for VRF "Tenant-1:VRF-Shared"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

192.168.1.0/24, ubest/mbest: 1/0
    *via 192.168.101.232%overlay-1, [200/0], 00:03:02, bgp-100, internal, tag
65501, rwVnid: vxlan-3112963
192.168.2.0/24, ubest/mbest: 1/0
    *via 172.16.2.1%Tenant-1:VRF-Shared, [20/0], 01:16:31, bgp-100, external, tag 30
```

注： 3112963は、Site1 の VRF1 のセグメント ID 値です。

ポリシー適用の観点からは、図 121 に示したのと同じ動作が VRF 間シナリオでも引き続き有効です。唯一の違いは、Ext-EPG の図 124 に示す「共有セキュリティインポート (Shared Security Import)」フラグ設定の結果として、リモート外部プレフィックスのクラス ID がインストールされることです。これは、VRF 内の使用例と同じコマンドを使用して確認できます。

Leaf 104 Site1

```
Leaf104-Site1# vsh -c 'show system internal policy-
mgr prefix'
Vrf-Vni VRF-Id Table-Id Table-State  VRF-
Name                    Addr                                Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
3112963 41     0x29          Up     Tenant-
1:VRF1                                   192.168.1.0/24  10930   True   True   False
3112963 41     0x29          Up     Tenant-
1:VRF1                                   192.168.2.0/24  10934   True   True   False
```

Leaf 201 Site2

```
Leaf201-Site2# vsh -c 'show system internal policy-mgr prefix'
Vrf-Vni VRF-Id Table-Id Table-State  VRF-
Name                    Addr                                Class Shared Remote Complete
======= ======  =========== =======  ============================
================================ ====== ====== ====== ========
2097156 34     0x22          Up     Tenant-1:VRF-
Shared                                   192.168.1.0/24  5492    True   True   False
2097156 34     0x22          Up     Tenant-1:VRF-
Shared                                   192.168.1.0/24  5492    True   True   False
```

図 126 からもわかるように、ローカルおよびシャドウ Ext-EPG に割り当てられたクラス ID 値は、VRF 内の使用例で使用されているものとは異なります。 グローバルな値は、VRF 全体で一意のものにする必要があるからです。

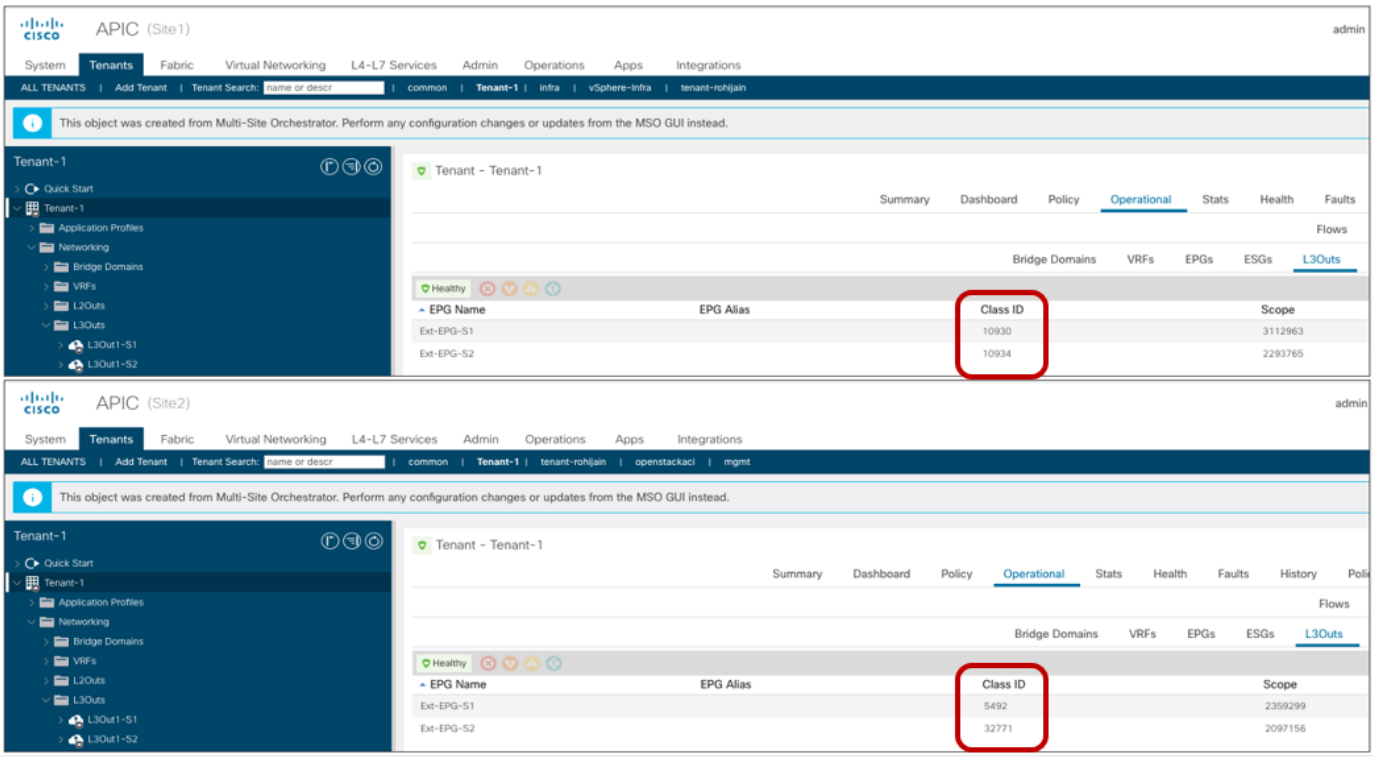


図 126.
各サイトのローカルおよびシャドウ Ext-EPG のクラス ID 値

BL ノードでのゾーン分割ルール エントリの設定により、外部ネットワークからトラフィック フローを受信する BL ノードで着信にセキュリティ ポリシーが適用されることを確認できます。

Leaf 104 Site1

```
Leaf104-Site1# show zoning-rule scope 3112963
+---------+--------+--------+----------+----------------+---------+---------+-------------+-
---------------+----------------------+

| Rule ID
| SrcEPG | DstEPG | FilterID |      Dir       |  operSt  |  Scope  |     Name    |      Actio
n     |       Priority       |

+---------+--------+--------+----------+----------------+---------+---------+-------------+-
---------------+----------------------+

|   4156  |   0    |   0    | implicit |    uni-dir     | enabled | 3112963
|             |     deny,log     |   any_any_any(21)    |

|   4232  |   0    |   0    | implarp  |    uni-dir     | enabled | 3112963
|             |      permit      |  any_any_filter(17)  |

|   4127  |   0    |   15   | implicit |    uni-dir     | enabled | 3112963
|             |     deny,log     | any_vrf_any_deny(22) |

|   4124  |   0    | 49154  | implicit |    uni-dir     | enabled | 3112963
|             |      permit      |   any_dest_any(16)   |
```

```
|   4212  |   0    | 49153  | implicit |    uni-dir     | enabled | 3112963
|            |      permit     |   any_dest_any(16)   |
|   4234  |   0    | 32771  | implicit |    uni-dir     | enabled | 3112963
|            |      permit     |   any_dest_any(16)   |
|   4213  | 10930  |   14   | implicit |    uni-dir     | enabled | 3112963
|            | permit_override |    src_dst_any(9)    |
|   4199  | 10930  | 10934  | default  | uni-dir-ignore | enabled | 3112963 | Tenant-1:C1
|      permit     |    src_dst_any(9)    |
|   4206  | 10934  | 10930  | default  |     bi-dir     | enabled | 3112963 | Tenant-1:C1
|      permit     |    src_dst_any(9)    |
+--------+-------+-------+---------+--------------+--------+--------+-----------+---------------+--------------------+
```

注： 3112963は、Site1 の VRF1 のセグメント ID 値です（この情報は、「show vrf<VRF_name> detail」コマンドで取得できます）。

Leaf 201 Site2

```
Leaf201-Site2# show zoning-rule scope 2097156
+---------+--------+--------+----------+---------------+---------+---------+-------------+-
---------+------------------------+
| Rule ID | SrcEPG | DstEPG | FilterID | Dir | operSt | Scope | Name | Action | Priority |
+---------+--------+--------+----------+---------------+---------+---------+-------------+-
---------+------------------------+
|   4182  |   0    |   0    | implicit |    uni-dir     | enabled | 2097156
|            | deny,log |    any_any_any(21)     |
|   4108  |   0    |   0    | implarp  |    uni-dir     | enabled | 2359299
|            |  permit  |  any_any_filter(17)  |
|   4190  |   0    |   15   | implicit |    uni-dir     | enabled | 2097156
|            | deny,log |  any_vrf_any_deny(22)  |
|   4198  |  5492  | 32771  | default  | uni-dir-ignore | enabled | 2097156 | Tenant-1:C1
|  permit  |     src_dst_any(9)     |
|   4176  | 32771  |  5492  | default  |     bi-dir     | enabled | 2097156 | Tenant-1:C1
|  permit  |     src_dst_any(9)     |
|   4222  |  5492  |   0    | implicit |    uni-dir     | enabled | 2097156
|            | deny,log | shsrc_any_any_deny(12) |
+---------+--------+--------+----------+---------------+---------+---------+-------------+-
---------+------------------------+
```

注： 2097156 は、Site2 の VRF 共有のセグメント ID 値です。

VRF が異なるテナントで定義されている場合、VRF 間トランジット ルーティング接続を確立するには、このセクションで説明したのと同じ設定が必要です。その場合に確認する唯一のことは、コントラクトがプロバイダー テナントの一部として範囲「グローバル」で定義されているかどうかです。

ACI マルチサイトとサービス ノードの統合

サービス ノードと ACI Multi-Site の統合の基本的な前提は、1 つ（または複数）の専用サービス ノードのセットが Multi-Site ドメインの各ファブリック部分に展開されることです。サイト間でのクラスタ化されたサービスのサポートは実際には制限されており、マルチサイト展開では最も一般的でも推奨されるアプローチでもないため、このホワイトペーパーでは考慮しません。

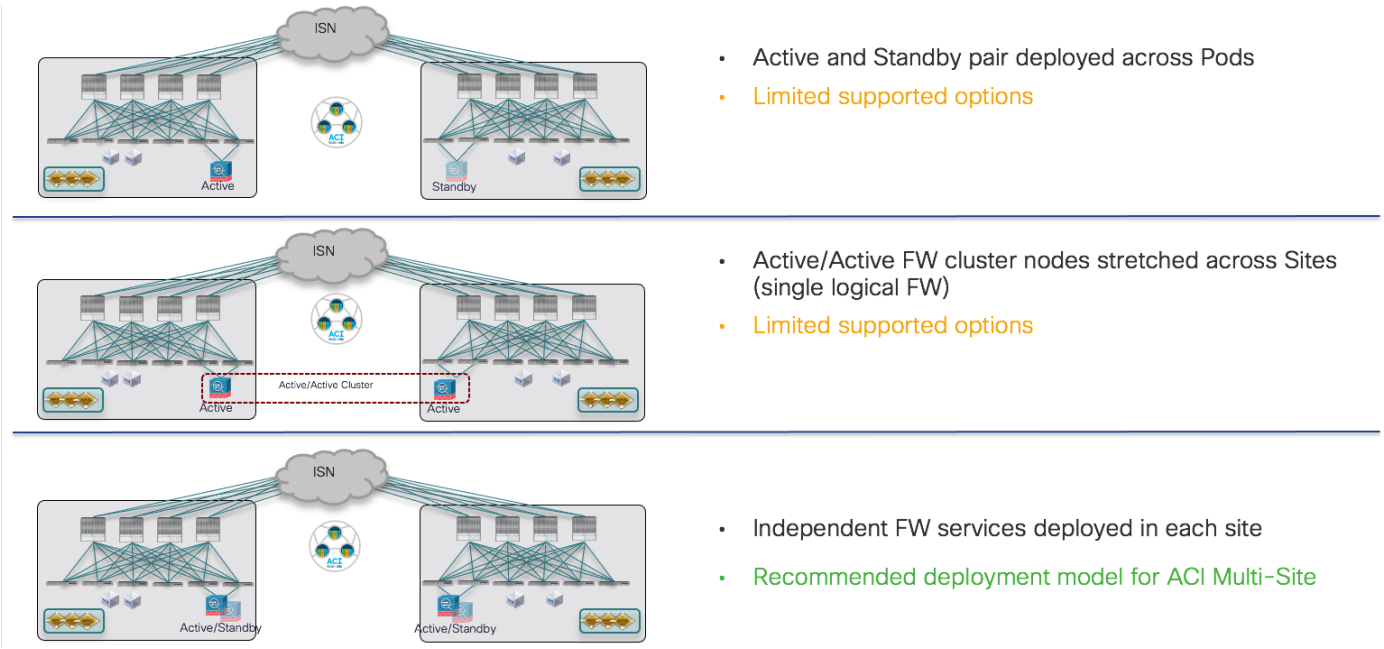


図 127.
ACI マルチサイトとサービス ノードの統合

最初の直接的な結果として、特定の各サービス ノードの機能を各ファブリックに最も復元力のある方法で導入する必要があります。図 128 は、各ファブリック内でローカルサービス ノードの復元力を実現するための3 つの異なる方法を示しています（図の特定の例はファイアウォール サービスを参照していますが、他のタイプのサービス ノードにも同じ考慮事項が適用されます）。

- アクティブ/スタンバイ クラスタの展開：これは通常、クラスタ全体が単一の MAC/IP アドレス ペアとして認識されることを意味します。これは、ノードスイッチ オーバーイベントの結果、マーケットに、アクティブな MAC アドレスを保たない固有のサービス ノードが存在する場合でもそうです（このケースについては、以下で詳しく説明します）。
- アクティブ/アクティブクラスタの導入：Cisco ASA/FTD 導入の特定のケースでは、単一の MAC/IP アドレスペア（クラスタに属するすべてのノードにより所有）によってクラスタ全体を参照できます。マーケットの他のアクティブ/アクティブ実装では、各クラスタ ノードが専用の一意の MAC/IP ペアを所有することになります。

注： Multi-Site ドメインのファブリック部分に A/Aクラスタを展開するには、そのサイトで少なくとも ACI リリース 5.2(2e) を使用する必要があります。

- 各ファブリックに複数の独立したサービス ノードを導入し、各ノードを一意の MAC/IP アドレスペアで参照する。

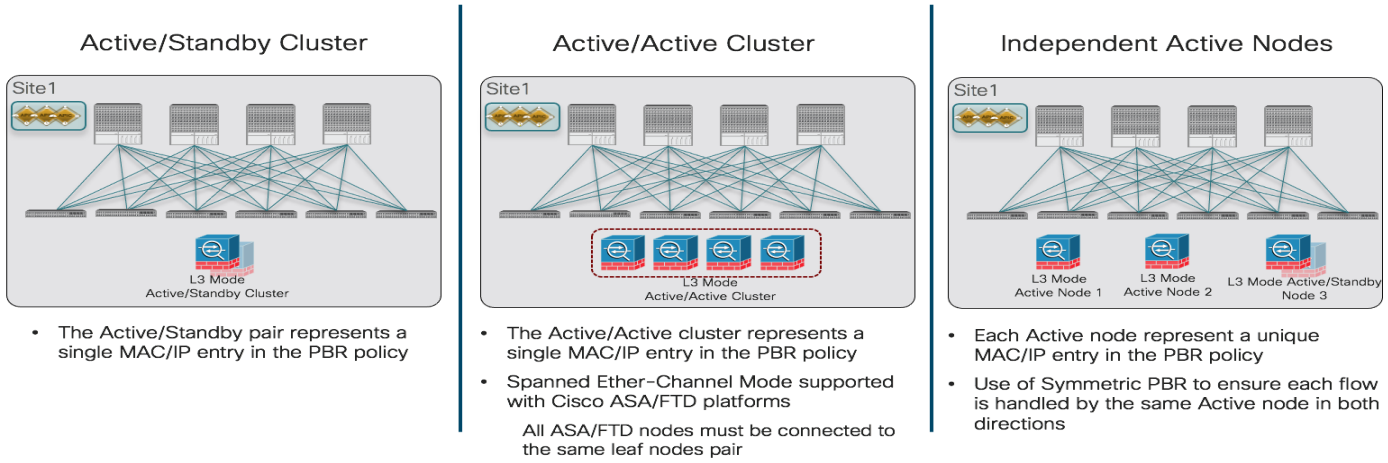


図 128.
ACI ファブリックでのサービス ノード機能の復元力のある展開のさまざまなオプション

注： このホワイトペーパーでは、最も一般的な導入シナリオであるレイヤ 3 モードでのサービス ノードの導入に焦点を当てています。サービス グラフ設定は、レイヤ1 およびレイヤ 2 PBr の使用もサポートします。詳細については、以下のペーパーを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739971.html

選択した特定の冗長性展開オプションとは別に、サービス ノードと関連する PBR ポリシーを定義するために必要な設定は、Multi-Site ドメインの各 ACI ファブリック部分に対して、常に APIC レベルで実行する必要があります。次のセクションで詳しく説明するように、図 128 に示すさまざまな冗長オプションは、APIC で作成された特定のサービス ノードおよびPBR ポリシー設定に基づいて展開できます。この設定は、EPG 間の通信に 1 つ以上のサービス ノードを挿入する必要があるかどうかによっても異なるため、これらのシナリオは個別に考慮されます。

サービス ノード統合オプションの詳細については、以下のペーパーを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-743107.htm

単一のサービス ノードの挿入に対するマルチサイトでの PBR を使用したサービス グラフ

最初に考慮すべき使用例は、2 つの EPG 間で確立されたトラフィック フローをリダイレクトする単一のサービス ノードの挿入です。EPG が内部エンドポイント用に展開されているか、L3Outs（Ext-EPG）に関連付けられているか、および EPG が同じ VRF の一部であるか、異なる VRF（および/またはテナント）であるかに応じて、さまざまなシナリオを展開できます。

特定の使用例とは関わりなく、最初の手順は、Multi-Site ドメインの一部である各ファブリックの論理サービス ノードを定義することです。次の図 129 に示すように、この単一の論理サービス ノードの作成は、NDO からではなく、APIC コントローラレベルで実行する必要があります。次の特定の例では、各サイトの 2 つのファイアウォール ノード（通常は「コンクリート デバイス」と呼ばれます）を利用しますが、異なるタイプのサービス ノード（サーバー ロードバランサなど）を導入する場合も同様の考慮事項が適用されます。

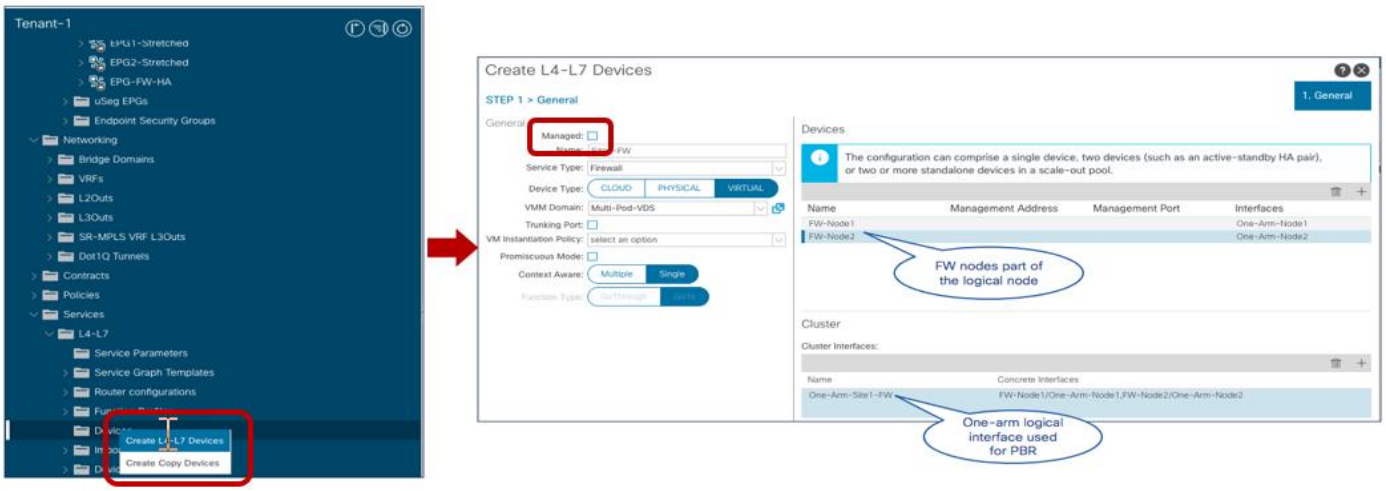


図 129.
APIC での単一サービス ノードの導入

注：上記の設定は、Multi-Site ドメインの一部であるファブリックを管理するすべての APIC コントローラで実行する必要があります。また、[管理対象（Managed)] フラグをオフにすることで、サービス ノードを [管理対象外（unmanaged)] として設定する必要があります。これは、マルチサイトとの統合の唯一のオプションです。

上記の 2 つの具体的なファイアウォール ノードは、クラスタの一部（アクティブ/スタンバイまたはアクティブ/アクティブ）として、または選択した特定の冗長オプション（前の図 128 に示すモデルの 1 つ）に基づいて独立したノードとして導入されます。Cisco ASA/FTDファイアウォールデバイスを使用してクラスタ構成を構築する方法の詳細については、以下のドキュメントを参照してください。

https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html

https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

特定の冗長性モデルとは別に、各 APIC コントローラは、単一の論理ワンアーム インターフェイス（「One-Arm-Site1-FW」という名前）を介してファブリックに接続されている単一の論理サービス ノード（上記の図では「Site1-FW」という名前）を NDO に公開します。 。これらの特定のオブジェクトは、このセクションで後述するように、NDO で PBR 設定を使用してサービス グラフをプロビジョニングするときに使用されます。

ファブリックごとに論理ファイアウォール サービス ノードを定義したら、APIC レベルで実行する必要がある2番目の設定手順は、PBR ポリシーの定義です。図 130 に、Ciscoファイアウォールでサポートされるアクティブ/スタンバイおよびアクティブ/アクティブ クラスタ オプションの PBR ポリシーの作成を示します。この場合、単一の MAC/IP ペアがファイアウォール クラスタ全体（つまり、クラスタ内のすべてのアクティブ ファイアウォール ノードに割り当てられます）。この場合の各ファブリックのリダイレクションは、特定の MAC/IP 値に対して常に実行されます。この値は、単一の具象デバイス（アクティブ/スタンバイ クラスタ）または多数の具象デバイス（独立したノード）に導入できます。

注： ACI リリース 5.2(1) 以降、PBR ポリシーでの MAC アドレスの設定は必須ではなくなり、指定された IP アドレスに関連付けられた MAC を動的に検出できるようになりました。この新しい機能を使用するには、PBR ポリシーのトラッキングを有効にする必要があります。この新しい PBR 機能の詳細については、以下のペーパーを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739971.html

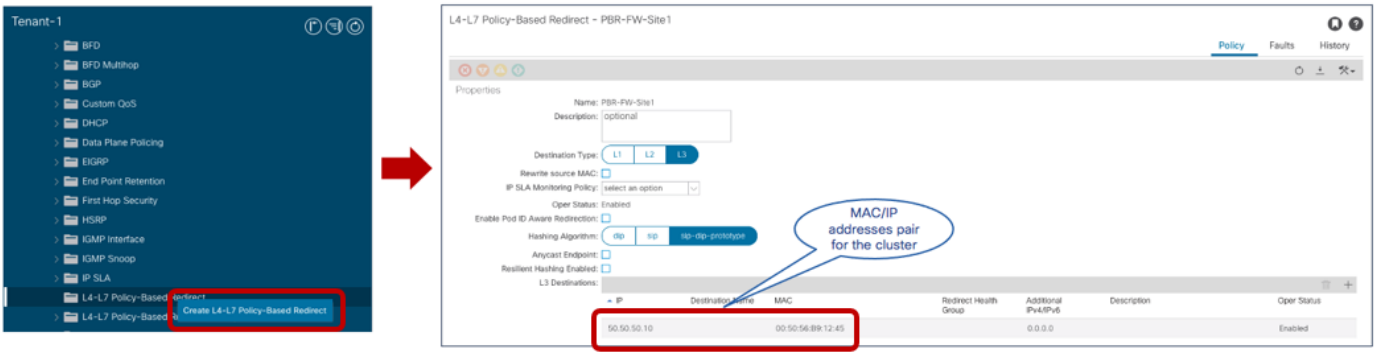


図 130.
ファイアウォール クラスタの PBR ポリシーの定義（単一の MAC/IP ペア）

図 131 は、論理ファイアウォール サービス ノードが個別の MAC/IP アドレスペアとして認識される場合に必要な PBR ポリシーの代わりを示しています。これは、各ファブリックに独立したサービス ノードを導入する場合、または一部のサードパーティ製ファイアウォール クラスタの実装でも同様です。この場合、トラフィックのリダイレクションはフロー単位で異なる MAC/IP アドレスに行われ、「対称 PBR」と呼ばれる機能（EX モデル以降の ACI リーフ ノードにおいてはデフォルトで有効になっている）により、両方のレッグが同じトラフィックのフローは常に同じ MAC/IP ペアにリダイレクトされます。

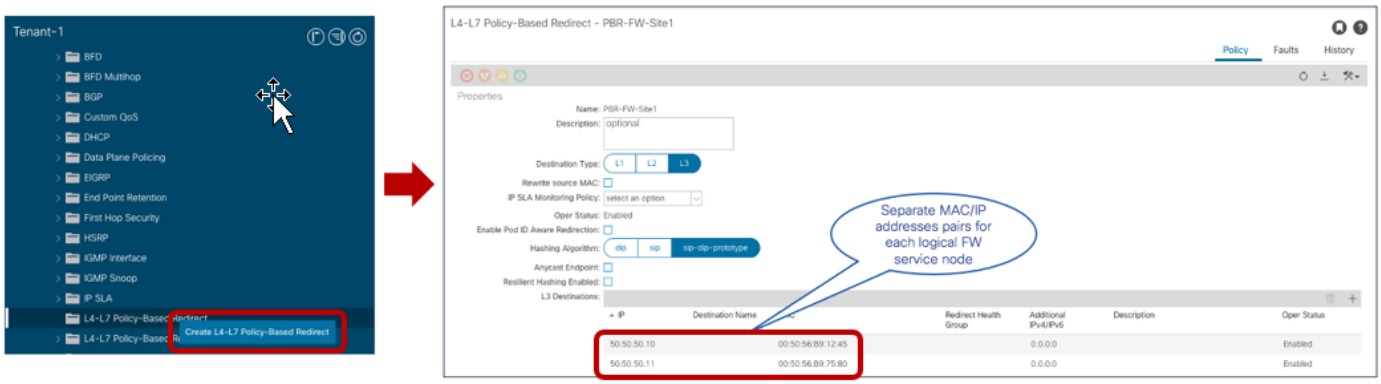


図 131.
「独立した」ファイアウォール ノードの PBR ポリシーの定義（複数の MAC/IP ペア）

作成された PBR ポリシーの名前（図 130と図 131 の特定の例の「PBR-FW-Site1」）は、PBR 設定を使用したサービス グラフのプロビジョニングに使用するために Nexus Dashboard Orchestrator に公開されます。

注： Nexus Dashboard Orchestrator ドメインのファブリック部分の他の APIC コントローラでも同様の設定が必要です。

MAC/IP アドレスペアにトラフィックをリダイレクトするように PBR ポリシーを定義し、前述の新しい 5.2(1) ダイナミック MAC ディスカバリ機能の使用から独立に、関連する「トラッキング」設定を作成することを推奨します。ファブリックがサービス ノードの状態を常に確認できるようにするためです。複数の MAC/IP ペアを使用する場合、特定の MAC/IP 値に関連付けられた障害が発生したノードがトラフィック リダイレクションに使用されないようにするために、トラッキングの重要性が明らかです。ただし、ファブリック内の複数のノードが同じ MAC/IP 値を使用するシナリオ（Cisco アクティブ/アクティブ ファイアウォール クラスタなど）で

も、トラッキングを使用することで収束が改善されます。ACI ファブリックでサービス ノード トラッキングを設定する方法の詳細については、次のドキュメントを参照してください。

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/5-x/l4-l7-services/cisco-apic-layer-4-to-layer-7-services-deployment-guide-50x/m_configuring_policy_based_redirect.html

PBr でサービス グラフを使用してファイアウォール サービス ノードを挿入するこのセクションで説明する使用例は、図 132 で強調表示されています。

図 132.
ファイアウォール サービス ノードの挿入に関する PBR を使用したサービス グラフ

上記のように、コンシューマー EPG とプロバイダー EPG は同じ VRF（およびテナント）の一部にすることも、または別の VRF（および必要に応じてテナント）に導入することもできます。また、最も一般的な導入モデルでは、ファイアウォール ノードはレイヤ 3 モードで導入され、サービスBD にワンアームモードで接続されます。これにより、ファイアウォールのルーティング設定が簡素化されます（サービス BD の IP アドレスを指す単純なスタティック デフォルト ルートは必要）が、必要に応じてファイアウォールの内部インターフェイスと外部インターフェイスを個別の BD に接続することもできます（ツーアーム モード）。

注： PBR でのサービス グラフを使用したサービス ノードの挿入は、サイト間中継ルーティングの使用例（つまり、L3Out から L3Out への通信）ではサポートされません。したがって、「サイト間トランジット ルーティングコネクティビティ（Intra-VRF）」および「サイト間トランジット ルーティングコネクティビティ（Inter-VRF）」セクションで前述したように、異なるサイトで定義された L3Out 間には、「通常の」ACI コントラクトのみを適用できます。

ノースサウス トラフィック フローのファイアウォール挿入（VRF 内）

プロビジョニングする最初の使用例は、VRF 内ノースサウス接続用のファイアウォール サービスの挿入を必要とする使用例です。

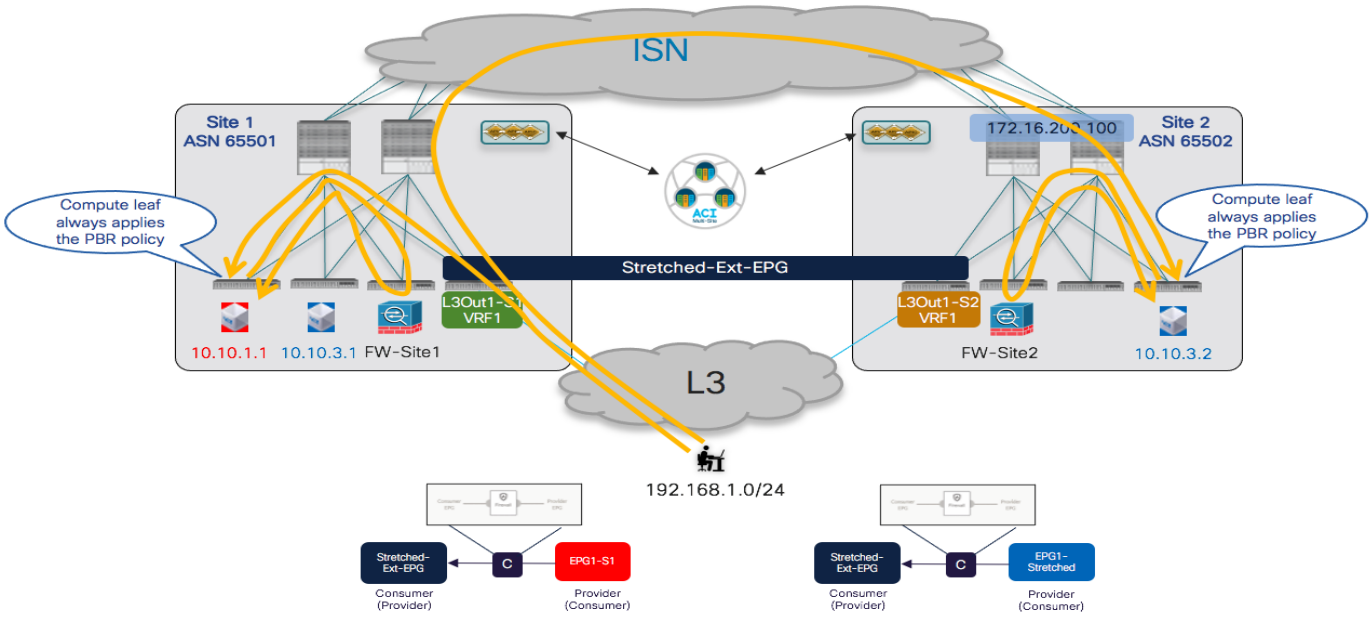


図 133.
着信トラフィック フローのコンピューティング リーフ ノードに適用される PBR ポリシー

図 133 に、トラフィックを受信する特定の L3Out に関係なく、すべての着信トラフィック フローのコンピューティング リーフ ノードに、どのように PBR ポリシーが常に適用されるかを示します。この動作では、VRF で「ポリシー制御適用方向 (Policy Control Enforcement Direction)」を「入力 (Ingress)」として設定する必要があります。これは、APIC または NDO で作成されたすべての VRF のデフォルト値です。

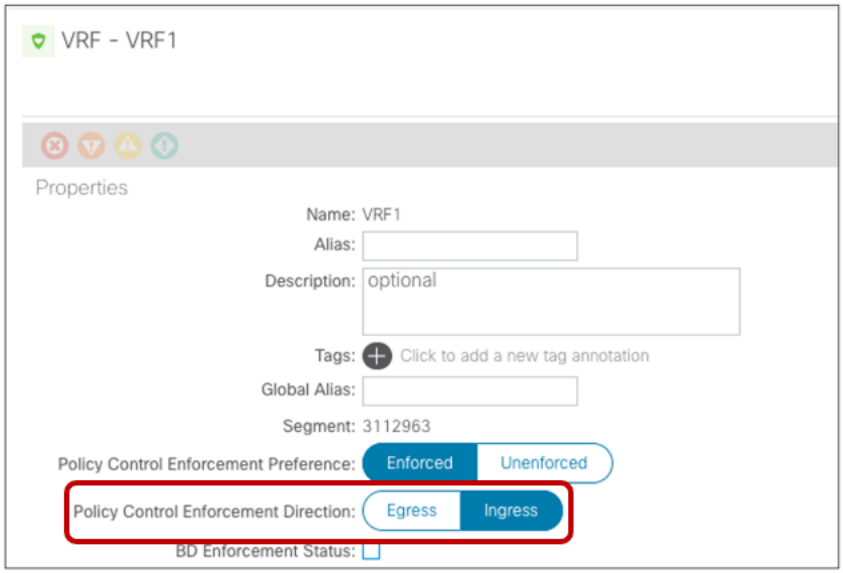


図 134.
ポリシー制御適用方向のデフォルトの VRF 設定

発信トラフィック フローにも同じ動作が適用されます。これは、着信フローにすでに使用されている同じファイアウォール サービス ノードに対してリダイレクションが発生することを保証する重要な機能です（利用されるファイアウォール サービスは、内部エンドポイントが接続されている同じファブリック内に常に存在します）。）。

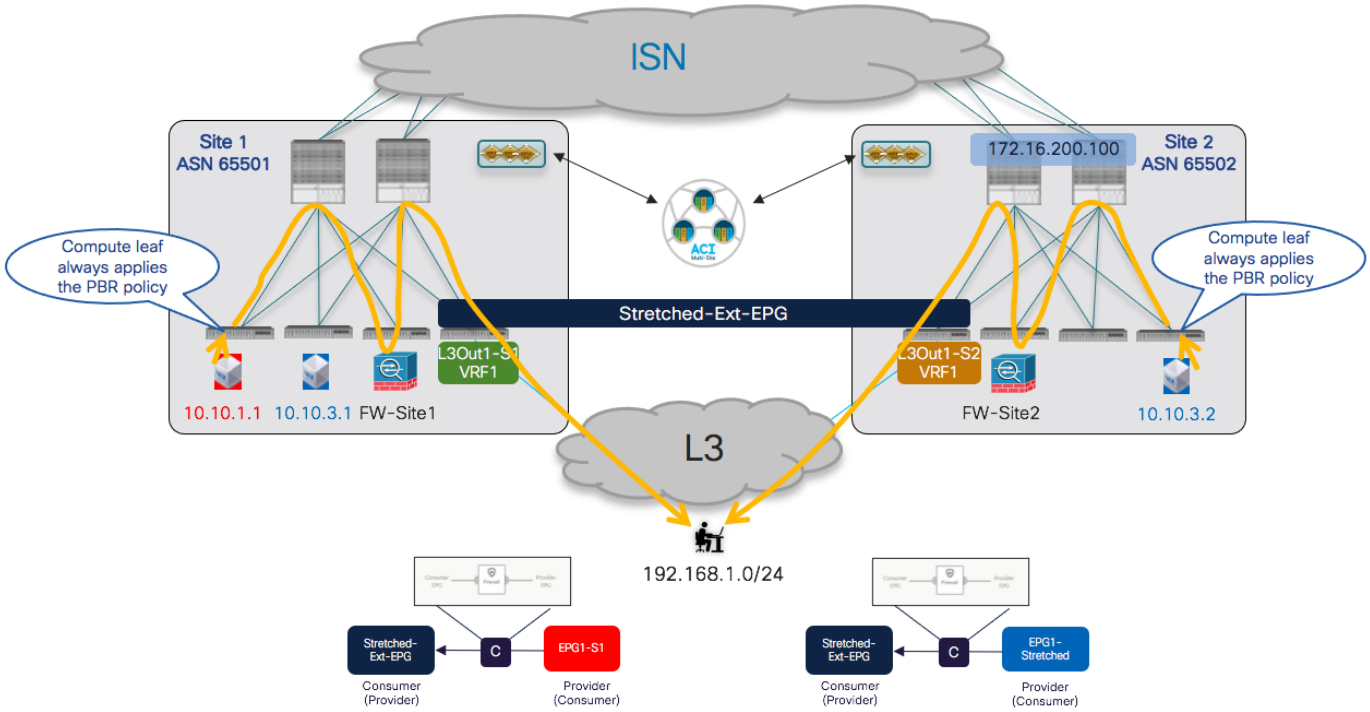


図 135.
発信トラフィック フローのコンピューティング リーフ ノードに適用される PBR ポリシー

このことが、外部デバイスとの通信に使用される特定の L3Out 接続とは無関係に常に成り立つことに注意してください。エンドポイント 10.10.3.2 からの発信トラフィックは、着信フローが L3Out Site1 で受信されていても、通常はローカルの L3Out を利用します（前の図 133 を参照）。

ノースサウス トラフィック フロー（VRF 内）のファイアウォールを統合するためにNDO で実行するプロビジョニング手順を以下に説明します。

- コンシューマーおよびプロバイダー BD のサブネットを設定して、各サイトの L3Out からアドバタイズできるようにします。これには、前の「外部レイヤ 3 ドメインへの接続」のセクションで説明したように、BD サブネットを「外部アドバタイズ (“Advertised Externally)」として設定し、プレフィックスをアドバタイズする特定の L3Out にマッピングする必要があります。
- 着信トラフィックを適切に分類するように外部 EPG を設定します。ストレッチされた Ext-EPG が展開されていると仮定すると、関連する「外部 EPG の外部サブネット (External Subnets for External EPGs)」フラグセットで「キャッチオール」0.0.0.0/0 プレフィックスを指定するのが一般的です。
- 各ファブリックに展開されたファイアウォール ノードの接続に使用される「サービス BD」を定義します。この BD は、すべてのサイトに関連付けられたテンプレートでNDO からプロビジョニングする必要があります。BD はレイヤ 2 ストレッチ オブジェクトとして設定されますが、BUM トラフィック転送を有効にする必要はありません（この特定の BD のクロスサイト トラフィック フラッディングを防ぐことができます）。また、この BD に接続されているファイアウォール ノードの EPG を設定する必要もありません。これは、サービス グラフを展開するときに自動的に作成されるためです。

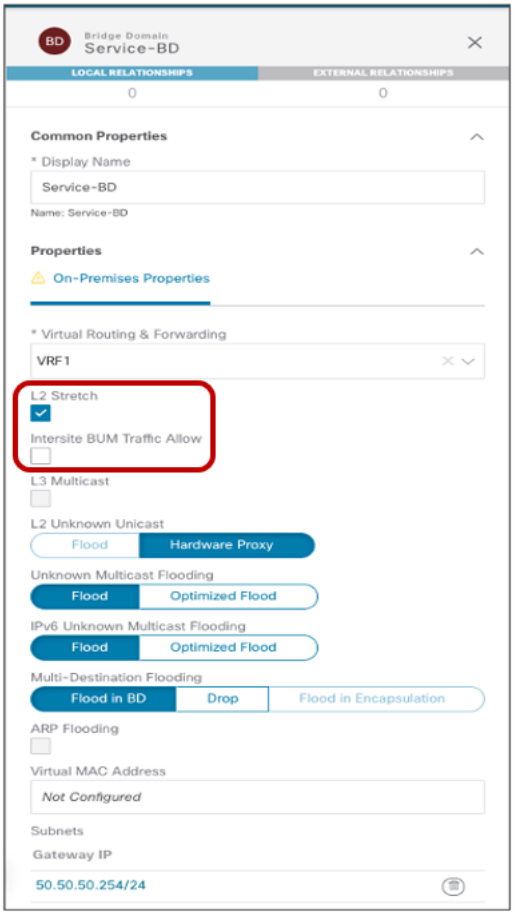


図 136.
ファイアウォール「サービス BD」のプロビジョニング

注： この例では、ファイアウォールが「ワンアーム」モードで設定されているため、単一の「サービス BD」が導入されています（図 130 を参照）。代わりに、ファイアウォールが「ツーアーム」モードで展開された場合は、2 つの個別の「サービス BD」が各ファイアウォール インターフェイスに 1 つずつプロビジョニングされます。また、このドキュメントの作成時点では、L3Out 接続を介してファブリックに接続されているサービス ノードをサービス グラフに挿入することはサポートされていません。

- Nexus Dashboard Orchestrator でファイアウォールを挿入するためのサービス グラフを作成します。異なるファブリックに接続されたエンドポイント間の通信にサービス ノードを挿入する必要がある場合、サービス グラフは、サイトドメイン（サービス グラフは「ストレッチ」オブジェクトとしてプロビジョニングされます）。図 137 に示すように、サービス グラフの設定は 2 つの部分でプロビジョニングされます。最初にグローバル テンプレート レベルで、挿入するサービス ノードを指定します（この例ではファイアウォール）。次に、サイト レベルで、APIC で定義された特定の論理ファイアウォールデバイスをマッピングします。これは Nexus Dashboard Orchestrator に公開されます（前の図 129を参照）。

図 137.
NDO でのサービス グラフの定義

- コントラクトを定義し、サービス グラフに関連付けます。コントラクトは通常、すべてのサイトにマッピングされたテンプレートで定義されます。図 138 の例では、すべてのトラフィックがファイアウォールにリダイレクトされるように「すべて許可 (Permit-All)」フィルタがコントラクトに関連付けられています。目的がファイアウォールに特定のトラフィック フローだけをリダイレクトすることである場合は、この動作を変更して、フィルタをより具体的にすることができます。

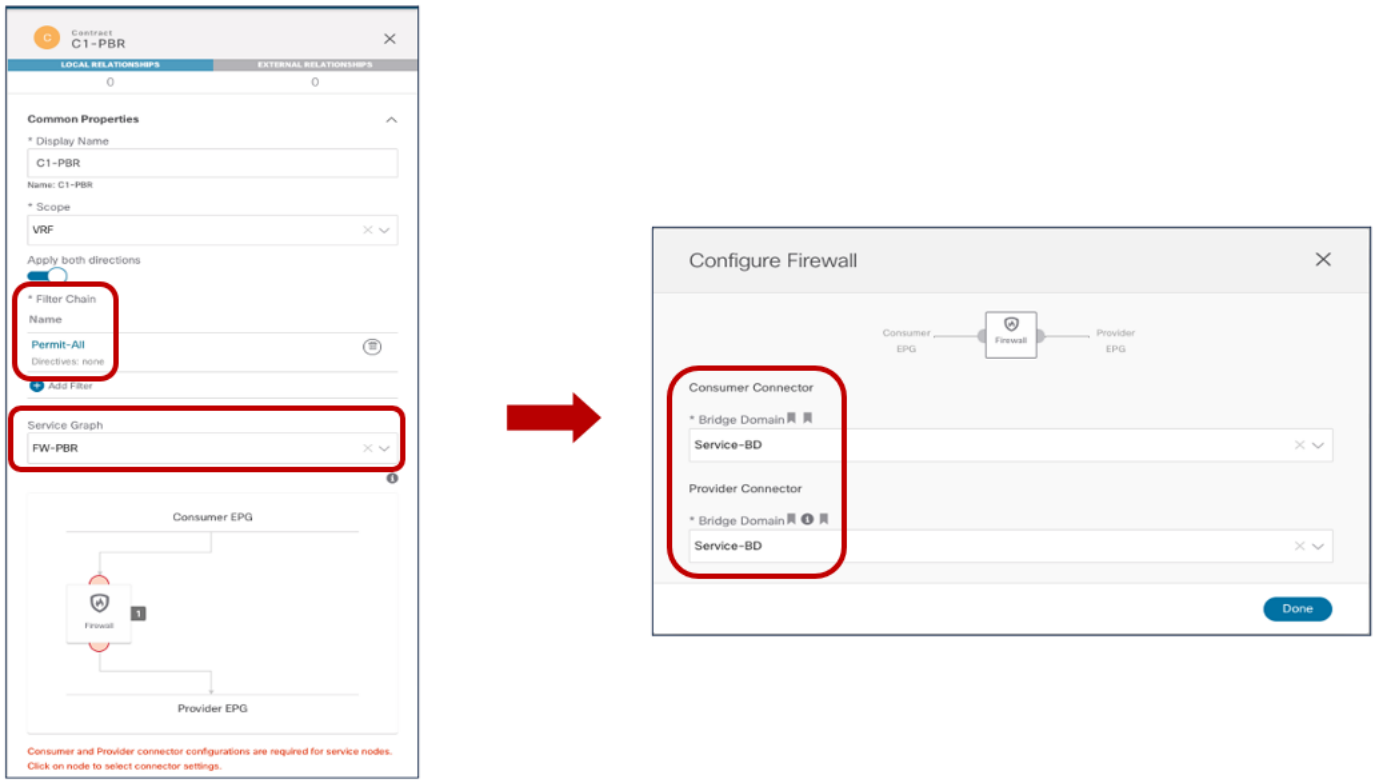


図 138.
関連付けられたサービス グラフとのコントラクトの定義（グローバル テンプレート レベル）

また、サービス グラフがコントラクトに関連付けられると、ファイアウォール論理ノードが接続されている BD を指定する必要があります。この例では、ファイアウォールはワンアーム モードで接続されているため、コンシューマーとプロバイダーの両方のファイアウォール コネクタ（インターフェイス）に同じ「サービス BD」を指定できます。また、「サービス BD」はグローバル テンプレート レベルでコネクタに関連付ける必要があります。これが、すべてのサイトで使用可能なストレッチ オブジェクトとして BD をプロビジョニングする必要がある主な理由です。

また、PBR ポリシーを各サービス ノードインターフェイス（コンシューマーおよびプロバイダーコネクタ）に関連付けるために、サイト ローカル レベルで設定を適用する必要があります。図 139 に示すように、サービス ノードが1アームモードで接続されている特定の例では、同じPBR ポリシーが両方のコネクタに適用されますが、ファイアウォールがツーアームモードで接続されている場合は適用されません。また、特定のサービス グラフの導入では、 1 つのインターフェイス（つまり、トラフィックの特定の方向）にのみ PBR ポリシーを適用する必要があり、両方には適用しないことがあります（たとえば、リターン トラフィックのみがサーバー ファームから発信される SLB導入の場合）。 SLBノードにリダイレクトする必要があります。

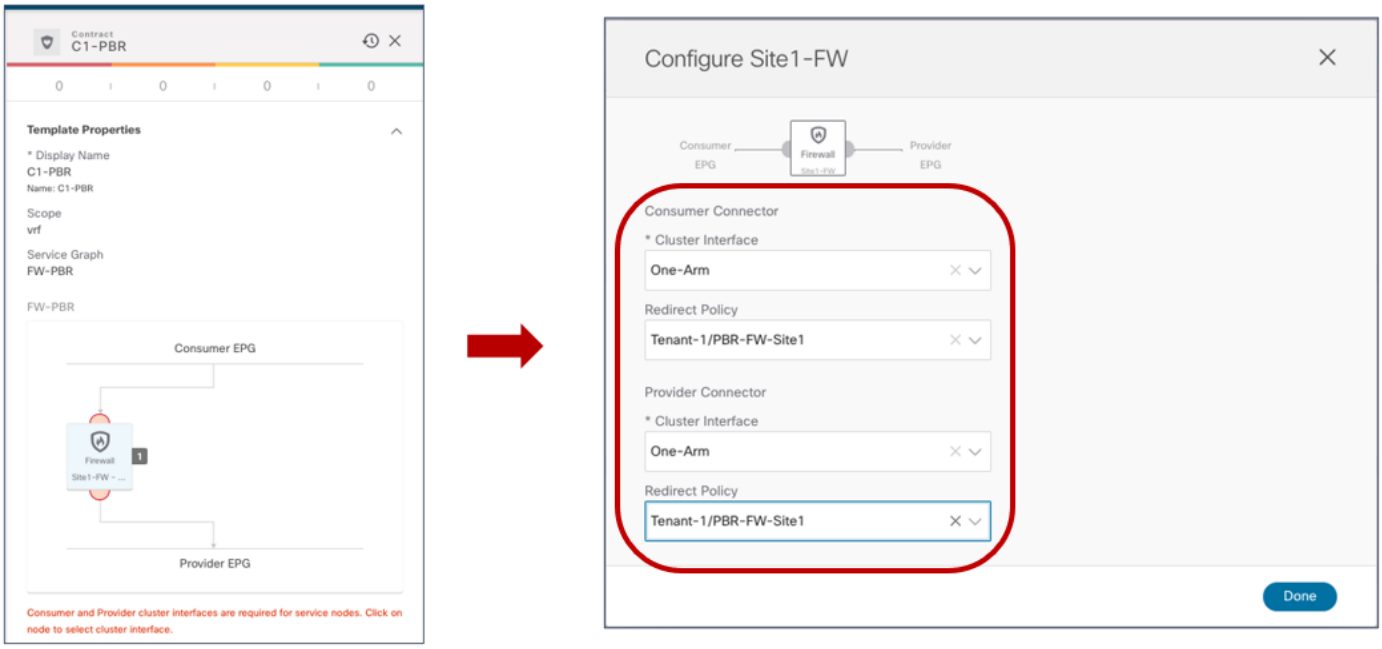


図 139.
サービス ノードのインターフェイスへの PBR ポリシーの関連付け

- 最後のプロビジョニング手順は、内部 EPG と外部 EPG の間に以前に定義したコントラクトを適用することです。「外部レイヤ 3 ドメインへの接続」のセクションで説明したように、拡張外部 EPG の定義は、同じ外部リソースのセットへのアクセスを提供するサイトに展開された L3Outs に推奨されます。これにより、セキュリティ ポリシーの適用が単純化されるからです。

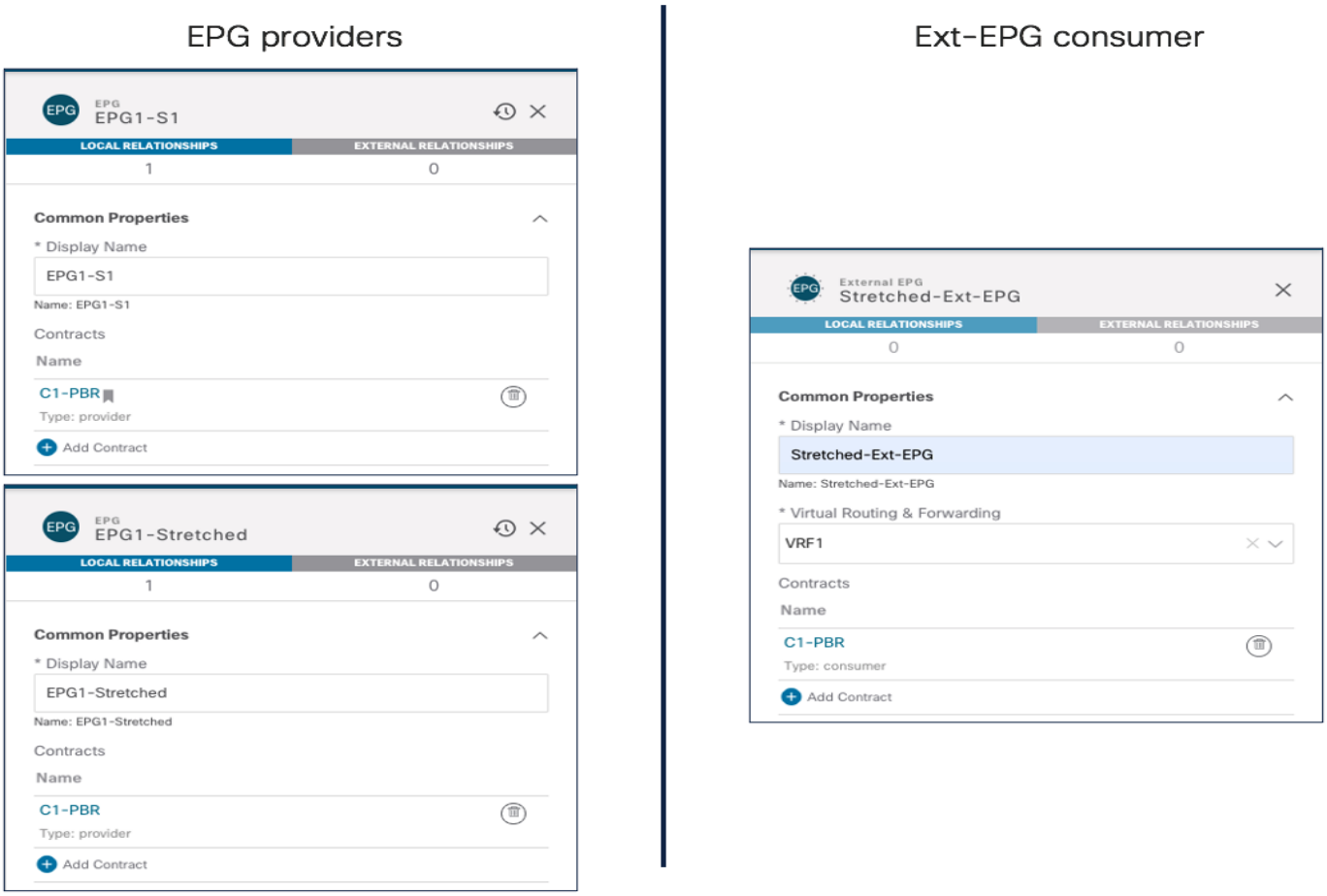


図 140.
コンシューマーおよびプロバイダー EPG へのコントラクトの適用

このセクションで説明するインフラ VRF シナリオでは、どちらの側がプロバイダーまたはコンシューマーであるかは関係ありません。VRF で「ポリシー制御適用方向」が「受信 (Ingress)」（デフォルト設定）として設定されている限り、PBR ポリシーは常にコンピューティング リーフ ノードに適用されます。

注： NDO リリース 3.1(1) 以降、vzAny はサービス グラフを関連付けたコントラクトと組み合わせて使用できません。したがって、2 つの EPG（内部および外部）間で PBR ポリシーを適用する唯一のオプションは、上記の例のように特定のコントラクトを作成することです。

上記のプロビジョニング手順が完了すると、各 APIC ドメインに個別のサービス グラフが展開され、ノースサウス トラフィック フローがファイアウォール ノードを介してリダイレクトされます。次の図 141 は、サービス グラフが APIC で正常にレンダリングされたことを確認する方法を示しています（導入の問題を強調する障害がないことを確認します）。

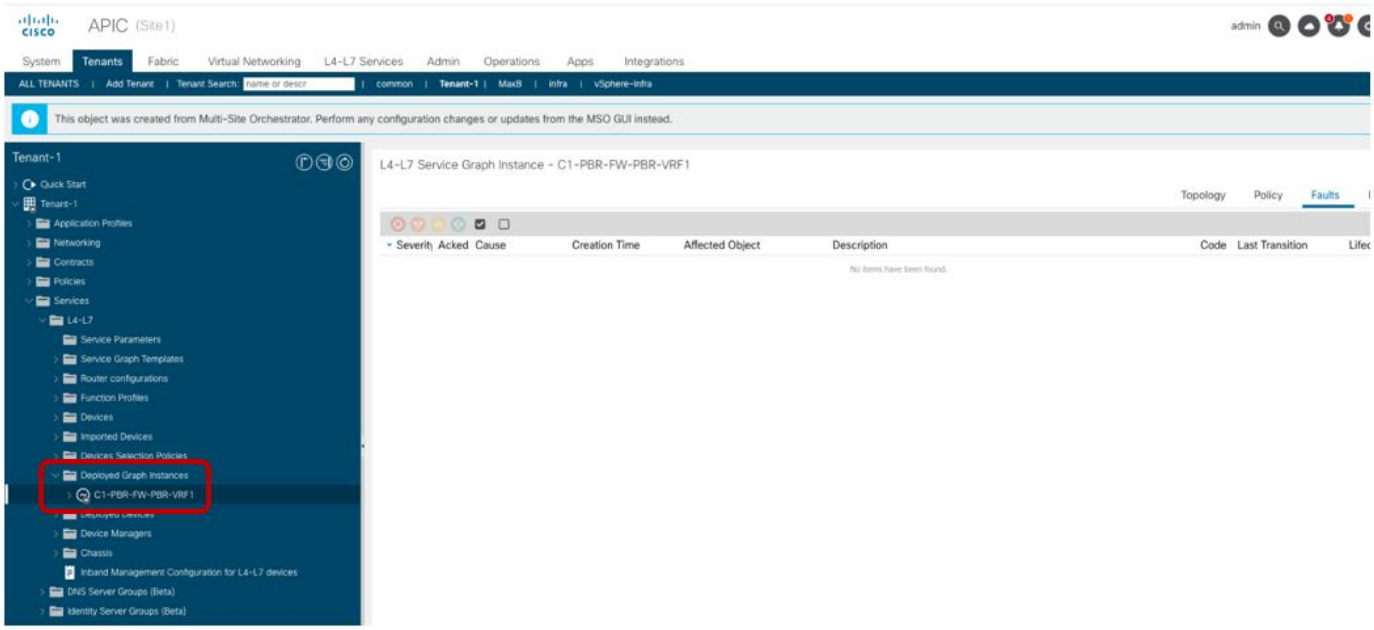


図 141.
APIC コントローラでのサービス グラフのレンダリング

次の出力で強調表示されているように、コンピューティング ノードで、トラフィックがファイアウォール ノードに適切にリダイレクトされていることを確認することもできます。

Leaf 101 Site1

```
Leaf101-Site1# show zoning-rule scope 3112963
+---------+--------+--------+----------+----------------+---------+---------+------+--------
----------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name
|      Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+--------
----------+----------------------+
|   4194  |   0    |   0    | implicit |    uni-dir     | enabled | 3112963
|      |     deny,log     |   any_any_any(21)    |
|   4203  |   0    |   0    | implarp  |    uni-dir     | enabled | 3112963
|      |      permit      |  any_any_filter(17)  |
|   4227  |   0    |   15   | implicit |    uni-dir     | enabled | 3112963
|      |     deny,log     | any_vrf_any_deny(22) |
|   4217  |   0    | 32771  | implicit |    uni-dir     | enabled | 3112963
|      |      permit      |   any_dest_any(16)   |
|   4197  |   0    | 49153  | implicit |    uni-dir     | enabled | 3112963
|      |      permit      |   any_dest_any(16)   |
|   4200  | 32773  | 16391  | default  |    uni-dir     | enabled | 3112963
|      |      permit      |    src_dst_any(9)    |
|   4223  | 32773  | 16388  | default  |    uni-dir     | enabled | 3112963
|      |      permit      |    src_dst_any(9)    |
|   4181  |   0    | 49157  | implicit |    uni-dir     | enabled | 3112963
|      |      permit      |   any_dest_any(16)   |
```

```
|   4109  | 16388  | 49158  | default  | uni-dir-ignore | enabled | 3112963
|      | redir(destgrp-4) |    src_dst_any(9)    |
|   4228  | 49158  | 16391  | default  |     bi-dir     | enabled | 3112963
|      | redir(destgrp-4) |    src_dst_any(9)    |
|   4170  | 16391  | 49158  | default  | uni-dir-ignore | enabled | 3112963
|      | redir(destgrp-4) |    src_dst_any(9)    |
|   4198  | 49158  | 16388  | default  |     bi-dir     | enabled | 3112963
|      | redir(destgrp-4) |    src_dst_any(9)    |
|   4208  | 32773  | 49158  | default  |    uni-dir     | enabled | 3112963
|      |      permit      |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+------+--------
----------+----------------------+
```

図 133 および図 135 に示すトポロジでは、Site1の 16388 は EPG1-S1 のクラス ID（エンドポイント 10.10.1.1が接続されている）を表し、49158 は Stretched-Ext-EPG のクラス ID です。同時に、16391 は Site1内の EPG1-Stretched のクラス ID を表します。上記の出力は、リダイレクション ポリシーが内部 EPG と外部 EPG 間の通信の両方のレッグにどのように適用されるかを示しています。次のコマンドは、トラフィックがリダイレクトされる特定のノード（50.50.50.10 は Site1 のファイアウォールの IP）を示します。

```
Leaf101-Site1# show service redir info group 4
================================================
================================================ ================================
凡例
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC:
Backup-Dest |  TRA: Tracking  | RES: Resiliency
================================================================================================
========================================
GrpID Name            destination                                                    HG-
name                          BAC  operSt     operStQual      TL   TH   HP   TRAC RES
=====
====            ==========                                                    =============
=                   ===   =======    ============    ===   ===   ===   ===   ===
4     destgrp-4       dest-[50.50.50.10]-[vxlan-3112963]                          Not
attached                    N    enabled    no-oper-
grp     0    0    sym  no   no
```

注： 複数の独立した具象デバイスを使用して論理ファイアウォール サービス ノードを構築した場合、リダイレクション ポリシーは複数の IP宛先（具象デバイスごとに 1 つ）を示します。

最後の 1 つの考慮事項は、ローカル L3Out 接続が展開されていない（または障害シナリオのために使用できなくなった）特定のシナリオに適用されます。この場合、「サイト間 L3Out の導入」で説明したように、サイト間 L3Out 機能を使用して、着信および発信トラフィック フローが Site1 の L3Out を Site2 に接続されたエンドポイントとの通信に利用できるようにします。サイト間 L3Outは、PBR を使用してサービス グラフと組み合わせることができます。 2 つの機能は相互に独立して動作しますが、内部検証のため、次の図 142 に示す動作は、ファブリックが ACI 4.2(5) （または 4.2(x) トレイン以降のリリース）または5.1(1) 以降のリリースを実行している場合にのみサポートされます。

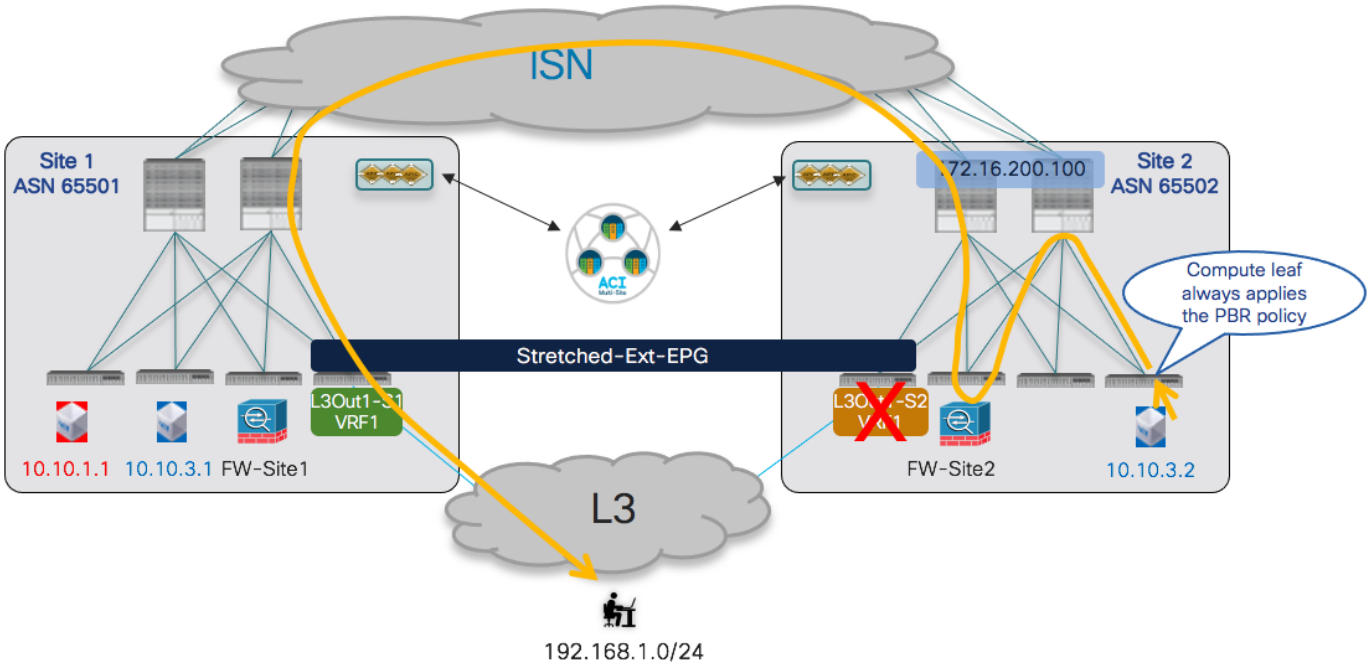


図 142.
PBR を使用したサイト間 L3Outおよびサービス グラフ

ノースサウストラフィック フロー（VRF 間）のファイアウォール挿入

ACI リリース4.2(5) および5.1(1) から、L3Out および内部 EPG が異なる VRF にマッピングされる VRF 間の使用例でも、ノースサウス トラフィック フローのサービス挿入がサポートされます（同じテナントまたは異なるテナント）。この場合の機能的な動作は、VRF 内のシナリオですでに示した図 133 および図 135と同じです。また、この場合、PBR ポリシーは常にコンピューティング リーフ ノードに適用され、個別の ACI ファブリックに展開された独立したサービス ノード機能間での非対称トラフィックの作成を回避します。

プロビジョニングの観点から、VRF 間の使用例では、次の特定の考慮事項が適用されます。

- ルート リークが発生し、BD サブネットが外部ネットワークにアドバタイズされるように、内部コンシューマー BD サブネットと Ext-EPG プレフィックスを適切に設定する必要があります。これを実現する方法の詳細については、前の「外部レイヤ 3 ドメインへの接続」セクションを参照してください。
- テナント内導入の場合、「Service-BD」は、拡張オブジェクトである限り、いずれかの VRF の一部として設定できます。テナント間シナリオでは、代わりに「Service-BD」をプロバイダー テナントで定義された VRF の一部にする必要があります。
- 関連付けられたサービス グラフとのコントラクトには、「テナント」（VRF が同じテナントの一部である場合）または「グローバル」（VRF が異なるテナントの一部である場合）の範囲が必要です。テナント間シナリオでは、プロバイダー テナントに関連付けられたテンプレート（通常は拡張テンプレート）でコントラクトを定義する必要があります。
- PBR ポリシーの適用が常にコンピューティング リーフ ノードで行われるようにするために、Ext-EPG は常にコントラクトのプロバイダーとして定義されますが、内部 EPG はコンシューマーです。

上記のプロビジョニング手順が完了すると、ノースサウス トラフィック フローは VRF 内の使用例とまったく同じように動作します。これは、図 142 の VRF 内の場合と同様に、サービス グラフがサイト間 L3Out と結合されるシナリオにも適用されます。

確認の観点から、最初に確認することは、ルートが VRF 間で適切にリークされていることです。次の出力は、外部プレフィックス 192.168.1.0/24 がコンピューティング リーフ ノードの VRF1 にリークされている特定の例を示しています。BD1-S1（10.10.1.0/24）の場合、ボーダー リーフ ノードの VRF-Shared にリークされます。

Leaf 101 Site1

```
Leaf101-Site1# show ip route vrf Tenant-1:VRF1
IP Route Table for VRF "Tenant-1:VRF1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.1.112.66%overlay-1, [1/0], 12:48:25, static
10.10.1.254/32, ubest/mbest: 1/0, attached, pervasive
    *via 10.10.1.254, vlan57, [0/0], 00:29:17, local, local
192.168.1.0/24, ubest/mbest: 1/0
    *via 10.1.0.69%overlay-1, [200/0], 01:18:33, bgp-65501, internal, tag 3, rwVnid: vxlan-2293765
```

Leaf 104 Site1

```
Leaf104-Site1# show ip route vrf Tenant-1:VRF-Shared
IP Route Table for VRF "Tenant-1:VRF-Shared"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.1.112.66%overlay-1, [1/0], 00:23:32, static, tag 4294967292, rwVnid: vxlan-3112963
192.168.1.0/24, ubest/mbest: 1/0
    *via 172.16.1.1%Tenant-1:VRF-Shared, [20/0], 21:11:40, bgp-65501, external, tag 3
```

リークされたプレフィックスに、他のリーフ ノードにトラフィックを送信するときに VXLAN ヘッダーに挿入する特定のセグメント ID の情報がどのように関連付けられるかに注意してください（vxlan-2293765 は vRF-Shared に割り当てられ、vxlan-3112963は vRF1 に割り当てられます）。これにより、受信側のリーフノードが正しい VRF でレイヤ 3 ルックアップを実行できるようになります。

セキュリティ ポリシーの観点からは、外部ネットワークから BL ノードで受信されたトラフィックは、Ext-EPG に関連付けられ（Ext-EPG で分類用に設定されたプレフィックスの照合に基づいて）、対応するクラス ID（以下の例）。コンシューマー VRF の内部エンドポイント部分は、代わりに「特殊な」クラス ID 値 14 で分類されるため、HW にインストールされたルールにより、着信フローがファブリックに転送されます。

Leaf 104 Site1

```
Leaf104-Site1# show zoning-rule scope 2293765
```

```
+---------+--------+--------+----------+---------+---------+---------+------+--------------
--+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  | Name
|      Action     |       Priority       |
+---------+--------+--------+----------+---------+---------+---------+------+--------------
--+----------------------+
|   4217  |   0    |   0    | implicit | uni-dir | enabled | 2293765
|       |     deny,log    |   any_any_any(21)    |
|   4181  |   0    |   0    | implarp  | uni-dir | enabled | 2293765
|       |      permit     |  any_any_filter(17)  |
|   4233  |   0    |   15   | implicit | uni-dir | enabled | 2293765
|       |     deny,log    | any_vrf_any_deny(22) |
|   4153  |  5493  |   14   | implicit | uni-dir | enabled | 2293765
|       | permit_override |    src_dst_any(9)    |
|   4201  |   0    | 16392  | implicit |    uni-dir     | enabled | 2359299
|            |  permit  |   any_dest_any(16)   |
|   4242  |   29   |  5493  | default  | uni-dir | enabled | 2293765
|       |      permit     |    src_dst_any(9)    |
|   4207  |   29   |   14   | implicit | uni-dir | enabled | 2293765
|       | permit_override |    src_dst_any(9)    |
+---------+--------+--------+----------+---------+---------+---------+------+--------------
--+----------------------+
```

トラフィックがコンピューティング リーフに到達すると、PBR ポリシーが開始され、トラフィックがサービス ノードにリダイレクトされます。これは、次の行で強調表示されています（EPG1-S1 を表す送信元クラス ID 5493、宛先クラス ID 16391）。また、EPG1-S1から発信され、外部ネットワーク ドメインを宛先とするリバース トラフィックのリダイレクション ルールが存在することにも注意してください。

Leaf 101 Site1

```
Leaf101-Site1# show zoning-rule scope 3112963
+---------+--------+--------+----------+---------------+---------+---------+------+--------
----------+-----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir      |  operSt |  Scope  | Name
|      Action      |        Priority        |
+---------+--------+--------+----------+---------------+---------+---------+------+--------
----------+-----------------------+
|   4194  |   0    |   0    | implicit |    uni-dir    | enabled | 3112963
|       |     deny,log     |    any_any_any(21)     |
|   4203  |   0    |   0    | implarp  |    uni-dir    | enabled | 3112963
|       |      permit      |  any_any_filter(17)  |
|   4227  |   0    |   15   | implicit |    uni-dir    | enabled | 3112963
|       |     deny,log     | any_vrf_any_deny(22) |
|   4180  |  5493  | 16391  | default  | uni-dir-ignore | enabled | 3112963
|       | redir(destgrp-5) |     src_dst_any(9)     |
|   4235  | 16391  |  5493  | default  |     bi-dir     | enabled | 3112963
|       | redir(destgrp-5) |     src_dst_any(9)     |
+---------+--------+--------+----------+---------------+---------+---------+------+--------
----------+-----------------------+
```

コンピューティング リーフは、外部宛先 192.168.1.0/24 を宛先とするトラフィックの正しいクラス ID を導出できることに注意してください。この情報は、 Ext-EPG で設定されたサブネットに関連付けられた「共有セキュリティ インポート (Shared Security Import)」フラグの設定の結果として、コンピューティング リーフにプログラムされているものです。この情報は、次のコマンドを使用して取得できます。

Leaf 101 Site1

```
Leaf101-Site1# vsh -c 'show system internal policy-
mgr prefix'
要求されたプレフィックス データ


Vrf-Vni VRF-Id Table-Id Table-State  VRF-
Name                        Addr                                Class Shared Remote Complete
======= ======  ========== =======  ============================
================================ ====== ====== ====== ========

3112963 42     0x2a           Up     Tenant-
1:VRF1                                    192.168.1.0/24  5493    True   True   False
```

イーストウェスト トラフィック フローのファイアウォール挿入（VRF 間）

2 つの内部 EPG 間の VRF 内通信にサービス ノードを挿入する必要がある場合（「イーストウェスト」の使用例とも呼ばれる）、ノースサウスに使用されるメカニズム（つまり、常に PBR ポリシーをコンピューティング リーフ ノードを適用する）とは異なるメカニズムを使用して、独立したサービス ノード間での非対称トラフィックの作成を回避する必要があります。

現在の実装では、EPG 間のすべてのコントラクト関係が常に「コンシューマー」側と「プロバイダー」側を定義するという事実を活用しています。したがって、ACI リリース 4.0(1) 以降、PBR ポリシーのアプリケーションは、常に「プロバイダー リーフ」と呼ばれるプロバイダーエンドポイントが接続されているコンピューティング リーフに固定されます。

図 143 は、コンシューマー エンドポイントから通信が開始されたときに動作する PBR ポリシーを示しています。これは最も一般的なシナリオです。トラフィックは Multi-Site によってプロバイダー リーフに転送され、そこで PBR ポリシーが適用されてトラフィックがサービス ノードにリダイレクトされます。サービス ノードがポリシーを適用すると、トラフィックはプロバイダー エンドポイントに配信されます。

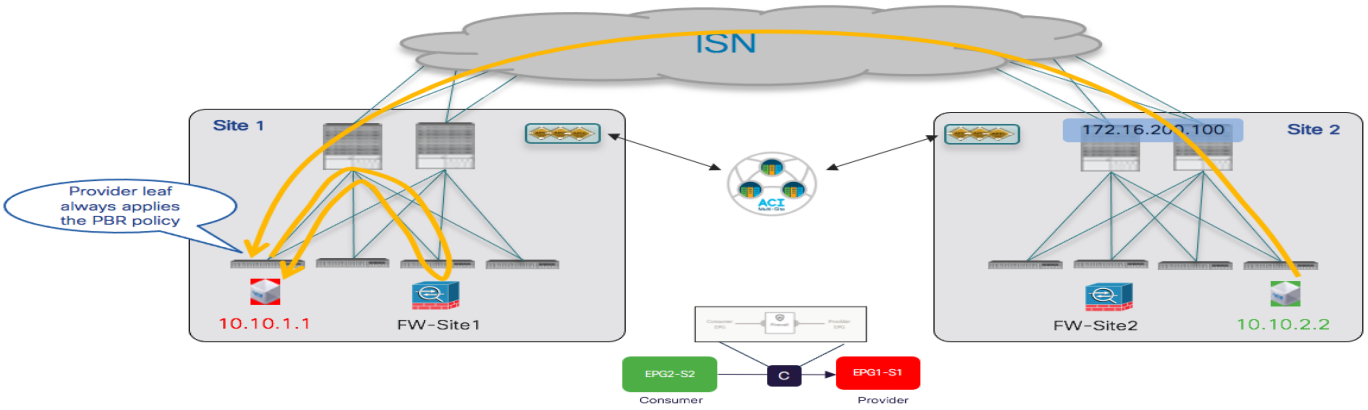


図 143.
コンシューマー EPG とプロバイダー EPG 間の通信用 PBR

上記の通信フローの結果として、特定のコンシューマーエンドポイント情報がプロバイダー リーフ ノードで学習されます。これは、プロバイダー エンドポイントが応答するときに、PBR ポリシーをプロバイダー リーフに再度適用して、通信の最初のレッグを処理した同じサービス ノードにトラフィックをリダイレクトできることを意味します（図 144）。サービス ノードがポリシーを適用すると、トラフィックは ISN を介してコンシューマー エンドポイントに転送されます。

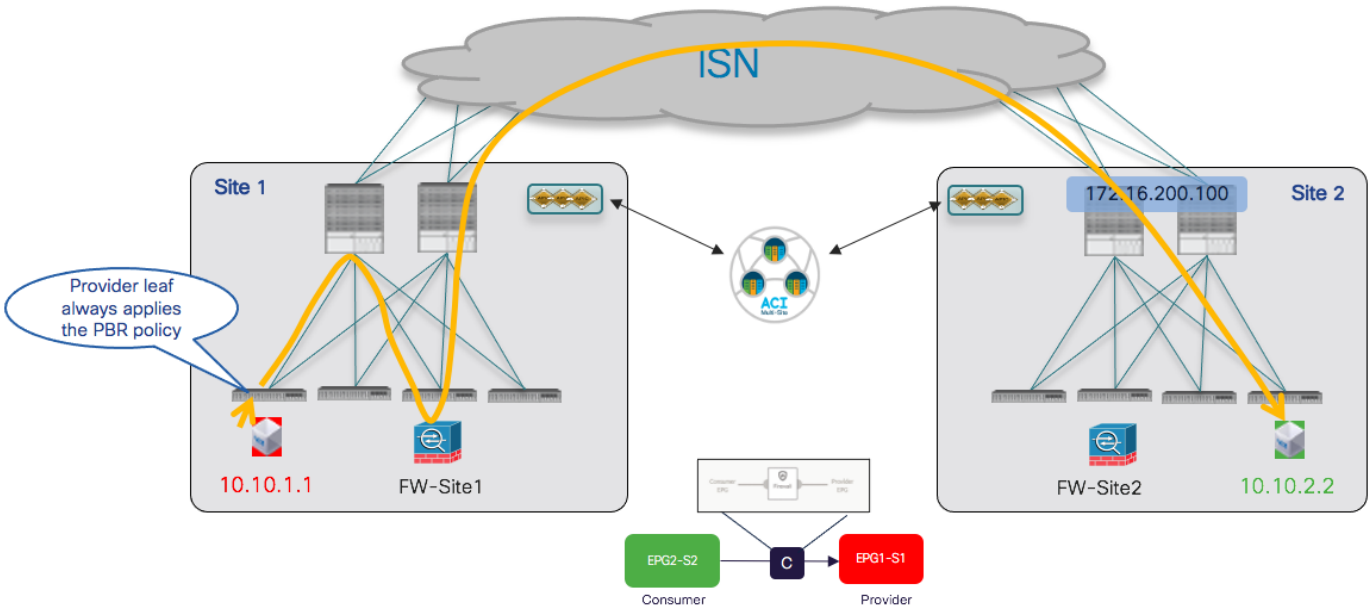


図 144.
プロバイダー EPG とコンシューマー EPG 間の通信用 PBR

上記の図から得られる結論は、ファブリックに接続されたエンドポイント間のすべてのイーストウェスト通信について、トラフィックは常にプロバイダー エンドポイントが存在するサイトのサービス ノードにリダイレクトされるということです。

EPG 間の特定のコントラクト関係ごとに、ゾーン分割ルールでコンシューマー側とプロバイダー側を常に識別できるようにすることが重要です。つまり、同じ EPG が同じコントラクトを消費して提供することはないので、特定の導入シナリオによっては異なるコントラクトの定義が必要になる場合があります。

また、EPG の同じペア間に 2 つの異なるコントラクトが適用された場合（それぞれのプロバイダーとコンシューマー EPG を区別できるようにするため）、これらの 2 つのコントラクトによって作成されたゾーン分割ルールが同じコントラクトとフィルタの優先順位を持つルールの重複。同じタイプのトラフィックを識別する同じプライオリティのゾーン分割ルールを定義すると、転送の動作が決定的ではなくなる可能性があります（異なるファイアウォールを通過する非対称トラフィックの作成）。

一般的な例として、すべてのトラフィックをリダイレクトする「すべて許可 (permit any)」ルールを使用して 2 つのコントラクトを作成することはできません。一方のコントラクトが「すべて許可 (permit any)」で、もう一方のコントラクトが「ICMP のみ許可（permit ICMP only）」の場合、「ICMP のみ許可（permit ICMP only）」のコントラクトによって作成されたゾーン分割ルールの優先順位が高くなります。

最後の重要な考慮事項として、プロバイダーエンドポイントによって通信が開始される可能性がある特定のシナリオでも、プロバイダーリーフにPBRポリシーを適用できるようにする必要がありますこのようなシナリオでは、プロバイダーリーフで使用可能なコンシューマーエンドポイント情報がまだない可能性があります（前述のデータプレーン通信で学習）。そのため、コンシューマーEPGの宛先クラスIDを導出し、ポリシーを適用するという異なったメカニズムが必要となります。現在の実装では、これは、コンシューマーEPGでサブネットプレフィックスを設定する「静的」アプローチに基づいて実現されます。この情報は、NDOからプロバイダーサイトのAPICドメインに伝達され、APICが、コンシューマーEPGを識別する関連付けられたクラスIDによって、プロバイダーリーフノードにそのプレフィックスをインストールできるようにします。

したがって、コンシューマーEPGで設定されたプレフィックスに、そのEPGのエンドポイント部分のすべてのIPアドレスが含まれていることを確認することが重要です。「ネットワーク中心」のACI展開（1つのEPGがBDで定義されている）では、これはBDに設定された同じIPサブネットをEPGに関連付けることで簡単に実現できます。同じBDで複数のEPGを定義できる「アプリケーション中心型」の使用例では、特定のEPGに接続されたエンドポイントのみを含むプレフィックスを特定することが非常に困難になります。唯一のソリューションは、EPGに接続されているすべてのエンドポイントの固有の/32プレフィックスを使用することです。この最後のアプローチは、実際の展開では実行可能なオプションではありません。したがって、通常、イーストウェストの通信にPBRでサービスグラフを使用することが推奨され、「ネットワーク中心」の設定にのみ制限されます。

上記の動作を実現するために必要な設定のプロビジョニングに関する懸念事項は、テナントEPG/BDがすでに展開されており、エンドポイントがそれらに接続されていることです（EPGは各サイトでローカルに定義するか、またはサイト間で拡張できます）。また、「単一サービスノードを挿入するためのマルチサイトでのPBRを使用したサービスグラフ」セクションで説明されているように、論理ファイアウォールサービスノードとPBRポリシーが各サイトに導入されています。これらの前提条件の手順が完了すると、「ノースサウストラフィックフロー（VRF内）のファイアウォール挿入」の一部としてすでに説明した手順とほぼ同じ手順を実行できます。

- ファイアウォールノードを接続するストレッチサービスBDを定義します。
- サービスグラフを（ストレッチオブジェクトとしても）作成します。ノースサウス通信に使用されるものと同じサービスグラフを、イーストウェストトラフィックフローにも使用できることに注意してください。
- コントラクトを作成し（スコープVRFを使用）、サービスグラフを関連付けます。
- コンシューマーEPGの下にプレフィックスを指定し、EPGの一部であるすべてのコンシューマーエンドポイントのIPアドレスを照合できるようにします。BDのサブネットに使用されるものと同じフラグをこのプレフィックスに設定し、「デフォルトのSVIゲートウェイなし(No Default SVI Gateway)」フラグを追加する必要があります。

  コンシューマーEPGとプロバイダーEPGの間にコントラクトを適用します。

コントラクトが適用されると、サービスノードへの適切なリダイレクションにより、イーストウェスト通信が正常に確立されます。

プロバイダーリーフのエンドポイントテーブルを見ると、コンシューマーエンドポイントが実際にどのように学習されているかを確認できます。コンシューマーエンドポイントはリモートにあるため、プロバイダーリーフとリモートサイトのスパインのO-UTEPアドレスの間に確立されたVXLANトンネル（tunnel26）を介して到達可能です。

Leaf 101 Site1

```
Leaf101-Site1# show endpoint vrf Tenant-1:VRF1
```

凡例：

```
 s - arp H - vtep V - vpc-attached p - peer-aged
 R - peer-attached-rl B - bounce S - static M - span
 D - bounce-to-proxy O - peer-attached a - local-aged m - svc-mgr
 L - local E - shared-service
+------------------------------------+-------------+----------------+-------------+------
-------+
      VLAN/ Encap MAC Address MAC Info/ Interface
      Domain VLAN IP Address IP Info
+------------------------------------+-------------+----------------+-------------+------
-------+
Tenant-1:VRF1 10.10.2.2 tunnel26
60 vlan-819 0050.56b9.1bee LV po1
Tenant-1:VRF1 vlan-819 10.10.1.1 LV po1
```

コンシューマー EPG でのプレフィックス設定の結果、プレフィックスは関連付けられたクラス ID（49163）とともにプロバイダー リーフにインストールされます。

Leaf 101 Site1

```
Leaf101-Site1# cat /mit/sys/ipv4/inst/dom-Tenant-1:VRF1/rt-\[10.10.2.0--24\]/summary
# IPv4 Static Route
prefix : 10.10.2.0/24
childAction :
ctrl : pervasive
descr :
dn               : sys/ipv4/inst/dom-Tenant-1:VRF1/rt-[10.10.2.0/24]
flushCount : 0
lcOwn : local
modTs            : 2020-12-16T13:27:29.275+00:00
monPolDn :
name :
nameAlias :
pcTag            : 49163
pref : 1
rn : rt-[10.10.2.0/24]
sharedConsCount : 0
status :
tag : 0
trackId : 0
```

これにより、特定のコンシューマー エンドポイント情報がまだ学習されていない場合でも、PBR ポリシーを常にプロバイダー リーフに適用できます。次の出力では、16388 がローカル プロバイダー EPG1-S1 のクラス ID であるため、サービス ノードへのリダイレクションがトラフィックの両方向（コンシューマーからプロバイダーへ、およびその逆）にどのように適用されるかを確認できます。

Leaf 101 Site1

```
Leaf101-Site1# show zoning-rule scope 3112963
+---------+--------+--------+----------+---------------+---------+---------+------+--------
----------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir      |  operSt |  Scope  | Name
|      Action      |       Priority       |
+---------+--------+--------+----------+---------------+---------+---------+------+--------
----------+----------------------+
|   4194  |   0    |   0    | implicit |    uni-dir    | enabled | 3112963
|      |     deny,log     |   any_any_any(21)    |
|   4203  |   0    |   0    | implarp  |    uni-dir    | enabled | 3112963
|      |      permit      |  any_any_filter(17)  |
|   4227  |   0    |   15   | implicit |    uni-dir    | enabled | 3112963
|      |     deny,log     | any_vrf_any_deny(22) |
|   4197  |   0    | 49153  | implicit |    uni-dir    | enabled | 3112963
|      |      permit      |   any_dest_any(16)   |
|   4138  |   0    | 16393  | implicit |    uni-dir    | enabled | 3112963
|      |      permit      |   any_dest_any(16)   |
|   4217  |   0    | 32771  | implicit |    uni-dir    | enabled | 3112963
|      |      permit      |   any_dest_any(16)   |
|   4222  |   0    | 49162  | implicit |    uni-dir    | enabled | 3112963
|      |      permit      |   any_dest_any(16)   |
|   4230  | 49163  | 16388  | default  |     bi-dir    | enabled | 3112963
|      | redir(destgrp-6) |    src_dst_any(9)    |
|   4170  | 16388  | 49163  | default  | uni-dir-ignore | enabled | 3112963
|      | redir(destgrp-6) |    src_dst_any(9)    |
|   4223  | 32773  | 16388  | default  |    uni-dir    | enabled | 3112963
|      |      permit      |    src_dst_any(9)    |
|   4174  | 16394  | 49163  | default  |    uni-dir    | enabled | 3112963
|      |      permit      |    src_dst_any(9)    |
+---------+--------+--------+----------+---------------+---------+---------+------+--------
----------+----------------------+
```

East-Westトラフィックフロー（Inter-VRF）のファイアウォール挿入

異なるVRFの一部であるEPG間のイーストウェスト通信のサービスノード統合は、前述のVRF内シナリオと基本的に同じです。PBRポリシーは常にプロバイダーリーフノードに適用されます。プロビジョニングに関するこのシナリオの特定の考慮事項のみを以下に詳しく説明します。

- コンシューマーとプロバイダーの両方のBDで「VRF間で共有(Shared between VRFs)」フラグを有効にします。
- コンシューマーEPGで設定されたプレフィックスにも同じフラグが設定されていることを確認します（設定されていない場合、Nexus Dashboard Orchestratorは設定を展開しません）。
- プロバイダーからコンシューマーVRFにBDサブネットをリークするには、プロバイダーBDに関連付けられたサブネットプレフィックスもプロバイダーEPGで設定する必要があります。

注： ルートリーク機能をトリガーするようにプロバイダーEPGでプレフィックスを設定する場合も、「ネットワーク中心」および「アプリケーション中心」の導入に関する同じ考慮事項が適用されます。

- 関連付けられたサービス グラフとのコントラクトの範囲は、「テナント」（VRF が同じテナントに展開されている場合）または「グローバル」（VRF が異なるテナントに展開されている場合）に変更する必要があります。
- テナント間展開の場合、サービス BD、サービス グラフ、およびコントラクトはすべて、プロバイダー テナントの一部として展開する必要があります。

VRF 内の場合と同様に、VRF 間イーストウェスト サービス グラフでも、PBR ポリシーは、そのプレフィックスのプロビジョニングをトリガーするコンシューマー EPG でのプレフィックスの設定により、適用することが可能です。また、関連するクラス ID をプロバイダー リーフ ノード上に適用できます。

Leaf 101 Site1

```
Leaf101-Site1# cat /mit/sys/ipv4/inst/dom-Tenant-1:VRF1/rt-\[10.10.2.0--24\]/summary
# IPv4 Static Route
prefix : 10.10.2.0/24
childAction :
ctrl : pervasive
descr :
dn               : sys/ipv4/inst/dom-Tenant-1:VRF1/rt-[10.10.2.0/24]
flushCount : 1
lcOwn : local
modTs            : 2020-12-16T14:30:51.006+00:00
monPolDn :
name :
nameAlias :
pcTag            : 10936
pref : 1
rn : rt-[10.10.2.0/24]
sharedConsCount : 0
status :
tag              : 4294967292
trackId          : 0
```

コンシューマープレフィックスに、すべての VRF で一意のグローバル範囲から取得したクラス ID 値（10936）がどのように割り当てられるかに注目してください。同じことがプロバイダー EPG のクラス ID にも当てはまります。これは、トラフィック フローをサービス ノードにリダイレクトするために使用されるルールを示す以下の出力に示すように、値 32 を取得します。

Leaf 101 Site1

```
Leaf104-Site1# show zoning-rule scope 2293765
+---------+--------+--------+----------+----------------+---------+---------+------+--------
----------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name
|      Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+--------
----------+----------------------+
```

```
|    4230   |    0     |    0     | implicit |     uni-dir      | enabled | 2293765
|       |      deny,log      |    any_any_any(21)     |
|    4200   |    0     |    0     | implarp  |     uni-dir      | enabled | 2293765
|       |       permit       |  any_any_filter(17)    |
|    4234   |    0     |   15     | implicit |     uni-dir      | enabled | 2293765
|       |      deny,log      | any_vrf_any_deny(22)   |
|    4222   | 10936    |   32     | default  |      bi-dir      | enabled | 2293765
|       | redir(destgrp-6) |     src_dst_any(9)     |
|    4191   |    32    | 10936    | default  | uni-dir-ignore | enabled | 2293765
|       | redir(destgrp-6) |     src_dst_any(9)     |
|    4236   |    0     | 49154    | implicit |     uni-dir      | enabled | 2293765
|       |       permit       |    any_dest_any(16)    |
+---------+--------+--------+----------+----------------+---------+---------+------+--------
----------+----------------------+
```

2 つ（またはそれ以上）のサービス ノードを挿入するためのマルチサイトの PBR を使用したサービス グラフ

サービス グラフとPBR を使用すると、2 つ（またはそれ以上）のサービス ノード機能を連結することもできるため、2 つの EPG のエンドポイント間の通信は、トラフィックが各サービス ノードによって実行される操作を通過した後にのみ許可されます。これは、図 145 に示すように、ノースサウスおよびイーストウェストのトラフィック フローに適用できます。

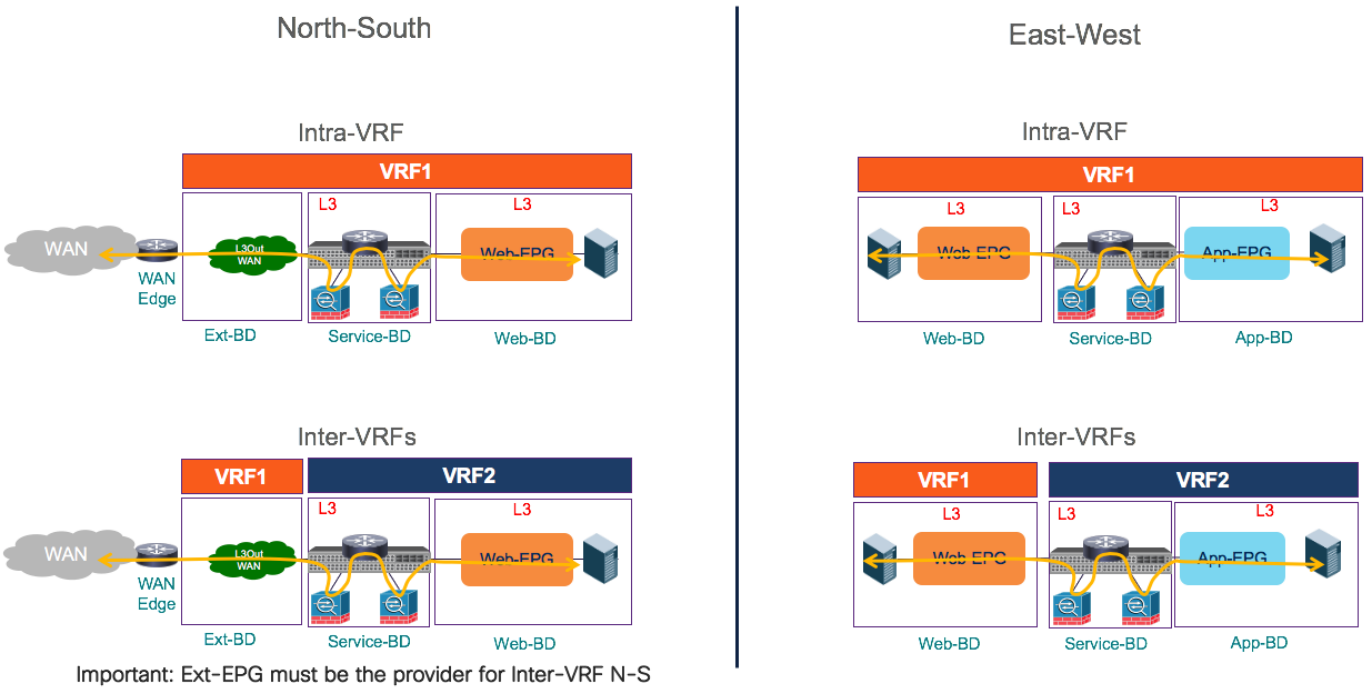


図 145.
PBR を使用した 2 ノードサービス グラフ

PBR を使用したマルチノード サービス グラフ機能のプロビジョニングは、単一ノードの使用例で説明したものと同様です。最初の手順は、Multi-Site ドメインの各ファブリック パーツによって提供される複数のサービス ノードの論理機能を定義することです。図 146 は、APIC レベルで実行される 2 つの論理 L4/L7 デバイスの作

成を示しています。各論理デバイスは、前の図 128 に示すように、選択した特定の導入/冗長性モデルに応じて、1 つ、2 つ、またはそれ以上の具体的なサービス ノードで実装されます。

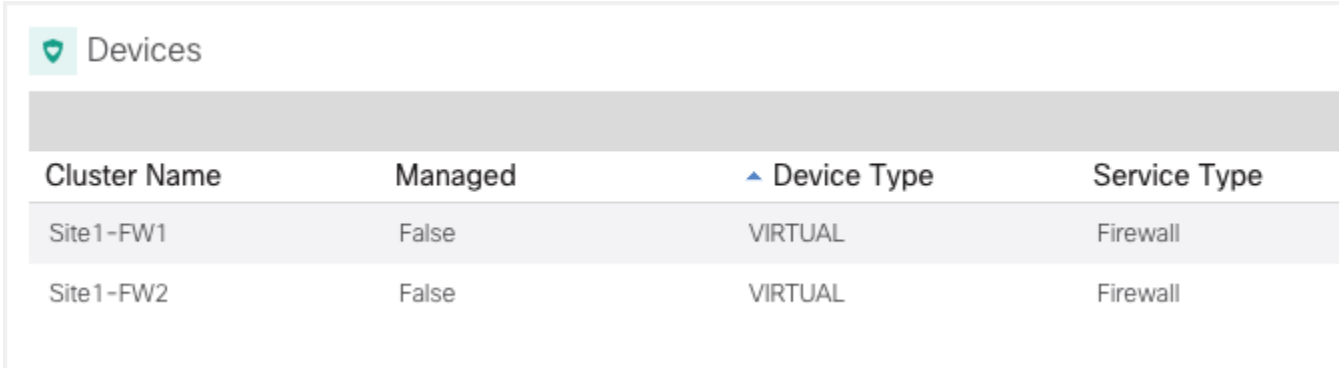


図 146.
Site1 の APIC の 2 つの論理ファイアウォール ノードの定義

APIC で実行される 2 番目のプロビジョニング手順は、サービス ノードを介したトラフィックのリダイレクトを許可する PBR ポリシーを定義することです。2 つのサービス ノードを定義したため、2 つの個別の PBR ポリシーも定義する必要があります。図 147 に示すように、各ポリシーはトラフィックを特定の MAC/IP ペアにリダイレクトし、特定の各サービス ノード機能を識別します。

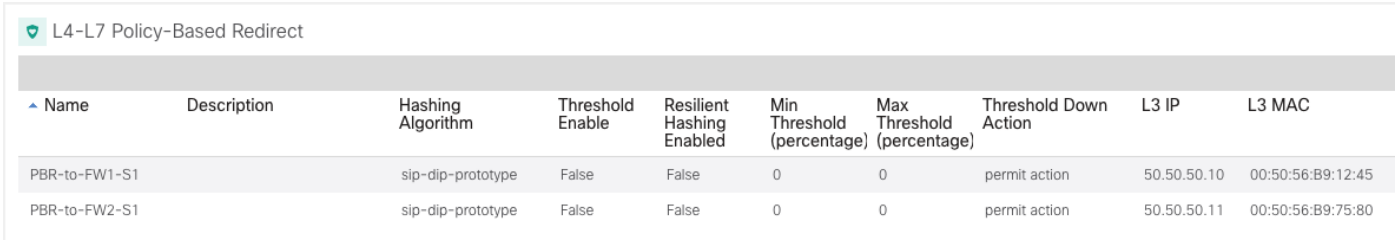


図 147.
2 つのサービス ノードリダイレクションの PBR ポリシー

注： Multi-Site ドメインのすべてのファブリック部分に対して、同様の設定を実行する必要があります。

この時点で、特定の設定を提供して、ノースサウスおよびイーストウェストの両方のトラフィック フローの EPG 間の通信の途中で2 つのサービス ノードをつなぐことができます。

単一サービス ノードの使用例では、ノースサウス通信の PBR ポリシーを常にコンピューティング リーフ ノードに適用する必要があります。これは、VRF がデフォルトの入力ポリシー適用方向で設定されている限り、VRF 内の使用例に常に当てはまります。VRF 間シナリオでは、Ext-EPG がサービス グラフに関連付けられているコントラクトのプロバイダーとして常に設定されていることを確認する必要があります。

ノースサウス トラフィック フローでのノードの挿入

図 148 は、ノースサウス フローの PBR リダイレクションによって、使用されるサービス ノードが内部エンドポイントと同じサイトにあることを常に保証する方法を示しています。

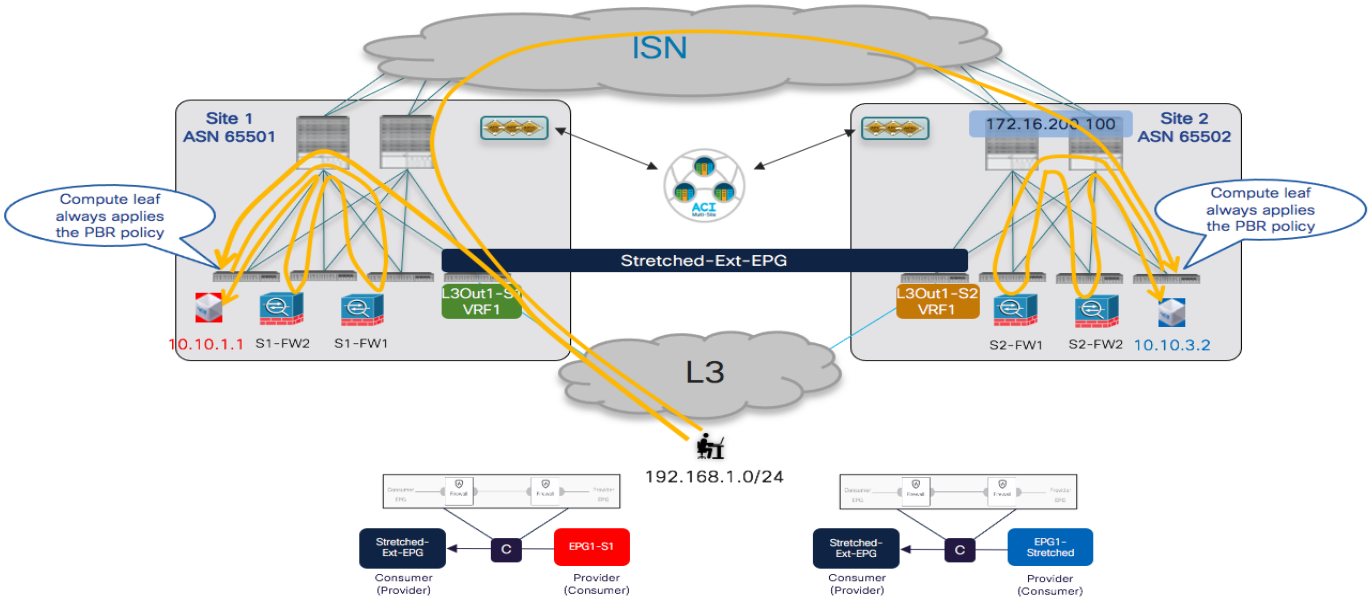


図 148.
ノースサウス トラフィック フローの PBRリダイレクション

ノースサウス トラフィック フロー（VRF 内）のファイアウォールを統合するために NDO で実行するプロビジョニング手順を以下に説明します。

- コンシューマーおよびプロバイダー BD のサブネットを構成して、それぞれのサイトで L3Out からアドバタイズされるようにします。これには、前の「外部レイヤ 3 ドメインへの接続」で説明したように、BD サブネットを「外部アドバタイズ (Advertised Externally)」として設定し、プレフィックスをアドバタイズする特定の L3Out にマッピングする必要があります。
- 着信トラフィックを適切に分類するように外部 EPG を設定します。ストレッチされた Ext-EPG が展開されていると仮定すると、関連する「外部 EPG の外部サブネット (External Subnets for External EPGs)」フラグセットで「キャッチオール」0.0.0.0/0 プレフィックスを指定するのが一般的です。
- 各ファブリックに展開されたファイアウォール ノードの接続に使用される「サービス BD」を定義します。この BD は、すべてのサイトに関連付けられたテンプレートで Nexus Dashboard Orchestrator からプロビジョニングする必要があります。サービス BD は、図 136 に示すように、単一サービス ノード挿入の使用例と同じようにプロビジョニングされます。
- 2 つのサービス ノードを挿入するため Orchestrator でサービス グラフを作成します。これは、Multi-Site ドメインのすべてのサイト部分に関連付けられているテンプレートでも実行する必要があります（つまり、サービス グラフは「ストレッチ」オブジェクトとしてプロビジョニングされます）。図 149 に示すように、サービス グラフの設定は 2 つに分けてプロビジョニングされます。最初に、どのサービス ノードを挿入するかを指定するグローバル テンプレート レベル（この例では 2 つのファイアウォール）です。次に、サイト レベルで、APIC で定義され、Nexus Dashboard Orchestrator に公開されている特定の論理ファイアウォール デバイスをマッピングします（前の図 146を参照）。

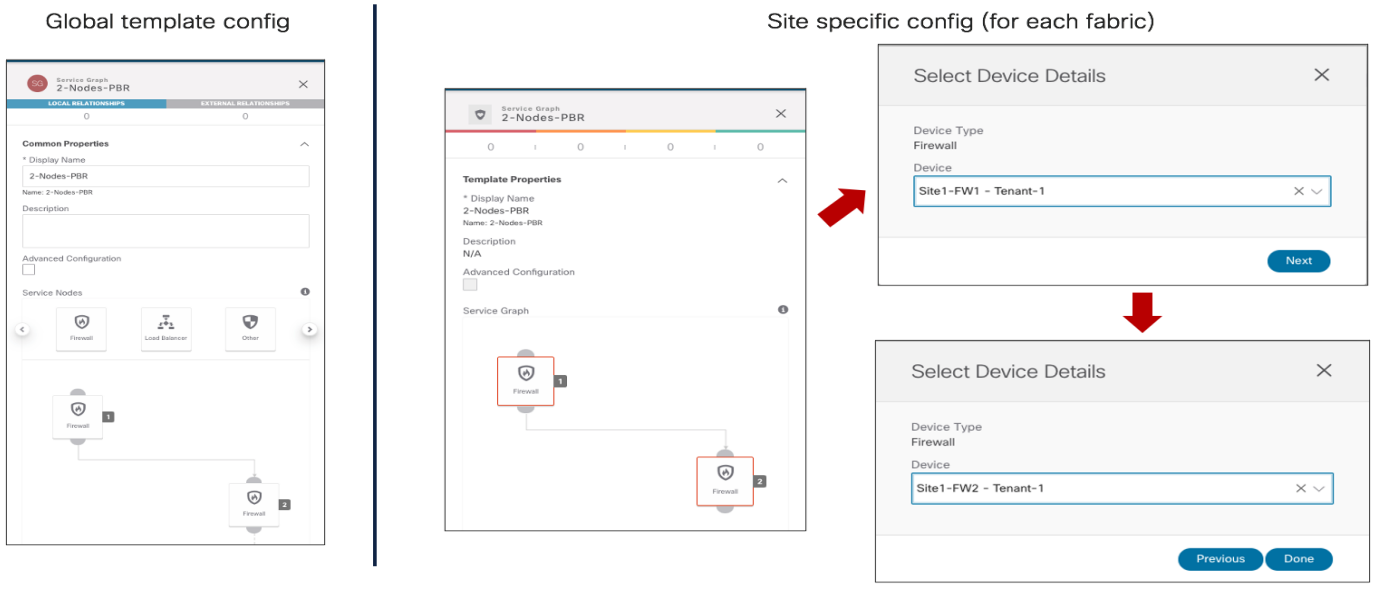


図 149.
NDO での 2 ノード サービス グラフの定義

- コントラクトを定義し、サービス グラフに関連付けます。コントラクトは通常、すべてのサイトに関連付けられたテンプレートで定義され、図 150 の例では、すべてのトラフィックがファイアウォールにリダイレクトされるように「すべて許可 (Permit-All)」フィルタがコントラクトに関連付けられています。目的が特定のトラフィック フローのみをファイアウォールにリダイレクトすることである場合は、この動作を変更してフィルタをより具体的にすることができます。

  次の 2 つの図に示すように、サービス グラフをコントラクトに関連付けた場合、2 つのステップの設定を実行する必要があります。グローバル テンプレート レベルでは、ファイアウォール論理ノードが接続されている BD を指定する必要があります（図 150）。この例では、ファイアウォールがワンアーム モードで接続されているため、コンシューマーとプロバイダーの両方のファイアウォールコネクタ（インターフェイス）に同じ「サービス BD」を指定できます。また、「サービス BD」はグローバル テンプレート レベルでコネクタに関連付ける必要があります。これが、その BD がすべてのサイトで拡張オブジェクトとしてプロビジョニングされる必要がある主な理由です。

  また、サイト レベルでは、代わりに各サービス ノードに PBR ポリシーを関連付ける必要があります（図 151）。リダイレクション ポリシーは、サービス ノードの各インターフェイス（コンシューマー コネクタとプロバイダー コネクタ）に関連付けられます。サービス ノードがワンアーム モードで接続されている特定の例では、同じ PBR ポリシーが各コネクタに適用されますが、たとえば、ファイアウォールがツーアーム モードで接続されている場合は適用されません。また、特定のサービス グラフの展開では、 1 つのインターフェイス（つまり、トラフィックの特定の方向）にのみ PBR ポリシーを適用する必要があります。

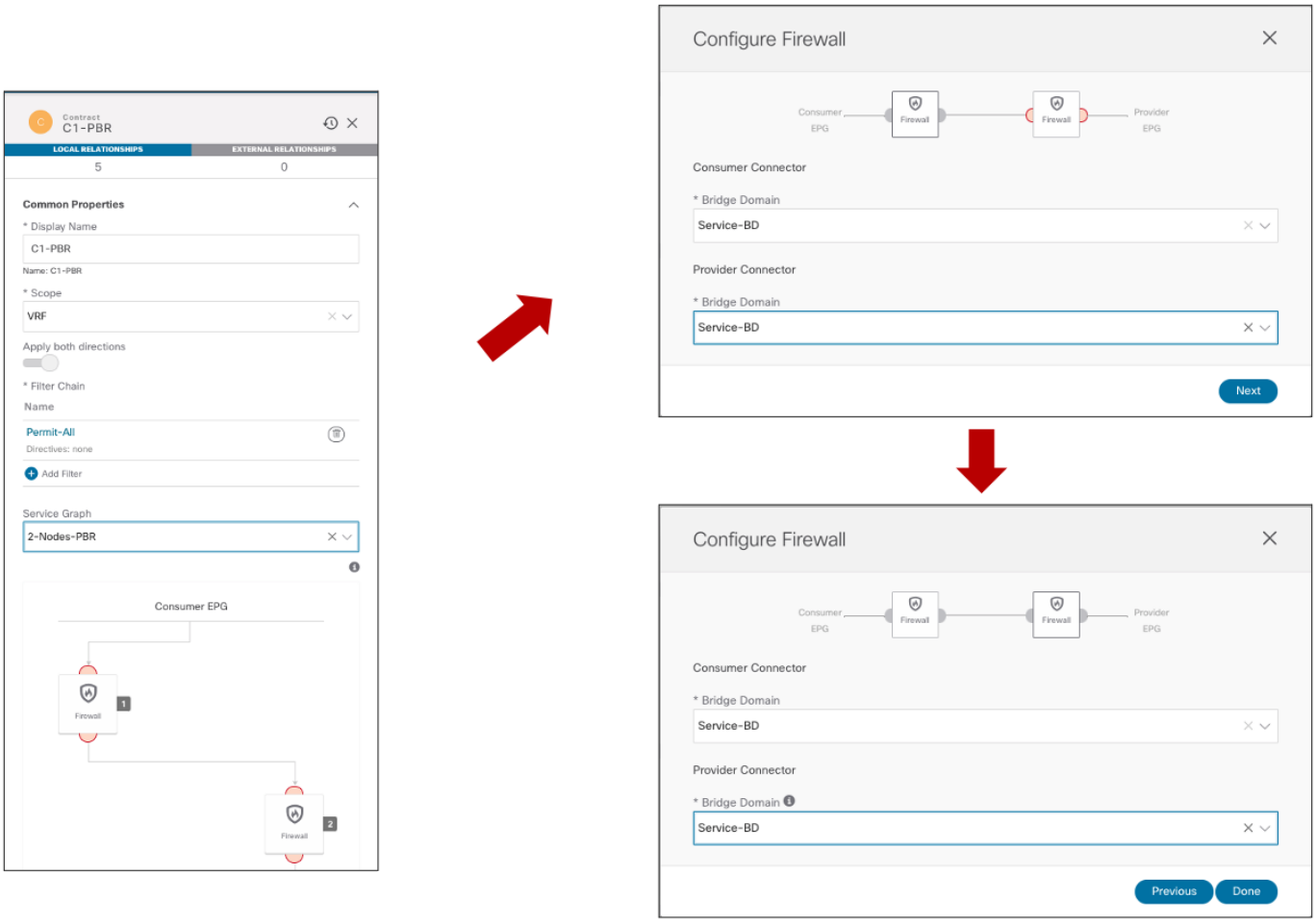


図 150.
関連付けられたサービス グラフのコントラクトの定義（グローバル テンプレート レベル）

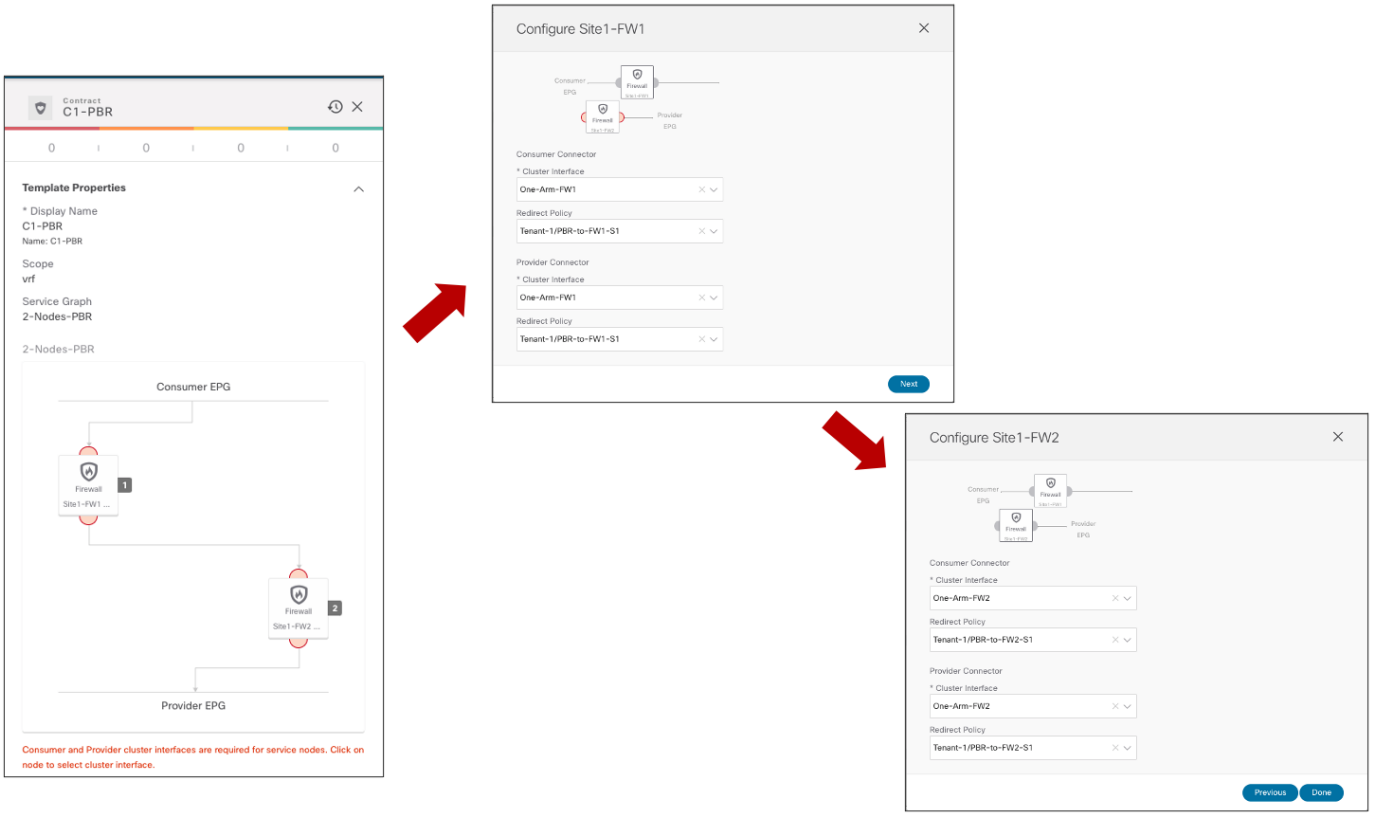


図 151.
各サービス ノードインターフェイスへの PBR ポリシーの関連付け（サイト ローカル レベル）

- 最後のプロビジョニング手順は、内部 EPG と外部 EPG の間に以前に定義したコントラクトを適用することです。「外部レイヤ 3 ドメインへの接続」のセクションで説明したように、拡張外部 EPG の定義は、同じ外部リソースのセットへのアクセスを提供するサイトに展開された L3Outs に推奨されます。これにより、セキュリティ ポリシーの適用が単純化されるからです。

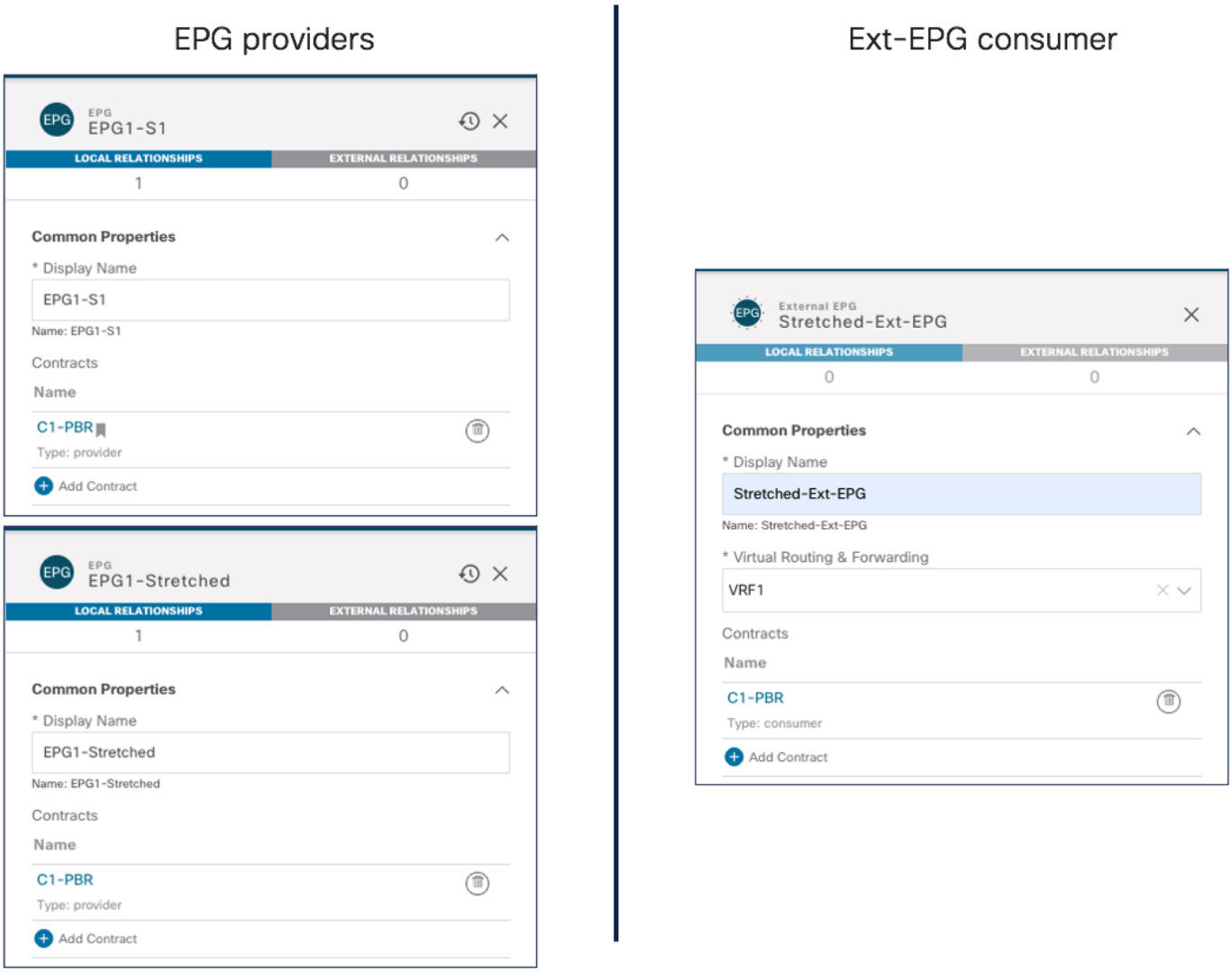


図 152.
コンシューマーおよびプロバイダー EPG へのコントラクトの適用

このセクションで説明するインフラ VRF シナリオでは、どちらの側がプロバイダーまたはコンシューマーであるかは関係ありません。PBR ポリシーは常にコンピューティング リーフ ノードに適用されます。

注： NDO リリース 3.5(1) の時点では、vzAny はサービス グラフを関連付けたコントラクトと組み合わせて使用できません。したがって、2 つの EPG（内部および外部）間で PBR ポリシーを適用する唯一のオプションは、上記の例のように特定のコントラクトを作成することです。

上記のプロビジョニング手順が完了すると、各 APIC ドメインに個別のサービス グラフが展開され、ノースサウス トラフィック フローがファイアウォール ノードを介してリダイレクトされます。リダイレクションの正しい動作を確認する方法の詳細については、「ノースサウス トラフィック フローでのファイアウォール挿入（VRF 内）」を参照してください。

VRF 間（またはテナント間あるいはその両方）の使用例では、非常によく似たプロビジョニング手順が必要です。このシナリオの展開方法の詳細については、前の「ノースサウス トラフィック フローでのファイアウォール挿入（VRF 間）」のセクションを参照してください。

イーストウェストトラフィック フローでの 2 つのサービス ノードの挿入

ノースサウス ユースケース用にプロビジョニングされた同じ 2 ノードサービス グラフは、図 153と図 154 に示すイーストウェスト シナリオでも再利用できます。

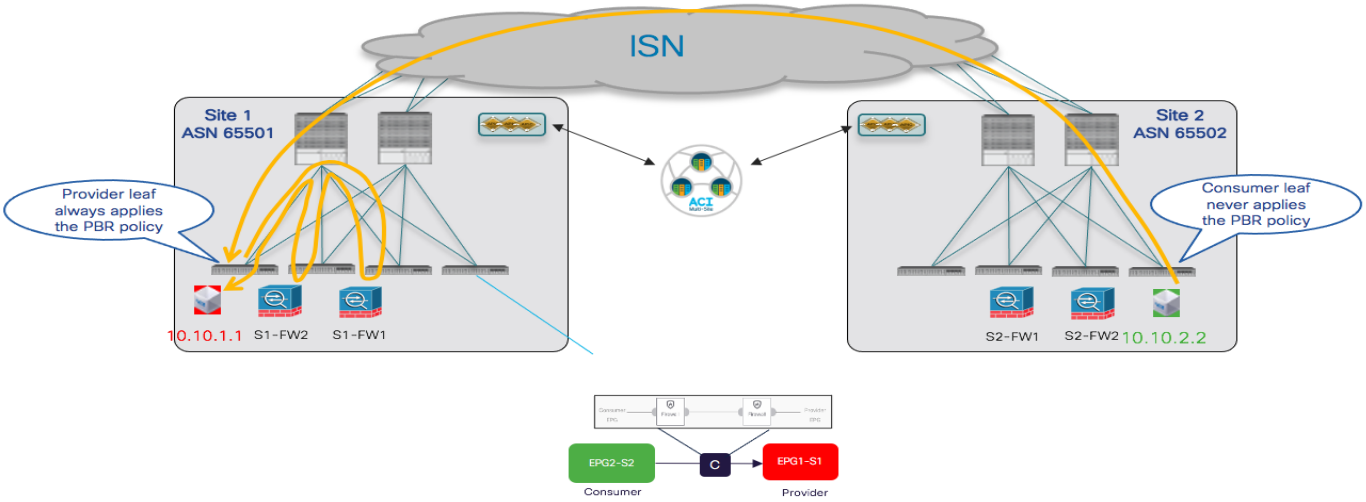


図 153.
コンシューマー EPG とプロバイダー EPG 間の通信用の 2 ノードPBR

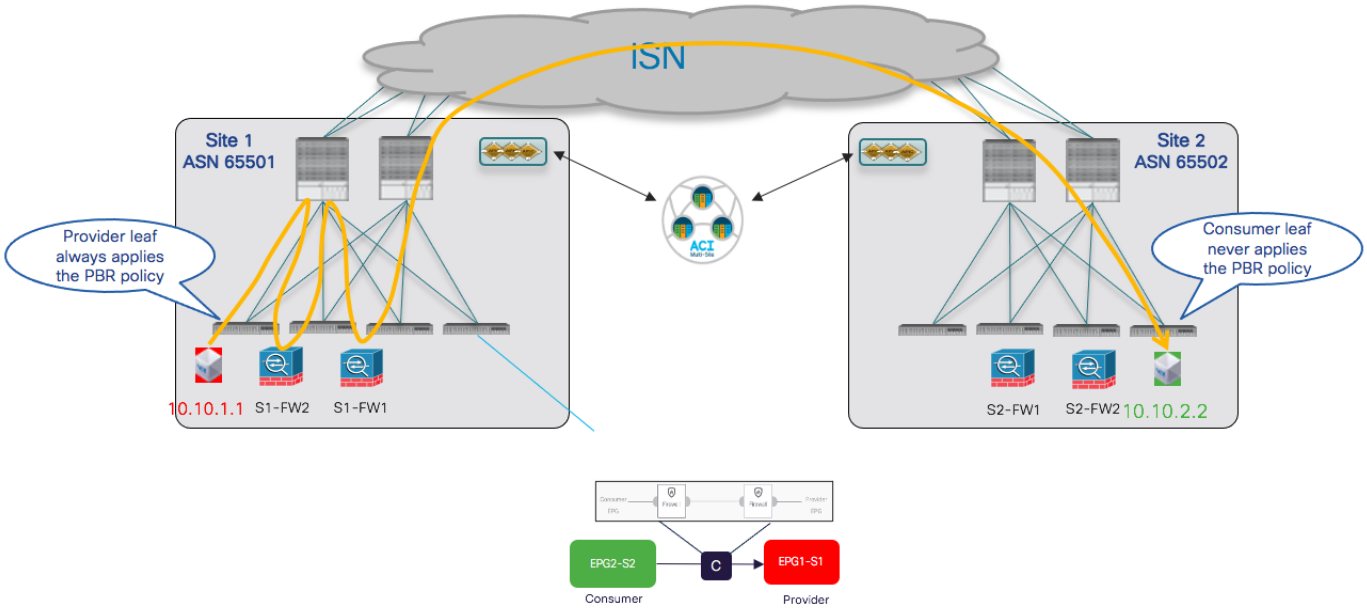


図 154.
プロバイダーとコンシューマー EPG 間の通信用の 2 ノードPBR

「イーストウェスト トラフィック フローでのファイアウォール挿入（VRF 内）」および「イーストウェスト トラフィック フローでのファイアウォールの挿入（VRF 間）」のセクションで説明したのと同じ考慮事項が、引き続き 2 ノードシナリオにも適用されます。つまり、プロバイダー リーフ ノードで PBR ポリシーの適用を「アンカー」するために必要な追加の設定手順は、コンシューマー EPG でのプレフィックスの設定だけです。

ACI マルチポッドと ACI マルチサイトの統合

実際の多くの導入シナリオでは、ACI Multi-PoD と Multi-Site アーキテクチャを統合して、疎結合 ACI DC（マルチサイト）を使用して密結合 ACI DC（マルチポッド）を展開することで満たすことができる特定の要件に対処する必要があります。

次の図 155 は、ACI マルチポッドファブリックと単一のポッド ACI ファブリックが同じ Multi-Site ドメインの一部として展開されているトポロジの例を示しています。

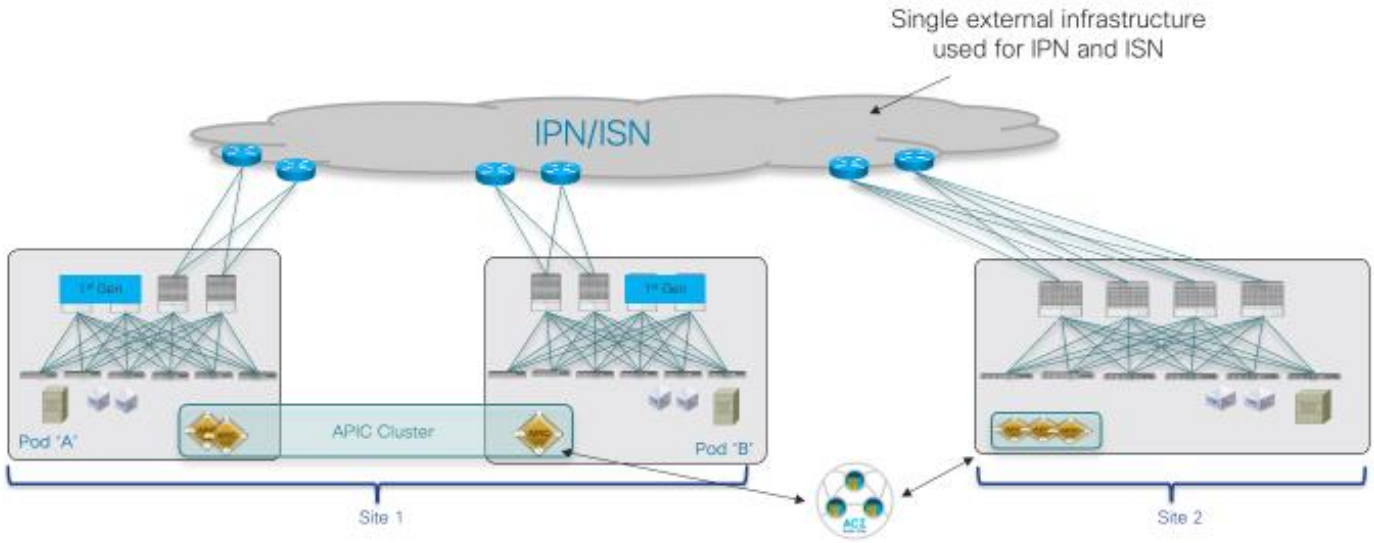


図 155.
ACI マルチポッドと ACI マルチサイト間の統合

これらのアーキテクチャを統合するための特定の導入に関する考慮事項の詳細については、『CI Multi-Site』ホワイトペーパーを参照してください。次の 2 つのセクションでは、上記のアーキテクチャを展開するために必要な設定手順について、2 つの特定の使用例を考慮して説明します。

- 同じマルチサイト ドメインへのマルチポッド ファブリックとシングルポッド ファブリックの追加
- 単一のポッド ファブリック（すでにマルチサイト ドメインの一部）のマルチポッド ファブリックへの変換

同じ Multi-Site ドメインへのマルチポッド ファブリックとシングルポッド ファブリックの追加

この使用例は、マルチポッド ファブリックがすでに展開され、同じ「論理 DC」の異なる ACI アイランド（特定の DC の場所、部屋、ホール、建物を表す）の一部としてバンドルされているシナリオの典型的な例です。別の単一のポッド ファブリック（たとえば、ディザスタ リカバリ サイト）を使用して同じ Multi-Site ドメインに追加する必要があります。

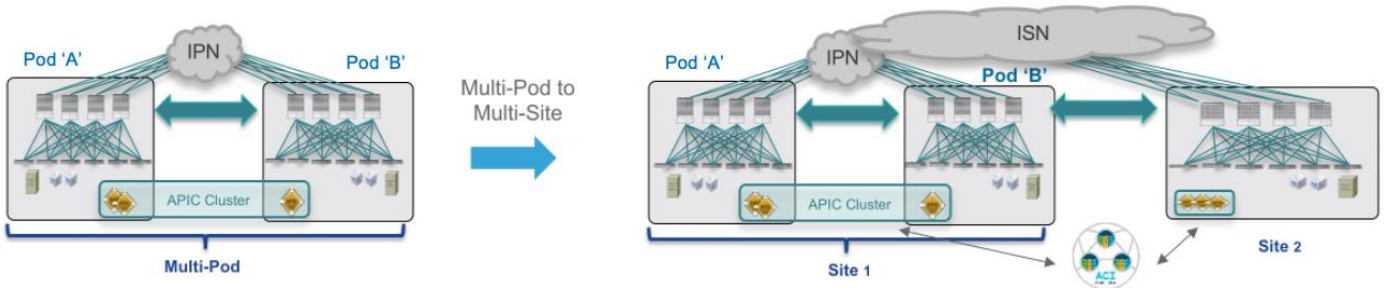


図 156.
同じ Multi-Site ドメインへのマルチポッド ファブリックとシングルポッド ファブリックの追加

初期の前提条件は次のとおりです。

- マルチポッド ファブリックはすでに稼働しているため、異なるポッドのスパイン ノードは、ポッドを相互接続する IPNインフラストラクチャ全体で EVPNをピアリングしています（つまり、「infra」テナントで必要な L3Out が手動または APIC マルチポッド ウィザードを利用してすでに作成されています）。

注： マルチポッド ファブリックを起動する方法の詳細については、以下の設定ドキュメントを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739714.html

- NDO 3.5(1) サービスが Nexus ダッシュボード コンピューティング クラスタで有効化されています。

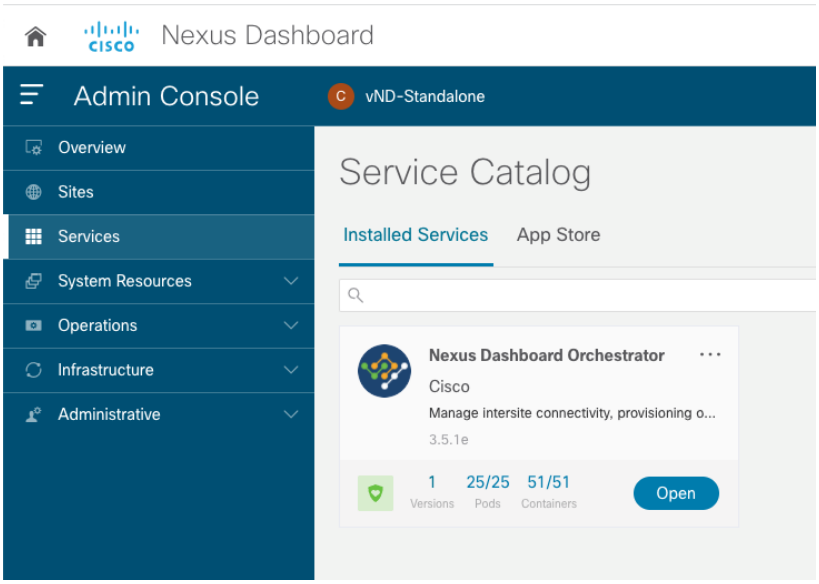


図 157.
Nexus ダッシュボードで有効なNDOサービス

注： 上記の VND スタンドアロン ノードの使用は、ラボまたは概念実（PoC）アクティビティでのみサポートされ、実稼働導入ではサポートされません。

- ACI マルチポッド ファブリックが Nexus ダッシュボードプラットフォームにオンボーディングされました。

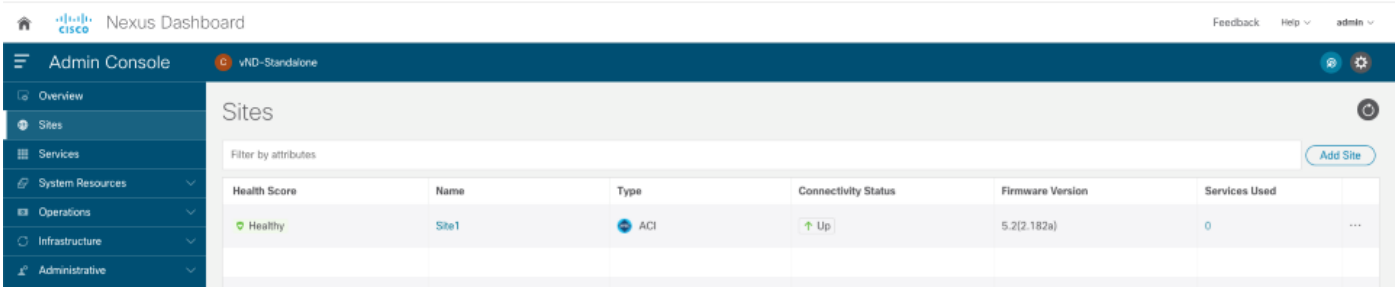


図 158.
Nexus ダッシュボードにオンボードされた Site1（ACI マルチポッド ファブリック）

ACI マルチポッド ファブリックを Multi-Site ドメインに追加する最初の手順は、Nexus Dashboard Orchestrator UI でファブリックの状態を「管理 (Managed)」に設定し、一意のサイト ID を割り当てることです。

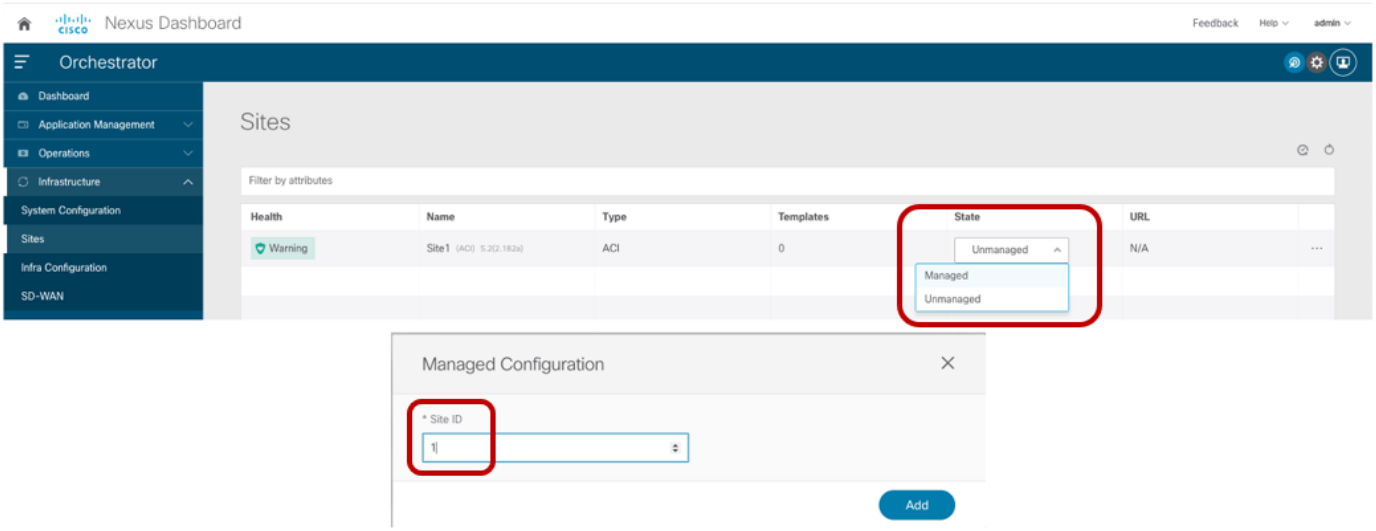


図 159.
ファブリックの状態を「管理 (Managed)」に設定し、一意のサイト ID を割り当てる

この時点で、[インフラストラクチャの設定 (Configure Infra)]セクションにアクセスして、Multi-Site ドメインにファブリックを追加するために必要なプロビジョニングを開始できます（「Nexus Dashboard Orchestrator サイトのインフラストラクチャ設定」のセクションを参照）。新しい単一のポッドファブリックを追加するシナリオとはいくつかの違いがあります。これは、インフラストラクチャテナントの L3Out 部分が APIC にすでに存在しているためです（マルチポッドファブリックのプロビジョニング中に作成されたため）。同じ L3Out をマルチサイトにも使用する必要があります。したがって、NDO はインフラ L3Out の所有権を取得し、APIC からいくつかの設定パラメータを自動的にインポートし、残りの項目を設定する責任はユーザーに委ねます。

- 次の図に示すようにサイト レベルの構成で、BGP および OSPF 関連のフィールドは、APIC のインフラ L3Out から取得した情報に基づいて自動的にプロビジョニングされます。サイト レベルで必要な唯一の設定は、「ACI Multi-Site」ノブを有効にし、L2 BUM および L3 マルチキャスト トラフィックを受信するために使用される「オーバーレイ Multicast TEP」アドレスを指定することです。このホワイトペーパ

ーの冒頭で説明したように、O-MTEP では、ACI ファブリックを接続する ISN インフラストラクチャ全体でルーティング可能な IP アドレスをプロビジョニングする必要があります。

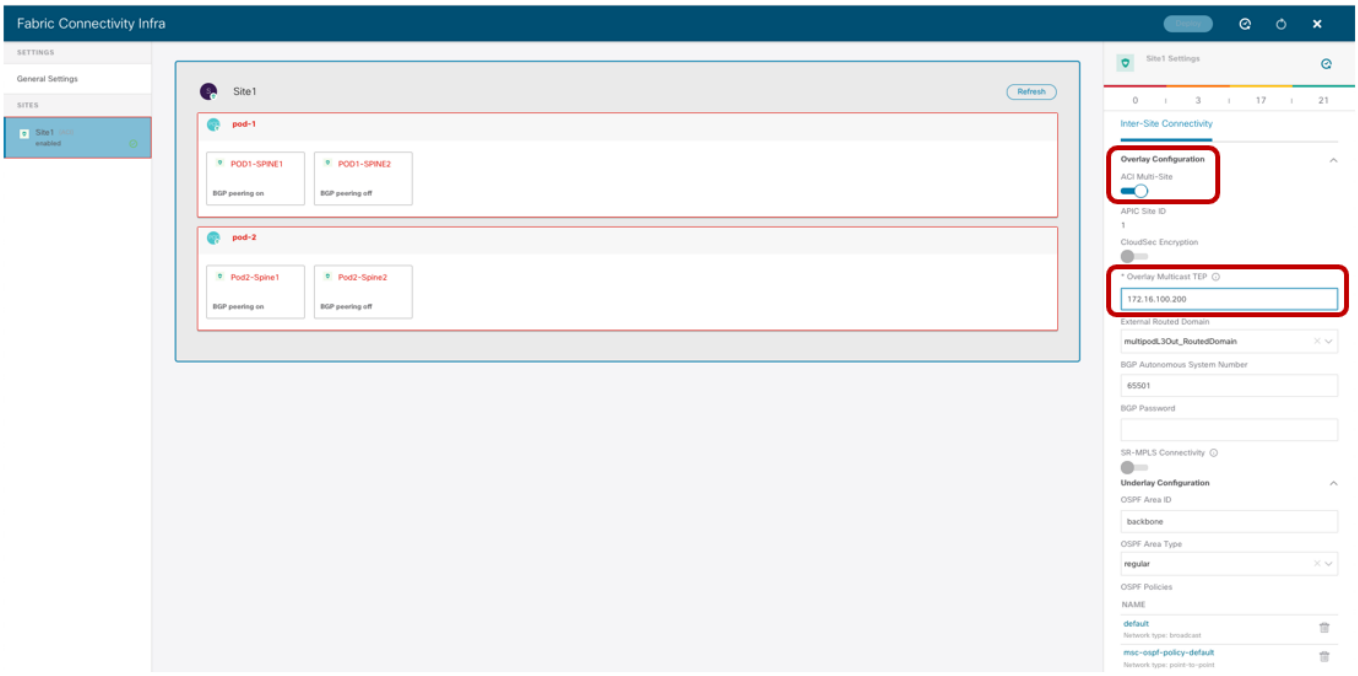


図 160.
ファブリック レベルの設定

- ポッド レベルの構成：各ポッドにプロビジョニングする必要がある唯一のパラメータは、ユニキャスト レイヤ 2 およびレイヤ 3 通信のサイト間 VXLAN トラフィックの送受信に使用されるオーバーレイ ユニキャスト TEP アドレスです。

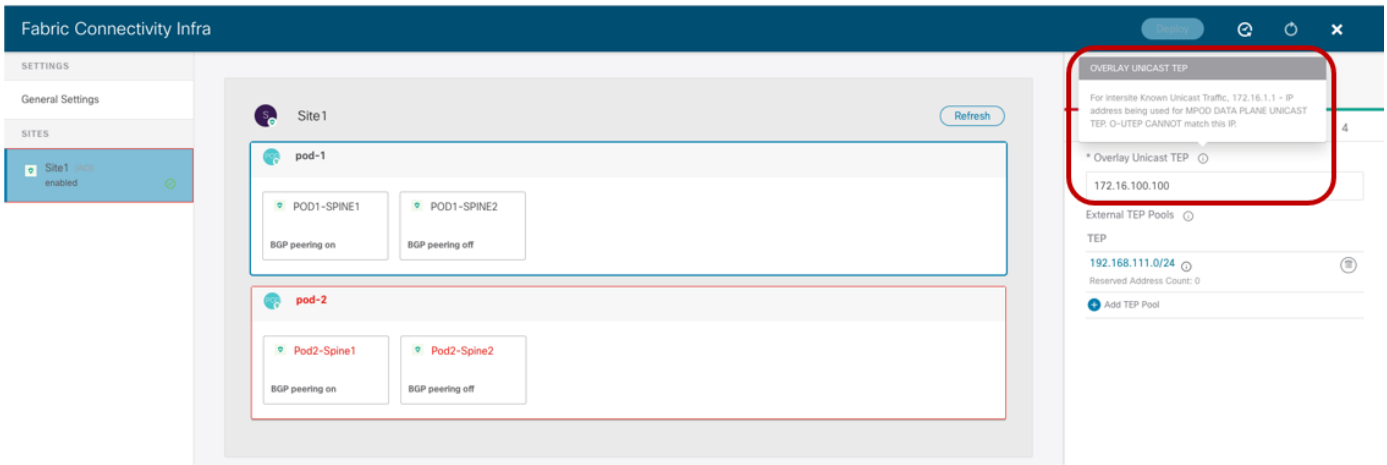


図 161.
ポッド レベルの設定

「i」アイコンの上にマウスを置いたときに表示される情報で説明されているように、プロビジョニングされた O-UTEP アドレスは、ACI マルチポッド ファブリック設定（172.16.1.1）中に APIC で設定されたデータ プレーン TEP アドレスとは異なる必要があります。O-MTEP アドレスの場合と同様に、サイト間の VXLAN データ

プレーン通信を正常に確立できるように、O-UTEP アドレスも ISN 全体でルーティング可能である必要があります。

注： リモート リーフ ノードがマルチポッド ファブリックに追加された場合、各ポッドとRL ノード間の VXLAN 通信を確立するために、各ポッドのスパインに個別のエニーキャストTEP アドレスも割り当てられます。それぞれで使用される O-UTEP マルチサイトのポッドは、RL 展開に使用されるエニーキャストTEP アドレスとも異なる必要があります。

上記の図 160 に示されているように、APIC ですでに定義されている外部 TEP プールも NDO によって自動的に継承されます (この特定の例では 192.168.111.0/24)。「サイト間 L3Out の展開」セクションで説明されているように、サイト間 L3Out 通信を有効にするには、外部 TEP プールを使用する必要があります。

- スパイン レベルの設定: スパインごとに、インフラ L3Out (およびマルチポッドに使用される) のインターフェイス部分が APIC から自動的に取得され、表示されます (以下の例のインターフェイス 1/63 および 1/64)。唯一必要な構成は、BGP スピーカーとして機能する必要があるスパインのサブセットで BGP を有効にし (つまり、リモート サイトの BGP スピーカーとの BGP EVPN 隣接関係を作成し)、これらのリモート隣接関係を確立するために使用されるループバック インターフェイスの IP アドレスを表す BGP-EVPN Router-ID を指定することです。以下に示すように、この場合、マルチポッドが必要とするポッド間の EVPN 隣接関係を確立するために、スパインにすでに割り当てられているのと同じアドレスを再利用することができます。

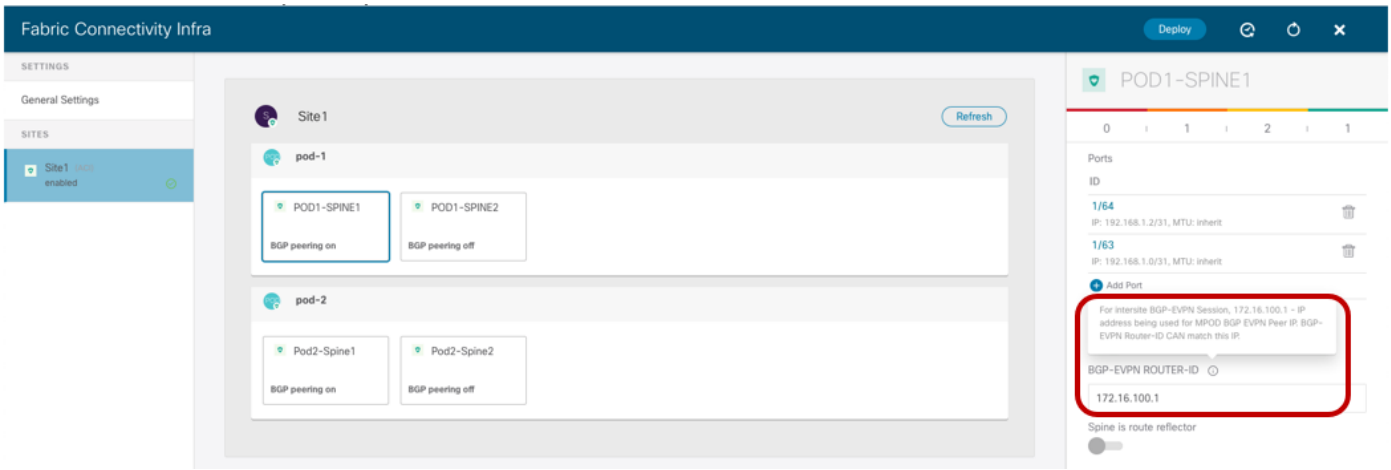


図 162.
スパイン レベルの設定

リモート サイトとの冗長 EVPN 隣接関係を提供するために、ファブリックごとに BGP スピーカーのペアを展開することを推奨します。ファブリックがマルチポッドの場合、2 つの個別のポッドの 1 つのスパインをスピーカーとしてプロビジョニングする必要があります（上記の特定の例では、Pod1-Spine 1 と Pod2-Spine1）。スピーカーではないスパインはデフォルトでフォワーダになり、ローカル スピーカーとの EVPN ピアリングのみを確立します。BGP スピーカーとフォワーダの役割、およびマルチポッドとマルチサイトを統合する際のコントロール プレーンとデータ プレーンの動作の詳細については、以下の『ACI マルチサイト』ペーパーを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.html#IntegrationofCiscoACIMultiPodandMultiSite

マルチポッドファブリックがMulti-Siteドメインに正常に追加されると、この例ではDRサイトを表す単一のポッドファブリックを追加できます。このタスクを実行する方法については、「Multi-Siteドメインへの ACIファブリックの追加」のセクションですでに説明しました。

単一のポッドファブリック（すでにMulti-Siteドメインの一部）をマルチポッドファブリックに変換する

この2番目のシナリオは、2つのシングルポッドファブリックがMulti-Siteドメインの一部としてすでに追加されている場合の開始点であるため、より簡単です。次に、2番目のポッドを追加して2つのファブリックのいずれかを拡張します。

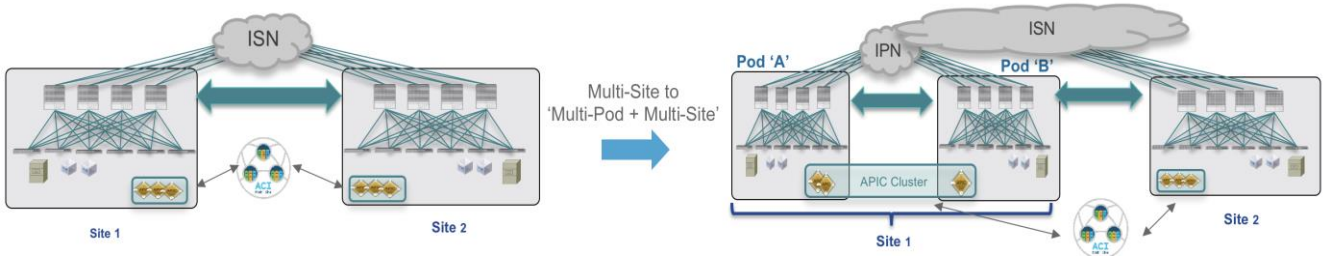


図 163.
単一のポッドファブリック（すでにMulti-Siteドメインの一部）をマルチポッドファブリックに変換する

次の図164は、最初はMulti-Siteドメインの一部である2つのシングルポッドファブリックを示しています。理解できるように、各ポッドの両方のスパインは、ファブリック レベルの復元力のためにBGPスピーカー（「BGPピアリングオン」）として展開されます。

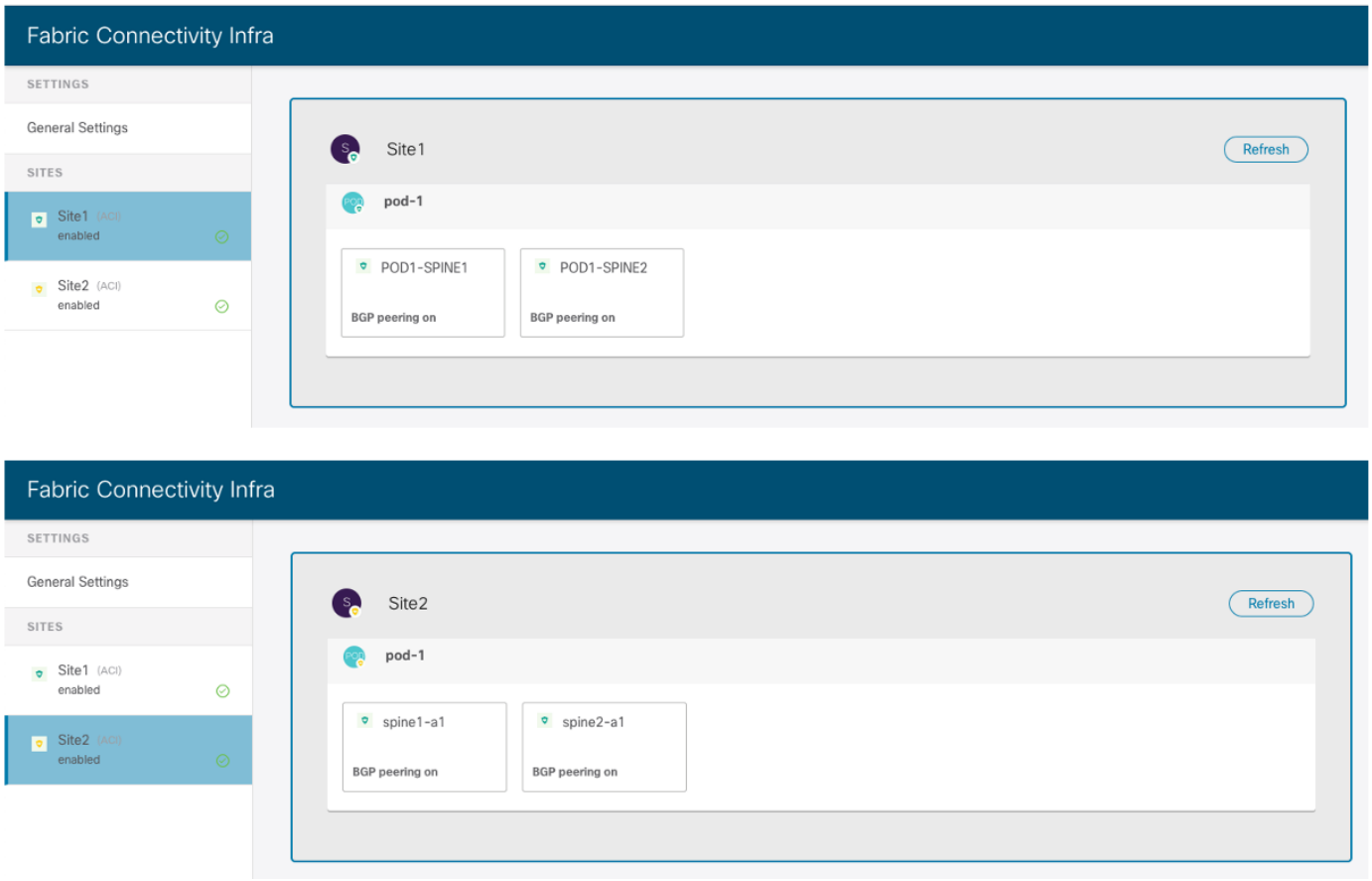


図 164.
Multi-Site ドメインの 2 つのシングルポッド ファブリック部分

最初の手順は、Site1 の APIC で ACI マルチポッド ウィザードを実行し、2 番目のポッドを追加してマルチポッド ファブリックを構築することです。マルチポッド ファブリックの構築方法の詳細については、以下のペーパーを参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739714.html

概要

この特定の使用例（CSCvu76783）に影響する特定のソフトウェア障害に注意してください。この問題は、APIC でマルチポッド ウィザードを実行して、すでに Multi-Site ドメインの一部であるファブリックに 2 番目のポッドを追加する場合にのみ発生します。マルチサイト用に作成されたインフラ L3Out がある場合、マルチポッド ウィザードはポッド 1 のノードの特定の設定の一部をスキップします。ACI リリース -5.2(1) 以前を実行中の場合では、マルチポッド ウィザードが完了したら、次のパラメータを手動で設定できます。

1. [tn-infra] > [ネットワーキング (networking)] > [L3Outs] > [インターサイト (intersite)] > [論理ノード プロファイル (Logical Node Profile)] > [プロファイル (Profile)] > [ノードの構成 (Configured Nodes）] で、各スパインの「ノード」に 2 つの項目がありません。最初に、[ルータをループバック アドレスとして使用 (Use Router as loopback address)] チェックボックスがオフになっています。2 番目に、「外部リモート ピアリング」というチェックボックスをオンにする必要があるときにオフになっています。

2. [tn-infra] > [ポリシー (Policies)] > [ファブリック外部接続ポリシー (Fabric External Connection Policy)]で作成された「ポリシー」にも 2 つの設定がありません。最初に、[ポッド ピアリング プロファイルを有効にする（Enable Pod Peering Profile)] をオンにしなければならないときに、オフになってます。2 つ目は、Fabric Ext Routing Profile に Pod-1 のネットワークがありません。

2 番目のポッドがマルチポッド ファブリックに正常に追加されると、NDO でインフラ再検出をトリガーしてポッドを Site1 に追加し、UI に表示できるようになります。

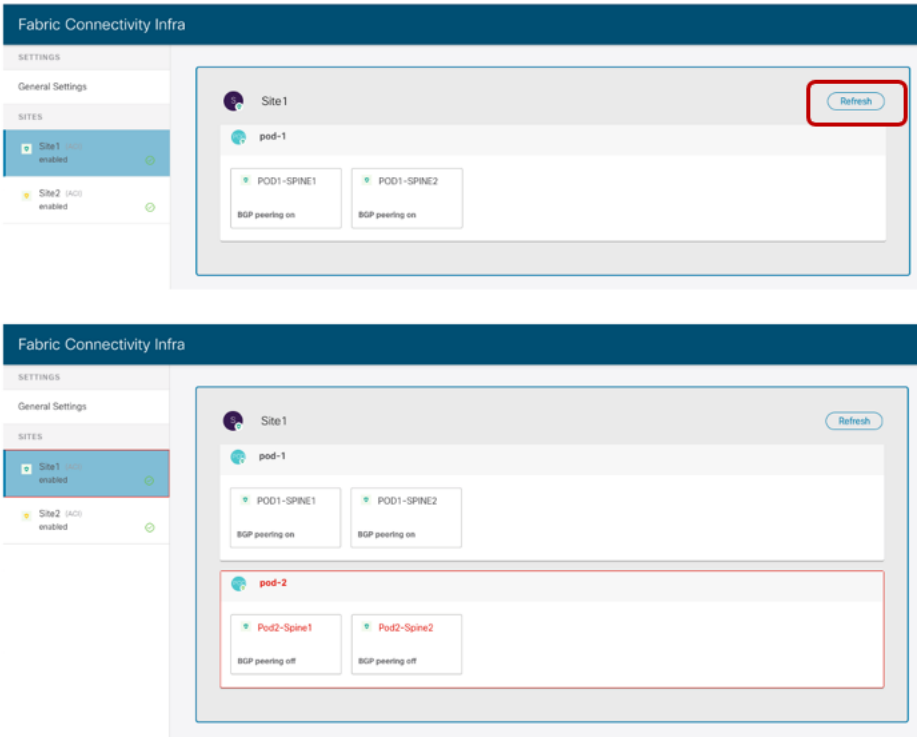


図 165.
新しく追加されたポッドを表示するためのインフラ ビューの更新

この時点で、ポッド レベルとスパイン レベルの両方で必要なパラメータをプロビジョニングすることで、Pod2 の設定を完了することができます。

- ポッド レベルの設定：各ポッドにプロビジョニングする必要がある唯一のパラメータは、オーバーレイ ユニキャスト TEP アドレス（この例では 172.16.200.100）です。外部 TEP プールは、マルチポッド ウィザード ワークフローの一部として設定されているため、APIC から自動的に継承されます。

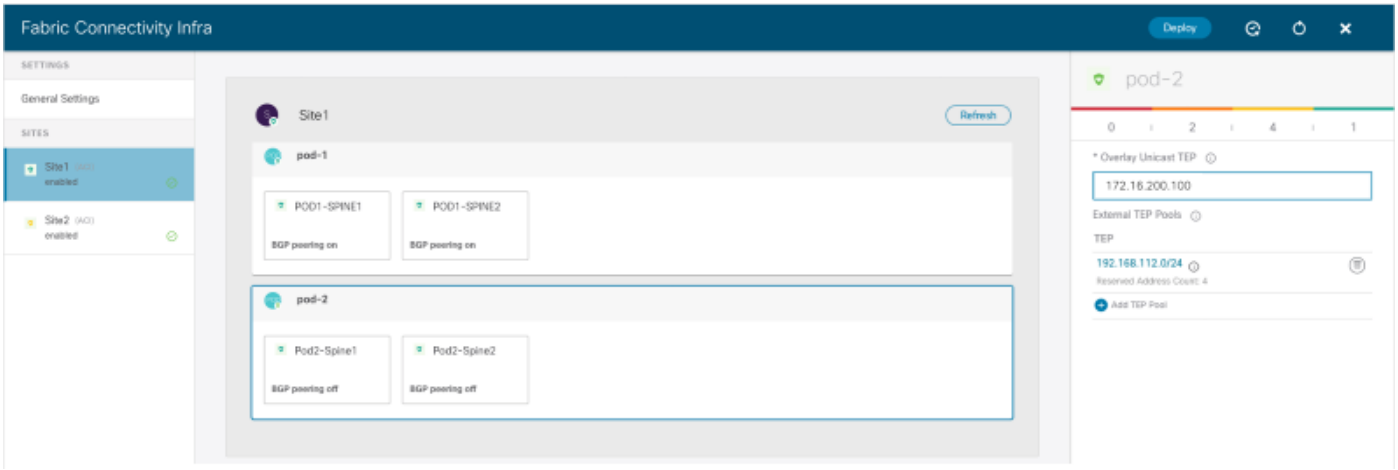


図 166.
新しく追加されたポッドのポッド レベル設定

- スパイン レベルの設定：インフラ L3Out で定義されたインターフェイスの設定は、APIC から自動的に継承されます。これは、マルチサイト トラフィックの送受信にも同じインターフェイスを使用する必要があるためです。新しいポッドで唯一必要な設定は、リモート Site2 のスパインと BGP EVPN 隣接関係を確立できるように、2 つのスパインの 1 つを BGP スピーカーとして定義することです（「BGP ピアリング (BGP peering)」ノブをオンにする）。

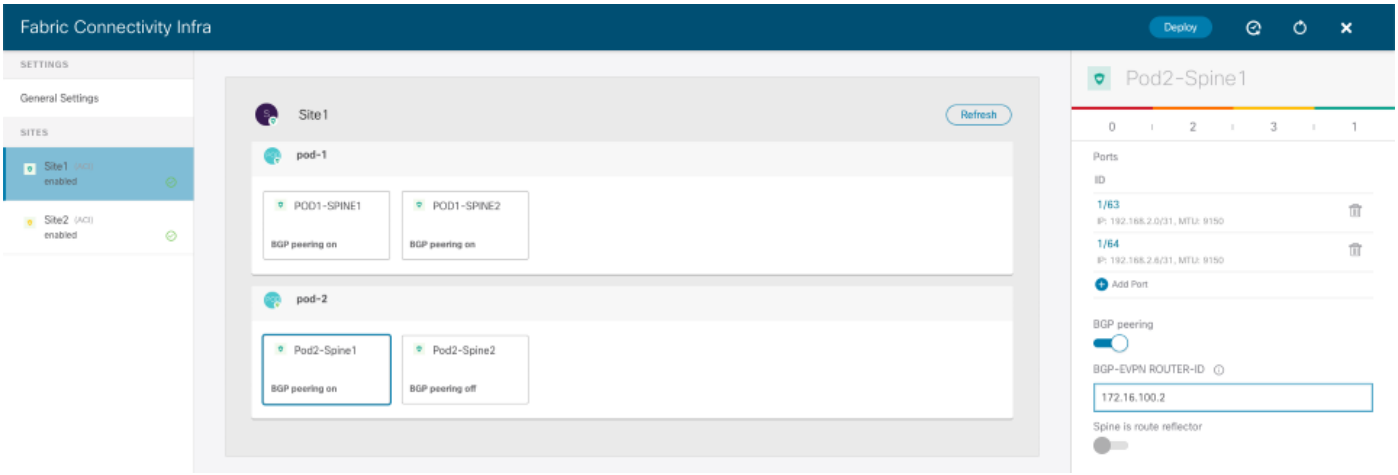


図 167.
新しく追加されたポッドのスパイン レベル設定

BGP スピーカーとして設定された 2 つのスパインが各ファブリックで十分であるため、Pod2 スパインに対して BGP を有効にした後、Pod1 スパイン 2 に対して BGP を無効にすることを推奨します。このスパインは単にフォワーダになります。

[展開 (Deploy)]ボタンをクリックすると、インフラ設定がプロビジョニングされ、マルチポッド ファブリックが Multi-Site ドメインに正しく追加されます。

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 9:00 - 17:00
0120-092-255

お問い合わせウェブフォーム
cisco.com/jp/go/vdc_callback

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
cisco.com/jp

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。