

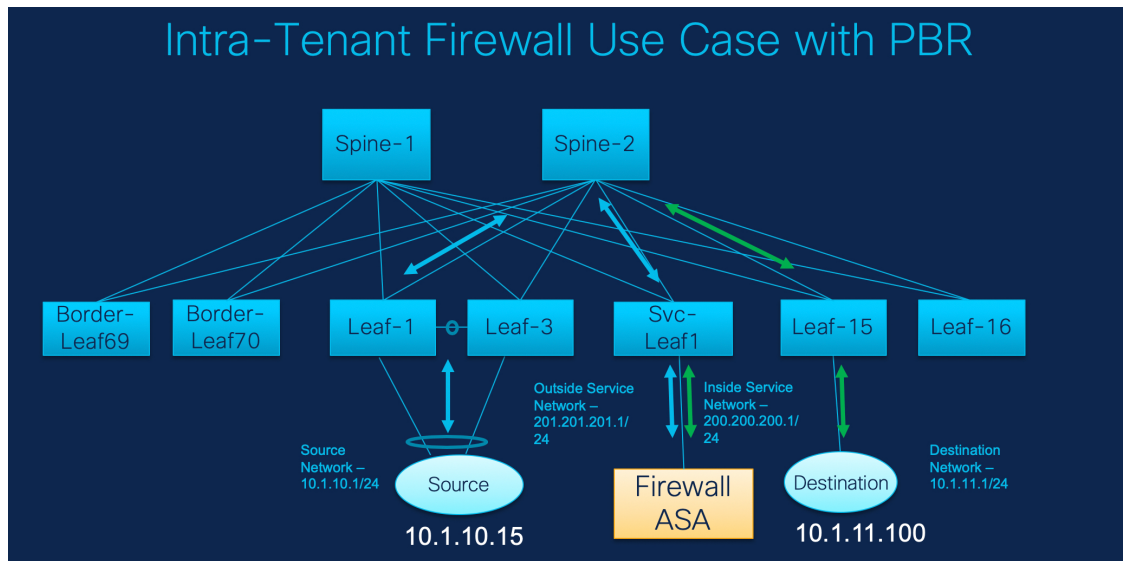


## L4-L7 サービスのユースケース

- ユースケース：ポリシーベースのルーティングを使用したテナント内ファイアウォール, on page 1
- ユースケース：eBGP ピアリングを使用したテナント間ファイアウォール, on page 21
- ユースケース：ワンアーム ロード バランサ, on page 28

### ユースケース：ポリシーベースのルーティングを使用したテナント内ファイアウォール

トポロジの詳細については、以下の図を参照してください。



このトポロジでは、Leaf1 と Leaf3 は vPC ペアであり、**Source** (10.1.10.15) に **Source Network** (10.1.10.1/24) で接続されています。サービス リーフは仮想 **Firewall ASA** に接続され、リーフ 15 は **Destination** (10.1.11.100) に接続されます。このユースケースでは、送信元ネットワークは「クライアント」を指し、宛先は「サーバー」を指します。

## 1. サービスノードの作成

**Source** から **Destination** へ横断するトラフィックはすべて外部サービス ネットワークに送られる必要があります、ファイアウォールはトラフィックを許可または拒否する機能を実行します。その後、このトラフィックは内部サービスネットワークにルーティングされ、宛先ネットワークに送信されます。トポロジはステートフルであるため、宛先から送信元に戻ってくるトラフィックは同じパスをたどります。

次に、DCNM でサービス リダイレクトを実行する方法を見てみましょう。

**Note**

- この使用例では、**Site\_A** VXLAN ファブリックをプロビジョニングする方法については説明していません。このトピックの詳細については、『Cisco Nexus LAN ファブリックの構成ガイド』を参照してください。
- このユースケースは、サービス ノード（ファイアウォールまたはロードバランサ）の構成には対応していません。

[制御 (Control)] > [ファブリック (Fabrics)] > [サービス (Services)] の順に選択します。

このユースケースは、次の手順で構成されます。

## 1. サービスノードの作成

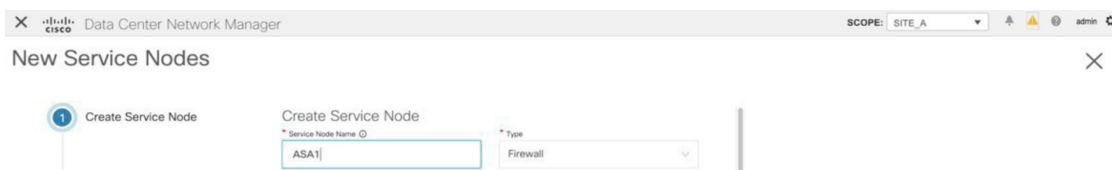
**Procedure**

**ステップ 1** [範囲 (Scope)] ドロップダウンリストから、**Site\_A** を選択します。

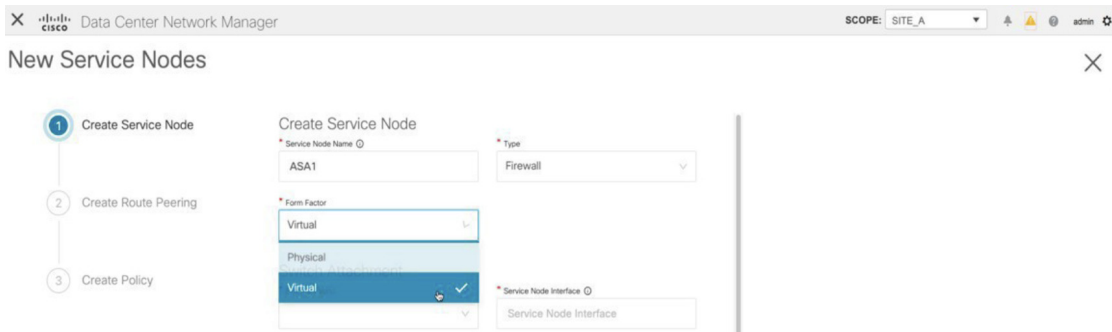
**ステップ 2** [追加 (Add)] アイコン ([サービスノード (Service Nodes)] ウィンドウ) をクリックします。



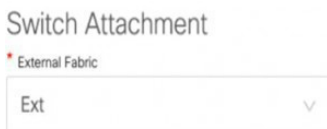
- ステップ 3** ノード名を入力し、[ファイアウォール (Firewall)] を指定します ([タイプ (Type)] ドロップダウンボックス)。[サービスノード名 (Service Node Name)] は一意である必要があります。



- ステップ 4** [フォームファクター (Form Factor)] ドロップダウンリストから、[仮想 (Virtual)] を選択します。



- ステップ 5** [スイッチの接続 (Switch Attachment)] セクションで、[外部ファブリック (External Fabric)] ドロップダウンリストから、サービスノード (たとえば、ASA ファイアウォール) が配置されている外部ファブリックを選択します。サービスノードは外部ファブリックに属している必要があることに注意してください。これは、サービスノードを作成する際の前提条件です。



- ステップ 6** サービスリーフに接続するサービスノードのインターフェイス名を入力します。

## 2. ルートピアリングの作成

\* Service Node Interface ⓘ

Giga0/0

**ステップ7** サービスリーフである接続されたスイッチと、サービスリーフ上の対応するインターフェイスを選択します。

\* Attached Switch ⓘ      \* Attached Switch Interface ⓘ

SVC-LEAF1      Ethernet1/34

**ステップ8** `service_link_trunk` テンプレートを選択します。DCNM は、トランク、ポートチャネル、および vPC リンク テンプレートをサポートします。[リンク テンプレート (Link Template)] ドロップダウン リストで使用可能なリンク テンプレートは、選択した [接続スイッチ インターフェイス (Attached Switch Interface)] のタイプに基づいてフィルタリングされます。

Link Template

service\_link\_trunk

**ステップ9** 必要に応じて、[一般パラメータ (General Parameters)] と [詳細 (Advanced)] パラメータを指定します。一部のパラメータには、デフォルト値が事前に入力されています。

General Parameters      Advanced

MTU ⓘ      SPEED ⓘ

jumbo      Auto

Trunk Allowed Vlans ⓘ      Enable BPDU Guard ⓘ

none      no

Enable Port Type Fast ⓘ      Enable Interface ⓘ

Next

**ステップ10** [次へ (Next)] をクリックして、作成したサービス ノードを保存します。

## 2. ルートピアリングの作成

サービスリーフとサービスノード間のピアリングを構成しましょう。

## Procedure

- ステップ 1** ピアリング名を入力し、[テナント内ファイアウォール (Intra-Tenant Firewall)] を [展開 (Deployment)] ドロップダウン リストから選択します。

\* Peering Name ①

peering1

\* Deployment

Intra-Tenant Firewall ^

Intra-Tenant Firewall ✓

Inter-Tenant Firewall

Inside Network v

Inside Network

\* VRF

v

- ステップ 2** [内部ネットワーク (Inside Network)] で、[VRF] ドロップダウンリストから既に存在している VRF を選択し、[内部ネットワーク (Inside Network)] を [ネットワーク タイプ (Network Type)] で選択します。

[サービス ネットワーク (Service Network)] の名前を入力し、[Vlan ID] を指定します。[提案 (Propose)] をクリックして、DCNM が次に使用可能な VLAN ID をファブリック設定で指定されたサービス ネットワーク VLAN ID の範囲からフェッチできるようにすることもできます。デフォルトの[サービス ネットワーク テンプレート (Service Network Template)] は **Service\_Network\_Universal** です。

[一般パラメータ] タブで、サービス ネットワークのゲートウェイアドレスを指定します。[ネクストホップ IP アドレス (Next Hop IP Address)] を指定します。このネクストホップアドレスは、「内部サービス ネットワーク」サブネット内にある必要があります。[詳細設定 (Advanced)] タブの、デフォルトの [ルーティング タグ (Routing Tag)] 値は 12345 です。

## 2. ルート ペアリングの作成

## Inside Network

<p>* VRF</p> <input type="text" value=""/>	<p>* Network Type</p> <input type="text" value="Inside Network"/>
<p>* Service Network</p> <input type="text" value="service_net_inside"/>	<p>* Vlan ID</p> <input type="text" value="2300"/> <input type="button" value="Propose"/>
<p>* Service Network Template</p> <input type="text" value="Service_Network_Universal"/>	

General Parameters    Advanced

<p>* IPv4 Gateway/NetMask ⓘ</p> <input type="text" value="200.200.200.1/24"/>	<p>IPv6 Gateway/Prefix ⓘ</p> <input type="text" value=""/>
<p>Vlan Name ⓘ</p> <input type="text" value=""/>	<p>Interface Description</p> <input type="text" value=""/>
<p>* Next Hop IP Address ⓘ</p> <input type="text" value="200.200.200.200"/>	

**ステップ 3** [外部ネットワーク (Outside Network)] で必要なパラメータを指定し、[リバース トラフィックのネクストホップ IP アドレス (Next Hop IP Address for Reverse Traffic)] を指定します。リバース トラフィックのこのネクストホップアドレスは、「外部サービス ネットワーク」サブネット内にある必要があります。

## Outside Network

* VRF	VRF_51000	* Network Type	Outside Network
* Service Network	service_net_outside	* Vlan ID	2301 <span>Propose</span>
* Service Network Template	Service_Network_Universal		

## General Parameters    Advanced

* IPv4 Gateway/NetMask ⓘ	201.201.201.1/24	IPv6 Gateway/Prefix ⓘ	
Vlan Name ⓘ		Interface Description	
Next Hop IP Address for Reverse Traffic ⓘ	201.201.201.201		

ステップ4 [次へ (Next)] をクリックして、作成したルートピアリングを保存します。

### 3. サービスポリシーの作成

#### Procedure

ステップ1 ポリシーの名前を指定し、[ピアリング名 (Peering Name)] ドロップダウンリストからルートピアリングを選択します。

* Policy Name ⓘ	policy1	Peering Name	peering1
-----------------	---------	--------------	----------

## 3. サービス ポリシーの作成

**ステップ 2** [送信元 VRF 名 (Source VRF Name)] および [接続先 VRF 名 (Destination VRF Name)] ドロップダウンリストから、送信元および接続先 VRF を選択します。テナント内ファイアウォール展開の送信元と宛先の VRF は同じである必要があります。

The screenshot shows two dropdown menus. The left one is labeled 'Source VRF Name' and has 'VRF\_51000' selected. The right one is labeled 'Destination VRF Name' and also has 'VRF\_51000' selected.

**ステップ 3** [送信元ネットワーク (Source Network)] および [接続先ネットワーク (Destination Network)] ドロップダウンリストから、送信元ネットワークと接続先ネットワークを選択するか、[制御 (Control)] > [ファブリック (Fabrics)] > [ネットワーク (Networks)] ウィンドウで定義されたネットワークサブネット内にある送信元ネットワークまたは接続先ネットワークを指定します。

The screenshot shows two text input fields. The left one is labeled 'Source Network' and contains 'VLAN\_10: 10.1.10.1/24'. The right one is labeled 'Destination Network' and contains 'VLAN\_11: 10.1.11.1/24'.

**ステップ 4** ネクスト ホップおよびリバース ネクスト ホップのフィールドは、ルートピアリングの作成中に入力された値に基づいて入力されます。[リバース ネクスト ホップ IP アドレス (Reverse Next Hop IP Address)] フィールドの横にあるチェックボックスをオンにして、リバーストラフィックに対するポリシーの適用を有効にします。

The screenshot shows two fields. The first is 'Next Hop IP Address' with a dropdown menu showing '201.201.201.201'. The second is 'Reverse Next Hop IP Address' with a checked checkbox and the value '200.200.200.200'. Below these is a 'Policy Template Name' dropdown menu showing 'service\_pbr'.

**ステップ 5** ポリシー テンプレートの [一般パラメータ (General Parameters)] タブで、[ip] を [プロトコル (Protocol)] ドロップダウンリストから選択します。また、[任意 (any)] を [送信元ポート (Source Port)] および [宛て先ポート (Destination Port)] フィールドで指定します。



**Note** [ip] および [icmp] プロトコルの場合、[任意 (any)] の送信元ポートと宛先ポートが常に ACL 生成に使用されます。別のプロトコルを選択して、対応する送信元ポートと宛先ポートを指定することもできます。DCNMは、既知のポート番号をスイッチで必要な形式に一致するように変換します。たとえば、ポート 80 を「www」に変換できます。

The screenshot shows the 'General Parameters' tab of an ACL configuration page. It contains three input fields: '\* Protocol' with a dropdown menu showing 'ip', '\* Source Port' with a text input field containing 'any', and '\* Destination Port' with a text input field containing 'any'. Below these fields are two buttons: a light blue 'Back' button and a dark blue 'Create' button.

**ステップ 6** [詳細 (Advanced)] タブでは、デフォルトで、[ルートマップアクション (Route Map Action)] には [permit (許可)]、[ネクストホップオプション (Next Hop Option)] には [none (なし)] が選択されています。必要に応じて、これらの値を変更し、ACL名とルートマップの一致シーケンス番号をカスタマイズできます。詳細については、『レイヤ4～レイヤ7サービス構成ガイド』の「[テンプレート](#)」を参照してください。

The screenshot shows the 'Advanced' tab of the ACL configuration page. It contains six input fields arranged in two columns. The left column has: 'Route Map Action' dropdown set to 'permit', 'ACL Name (auto-generated if not specified)' empty text input, and 'Route map match number (auto-generated if not specified)' empty text input. The right column has: 'Next Hop Option' dropdown set to 'none', 'ACL Name for reversed traffic (auto-generated if not specified)' empty text input, and 'Route map match number for reversed traffic (auto-generated if not specified)' empty text input.

## 4. ルートピアリングを展開する

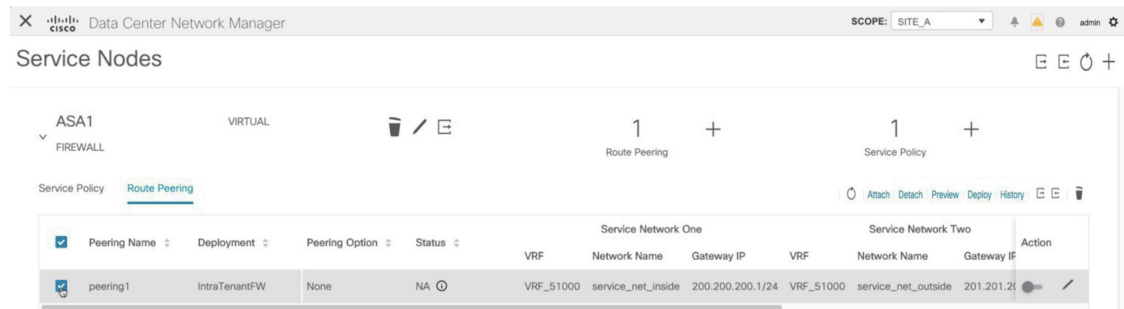
ステップ7 [作成 (Create)] をクリックして、作成したサービスポリシーを保存します。

これで、リダイレクトのフローを実行して指定する手順は完了です。

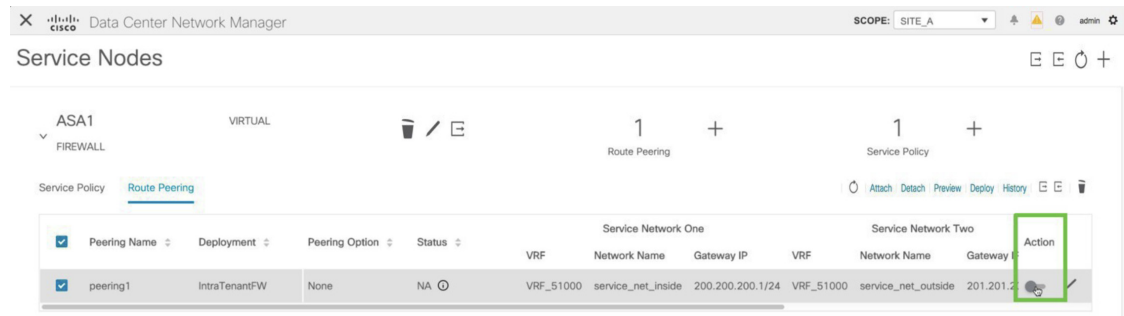
## 4. ルートピアリングを展開する

## Procedure

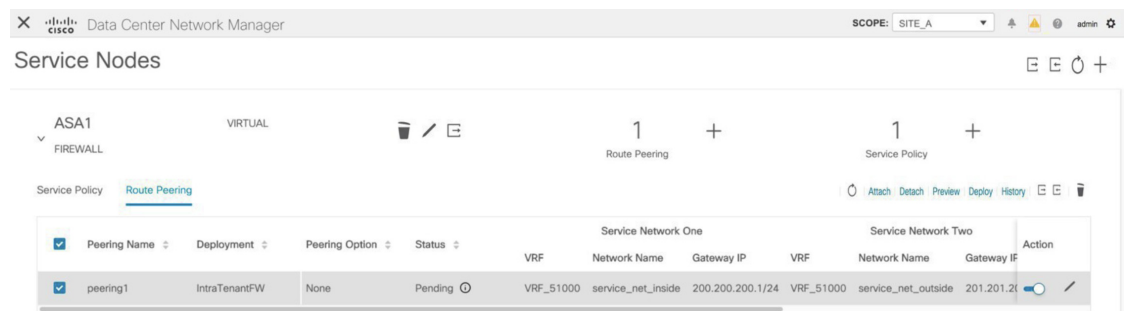
ステップ1 [サービスノード (Service Nodes)] ウィンドウの [ルートピアリング (Route Peering)] タブで、必要なピアリングを選択します。



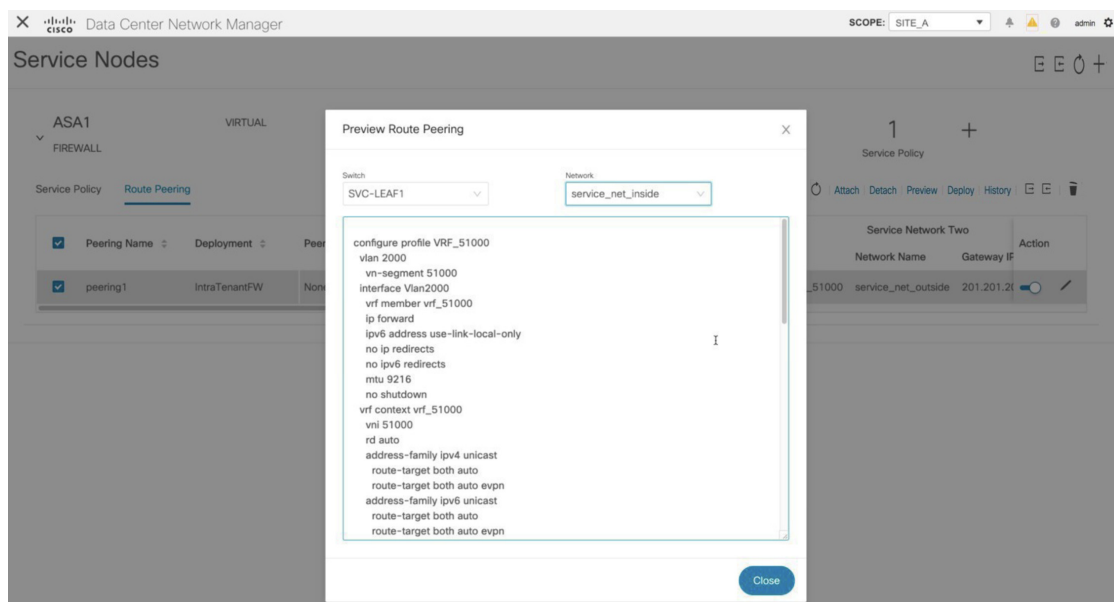
ステップ2 [アクション (Action)] の下のトグルボタンをクリックして、サービスネットワークをサービスリーフに接続します。



ステップ3 [プレビュー (Preview)] をクリックして、サービスリーフにプッシュされる構成を表示します。

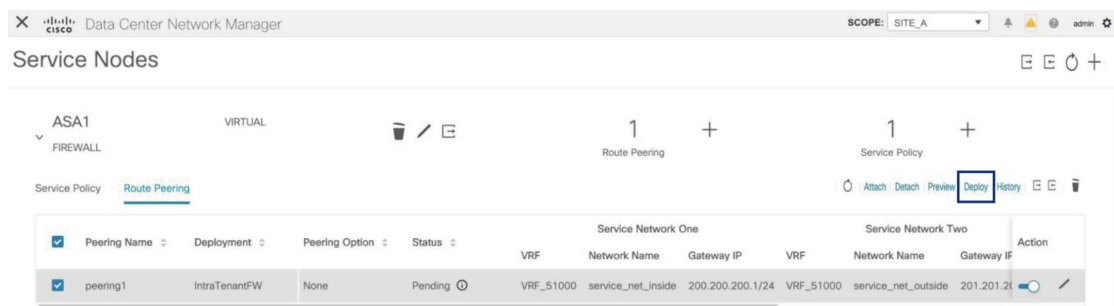


以前は、内部および外部のサービスネットワークを作成していました。サービスリーフにプッシュされるこれらのネットワーク構成を表示できます。

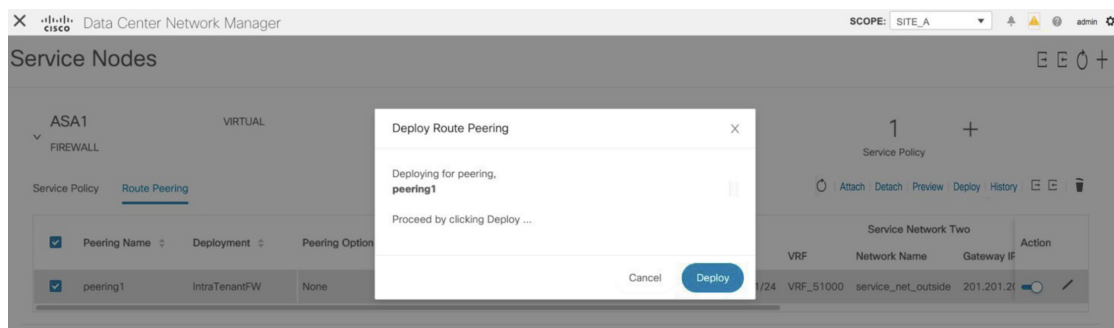


**ステップ 4** [閉じる (Close)] をクリックして、[ルートピアリングのプレビュー (Preview Route Peering)] ウィンドウを閉じます。

**ステップ 5** [サービス ノード (Service Nodes)] ウィンドウで [展開 (Deploy)] をクリックして、接続されたスイッチ (ルートピアリング用のサービスリーフ) に構成を展開します。

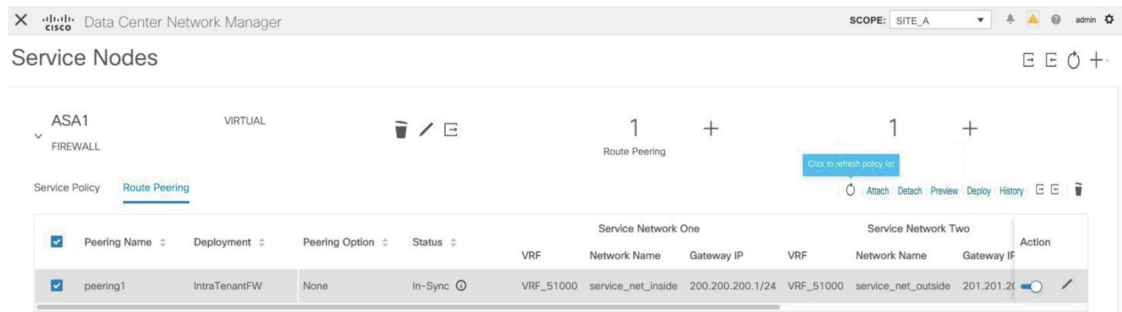


ポップアップ ウィンドウの [展開 (Deploy)] ボタンをクリックして、展開を確認します。



## 5. サービスポリシーの展開

**ステップ6** 最新のピアリング構成のアタッチメントと展開のステータスについては、[更新 (Refresh)] アイコンをクリックします。

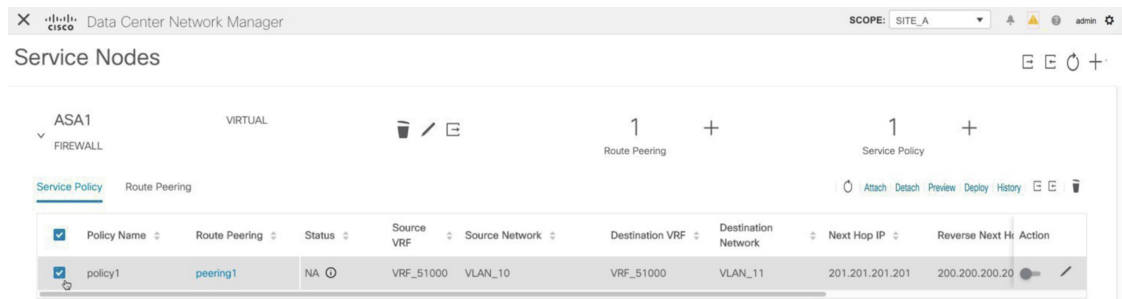


## 5. サービスポリシーの展開

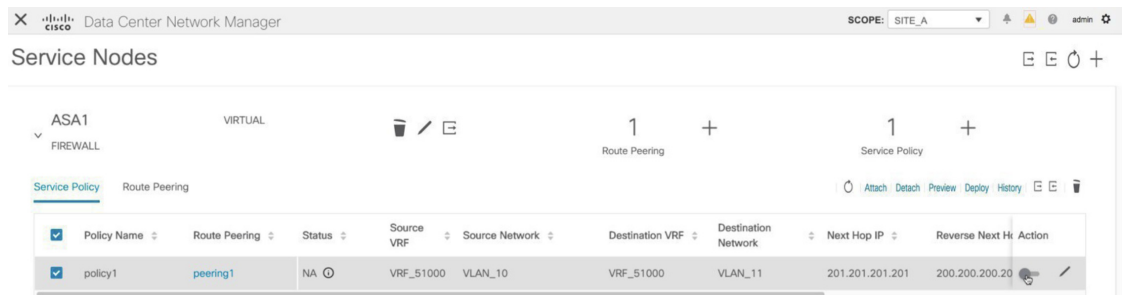
サービスポリシーを展開するには、次の手順を実行します。このポリシーの対応する構成は、送信元および接続先ネットワークが接続されているスイッチおよびサービスリーフに展開されます。

## Procedure

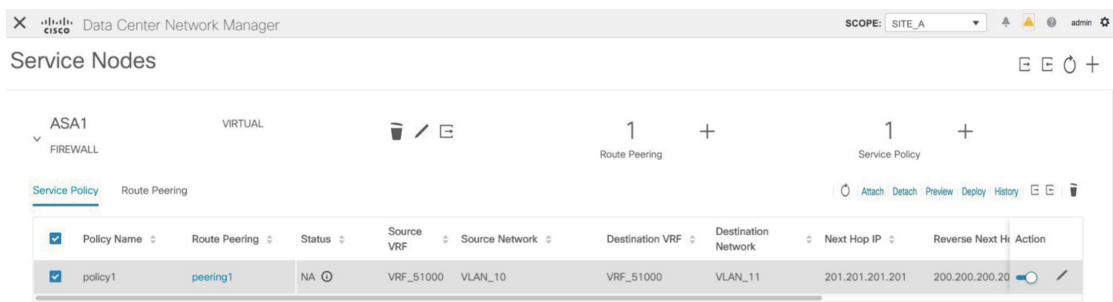
**ステップ1** [サービスポリシー (Service Policy)] タブで、必要なポリシーの横にあるチェックボックスを選択します。



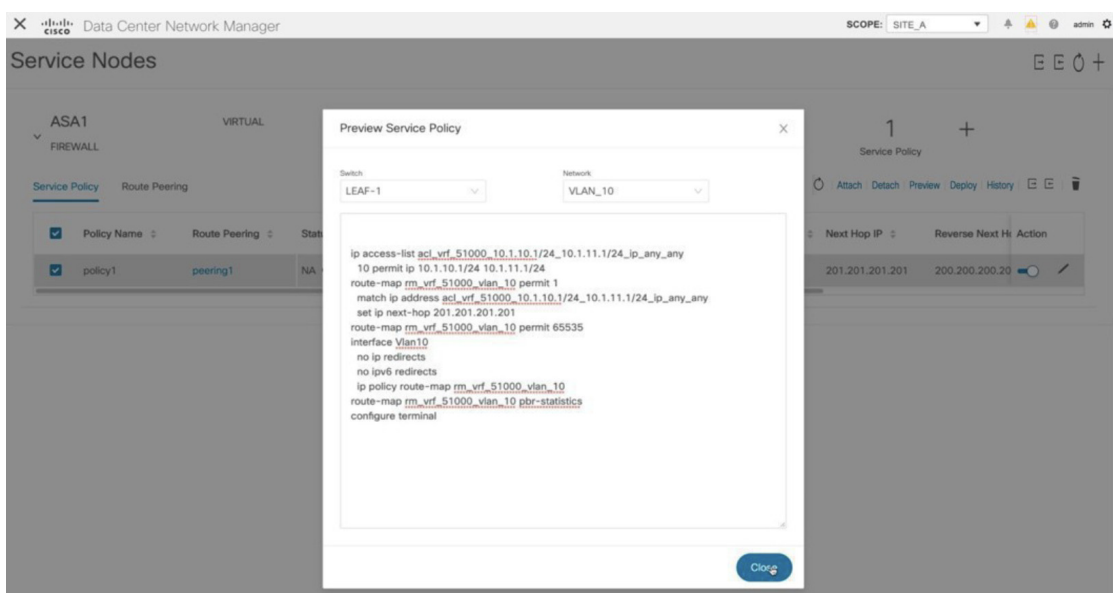
**ステップ2** [アクション (Action)] の下のトグルボタンをクリックして、このポリシーを有効にします。



**ステップ3** [プレビュー (Preview)] をクリックして、選択したネットワークの構成を表示します。

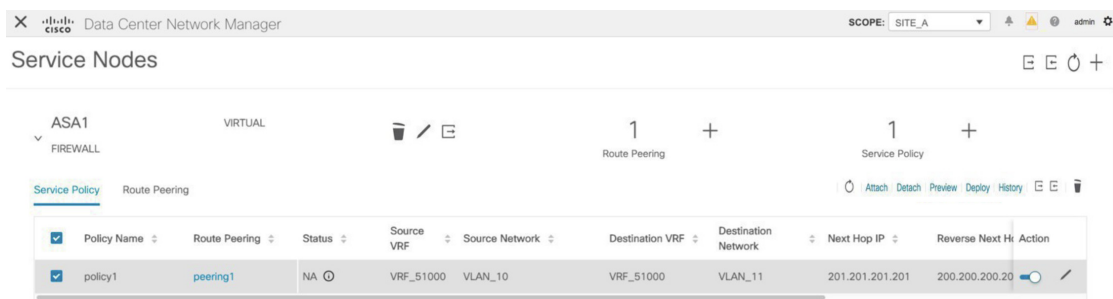


**ステップ 4** ドロップダウンリストからスイッチと送信元、接続先、またはサービスネットワークを選択して、選択したスイッチ上の特定の送信元、接続先、またはサービスネットワークの目的の構成を表示します。このウィンドウでは、ルートマップで作成されるアクセスリストがあることがわかります。この構成は SVI にプッシュされます。



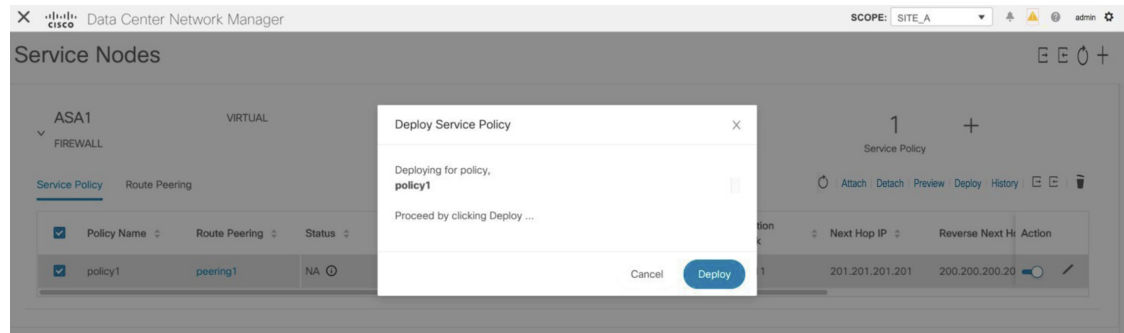
[閉じる (Close)] をクリックして、[サービスポリシーのプレビュー (Preview Service Policy)] ウィンドウを閉じます。

**ステップ 5** [サービス ノード (Service Nodes)] ウィンドウで [展開 (Deploy)] をクリックして、接続されたスイッチ (サービス リーフ) に構成を展開します。

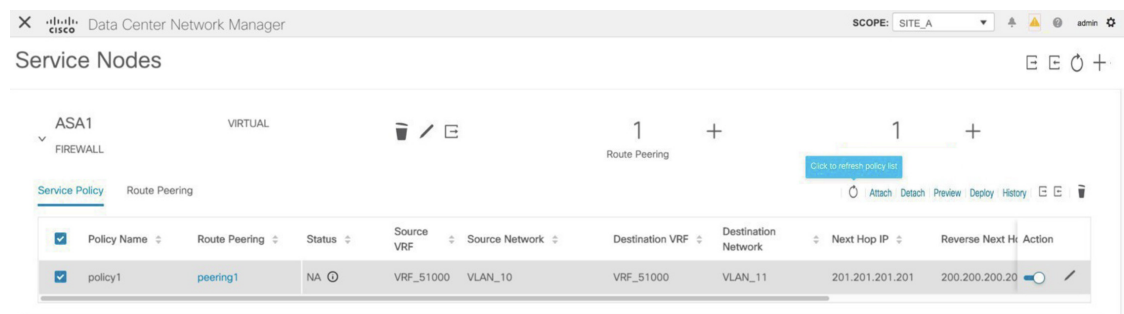


ポップアップ ウィンドウの [展開 (Deploy)] ボタンをクリックして、展開を確認します。

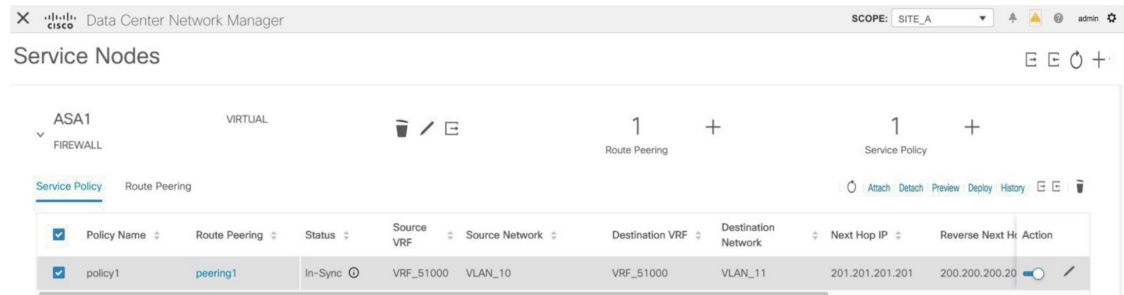
## 6. 統計情報を表示する



**ステップ6** 最新のポリシーアタッチメントと展開のステータスについては、[更新 (Refresh)] アイコンをクリックします。



このポリシーは、送信元ネットワークと接続先ネットワークが接続されているスイッチ、およびサービスリーフにプッシュされます。ポリシーをプッシュすると、ステータス列に **[In-Sync]** と表示されます。



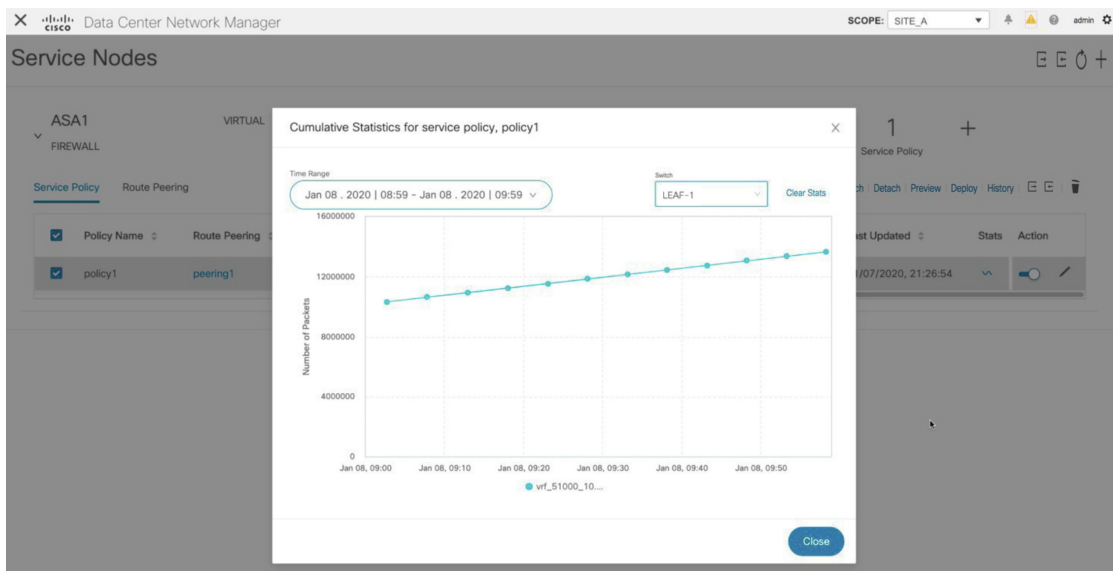
## 6. 統計情報を表示する

それぞれのリダイレクトポリシーが展開されたので、ping トラフィックはファイアウォールにリダイレクトされます。

DCNM でこのシナリオを視覚化するには、[Stats] 列の下にあるアイコンをクリックします。

Policy Name	Route Peering	Destination VRF	Destination Network	Next Hop IP	Reverse Next Hop IP	Reverse Enabled	Last Updated	Stats	Action
policy1	peering1	1000	VLAN_11	201.201.201.201	200.200.200.200	Yes	01/07/2020, 21:26:54		

指定した時間範囲のポリシーの累積統計を表示できます。

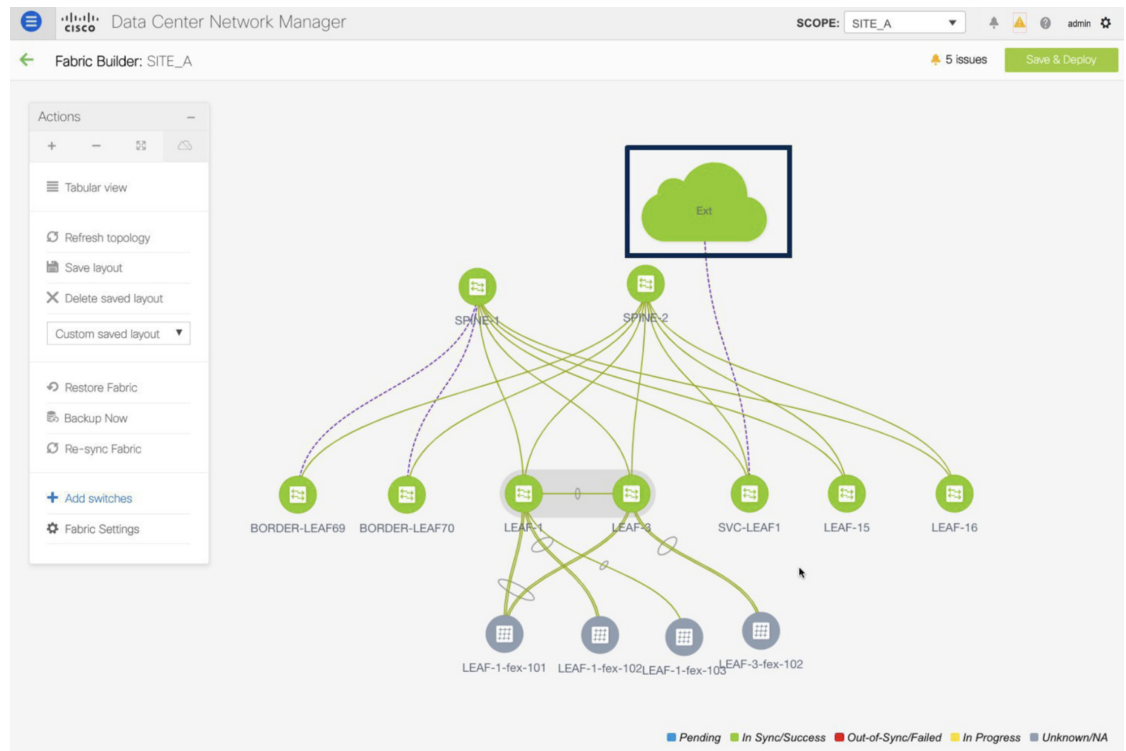


送信元スイッチの転送トラフィック、接続先スイッチのリバーストラフィック、およびサービススイッチの両方向のトラフィックの統計が表示されます。

## 7. Fabric Builder でのトラフィック フローの表示

外部ファブリックのサービス ノードはサービス リーフにアタッチされ、この外部ファブリックはファブリック ビルダの DCNM トポロジでクラウドアイコンとして表示されます。

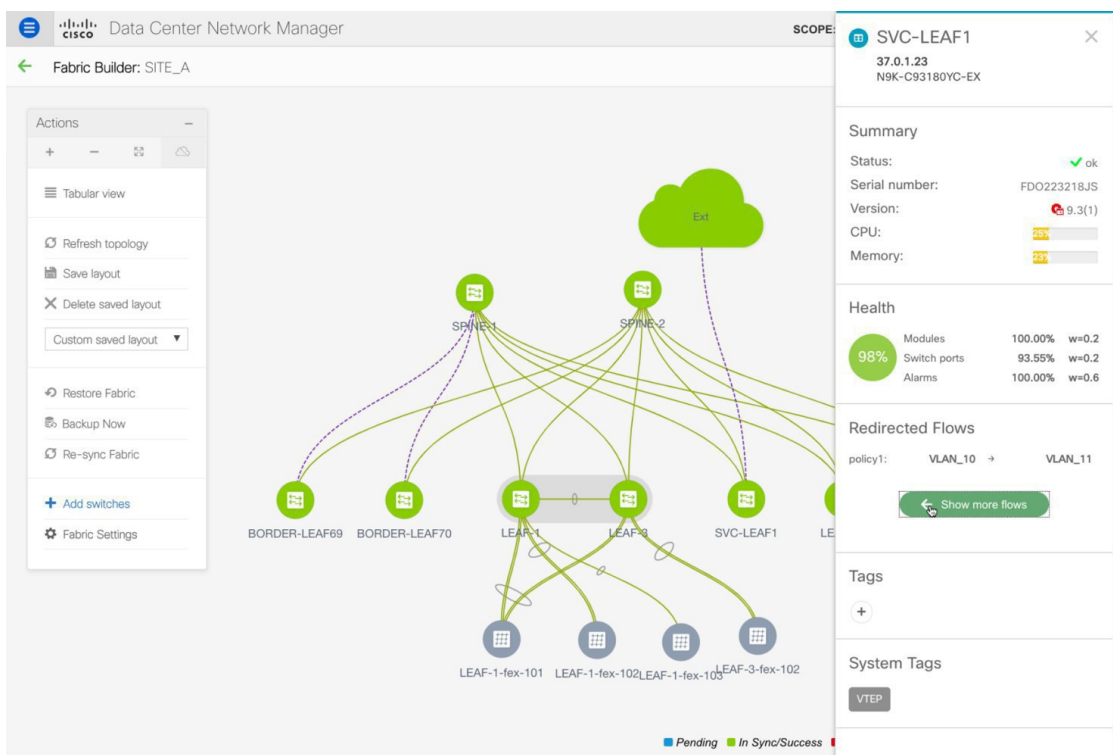
## 7. Fabric Builder でのトラフィック フローの表示



## Procedure

- ステップ 1** サービスリーフをクリックし、[さらにフローを表示 (Show more flows)] をクリックします。リダイレクトされたフローを確認できます。



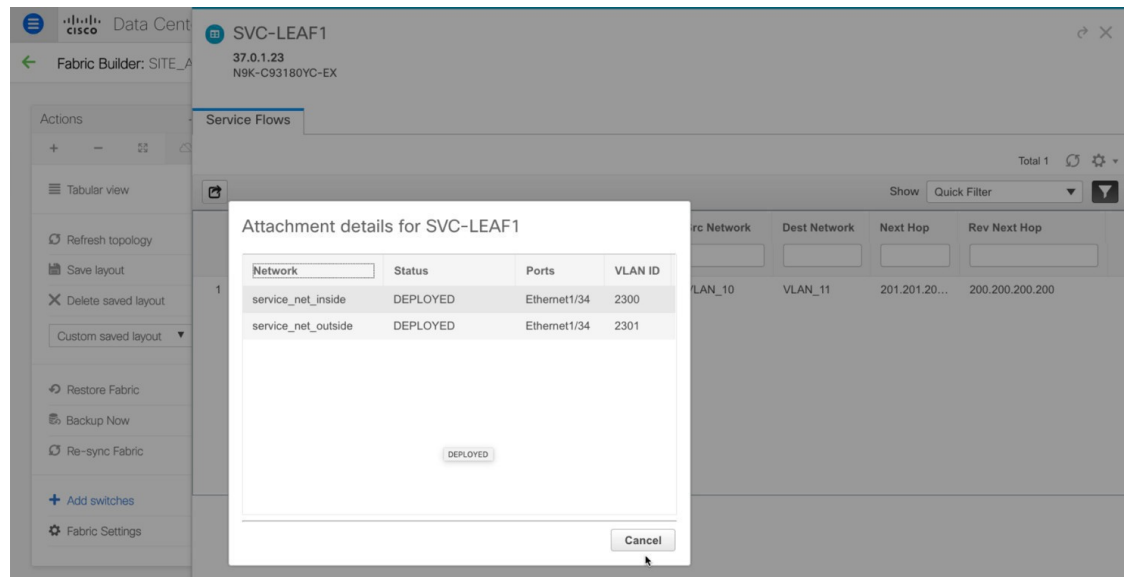


ステップ 2 [詳細 (Details)] ([サービス フロー (Service Flows)] ウィンドウ) をクリックして、付属ファイルの詳細を表示します。

The screenshot shows the 'Service Flows' window for SVC-LEAF1. It features a table with the following columns: Node, Policy, Details, Peering, VRF, Src Network, Dest Network, Next Hop, and Rev Next Hop. A single row is displayed with the following values:

Node	Policy	Details	Peering	VRF	Src Network	Dest Network	Next Hop	Rev Next Hop
1 ASA1	policy1	Details	peering1	VRF_51000	VLAN_10	VLAN_11	201.201.20...	200.200.200.200

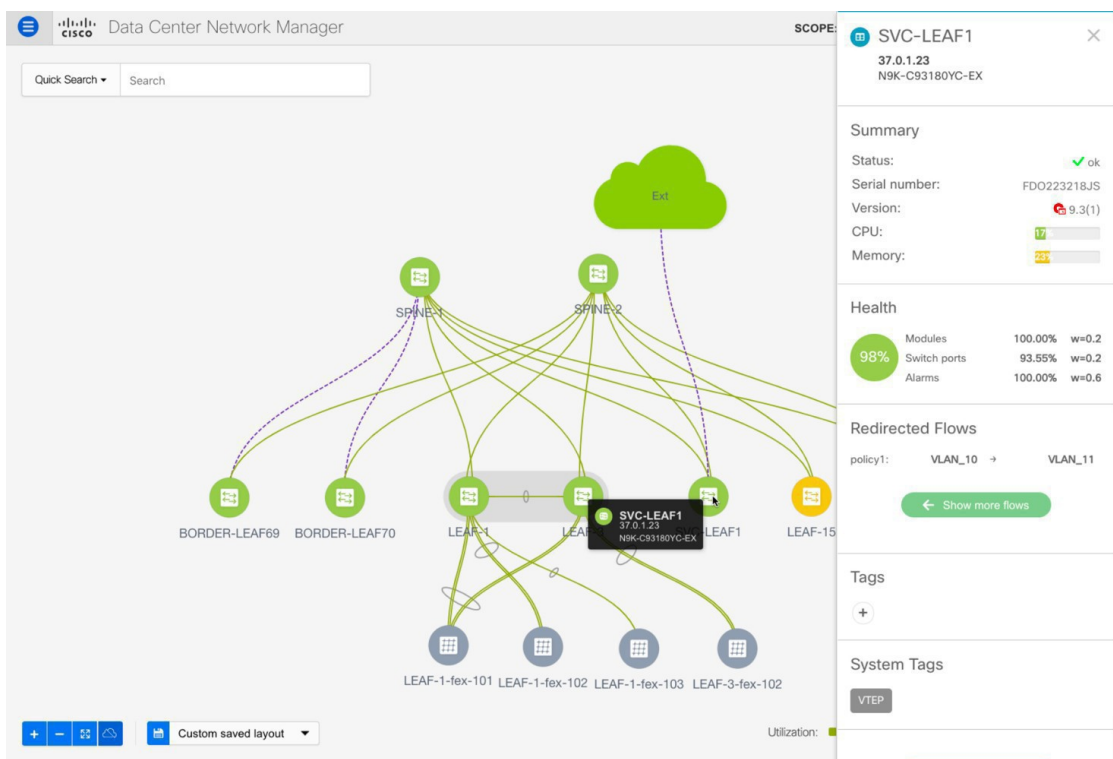
## 8. [トポロジ (Topology)] ウィンドウでの宛先へリダイレクトされたフローの視覚化



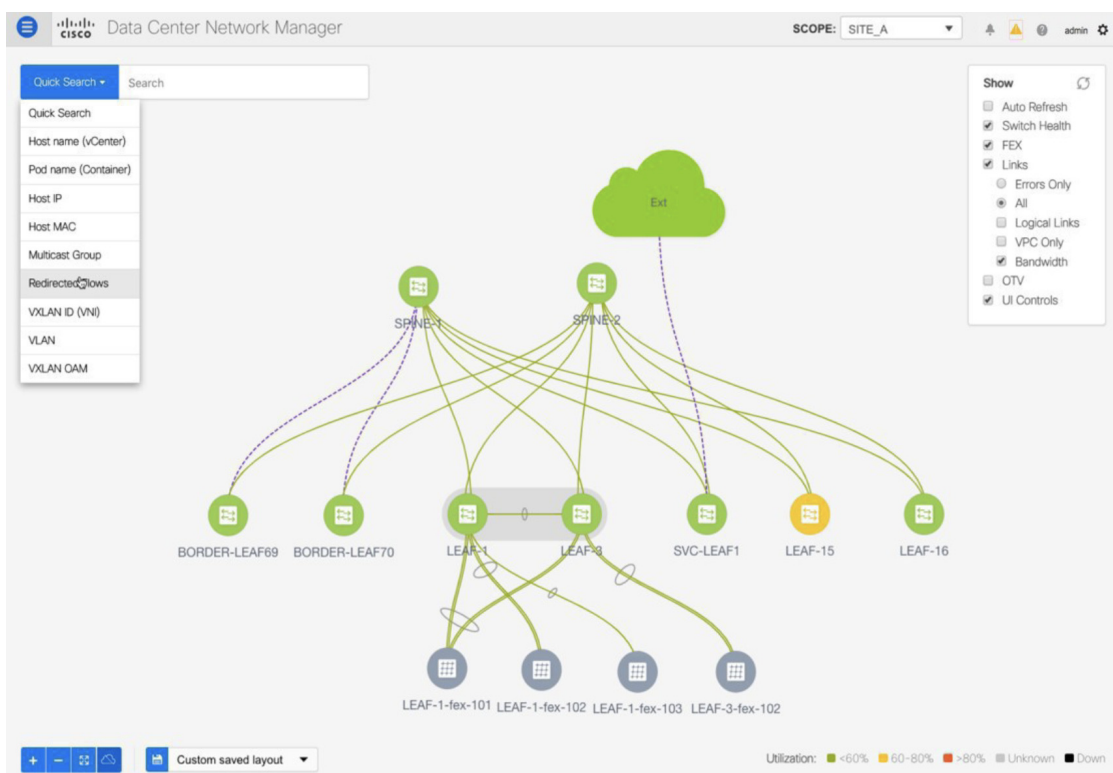
## 8. [トポロジ (Topology)] ウィンドウでの宛先へリダイレクトされたフローの視覚化

## Procedure

**ステップ1** [トポロジ (Topology)] をクリックし、リーフをクリックして、宛先にリダイレクトされたフローを視覚化します。

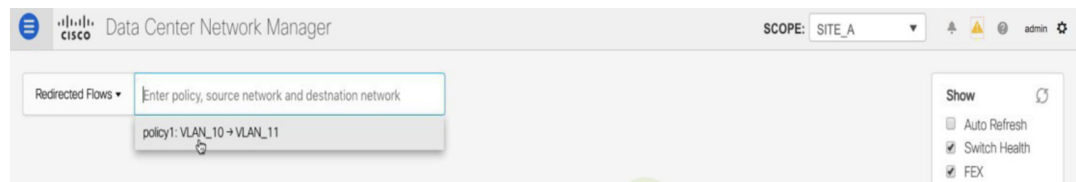


ステップ2 ドロップダウンリストから[リダイレクトされたフロー (Redirected Flows)]を選択します。

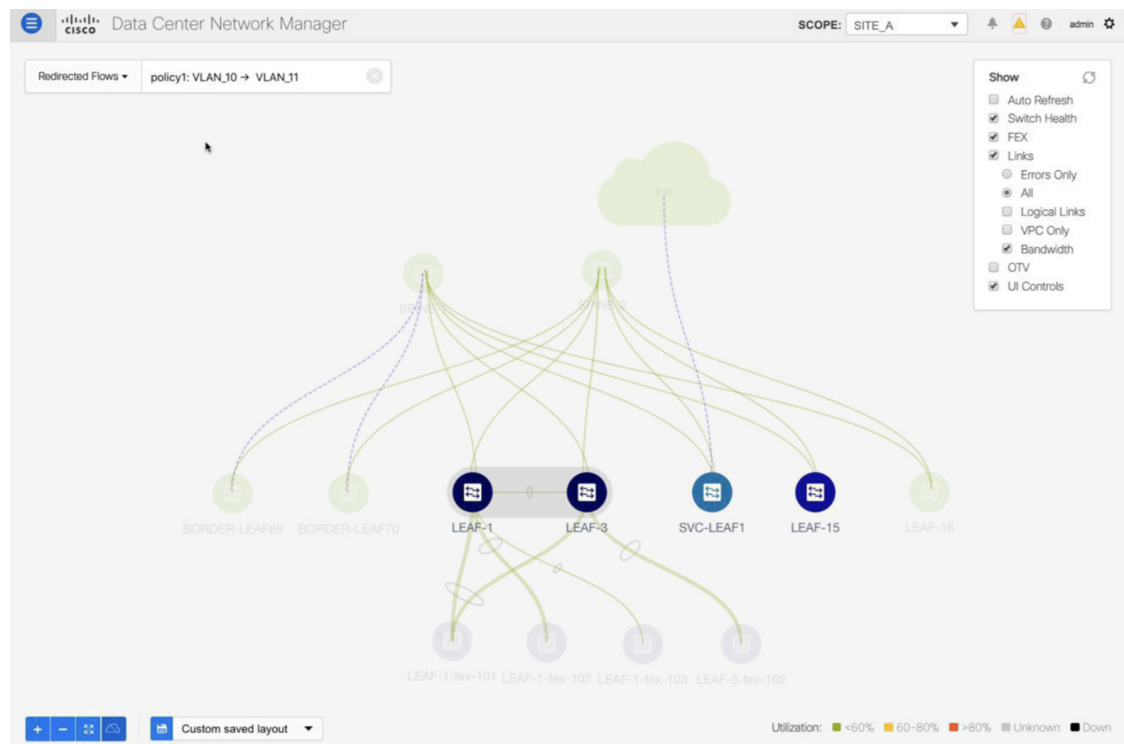


## 8. [トポロジ (Topology)] ウィンドウでの宛先へリダイレクトされたフローの視覚化

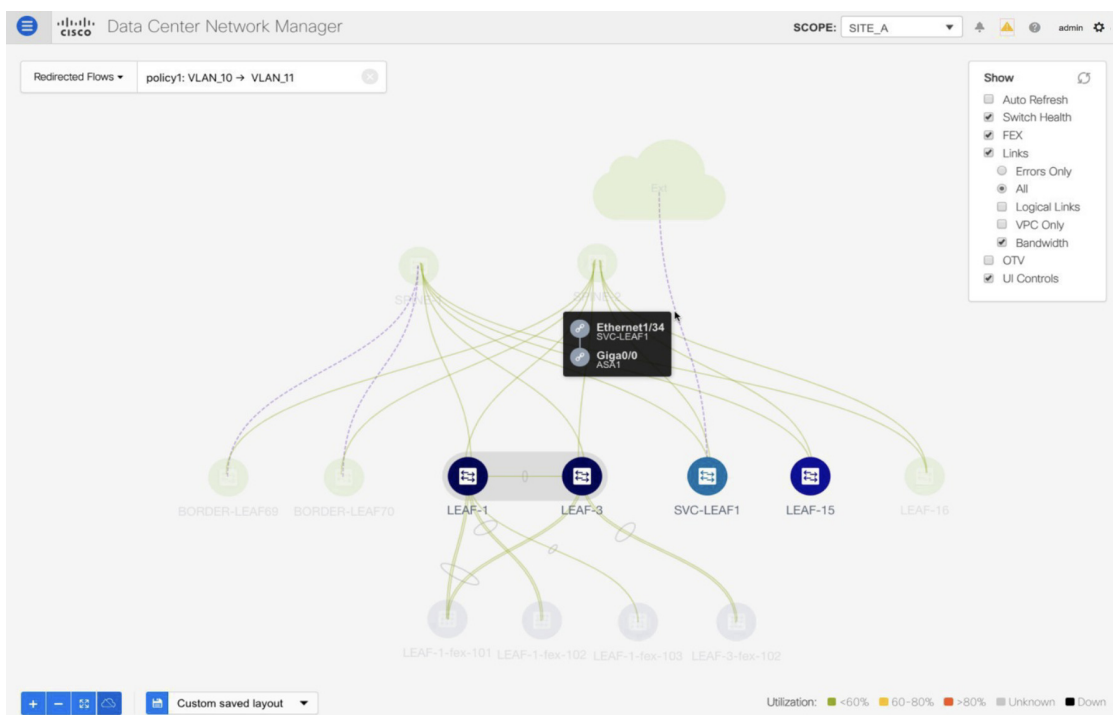
**ステップ 3** ドロップダウンリストからポリシーを選択するか、検索フィールドにポリシー名、送信元ネットワーク、および接続先ネットワークを入力して検索を開始します。検索フィールドへの入力を始めると、自動的に補完されます。



送信元ネットワークと接続先ネットワークが接続され、フローがリダイレクトされたスイッチは、強調表示されます。



**ステップ 4** サービス ノードは、トポロジ ウィンドウのリーフ スイッチに点線で接続されているように表示されます。点線にカーソルを合わせると、インターフェイスの詳細が表示されます。



送信元からのトラフィックは、ファイアウォールが構成されているサービスリーフを横断します。

ファイアウォールルールに基づいて、トラフィックは宛先であるリーフ 15 に到達することが許可されます。

## ユースケース：eBGP ピアリングを使用したテナント間ファイアウォール

トポロジの詳細については、以下の図を参照してください。

## 1. サービスノードの作成

このトポロジでは、es-leaf1 と es-leaf2 が vPC ボーダー リーフ スイッチです。

次に、DCNM でサービス リダイレクトを実行する方法を見てみましょう。

[制御 (Control)] > [ファブリック (Fabrics)] > [サービス (Services)] の順に選択します。

このユースケースは、次の手順で構成されます。



## Note

- 一部の手順は、テナント内ファイアウォール展開のユースケースで示されている手順に似ているため、そのユースケースへの参照リンクが含まれています。
- サービス ポリシーは、テナント間ファイアウォールの展開には適用されません。

## 1. サービスノードの作成

## Procedure

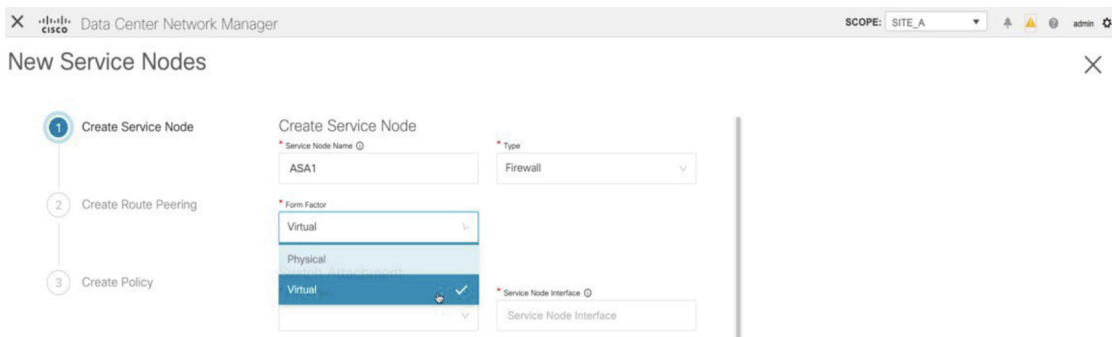
ステップ 1 [範囲 (Scope)] ドロップダウンリストから、[Site\_A] を選択します。

ステップ 2 [追加 (Add)] アイコン ([サービスノード (Service Nodes)] ウィンドウ) をクリックします。

- ステップ 3** ノード名を入力し、[ファイアウォール (Firewall)] を指定します ([タイプ (Type)] ドロップダウンボックス)。[サービスノード名 (Service Node Name)] は一意である必要があります。

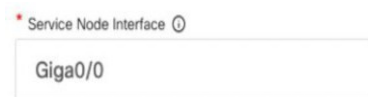


- ステップ 4** [フォームファクター (Form Factor)] ドロップダウンリストから、[仮想 (Virtual)] を選択します。



- ステップ 5** [スイッチの接続 (Switch Attachment)] セクションで、[外部ファブリック (External Fabric)] ドロップダウンリストから、サービスノード (たとえば、ASA ファイアウォール) が配置されている外部ファブリックを選択します。サービスノードは外部ファブリックに属している必要があることに注意してください。これは、サービスノードを作成する際の前提条件です。

- ステップ 6** サービスリーフに接続するサービスノードのインターフェイス名を入力します。



- ステップ 7** サービスリーフである接続されたスイッチと、サービスリーフ上の対応するインターフェイスを選択します。

- ステップ 8** `service_link_trunk` テンプレートを選択します。DCNM は、トランク、ポートチャネル、および vPC リンク テンプレートをサポートします。[リンク テンプレート (Link Template)] ドロップダウンリストで使用可能なリンク テンプレートは、選択した [接続スイッチ インターフェイス (Attached Switch Interface)] のタイプに基づいてフィルタリングされます。



- ステップ 9** 必要に応じて、[一般パラメータ (General Parameters)] と [詳細 (Advanced)] パラメータを指定します。一部のパラメータには、デフォルト値が事前に入力されています。

ステップ 10 [次へ (Next)] をクリックして、作成したサービス ノードを保存します。

**Note** その他のサンプル スクリーンショットについては、ポリシー ベース ルーティング使用例の、テナント内ファイアウォールの [1. サービス ノードの作成, on page 2](#) を参照してください。

## 2. ルートピアリングの作成

サービス リーフとサービス ノード間のピアリングを構成しましょう。

### Procedure

ステップ 1 ピアリング名を入力し、[テナント間ファイアウォール (Inter-Tenant Firewall)] を [展開 (Deployment)] ドロップダウンリストから選択します。[ピアリング オプション (Peering Option)] ドロップダウンリストから、[eBGP ダイナミック ピアリング (eBGP Dynamic Peering)] を選択します。

ステップ 2 [内部ネットワーク (Inside Network)] で、[VRF] ドロップダウンリストから既に存在する VRF を選択し、[内部ネットワーク (Inside Network)] を [ネットワーク タイプ (Network Type)] で選択します。

[サービス ネットワーク (Service Network)] の名前を入力し、[Vlan ID] を指定します。[提案 (Propose)] をクリックして、DCNM が次に使用可能な VLAN ID をファブリック設定で指定されたサービス ネットワーク VLAN ID の範囲からフェッチできるようにすることもできます。デフォルトの [サービス ネットワーク テンプレート (Service Network Template)] は `Service_Network_Universal` です。

[一般パラメータ] タブで、サービス ネットワークのゲートウェイ アドレスを指定します。[ネクストホップ IP アドレス (Next Hop IP Address)] を指定します。このネクストホップアドレスは、「内部サービス ネットワーク」サブネット内にある必要があります。[詳細設定 (Advanced)] タブの、デフォルトの [ルーティング タグ (Routing Tag)] 値は 12345 です。

ステップ 3 eBGP ダイナミック ピアリングのデフォルトのピアリングテンプレートは、`service_ebgp_route` です。

Peering Template

service\_ebgp\_route

[一般パラメータ (General Parameters)] タブで、[ネイバー IPv4 (Neighbor IPv4)] アドレス、[ループバック IP (Loopback IP)] アドレス、および [vPC ピアのループバック IP (vPC Peer's Loopback IP)] アドレスを指定します。ボーダー スイッチは vPC ペアです。



The screenshot shows the 'General Parameters' tab of a configuration interface. It contains three input fields:

- \* Neighbor IPv4**: 192.168.32.254
- \* Loopback IP**: 60.1.1.60
- vPC Peer's Loopback IP**: 60.1.1.61

**ステップ 4** [詳細設定 (**Advanced**)] タブで、[ローカル ASN (**Local ASN**)] を指定し、[ホスト ルートのアドバタイズ (**Advertise Host Routes**)] チェックボックスをオンにします。このローカル ASN 値は、スイッチのシステム ASN を上書きするために使用され、ルーティング ループを回避するために必要です。

[ホスト ルートのアドバタイズ (**Advertise Host Routes**)] チェックボックスがオンになっている場合、/32 および /128 ルートがアドバタイズされます。このチェックボックスが選択されていない場合、プレフィックス ルートがアドバタイズされます。

デフォルトでは、[インターフェイスの有効化 (**Enable Interface**)] チェックボックスがオンになっています。

The screenshot shows the 'Advanced' tab of a configuration interface. It contains several input fields and checkboxes:

- Neighbor IPv6**: (empty)
- Loopback IPv6**: (empty)
- vPC Peer's Loopback IPv6**: (empty)
- \* Route-Map TAG**: 12345
- Interface Description**: (empty)
- Local ASN**: 65501
- Advertise Host Routes**:
- \* Enable Interface**:

## 2. ルートピアリングの作成

**ステップ5** [外部ネットワーク (Outside Network)] で必要なパラメータを指定し、[リバーストラフィックのネクストホップ IP アドレス (Next Hop IP Address for Reverse Traffic)] を指定します。リバーストラフィックのこのネクストホップアドレスは、「外部サービスネットワーク」サブネット内にある必要があります。

**ステップ6** eBGPダイナミックピアリングのデフォルトのピアリングテンプレートは、**service\_ebgp\_route**です。

Peering Template

service\_ebgp\_route

[一般パラメータ (General Parameters)] タブの、[ネイバー IPv4 (Neighbor IPv4)] アドレス、[ループバック IP (Loopback IP)] アドレス、および [vPC ピアのループバック IP (vPC Peer's Loopback IP)] アドレスです。リーフスイッチは vPC ペアです。

General Parameters    Advanced

\* Neighbor IPv4 ⓘ

32.32.32.254

\* Loopback IP ⓘ

61.1.1.60

vPC Peer's Loopback IP ⓘ

61.1.1.61

**ステップ7** [詳細設定 (Advanced)] タブで、[ローカル ASN (Local ASN)] を指定し、[ホストルートのアドバタイズ (Advertise Host Routes)] チェックボックスをオンにします。このローカル ASN 値は、スイッチのシステム ASN を上書きするために使用され、ルーティングループを回避するために必要です。

[ホストルートのアドバタイズ (Advertise Host Routes)] チェックボックスがオンになっている場合、/32 および /128 ルートがアドバタイズされます。このチェックボックスが選択されていない場合、プレフィックスルートがアドバタイズされます。

デフォルトでは、[インターフェイスの有効化 (Enable Interface)] チェックボックスがオンになっています。

ステップ 8 [次へ (Next)] をクリックして、作成したルート ピアリングを保存します。

### 3. ルート ピアリングを展開する

テナント内ファイアウォール展開のユースケースの [4. ルート ピアリングを展開する, on page 10](#) を参照してください。[InterTenantFW] が [展開 (Deployment)] の下に表示されていることに注意してください。

このユースケースの vPC ボーダー リーフの BGP 設定を以下に示します。

```
router bgp 12345
router-id 10.2.0.1
address-family l2vpn evpn
advertise-pip
neighbor 10.2.0.4
remote-as 12345
update-source loopback0
address-family l2vpn evpn
send-community
send-community extended
vrf myvrf_50001
address-family ipv4 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redis-subnet
maximum-paths ibgp 2
address-family ipv6 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redis-subnet
maximum-paths ibgp 2
neighbor 192.168.32.254
```

```

remote-as 9876
local-as 65501 no-prepend replace-as // Note: This configuration corresponds to the
Local ASN template parameter value of the service_ebgp_route template of the inside
network with VRF myvrf_50001. The no-prepend replace-as keyword is generated along with
the local-as command.
update-source loopback2
ebgp-multihop 5
address-family ipv4 unicast
send-community
send-community extended
route-map extcon-rmap-filter-allow-host out
vrf myvrf_50002
address-family ipv4 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redist-subnet
maximum-paths ibgp 2
address-family ipv6 unicast
advertise l2vpn evpn
redistribute direct route-map fabric-rmap-redist-subnet
maximum-paths ibgp 2
neighbor 32.32.32.254
remote-as 9876
local-as 65502 no-prepend replace-as // Note: This configuration corresponds to the
Local ASN template parameter value of the service_ebgp_route template of the outside
network with VRF myvrf_50002. The no-prepend replace-as keyword is generated along with
the local-as command.
update-source loopback3
ebgp-multihop 5
address-family ipv4 unicast
send-community
send-community extended
route-map extcon-rmap-filter-allow-host out

```

このユースケースの vPC スイッチ `es-leaf1` のループバック インターフェイス設定を以下に示します。構成のループバック インターフェイスは、`service_ebgp_route` テンプレートの「ループバック IP」パラメータに対応します。[ループバック IP (Loopback IP)] パラメータ値 (`[service_ebgp_route]` テンプレートで指定されたもの) を使用して、2つの個別の VRF インスタンスの各 vPC スイッチに2つのループバック インターフェイスが自動的に作成されます。

```

interface loopback2
vrf member myvrf_50001
ip address 60.1.1.60/32 tag 12345
interface loopback3
vrf member myvrf_50002
ip address 61.1.1.60/32 tag 12345

```

vPC ピア スイッチ `es-leaf2` のループバック インターフェイス設定 :

```

interface loopback2
vrf member myvrf_50001
ip address 60.1.1.61/32 tag 12345
interface loopback3
vrf member myvrf_50002
ip address 61.1.1.61/32 tag 12345

```

## ユースケース : ワンアーム ロード バランサ

トポロジの詳細については、以下の図を参照してください。

このトポロジでは、es-leaf1 と es-leaf2 が vPC リーフです。

次に、DCNM でサービス リダイレクトを実行する方法を見てみましょう。

[制御 (Control)] > [ファブリック (Fabrics)] > [サービス (Services)] の順に選択します。

このユースケースは、次の手順で構成されます。



**Note** 一部の手順は、テナント内ファイアウォール展開のユースケースで示されている手順に似ているため、そのユースケースへの参照リンクが含まれています。

## 1. サービスノードの作成

### Procedure

**ステップ 1** [範囲 (Scope)] ドロップダウンリストから、**Site\_A** を選択します。

Service Nodes

Service nodes cannot be defined for selected fabric scope. Select a valid fabric scope.  
In a valid fabric scope, you can define

- Service Node**  
Onboard a service device such as a *firewall* or *load balancer*. Specify service node name, type, and interface attachment details
- Route Peering**  
Specify deployment type, network parameters, peering protocol, and service IP
- Service Policy**  
Specify traffic redirection rules to/from the service node

**ステップ 2** [追加 (Add)] アイコン ([サービスノード (Service Nodes)] ウィンドウ) をクリックします。

Service Nodes

Selected fabric scope has no service node. Add a service node to continue.  
In selected fabric scope, you can define

- Service Node**  
Onboard a service device such as a *firewall* or *load balancer*. Specify service node name, type, and interface attachment details
- Route Peering**  
Specify deployment type, network parameters, peering protocol, and service IP
- Service Policy**  
Specify traffic redirection rules to/from the service node

## 1. サービスノードの作成

**ステップ3** ノード名を入力し、[ロードバランサ (Load Balancer)] を指定します ([タイプ (Type)] ドロップダウン ボックス)。[サービス ノード名 (Service Node Name)] は一意である必要があります。

**ステップ4** [フォーム ファクター (Form Factor)] ドロップダウン リストから、[仮想 (Virtual)] を選択します。

\* Form Factor

Virtual ^

Physical

Virtual ✓

**ステップ5** [スイッチの接続 (Switch Attachment)] セクションで、[外部ファブリック (External Fabric)] ドロップダウン リストから、サービス ノード (たとえば、ASA ファイアウォール) が配置されている外部ファブリックを選択します。サービス ノードは外部ファブリックに属している必要があることに注意してください。これは、サービス ノードを作成する際の前提条件です。

**ステップ6** サービス リーフに接続するサービス ノードのインターフェイス名を入力します。

\* Service Node Interface ⓘ

Giga0/0

**ステップ7** サービス リーフである接続されたスイッチと、サービス リーフ上の対応するインターフェイスを選択します。

**ステップ8** `service_link_trunk` テンプレートを選択します。DCNM は、トランク、ポートチャネル、および vPC リンク テンプレートをサポートします。[リンク テンプレート (Link Template)] ドロップダウン リストで使用可能なリンク テンプレートは、選択した [接続スイッチ インターフェイス (Attached Switch Interface)] のタイプに基づいてフィルタリングされます。

Link Template

service\_link\_trunk v

**ステップ9** 必要に応じて、[一般パラメータ (General Parameters)] と [詳細 (Advanced)] パラメータを指定します。一部のパラメータには、デフォルト値が事前に入力されています。

**ステップ10** [次へ (Next)] をクリックして、作成したサービス ノードを保存します。

**Note** その他のサンプル スクリーンショットについては、ポリシー ベース ルーティング使用例の、テナント内ファイアウォールの [1. サービス ノードの作成, on page 2](#) を参照してください。

## 2. ルート ピアリングの作成

サービス リーフとサービス ノード間のピアリングを構成しましょう。このユースケースでは、静的ルート ピアリングを設定します。

### Procedure

- ステップ1** ピアリング名を入力し、[ワンアーム モード (One-Arm Mode)] を選択します ([展開 (Deployment)] ドロップダウンリスト)。また、[ピアリング オプション (Peering Option)] ドロップダウンリストから、[静的ピアリング (Static Peering)] を選択します。
- ステップ2** [最初のアーム (First Arm)] で、必要な値を指定します。[VRF] ドロップダウンリストからすでに存在する VRF を選択し、[最初のアーム (First Arm)] を [ネットワーク タイプ (Network Type)] から選択します。
- ステップ3** [サービス ネットワーク (Service Network)] の名前を入力し、[Vlan ID] を指定します。[提案 (Propose)] をクリックして、DCNM が次に使用可能な VLAN ID をファブリック設定で指定されたサービス ネットワーク VLAN ID の範囲からフェッチできるようにすることもできます。デフォルトの [サービス ネットワーク テンプレート (Service Network Template)] は **Service\_Network\_Universal** です。

[一般パラメータ] タブで、サービス ネットワークのゲートウェイアドレスを指定します。[ネクストホップ IP アドレス (Next Hop IP Address)] を指定します。このネクストホップアドレスは、最初のアームのサブネット内にある必要があります。[詳細設定 (Advanced)] タブの、デフォルトの [ルーティング タグ (Routing Tag)] 値は 12345 です。

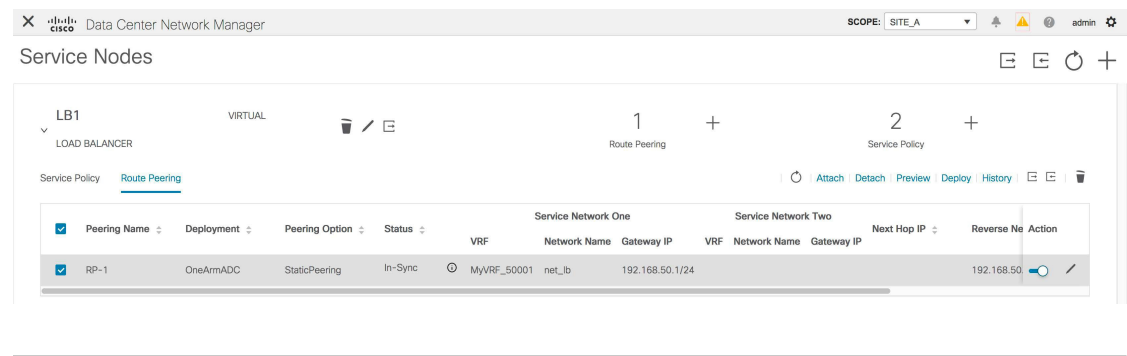
## 3. サービス ポリシーの作成

**ステップ 4** デフォルトの [ピアリング テンプレート (Peering Template)] は `service_static_route` です。必要に応じて、[静的ルート (Static Routes)] フィールドにルートを追加します。



**ステップ 5** リバース トラフィックの [ネクスト ホップ IP アドレス (Next Hop IP Address)] を指定します。

**ステップ 6** [次へ (Next)] をクリックして、作成したルート ピアリングを保存します。



## 3. サービス ポリシーの作成

Intra-Tenant ファイアウォール展開のユースケースの [3. サービス ポリシーの作成, on page 7](#) を参照してください。

## 4. ルート ピアリングを展開する

テナント内ファイアウォール展開のユースケースの [4. ルート ピアリングを展開する, on page 10](#) を参照してください。[OneArmADC] が [展開 (Deployment)] の下に表示されていることに注意してください。

## 5. サービス ポリシーの展開

テナント内ファイアウォール展開のユースケースの [5. サービス ポリシーの展開, on page 12](#) を参照してください。ただし、このロードバランサのユースケースには2台のサーバーがあるため、サーバー ネットワークごとに2つのサービス ポリシーを定義する必要があります。



Policy Name	Route Peering	Status	Source VRF	Source Network	Destination VRF	Destination Network	Next Hop IP	Reverse Next Hop IP	Stats	Action
SP-1	RP-1	In-Sync	MyVRF_50...	ClientNet	MyVRF_50001	ServerNet		192.168.50.254		
SP-2	RP-1	In-Sync	MyVRF_50...	ClientNet	MyVRF_50001	ServerNet2		192.168.50.254		

## 6. 統計情報を表示する

テナント内ファイアウォール展開のユースケースの [6. 統計情報を表示する, on page 14](#) を参照してください。

## 7. Fabric Builder でのトラフィック フローの表示

テナント内ファイアウォール展開のユースケースの [7. Fabric Builder でのトラフィック フローの表示, on page 15](#) を参照してください。

## 8.[トポロジ (Topology) ]ウィンドウでの宛先へリダイレクトされたフローの視覚化

テナント内ファイアウォール展開のユースケースの [8.\[トポロジ \(Topology\) \]ウィンドウでの宛先へリダイレクトされたフローの視覚化, on page 18](#) を参照してください。

サービス リーフの VRF 構成は以下のとおりです。

```
interface Vlan2000
  vrf member myvrf_50001
  ip policy route-map rm_myvrf_50001

interface Vlan2306
  vrf member myvrf_50001
  vrf context myvrf_50001
  vni 50001
  ip route 55.55.55.55/32 192.168.50.254 // Note: This is the static route
  rd auto
  address-family ipv4 unicast
    route-target both auto
    route-target both auto evpn
  address-family ipv6 unicast
    route-target both auto
    route-target both auto evpn
router bgp 12345
  vrf myvrf_50001
  address-family ipv4 unicast
    advertise l2vpn evpn
    redistribute direct route-map fabric-rmap-redirect-subnet
    redistribute static route-map fabric-rmap-redirect-static
    maximum-paths ibgp 2
  address-family ipv6 unicast
    advertise l2vpn evpn
    redistribute direct route-map fabric-rmap-redirect-subnet
    redistribute static route-map fabric-rmap-redirect-static
    maximum-paths ibgp 2
```

**8. [トポロジ (Topology) ] ウィンドウでの宛先へリダイレクトされたフローの視覚化**

## 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。