

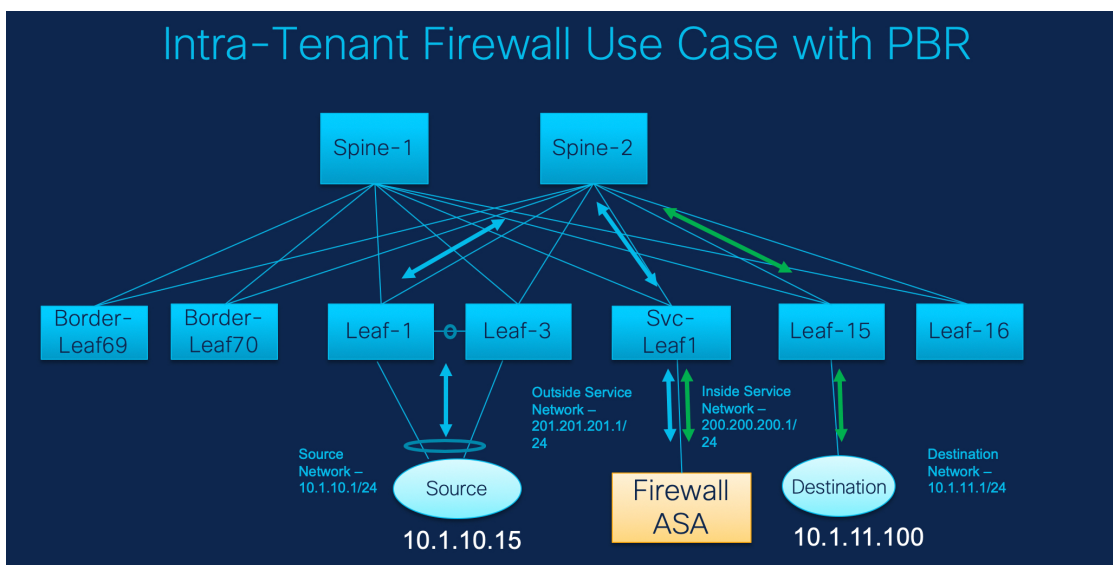


L4～L7 サービスのユースケース

- 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 9
- ユースケース：ワンアーム ロード バランサ, on page 15

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。

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、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、NDFC 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 Dashboard Fabric Controller for LAN Configuration Guide』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。

以下のいずれかのパスを使用して、[サービス (Services)] タブに移動できます。

[LAN] > [サービス (Services)]

[LAN] > [ファブリック (Fabrics)] > [ファブリックの概要 (Fabric Overview)] > [サービス (Services)]

[LAN] > [スイッチ (Switches)] > [スイッチの概要 (Switches Overview)] > [サービス (Services)]

1. サービス ノードの作成

Procedure

- ステップ 1** [LAN] > [ファブリック (Fabrics)] > [ファブリックの概要 (Fabric Overview)] > [サービス (Services)] へ移動します。

- ステップ 2** [サービス (Service)] タブで、[アクション (Actions)] > [追加 (Add)] を選択します。
- ステップ 3** サービス ノード名を入力し、[ファイアウォール (Firewall)] を [タイプ (Type)] ドロップダウン ボックスで指定します。
- [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** ドロップダウン リストから外部ファブリックを選択し、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。



Note サービス ノードが外部ファブリックに属する必要があることを確認します。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。NDFC 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。

2. ルート ピアリングの作成

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 [保存 (Save)] 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。

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、NDFC 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 [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 4 [保存 (Save)] 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。

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 [宛先 VRF 名 (Destination VRF Name)] ドロップダウン リストから、送信元および宛先 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。

ステップ 3 [送信元ネットワーク (Source Network)] および [宛先ネットワーク (Destination Network)] ドロップダウン リストから、送信元ネットワークと宛先ネットワークを選択するか、[ファブリックの概要 (Fabric Overview)] > [サービス (Services)] 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宛先ネットワークを指定します。

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。

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、任意の送信元ポートと宛先ポートが 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。NDFC 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。

ステップ6 [詳細設定 (Advanced)] タブでは、許可が[ルート マップ アクション (Route Map Action)] のデフォルト、なしが[ネクスト ホップ オプション (Next Hop Option)] のデフォルトになっています。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」の章の「テンプレート」セクションを参照してください。

ステップ7 [保存 (Save)] 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。

5. サービス ポリシーの展開

1. [サービス (Services)] タブの [サービス ポリシー (Service Policy)] ウィンドウで、必要なピアリングを選択します。
2. [アクション (Actions)] > [展開 (Deploy)] を選択します。
[サービス ポリシーの展開 (Deploy Service Policy)] ウィンドウが表示されます。
3. [展開 (Deploy)] をクリックして展開を確認します。

4. ルート ピアリングを展開する

1. [サービス (Services)] タブの [ルート ピアリング (Route Peering)] ウィンドウで、必要なピアリングを選択します。
2. [アクション (Actions)] > [展開 (Deploy)] を選択します。
[ルート ピアリングの展開 (Deploy Route Peering)] ウィンドウが表示されます。
3. [展開 (Deploy)] 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

それぞれのリダイレクトポリシーが展開されたので、対応する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。

このシナリオを NDFC で可視化するには、サービス ポリシーをクリックします。スライドイン ペインが表示されます。

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。

次の統計が表示されます。

- 送信元スイッチでの転送トラフィック
- 宛先スイッチでのリバース トラフィック
- サービス スイッチの双方向のトラフィック

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 NDFC トポロジで雲のアイコンとして表示されます。

Procedure

-
- ステップ 1 サービス リーフをクリックすると、スライドイン ペインが表示されます。**[さらにフローを表示 (Show more flows)]** をクリックします。リダイレクトされる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。
-

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。
 - 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、および宛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宛先ネットワークがアタッチされていて、フローがリダイレクトされているスイッチが、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、NDFC 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。

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の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、そのユースケースの手順への参照リンクが追加されています。
- 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 [LAN] > [ファブリック (Fabrics)] > [ファブリックの概要 (Fabric Overview)] > [サービス (Services)] へ移動します。

ステップ 2 [サービス (Service)] タブで、[アクション (Actions)] > [追加 (Add)] を選択します。

ステップ 3 サービス ノード名を入力し、[タイプ (Type)] ドロップダウン ボックスで [ファイアウォール (Firewall)] を指定します。[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** **[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。



Note サービス ノードが外部ファブリックに属する必要があることを確認します。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。NDFC 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)]** 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** **[保存 (Save)]** 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 ベースのルーティング ユースケースで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](#) セクション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。

2. ルートピアリングの作成

Create Route Peering

1 Create Service Node 2 Create Route Peering 3 Create Service Policy

Detach ☐ Attach ☒

Peering Name*
peeringInterTenant

Deployment*
Inter-Tenant Firewall

Peering Option*
eBGP Dynamic Peering

Inside Network

VRF*
MyVRF_51000

Network Type*
Inside Network

Service Network*
net_inside_inter_tenant

VLAN ID*
3001

Network ID*
30010

Service Network Template*
Service_Network_Universal

General Parameters

IPv4 Gateway/NetMask*
192.168.32.1/24

IPv6 Gateway/Prefix*
example 2001:db8:1:0/4

VLAN Name
if + 32 chars enable system vlan long name

Interface Description
fw.inside SITE_B ASA2 Giga1/1 peeringInterTenant

Peering Template*
service_ebgp_route

General Parameters

Neighbor IPv4 address or subnet*
192.168.32.254

Loopback IP*
60.1.1.60

vPC Peer's Loopback IP
60.1.1.61

Outside Network

VRF*
MyVRF_51000

Network Type*
Outside Network

Service Network*
net_outside_inter_tenant

VLAN ID*
3002

Network ID*
30011

Service Network Template*
Service_Network_Universal

General Parameters

IPv4 Gateway/NetMask*
32.32.32.1/24

IPv6 Gateway/Prefix*
example 2001:db8:1:0/4

VLAN Name
if + 32 chars enable system vlan long name

Interface Description
fw.outside SITE_B ASA2 Giga1/1 peeringInterTenant

Peering Template*
service_ebgp_route

General Parameters

Neighbor IPv4 address or subnet*
32.32.32.254

Loopback IP*
61.1.1.60

vPC Peer's Loopback IP
61.1.1.61

Cancel Done

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）]を[VRF]ドロップダウンリストで選択し、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、NDFC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ができます。デフォルトのサービスネットワークテンプレートはService_Network_Universalです。

[一般パラメータ (General Parameters)] 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。

[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。

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 ルートが表示されます。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 ルートが表示されます。

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 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。

[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。リーフ スイッチは vPC ペアです。

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 [保存 (Save)] 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 7](#) 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を確認します。

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-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 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。

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 リーフです。

次に、NDFC 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。

以下のいずれかのパスを使用して、**[サービス (Services)]** タブに移動できます。

[LAN] > [サービス (Services)]

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 **[LAN] > [ファブリック (Fabrics)] > [ファブリックの概要 (Fabric Overview)] > [サービス (Services)]** へ移動します。

Create New Service Node ? X

1 Create Service Node 2 Create Route Peering 3 Create Service Policy

Service Node Name*
LB1

Service Node Type*
Load Balancer X v

Form Factor*
Physical X v

External Fabric*
SITE_B X v

Service Node Interface*
G1/1

Attached Fabric*
SITE_A X v

Attached Switch*
es-leaf2 X

Attached Switch Interface*
Ethernet1/50 X v

Link Template*
service_link_trunk X

General Parameters Advanced

MTU*
jumbo MTU for the interface

SPEED*
Auto Interface Speed

Trunk Allowed VLANs*
none Allowed values: 'none', 'all', or vlan ranges (ex: 1-200,200-2000,2000)

Enable BPDU Guard*
no Enable spanning-tree bpduguard: 'none' enables, 'false' disables, 'no' return to default settings.

Enable Port Type Fast*
☒ Enable spanning-tree edge port behavior

Enable Interface*
☒ Uncheck to disable the interface

Cancel Save

- 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、[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。
- 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。NDFC 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** [保存 (Save)] 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。

3. サービス ポリシーの作成

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、NDFC が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 の範囲から次に使用可能な VLAN ID をフェッチできるようにします。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。

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 **[保存 (Save)]** 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

テナント内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 5](#) 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についての [4. ルート ピアリングを展開する, on page 7](#) 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についての [5. サービス ポリシーの展開, on page 7](#) 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。

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 7](#) 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 8](#) 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 8](#) 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
```

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。