レイヤ 4 ~ レイヤ 7 サービスの使用例
リリース 12.2.1

目次

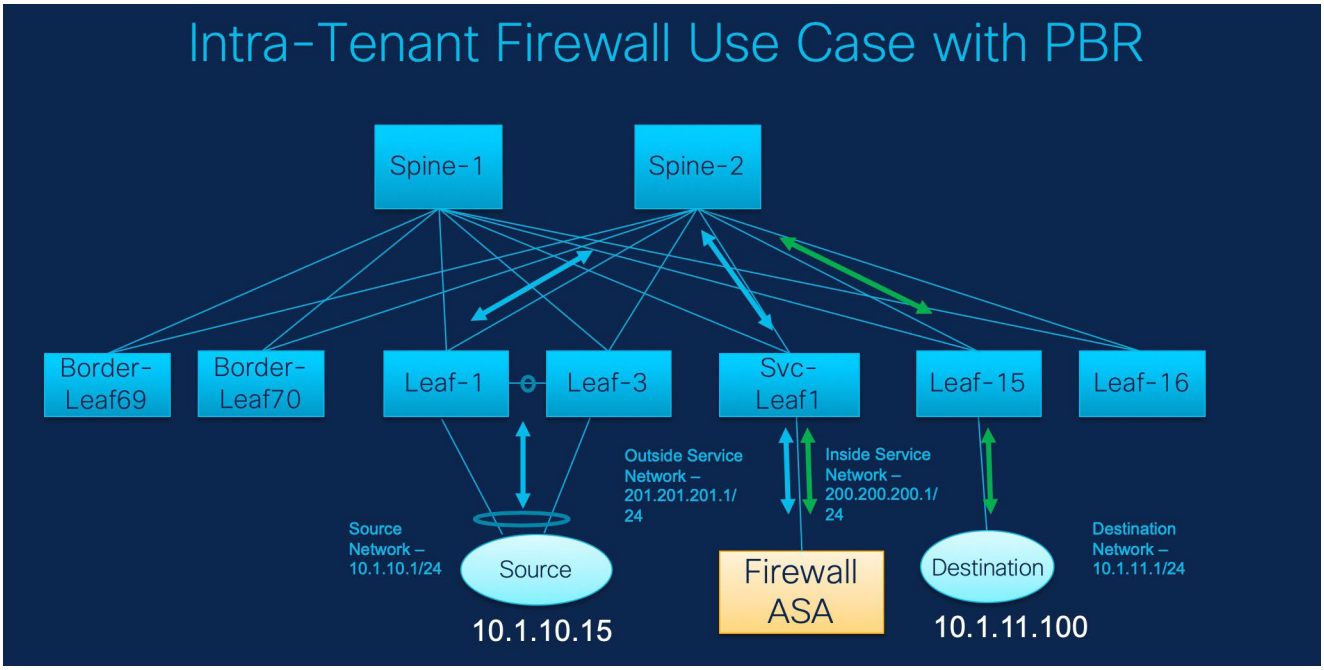
新規情報および変更情報

次の表は、この最新リリースまでの主な変更点の概要を示したものです。ただし、今リリースまでの変更点や新機能の一部は表に記載されていません。

リリース バージョン	特長	説明
以前のリリースからの大きな変更はありません。		

使用例：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、送信元（10.1.10.15）に送信元ネットワーク（10.1.10.1/24）で接続されています。サービス リーフは仮想ファイアウォール ASA に接続され、リーフ 15 は宛先（10.1.11.100）に接続されます。この使用例では、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」を指します。

送信元から宛先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。

- 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、『LAN 用 Cisco Nexus Dashboard Fabric Controller 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。

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。

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

[管理（Manage）] > [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

1. **[管理（Manage）] > [ファブリック（Fabrics）] > [ファブリックの概要（Fabric Overview）] > [サービス（Services）]** に移動します。
2. **[サービス（Service）]** タブで、**[アクション（Actions）] > [追加（Add）]** を選択します。
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。
4. **[フォーム ファクタ（Form Factor）]** ドロップダウン リストから、**[仮想（Virtual）]** を選択します。
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。

   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。

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。
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。
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。
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。
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。

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。
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（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。

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。
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

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。
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。
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。
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。
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。

   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。 また 、別の プロトコル を選択 し、対応する送信元および 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に変換し、スイッチで必要な形式に一致するようにします。たとえば、ポート80 を「www」に変換します。

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。
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。

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。

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。

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。

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。
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

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。
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。
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。

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。

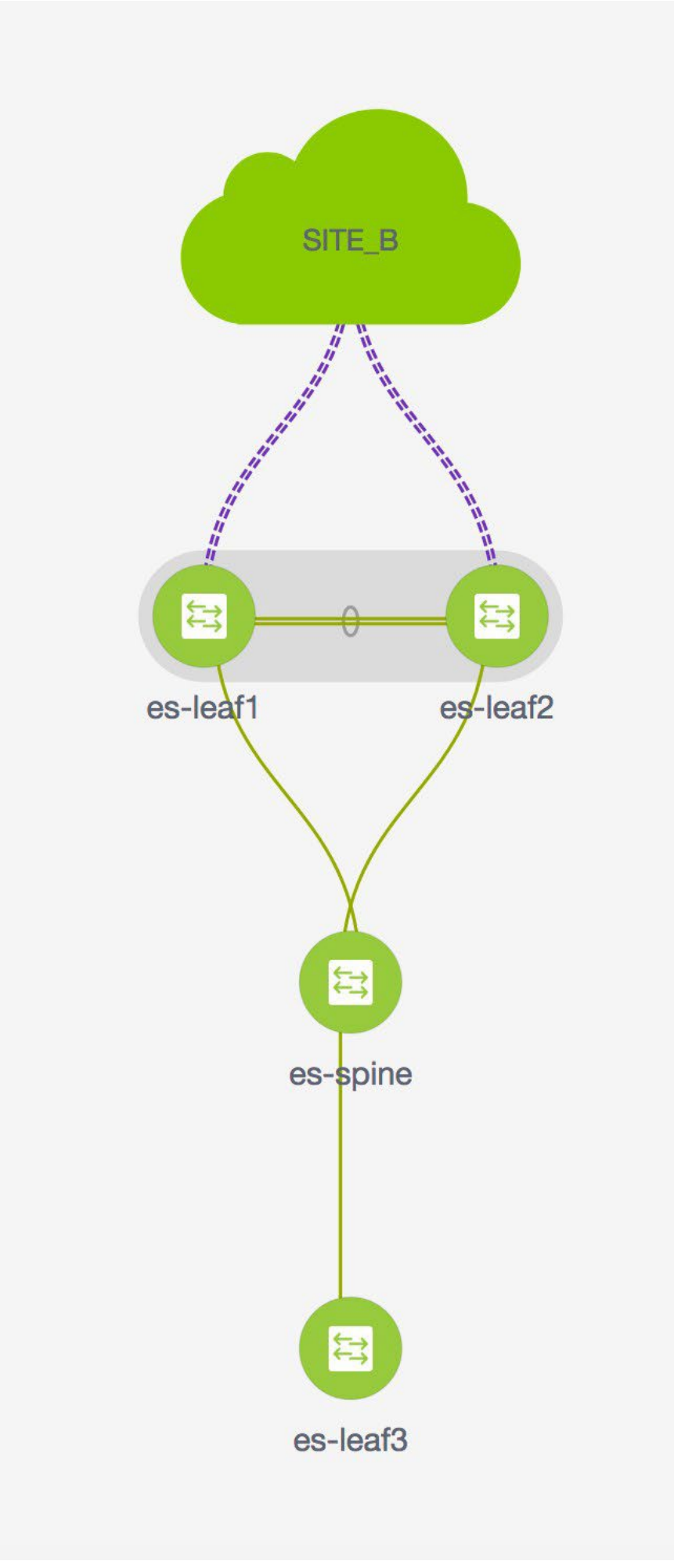
   送信元からのトラフィックは、ファイアウォールが構成されているサービス リーフを横断し

   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。



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。

- 一部のステップはテナント内ファイアウォール展開の使用例の手順と同様のため、その使用例のステップに参照リンクを追加しました。
- 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

1. **[管理（Manage）] > [ファブリック（Fabrics）] > [ファブリックの概要（Fabric Overview）] > [サービス（Services）]** に移動します。
2. **[サービス（Service）]** タブで、**[アクション（Actions）] > [追加（Add）]** を選択します。
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。
4. **[フォーム ファクタ（Form Factor）]** ドロップダウン リストから、**[仮想（Virtual）]** を選択します。
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。

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。

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。
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。
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。
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。
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。

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 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。

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。

2. **[*VRF** からの内部ネットワーク**（**Inside Network*from the *VRF**）] 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
   修正を行う。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（**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。

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。

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。

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。

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。

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。

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

4 を参照してください。テナント内ファイアウォール展開の使用例のルート ピアリングを展開します。
[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-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 // 注：この構成は、VRF myvrf_50001 を持つ内部ネットワークの service_ebgp_route テンプレートのローカル ASN テンプレート パラメータ値に対応します。no-prepend replace-as キーワードは、local-as コマンドとともに生成されます。
  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 // 注：この構成は、VRF myvrf_50002 を持つ外部ネットワークの service_ebgp_routeテンプレートのローカルASNテンプレートパラメータ値に対応します。no-prepend replace-as キーワードは、local-as コマンドとともに生成されます。
  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。+

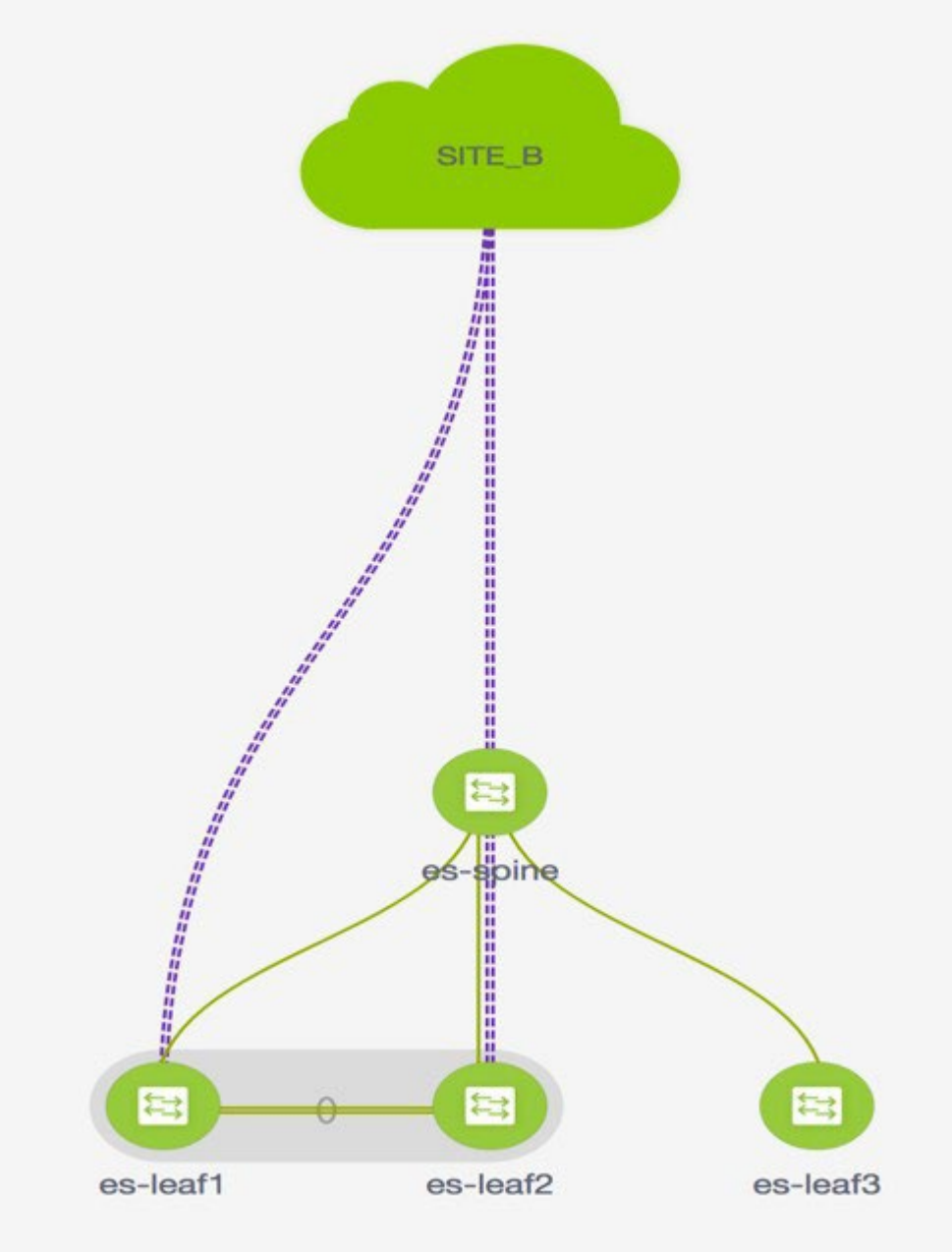
```
interface loopback2
 vrf member myvrf_50001
 ip address 60.1.1.60/32 tag 12345 interface
loopback3
 vrf member myvrf_50002
 ip address 61.1.1.60/32 tag 12345
```

The loopback interface config on vPC peer switch es-leaf2:+

```
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、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。

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

[管理（**Manage**）**] > [**スイッチ（**Switches**）**] > [**スイッチの概要（**Switches Overview**）**] > [**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。

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められています。

1. サービス ノードの作成

1. **[管理（Manage）] > [ファブリック（Fabrics）] > [ファブリックの概要（Fabric Overview）] > [サービス（Services）]** に移動します。
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。
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。
4. **[フォーム ファクタ（Form Factor）]** ドロップダウン リストから、**[仮想（Virtual）]** を選択します。
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。
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。
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。
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。
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。
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。

ヒ

スクリーンショットの例については、 1 を参照してください。ポリシー ベースのルーティングの使用例でのテナント内ファイアウォールのサービス ノードを作成します。

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。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。

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。
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。
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（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、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。

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。
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。
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

詳細については、「3. テナント内ファイアウォール展開の使用例のサービス ポリシーを作成します。

4. ルート ピアリングを展開する

4 を参照してください。テナント内ファイアウォール展開の使用例のルート ピアリングを展開します。次に、
[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

手順については、「5. テナント内ファイアウォール展開の使用例のサービス ポリシーを展開します。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

手順については、「6. テナント内ファイアウォール展開の使用例のステータスを表示します。

7. Fabric Builder でのトラフィック フローの表示

詳細については、「7. テナント内ファイアウォール展開の使用例のファブリック ビルダのトラフィック フローを表示します。

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

手順については、「8. テナント内ファイアウォール展開の使用例の［トポロジ（Topology）］ウィンドウの宛先へリダイレクトされたフローを視覚化します

サービス リーフの VRF 構成は以下のとおりです。

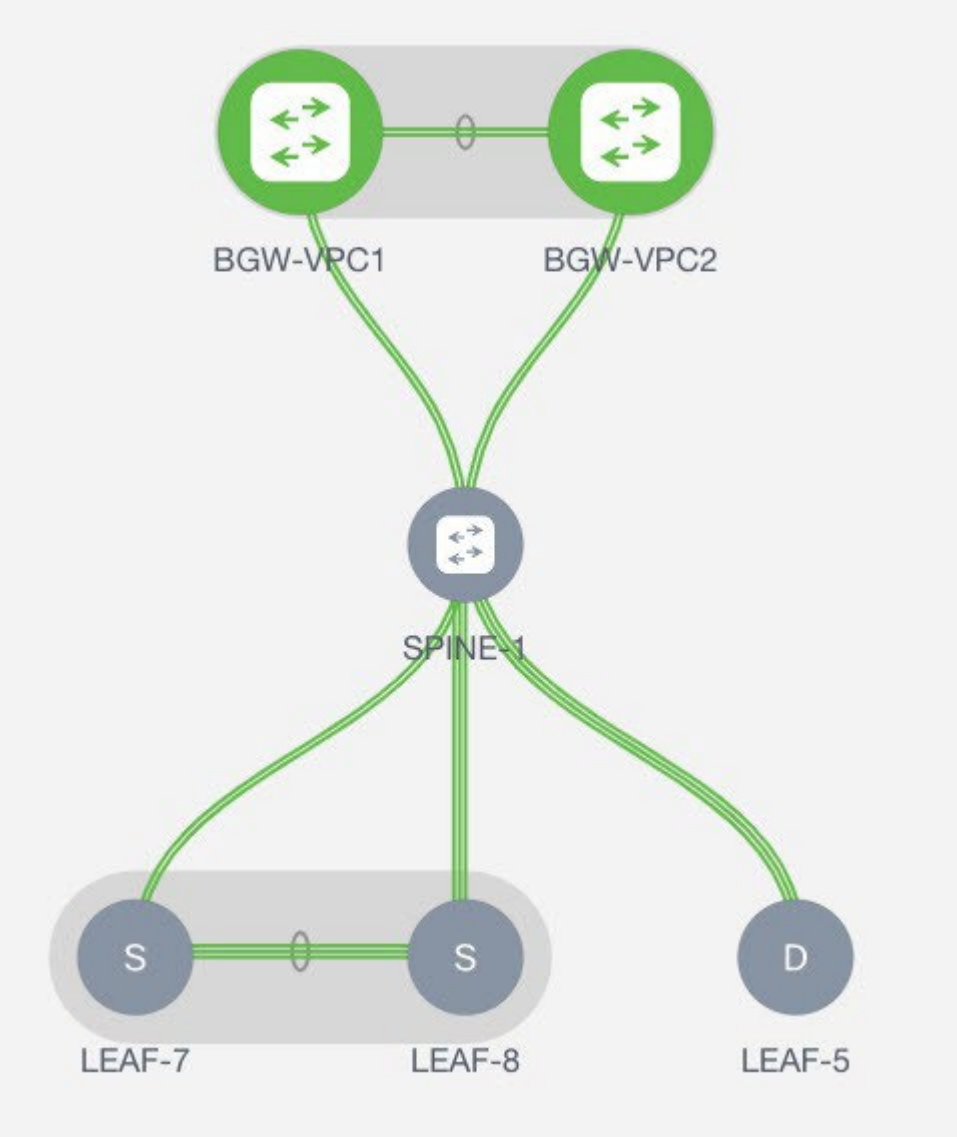
```
interface Vlan2000
 vrf member myvrf_50001
 ip policy route-map rm_myvrf_50001

interface Vlan2306
 vrf member myvrf_50001
vrf context myvrf_50001
vni 50001
 ip route 55.55.55.55/32 192.168.50.254 // 注：これは 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-redist-subnet
   redistribute static route-map fabric-rmap-redist-static
   maximum-paths ibgp 2
  address-family ipv6 unicast
   advertise l2vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   redistribute static route-map fabric-rmap-redist-static
   maximum-paths ibgp 2
```

ユースケース：ワンアーム ファイアウォール

Cisco NDFC リリース 12.1.1e から、新しい展開のワンアーム ファイアウォールが追加されました。

トポロジの詳細については、図を参照してください。このトポロジでは、BGW-VPC1 および BGW-VPC2 が、サービス スイッチとして追加される vPC ボーダー ゲートウェイです。LEAF-7 および LEAF-8 は、リダイレクトされたフローの送信元（S）ネットワークがアタッチされている vPC リーフ スイッチです。LEAF-5 は、リダイレクトされたフローの宛先（D）ネットワークにアタッチされます。



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。

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。

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

[管理（**Manage**）**] > [**スイッチ（**Switches**）**] > [**スイッチの概要（**Switches Overview**）**] > [**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。

ヒ　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。

1. サービス ノードの作成

1. **[管理（Manage）] > [ファブリック（Fabrics）] > [ファブリックの概要（Fabric Overview）] > [サービス（Services）]** に移動します。
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。
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
一意でなければなりません
4. **[フォーム ファクタ（Form Factor）]** ドロップダウン リストから、**[仮想（Virtual）]** を選択します。
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。
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。
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。
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。
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。
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。

ヒ

スクリーンショットの例については、 1 を参照してください。ポリシー ベースのルーティングの使用例でのテナント内ファイアウォールのサービス ノードを作成します。

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。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。

1. ピアリング名を入力し、**[ワンアーム ファイアウォール（One-Arm Firewall）]** を **[展開（Deployment）]** ドロップダウン リストから選択します。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。

[eBGP ピアリング（eBGP Peering）] オプションを選択することもできます。

2. **[内部ネットワーク（Inside Network）]** 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、[ネットワーク タイプ（Network Type）] の下の **[内部ネットワーク（Inside Network）]** を選択します。
3. **[サービス ネットワーク（Service Network）]** の名前を入力し、**[Vlan ID]**、および **[ネットワーク ID（Network ID）]** を指定します。**[提案（Propose）]** をクリックすると、NDFC は、指定されたサービス ネットワークの Vlan ID 範囲から次に使用可能な Vlan ID をフェッチし、ファブリック設定で定義された指定されたレイヤ 2 VXLAN VNI 範囲から次に使用可能なネットワーク ID をフェッチ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（Service Network Template）]**

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、内部ネットワーク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。

4. 静的ピアリングのデフォルトの **[**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。
5. **[**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

詳細については、「3. テナント内ファイアウォール展開の使用例のサービス ポリシーを作成します。

4. ルート ピアリングを展開する

手順については、「4. テナント内ファイアウォール展開の使用例のルート ピアリングを展開します。

5. サービス ポリシーの展開

手順については、「5. テナント内ファイアウォール展開の使用例のサービス ポリシーを展開します。

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

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 を参照してください。テナント内ファイアウォール展開の使用例の [トポロジ（Topology）] ウィンドウの宛先へリダイレクトされたフローを視覚化します

著作権

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されており、この参照により本マニュアルに組み込まれるものとします。添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアルの中の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際の IP アドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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。

Cisco およびCisco のロゴは、Cisco またはその関連会社の米国およびその他の国における商標または登録商標です。
商標または登録商標です。シスコの商標の一覧は、http://www.cisco.com/ go/trademarks でご確認いただけます。記載されているサードパーティの商標は、それぞれの所有者に帰属します。「パートナー」という言葉が使用されていても、シスコと他社の間にパートナー関係が存在することを意味するものではありません。（1110R）。