

## 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)]タブに移動します。

[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。

Service Node	
	2 3 Create Service Node Create Route Peering Create Service Policy
Service Node Name*	
ASA1	
Canica Noda Tuna*	
Firewall X V	
True Destant	
Virtual	
Commit Scholat	
SITE_B X V	
Contraction in the International	
Giga0/0	
Attached Faonc*	
Attached Switch* es-leaf3 ×	
Attached Switch Interface*	
Ethernet1/3 $ imes \sim$	
Link Template* service_link_trunk ×	
General Parameters Advanced	
мто	
Jumbo	V MTU for the interface
SPEED*	
Auto	V Interface Speed
Truck Allowed March	
none	Allowed values: 'none', 'all', or vian ranges (ex: 1-200.500-2000, 0000)
Fachin RRNU Currell	
Enable DPDU Guard*	Enable spanning-tree borduguerit truer i enable , faise-i disable , noi return to default
Forther Date Toron Front	wellings"
Port Type Fast*	Enable spanning-tree edge port behavior
Enable Interface*	

- 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(External Fabric)]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。
- **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。

Peening					
	Create Service Nor	e Create Route Peering	Create	3 a Service Policy	
Detach Attach					
Design Married					
peering value					
Deployment*					
Intra-Tenant Firewall X V					
Inside Network		Outside Network			
VRF*		VRF*			
MyVRF_51000 × ~		MyVRF_51000 × V			
Network Type*		Outside Network			
Service Network*		Service Network*			
service_net_inside: 200.200.200 $\times \sim$		service_net_outside: 201.201.20 × ∨			
VLAN ID*		VLAN ID*			
3002		3003			
Propose		Propose			
30002		30003			
Service_Network_Template* Service_Network_Universal ×		Service_Network_Universal ×			
General Parameters Advanced		General Parameters Advanced			
IPv4 Gateway/NetMask*		IPv4 Gateway/NetMask*			
200.200.200.1/24	example 192.0.2.1/24. lpv4	201.201.201.1/24	example 192.0.2.1/24. lpv4		
	or lpv6 gateway is mandatory.		or tov6 gateway is mandatory.		
IPv6 Gateway/Prefix		IPv6 Gateway/Prefix			
	example 2001:db8::1/64		example 2001:ds8::1/64		
VLAN Name		VLAN Name			
	if > 32 chars ecable system vian		# > 32 chars enable system vian		
	long-name		long-name		
Interface Description		Interface Description			
fw:inside:SITE_B:ASA1:Giga0/0:peering1		fw:outside:SITE_B:ASA1:Giga0/0;peering1			
At least one of the IP fields is mandatory*		At least one of the IP fields is mandatory*			
		Next Hop IP Address for Reverse Traffic			
Next Hop IP Address		201.201.201.201			
Next Hop IP Address 200.200.200.200					
Next Hop IP Address 200.200.200.200 Next Hop IPv6 Address		Next Hop IPv6 Address for Reverse Traffic			

#### 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(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 [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。

eate Service Policy		
	Solution (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	
	Create Service Node Create Route Peering Create Service Policy	
	Detach 🕒 Attach	
	Service Policy Name*	
	policy1	
	Peering Name*	
	period	
	Source VRF Name* MVVFF 51000 V ~	
	altin Totoo. V A	
	Destination VRF Name*	
	My/WFF_51000 × V	
	Source Network*	
	VLAN_10: 10.1.10.1/24 X V	
	Destination Network*	
	VLAN_11:10.1.11.1/24 X V	
	Next Next (0. defended	
	200.200.200 X	
	Reverse Next Hop IP Address: 201.201.201.201	
	Unit Template*	
	General Parameters Advanced	
	Protocol*	
	lp v the protocol, example top.	
	Source Port*	
	Source port number, example any or 43. Value is ignored for 'p' and form' orsteool	
	Destination Port*	
	any Detentions you number, example any or 423. Value is ignored for the set of semi-seminal	
	a mark starts Manager	

- 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サービス構成ガイド』の テンプレート (Templates) 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 で視覚化するには、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、アタッ チメントの詳細を表示します。

# 8.[トポロジ(Topology)]ウィンドウでの宛先ヘ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。

このトポロジでは、es-leafl 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。

Service Node					? >
		1 Create Service Node	2 Create Route Peering	3 Create Service Policy	
Service Node Name*					
ASA2					
Service Node Type*					
Firewall	×v				
Form Factor*					
Physical	×v				
External Fabric*					
SITE_B	×v				
Service Node Interface*					
Giga1/1					
Attached Fabric*					
SITE_A					
Attached Switch* es-leaf1 ~ es-leaf2 ×					
Attached Switch Interface*					
vPC1	$\times \vee$				
Link Template* service_link_vpc $\times$					
			No Data in Template		

- 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。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)]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。

	Create Service Node	2 3 Create Route Peering Create Service Policy	
Detach			
Booring Namet			
peeringInterTenant			
Deployment*			
Peering Option*			
EBGP Dynamic Peering XV			
Inside Network		Outside Network	
VRF*		VRF*	
MyVRF_51000 X V		MyVRF_51000 X V	
Network Type*		Network Type*	
Inside Network $ imes \lor$		Outside Network $ imes \lor$	
Service Network*		Service Network*	
net_inside_inter_tenant $\times \lor$		net_outside_inter_tenant $\times \vee$	
VLAN ID*		VLAN ID*	
3001		3002	
Propose		Propose	
30010		30011	
Sonico Notwork Tomolatof		Sonico Network Tomolato*	
Service_Network_Universal ×		Service_Network_Universal ×	
General Parameters Advanced		General Parameters Advanced	
192.168.32.1/24	example 192.0.2.1/24. Ipv4 or Ipv6	32.32.32.1/24	example 192.0.2.1/24. lpv4 or lpv5
Pur Gateway/Prefy	gateway is mandatory.	IDv8 Gataway/Prafix	gateway is mandatory.
irvo Gateway/Fleix	example 2001:db8::1/64	invo Gateway/Frenk	example 2001:db8:1/64
VI AN Name		VI AN Name	
A series of the	if > 32 chars enable:system vian long- name		if > 32 chars enable:system vian long- name
Interface Description		Interface Description	
fw:inside:SITE_B:ASA2:Giga1/1:peeringInterTenant		fw:outside:SITE_B:ASA2:Giga1/1:peeringInterTenant	
Peering Template*		Peering Template*	
service_ebgp_route ×		service_ebgp_route ×	
General Parameters Advanced		General Parameters Advanced	
Neighbor IPv4 address or subnet*		Neighbor IPv4 address or subnet*	
192.168.32.254	reeghtor IPv4 address or address with netmask, ex 1.2.3.4 or 1.2.3.1/24.	32.32.32.254	Neightor II-V4 address or address with netmask, ex 1.2.3.4 or 1.2.3.1/24.
	rvegnoor IPv4 or IPv6 address is mandatory.		reegnoor e-v4 or IPv6 address is mandatory.
Loopback IP*	Westman of the Involved Landson	Loopback IP*	Balance data terratuk lanakat
60.1.1.60	er excrets of the topptack. Loopback IPv4 or IPv6 address is mandatory.	61.1.1.60	Pvd or IPv6 address is mandatory.
vPC Peer's Loopback IP		vPC Peer's Loopback IP	
60.1.1.61	IP address of the peer's loopback	61.1.1.61	IP address of the peer's loopback

#### 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 12vpn evpn
 advertise-pip
neighbor 10.2.0.4
  remote-as 12345
 update-source loopback0
 address-family 12vpn evpn
  send-community
   send-community extended
 vrf myvrf 50001
  address-family ipv4 unicast
   advertise 12vpn evpn
   redistribute direct route-map fabric-rmap-redist-subnet
   maximum-paths ibqp 2
  address-family ipv6 unicast
   advertise 12vpn 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 12vpn evpn
 redistribute direct route-map fabric-rmap-redist-subnet
 maximum-paths ibgp 2
 address-family ipv6 unicast
  advertise 12vpn 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-leafl 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-leafl 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、そのユースケースの手順に提供されているリンクを参照してください。

## 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。

Service Node		
	1 3 Create Service Node Create Route Peering Create Service Policy	
Service Node Name*		
LB1		
Service Node Type*		
Load Balancer X V		
Form Factor*		
Physical $\times$ $\vee$		
External Fabric*		
SITE_B × V		
Service Node Interface*		
G1/1		
Attached Fabric*		
SITE_A × ∨		
Attached Switch* es-leaf3 ×		
Attached Switch Interface*		
Ethernet1/50 X V		
Link Template* service_link_trunk ×		
General Parameters Advanced		
мто•		
Jumbo	V MITU for the interface	
SPEED*		
Auto	✓ Interface Speed	
Trunk Allowed Vlans*		
none	Allowed values: 'none', 'all', or vian ranges (ec: 1-200,500-2000,000)	
Enable BPDU Guard*		
no	Entities spenning-thee boologuent: thee reader, teser disable, normatum to desuit     settings*	
Enable Port Type Fast*	Enable spanning-tree edge port behavior	
Enable Interface*		

**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。

- 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 (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。

- **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。

	ervice Policy		? >
But But   Succon Price years   pering Lama*	Create Service Node	Create Route Pearing Create Service Policy	
Berdon Policy Manne*   Description   Perstription   Perstription   Perstription   MAVRP_5000   Scores Methand*   Market Scores   Market Scores   Methander   Market Scores   Methander   Market Scores   Methander   Market Scores   Methander   Methander<	Detach Attach		
pering Name"   pering Name"   pering Name"   more Net Name"   MyRE_51000   Score Net Name"   More Name" <	Service Policy Name*		
Pering Name*   pering 1   MVPC_51000   Destantion VEP Name*   MVPC_51000   MVPC_51000   MVPC_51000   MVPC_51000   MVPC_51000   VENNER VERNER*   MVPC_51000   MVPC_51000   MVPC_51000   MVPC_51000   MVPC_510000   MVPC_510000   MVPC_510000   MVPC_510000   MVPC_510000   MVPC_5100000   MVPC_5100000   MVPC_5100000   MVPC_51000000   MVPC_5100000000   MVPC_51000000000000000000000000000000000000	policy1		
pering tansar     pering tansar     Source MP Numer     MyNPE_51000           Destination Vide Namer   MyNPE_51000   Cource Memorit*   MyNPE_5000   MyNPE_5000 <t< td=""><td></td><td></td><td></td></t<>			
Internation   MANPE_51000   MANPE_51000   Destination VDF Name*   MANPE_51000   Destination NDF Name*   ManPE_51000   Destination NDF Name*   ManPE_51000   Destination NDF Name*   Destination NDF Name*   Destination NDF	Peering Name*	X v	
Source WER Name*   Moversg. 1000   Moversg. 1000  <			
MVRF_51000   Destination VMF Name*   MVRF_51000   MVRF_510000   MVRF_5100000   MVRF_51000000   MVRF_51000000   MVRF_510000000   MVRF_510000000   MVRF_510000000   MVRF_5100000000   MVRF_51000000000000000000000000000000000000	Source VRF Name*		
Destration WP Name*   MVWP_51000   VALVE_51000   VALVE_51000   VALVE_51000   VALVE_51000   VALVE_51000   VALVE_5000   VALVE_50000   VALVE_500000   VALVE_500000   VA	MyVRF_51000	××	
MARE_5000 X v   Source Network* X v   MARE_11: 10.11.1/24 X v   Destruction Network* X v   MARE_10: 10.12.42 X v   Reverse Netxt Hop IP   12: 10.95 2.54   Barticle Farmine*   Market Source   Source Network   International Network*   Source Network   International Network   Source Network   International Network   Source Network   International Network	Destination VRF Name*		
Source Network* VAAU_11: 10.11.11/24 % Exercision Network* VAAU_10: 10.11.01/24 % Receive Network 00: P 102: 106: 0.254 Lisk Twengiat* Second Farameters Advanced Formation Second Seco	MyVRF_51000	$\times$ $\vee$	
WAR(11: 10.11.1/24   Destruction Network*   WAR(10: 10.10.1/24   WAR(10: 10.10.1/24   Reverse Nets Hots P*   10.10.024   Bore prime Nets Hots P*   10.10.024   10.10.024   11.11.11.11.11.11.11.11.11.11.11.11.11.	Source Network*		
Destination Network*       VKAN_10: 10.1.0 1/24       VKAN_20: 10.1.0 1/24       Newrite Next Hop IP       12.1.06.50.354       Existination*       Service_inerx*       Advanced       Protocol*       Source Pure*       Source Pure* <td>VLAN_11: 10.1.11.1/24</td> <td>×~</td> <td></td>	VLAN_11: 10.1.11.1/24	×~	
Measurement       MALLE 10.11.01/24       Measure Not Hop IP       120.106.50.254       Dist Template*       Advanced       Protocot*       Kop       Market*       Advanced       Protocot*       Kop       Market*       Bornet* Fort*       Bornet*       Bornet			
Reverse Next Ney P 192108.50.254 Link: Template's Concert Future Set Set Set Set Set Set Set Set Set Se	VLAN 10: 10.1.10.1/24		
Nervise Navi Hop IP 192:104-50:254 Link Template* Metrice_ptor ×			
12. tots out and Concernal Platameters Advanced Protocof* Top  Protocof* Top  Protocof*	Reverse Next Hop IP		
Concertal Farameters     Advanced       Concertal Farameters     Advanced       Protocol*     The protocol, sample train.       Source Port*     Source Port*       Source Port*     Source port number, sample train.       Target     and target protocol.       Addition Fort*     Source port number, sample any of A3, Value is grower for 'g' and target protocol.       Addition Fort*     Destention port number, sample any add, Value is grower for 'g' and target protocol.	192.108.30.254		
Ceneral Parameters Protocot*     Advanced       Top     Toppendix, sample up of 43. Wate a sporter for end toppendix       Source Post*     Source part notice, sample up of 43. Wate a sporter for end toppendix       Toppendix     Source part notice, sample up of 43. Wate a sporter for end toppendix       Concolition Post*     Destination part notice, sample up of 43. Wate a sporter for end toppendix       445     Vale not protein	Link Template* service_pbr ×		
Destination Port*       Additional Port*       Destination Port*       4d3     Sense per unlike sample any or 43. Sole is ignored for the run per unlike sample any or 43. Sole is ignored for the run per unlike sample any or 43. Sole is ignored for the run per unlike sample any or 43. Sole is ignored for the run per unlike sample any or 43. Sole is ignored for	Concert Recemptors Advanced		
Protocol*     To protocol wangin top.       Scarce Port*     Scarce port vertice, cample any or 443. Walk is ignored for for and their protocol       Destination Port*     Destination Port       443     Destination for for			
kg     No     The premote sample real.       Statutes Port*     Source port investic, sample real.     Source port investic, sample real.       Any     Source port investic, sample real.     Source port investic, sample real.       Destination Flopt*     Source port investic, sample real investic, sample real investic.       443     Source port investic, sample real.	Protocol*		
Borne Port     Borne portunities; extendit with of 43. Value is growed for "p"       atty     att 'unip intensit'       Destination Port+     Bestinations extendits port values; extendits port 43. Value is growed for "p"       443     Watch for protect	top	The protocol, example top.	
any boxes por threads, example any or 443, tokes a growter for the extension proved. Destination Poyrt*  443  Use Instance of the Poyre of 443, tokes a growter for the of end proved.	Source Port*		
Destination Port* 443 <sup>1</sup> W and Simp Portal <sup>1</sup> W and Simp Portal	any	ocurce por mattee, example any or 4+3, value is gnored for ip and 'iong' protocol	
443 Demoto por tarble, example any or 421. Value is groups for Varial forger process	Destination Port*		
	443	Destination port number, example any or 443. Value is ignored for '(p' and 'isomp' protocol	

## 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ヘ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 12vpn 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
```

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。