ACIポリシーベースのリダイレクトのトラブルシューティング

内容

概要

このドキュメントでは、ACIポリシーベースリダイレクト(PBR)のシナリオを理解してトラブルシューティングする手順について説明します。

背景説明

このドキュメントの内容は、『Troubleshooting Cisco Application Centric Infrastructure, Second Edition』に記載されている、ポリシーベースのリダイレクト – 概要、ポリシーベースのリダイレクト – サービスグラフの導入、ポリシーベースのリダイレクト – 転送およびポリシーベースのリダイレクト – その他のトラフィックフローの例の章から抜粋したものです。

ポリシーベースリダイレクトの概要

この章では、ポリシーベースのリダイレクト(PBR)を使用したアンマネージドモードのサービスグラフのトラブルシューティングについて説明します。

次に、一般的なトラブルシューティング手順を示します。この章では、PBRに固有のステップ2と3を確認する方法について説明します。ステップ1と4については、「Intra-Fabric Forwarding」、「External forwarding」、および「Security policies」の章を参照してください。

1. PBRサービスグラフなしでトラフィックが動作していることを確認します。
    - コンシューマとプロバイダーのエンドポイントが学習されます。
    - コンシューマとプロバイダーのエンドポイントが通信できる。
2. サービスグラフが展開されていることを確認します。
    - 配置されたグラフ・インスタンスにエラーはありません。
    - サービスノード用のVLANとクラスIDが展開されます。
    - サービスノードのエンドポイントが学習されます。
3. 転送パスを確認します。
    - リーフノードにチェックポリシーがプログラムされています。
    - サービスノード上のトラフィックをキャプチャして、トラフィックがリダイレクトされるかどうかを確認します。
    - ACIリーフのトラフィックをキャプチャして、PBRの後にトラフィックがACIファブリックに戻るかどうかを確認します。
4. トラフィックがコンシューマおよびプロバイダーのエンドポイントに到達し、エンドポイントがリターントラフィックを生成することを確認します。

このドキュメントでは、設計または設定オプションについては説明しません。詳細については、Cisco.comの「ACI PBRホワイトペーパー」を参照してください。

この章では、サービスノードとサービスリーフは次のことを意味します。

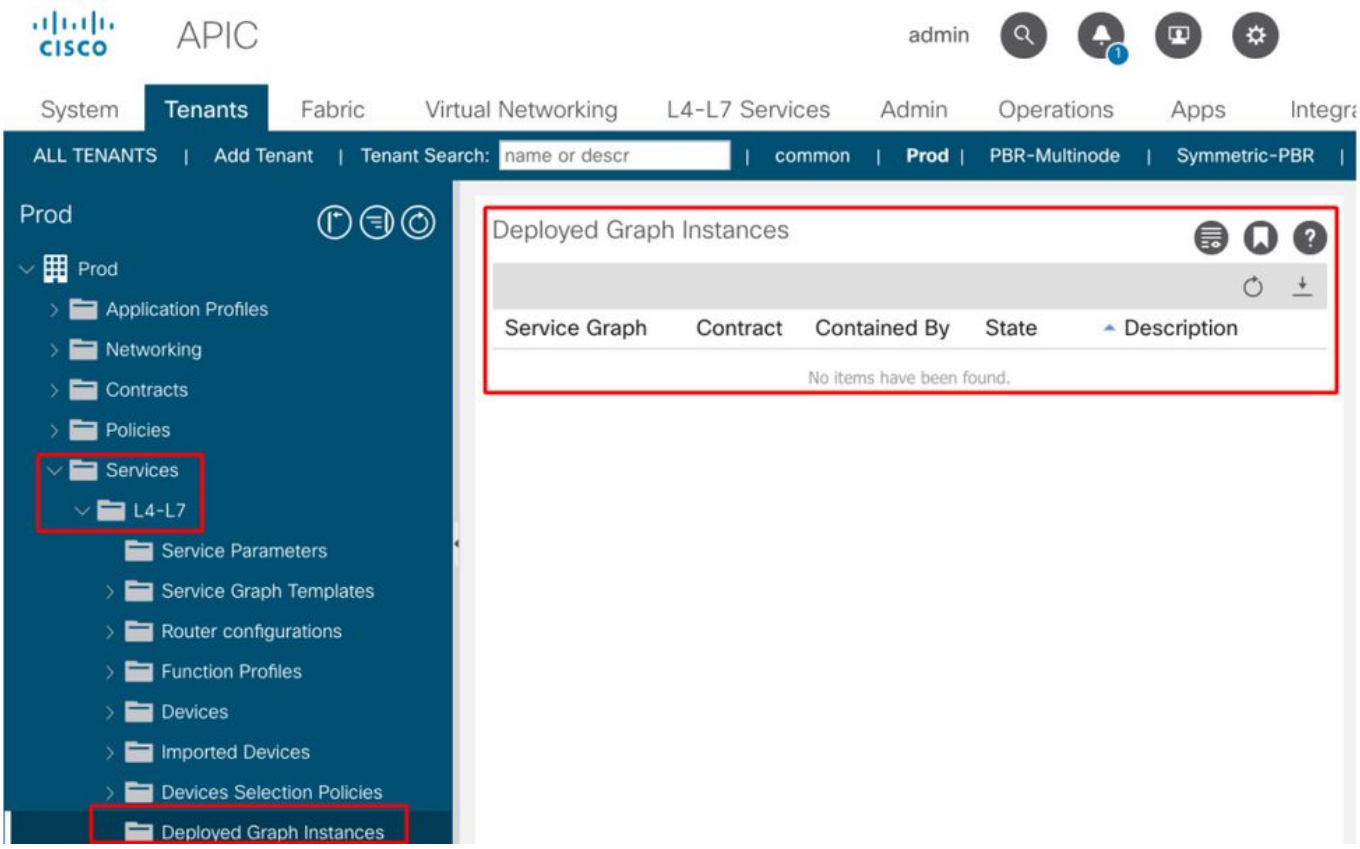
- サービスノード：PBRがトラフィックをリダイレクトする外部ノード（ファイアウォールやロードバランサなど）。
- サービスリーフ：サービスノードに接続されているACIリーフ。

サービスグラフ導入のトラブルシューティング

この章では、サービスグラフが導入されていない場合のトラブルシューティング例について説明します。

サービスグラフポリシーを定義してコントラクト対象に適用すると、ACI GUIに展開済みのグラフインスタンスが表示されます。次の図は、サービスグラフが導入済みとして表示されないトラブルシューティングシナリオを示しています。

サービスグラフは展開済みグラフインスタンスとして表示されません。



1.設定手順と障害を確認する

トラブルシューティングの最初のステップは、必要なコンポーネントが何の障害もなく設定されていることを確認することです。ここでは、次の一般的な設定がすでに行われていることを前提としています。

- コンシューマEPG、プロバイダーEPG、およびサービスノード用のVRFおよびBD
- コンシューマおよびプロバイダーのEPG
- コントラクトとフィルタ。

サービスノードのEPGは手動で作成する必要がないことに注意してください。サービスグラフの導入によって作成されます。

PBRを使用したサービスグラフの設定手順は次のとおりです。

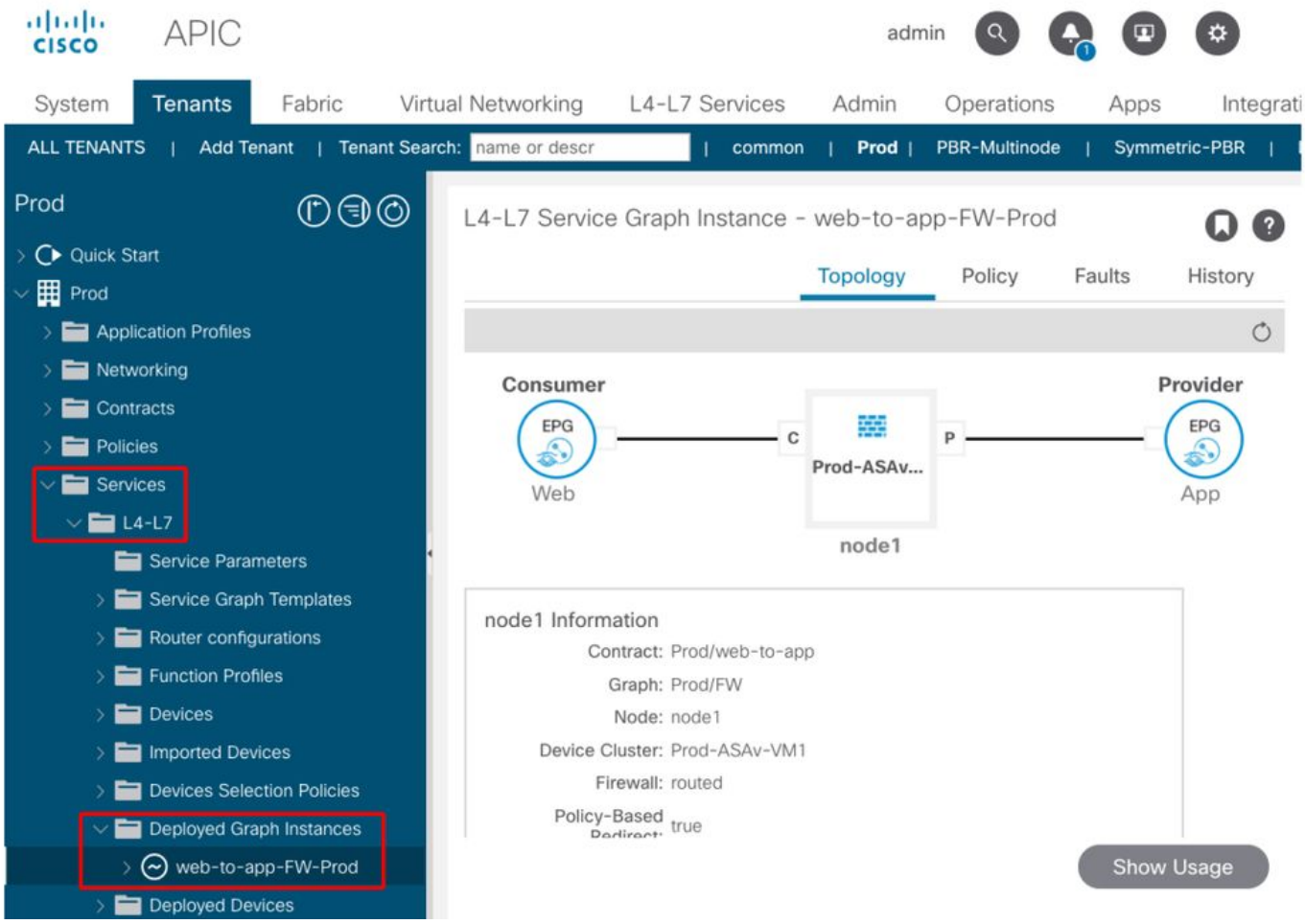
- L4-L7デバイス（論理デバイス）を作成します。
- サービスグラフを作成します。
- PBRポリシーを作成します。
- デバイス選択ポリシーを作成します。
- サービスグラフを契約の件名に関連付けます。

2. UIでサービスグラフの展開を確認します

サービスグラフをコントラクト対象に関連付けると、展開されたグラフインスタンスがサービスグラフを使用してコントラクトごとに表示されます（下図）。

場所は、「テナント」>「サービス」>「L4-L7」>「導入済みグラフインスタンス」です。

配置されたグラフインスタンス



導入済みグラフインスタンスが表示されない場合は、コントラクト設定に問題があります。主な理由は次のとおりです。

- 契約にコンシューマEPGまたはプロバイダーEPGがない。
- コントラクト対象にフィルターがありません。
- コントラクトの範囲はVRFですが、VRF間またはテナント間のEPG通信用です。

サービスグラフのインスタンス化が失敗すると、展開済みグラフインスタンスでエラーが発生します。これは、サービスグラフの設定に問題があることを意味します。設定によって発生する一般的な障害は次のとおりです。

F1690: ID割り当ての失敗により、構成が無効です

このエラーは、サービスノードのカプセル化されたVLANが使用できないことを示します。たとえば、論理デバイスで使用されるVMMドメインに関連付けられたVLANプールに、使用可能なダイナミックVLANがありません。

解決策：論理デバイスに使用されるドメインのVLANプールを確認します。物理ドメイン内にある場合は、論理デバイスインターフェイスでカプセル化されたVLANを確認します。場所は、「テナント」>「サービス」>「L4-L7」>「デバイスとファブリック」>「アクセスポリシー」>「プ

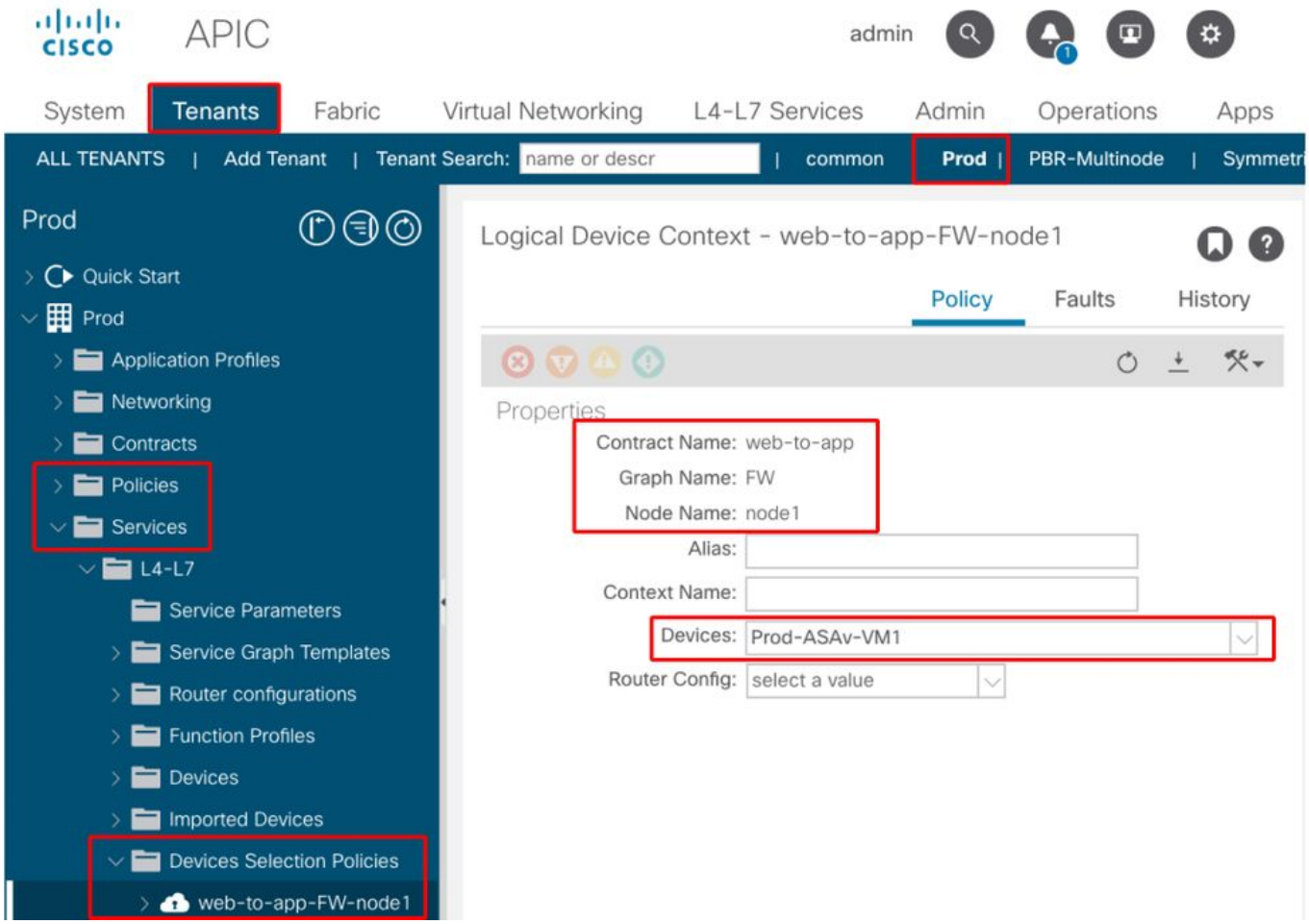
ール」>「VLAN」です。

F1690: LDevのデバイスコンテキストが見つからないため、構成が無効です

このエラーは、サービスグラフのレンダリングに論理デバイスが見つからないことを示します。たとえば、サービスグラフの契約に一致するデバイス選択ポリシーがありません。

解決策：デバイス選択ポリシーが定義されていることを確認します。デバイス選択ポリシーは、サービスデバイスとそのコネクタの選択基準を提供します。基準は、契約名、サービスグラフ名、およびサービスグラフ内のノード名に基づいています。場所は、「Tenant > Services > L4-L7 > Device Selection Policy」です。

デバイス選択ポリシーの確認



F1690：クラスタインターフェイスが見つからないため、構成が無効です

このエラーは、サービスノードのクラスタインターフェイスが見つからないことを示します。たとえば、クラスタインターフェイスはデバイス選択ポリシーで指定されていません。

解決策：デバイス選択ポリシーでクラスタインターフェイスが指定されており、コネクタ名が正しいことを確認します（下図）。

F1690:BDが見つからないため、構成が無効です

このエラーは、サービスノードのBDが見つからないことを示します。たとえば、BDはデバイス

選択ポリシーでは指定されません。

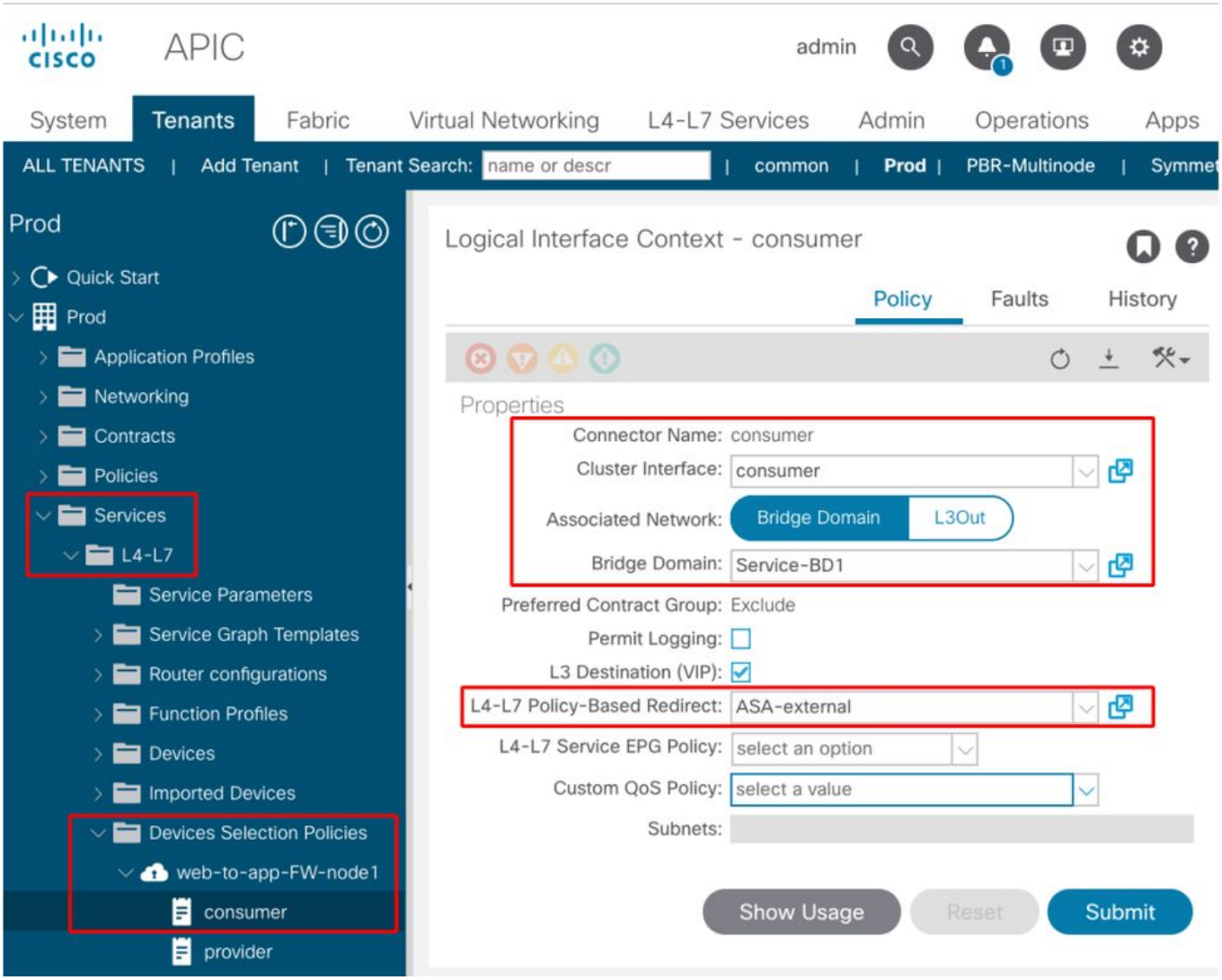
解決策：デバイス選択ポリシーでBDが指定されており、コネクタ名が正しいことを確認します（下図）。

F1690：無効なサービスリダイレクトポリシーのため、構成が無効です

このエラーは、サービスグラフのサービス機能でリダイレクトが有効になっていても、PBRポリシーが選択されていないことを示します。

解決策：デバイス選択ポリシーでPBRポリシーを選択します（下図）。

デバイス選択ポリシーの論理インターフェイスの設定



PBR転送のトラブルシューティング

この章では、PBR転送パスのトラブルシューティング手順について説明します。

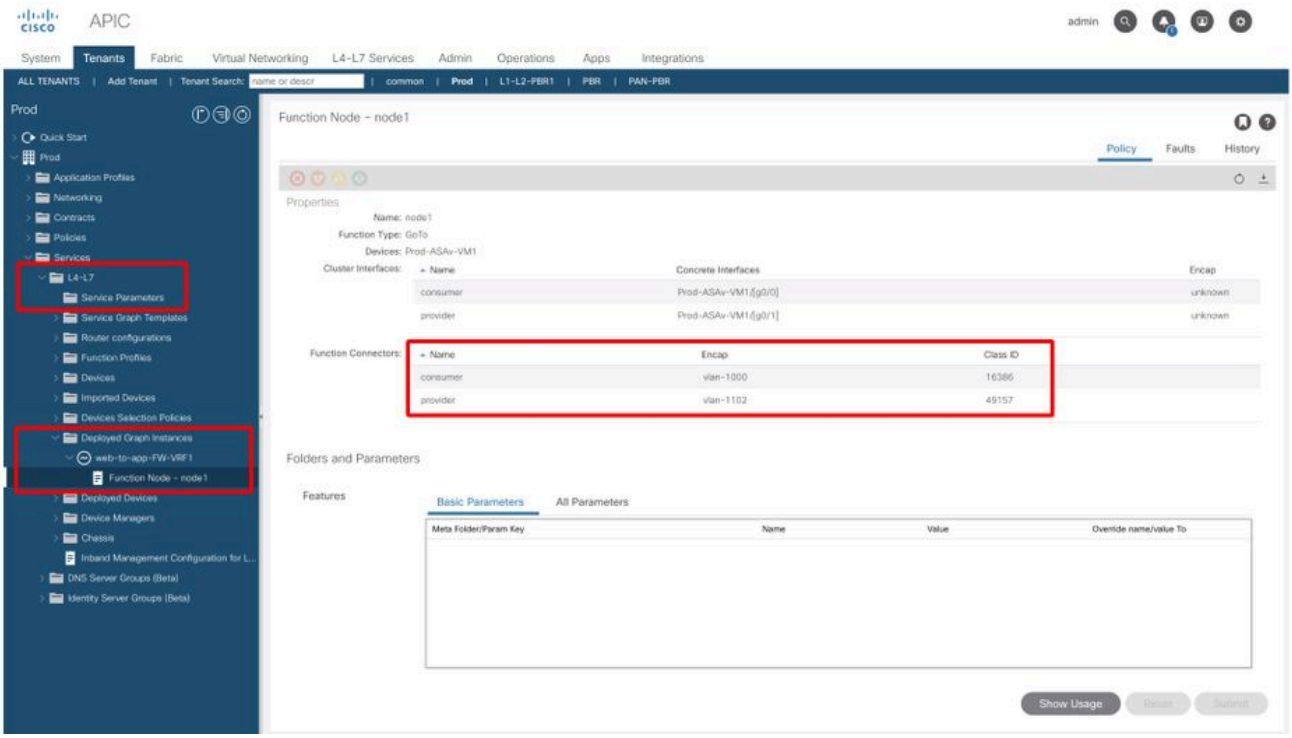
1. VLANが展開され、エンドポイントがリーフノードで学習されていることを確認します

サービスグラフが問題なく正常に導入されると、サービスノードのEPGとBDが作成されます。次

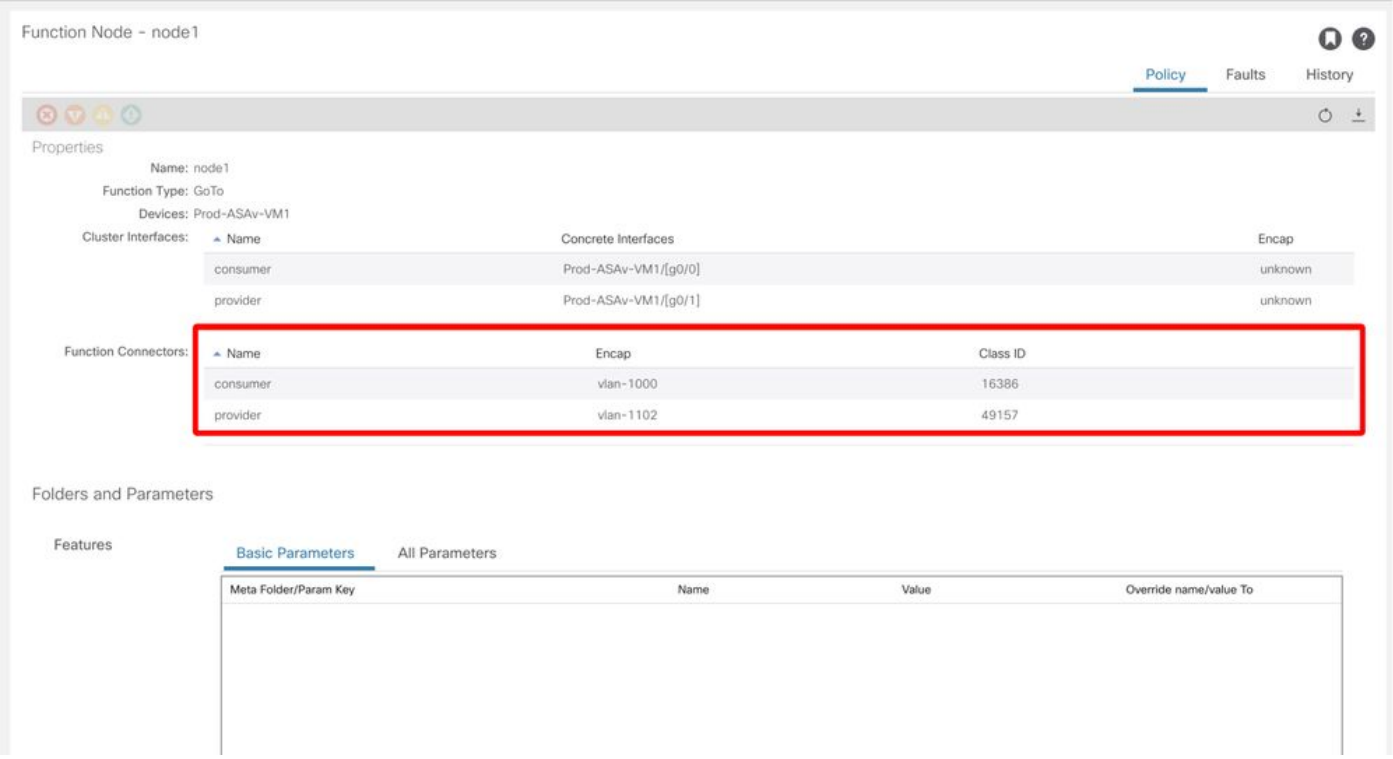
の図は、サービスノードインターフェイス（サービスEPG）のカプセル化されたVLAN IDとクラスIDの場所を示しています。この例では、ファイアウォールのコンシューマ側はVLANカプセル化1000を使用したクラスID 16386で、ファイアウォールのプロバイダー側はVLANカプセル化1102を使用したクラスID 49157です。

場所は、「Tenant」>「Services」>「L4-L7」>「Deployed Graph instances」>「Function Nodes」です。

サービスノード



サービスノードインターフェイスクラスID



これらのVLANは、サービスノードが接続されているサービスリーフノードインターフェイスに導入されます。サービスリーフノードのCLIで「show vlan extended」および「show endpoint」を使用すると、VLANの導入とエンドポイントのラーニングステータスを確認できます。

<#root>

```
Pod1-Leaf1#

 show endpoint vrf Prod:VRF1


Legend:
s - arp              H - vtep             V - vpc-attached     p - peer-aged
R - peer-attached-rl B - bounce           S - static           M - span
D - bounce-to-proxy  O - peer-attached    a - local-aged       m - svc-mgr
L - local            E - shared-service
+------------------------------------+---------------+-----------------+--------------+-------------+
      VLAN/                           Encap           MAC Address       MAC Info/       Interface
      Domain                          VLAN            IP Address        IP Info
+------------------------------------+---------------+-----------------+--------------+-------------+
53                                      vlan-1000     0050.56af.3c60 LV                      po1
Prod:VRF1                               vlan-1000    192.168.101.100 LV                      po1
59                                      vlan-1102     0050.56af.1c44 LV                      po1
Prod:VRF1                               vlan-1102    192.168.102.100 LV                      po1
```

サービスノードのエンドポイントIPがACIファブリックのエンドポイントとして学習されない場合、サービスリーフとサービスノード間の接続または設定の問題である可能性が高くなります。次のステータスを確認してください。

- サービスノードは、正しいリーフダウンリンクポートに接続されます。
  - サービスノードが物理ドメインにある場合、リーフスタティックパスエンドカプセル

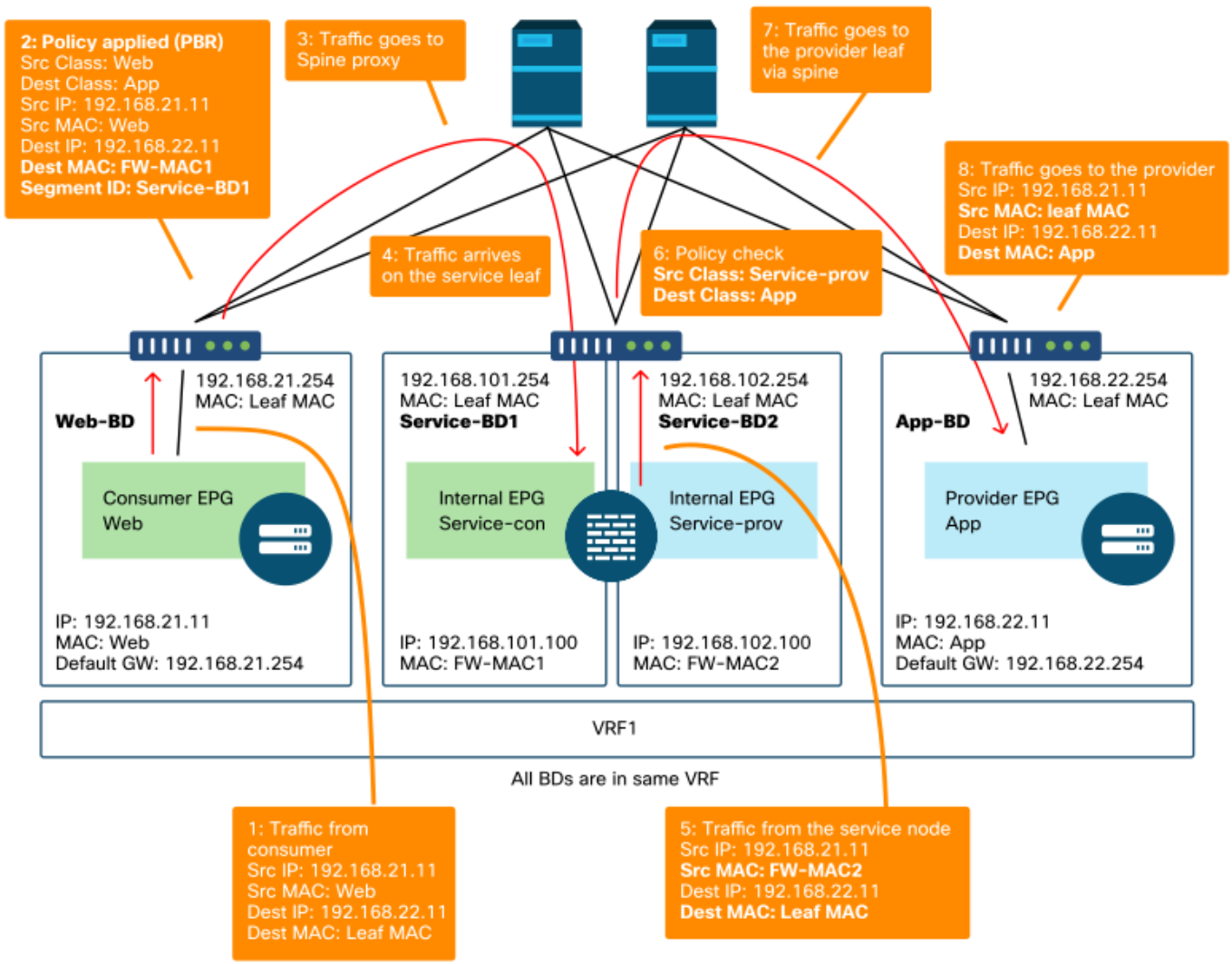
化VLANを論理デバイスで定義する必要があります。
    - サービスノードがVMMドメイン内にある場合は、VMMドメインが機能していること、およびサービスグラフで作成したポートグループがサービスノードVMに正しく関連付けられていることを確認してください。
- サービスノードVMが存在するサービスノードまたはハイパーバイザに接続されているリーフダウンリンクポートはUPです。
- サービスノードに正しいVLANとIPアドレスがある。
- サービスリーフとサービスノード間の中間スイッチのVLAN設定が正しい。

2.予想されるトラフィックパスを確認する

PBRを有効にすると、サービスノードのエンドポイントがACIファブリックで学習された場合でも、エンドツーエンドのトラフィックが機能しなくなった場合、次のトラブルシューティング手順では、想定されるトラフィックパスを確認します。

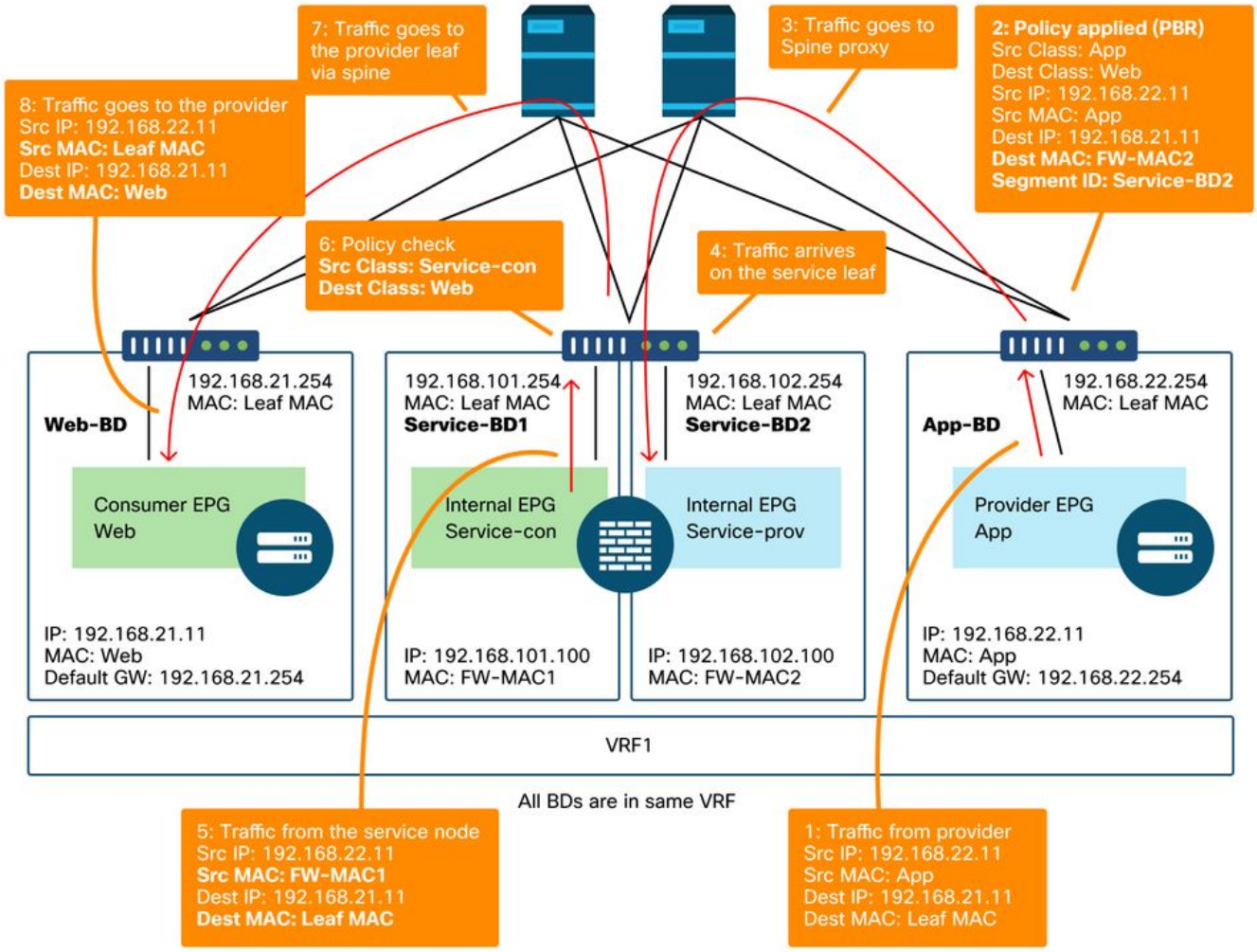
図「PBR転送パスの例 – コンシューマからプロバイダー」および「PBR転送パスの例 – プロバイダーからコンシューマ」は、コンシューマエンドポイントとプロバイダーエンドポイント間でPBRを使用してファイアウォールを挿入した転送パスの例を示しています。ここでは、リーフノードでエンドポイントがすでに学習されていると想定しています。

PBR転送パスの例：コンシューマからプロバイダー



注：送信元MACはACIリーフMACに変更されないため、コンシューマエンドポイントとPBRノードが同じBD内にない場合、PBRノードは送信元MACベースの転送を使用できません

PBR転送パスの例：プロバイダーからコンシューマ



注：PBRポリシーはコンシューマリーフまたはプロバイダーリーフのいずれかに適用され、図「PBR転送パスの例 – コンシューマからプロバイダー」および「PBR転送パスの例 – プロバイダーからコンシューマ」に示すようにACI PBRが宛先MAC書き換えを行うことに注意してください。PBR宛先MACに到達するには、送信元エンドポイントとPBR宛先MACが同じリーフの下にある場合でも、常にスパインプロキシを使用します。

「PBR転送パスの例 – コンシューマからプロバイダー」および「PBR転送パスの例 – プロバイダーからコンシューマ」の図は、トラフィックがリダイレクトされる場所の例を示していますが、ポリシーが適用される場所は、コントラクトの設定とエンドポイントの学習ステータスによって異なります。「ポリシーが適用される場所」の表は、1つのACIサイトでポリシーが適用される場所をまとめたものです。マルチサイトでポリシーが適用される場所は異なります。

ポリシーはどこに適用されますか。

シナリオ	VRF適用モード	消費者	プロバイダー	ポリシーの適用
VRF内	入力/出力	EPG	EPG	・ 宛先エンドポイントが学習された場

シナリオ	VRF適用モード	消費者	プロバイダー	ポリシーの適用
				合：入力リーフ* ・ 宛先エンドポイントが学習されない場合：出力リーフ
	入力	EPG	L3出力EPG	コンシューマリーフ（非ボーダーリーフ）
	入力	L3出力EPG	EPG	プロバイダーリーフ（非ボーダーリーフ）
	出力	EPG	L3出力EPG	境界リーフ –>非境界リーフトラフィック ・ 宛先エンドポイントが学習された場合：境界リーフ ・ 宛先エンドポイントが学習されない場合：非ボーダーリーフ
	出力	L3出力EPG	EPG	非ボーダーリーフ –>ボーダーリーフトラフィック ・ 境界リーフ
	入力/出力	L3出力EPG	L3出力EPG	入力リーフ*
VRF間	入力/出力	EPG	EPG	コンシューマリーフ
	入力/出力	EPG	L3出力EPG	コンシューマリーフ（非ボーダーリーフ）
	入力/出力	L3出力EPG	EPG	入力リーフ*
	入力/出力	L3出力	L3出力	入力リーフ*

シナリオ	VRF適用モード	消費者	プロバイダー	ポリシーの適用
		EPG	EPG	

*ポリシーの適用は、パケットによる最初のリーフヒットに適用されます。

次に例を示します。

- VRF1のL3Out EPGの外部エンドポイントがVRF1のWeb EPGのエンドポイントにアクセスしようとし、VRF1が入力強制モードに設定されている場合、コントラクトの方向に関係なく、トラフィックはWeb EPGのエンドポイントが存在するリーフによってリダイレクトされます。
- VRF1のコンシューマWeb EPGのエンドポイントがVRF1のプロバイダーアプリケーションEPGのエンドポイントにアクセスしようとし、エンドポイントがコンシューマおよびプロバイダーリーフノードで学習された場合、トラフィックは入力リーフによってリダイレクトされます。
- VRF1のコンシューマWeb EPGのエンドポイントがVRF2のプロバイダーアプリケーションEPGのエンドポイントにアクセスしようとすると、VRF強制モードに関係なく、コンシューマエンドポイントが存在するコンシューマリーフによってトラフィックがリダイレクトされます。

3.トラフィックがサービスノードにリダイレクトされるかどうかを確認します

予想される転送パスがクリアされたら、ELAMを使用して、トラフィックがスイッチノードに到達したかどうかを確認し、スイッチノードでの転送の決定を確認できます。ELAMの使用方法については、「Intra-Fabric Forwarding」の章の「ツール」の項を参照してください。

たとえば、「PBR転送パスの例 – コンシューマからプロバイダー」の図のトラフィックフローをトレースするために、これらをキャプチャして、コンシューマからプロバイダーへのトラフィックがリダイレクトされるかどうかを確認できます。

- 1と2をチェックするコンシューマリーフのダウンリンクポート（トラフィックはコンシューマリーフに到達し、PBRが適用されます）。
- チェック対象のスパインノードのファブリックポート3（トラフィックはスパインプロキシに送信される）
- 4をチェックするサービスリーフのファブリックポート（トラフィックはサービスリーフに到達）。

次に、これらをキャプチャして、サービスノードから戻ってくるトラフィックがプロバイダーに向かうかどうかを確認できます。

- サービスリーフ上のダウンリンクポートをチェック5および6（トラフィックはサービスノードから戻され、許可される）。
- スパインノード上のファブリックポートをチェック7（スパイン経由でトラフィックがプロバイダーリーフに送られる）。

- チェックするプロバイダーリーフのファブリックポート8（トラフィックはサービスリーフに到達し、プロバイダーエンドポイントに向かう）。

注：コンシューマとサービスノードが同じリーフの下にある場合、両方が同じ送信元IPと宛先IPを使用するため、図「PBR転送パスの例：コンシューマからプロバイダー」の1または5でELAMがチェックするように、送信元/宛先IPに加えてインターフェイスまたは送信元MACを指定します。

コンシューマからプロバイダーへのトラフィックがサービスノードにリダイレクトされても、サービスリーフに戻ってこない場合は、次の点を確認してください。これらは一般的な誤りです。

- サービスノードルーティングテーブルがプロバイダーサブネットに到達します。
- ACLなどのサービスノードのセキュリティポリシーにより、トラフィックが許可されます。

トラフィックがリダイレクトされてプロバイダーに到達する場合は、同様の方法でプロバイダーからコンシューマへのリターントラフィックパスを確認してください。

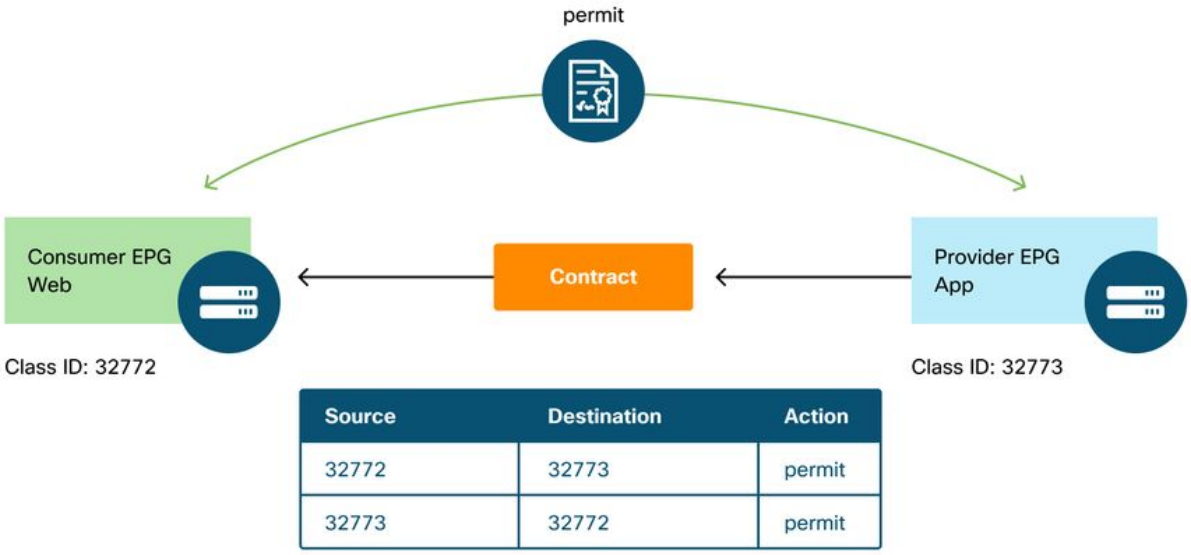
4.リーフノードにプログラムされているポリシーを確認します

それに応じてトラフィックが転送またはリダイレクトされない場合、次のトラブルシューティング手順は、リーフノードにプログラムされているポリシーを確認することです。このセクションでは、例としてzoning-ruleとcontract_parserを示します。ゾーン分割ルールの確認方法の詳細については、「セキュリティポリシー」の章の「ツール」の項を参照してください。

注：ポリシーは、リーフ上のEPG展開ステータスに基づいてプログラムされます。このセクションのshowコマンド出力では、サービスノードのコンシューマEPG、プロバイダーEPG、およびEPGを持つリーフを使用します。

「show zoning-rule」コマンドの使用

次の図と「show zoning-rule」の出力は、サービスグラフを展開する前のゾーン分割ルールを示しています。



Source	Destination	Action
32772	32773	permit
32773	32772	permit

VRFスコープIDは、「Tenant」>「Networking」>「VRF」にあります。

<#root>

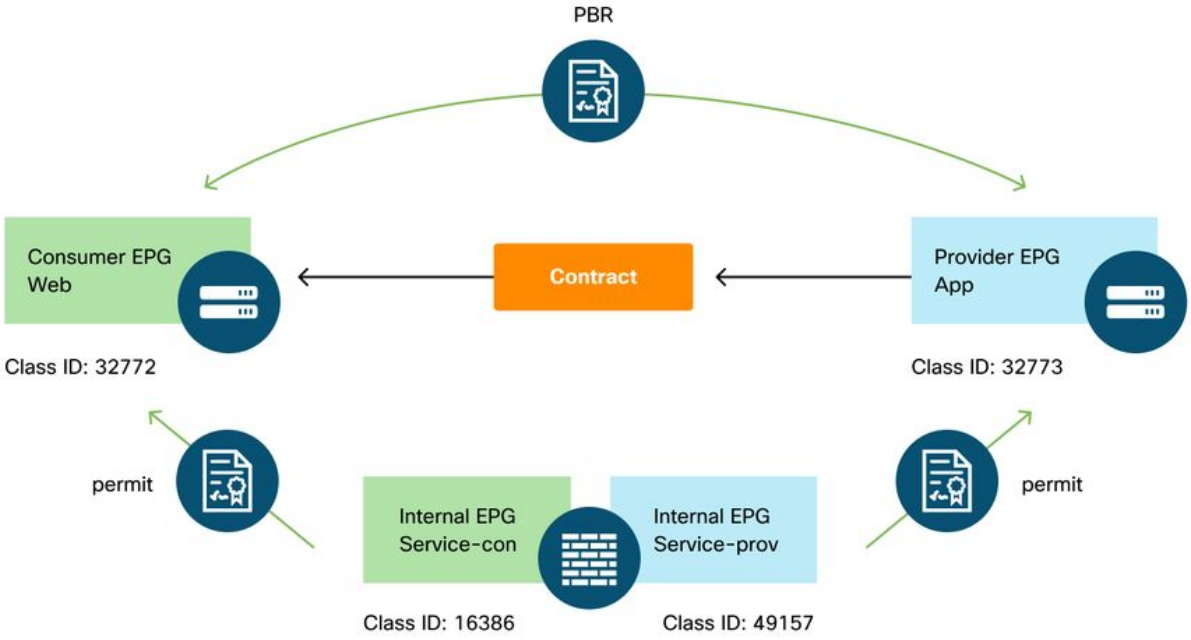
```
Pod1-Leaf1#

show zoning-rule scope 2752513

+---------+--------+--------+----------+----------------+---------+---------+------------+----------+--
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |    Name    |  Action  |
+---------+--------+--------+----------+----------------+---------+---------+------------+----------+--
|   4237  | 32772  | 32773  |    8     |     bi-dir     | enabled | 2752513 | web-to-app |  permit  |
|   4172  | 32773  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 | web-to-app |  permit  |
+---------+--------+--------+----------+----------------+---------+---------+------------+----------+--
```

サービスグラフが展開されると、サービスノードのEPGが作成され、ポリシーが更新されてコンシューマEPGとプロバイダーEPG間のトラフィックがリダイレクトされます。次の図と「show zoning-rule」の出力は、サービスグラフ導入後のゾーン分割ルールを示しています。この例では、pcTag 32772(Web)からpcTag 32773(App)へのトラフィックは「destgrp-27」（サービスノードのコンシューマ側）にリダイレクトされ、pcTag 32773(App)からpcTag 32772(Web)へのトラフィックは「destgrp-28」（サービスノードのプロバイダ側）にリダイレクトされます。

サービスグラフ導入後のゾーン分割ルール



Source	Destination	Action
32772	32773	PBR to the consumer side of the service node
49157	32773	permit
32773	32772	PBR to the provider side of the service node
16386	32772	permit

<#root>

Pod1-Leaf1#

show zoning-rule scope 2752513

```
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------
...
|   4213  | 16386  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |       permit
|   4249  | 49157  | 32773  | default  |    uni-dir     | enabled | 2752513 |      |       permit
|   4237  | 32772  | 32773  |    8     |     bi-dir     | enabled | 2752513 |      | redir(destgrp-27)
|   4172  | 32773  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      | redir(destgrp-28)
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------
```

各destgrpの宛先情報は、「show service redir info」コマンドを使用して確認できます。

<#root>

Pod1-Leaf1#

```
show service redir info
```

```
========================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-Dest |
========================================================================================
List of Dest Groups
GrpID Name            destination                                HG-name           BAC  operSt     ope
===== ====            ===========                                ==============    ===  =======    ===
28    destgrp-28      dest-[192.168.102.100]-[vxlan-2752513]     Not attached      N    enabled    no-
27    destgrp-27      dest-[192.168.101.100]-[vxlan-2752513]     Not attached      N    enabled    no-

List of destinations
Name                                        bdVnid            vMac                 vrf          op
====                                        ======            ====                 ====         ==
dest-[192.168.102.100]-[vxlan-2752513]      vxlan-16023499    00:50:56:AF:1C:44    Prod:VRF1    en
dest-[192.168.101.100]-[vxlan-2752513]      vxlan-16121792    00:50:56:AF:3C:60    Prod:VRF1    en
...
```

ゾーニング・ルールが適切にプログラムされているが、それに応じてトラフィックがリダイレクトまたは転送されない場合は、次の点を確認してください。これらは一般的な間違いです。

- ELAMを使用して、送信元クラスIDまたは宛先クラスIDが期待どおりに解決されるかどうかを確認します。そうでない場合は、間違ったクラスIDと、パスやカプセル化VLANなどのEPG導出基準を確認してください。
- 送信元と宛先のクラスIDが適切に解決され、PBRポリシーが適用されてもトラフィックがPBRノードに到達しない場合でも、redirアクション(「show service redir info」)で宛先のIP、MAC、およびVRFが正しいことを確認してください。

デフォルトでは、PBRが有効になっている場合、サービスノード(コンシューマ側)に対するコンシューマEPGの許可ルールと、サービスノード(プロバイダー側)に対するプロバイダーEPGの許可ルールはプログラムされません。したがって、コンシューマまたはプロバイダーのエンドポイントは、デフォルトではサービスノードと直接通信できません。このトラフィックを許可するには、Direct Connectオプションを有効にする必要があります。使用例については、「その他のトラフィックフローの例」の項で説明します。

contract_parserの使用

contract_parserツールは、ポリシーの確認にも役立ちます。C-consumerはサービスノードのコンシューマ側で、C-providerはサービスノードのプロバイダー側です。

```
Pod1-Leaf1# contract_parser.py --vrf Prod:VRF1
Key:
[prio:RuleId] [vrf:{str}] action protocol src-epg [src-l4] dst-epg [dst-l4] [flags][contract:{str}] [hi

[7:4213] [vrf:Prod:VRF1] permit ip tcp tn-Prod/G-Prod-ASAv-VM1ctxVRF1/C-consumer(16386) eq 80 tn-Prod/a
[7:4237] [vrf:Prod:VRF1] redir ip tcp tn-Prod/ap-app1/epg-Web(32772) tn-Prod/ap-app1/epg-App(32773) eq
                                destgrp-27 vrf:Prod:VRF1 ip:192.168.101.100 mac:00:50:56:AF:3C:60 bd:uni
[7:4172] [vrf:Prod:VRF1] redir ip tcp tn-Prod/ap-app1/epg-App(32773) eq 80 tn-Prod/ap-app1/epg-Web(3277
                                destgrp-28 vrf:Prod:VRF1 ip:192.168.102.100 mac:00:50:56:AF:1C:44 bd:uni
[9:4249] [vrf:Prod:VRF1] permit any tn-Prod/G-Prod-ASAv-VM1ctxVRF1/C-provider(49157) tn-Prod/ap-app1/ep
```

...

その他のトラフィックフローの例

このセクションでは、トラブルシューティングに必要なフローを特定するために、その他の一般的なトラフィックフローの例を検討します。トラブルシューティングの手順については、このセクションの前の章を参照してください。

1. SNATのないロードバランサ：
    - この例では、コンシューマEPG WebおよびプロバイダEPGアプリケーションに、ロード・バランサ・サービス・グラフとの契約があります。App EPGのエンドポイントは、ロードバランサのVIPに関連付けられた実サーバです。
    - プロバイダーからコンシューマトラフィックの方向に対して、ロードバランサへのPBRが有効になっています。
2. SNATのないファイアウォールとロードバランサ：
    - この例では、コンシューマEPG WebおよびプロバイダーEPGアプリケーションに、ファイアウォールおよびロードバランサのサービスグラフとの契約があります。App EPGのエンドポイントは、ロードバランサのVIPに関連付けられた実サーバです。
    - 両方向でファイアウォールへのPBRが有効になっている。
    - プロバイダーからコンシューマトラフィックの方向に対して、ロードバランサへのPBRが有効になっています。
3. 共有サービス（VRF間契約）：
    - この例では、コンシューマEPG WebおよびプロバイダーEPGアプリケーションにファイアウォールサービスグラフとの契約があります。EPG WebとEPG Appは異なるVRFにあります。
    - 両方向でファイアウォールへのPBRが有効になっている。
    - ファイアウォールはVRFの間にあります。

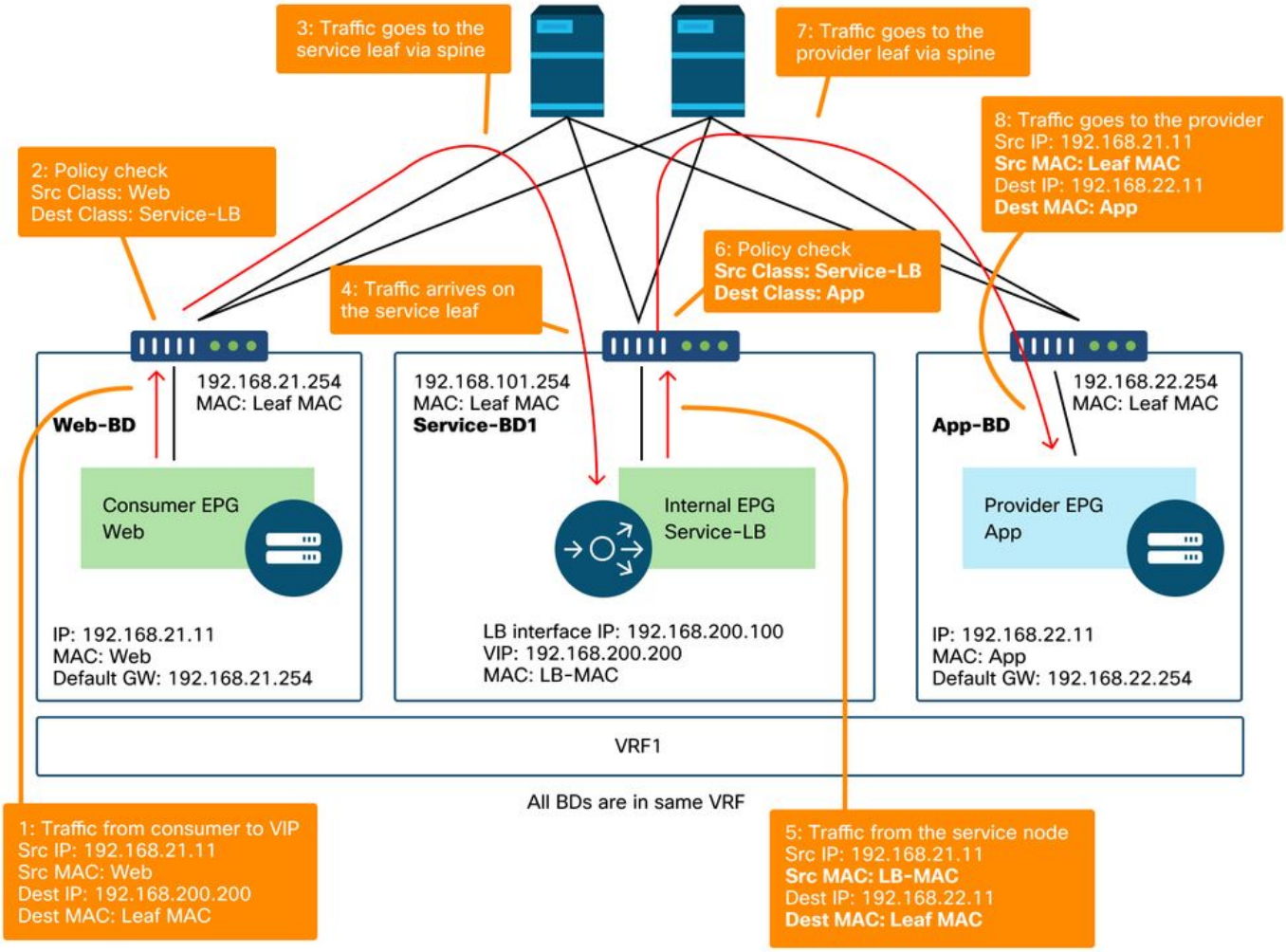
1. SNATのないロードバランサ

PBRは、双方向PBRまたは単方向PBRとして導入できます。単方向PBRの使用例の1つは、送信元ネットワークアドレス変換(NAT)を使用しないロードバランサの統合です。ロードバランサが送信元NATを実行する場合、PBRは必要ありません。

トラフィックパスの例

次の図は、2つの接続を持つコンシューマEPG WebからプロバイダーEPGアプリケーションへの着信トラフィックフローの例を示しています。1つはコンシューマEPG Web内のエンドポイントからロードバランサーVIPへの着信トラフィックフロー、もう1つはロードバランサーからプロバイダーEPGアプリケーション内のエンドポイントへの着信トラフィックフローです。着信トラフィックはVIP宛てであるため、VIPが到達可能であれば、トラフィックはPBRを使用しないロードバランサに到達します。ロードバランサは、宛先IPをVIPに関連付けられたEPGアプリケーションのいずれかのエンドポイントに変更しますが、送信元IPは変換しません。したがって、トラフィックはプロバイダーエンドポイントに向かいます。

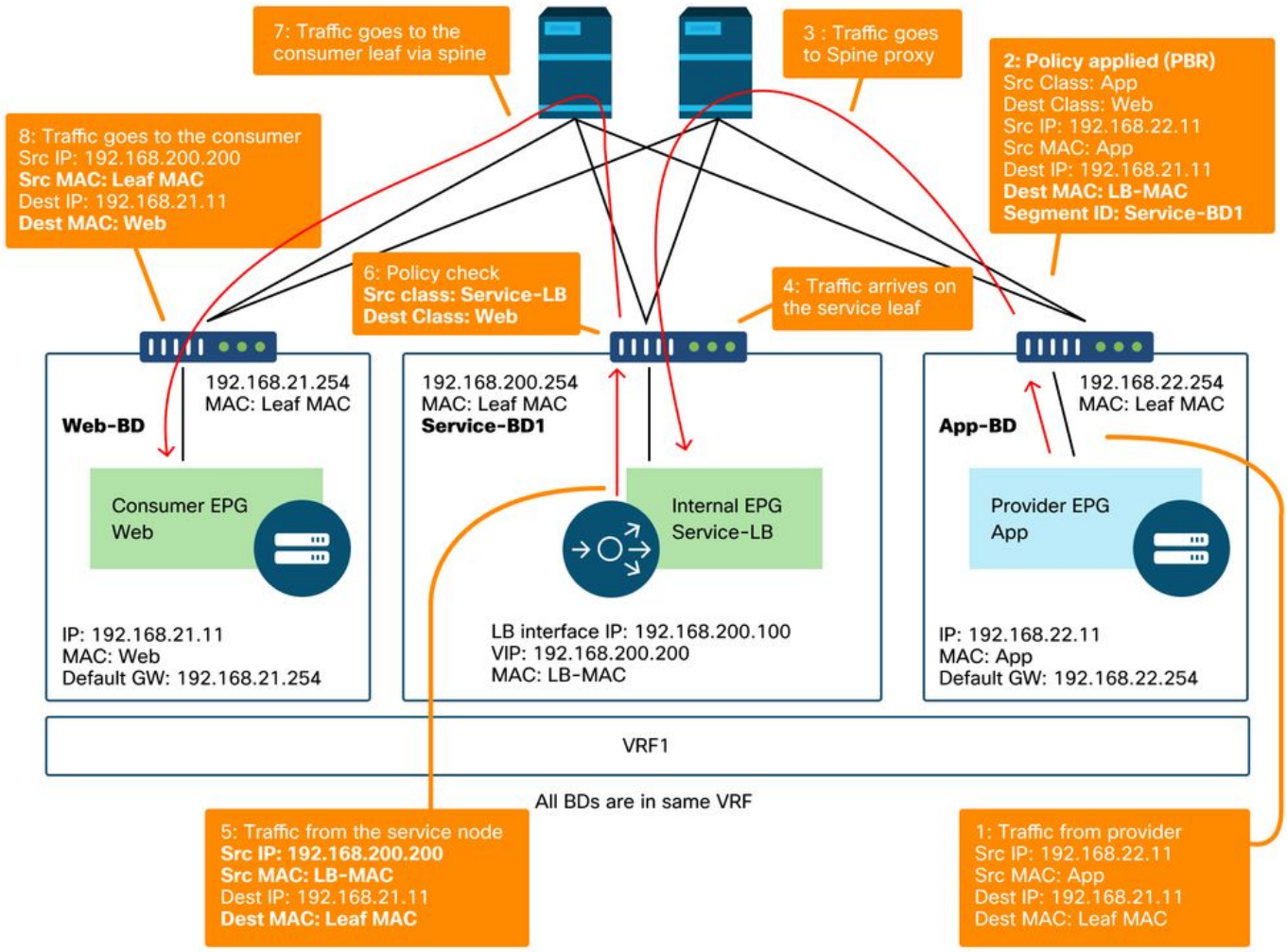
SNAT転送パスのないロードバランサの例：コンシューマからVIP、ロードバランサからプロバイダー（PBRなし）



次の図は、プロバイダーEPGアプリケーションからコンシューマEPG Webへのリターントラフィックフローを示しています。リターントラフィックは元の送信元IPを宛先としているため、PBRはリターントラフィックをロードバランサに戻すために必要です。それ以外の場合、コンシューマエンドポイントは、送信元IPがVIPではなくプロバイダーエンドポイントであるトラフィックを受信します。ACIファブリックなどの中間ネットワークがパケットをコンシューマエンドポイントに転送しても、コンシューマエンドポイントがプロバイダーエンドポイントへのトラフィックを開始しなかったため、このようなトラフィックはドロップされます。

プロバイダーエンドポイントからコンシューマエンドポイントへのトラフィックがロードバランサにリダイレクトされた後、ロードバランサは送信元IPをVIPに変更します。その後、トラフィックはロードバランサから戻り、コンシューマエンドポイントに戻ります。

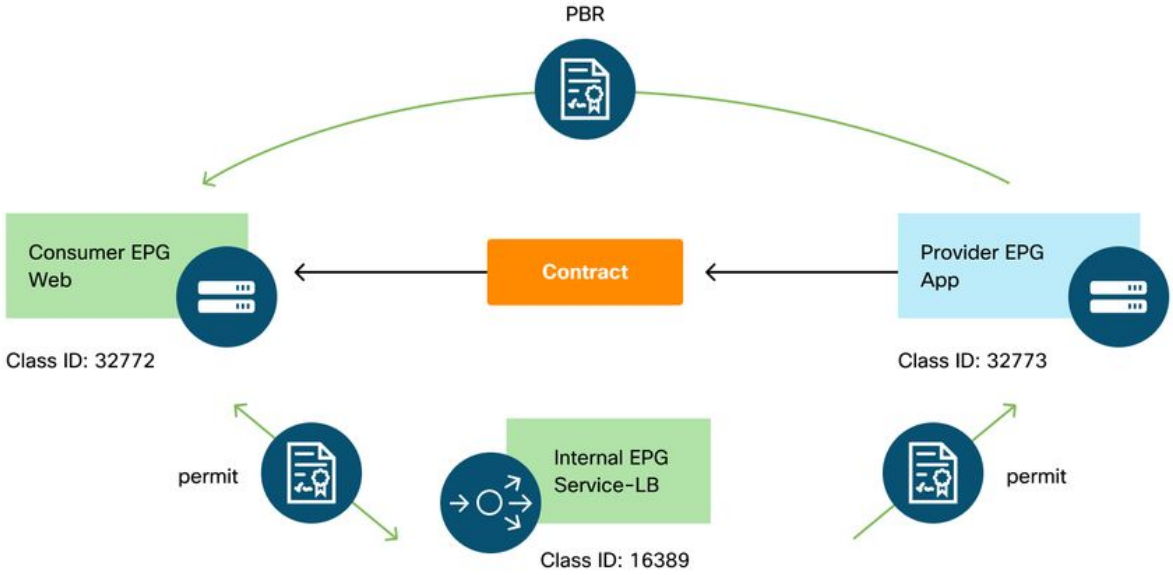
SNAT転送パスを使用しないロードバランサの例：PBRを使用したコンシューマへのプロバイダー



リーフノードにプログラムされたポリシー。

次の図と「show zoning-rule」の出力は、サービスグラフ導入後のゾーン分割ルールを示しています。この例では、pcTag 32772(Web)からpcTag 16389(Service-LB)へのトラフィックは許可され、pcTag 16389(Service-LB)からpcTag 32773(App)へのトラフィックは許可され、pcTag 32773(App)からpcTag 32772(Web)へのトラフィックは「destgrp-31」（ロードバランサ）にリダイレクトされます。

サービスグラフ導入後のゾーニングルール：SNATを使用しないロードバランサ



Source	Destination	Action
32772	16389	permit
16389	32773	permit
32773	32772	PBR to the service node
16389	32772	permit

<#root>

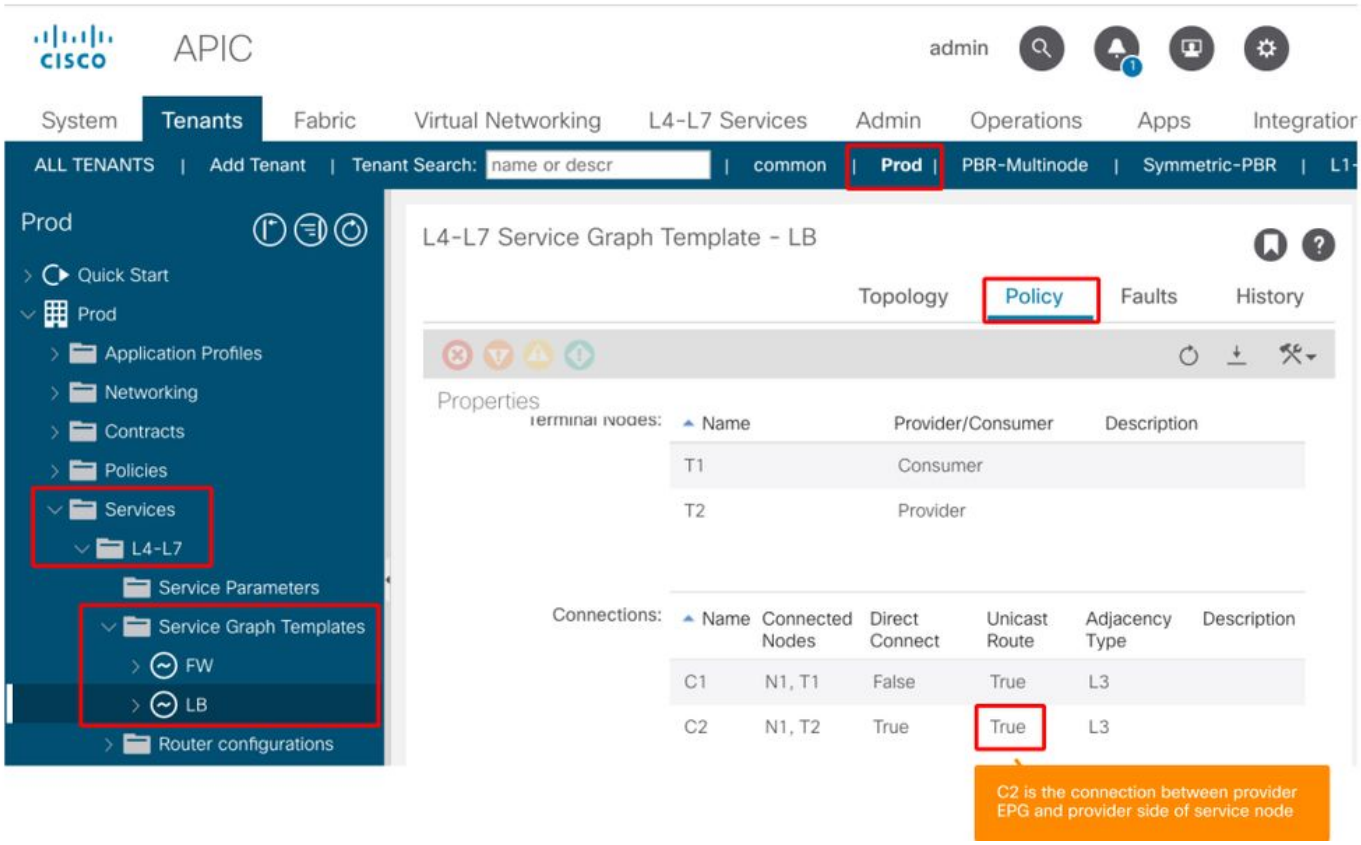
Pod1-Leaf1#

show zoning-rule scope 2752513

```
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+----------------+---------+---------+------+--------------------
|   4248  | 16389  | 32773  | default  |    uni-dir     | enabled | 2752513 |      |       permit
|   4143  | 32773  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      | redir(destgrp-31)
|   4234  | 16389  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      |       permit
|   4133  | 32772  | 16389  |    8     |     bi-dir     | enabled | 2752513 |      |       permit
...
```

デフォルトでは、プロバイダーEPG(pcTag 32773)からService-LB(pcTag 16389)への許可ルールはプログラムされていません。ロードバランサからプロバイダーエンドポイントへのヘルスチェックのために、これらの間の双方向通信を許可するには、接続のDirect Connectオプションを Trueに設定する必要があります。場所は、「Tenant > L4-L7 > Service Graph Templates > Policy」です。デフォルト値はFalseです。

直接接続オプションの設定



次のように、プロバイダーEPG(32773)の許可ルールをService-LB(16389)に追加します。

<#root>

Pod1-Leaf1#

show zoning-rule scope 2752513

```
+---------+--------+--------+----------+----------------+---------+---------+------+----------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+----------------+---------+---------+------+----------------------
|   4248  | 16389  | 32773  | default  |     bi-dir     | enabled | 2752513 |      |       permit
|   4143  | 32773  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      | redir(destgrp-31)
|   4234  | 16389  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      |       permit
|   4133  | 32772  | 16389  |    8     |     bi-dir     | enabled | 2752513 |      |       permit
|   4214  | 32773  | 16389  | default  | uni-dir-ignore | enabled | 2752513 |      |       permit
+---------+--------+--------+----------+----------------+---------+---------+------+----------------------
```

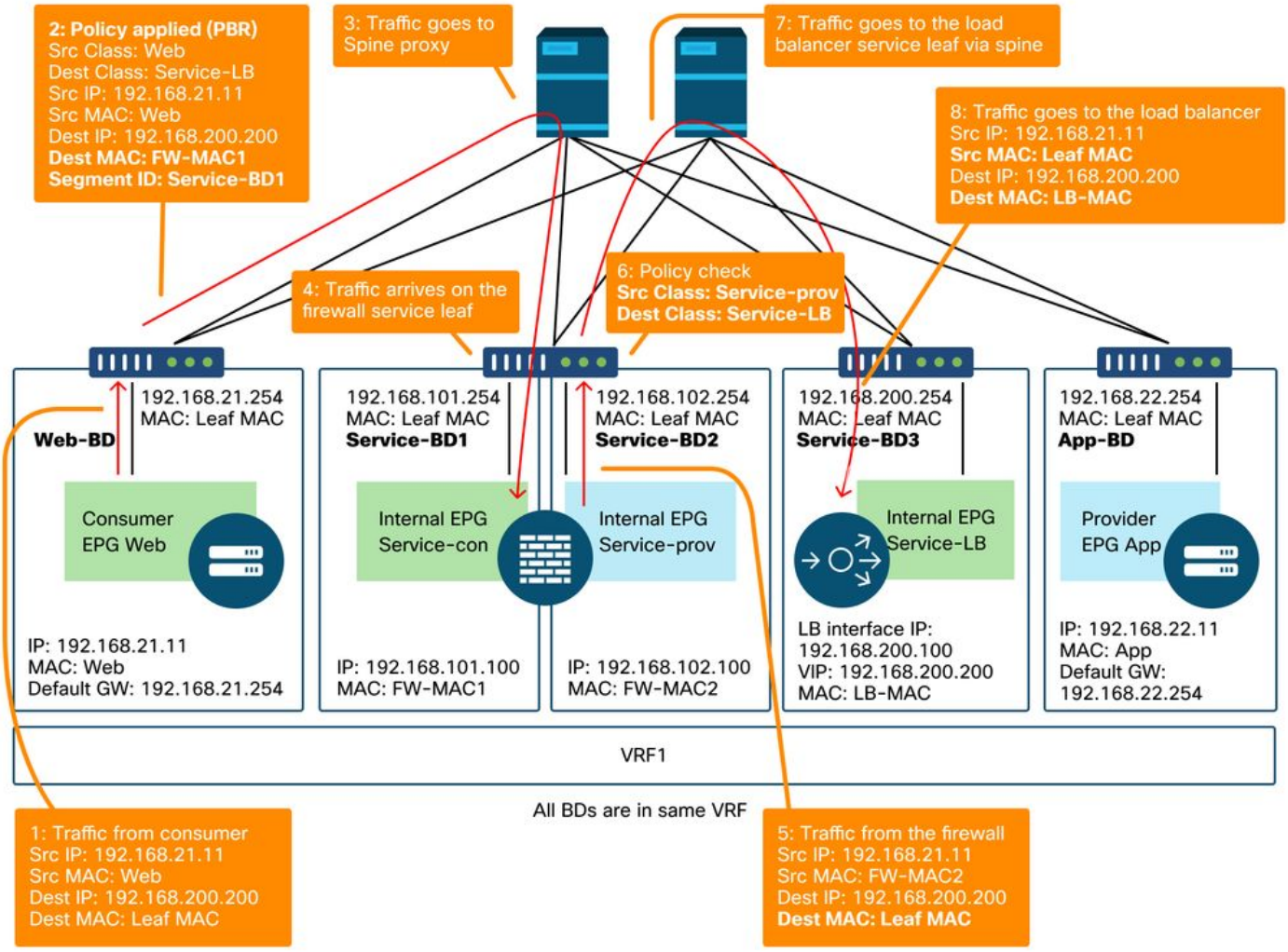
2.トラフィックフローの例：SNATを使用しないファイアウォールとロードバランサ

PBRは、1番目のノードとしてのファイアウォール、2番目のノードとしてのロードバランサなど、複数のサービス機能をサービスグラフに配置できます。

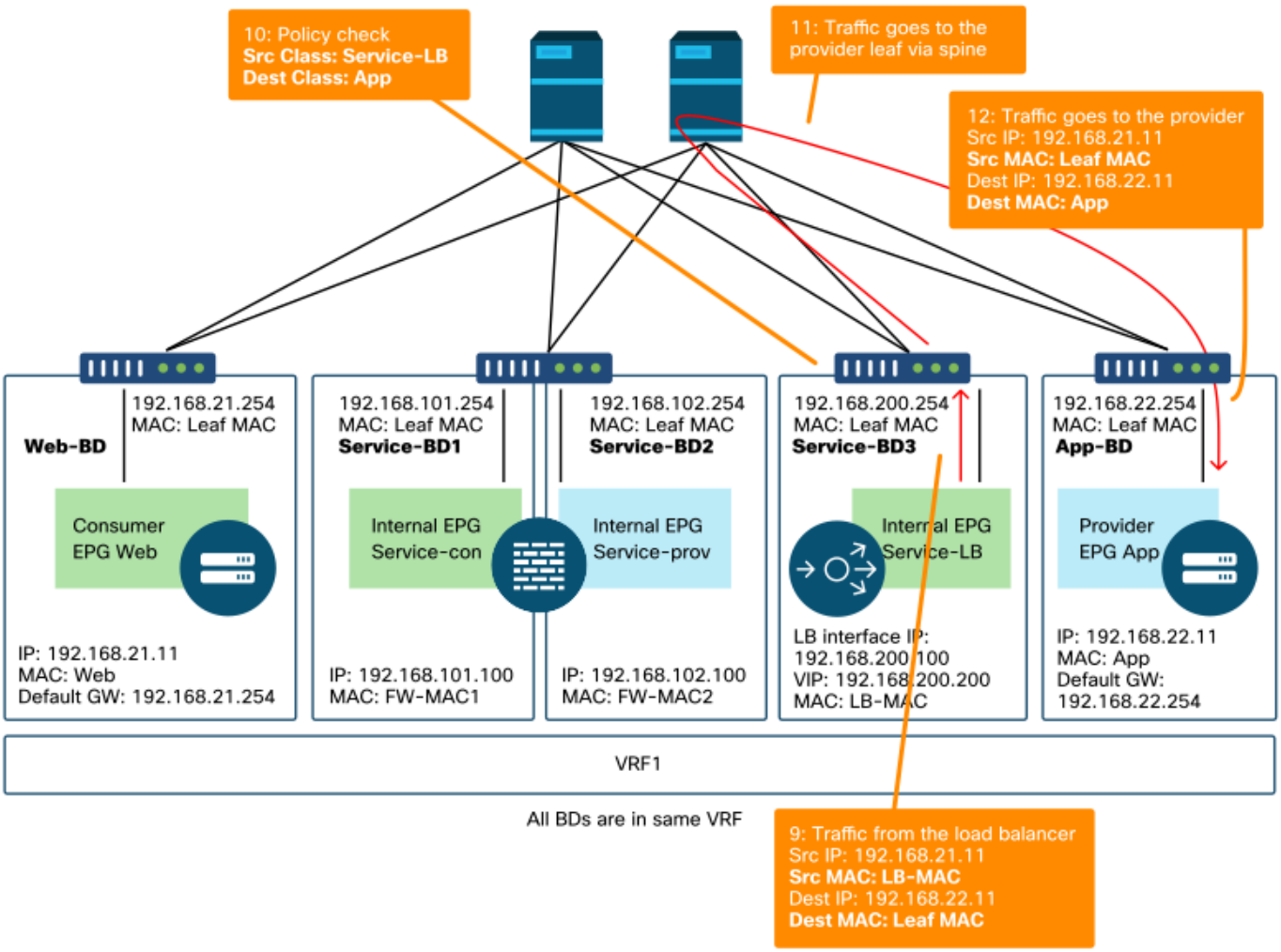
トラフィックパスの例

次の図は、2つの接続を持つコンシューマEPG Webからプロバイダーエンドポイントへの着信トラフィックフローの例を示しています。1つはコンシューマEPG Web内のエンドポイントからファイアウォール経由でロードバランサーVIPに到達するもので、もう1つはロードバランサーからプロバイダーEPGアプリケーション内のエンドポイントに到達するものです。VIP宛ての着信トラフィックはファイアウォールにリダイレクトされ、PBRを使用せずにロードバランサに送られます。ロードバランサは、宛先IPをVIPに関連付けられたApp EPGのいずれかのエンドポイントに変更しますが、送信元IPは変換しません。その後、トラフィックはプロバイダーエンドポイントに送信されます。

SNAT転送パスのないファイアウォールとロードバランサの例：コンシューマからVIP、ロードバランサからプロバイダー



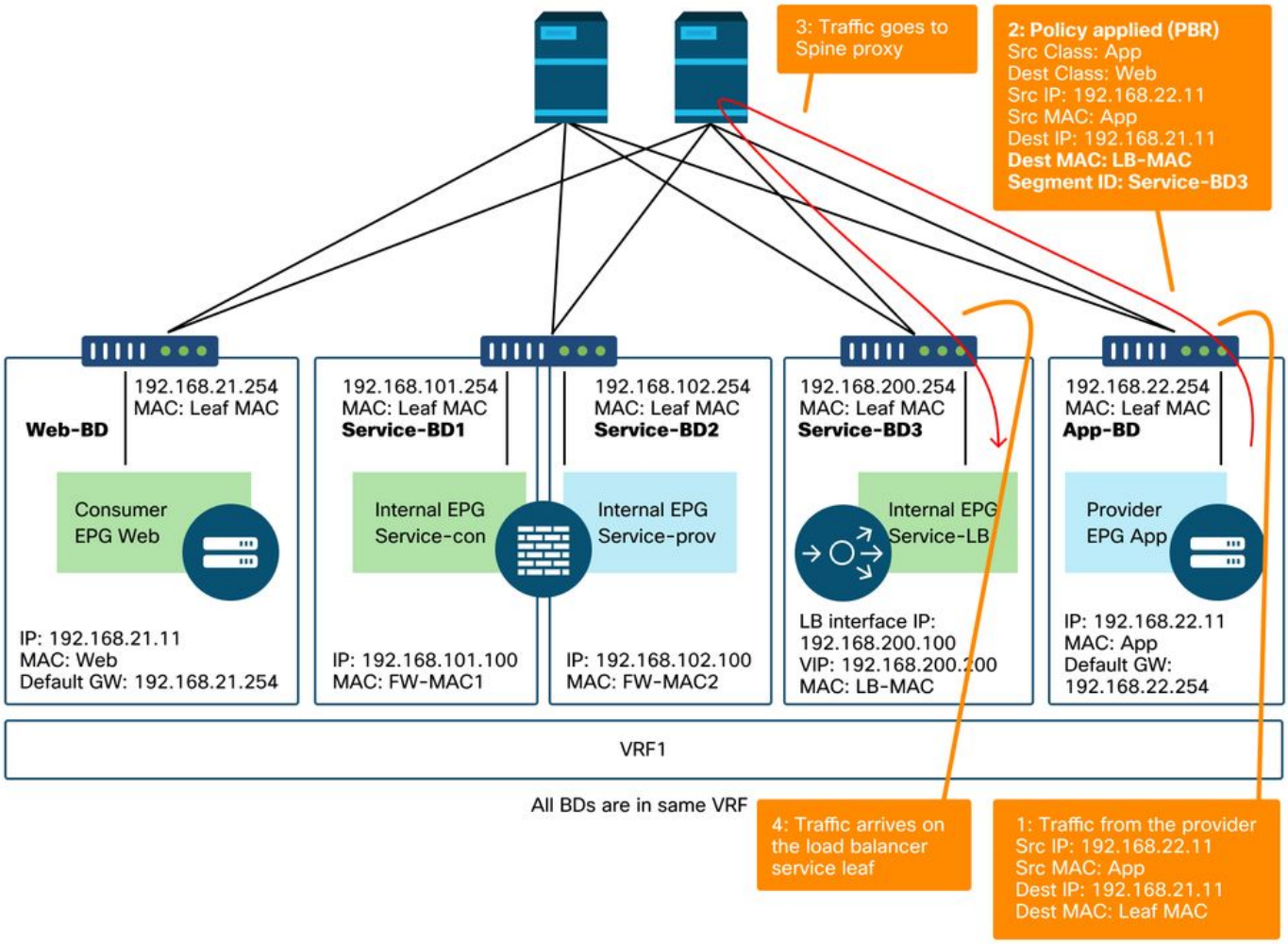
SNAT転送パスのないファイアウォールとロードバランサの例：コンシューマからVIP、ロードバランサからプロバイダー（続き）

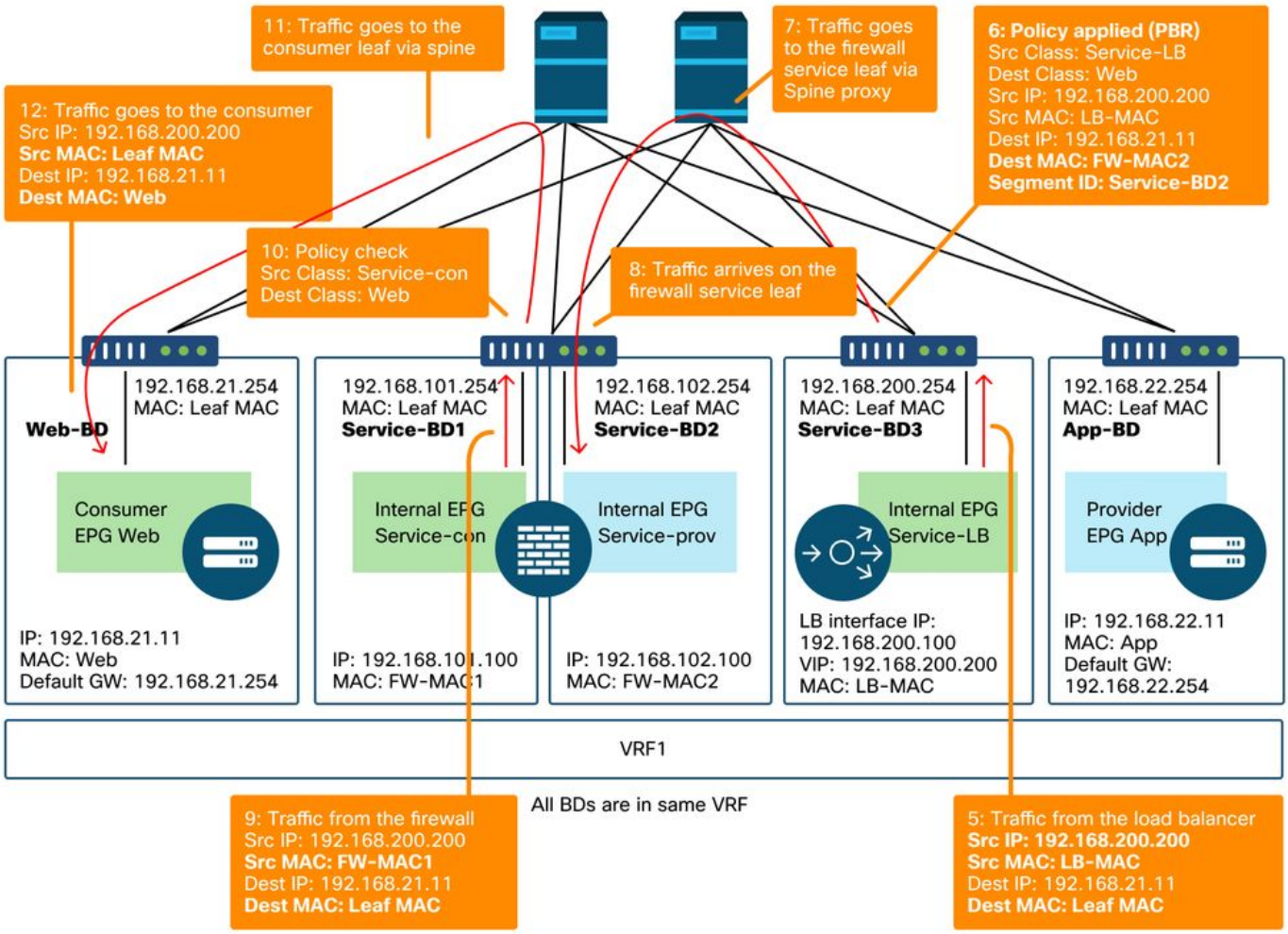


次の図は、プロバイダーEPGアプリケーションからコンシューマEPG Webへのリターントラフィックフローを示しています。リターントラフィックは元の送信元IPを宛先としているため、リターントラフィックをロードバランサに戻すためにPBRが必要になります。

プロバイダーエンドポイントからコンシューマエンドポイントへのトラフィックがロードバランサにリダイレクトされた後、ロードバランサは送信元IPをVIPに変更します。トラフィックはロードバランサから戻り、ファイアウォールにリダイレクトされます。その後、トラフィックはファイアウォールから戻り、コンシューマエンドポイントに戻ります。

SNAT転送パスを使用しないファイアウォールとロードバランサの例：プロバイダーからコンシューマへ

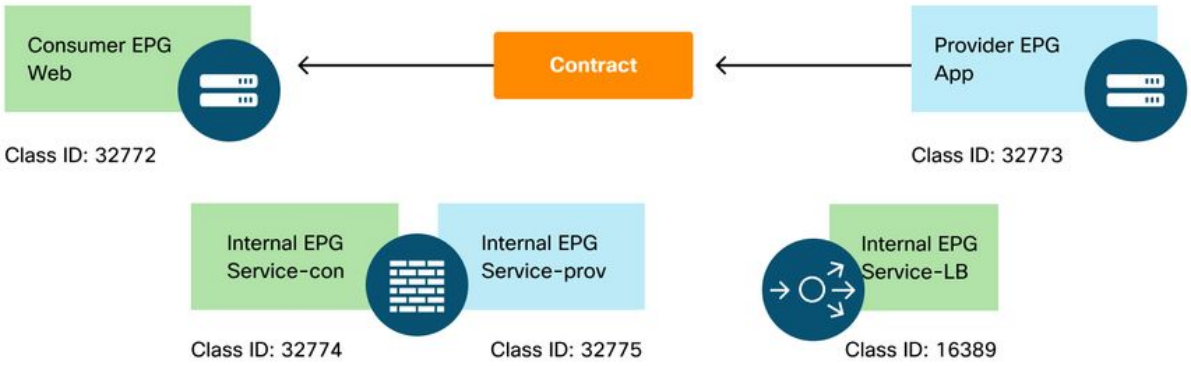

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254
MAC: Leaf MAC
Service-BD1
Internal EPG Service-con
IP: 192.168.101.100
MAC: FW-MAC1
192.168.102.254
MAC: Leaf MAC
Service-BD2
Internal EPG Service-prov
IP: 192.168.102.100
MAC: FW-MAC2
192.168.200.254
MAC: Leaf MAC
Service-BD3
Internal EPG Service-LB
LB interface IP:
192.168.200.100
VIP: 192.168.200.200
MAC: LB-MAC
192.168.22.254
MAC: Leaf MAC
App-BD
Provider EPG App
IP: 192.168.22.11
MAC: App
Default GW:
192.168.22.254
VRF1
All BDs are in same VRF
4: Traffic arrives on the load balancer service leaf
1: Traffic from the provider
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: Leaf MAC



リーフノードにプログラムされたポリシー

次の図と「show zoning-rule」の出力は、サービスグラフ導入後のゾーン分割ルールを示しています。この例では、pcTag 32772(Web)からpcTag 16389(Service-LB)へのトラフィックは「destgrp-32」（ファイアウォールのコンシューマ側）に、pcTag 32773(App)からpcTag 32772(Web)へのトラフィックは「destgrp-33」（ロードバランサ）に、pcTag 16389(Service-LB)からpcTag 32772(Web)へのトラフィックは「destgrp-34」（ファイアウォールのプロバイダー側）にリダイレクトされます。

サービスグラフ導入後のゾーニングルール：SNATを使用しないファイアウォールとロードバランサ



Source	Destination	Action
32772	16389	PBR to the consumer side of the firewall
32775	16389	permit
16389	32773	permit
32773	16389	Permit (Direct Connect must be set to True)
32773	32772	PBR to the the load balancer
16389	32772	PBR to the provider side of the firewall
32774	32772	permit

<#root>

Pod1-Leaf1#

show zoning-rule scope 2752513

```
+---------+--------+--------+----------+----------------+---------+---------+------+------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+----------------+---------+---------+------+------------------
|   4236  | 32772  | 16389  |    8     |     bi-dir     | enabled | 2752513 |      | redir(destgrp-32)
|   4143  | 32773  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      | redir(destgrp-33)
|   4171  | 16389  | 32773  | default  |     bi-dir     | enabled | 2752513 |      |       permit
|   4248  | 16389  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      | redir(destgrp-34)
|   4214  | 32774  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |       permit
|   4244  | 32775  | 16389  | default  |    uni-dir     | enabled | 2752513 |      |       permit
|   4153  | 32773  | 16389  | default  | uni-dir-ignore | enabled | 2752513 |      |       permit
+---------+--------+--------+----------+----------------+---------+---------+------+------------------
```

上記の例では、ロードバランサのプロバイダー側とプロバイダーEPG間の接続でDirect Connectオプションが「True」に設定されています。ロードバランサからプロバイダーエンドポイントへのヘルスチェック用に有効にする必要があります。場所は、「Tenant > L4-L7 > Service Graph Templates > Policy」です。図「Set Direct Connect option」を参照してください。

3.シェアードサービス（VRF間契約）

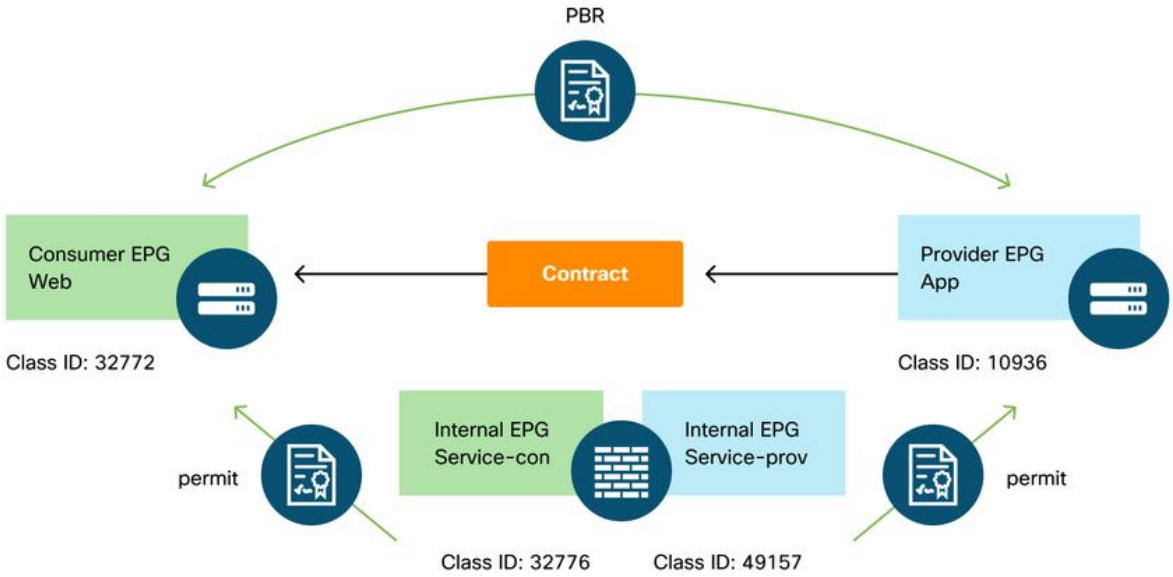
PBRはVRF間契約で有効にできます。このセクションでは、EPGからEPGへのVRF間コントラクトの場合にゾーン分割ルールがどのようにプログラムされるかについて説明します。

リーフノードにプログラムされたポリシー

EPGとEPGのVRF間契約の場合、ポリシーは常にコンシューマVRFに適用されます。したがって、リダイレクトはコンシューマVRFで発生します。その他の組み合わせについては、「転送」の項の表「ポリシーが適用される場所」を参照してください。

次の図と「show zoning-rule」の出力は、サービスグラフ導入後のゾーン分割ルールを示しています。この例では、pcTag 32772(Web)からpcTag 10936(App)へのトラフィックは「destgrp-36」（サービスノードのコンシューマ側）にリダイレクトされ、pcTag 10936(App)からpcTag 32772(Web)へのトラフィックは「destgrp-35」（サービスノードのプロバイダ側）にリダイレクトされます。いずれも、コンシューマVRFであるVRF1に適用されます。pcTag 32776（ファイアウォールのコンシューマ側）からpcTag 32772(Web)へのトラフィックは、VRF1で許可されます。

サービスグラフ導入後のゾーニングルール：VRF間コントラクト



VRF1 (scope: 2752513)

VRF1 zoning-rules

Source	Destination	Action
32772	10936	PBR to the consumer side of the service node
10936	32772	PBR to the provider side of the service node
32776	32772	permit

VRF2 (scope: 2555904)

VRF2 zoning-rule

Source	Destination	Action
49157	10936	permit

```
Pod1-Leaf1# show zoning-rule scope 2752513
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |       Action
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------
|   4191  | 32776  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |       permit
|   4143  | 10936  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      | redir(destgrp-35)
|   4136  | 32772  | 10936  |    8     |     bi-dir     | enabled | 2752513 |      | redir(destgrp-36)
+---------+--------+--------+----------+----------------+---------+---------+------+-------------------
```

pcTag 49157（ファイアウォールのプロバイダー側）からpcTag 10936(App)へのトラフィックは、両方ともVRF2にあるため、VRF2で許可されます。

<#root>

Pod1-Leaf1#

show zoning-rule scope 2555904

```
+---------+--------+--------+----------+---------+---------+---------+------+----------+----------------
| Rule ID | SrcEPG | DstEPG | FilterID |   Dir   |  operSt |  Scope  | Name |  Action  |       Priority
+---------+--------+--------+----------+---------+---------+---------+------+----------+----------------
|   4249  | 49157  | 10936  | default  | uni-dir | enabled | 2555904 |      |  permit  |    src_dst_any
+---------+--------+--------+----------+---------+---------+---------+------+----------+----------------
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。