排除ACI基於策略的重定向故障

目錄

簡介
背景資訊
基於策略的重定向概述
服務圖部署故障排除
1.檢查配置步驟和故障
2.檢查UI中的Service Graph部署
PBR轉發故障排除
1.檢查是否已在枝葉節點上部署了VLAN並學習了終端
2.檢查預期的流量路徑
在哪裡執行策略？
3.檢查流量是否重定向到服務節點
4.檢查在枝葉節點上程式設計的策略
其他流量示例
1.無SNAT的負載均衡器
流量路徑示例
在枝葉節點上程式設計的策略。
2.流量示例 — 不帶SNAT的防火牆和負載均衡器
流量路徑示例
在枝葉節點上程式設計的策略
3.共用服務（VRF間合約）
在枝葉節點上程式設計的策略

簡介

本檔案介紹瞭解ACI原則型重新導向(PBR)案例並對其進行疑難排解的步驟。

背景資訊

本文檔中的資料摘自Troubleshooting Cisco Application Centric Infrastructure， Second Edition書，特別是**Policy-Based Redirect - Overview、Policy-Based Redirect - Service Graph Deployment、Policy-Based Redirect - ForwardingandPolicy-Based Redirect - Other traffic flow examples** 章。

基於策略的重定向概述

本章介紹使用基於策略的重定向(PBR)對非託管模式服務圖進行故障排除的過程。

以下是典型的故障排除步驟。本章說明如何驗證特定於PBR的步驟2和步驟3。有關步驟1和4，請參閱章節：「交換矩陣內轉發」、「外部轉發」和「安全策略」。

1. 檢查沒有PBR服務圖的流量工作情況： 消費者端點和提供商端點被學習。消費者和提供商端點可以通訊。
2. 已部署檢查服務圖： 部署的圖形例項沒有錯誤。部署服務節點的VLAN和類ID。服務節點端點獲知。
3. 檢查轉發路徑： 已在枝葉節點上程式設計檢查策略。捕獲服務節點上的流量以確認是否重定向流量。捕獲ACI枝葉上的流量，以確認流量在PBR之後是否返回到ACI交換矩陣。
4. 檢查流量是否到達消費者和提供商端點，以及端點是否生成返回流量。

本文檔不包括設計或配置選項。有關詳情，請參閱Cisco.com上的「ACI PBR白皮書」

在本章中，服務節點和服務枝葉包含以下內容：

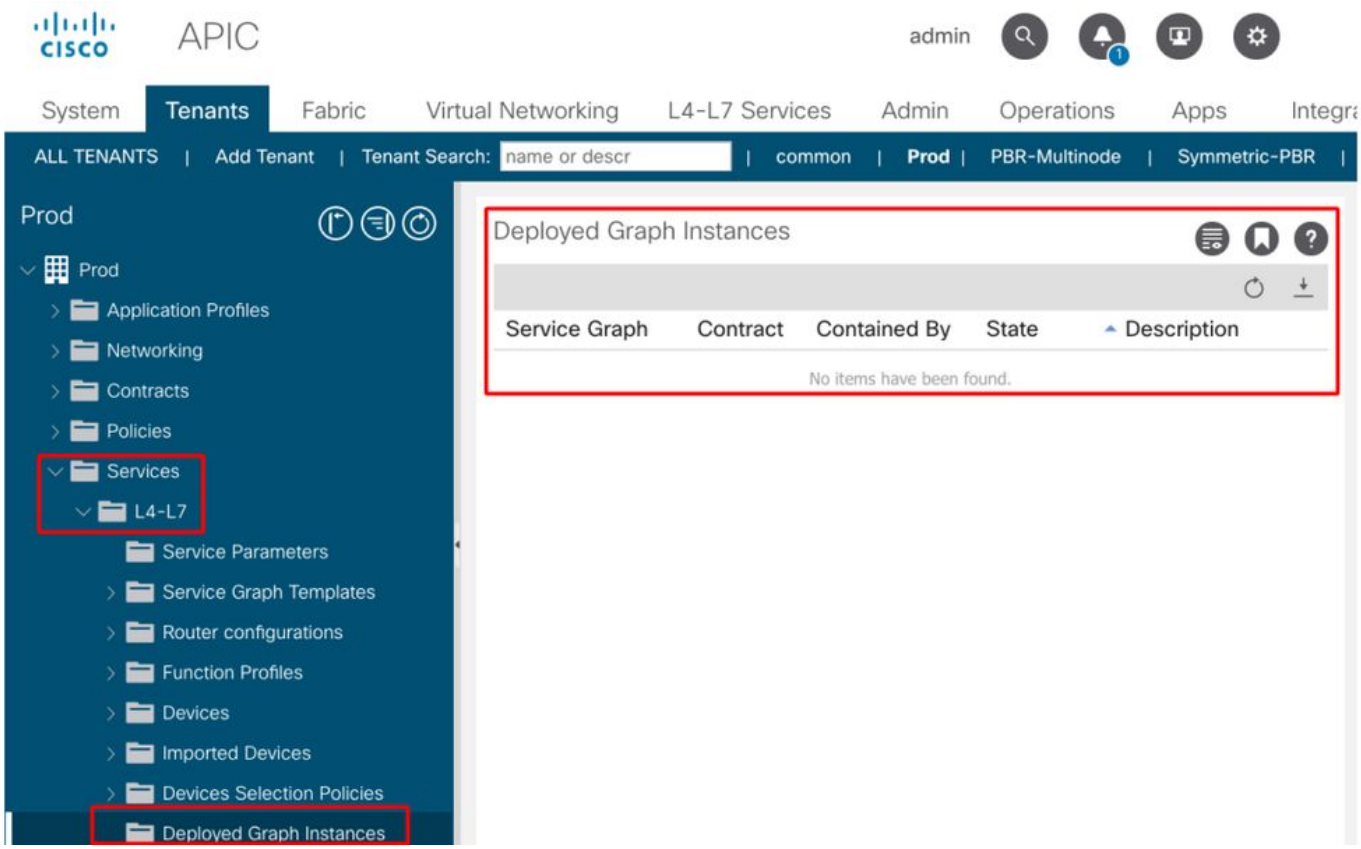
- 服務節點 — PBR將流量重定向到的外部節點，例如防火牆或負載均衡器。
- 服務枝葉 — 連線到服務節點的ACI枝葉。

服務圖部署故障排除

本章介紹未部署服務圖的故障排除示例。

定義服務圖策略並將其應用於合約主題後，ACI GUI上應顯示一個已部署的圖例項。下圖顯示了服務圖未顯示為部署的故障排除場景。

服務圖未顯示為已部署的圖例項。



1.檢查配置步驟和故障

故障排除的第一步是檢查是否配置了必要的元件，沒有出現故障。假設以下常規配置已經完成：

- 適用於消費者EPG、提供商EPG和服務節點的VRF和BD
- 消費者和提供商EPG。
- 合約和篩選條件。

值得一提的是，不需要手動為服務節點建立EPG。將通過服務圖部署建立。

帶PBR的Service Graph配置步驟如下：

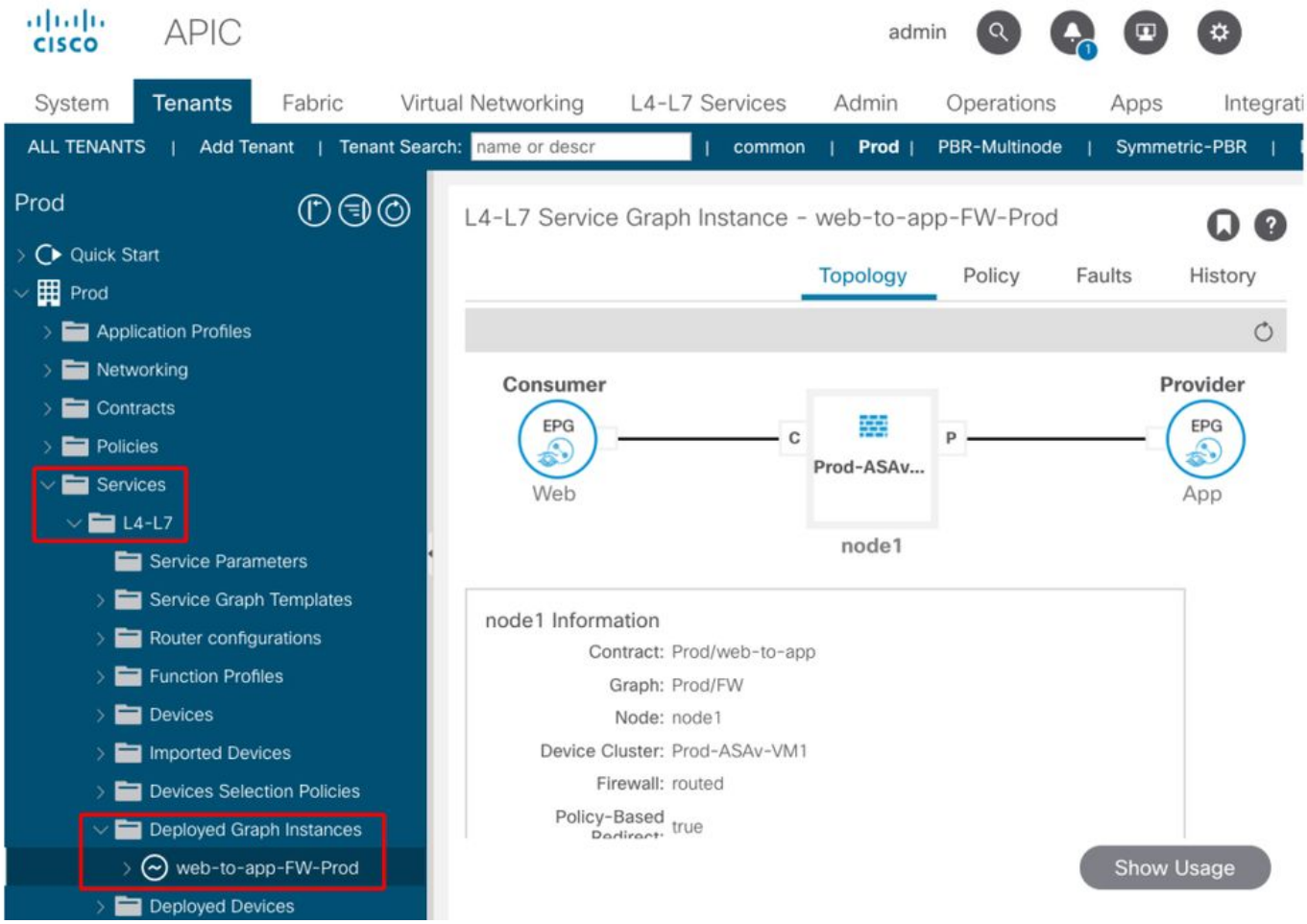
- 建立L4-L7裝置（邏輯裝置）。
- 建立服務圖。
- 建立PBR策略。
- 建立裝置選擇策略。
- 將服務圖與合約主題相關聯。

2.檢查UI中的Service Graph部署

將服務圖與合約主題關聯後，應為具有服務圖的每個合約顯示一個已部署的圖例項（如下圖）。

位置為「Tenant > Services > L4-L7 > Deployed Graph Instances」

部署的圖形例項



如果未顯示部署的圖形例項，則合約配置存在問題。主要原因可能是：

- 合約沒有消費者或提供商EPG。
- 合約主題沒有任何篩選器。

- 合約範圍是VRF，即使它用於VRF間或租戶間EPG通訊。

如果Service Graph例項化失敗，則在Deployed Graph Instance中引發故障，這意味著服務圖配置存在錯誤。由配置引起的典型故障如下：

F1690:由於ID分配失敗，配置無效

此故障表示服務節點的封裝VLAN不可用。例如，與邏輯裝置中使用的VMM域關聯的VLAN池中沒有可用的動態VLAN。

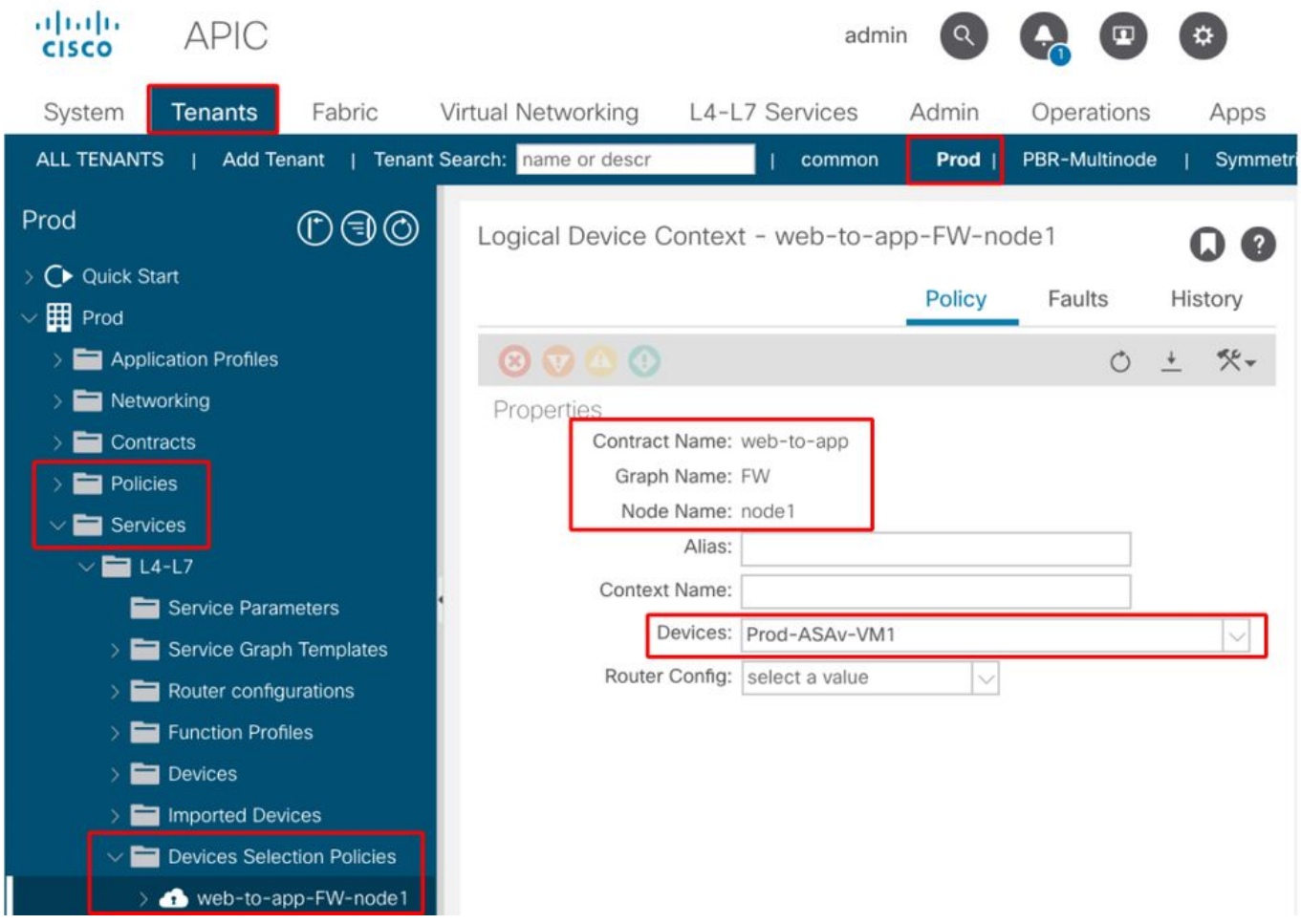
解析度：檢查用於邏輯裝置的域中的VLAN池。檢查邏輯裝置介面中的封裝的VLAN（如果它在物理域中）。位置為「Tenant > Services > L4-L7 > Devices and Fabric > Access Policies > Pools > VLAN」。

F1690:配置無效，因為找不到LDev的裝置上下文

此故障表示找不到服務圖形呈現的邏輯裝置。例如，沒有與服務圖合約匹配的裝置選擇策略。

解析度：檢查裝置選擇策略是否已定義。裝置選擇策略為服務裝置及其聯結器提供了選擇標準。條件基於服務圖中的合約名稱、服務圖名稱和節點名稱。位置為「Tenant > Services > L4-L7 > Device Selection Policy」。

檢查裝置選擇策略



F1690:配置無效，因為找不到群集介面

此故障表示找不到服務節點的群集介面。例如，未在裝置選擇策略中指定群集介面。

解析度：檢查群集介面是否在「裝置選擇」策略中指定，以及聯結器名稱是否正確（如下圖）。

F1690:配置無效，因為找不到BD

此故障表示找不到服務節點的BD。例如，未在裝置選擇策略中指定BD。

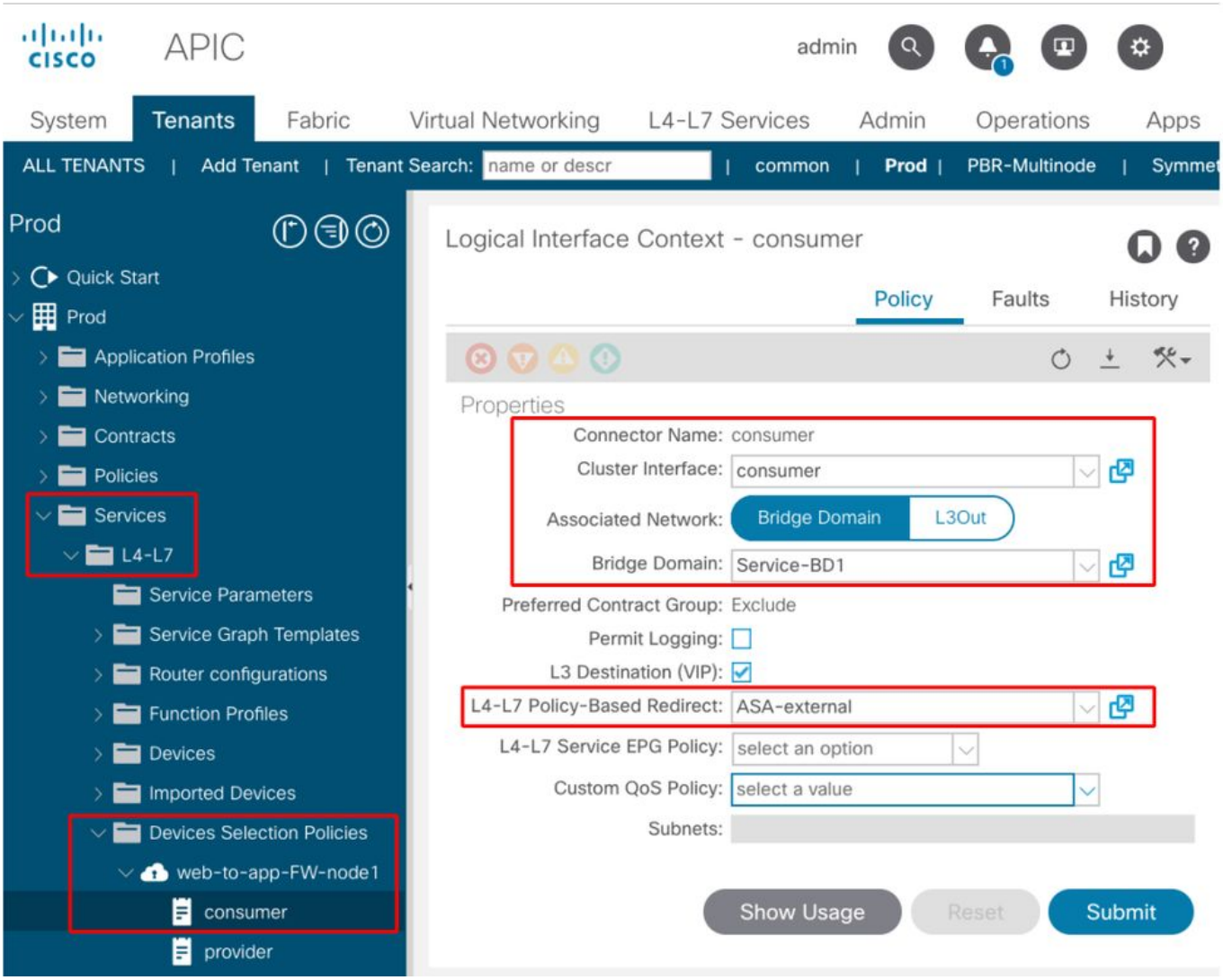
解析度：檢查「Device Selection」策略中是否指定BD，以及聯結器名稱是否正確（如下圖）。

F1690:由於服務重定向策略無效，配置無效

此故障表示未選擇PBR策略，即使已在服務圖中的服務功能上啟用重定向。

解析度：在「Device Selection Policy（裝置選擇策略）」中選擇PBR策略（下圖）。

裝置選擇策略中的邏輯介面配置



PBR轉發故障排除

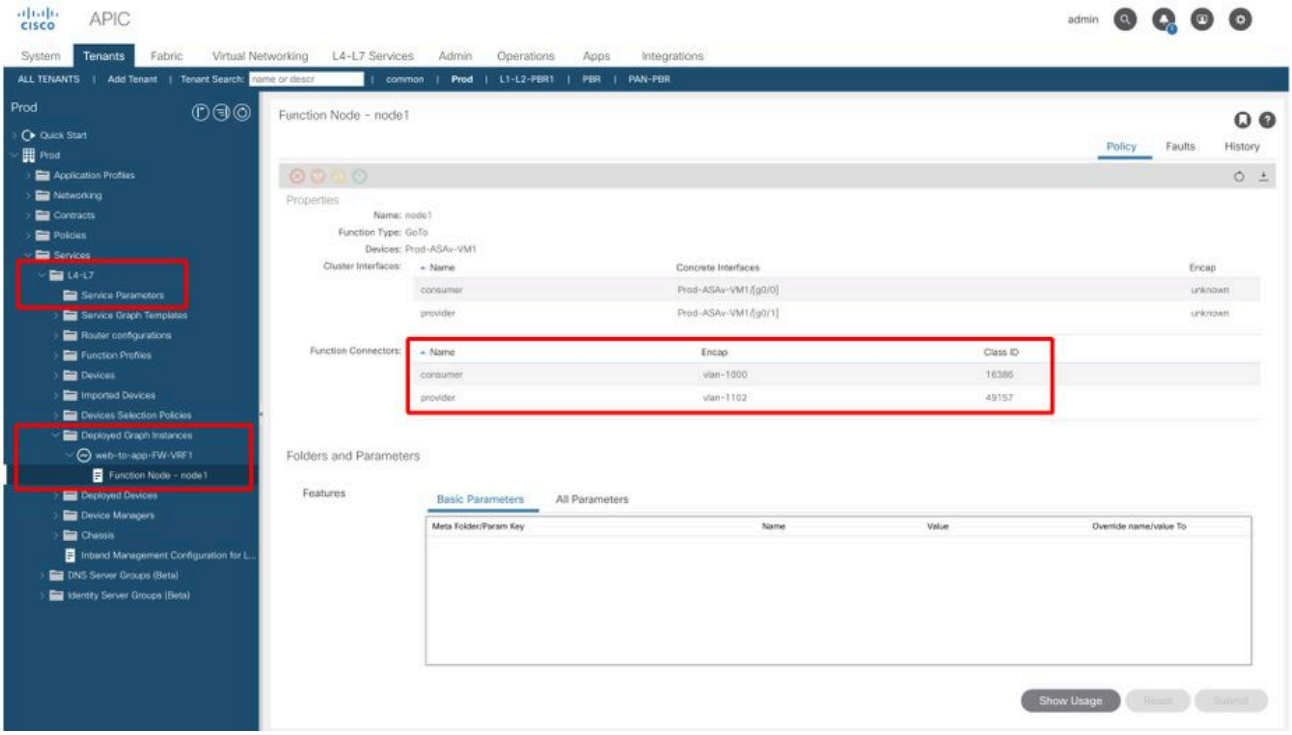
本章介紹PBR轉發路徑的故障排除步驟。

1.檢查是否已在枝葉節點上部署了VLAN並學習了終端

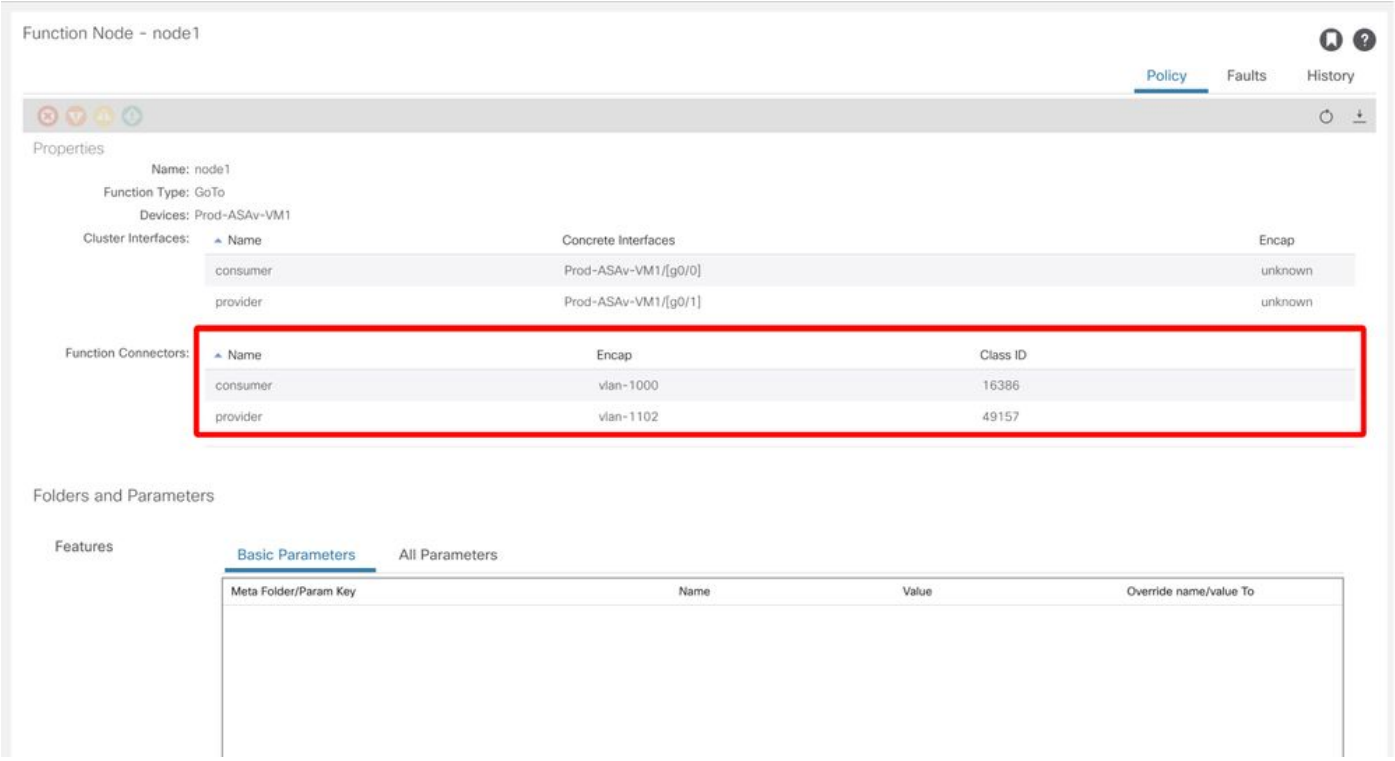
成功部署服務圖而不出現任何故障後，即可為服務節點建立EPG和BD。下圖顯示了在何處查詢服務節點介面（服務EPG）的封裝VLAN ID和類ID。 在本例中，防火牆的使用者端是具有VLAN封裝1000的類ID 16386，而防火牆的提供者端是具有VLAN封裝1102的類ID 49157。

位置為「Tenant > Services > L4-L7 > Deployed Graph instances > Function Nodes」。

服務節點



服務節點介面類ID



這些VLAN部署在連線服務節點的服務枝葉節點介面上。在服務枝葉節點CLI上使用「show vlan extended」和「show endpoint」可以檢查VLAN部署和終端學習狀態。

```
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
```

如果服務節點的終端IP未獲知為ACI交換矩陣中的終端，則很可能是因為服務枝葉和服務節點之間的連線或配置問題。請檢查以下狀態：

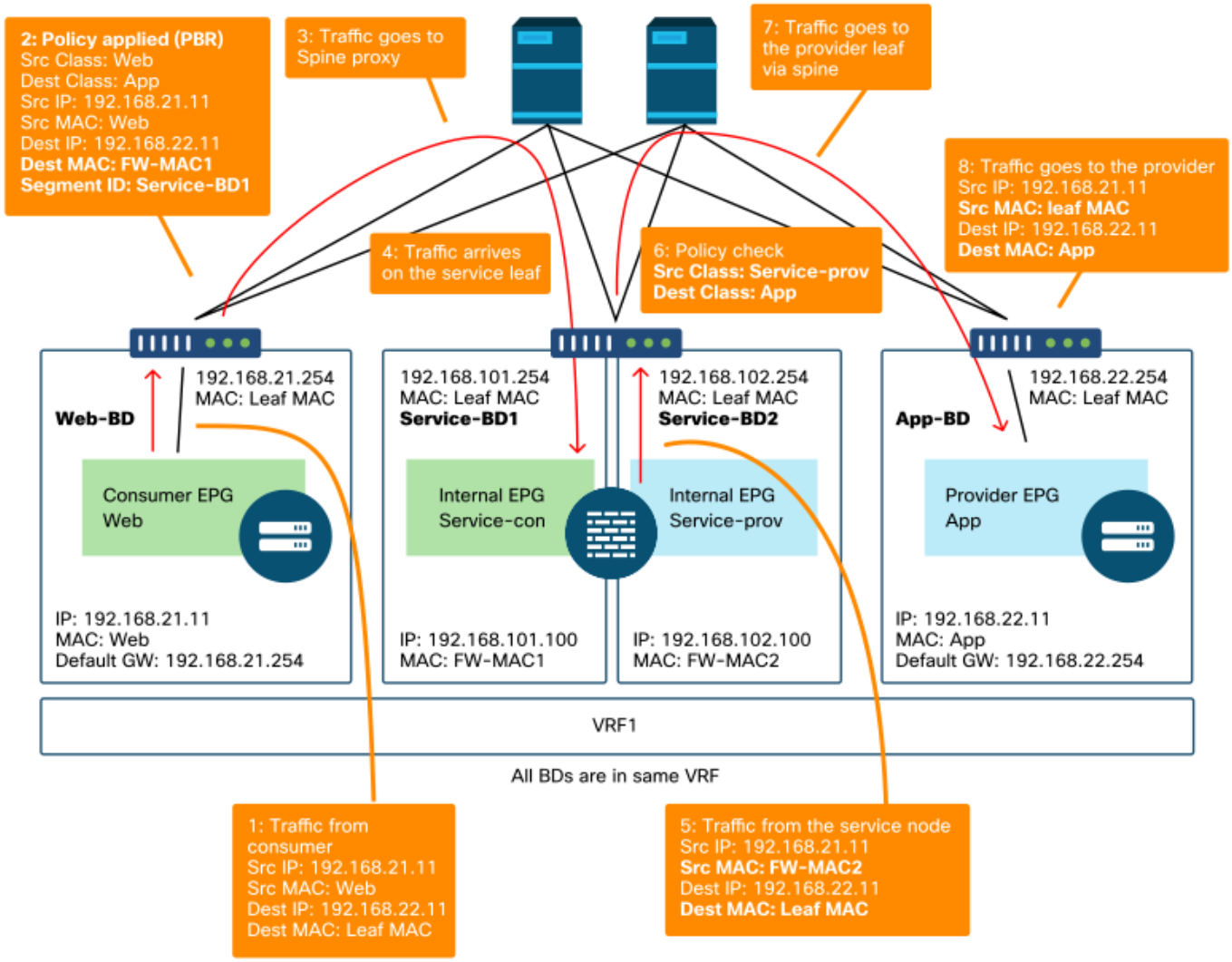
- 服務節點連線到正確的枝葉下行鏈路埠。 如果服務節點在物理域中，則需要在邏輯裝置中定義枝葉靜態路徑終端封裝VLAN。如果服務節點在VMM域中，請檢查VMM域是否工作並且通過服務圖建立的埠組已正確連線到服務節點VM。
- 連線到服務節點或服務節點VM所在的虛擬機器監控程式的枝葉下行鏈路埠為UP。
- 服務節點具有正確的VLAN和IP地址。
- 服務枝葉和服務節點之間的中間交換機具有正確的VLAN配置。

2.檢查預期的流量路徑

啟用PBR後，如果端到端流量停止工作，即使在ACI交換矩陣中學習服務節點終端，下一個故障排除步驟是檢查預期流量路徑。

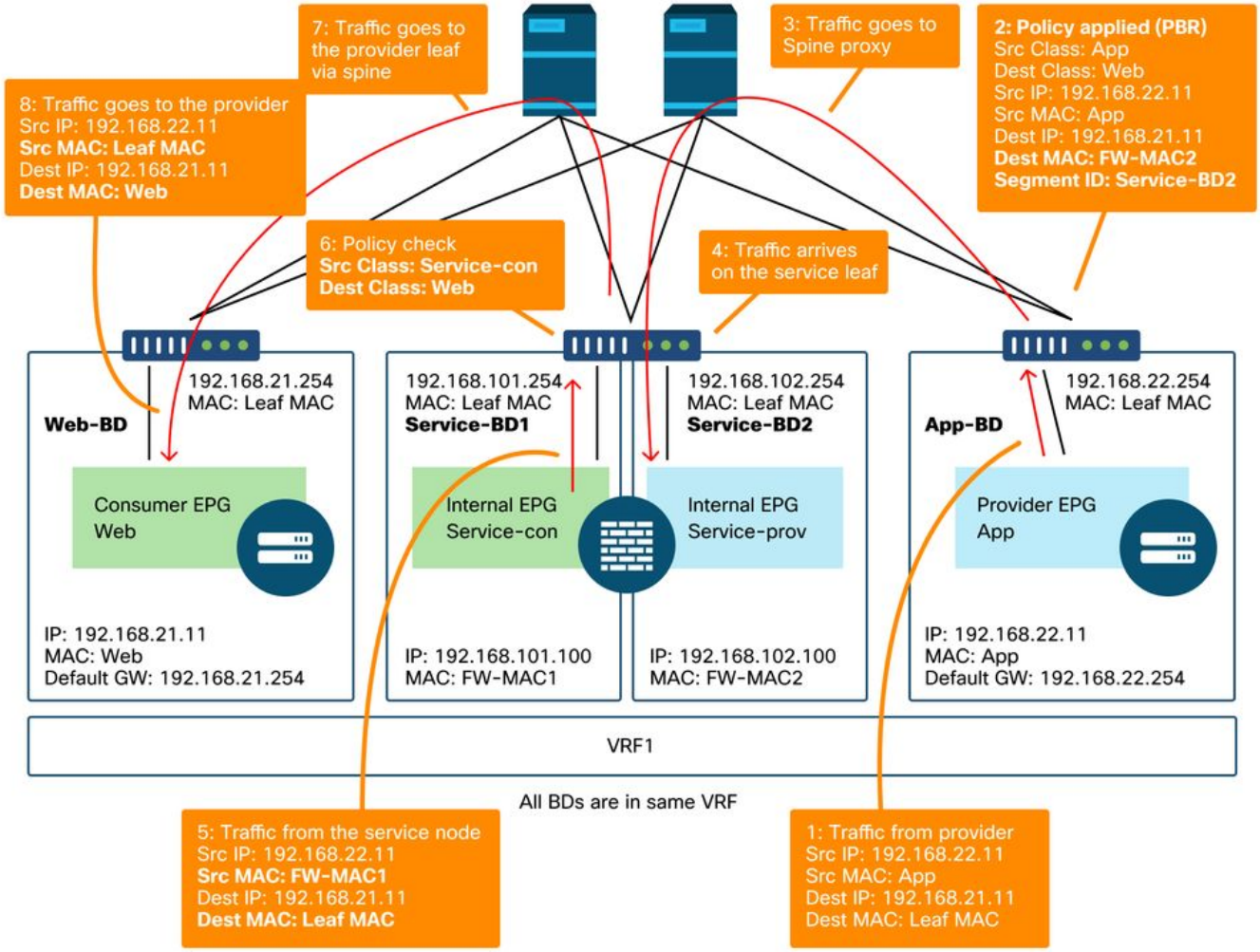
圖「PBR轉發路徑示例 — 使用者到提供程式」和「PBR轉發路徑示例 — 提供程式到使用者」說明了在使用者端點和提供程式端點之間使用PBR插入防火牆的轉發路徑示例。假設端點已在枝葉節點上獲取。

PBR轉發路徑示例 — 消費者到提供商



附註：由於源MAC未更改為ACI枝葉MAC，因此，如果使用者終端和PBR節點不在同一個BD中，則PBR節點不得使用基於源MAC的轉發

PBR轉發路徑示例 — 提供商到消費者



附註：值得一提的是，PBR策略在使用者或提供商枝葉上實施，ACI PBR的作用是目標MAC重寫，如圖「PBR轉發路徑示例 — 使用者到提供商」和「PBR轉發路徑示例 — 提供商到消費者」所示。 即使源終端和PBR目標MAC位於同一枝葉下，到達PBR目標MAC始終使用主幹代理。

雖然圖「PBR轉發路徑示例 — 使用者到提供程式」和「PBR轉發路徑示例 — 提供者到使用者」顯示了一個將重定向流量的示例，其中策略的實施取決於合約配置和端點學習狀態。表「策略實施位置」彙總了單個ACI站點策略實施位置。在多站點中實施策略的位置不同。

在哪裡執行策略？

案例	VRF實施模式	消費者	提供商	策略實施於
VRF內	輸入/輸出	EPG	EPG	·如果獲知目標端點：入口枝葉* ·如果未獲知目標終結點：出口分葉
	輸入	EPG	L3Out EPG	消費者枝葉（非邊界枝葉）
	輸入	L3Out EPG	EPG	提供程式分葉（非邊界分葉）
	輸出	EPG	L3Out EPG	邊界枝葉 — >非邊界枝葉流量 ·如果獲知目標端點：邊界枝葉 ·如果未獲知目標終結點：非邊界枝葉
	輸出	L3Out EPG	EPG	非邊界枝葉 — >邊界枝葉流量 ·邊界枝葉
	輸入/輸出	L3Out	L3Out	入口枝葉*

		EPG EPG	EPG EPG	
	輸入/輸出	EPG	EPG	消費者枝葉
	輸入/輸出	EPG	L3Out EPG	消費者枝葉（非邊界枝葉）
VRF間	輸入/輸出	L3Out EPG	EPG	入口枝葉*
	輸入/輸出	L3Out EPG	L3Out EPG	入口枝葉*

*策略實施應用於資料包所命中的第一個枝葉。

以下是範例：

- 如果VRF1中L3Out EPG中的外部終端嘗試訪問VRF1中Web EPG中的終端且VRF1配置為入口強制模式，則無論合約方向如何，流量都會被網路EPG中終端所在的枝葉重新導向。
- 如果VRF1中的使用者Web EPG中的終端嘗試存取VRF1中的提供者應用EPG中的終端，且終端在使用者節點和提供者枝葉節點上得知，則流量會由輸入枝葉重定向。
- 如果VRF1中的使用者Web EPG中的終端嘗試存取VRF2中的提供者App EPG中的終端，則無論採用VRF實施模式，流量都會由使用者終端所在的使用者枝葉重新導向。

3.檢查流量是否重定向到服務節點

清除預期的轉發路徑後，ELAM可用於檢查流量是否到達交換機節點，並檢查交換機節點上的轉發決策。有關如何使用ELAM的說明，請參閱「交換矩陣內轉發」一章中的「工具」一節。

例如，要跟蹤圖「PBR轉發路徑示例 — 消費者到提供商」中的流量，可以捕獲這些流量以確認是否重定向了消費者到提供商的流量。

- 消費者枝葉上的下行鏈路埠檢查1和2（流量到達消費者枝葉並強制執行PBR）。
- 要檢查的脊柱節點上的交換矩陣埠3（流量流向脊柱代理）。
- 服務枝葉上的交換矩陣埠檢查4（流量到達服務枝葉）。

然後，可以捕獲這些流量以確認從服務節點返回的流量是否流向提供商。

- 服務枝葉上的下行鏈路埠檢查5和6（流量從服務節點返回並允許）。
- 要檢查的脊柱節點上的交換矩陣埠7（流量通過脊柱流向提供商枝葉）。
- 提供商枝葉上的交換矩陣埠檢查8（流量到達服務枝葉並到達提供商端點）。

附註：如果消費者和服務節點位於同一枝葉下，則除了源/目標IP之外，請指定一個介面或源MAC以使ELAM在圖「PBR轉發路徑示例 — 消費者到提供商」中檢查1或5，特別是因為兩者使用相同的源IP和目標IP。

如果消費者到提供商的流量被重定向到服務節點但並未返回服務分葉，請檢查以下情況，因為它們是常見錯誤：

- 服務節點路由表到達提供商子網。
- 服務節點安全策略（例如ACL）允許流量。

如果流量被重定向並到達提供商，請以類似方式檢查提供商到消費者的返回流量路徑。

4.檢查在枝葉節點上程式設計的策略

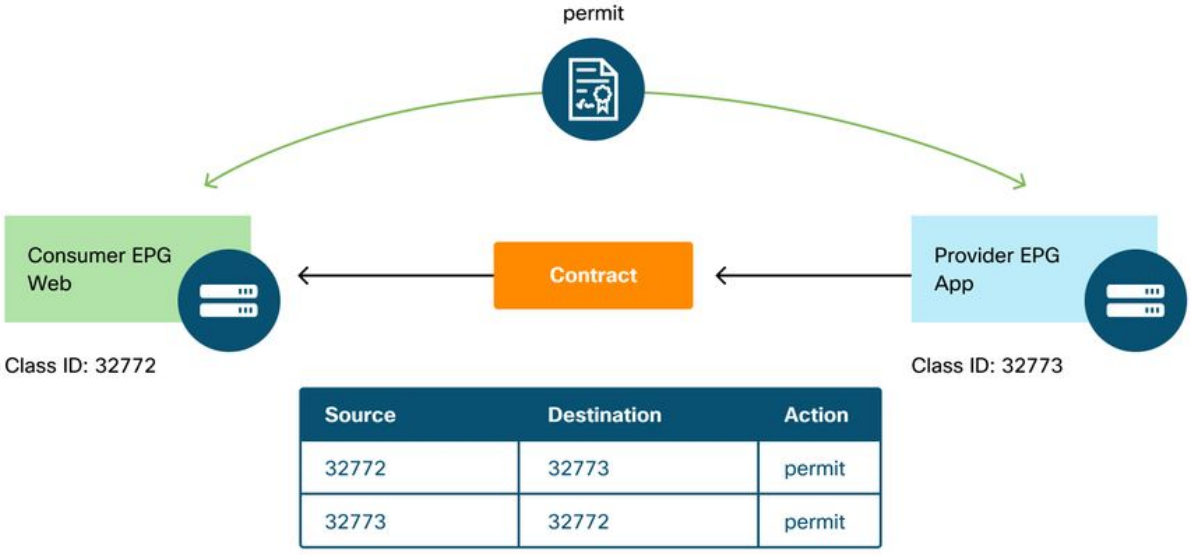
如果沒有相應地轉發或重定向流量，下一個故障排除步驟是檢查在枝葉節點上程式設計的策略。本

部分以示例形式顯示zoning-rule和contract_parser。有關如何檢查分割槽規則的詳細資訊，請參考「安全策略」一章中的「工具」一節。

附註：基於枝葉上的EPG部署狀態來程式設計策略。本節中的show命令輸出使用具有服務節點的使用者EPG、提供程式EPG和EPG的枝葉。

使用「show zoning-rule」命令

下圖和「show zoning-rule」輸出描述了服務圖部署之前的分割槽規則。



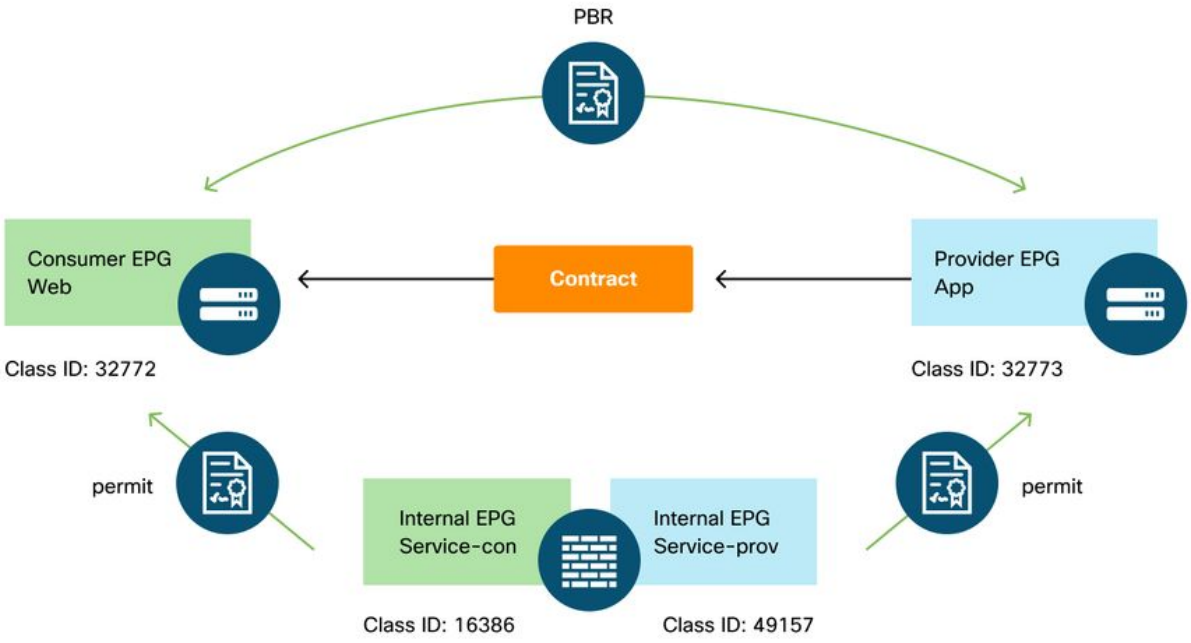
Source	Destination	Action
32772	32773	permit
32773	32772	permit

VRF作用域ID可在「Tenant > Networking > VRF」中找到。

```
Pod1-Leaf1# show zoning-rule scope 2752513
+---------+--------+--------+----------+----------------+---------+---------+------------+------
----+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  |    Name    |
Action  |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------------+------
----+----------------------+
|   4237  | 32772  | 32773  |    8     |     bi-dir     | enabled | 2752513 | web-to-app |
permit  |    fully_qual(7)     |
|   4172  | 32773  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 | web-to-app |
permit  |    fully_qual(7)     |
+---------+--------+--------+----------+----------------+---------+---------+------------+------
----+----------------------+
```

部署服務圖後，將建立服務節點的EPG並更新策略以重定向消費者和提供商EPG之間的流量。下圖和下方的「show zoning-rule」輸出描述了服務圖部署後的分割槽規則。在本示例中，從pcTag 32772(Web)到pcTag 32773(App)的流量重定向到「destgrp-27」（服務節點的消費者端），從pcTag 32773(App)到pcTag 32772(Web)的流量重定向到「destgrp-28」（服務節點的提供商端）。

服務圖部署後的分割槽規則



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

```
Pod1-Leaf1# show zoning-rule scope 2752513
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |
Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
...
|   4213  | 16386  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |
permit      |    fully_qual(7)     |
|   4249  | 49157  | 32773  | default  |    uni-dir     | enabled | 2752513 |      |
permit      |    src_dst_any(9)    |
|   4237  | 32772  | 32773  |    8     |     bi-dir     | enabled | 2752513 |      |
redir(destgrp-27) |    fully_qual(7)     |
|   4172  | 32773  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      |
redir(destgrp-28) |    fully_qual(7)     |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
```

使用「show service redir info」命令可以找到每個目標的目標資訊。

```
Pod1-Leaf1# show service redir info
========================================================================================
LEGEND
TL: Threshold(Low)  |  TH: Threshold(High) |  HP: HashProfile  |  HG: HealthGrp  | BAC: Backup-
Dest |  TRA: Tracking  | RES: Resiliency
========================================================================================
List of Dest Groups
```

```
GrpID Name            destination                                   HG-name           BAC
operSt     operStQual      TL   TH   HP   TRAC RES
===== ====            ===========                                   ==============    ===
=======    ============    ===  ===  ===  ===  ===
28    destgrp-28      dest-[192.168.102.100]-[vxlan-2752513]      Not attached      N
enabled    no-oper-grp     0    0    sym  no   no
27    destgrp-27      dest-[192.168.101.100]-[vxlan-2752513]      Not attached      N
enabled    no-oper-grp     0    0    sym  no   no

List of destinations
Name                                        bdVnid             vMac
vrf         operSt     operStQual      HG-name
====                                        ======             ====
====        =====      =========       =======
dest-[192.168.102.100]-[vxlan-2752513]        vxlan-16023499     00:50:56:AF:1C:44
Prod:VRF1   enabled    no-oper-dest    Not attached
dest-[192.168.101.100]-[vxlan-2752513]        vxlan-16121792     00:50:56:AF:3C:60
Prod:VRF1   enabled    no-oper-dest    Not attached
...
```

如果分割槽規則已相應地程式設計，但流量沒有相應地重定向或轉發，請檢查以下情況，因為它們是常見錯誤：

- 檢查使用ELAM是否按預期解析源或目標類ID。如果不是，請檢查錯誤的類ID以及EPG派生條件，如路徑和封裝VLAN。
- 即使相應地解析源和目標類ID，並應用PBR策略，但流量未到達PBR節點，請在redir操作(「show service redir info」)中檢查目標的IP、MAC和VRF是否正確。

預設情況下，如果啟用PBR，則不會將使用者EPG的允許規則程式設計到服務節點（使用者端），以及將提供者EPG程式設計到服務節點（提供者端）。因此，在預設情況下，使用者或提供商端點不能直接與服務節點通訊。要允許此流量，需要啟用Direct Connect選項。使用情形將在「其他流量示例」部分中**說明**。

contract_parser的使用

contract_parser工具還可幫助驗證策略。C-consumer是服務節點的消費者端，C-provider是服務節點的提供商端。

```
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}] [hit=count]

[7:4213] [vrf:Prod:VRF1] permit ip tcp tn-Prod/G-Prod-ASAv-VM1ctxVRF1/C-consumer(16386) eq 80
tn-Prod/ap-app1/epg-Web(32772)  [contract:uni/tn-Prod/brc-web-to-app] [hit=0]
[7:4237] [vrf:Prod:VRF1] redir ip tcp tn-Prod/ap-app1/epg-Web(32772) tn-Prod/ap-app1/epg-
App(32773) eq 80  [contract:uni/tn-Prod/brc-web-to-app] [hit=0]
                            destgrp-27 vrf:Prod:VRF1 ip:192.168.101.100 mac:00:50:56:AF:3C:60
bd:uni/tn-Prod/BD-Service-BD1
[7:4172] [vrf:Prod:VRF1] redir ip tcp tn-Prod/ap-app1/epg-App(32773) eq 80 tn-Prod/ap-app1/epg-
Web(32772)  [contract:uni/tn-Prod/brc-web-to-app] [hit=0]
                            destgrp-28 vrf:Prod:VRF1 ip:192.168.102.100 mac:00:50:56:AF:1C:44
bd:uni/tn-Prod/BD-Service-BD2
[9:4249] [vrf:Prod:VRF1] permit any tn-Prod/G-Prod-ASAv-VM1ctxVRF1/C-provider(49157) tn-Prod/ap-
app1/epg-App(32773) [contract:uni/tn-Prod/brc-web-to-app] [hit=15]
...
```

其他流量示例

本節將考慮其他常見流量流示例，以確定故障排除所需的流量。有關疑難解答步驟，請參閱本節的前一章。

1. 沒有SNAT的負載平衡器： 在此示例中，消費者EPG Web和提供商EPG App與負載均衡器服務圖存在合約。App EPG中的終端是與負載均衡器上的VIP關聯的實際伺服器。為提供商到使用者通訊方向啟用了PBR到負載平衡器。
2. 不帶SNAT的防火牆和負載均衡器： 在此示例中，消費者EPG Web和提供商EPG App與防火牆和負載均衡器服務圖存在合約。App EPG中的終端是與負載均衡器上的VIP關聯的實際伺服器。兩個方向都啟用PBR到防火牆。為提供商到使用者通訊方向啟用了PBR到負載平衡器。
3. 共用服務（VRF間合約）： 在本示例中，消費者EPG Web和提供商EPG App與防火牆服務圖存在合約。EPG Web和EPG App位於不同的VRF中。兩個方向都啟用PBR到防火牆。防火牆位於VRF之間。

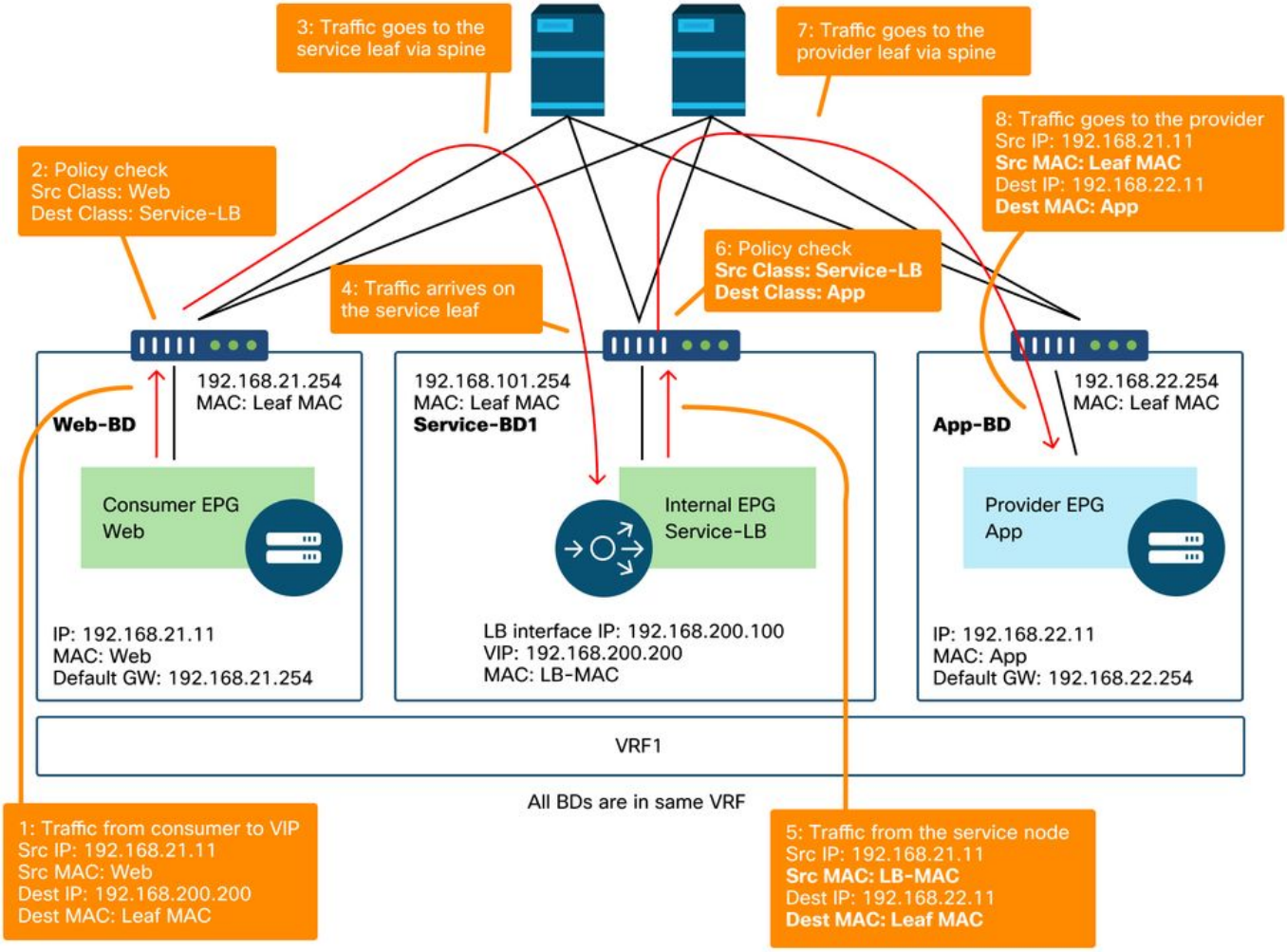
1.無SNAT的負載均衡器

PBR可以部署為雙向PBR或單向PBR。單向PBR的一個使用案例是不使用源網路地址轉換(NAT)的負載平衡器整合。 如果負載平衡器執行源NAT，則不需要PBR。

流量路徑示例

下圖顯示從消費者EPG Web到提供商EPG應用有兩個連線的傳入流量的示例：一個是從消費者EPG Web中的終結點到負載平衡器VIP，另一個是從負載平衡器到提供程式EPG應用中的終結點。由於傳入流量將發往VIP，因此，如果VIP可訪問，流量將到達負載均衡器（不帶PBR）。負載均衡器將目標IP更改為與VIP關聯的EPG應用中的一個終端，但不會轉換源IP。因此，流量將轉至提供商端點。

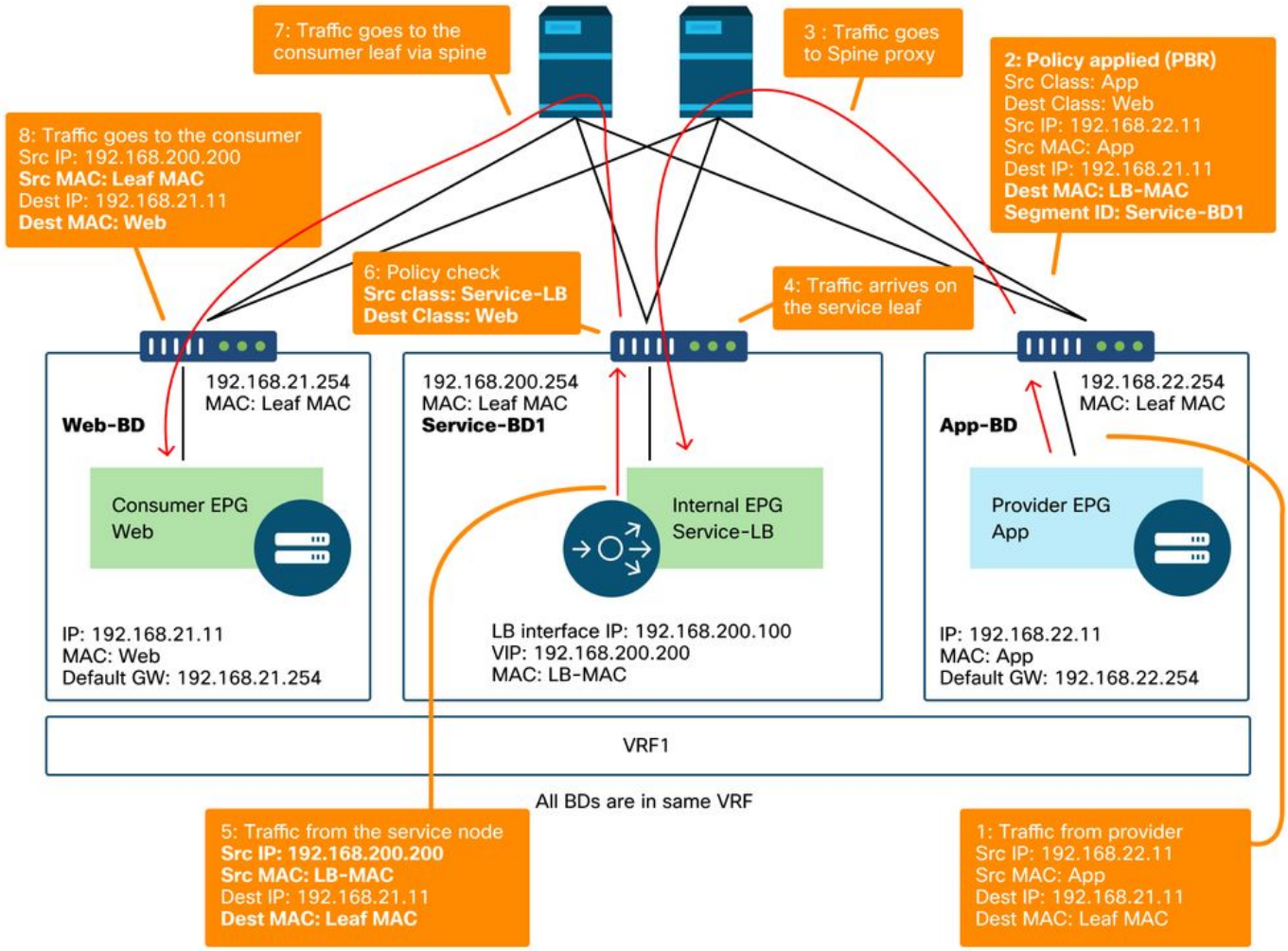
無SNAT的負載均衡器轉發路徑示例 — 消費者到VIP以及負載均衡器到提供商而無PBR



下圖說明了從提供商EPG應用到消費者EPG網路的返回流量。由於返回流量以原始源IP為目的地，因此PBR需要使返回流量返回到負載均衡器。否則，使用者終端會接收其中來源IP是提供者終端而不是VIP的流量。此類流量將被丟棄，因為即使中間網路（如ACI交換矩陣）將資料包轉發回使用者端點，使用者端點也沒有向提供商端點發起流量。

從提供商端點到使用者端點的流量重定向到負載均衡器後，負載均衡器會將源IP更改為VIP。然後，流量從負載均衡器返回，並且流量返回到使用者端點。

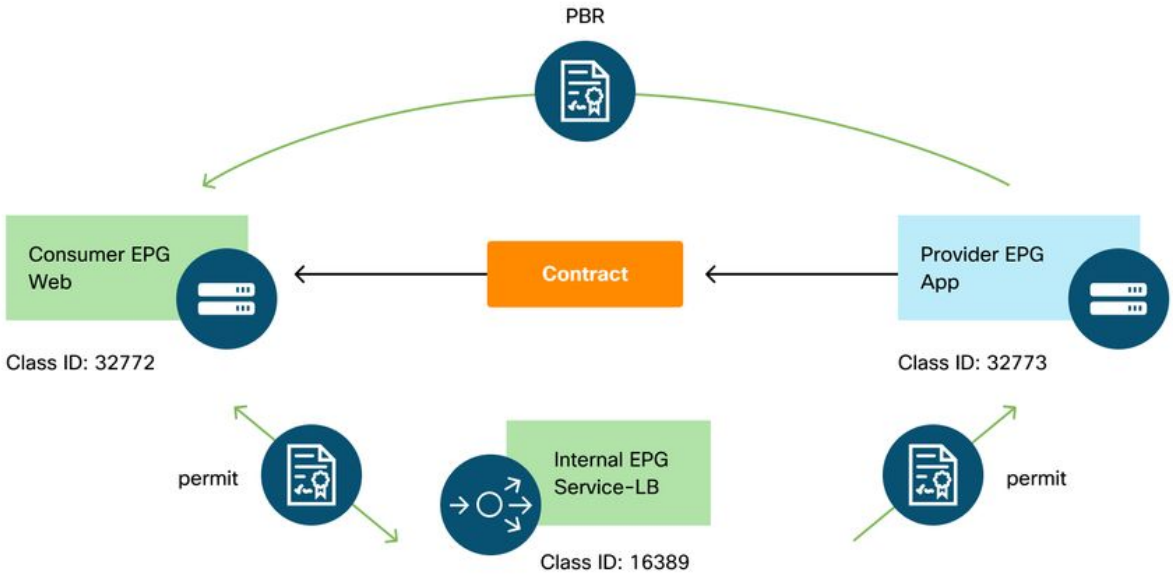
沒有SNAT的負載平衡器轉發路徑示例 — 使用PBR向使用者提供程式的示例



在枝葉節點上程式設計的策略。

下圖和下方的「show zoning-rule」輸出描述了服務圖部署後的分割槽規則。在本示例中，允許從pcTag 32772(Web)到pcTag 16389(Service-LB)的流量，允許從pcTag 16389(Service-LB)到pcTag 32773(App)的流量，並且從pcTag 32773(App)到pcTag 32772(Web)的流量重定向到「destgrp-31」（負載均衡器）。

服務圖部署後的分割槽規則 — 不帶SNAT的負載平衡器

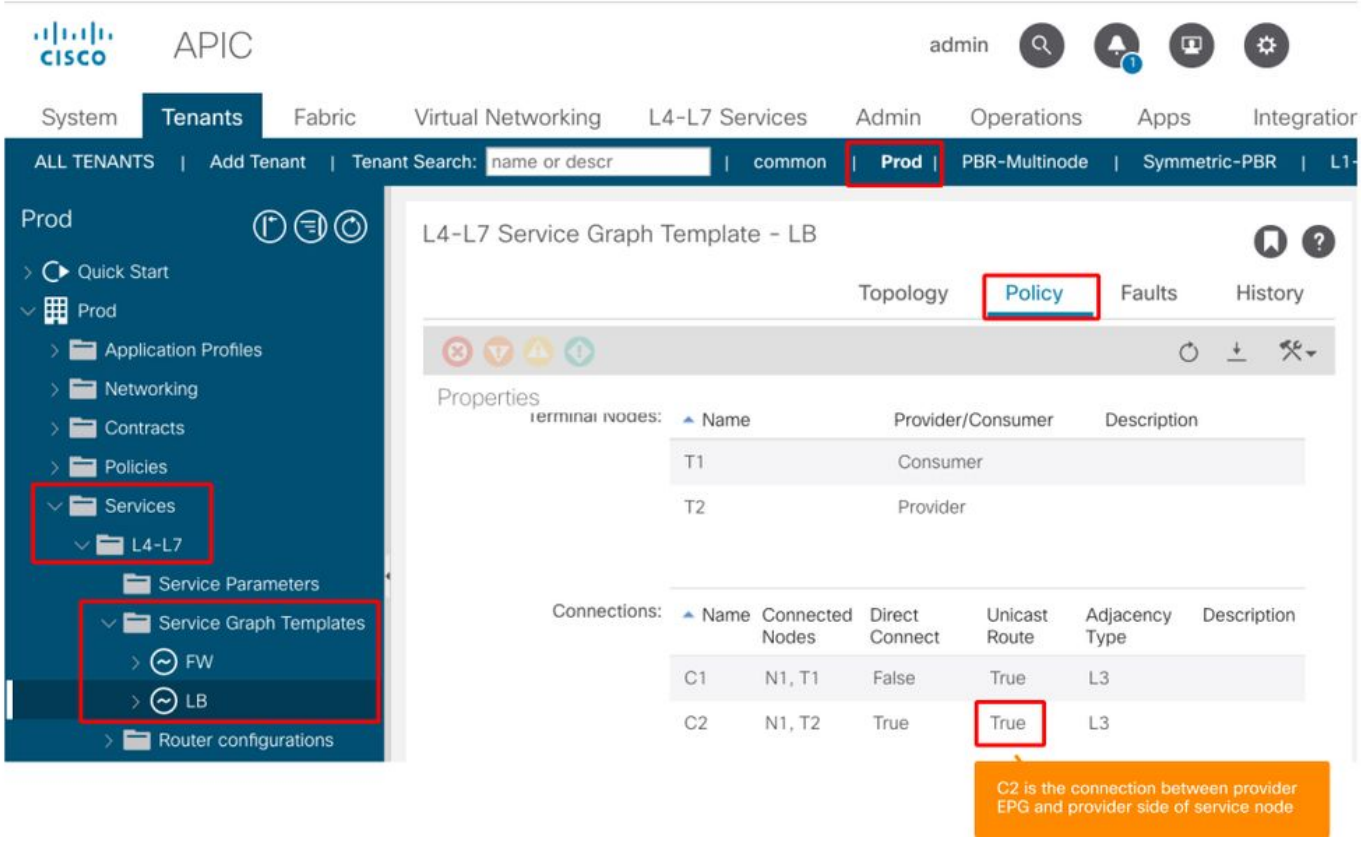


Source	Destination	Action
32772	16389	permit
16389	32773	permit
32773	32772	PBR to the service node
16389	32772	permit

```
Pod1-Leaf1# show zoning-rule scope 2752513
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |
Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
|   4248  | 16389  | 32773  | default  |    uni-dir     | enabled | 2752513 |      |
permit      |    src_dst_any(9)    |
|   4143  | 32773  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |
redir(destgrp-31) |    fully_qual(7)     |
|   4234  | 16389  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      |
permit      |    fully_qual(7)     |
|   4133  | 32772  | 16389  |    8     |     bi-dir     | enabled | 2752513 |      |
permit      |    fully_qual(7)     |
...
```

預設情況下，不會將提供程式EPG(pcTag 32773)到Service-LB(pcTag 16389)的允許規則程式設計。要允許它們之間進行雙向通訊，以便進行從負載平衡器到提供程式端點的運行狀況檢查，必須將連線上的直接連線選項設定為True。位置為「Tenant > L4-L7 > Service Graph Templates > Policy」。 預設值為False。

設定直接連線選項



如下所述，它將為提供商EPG(32773)新增允許規則到Service-LB(16389)。

```
Pod1-Leaf1# show zoning-rule scope 2752513
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |
Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
|   4248  | 16389  | 32773  | default  |     bi-dir     | enabled | 2752513 |      |
permit      |    src_dst_any(9)    |
|   4143  | 32773  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |
redir(destgrp-31) |    fully_qual(7)     |
|   4234  | 16389  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      |
permit      |    fully_qual(7)     |
|   4133  | 32772  | 16389  |    8     |     bi-dir     | enabled | 2752513 |      |
permit      |    fully_qual(7)     |
|   4214  | 32773  | 16389  | default  | uni-dir-ignore | enabled | 2752513 |      |
permit      |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
```

2.流量示例 — 不帶SNAT的防火牆和負載均衡器

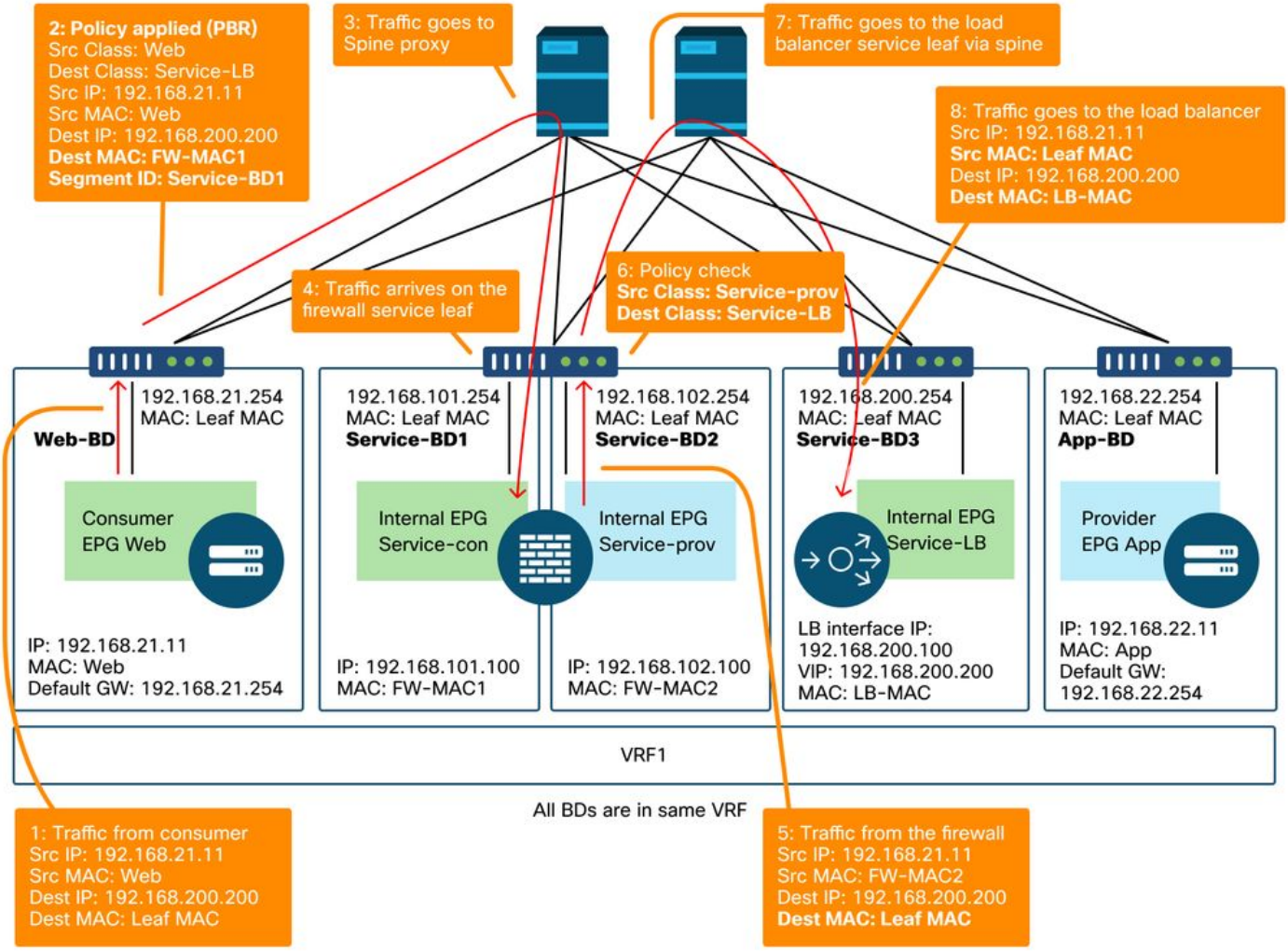
PBR可以部署為服務圖中的多個服務功能，例如防火牆作為第一節點，負載平衡器作為第二節點。

流量路徑示例

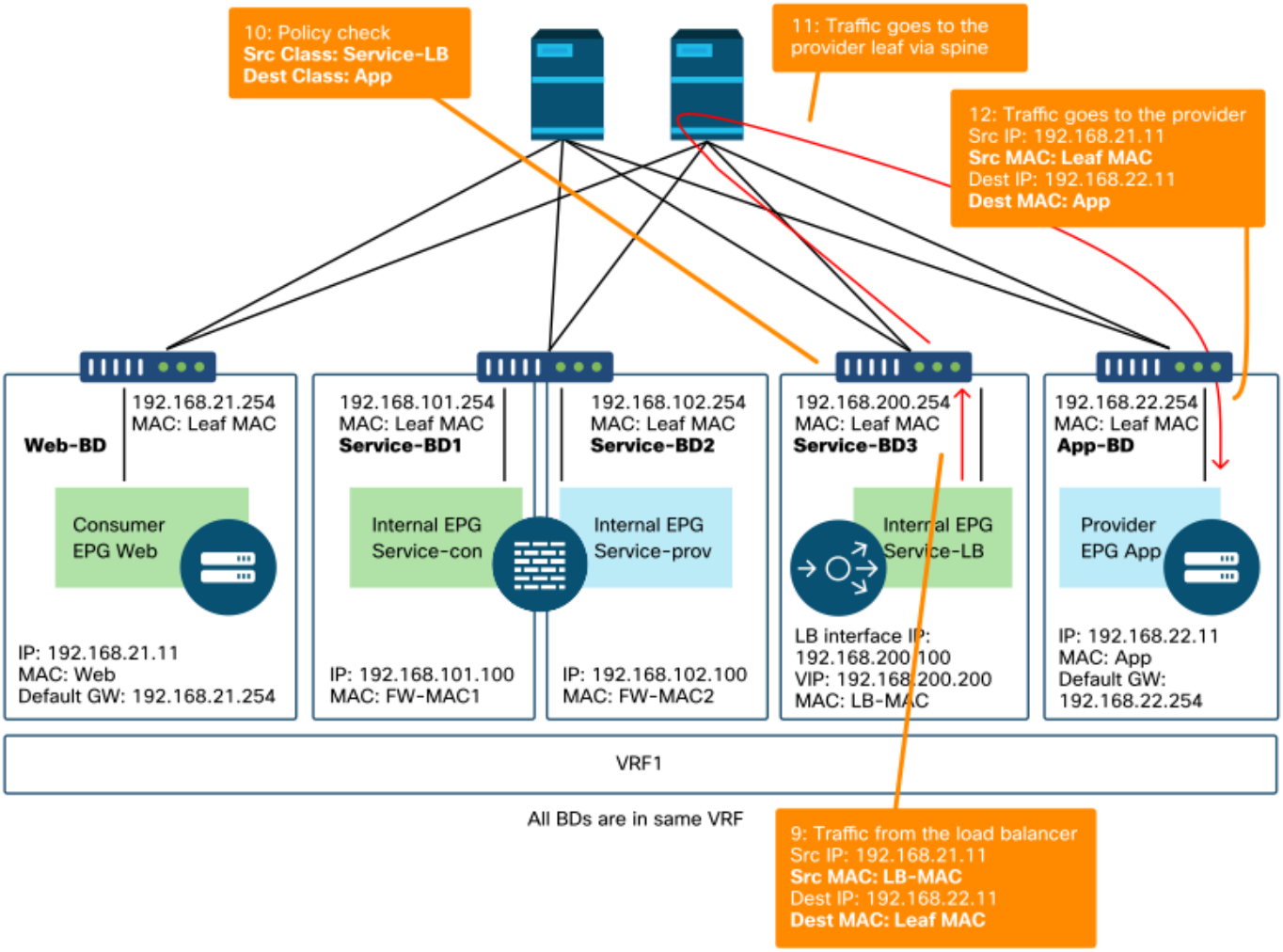
下圖顯示從消費者EPG Web到提供商EPG應用有兩個連線的傳入流量的示例：一個是從消費者EPG Web中的終結點通過防火牆連線到負載均衡器VIP，另一個是從負載均衡器連線到提供商EPG應用中的終結點。目的地為VIP的傳入流量將重定向到防火牆，然後轉到沒有PBR的負載均衡器。負載均衡器將目標IP更改為與該VIP關聯的App EPG中的一個終端，但不會轉換源IP。然後

，流量流向提供商端點。

無SNAT的防火牆和負載均衡器轉發路徑示例 — 消費者到VIP和負載均衡器到提供商



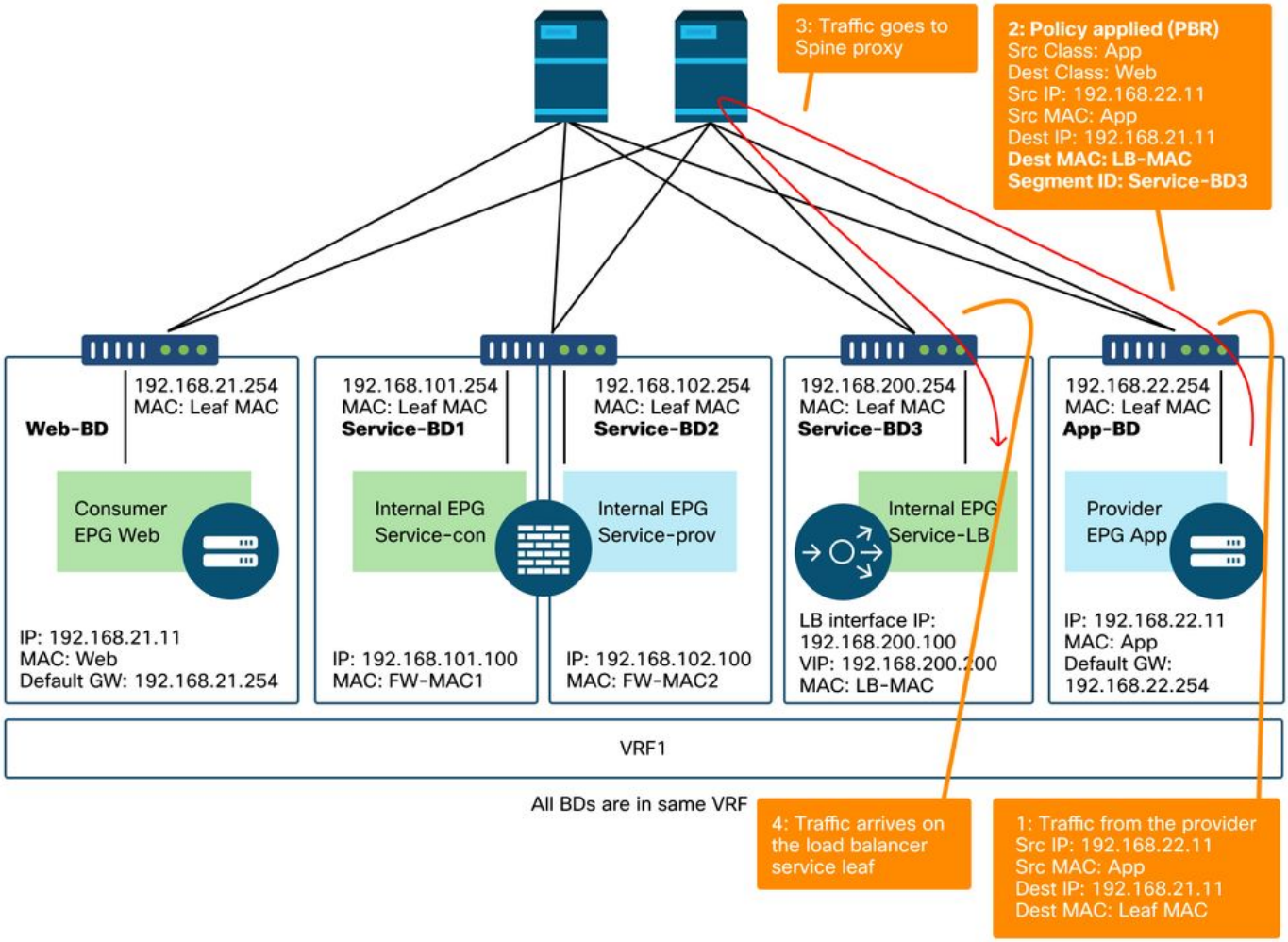
無SNAT的防火牆和負載均衡器轉發路徑示例 — 消費者對VIP和負載均衡器對提供商（續）

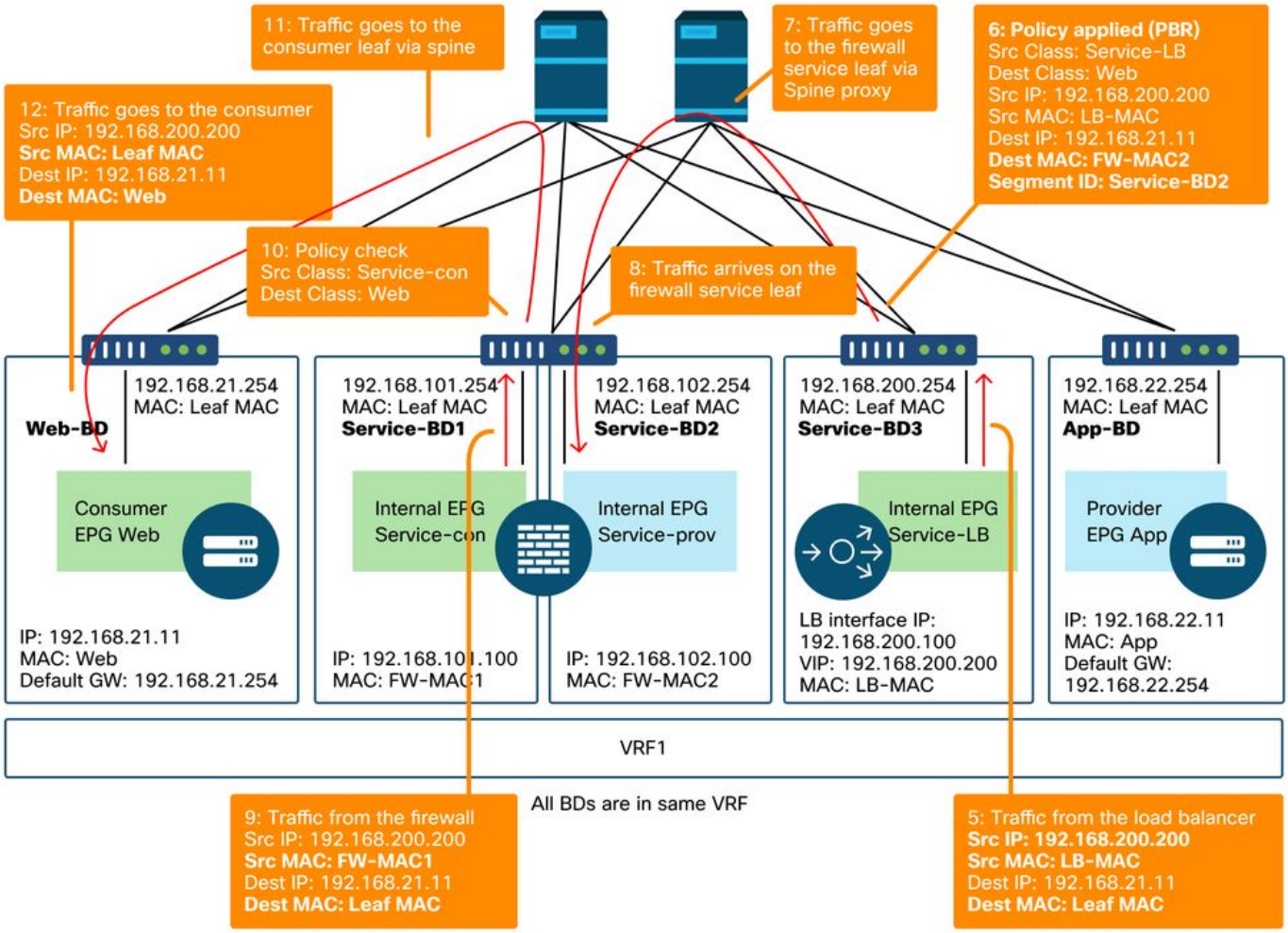


下圖說明了從提供商EPG應用到消費者EPG網路的返回流量。由於返回流量以原始源IP為目的地，因此PBR需要使返回流量返回到負載均衡器。

從提供商端點到使用者端點的流量重定向到負載均衡器後，負載均衡器會將源IP更改為VIP。流量從負載均衡器返回並重新定向到防火牆。然後，流量從防火牆返回並返回到使用者端點。

無SNAT的防火牆和負載均衡器轉發路徑示例 — 提供商到消費者

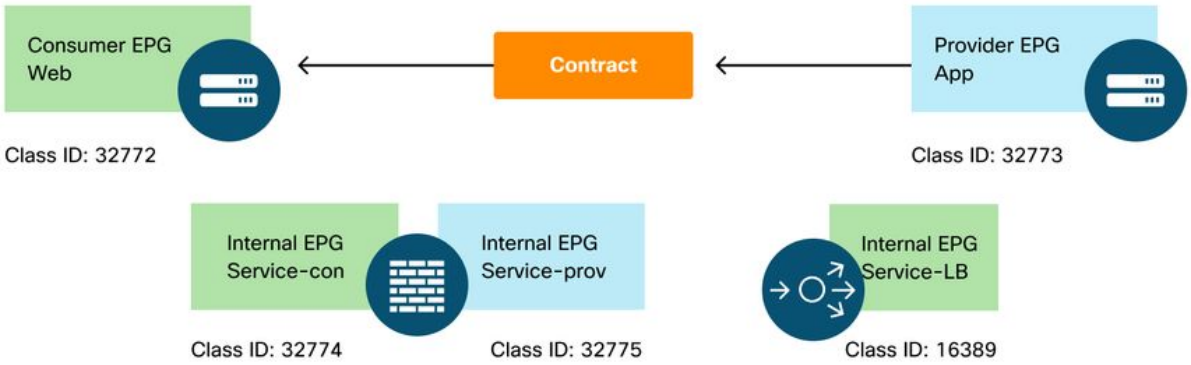

3: Traffic goes to Spine proxy
2: Policy applied (PBR)
Src Class: App
Dest Class: Web
Src IP: 192.168.22.11
Src MAC: App
Dest IP: 192.168.21.11
Dest MAC: LB-MAC
Segment ID: Service-BD3
192.168.21.254
MAC: Leaf MAC
Web-BD
Consumer EPG Web
IP: 192.168.21.11
MAC: Web
Default GW: 192.168.21.254
192.168.101.254
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



在枝葉節點上程式設計的策略

下圖和下圖所示的「show zoning-rule」輸出描述了服務圖部署後的分割槽規則。在本示例中，從pcTag 32772(Web)到pcTag 16389(Service-LB)的流量重定向到「destgrp-32」（防火牆的使用者端），從pcTag 32773(App)到pcTag 32772(Web)的流量重定向到「destgrp-33」（負載均衡器），從pcTag 16389(Service-LB)到pcTag 32772(Web)的流量重定向到「destgrp-34」（防火牆的提供商端）。

Zoning-rules after Service Graph deployment — 不帶SNAT的防火牆和負載均衡器



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

```
Pod1-Leaf1# show zoning-rule scope 2752513
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
| Rule ID | SrcEPG | DstEPG | FilterID |      Dir       |  operSt |  Scope  | Name |
Action      |       Priority       |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
|   4236  | 32772  | 16389  |    8     |     bi-dir     | enabled | 2752513 |      |
redir(destgrp-32) |    fully_qual(7)     |
|   4143  | 32773  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |
redir(destgrp-33) |    fully_qual(7)     |
|   4171  | 16389  | 32773  | default  |     bi-dir     | enabled | 2752513 |      |
permit      |    src_dst_any(9)    |
|   4248  | 16389  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      |
redir(destgrp-34) |    fully_qual(7)     |
|   4214  | 32774  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |
permit      |    fully_qual(7)     |
|   4244  | 32775  | 16389  | default  |    uni-dir     | enabled | 2752513 |      |
permit      |    src_dst_any(9)    |
|   4153  | 32773  | 16389  | default  | uni-dir-ignore | enabled | 2752513 |      |
permit      |    src_dst_any(9)    |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
-------+----------------------+
```

在上方示例中，在負載均衡器的提供商端與提供商EPG之間的連線上，Direct Connect選項設定為「True」。必須啟用它才能進行從負載平衡器到提供程式終結點的運行狀況檢查。位置為「Tenant > L4-L7 > Service Graph Templates > Policy」。 請參閱圖「設定直接連線選項」。

3.共用服務（VRF間合約）

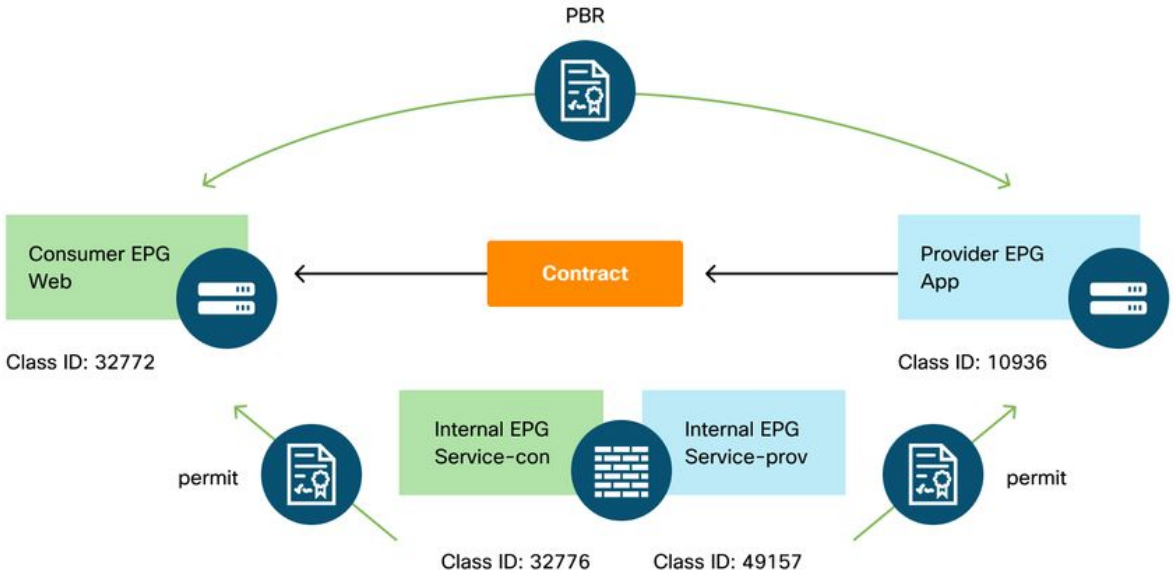
可以在VRF間合約中啟用PBR。本節介紹如何在EPG到EPG間VRF合約的情況下對分割槽規則進行程式設計。

在枝葉節點上程式設計的策略

在從EPG到EPG的VRF間合約中，策略始終在消費者VRF中實施。因此，在使用者VRF上發生重新導向。有關其他組合，請參閱表「在何處實施策略？」 在「轉發」部分。

下圖和下方的「show zoning-rule」輸出描述了服務圖部署後的分割槽規則。在本示例中，從pcTag 32772(Web)到pcTag 10936(App)的流量重定向到「destgrp-36」（服務節點的消費者端），從pcTag 10936(App)到pcTag 32772(Web)的流量重定向到「destgrp-35」（服務節點的提供商端）。 兩者都在作為使用者VRF的VRF1中實施。VRF1中允許從pcTag 32776（防火牆的使用者端）到pcTag 32772(Web)的流量。

服務圖部署後的分割槽規則 — VRF間合約



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      |        Priority        |
+---------+--------+--------+----------+----------------+---------+---------+------+-----------
```

```
-------+------------------------+
|   4191  | 32776  | 32772  |    9     |    uni-dir     | enabled | 2752513 |      |
permit      |     fully_qual(7)      |
|   4143  | 10936  | 32772  |    9     | uni-dir-ignore | enabled | 2752513 |      |
redir(destgrp-35) |     fully_qual(7)      |
|   4136  | 32772  | 10936  |    8     |     bi-dir     | enabled | 2752513 |      |
redir(destgrp-36) |     fully_qual(7)      |
+---------+--------+--------+----------+----------------+---------+---------+------+------------
-------+------------------------+
```

VRF2中允許從pcTag 49157（防火牆的提供商端）到pcTag 10936（應用）的流量，因為兩者都在VRF2中。

```
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(9)    |
+---------+--------+--------+----------+---------+---------+---------+------+----------+--------
--------------+
```

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。